Hans Ruegg

Matemática activa

para familias educadoras y escuelas alternativas

Secundaria II *(Pre-Universitario)*

Bloque V (Teoría de números)

OBRA EN PROGRESO

Esta edición es una parte de una obra mayor. Decidí publicarla de esta manera, porque no sé si me será posible completar la obra entera. Es una edición provisional:
- No está revisada completamente por errores de tipeo, de matemática, y de diseño.
- Puede contener unos vacíos que se rellenarán recién en la edición definitiva.
- La paginación no coincidirá con la edición definitiva.

Está planeado que la edición definitiva contenga los siguientes bloques:
Algebra; Geometría; Trigonometría; Combinatoria y temas diversos; Teoría de números; Geometría vectorial; Números complejos.

Actualización: Marzo de 2024

Contacto por internet para consultas:
https://educacionCristianaAlternativa.wordpress.com/libros-de-matematica-activa/

Unas demostraciones en video de los métodos de la matemática activa se encuentran en:
http://www.youtube.com/user/educadorDiferente

Bloque IV: Teoría de números

La teoría de números es un campo ideal para entrenar el razonamiento y la capacidad de pensar matemáticamente. Muchos de sus problemas se pueden plantear de una manera sencilla, y no requieren conocimientos especializados para resolverlos. Sin embargo, pueden requerir mucho ingenio para encontrar el camino hacia la solución.

Entonces, si tu deseo es fortalecer los "músculos" de tu razonamiento, y si te gustan los problemas intricados, adéntrate en este bloque. De paso encontrarás diversas curiosidades históricas y matemáticas; y acompañarás a Sherlock Numbers en una nueva aventura en Aritmenia, el país donde los números son personas.

Por el otro lado, si tu única meta es aprobar algún examen de egreso o de admisión, entonces probablemente no necesitas este bloque. La mayoría de las instituciones del sistema tradicional no requieren conocimientos de los temas que se tratan aquí. En cuanto a la teoría de números, suelen contentarse con reglas de divisibilidad, propiedades de los múltiplos y divisores y factores primos, y sistemas de numeración en otras bases – temas que ya tratamos en *Secundaria I*. Solamente para entrar en carreras especializadas en matemática, ciencias o ingenierías, algunas universidades requieren conocimientos de algunos temas de este bloque, tales como la resolución de ecuaciones diofánticas, la función Φ de Euler, y la congruencia modular en potencias; o sea aproximadamente la primera mitad de este bloque.

Contenido

Unidad N 1 - Números defectivos, perfectos, y abundantes

Prerrequisitos:
- Suma de los divisores de un número *(Secundaria I, Unidad 36).*

Introducción

En Secundaria I hemos aprendido el símbolo **σ** (sigma) para la **suma de los divisores de un número**. Por ejemplo σ (14) = 24, porque 1+2+7+14 = 24. (Repasa cómo calcular fácilmente σ (***n***).)
El tema de esta Unidad se remonta a los antiguos griegos, particularmente los seguidores de Pitágoras. Ellos atribuyeron toda clase de propiedades a los números. Un criterio que usaron, es la suma de los divisores de un número, ***menos el número mismo***. O sea, para ellos, la propiedad decisiva no era σ(***n***), sino σ(***n***) – ***n***. Eso se llama también la suma de los ***divisores propios*** de ***n***.
Ellos definieron las siguientes clases de números:

Números perfectos. Son números que son iguales a la suma de sus divisores propios.
O sea, σ(***n***) – ***n*** = ***n***, lo que equivale a σ(***n***) = 2***n***.
Por ejemplo 28 es un número perfecto, porque
1+2+4+7+14 = 28.

Números defectivos. Son números cuya suma de divisores propios es ***menor*** que el número mismo.
O sea, σ(***n***) – ***n*** < ***n.***
Por ejemplo 15 es un número defectivo, porque
1+3+5 = 9 < 15.

Números abundantes. Son números cuya suma de divisores propios es ***mayor*** que el número mismo.
O sea, σ(***n***) – ***n*** > ***n.***
Por ejemplo 30 es un número abundante, porque
1+2+3+5+6+10+15 = 42 > 30.

Números amigables. Son pares de números donde cada uno es la suma de los divisores propios del otro.
Por ejemplo 220 y 284 son números amigables, porque
1+2+4+5+10+11+20+22+44+55+110 = 284
1+2+4+71+142 = 220

En tiempos modernos, los matemáticos han ampliado estas clases de números por algunos más. Por ejemplo:

Números doblemente perfectos. Son números cuya suma de divisores propios es ***el doble*** del número mismo.
O sea, σ(***n***) – ***n*** = 2***n***, lo que equivale a σ(***n***) = 3***n***.
Por ejemplo 120 es un número doblemente perfecto, porque σ(120) – 120 = 240. (Verifícalo tú.)

Números sociables. Son conjuntos de varios números, donde cada uno es la suma de los divisores propios del siguiente, hasta el último que es la suma de los divisores propios del primero.
Por ejemplo, los siguientes números son sociables entre sí (en este orden):
12496, 14288, 15472, 14536, 14264.

Para practicar:

- Determina si los siguientes números son defectivos, perfectos o abundantes:
6; 7; 9; 12; 75; 100; 496; 999.

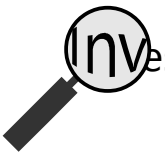
- Verifica que la siguiente afirmación es verdadera:
Sea $n = p^a \cdot m$, con p primo y m, p PESI. (O sea, hemos sacado aparte todos los factores p.) Entonces:

$$\sigma(n) = (1+p+p^2+\ldots+p^a) \cdot \sigma(m)$$

Sherlock Numbers y los cuatro residuos

I

Este caso sucedió en el país de Aritmenia, donde los números son personajes. Una mañana, un visitante tocó la puerta del detective privado Sherlock Numbers. Era un hombre pequeño con una cara asustada. "Me escapé", fue lo primero que dijo después de tomar asiento.
"Usted se escapó", repitió el detective, y echó una mirada interrogativa a su visitante.
– "Fue un lugar tétrico. Pienso que alguien debería investigarlo."
– "¿Investigar qué?"
– "Tenían a un muchacho grande allí dentro. Un primo, según dijeron. Le estaban aplicando unas pruebas de división. Yo soy un resultado de eso. Solamente un residuo."
– Sherlock Numbers sintió ganas de decir: "Eso ya lo noté." Pero inmediatamente se dio cuenta de que eso hubiera sido muy insensible. Ante él se encontraba una persona en necesidad de ayuda, y era su deber ayudarle. Así que dijo: "Entiendo. ¿Usted ya me dijo su nombre?"
– "Ocho."
– "Bien, señor Ocho. ¿Entonces usted tuvo la impresión de que algo ilegal sucedía allí?"



1) ¿Existen números abundantes impares?
Si existen, ¿cuál es el menor de ellos?
Si no existen, demuestra por qué no.

2) ¿Existen números abundantes sucesivos?
Si existen, ¿cuál es el menor par de números abundantes sucesivos?
Si no existen, demuestra por qué no.

3) Demuestra o refuta:
a) Todo múltiplo de un número abundante es abundante.
b) Todo múltiplo de un número perfecto, excepto el número mismo, es abundante.

***4)** Investiga los números perfectos: ¿Qué propiedades tienen? ¿Como se pueden encontrar números perfectos de manera sistemática?

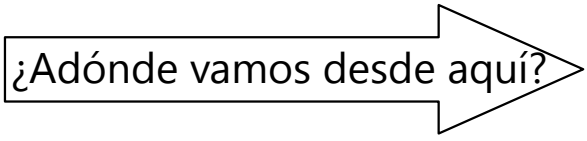
***5)** Investiga números "doblemente perfectos". Ya hemos visto que 120 es uno de ellos. ¿Cómo se pueden encontrar otros números "doblemente perfectos"?

****6)** Un problema sin resolver: ***Sucesiones de sumas de divisores***
Comienza con cualquier número ***n***. Calcula la suma de sus divisores propios. Del resultado, calcula otra vez la suma de sus divisores propios; y así sucesivamente. Por ejemplo, empezando con 66, resulta la siguiente sucesión:
66, 78, 90, 144, 259, 45, 33, 15, 9, 4, 3, 1.
Con la gran mayoría de los números, la secuencia llega finalmente al 1.
Con unos pocos números, la secuencia es periódica; o sea, vuelve al número inicial. Ese es el caso de los "números amistosos" y de los "números sociables". (¡Es bastante difícil encontrar números sociables!).
Y finalmente, queda la pregunta abierta: ¿Existe una tal secuencia que crece sin límite? O sea, que nunca llega al 1, ni es periódica?

****7)** Otro problema sin resolver:
¿Existen números perfectos impares? Y si existen, ¿cómo se pueden encontrar?
(Este es un problema "clásico" que muchos matemáticos intentaron resolver y aportaron diversas pautas, pero nadie llegó a una respuesta definitiva. La mayoría conjeturan que tales números no existen. Y se sabe que en el caso que existen, tienen que ser inmensos – con cientos de cifras o aun más.)

Sherlock Numbers y los cuatro residuos (continuación)

– "Casi seguro. Parece que al muchacho lo habían secuestrado. Lo vi de lejos no más. Pero noté que no quiso estar en ese lugar."
– "¿Ese lugar ...?"
– "Usted sabe, donde hacen toda clase de operaciones. Pero todo escondido."
– "O sea, ¿algo como un laboratorio clandestino?"
– "Bueno, sí, supongo que algo así."
– "¿Y dónde se encuentra ese lugar?"
– "De verdad no lo volvería a encontrar. Me fui de noche, por la parte trasera, y no recuerdo bien las calles. Después de mucho tiempo llegué a una avenida y pude tomar un taxi."
– "Eso será difícil entonces. ¿Qué más me puede decir acerca de la identidad de ese muchacho grande?"
– "No sé nada más, lo siento mucho."
– "¿Y acerca de las operaciones que hicieron con él?"
– "No mucho. Solamente me enteré de que dos otros residuos escaparon también."
– "¿Conoce sus identidades?"
– "Uno de ellos se llamaba Seis. Con él me vi una vez. Me dijo que había salido de una división entre 7. Del otro solamente escuché decir que logró escapar a la zona de Tríplicos."
– "Hm. ¿Y acerca de la procedencia de usted mismo?"
– "El divisor se llamaba Once."
– "¿Y el cociente?"
– "No sé nada de él. Nunca lo conocí."
– "Son pocas pistas para comenzar una investigación. Me gustaría encontrar a ese tercer residuo y saber más de él. ¿Seguro que no recuerda nada más acerca de su historia, o su ubicación?"
– "Como le dije, nunca lo conocí."
– "Entonces el otro, el señor Seis – ¿usted cree que podrá ubicarlo?"
– "Creo que era amigo del otro, y que planeaban escapar juntos. Quizás se han ido juntos a Tríplicos."
– "Bueno, vamos allá. ¿Usted estaría dispuesto a acompañarme?"



Se recomienda trabajar las siguientes cuatro Unidades *(N2 a N5)* en su orden, porque siguen una secuencia lógica. Las que siguen después, son opcionales, y se pueden trabajar en cualquier orden.

Unidad N 2 - División modular, y otros temas de congruencia modular

Prerrequisitos:
- Concepto de la congruencia modular *(Secundaria I, Unidad 31).*
- Ecuaciones diofánticas lineales *(Secundaria I, Unidad 35).*

Tablas de multiplicación modular

Volvamos a este tema que ya hemos empezado a tratar en Secundaria I. Observemos la tabla de multiplicación (mod.12):

1	2	3	4	5	6	7	8	9	10	11	0
2	4	6	8	10	0	2	4	6	8	10	0
3	6	9	0	3	6	9	0	3	6	9	0
4	8	0	4	8	0	4	8	0	4	8	0
5	10	3	8	1	6	11	4	9	2	7	0
6	0	6	0	6	0	6	0	6	0	6	0
7	2	9	4	11	6	1	8	3	10	5	0
8	4	0	8	4	0	8	4	0	8	4	0
9	6	3	0	9	6	3	0	9	6	3	0
10	8	6	4	2	0	10	8	6	4	2	0
11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0	0

Algunas filas contienen todos los números de 0 a 11. (¿Cuáles son?) - En otras se repite una secuencia de pocos números periódicamente. ¿A qué se debe eso?
Tomamos como ejemplo la tabla del 3. En la cuarta posición aparece un cero, porque $3\cdot4 = 12 \equiv 0$ (mod.12). Y a partir de allí se repite todo de nuevo: 3, 6, 9, ...
Eso sucede en la tabla de cada número que tiene algún divisor en común con 12: $2\cdot6 = 12$, $3\cdot4 = 12$, $4\cdot3 = 12$, $6\cdot2 = 12$, $8\cdot3 = 24 (\equiv0)$, $9\cdot4 = 36 (\equiv0)$, $10\cdot6 = 60 (\equiv0)$.
O sea, las tablas donde aparecen todos los números de 0 a 11, son las que son PESI con 12.
Podemos generalizarlo:

Si a y m son PESI, entonces los múltiplos de a (mod. m) abarcan todos los residuos posibles de 0 a m–1.

En otras palabras:
En este caso, los múltiplos a, $2a$, $3a$, ... ma (mod. m) son una *permutación* de los números de 0 a m–1.

Demostración:
Sean a, m PESI. ¿Pueden existir dos números b, c, ambos menores a m, de manera que $ab \equiv ac$ (mod.m) ? (Suponemos que $b > c$.)
En este caso, $ab - ac = km$ (por la definición de la congruencia modular), o sea $a(b - c) = km$.
Según las condiciones iniciales, a y m son PESI. Entonces, para que $a(b - c)$ sea un múltiplo de m, $b - c$ tiene que ser un múltiplo de m.
Pero eso contradice las condiciones iniciales: Si b, c son ambos menores a m, también $b - c < m$, y por tanto $b - c$ no puede ser un múltiplo de m.
Entonces, entre los múltiplos 0, a, $2a$, $3a$, ... $(m–1)a$ no pueden existir dos que sean congruentes entre sí (mod.m). Todos tienen que ser distintos, y por tanto aparece entre ellos cada residuo de 0 a m–1 exactamente una vez. Eso concluye la demostración.

El razonamiento anterior nos ayuda también a analizar la situación donde m, a no son PESI. En este caso, definimos que D = MCD(a, m). Ahora, la ecuación anterior se puede dividir entre D, y tenemos asegurado que las fracciones que aparecen, seguirán equivalentes a números enteros:

$$\frac{a}{D}(b-c) = k\frac{m}{D}$$

Ahora se requiere solamente que ($b - c$) sea un múltiplo de $\frac{m}{D}$, y éso sí es posible. Se repite un "período" de longitud $\frac{m}{D}$, D veces.

Para practicar:
1.a) ¿Cuántos resultados diferentes puede tener la multiplicación $18k$, (mod.30)?
b) ¿y la multiplicación $686k$ (mod.896)?
2.a) ¿Cuántas soluciones tiene la ecuación $44x \equiv 99$ (mod.143), si adicionalmente $0 \le x < 143$?
b) ¿y para $56x \equiv 100$ (mod.208), si $0 \le x < 208$?

Sherlock Numbers y los cuatro residuos

II

No era fácil orientarse en las calles de Tríplicos. No se cruzaban en ángulos rectos, como los dos extraños estaban acostumbrados. La mayoría de las intersecciones tenían ángulos de 60º, ó de 120º. Pero por fin lograron encontrar una calle donde la gente les confirmaba que hace pocas semanas habían llegado dos nuevos inquilinos; dos residuos pequeños. Una señora les indicó la casa donde vivían.
Un desconocido les abrió la puerta. Sherlock Numbers, notando el desconcierto de su acompañante, se adelantó: "Somos amigos de Seis. ¿Se encuentra?"

División modular

Los ejemplos anteriores nos muestran que la "división modular" no es una operación bien definida. Es resolver ecuaciones como $8\boldsymbol{x} \equiv 5 \pmod{13}$ - eso se podría escribir como $\boldsymbol{x} = \frac{5}{8} \pmod{13}$, pero no es usual escribirlo así. Se trata de ecuaciones diofánticas, y sabemos que ésas pueden tener muchas soluciones, o ninguna. Examinemos los diversos casos:

El ejemplo anterior se puede solucionar probando. Avanzamos en la tabla del 8, hasta encontrar un número ≡ 5 (mod.13). O avanzamos en la sucesión de los números ≡ 5 (mod.13), hasta encontrar uno que es múltiplo de 8. Eso es un poco más eficaz, porque avanzamos en pasos mayores.
Comenzamos entonces con 13+5 = 18.
Ya que todos los múltiplos de 8 son pares, los miembros impares de esa sucesión no nos interesan. Podemos entonces avanzar directamente en pasos de 26: 18, 44, 70, 96 – ya lo tenemos. $8\boldsymbol{x} = 96$; $\boldsymbol{x} = 12$.
Podríamos decir entonces que $\frac{5}{8} \equiv 12 \pmod{13}$.
En este caso hay una única solución, porque 8 y 13 son PESI. Hemos visto antes que en este caso, cada resultado de la multiplicación es "único".
Lo podemos explicar también con el teorema chino de los residuos *(Unidad N 3)*. Éste nos dice que si 8 y 13 son PESI, entonces en el intervalo [1; 8·13] existe un único número que es ≡ 5 (mod.13) y ≡ 0 (mod.8).

¿Cómo es en el caso de que los divisores no son PESI? Por ejemplo, ¿cuál es el equivalente de $\frac{15}{18} \pmod{24}$?
Si intentamos usar el método anterior, encontramos: Todos los números ≡ 15 (mod.24) son impares; pero todos los múltiplos de 18 son pares. No hay solución.
Generalizado: Sea $\boldsymbol{D}$ = MCD ($\boldsymbol{d}$; $\boldsymbol{m}$). Entonces $\frac{\boldsymbol{n}}{\boldsymbol{d}} \pmod{\boldsymbol{m}}$ tiene solución **solamente si *n* es un múltiplo de *D*.** *(Eso fue también el tema de la tarea 2.b) en la sección anterior.)*
Compara la tabla (mod.12) en la sección anterior: Por ejemplo los múltiplos de 8 son todos múltiplos de 4, porque MCD(12; 8) = 4.
Para pensar: *Demuestra* que esta afirmación es cierta.

Ejemplos: *(Estos ejemplos muestran que no hay un único procedimiento a seguir al pie de la letra. A menudo hay posibilidades de simplificar el proceso, que difieren de un caso al otro.)*

A) $38\boldsymbol{x} \equiv 7 \pmod{25}$
Calculando (mod.25), 38 ≡ 13. Así podemos reducir los números un poco: la ecuación es equivalente a:
$13\boldsymbol{x} \equiv 7 \pmod{25}$.
Hay una sola solución, porque 13 y 25 son PESI.
Examinamos los números ≡ 7 (mod.25):
32, 57, 82, ... , 182 = 13 · 14; $\boldsymbol{x} \equiv 14$.

Nota: Con estos números pequeños se puede encontrar la solución, probando. Con números mayores necesitaremos un procedimiento un poco más sistemático. De eso se ocupa el problema de investigación de esta Unidad. Quizás querrás realizar esa investigación ahora, para tener unas herramientas mejores.

B) $6\boldsymbol{x} \equiv 15 \pmod{21}$
MCD(6; 21) = 3; entonces deben existir 3 soluciones.
La ecuación entera se puede "simplificar" con el MCD; entonces tenemos:
$2\boldsymbol{x} \equiv 5 \pmod{7}$
Esta nueva ecuación tiene una única solución: $\boldsymbol{x} \equiv 6$.
Pasamos de regreso a (mod.21): Esta solución se convierte ahora en tres, porque 6 ≡ 13 ≡ 20 (mod.7), pero (mod.21) ésos son diferentes. C.S. = {6; 13; 20}.

C) $58\boldsymbol{x} \equiv 77 \pmod{99}$
58 y 99 son PESI; hay una única solución.
Por el otro lado, observamos que el producto es un múltiplo de 11, porque MCD(77; 99) = 11. Por tanto, también $\boldsymbol{x}$ es un múltiplo de 11.
Definimos $\boldsymbol{x} = 11\boldsymbol{y}$; y simplificamos la ecuación con 11:
$58\boldsymbol{y} \equiv 7 \pmod{9}$
... y reducimos los números (mod.9):
$4\boldsymbol{y} \equiv 7 \pmod{9}$
Fácilmente vemos que $\boldsymbol{y} \equiv 4$; entonces $\boldsymbol{x} \equiv 44$.

D) $0\boldsymbol{x} \equiv 13 \pmod{13}$
Si escribiéramos esto como división, sería una operación prohibida (división entre cero). Pero dijimos al inicio que la "división modular" en realidad no está definida como operación, solamente como la solución de una ecuación diofántica. Esta ecuación equivale a:
$0 \equiv 0 \pmod{13}$,
una identidad que es verdadera para toda $\boldsymbol{x}$. Todo número entero es una solución.

Para practicar:
Resuelve las siguientes ecuaciones:
3) $5\boldsymbol{x} \equiv 6 \pmod{7}$
4) $5\boldsymbol{x} \equiv 1 \pmod{12}$
5) $5\boldsymbol{x} \equiv 4 \pmod{6}$
6) ¿Cuál es el equivalente de 9÷3 (mod.11)?
7) ¿Cuál es el equivalente de 9÷3 (mod.12)?
8) ¿Cuál es el equivalente de 10÷13 (mod.100)?
9) El contenido de 18 cajas iguales de cuadernos se reparte en partes iguales entre 31 estudiantes. Sobran 3 cuadernos. ¿Cuántos había en cada caja?
10) Se construye un muro con 29 ladrillos en cada fila. Los ladrillos vienen en paletas de 90 ladrillos cada una. Al final sobran 11 ladrillos. ¿Cuántas filas de ladrillos tiene el muro?
Resuelve:
11) $58\boldsymbol{x} \equiv 95 \pmod{113}$
12) $91\boldsymbol{x} \equiv 105 \pmod{119}$
13) $998\boldsymbol{x} \equiv 594 \pmod{1001}$

El valor recíproco modular

Si tenemos que resolver varias divisiones modulares con los mismos divisores, nos ahorramos trabajo si primero calculamos el valor recíproco. Recordarás que el valor recíproco es el inverso multiplicativo de un número, y por tanto permite convertir una división en una multiplicación. Eso es lo mismo en la aritmética modular.

Por ejemplo, queremos resolver las ecuaciones:

a) $9\boldsymbol{x} \equiv 13 \pmod{23}$

b) $9\boldsymbol{x} \equiv 5 \pmod{23}$

c) $9\boldsymbol{x} \equiv 11 \pmod{23}$.

Resolvemos primero la ecuación: $9\boldsymbol{r} \equiv 1 \pmod{23}$. Ésta nos da el valor recíproco de 9 (mod.23). Resulta $\boldsymbol{r} = 18$.

Ahora, las soluciones de las ecuaciones anteriores se encuentran multiplicando:

a) $\boldsymbol{x} \equiv 13\boldsymbol{r} \equiv 234 \equiv 4 \pmod{23}$

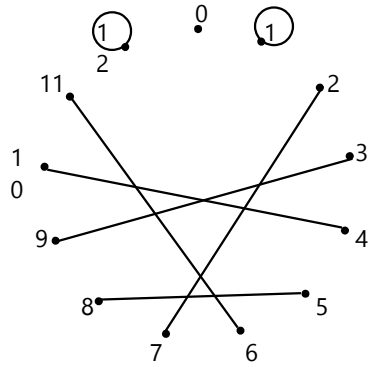
b) $\boldsymbol{x} \equiv 5\boldsymbol{r} \equiv 90 \equiv 21 \pmod{23}$

c) $\boldsymbol{x} \equiv 11\boldsymbol{r} \equiv 198 \equiv 14 \pmod{23}$.

Según la sección anterior, entenderás que el valor recíproco de $\boldsymbol{n} \pmod{\boldsymbol{m}}$ existe solamente si $\boldsymbol{n}$ y $\boldsymbol{m}$ son PESI. Pero si tenemos $D = MCD(\boldsymbol{n}; \boldsymbol{m}) \neq 1$, entonces podemos resolver primero la ecuación $\boldsymbol{nr} \equiv \boldsymbol{D} \pmod{\boldsymbol{m}}$, y después realizar las multiplicaciones de manera correspondiente.

Para hacer (Proyecto gráfico):

Los valores recíprocos vienen en pares: si $\boldsymbol{a}$ es valor recíproco de $\boldsymbol{b}$, también $\boldsymbol{b}$ es valor recíproco de $\boldsymbol{a}$. Podemos graficar los números $\pmod{\boldsymbol{m}}$ como puntos a lo largo de una circunferencia, como un reloj. Después unimos los pares recíprocos con una línea recta. Si un número es su propio recíproco, se dibuja un círculo que regresa al mismo punto. Si un número no tiene recíproco, se queda sin línea. Por ejemplo, éste sería el diagrama de los valores recíprocos (mod.13):



Grafica los valores recíprocos para algunas otras $\boldsymbol{m}$.

Investigación

Ecuaciones diofánticas lineales

En el nivel de Secundaria I ya nos hemos ocupado de ecuaciones diofánticas lineales (Unidad 35). Éstas por lo general no son difíciles. Pero pueden ser problemáticas cuando contienen números grandes y no hay manera de simplificarlas. En este caso demorarías mucho tiempo con buscar la solución sólo probando. Por ejemplo:

$$\mathbf{2749}\boldsymbol{x} \mathbf{+ 6082 = 8575}\boldsymbol{y}$$

Éste es entonces el desafío de investigación: Encuentra un procedimiento que permite resolver tales ecuaciones diofánticas con números grandes, de una manera relativamente fácil y rápida. Fundamenta por qué funciona tu procedimiento.

Otros problemas

14) ¿Cuántos números hay entre 1000 y 2000 que terminan con 7 y son múltiplos de 13?

15) ¿Cuántos números hay entre 2000 y 3000 que son PESI con 588?

16) ¿Cuántos números naturales existen que al sacar su raíz cuadrada dejan un residuo que es exactamente la décima parte del número?

17) Resuelve: (Ninguna letra significa cero.)

$$\overline{\boldsymbol{ab}}_{\mathbf{12}} \cdot \overline{\boldsymbol{cd}}_{\mathbf{12}} = \overline{\boldsymbol{ce}}_{\mathbf{12}} \cdot \overline{\boldsymbol{bf}}_{\mathbf{12}} = 1000_{\mathbf{12}}$$

Sherlock Numbers y los cuatro residuos (Continuación)

– "¿Amigos? ¿De dónde?", respondió el residuo, desconfiado.

– "Hemos salido del mismo dividendo", dijo ahora Ocho.

– "¿Y si no lo conozco?"

Sherlock Numbers bajó la voz: – "Entiendo que su situación es delicada. Pero no tiene nada que temer de nosotros. Al contrario, hemos venido a ayudarle. Tenga por asegurado que nadie se enterará de ningún detalle por parte de nosotros."

Y Ocho, ahora ya más valiente, añadió: "Seis y yo hemos escapado del mismo lugar. Y él" (señalando al detective) "es un hombre que hace temblar a los delincuentes."

– "No es para tanto", se apresuró Sherlock a decir. Y notó con satisfacción que la tensión en la cara de su interlocutor empezó a disminuir. Después de algún tiempo, éste dijo:

– "Bueno ... la verdad es que Seis se fue, y no sé cuándo volverá, ni si volverá en absoluto. Así que ... temo que no puedo ayudarles mucho."

MCD extendido

PARI provee la palabra clave **gcdext(x, y)**. Esta función devuelve como resultado un vector con tres componentes [***u***, ***v***, ***d***], de manera que ***d*** = MCD(***x***; ***y***), y ***ux*** + ***vy*** = ***d***.
Descubre tú mismo(a) cómo te ayuda esta función a resolver problemas de división modular, y ecuaciones diofánticas lineales. Experimenta ...

Números modulares

En PARI existe un tipo especial de números que se llaman "números modulares". Consisten en dos componentes: el número mismo, y un divisor. Ambos tienen que ser enteros. Juntos definen una clase de residuos, resp. de congruencia modular. Se definen con la palabra clave **Mod(n, m)**.
Por ejemplo, **Mod(4, 7)** significa todos los números que son congruentes con 4, (mod.7).
PARI convierte internamente cada número modular al menor número positivo que cumple la congruencia.
Ejemplos:

```
> a = Mod(469, 10)
%1 = Mod(9, 10)
> b = Mod(-7, 9)
%2 = Mod(2, 9)
```

Con los números modulares se pueden efectuar toda clase de operaciones, y PARI calcula los resultados según las reglas de la aritmética modular. Si la operación deseada no es posible, PARI devuelve un error.
Ejemplo:

```
> Mod(7,10)/3
%3 = Mod(9, 10)
```

Además, existen las siguientes operaciones:

n.mod devuelve el "divisor" de un número modular. Con la variable **a** definida arriba:

```
> a.mod
%4 = 10
```

lift(n) convierte un número modular **n** en un número entero de 0 a **n.mod–1**.

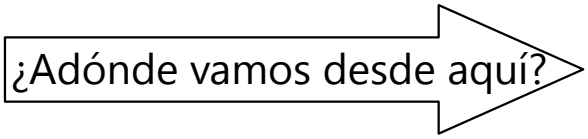
centerlift(n) convierte un número modular **n** en un número entero, usando también números negativos. Por ejemplo:

```
> centerlift(Mod(7,10))
%5 = -3
```

Los números modulares son otra herramienta que permite resolver divisiones modulares y ecuaciones diofánticas en PARI, si los usas de la manera correcta.
Experimenta...

Sherlock Numbers y los cuatro residuos (Continuación)

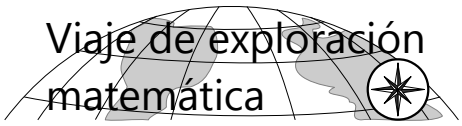
– "Ya nos ayudaría si pudiera contarnos algo acerca de la operación de la cual usted salió. Por ejemplo dónde sucedió eso, y quiénes fueron los operandos."
Finalmente, el residuo entró en suficiente confianza para comentar unos detalles. Se llamaba Doce, y fue el resultado de una división entre 17. Acerca del dividendo, confirmó que era un "muchacho grande", y que los operadores estaban interesados en números primos. Aparte de eso, no pudo aportar más detalles. Igual como Ocho, afirmó que de ninguna manera sería capaz de encontrar el camino de regreso al lugar de donde escapó.
– "Bueno", concluyó el detective, "supongo que eso es todo lo que podemos hacer por hoy. Usted" (dirigiéndose a Doce) "está justificado en su desconfianza hacia personas que hacen preguntas. Por favor mantengan todo eso en máxima reserva. Aunque prefiero no pensar en lo peor ... pero si esa es una mafia de trata de números, ustedes podrían estar en peligro. Voy a encargarme de encontrar ese lugar, y más que todo, de descubrir la identidad de aquel muchacho grande. Sólo quisiera pedirles, si no es exigir mucho, que me dejen una prenda del lugar donde escaparon, por la duración de la investigación."
Ahora fue el turno de los residuos, echar miradas interrogativas. Numbers explicó: "A veces, una búsqueda con sabuesos da resultados. O un análisis químico. Para eso se necesita algún objeto que puede estar impregnado de olores o sustancias químicas del lugar de su procedencia."
– "Si es así ...", dijo Ocho, y entregó al detective un pañuelo que tenía en el bolsillo. "Lo tengo conmigo desde que escapé de allí." – De la misma manera, Doce le facilitó un lápiz.



Se recomienda continuar con las siguientes tres Unidades *(N3, N4, N5)* en orden.

Unidad N 3 - El teorema chino de los residuos

Prerrequisitos:
- Aritmética modular básica.



1) Planteamos primero el problema de manera muy general:
Se busca un número n que al dividir entre p da un residuo a, y al dividir entre q da un residuo b.
O sea: $n \equiv a \pmod{p}$; y $n \equiv b \pmod{q}$.
¿Hay siempre una solución? ¿o varias?
¿Qué propiedades tienen las soluciones, respecto a las propiedades de los números a, b, p, q?
¿Cómo se pueden encontrar las soluciones?

Por si necesitas más dirección, aquí unas preguntas más específicas:
2) Explora para las siguientes situaciones:
- ¿Cuáles son las soluciones?
- Expresa la totalidad de las soluciones de manera generalizada.
- ¿En qué se distinguen los problemas planteados? ¿Hay algunos que tienen más soluciones que otros?

a) $x \equiv 2 \pmod{7}$, y $x \equiv 1 \pmod{3}$.
b) $x \equiv 2 \pmod{8}$, y $x \equiv 0 \pmod{15}$.
c) $x \equiv 3 \pmod{10}$, y $x \equiv 13 \pmod{20}$.
d) $x \equiv 3 \pmod{10}$, y $x \equiv 14 \pmod{20}$.
e) $x \equiv 6 \pmod{9}$, y $x \equiv 9 \pmod{12}$.
f) $x \equiv 5 \pmod{9}$, y $x \equiv 11 \pmod{12}$.
g) $x \equiv 5 \pmod{9}$, y $x \equiv 10 \pmod{12}$.

3) Investiga, respecto a los problemas anteriores:
- ¿Los problemas del tipo a) y b) siempre tienen una solución? ¿Cuál es la propiedad particular que distingue este tipo de problemas?
- ¿Bajo qué condiciones tienen solución los problemas del tipo e), f), g)?
- ¿Cómo se calcula la longitud de los "pasos" en los que se repiten las soluciones, en problemas del tipo a) y b)? ¿Y en el caso de problemas del tipo e), f), g)?

Sherlock Numbers y los cuatro residuos

III

Unos días después, Sherlock Numbers supo que sus temores habían sido justificados. Se encontraba en medio de un experimento, comparando sustancias químicas desprendidas del pañuelo y del lápiz. Aunque fue difícil encontrar alguna sustancia ajena en el lápiz; pero llegó cerca de asegurarse de que sí se encontraban trazas de un mismo desinfectante en ambos objetos.
En ese momento fue interrumpido por la llegada de su amigo Less, quien trajo el diario: "¡Mira, un asesinato! ¿Te imaginas dónde?"
– "No, ¿dónde?"
– "¡En la misma puerta de la comisaría!"
– "¿Verdad? ¡Qué atrevido!"
– "Eso digo yo también. Y parece que no tienen ni una pista de quién fue."
– "¿La víctima?"
– "No, el asesino. La víctima sí la identificaron ... a ver ..."
– "Permíteme ver. Ah sí, aquí: 'La víctima fue identificada como un cierto 622, un residuo. No se sabe nada más acerca de su procedencia. La policía pide la ayuda de la población para esclarecer este caso.' – Un residuo. Mi intuición me dice que eso está relacionado con mi caso actual. Less, ¡tengo que ir a la comisaría inmediatamente!"
Numbers tuvo mucho cuidado de no revelar ante los oficiales nada de su caso actual. No quiso poner en peligro a su cliente. Pero ofreció su ayuda, con su laboratorio químico y su experiencia, para contribuir a una mejor identificación de la víctima. Al mismo tiempo, esperaba encontrar alguna pista adicional para su propio caso.
Y así fue. Sus análisis indicaron que el pobre 622 debía haberse escapado del mismo lugar como su cliente. "Seguramente quiso avisar a la policía", se dijo Sherlock Numbers. "Pero le siguieron. Y esperaron con dispararlo hasta la misma puerta de la comisaría, para dar una advertencia a los otros escapados. Ahora tengo que descubrir urgentemente la identidad de aquel muchacho grande. Espero que lo pueda liberar a tiempo."
Desafortunadamente, por el momento no fue posible descubrir nada más acerca del trasfondo de 622. "Tengo que trabajar con los datos que tengo", dijo Numbers.

Desafío a los lectores:
Tú tienes los mismos datos como Sherlock Numbers. ¿Puedes con eso descubrir la identidad del "muchacho grande"?
Por lo menos puedes comenzar con los primeros pasos. ¿Qué cálculos tiene que hacer Sherlock Numbers primero? ¿Y cómo puede proceder después, para identificar al "muchacho grande"?

... *(Continúa al fin de la Unidad)*

VIAJE GUIADO

Este es un tipo "clásico" de problemas, que se pueden encontrar en diversas variaciones:

Jorge tiene una cantidad de soldaditos de juguete; son más que 40, pero menos que 60. Si los coloca a todos en filas de 7, sobran dos soldaditos. Si los coloca en filas de 3, sobra un único soldadito. ¿Cuántos soldaditos son?

Algebraicamente, el problema se puede formular así:

$$\left\{\begin{array}{l} \boldsymbol{x} \equiv 2 (\text{mod}.7) \\ \boldsymbol{x} \equiv 1 (\text{mod}.3) \\ 40 < \boldsymbol{x} < 60 \end{array}\right\}$$

Esto es un sistema de ecuaciones diofánticas. Con números tan pequeños, la solución se puede encontrar probando. Considerando solamente las dos primeras ecuaciones, la primera solución es $\boldsymbol{x} = 16$.
Para que se cumpla la primera ecuación, las posibles $\boldsymbol{x}$ se siguen en pasos de 7. Para que se cumpla la segunda ecuación, se siguen en pasos de 3. Entonces, para que se cumplan *ambas* ecuaciones, las soluciones se repiten en pasos de MCM (7; 3) = 21. Eso da la secuencia: 16, 37, 58, 79, ...
La solución que se encuentra en el intervalo requerido es 58.

Nota: Para resolver el problema planteado, podríamos haber evaluado las soluciones posibles empezando con 41. Pero para entender los principios generalizados, hemos formulado primero la solución general de las ecuaciones diofánticas, y después hemos escogido aquélla que cumple la condición adicional del intervalo.

Veamos otro ejemplo, directamente de forma algebraica:
¿Cuáles son los números que cumplen:
$\boldsymbol{x} \equiv 2$ (mod.8), y $\boldsymbol{x} \equiv 0$ (mod.15) ?
Examinando la tabla del 15, encontramos que $90 \equiv 2$ (mod.8), ésa es la primera solución.
MCM (8; 15) = 120; entonces la solución generalizada es: $\boldsymbol{x} = 90 + 120\boldsymbol{k}$.

Nota: No tratamos aquí los métodos para resolver ecuaciones diofánticas. Eso fue el tema del problema de investigación en la Unidad anterior (N 2).

Podemos generalizar este tipo de problemas: Se busca un número $\boldsymbol{x}$, tal que $\boldsymbol{x} \equiv \boldsymbol{a}$ (mod.$\boldsymbol{m}$), y $\boldsymbol{x} \equiv \boldsymbol{b}$ (mod.$\boldsymbol{n}$).
En los casos anteriores, $\boldsymbol{m}$ y $\boldsymbol{n}$ eran PESI. Y hemos visto que en estos casos existe una única solución entre los números de 1 a $\boldsymbol{mn}$. Eso es básicamente lo que dice el teorema chino de los residuos:

Si m y n son PESI,
entonces cada combinación posible de residuos (mod.m) y residuos (mod.n) ocurre exactamente una vez entre los números de 1 a mn.

Demostración:
Supongamos que existieran dos números distintos $\boldsymbol{x}$, $\boldsymbol{y}$, que ambos cumplen las condiciones. En este caso:
$\boldsymbol{x} \equiv \boldsymbol{y}$ (mod.$\boldsymbol{m}$), y $\boldsymbol{x} \equiv \boldsymbol{y}$ (mod.$\boldsymbol{n}$).
Entonces $\boldsymbol{x} - \boldsymbol{y}$ es un múltiplo de $\boldsymbol{m}$, y también de $\boldsymbol{n}$; entonces $\boldsymbol{x} - \boldsymbol{y}$ es un múltiplo de MCM($\boldsymbol{m}$; $\boldsymbol{n}$).
Pero si $\boldsymbol{m}$ y $\boldsymbol{n}$ son PESI, entonces MCM($\boldsymbol{m}$; $\boldsymbol{n}$) = $\boldsymbol{mn}$;
y entonces $\boldsymbol{x}$ y $\boldsymbol{y}$ no pueden pertenecer ambos a los números de 1 a $\boldsymbol{mn}$.
Con eso está demostrado que cada combinación de residuos es *única* entre los números de 1 a $\boldsymbol{mn}$. Ahora falta demostrar todavía que *todas* estas combinaciones ocurren:
Existen $\boldsymbol{m}$ diferentes residuos (mod.$\boldsymbol{m}$), y $\boldsymbol{n}$ diferentes residuos (mod.$\boldsymbol{n}$). Según las leyes de la combinatoria, existen $\boldsymbol{mn}$ combinaciones de los dos (producto cartesiano). De 1 a $\boldsymbol{mn}$ hay $\boldsymbol{mn}$ números. Ya que ninguna combinación ocurre duplicada en este intervalo, cada una tiene que ocurrir exactamente una vez. Eso es lo que había que demostrar.

Vemos también que este tema está muy relacionado con la "división modular". Nuestro problema era:

$\boldsymbol{x} \equiv \boldsymbol{a}$ (mod.$\boldsymbol{m}$), y $\boldsymbol{x} \equiv \boldsymbol{b}$ (mod.$\boldsymbol{n}$)

Eso puede también escribirse así:

$\boldsymbol{my} + \boldsymbol{a} = \boldsymbol{nz} + \boldsymbol{b}$ $\quad | - \boldsymbol{b}$
$\boldsymbol{my} + (\boldsymbol{a} - \boldsymbol{b}) = \boldsymbol{nz}$
resp. $\boldsymbol{nz} \equiv \boldsymbol{a} - \boldsymbol{b}$ (mod.$\boldsymbol{m}$)

... lo cual es un problema de división modular.
Por tanto aplican también los mismos principios, para los casos donde $\boldsymbol{m}$ y $\boldsymbol{n}$ tienen un divisor común:

$\boldsymbol{x} \equiv 3$ (mod.10), y $\boldsymbol{x} \equiv 13$ (mod.20)

Aquí, la segunda condición implica la primera. *Todo* número ≡ 13 (mod.20) es también ≡ 3 (mod.10).

$\boldsymbol{x} \equiv 3$ (mod.10), y $\boldsymbol{x} \equiv 14$ (mod.20)

Aquí tenemos una contradicción. Si un número es ≡ 14 (mod.20), entonces necesariamente es ≡ 4 (mod.10). Las dos condiciones se excluyen mutuamente; no hay ninguna solución.

$\boldsymbol{x} \equiv 6$ (mod.9), y $\boldsymbol{x} \equiv 9$ (mod.12)

Aquí podemos "simplificar" todo con el MCD=3, y resolver $\boldsymbol{x}/3 \equiv 2$ (mod.3), y $\boldsymbol{x}/3 \equiv 3$ (mod.4). Esta es una situación de $\boldsymbol{m}$, $\boldsymbol{n}$ PESI, con la única solución $\boldsymbol{x}/3 \equiv 11$ (mod.12). Lo "amplificamos" con 3, y tenemos la solución del problema original: $\underline{\boldsymbol{x} \equiv 33 \text{ (mod.36)}}$.

$\boldsymbol{x} \equiv 5$ (mod.9), y $\boldsymbol{x} \equiv 11$ (mod.12)

Así no podemos simplificar; pero podemos calcular con $\boldsymbol{x}+1$:

$\boldsymbol{x}+1 \equiv 6$ (mod.9), y $\boldsymbol{x}+1 \equiv 0$ (mod.12)
$(\boldsymbol{x}+1)/3 \equiv 2$ (mod.3), y $(\boldsymbol{x}+1)/3 \equiv 0$ (mod.4)
$(\boldsymbol{x}+1)/3 \equiv 8$ (mod.12)
$\underline{\boldsymbol{x} \equiv 23 \text{ (mod.36)}}$

$\boldsymbol{x} \equiv 5$ (mod.9), y $\boldsymbol{x} \equiv 10$ (mod.12)

Aquí tenemos una contradicción, porque las condiciones equivalen a:

$\boldsymbol{x} \equiv 2$ (mod.3), y $\boldsymbol{x} \equiv 1$ (mod.3)

No hay solución.

Resumimos algunas observaciones:

- En los problemas de este tipo, las soluciones se repiten en períodos de MCM(***m***; ***n***). Por tanto, la solución se indica (mod. MCM(***m***; ***n***)).
- Si ***m***, ***n*** tienen un divisor común, entonces ***no todas las combinaciones posibles de residuos*** aparecen entre los números de 1 a MCM(***m***; ***n***).
- Sea D = MCD(***m***; ***n***); entonces las combinaciones que existen son aquellas donde ***a*** ≡ ***b*** (mod.D). De otro modo tenemos una contradicción, y la combinación respectiva no existe.
- Entonces, la cantidad de combinaciones que existen, es ***mn*** ÷ MCD(***m***; ***n***) = MCM(***m***; ***n***).

De eso concluimos que también en el caso donde ***m***, ***n*** no son PESI, cada combinación de residuos ***que no implica una contradicción***, aparece ***exactamente una vez*** entre los números de 1 a MCM(***m***; ***n***).

Para pensar: En el tema de la división modular hemos visto que si los divisores no son PESI, hay varias soluciones. En estos problemas relacionados con el teorema chino, sin embargo, vimos que o no hay solución, o hay una única. ¿Cómo te explicas eso?
(*Pauta:* Analiza detenidamente lo que sucede en uno de los ejemplos donde hemos "simplificado" y después "amplificado". Escribe el mismo ejemplo en forma de una división modular, y analiza lo que sucede allí, y cuáles son sus soluciones.)

Para practicar

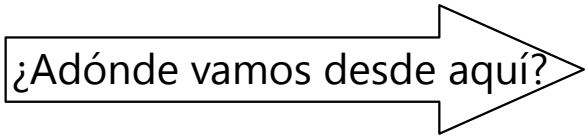
1) Si ***n*** ≡ 7 (mod.10) y ***n*** ≡ 5 (mod.9), ¿a cuánto equivale ***n*** (mod.90)?
2) Si ***n*** ≡ 13 (mod.14) y ***n*** ≡ 3 (mod.23), ¿a cuánto equivale ***n*** (mod.322)?
3) Si ***n*** ≡ 13 (mod.16), ¿a cuánto equivale ***n*** (mod.8)?
4) Si ***n*** ≡ 7 (mod.11), ¿a cuánto equivale ***n*** (mod.33)?
5) Si ***n*** ≡ 15 (mod.28) y ***n*** ≡ 22 (mod.49), ¿a cuánto equivale ***n*** (mod.196)?
6) Si ***n*** ≡ 31 (mod.36) y ***n*** ≡ 5 (mod.21), ¿a cuánto equivale ***n*** (mod.252)?
7) Si ***n*** ≡ 4 (mod.9), ***n*** ≡ 6 (mod.10), y ***n*** ≡ 2 (mod.11), ¿a cuánto equivale ***n*** (mod.990)?
8) Si ***n*** ≡ 15 (mod.21) y ***n*** ≡ 4 (mod.25), ¿cómo podemos expresar ***n*** con un único módulo?
9) Si ***n*** ≡ 11 (mod.35) y ***n*** ≡ 53 (mod.56), ¿cómo podemos expresar ***n*** con un único módulo?
10) Si ***n*** ≡ 0 (mod.38) y ***n*** ≡ 10 (mod.57), ¿cómo podemos expresar ***n*** con un único módulo?
11) Si ***n*** ≡ 5 (mod.7), ***n*** ≡ 6 (mod.9), y ***n*** ≡ 12 (mod.28), ¿cómo podemos expresar ***n*** con un único módulo?
12) ¿Cuál es el menor número que da un residuo de 4 al dividirlo entre 5, un residuo de 5 al dividirlo entre 6, y un residuo de 6 al dividirlo entre 7? - ¿Y cuál es el siguiente número que cumple las condiciones?
13) Carla, Braulia y Ana entrenan juntas en un estadio para un maratón. Las tres comenzaron juntas en el mismo lugar a correr. Carla demora 184 segundos para dar una vuelta, Braulia 168 segundos, y Ana 161 segundos. En cierto momento, cuando Ana justo pasa por el lugar de inicio, Braulia se encuentra a 1/12 de una vuelta por delante de ella, y Carla a 1/4 de una vuelta. Si todas corrieron con velocidad constante, ¿cuántas vueltas ha dado Ana hasta ese momento, cuántas Braulia, y cuántas Carla?
14.a) Encuentra el primer número que es PESI con todos los números de 3 a 12, y que no da un residuo de 1 al dividirlo entre ninguno de esos números.
b) Encuentra el primer número *compuesto* que cumple con la condición mencionada.

PARI permite calcular directamente las soluciones de problemas relacionados con el teorema chino, usando números modulares *(vea Unidad N 2)*. La palabra clave es **`chinese(a, b)`**. Por ejemplo:

```
> chinese(Mod(1,2), Mod(2,3))
%1 = Mod(5, 6)
```

Sherlock Numbers y los cuatro residuos (Continuación)

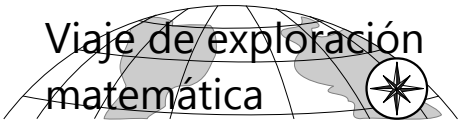
Para los últimos pasos podrías necesitar una computadora, a no ser que te guste estar calculando por muchas horas. Y pueden existir varios "muchachos grandes" que coinciden con los datos. Pero puedes por lo menos comenzar con los primeros pasos y esbozar el camino, antes de leer la continuación. Las condiciones que debe cumplir el número buscado, se pueden establecer con mucha claridad matemática.



Se recomienda continuar con las siguientes dos Unidades *(N 4, N 5)* en orden.

Unidad N 4 - La función Φ de Euler

Prerrequisitos:
- Concepto de números PESI *(Primaria II, Unidad 17)*.



¿Cuántos números menores a 12 son PESI con 12?
¿Cuántos números menores a 13 son PESI con 13?
Averigua para algunos otros números ***n***: ¿Cuántos números menores a ***n*** son PESI con ***n***?
Después investiga y razona:

1) Si tienes un número ***n***, ¿cómo puedes calcular de una manera relativamente sencilla la cantidad de números < ***n*** que son PESI con ***n***?

2) ¿Cómo es en el caso especial de que ***n*** es primo?

3) Tenemos un número ***n***, del cual ya conocemos cuántos números < ***n*** son PESI con ***n***. ¿Cómo nos facilita eso el cálculo correspondiente para múltiplos de ***n***?
O dicho con otras palabras: Si sabemos cuántos números < ***n*** son PESI con ***n***, encuentra una regla que te permite deducir de allí, cuántos números < ***kn*** son PESI con ***kn*** (dependiendo de ciertas propiedades del factor de multiplicación ***k***; y por supuesto asumiendo que ***k*** es un número natural.)

4) A base de la observaciones hechas hasta ahora, establece una fórmula general (si todavía no la encontraste), que te permite calcular para cualquier número natural ***n***, cuántos números < ***n*** son PESI con ***n***.

5) Tomando en cuenta los resultados de 3) y 4), demuestra o refuta la siguiente afirmación:
"La cantidad de números < ***kn*** que son PESI con ***kn***, es un múltiplo de la cantidad de números < ***n*** que son PESI con ***n***."

6) Describe cualquier otra observación interesante acerca de los números que son PESI con un número dado.

Sherlock Numbers y los cuatro residuos

IV

"Ahora necesito ayuda profesional", dijo Sherlock Numbers. "En matemática no soy más que un aficionado." – Y se dirigió adonde el Dr.Raíz, un matemático al que conocía desde hace tiempo.
"Mi querido doctor, le estoy trayendo un problema matemático de un amigo mío. ¿Es posible descubrir un número a partir de sus residuos?"
– "Eso depende. ¿Podría especificar más exactamente lo que entiende con 'sus residuos'?"
– "Bueno, se sabe que un número fue dividido entre distintos divisores, y se conocen los residuos."
– "Ajá. ¿Y se conocen también esos divisores? ¿Y los cocientes?"
– "De los divisores, algunos. De los cocientes, ninguno."
– "En este caso, habrá que contar con que existen varias soluciones", respondió el erudito. "Pero ésas se pueden expresar de manera generalizada por una fórmula. Se aplicaría en este caso el teorema chino de los residuos."
– "Té de residuos chinos ..." murmuró Numbers con una mirada distraída. Después se interrumpió a sí mismo: "Disculpe, Doctor. Creo que mi mente estaba divagando. ¿Qué había dicho usted?"
– El Dr.Raíz se dio cuenta de que el detective no entendió de qué estaba hablando. Sacó papel y lápiz y se puso a explicar:
– "Observemos, por ejemplo, la división de un número entre 3 y entre 5. La división entre 3 puede producir los residuos 0, 1, 2. La división entre 5 puede producir residuos de 0 a 4. Veamos ahora cómo se combinan estos residuos, si aplicamos las divisiones a los números de 1 a 15:

n	entre 3	entre 5
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4
15	0	0

El matemático señaló las columnas con su lápiz: "Vemos que del 1 al 15, cada combinación de residuos aparece exactamente una vez. Por ejemplo, el número 8 se caracteriza por los residuos 2 y 3. Ningún otro número en la tabla tiene esta misma combinación de residuos.

VIAJE GUIADO

El tema del viaje de exploración se llama "la función Φ (fi) de Euler". Leonardo Euler definió esta función así:

Φ(*n*) es la cantidad de números naturales menores a *n*, que son PESI con *n*.

Así por ejemplo, Φ(12) = 4, porque hay 4 números menores a 12 que son PESI con 12: 1, 5, 7, y 11.
Φ(13) = 12, porque todos los números de 1 a 12 son PESI con 13.
Notamos aquí que este es el caso de todos los números primos: Un número primo no tiene divisores menores que él mismo, excepto el 1. Por tanto, todos los números menores a un número primo, son PESI con él.

Cálculo de Φ(n)

Volvamos al ejemplo Φ(12). Con un número tan pequeño, se puede evaluar cada número < 12 y contar los que son PESI con 12.
Pero veremos ahora una manera más sistemática de calcularlo, una que funciona también con números mayores.
Los factores primos de 12 son: $12 = 2 \cdot 2 \cdot 3$.
Por tanto, un número es PESI con 12 si no contiene el 2 ni el 3 entre sus factores primos.
El que el factor 2 esté duplicado, no cambia nada: Aun los números que contienen una sola vez el factor 2, no son PESI con 12, porque tienen el 2 como divisor común.
Entonces, para calcular Φ(12), podemos considerar todos los números hasta 12, y excluir de ellos los que tienen el factor 2, y los que tienen el factor 3. *(Para que el cálculo salga sin problemas, tenemos que comenzar con 12 números, no con 11. Pero veremos que el 12 será excluido automáticamente en el primer paso, no importa cómo comenzamos; porque el 12 obviamente contiene cada uno de sus factores.)*
En cualquier intervalo de números naturales, exactamente la mitad de ellos contiene el factor 2 (si es que la cantidad de los números es par). Entonces la otra mitad no contiene ese factor, y nos quedamos con $12 \cdot \frac{1}{2} = 6$ números.
De éstos, exactamente un tercio contiene el factor 3. Si excluimos ésos, nos quedamos con dos tercios de lo que había: $6 \cdot \frac{2}{3} = 4$ números.
Ahora hemos terminado, porque hemos excluido todos los factores primos distintos del 12. Y efectivamente, al inicio ya hemos verificado que Φ(12) = 4.

Resumiendo el proceso:
$\Phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.
Generalizamos ahora esta regla:
Con cada factor primo ***p*** de ***n***, se excluyen 1/***p*** de los números que había; y quedan (***p*** – 1)/***p*** de ellos.
Por tanto, si la factorización de ***n*** en factores primos es:
$n = p^a \cdot q^b \cdot r^c \cdot \ldots \cdot z^k$, entonces:

$$\Phi(n) = n \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r} \cdot \ldots \cdot \frac{z-1}{z}$$

Por ejemplo: $60 = 2^2 \cdot 3 \cdot 5$, entonces:
$\Phi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$.
(Si deseas, verifícalo, evaluando todos los números.)

Y si ***n*** es primo, obviamente Φ(***n***) = ***n*** – 1.
*(Así sale también con la fórmula, si colocamos **n** como único factor primo.)*

Dos preguntas:

Pueden quedar unas dudas acerca de esta fórmula:
6) *¿Las divisiones siempre salen exactas?*
Sabemos que el resultado siempre es un número entero. – ¿Y si "por accidente" no sale así? – No, eso no es posible. Los denominadores ***p***, ***q***, ***r***, ... ***z*** son los factores primos distintos de ***n***. Por tanto, ***n*** es necesariamente divisible entre todos ellos.
7) En el ejemplo con Φ(12) hemos excluido la mitad de los números porque contienen el factor 2. Después hemos *asumido* que de los restantes, exactamente un tercio contiene el factor 3. ¿Cómo sabemos que eso es así? *¿No podrían los factores ser distribuidos de una manera desigual, que por ejemplo en una de las mitades haya más múltiplos de 3 que en la otra mitad?*
Esta pregunta es más intricada. Pero si eliminamos números según los criterios que hemos mencionado, entonces existe una propiedad que nos garantiza que los múltiplos de 3 son distribuidos de una manera "equitativa". Esa propiedad es el teorema chino de los residuos *(Unidad N)*. Intenta tú mismo(a) completar el razonamiento, usando esta pauta.

Para practicar:

8) Calcula:
a) Φ(100), b) Φ(96), c) Φ(210), d) Φ(221), e) Φ(2210).
9) Encuentra por lo menos un número ***x*** que cumple la condición:
a) Φ(***x***) = 4, b) Φ(***x***) = 10, c) Φ(***x***) = 24, d) Φ(***x***) = 7.
***10)** Encuentra *todas* las soluciones posibles de las ecuaciones en 9).

Para programadores

PARI te permite calcular **ϕ(*n*)** directamente, con la palabra clave **`eulerphi(n)`**.
Experimenta un poco. Por ejemplo, tipea **`eulerphi(30)`**, y debe aparecer 8 como resultado.

Quizás querrás usar esta función también para explorar un poco más el tema de investigación que sigue a continuación. Por ejemplo, podrías escribir un script que calcula automáticamente las probabilidades que se piden en la investigación – una vez que entiendes cómo se debe hacer eso.

Números aleatorios PESI

a) Si escoges al azar dos números naturales de 1 a 50, ¿cuál es la probabilidad de que son PESI? ¿Cómo puedes calcular eso? ¿Y cómo puedes simplificar el cálculo?
b) Generaliza el problema para números naturales de 1 a ***n***. ¿Encuentras una fórmula que expresa la probabilidad de que dos números naturales cualesquieras, de 1 a ***n***, son PESI?

- Probablemente no encontrarás ninguna fórmula sencilla y exacta. ¿Pero quizás una que provee una buena aproximación?
c)** ¿Qué pasará si ***n se vuelve muy grande, o si incluso llega a ser infinito?

El problema no define si escogemos los números "con devolución" o "sin devolución"; o sea si los dos números tienen que ser distintos, o si se pueden también escoger dos números iguales. Descubre tú mismo(a) cuál es la variante que más facilita el cálculo. Después será relativamente fácil, deducir el resultado de la otra variante. (¿Cómo harías eso?)

Sherlock Numbers y los cuatro residuos (Continuación)

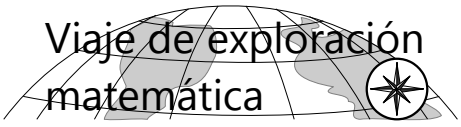
"Eso es lo que dice el teorema chino de los residuos. Usando el 3 y el 5 como divisores, existen $3 \cdot 5 = 15$ combinaciones distintas de residuos. Entre los primeros 15 números, ninguna combinación se duplica, y ninguna falta. Cada una aparece exactamente una vez. Eso es, por supuesto, si los divisores son primos entre sí. Si tuvieran un factor común, es obvio que la cantidad de combinaciones que aparecen, sería solamente el MCM de los divisores."
"¿Obvio?", pensó Sherlock. Y recordó lo que una vez le había dicho un estudiante de matemática: "Si un matemático usa expresiones como 'es obvio', o 'inmediatamente vemos', o algo similar, lo que quiere decir en realidad es que necesitas calcular y razonar por una hora hasta que lo entiendas." – Pero se esforzó por prestar atención al Dr.Raíz, quien continuó:
"En el 15 se repite la combinación del cero, '0', '0'. Y si continuáramos con 16, 17, etc, se repetirían todas las combinaciones anteriores. Si sumamos 15 a un número, el nuevo número tiene la misma combinación como el anterior. Eso es porque el 15 tiene un residuo de cero, tanto módulo 3 como módulo 5.
Entonces, si tuviéramos cualquier combinación de residuos módulo 3 y módulo 5, esa combinación determinaría un único número de 1 a 15; además de todos los números congruentes a ése, módulo 15. Por ejemplo, si supiéramos que el residuo al dividir entre 3 era 2, y entre 5 era 3, entonces la solución sería: $8 + 15\boldsymbol{k}$, donde ***k*** es un número entero."
– "Creo que entiendo", respondió Numbers. "Entonces, si tuviéramos por ejemplo los residuos al dividir entre 19, 20, y 21, ¿esos residuos determinarían un único número de 1 hasta $19 \cdot 20 \cdot 21$?"
– "Correcto", asintió el Dr.Raíz. "O sea, desde 1 hasta 7980. Y todos los números que sean congruentes a ése, módulo 7980."
– "Entonces, si los divisores son un poco grandes, o si hay varios de ellos, ¿habría bastantes números a examinar, hasta encontrar el correcto?"
– "Así es. Pero normalmente uno empezaría con examinar la combinación de solamente dos residuos, como lo hice en mi ejemplo. Si después conociéramos adicionalmente un residuo módulo 7, tendríamos que examinar solamente la solución de la primera combinación, y los siguientes en pasos de 15."
– "Ya veo. Pero aun así, si por ejemplo un divisor sería aproximadamente mil, sería bastante trabajo."
– "Por supuesto. ¿Usted vino para encargarme con eso?"
Pero Numbers prefirió no meter al matemático tan profundamente en su caso. Por eso dijo: "Usted ya debe estar suficientemente ocupado; no deseo cargarle más. Intentaré hacerlo yo mismo."
El Dr.Raíz se quedó pensando por algún tiempo. Después ofreció: "Le podría prestar un calculador. Con eso avanzaría más rápidamente."
– "Eso es muy amable de usted. Explíqueme cómo funciona, y me pondré a trabajar."
Numbers estuvo muy satisfecho. El problema parecía posible de resolver. Aunque podían existir varias soluciones. "Pero si fuera un primo *realmente* grande, no podrían haberlo secuestrado", pensó dentro de sí. "Hubiera ofrecido demasiada resistencia. Puedo esperar entonces que la primera solución que encuentre, sea la correcta."
Al despedirse, dijo como de paso: "Hay otra cosa que quise preguntarle hace tiempo. ¿Cómo se procede para una prueba de divisiones en un número primo?"
– "Oh, eso es un algoritmo sencillo, pero un poco anticuado e ineficaz en números grandes. Para probar un número ***n***, se lo divide entre todos los números primos $\leqslant \sqrt{\boldsymbol{n}}$. "
– "Muchas, pero muchas gracias doctor. Espero poder devolverle su calculador pronto."

Desafío a los lectores:
El Dr.Raíz te ha señalado el camino. ¿Te atreves a concluir la investigación, antes que lo haga Sherlock Numbers?

Unidad N 5 - Congruencia modular en potencias

Prerrequisitos:
- Operaciones básicas de aritmética modular.
- La función Φ de Euler *(Unidad N 4)*.

Nota: *Los temas de la sección "Ampliaciones" son opcionales; no figuran en los currículos escolares usuales.*



Investiga sucesiones de potencias $\boldsymbol{b}^0$, $\boldsymbol{b}^1$, $\boldsymbol{b}^2$, $\boldsymbol{b}^3$, ..., respecto a sus residuos módulo algún divisor ***m***.
Por ejemplo, si ***b*** = 5, la sucesión de potencias es:
1, 5, 25, 125, 625, ...
Para ***m*** = 7, sus residuos módulo 7 son:
1, 5, 4, 6, 2, ...

Prueba con diversas combinaciones {***b***; ***m***}. Investiga y observa:
¿Qué regularidades o patrones observas?
¿Hay una manera de predecir ciertas características de la sucesión de residuos que resultará?
¿A qué conclusiones llegas?
¿Puedes establecer algunas propiedades o teoremas acerca de esta clase de sucesiones?
¿Encuentras conexiones entre este tema y otros que investigaste anteriormente?
- Encuentra propiedades que te ayudan a resolver problemas como el siguiente de manera eficaz:

¿Cuál es el residuo de 2^{5487} al dividirlo entre 13?

Unas pautas adicionales:
- Para calcular estas sucesiones de residuos, no es necesario calcular la entera sucesión de potencias. El cálculo puede efectuarse también con números menores. ¿Encuentras cómo? Con eso te ahorrarás trabajo.
- Después de coleccionar suficientes ejemplos, examina primero aquellas sucesiones donde ***m*** es primo. Allí es más fácil llegar a unas conclusiones.
- Puede ser de ayuda, distinguir los casos donde ***m*** es PESI con ***b***, y donde no lo es.
- Puedes hacer una observación interesante, si usas el módulo *negativo* para aquellos residuos donde el módulo positivo es mayor a ***m***/2. (Por si no encuentras nada interesante aquí, la sección "Ampliaciones" trata un poco de este tema.)

Sherlock Numbers y los cuatro residuos

V

El calculador realmente fue de mucha ayuda. Pronto descubrió Numbers que 811 era el primer número capaz de producir los tres residuos pequeños, cuyos datos él tenía. Los siguientes debían seguirle en pasos de 7·11·17 = 1309.
– "Y tiene que ser un primo", dijo Numbers. "Pero ¿qué hago con el dato del infeliz 622? No conozco el divisor de esa operación." – Hizo un esfuerzo de recordar los estudios matemáticos de su juventud. "El residuo es menor al divisor", recordó. "Entonces ese divisor tiene que ser mayor a 622. Y al mismo tiempo, según lo que me dijo el buen doctor, tiene que ser menor o igual a $\sqrt{\boldsymbol{n}}$. Así ya puedo excluir muchas opciones."
Mientras que el detective estuvo absorbido en esos razonamientos, el calculador había arrojado una lista de los primeros números primos que cumplen 811 + 1309***k***:

811
6047
13901
16519
24373
37463
45317
53171
68879
76733
102913

"Perfecto", dijo Numbers. "Ahora me puedo limitar a estos candidatos. Espero que el muchacho que buscamos se encuentre entre ellos. A ver ..."

Desafío a los lectores:
Bueno, ahora Sherlock Numbers y el calculador ya hicieron una parte del trabajo. ¿Quieres adelantarte a él en los últimos pasos, antes de seguir leyendo? ¿O darle una pauta? Quién sabe, si esta vez el detective necesita una pauta de tu parte ...

VIAJE GUIADO

Volvamos al primer ejemplo del viaje de exploración: las potencias de 5, (mod. 7). Añadimos unos miembros adicionales:

1, 5, 25, 125, 625, 3125, 15625, 78125, 390625, ...
Los residuos módulo 7:
1, 5, 4, 6, 2, 3, 1, 5, 4, ...

Notamos que a partir de 5^6, la sucesión de los residuos comienza a repetirse. Conjeturamos que **las sucesiones de este tipo son periódicas**.

Verificamos: Al inicio de la sucesión, 5 es el resultado de multiplicar 1 · 5. Después, 4 es el resultado de multiplicar 5 · 5 (mod.7). Y después multiplicamos 4 · 5, y otra vez tomamos el residuo (mod.7), da 6.
La conclusión es obvia: Tan pronto como vuelve a aparecer el 1, se repiten las mismas operaciones, y entonces se repite la misma sucesión de residuos.

Con eso tenemos a la vez una manera más práctica de calcular estas sucesiones: En vez de calcular todas las potencias, podemos simplemente multiplicar los *residuos* sucesivamente por 5. Por las leyes de la congruencia modular, los resultados son los mismos como si hubiéramos calculado los residuos de las potencias.

La longitud del período

Ahora, el matemático desea saber cuántos miembros tiene el período de una tal sucesión. Si tenemos ***b***, ***m*** dados, ¿podemos predecir después de cuántos miembros se repetirá la sucesión?
(Esta longitud del período se llama el *orden* del grupo. Cuando se trata de sucesiones de potencias, algunos autores usan también el término "*gaussiano*".)

Eso depende más de ***m*** que de ***b***, porque el divisor ***m*** define *cuántos diferentes residuos son posibles*.
Si ***m***=7, tenemos 7 residuos diferentes. Sin embargo, con una base de 5 no es posible que aparezca el residuo 0.
1) ***Piensa:*** *¿Por qué no? ¿Y cómo sería si* ***b****=7?*
Entonces nos quedan 6 diferentes residuos. Y efectivamente, todos ellos aparecen en nuestra sucesión. Es un grupo de orden 6.

Consideramos ahora un divisor compuesto; por ejemplo el 18. Los residuos de las potencias de 5, (mod.18), son:
1, 5, 7, 17, 13, 11, 1, 5, 7, 17, ...
Otra vez, el orden del grupo es 6. ¿Por qué?
Razona: Al dividir una potencia de 5 entre 18, ¿puede resultar un residuo de 2? ¿o de 3? ¿o de 4?
18 es un múltiplo de 2, y también de 3. Entonces, si un número es ≡ 2 (mod.18), ese número es par.
Igualmente, si un número es ≡ 3 (mod.18), ese número es un múltiplo de 3.
Y si un número es ≡ 4 (mod.18), ese número nuevamente es par.
Pero una potencia de 5 no puede tener otros factores primos aparte del 5. O sea, no puede ser par, ni puede ser un múltiplo de 3.
Por tanto, no pueden aparecer residuos que contengan el 2 ó el 3 como factor primo.
En otras palabras: *No pueden aparecer residuos que tengan un divisor común con 18.*
Entonces, los únicos residuos posibles son los que son PESI con 18. En la Unidad anterior *(N 4)* hemos expresado esa cantidad con Φ(18). Y efectivamente, Φ(18) = 6, el orden de nuestro grupo.

Con eso todavía no estamos al final de nuestro viaje. Pero hemos llegado a una observación importante:
La longitud del período (o sea el orden del grupo, o el "gaussiano"), está relacionada con el valor de Φ(***m***).

Verificamos eso. Por ejemplo, usamos ***b***=2, ***m***=7:
1, 2, 4, 8, 16, 32, 64, 128, ...
Los residuos (mod.7):
1, 2, 4, 1, 2, 4, 1, 2, ...

La sucesión se repite después de solamente 3 miembros; pero Φ(7) = 6. O sea, aquí el orden es solamente la mitad de la cantidad de residuos posibles. Los residuos 3, 5, 6, no aparecen.

De hecho, vale la siguiente regla:

> **El orden del grupo de los residuos de b^k (mod. m) es un divisor de Φ(m).**

2)** ***Para pensar: ¿Puedes demostrar que si el orden es menor a Φ(***m***), que entonces es un *divisor* de Φ(***m***)?

Longitud del período si hay un divisor común

Examinemos ahora el caso donde ***b*** y ***m*** no son PESI. Por ejemplo las potencias de 6, (mod.21):

1, 6, 36, 216, 1296, ...
1, 6, 15, 6, 15, ...

Se verifica aquí también, que el orden (2) es un divisor de Φ(21). Pero en este caso podemos decir aun más:
El MCD de 6 y 21 es 3. Por tanto, pueden aparecer únicamente residuos que son múltiplos de 3.
En otras palabras, podemos "simplificar" las sucesiones enteras con 3; y entonces ya no tenemos residuos (mod.21), sino (mod.7): *(Dejamos el 1 afuera porque no es divisible entre 3.)*

2, 12, 72, 432, ...
(mod.7) 2, 5, 2, 5, ...

Por tanto, el orden del grupo necesariamente tiene que ser un divisor de Φ(7). En general:

> **El orden del grupo de los residuos de b^k (mod. m) es un divisor de $\Phi\left(\frac{m}{MCD(m,b)}\right)$.**

En el ejemplo arriba notamos además, que el 1 queda

fuera de la secuencia: El residuo 1 es "único", no vuelve a repetirse. ¿En qué otro contexto nos hemos encontrado con un fenómeno similar? (Si no lo descubres, consulta la sección "Ampliaciones".)

Observa ahora el siguiente ejemplo: Los residuos de las potencias de 6, (mod.24):

1, 6, 36, 216, 1296, 7776, ...
1, 6, 12, 0, 0, 0, ...

3) ***Para pensar:*** En este ejemplo, a partir de cierto momento, todos los residuos se vuelven cero. ¿Por qué sucede eso?
(Si no lo descubres, consulta el *Anexo A*.)

Cálculo rápido del residuo de potencias

Volvamos al ejemplo del viaje de exploración:
¿Cuál es el residuo de 2^{5487} al dividirlo entre 13?

Con lo que sabemos ahora, podemos calcularlo con bastante rapidez. Podríamos averiguar cuál es el orden del grupo (el "gaussiano") para este caso, estableciendo la secuencia de residuos (mod.13). Pero ya sabemos que ese orden es un divisor de Φ(13). Por tanto, después de 12 miembros necesariamente hay una repetición; y por ejemplo 2^{17} tendrá el mismo residuo como 2^5. Lo podemos formular como regla:

Si $f \equiv g$ (mod. Φ(m)), entonces $b^f \equiv b^g$ (mod. m).

Entonces, para nuestro ejemplo:
5487 ÷ 12 deja el residuo 3; entonces $2^{5487} \equiv 2^3$ (mod.13); la respuesta es $2^3 = 8$.

Para practicar:

4) ¿Cuál es el residuo de 13^{8934} al dividirlo entre 16?

5) ¿Cuáles son las últimas d os cifras de 12^{777}?

6) ¿Cuál es el residuo de 63^{2021} al dividirlo entre 6561?

7) ¿Cuál es el residuo de 5^{813} al dividirlo entre 1953?

8) ¿Cuál es el residuo de 173^{6833} al dividirlo entre 172?

9) ¿Cuál es el residuo de 172^{6833} al dividirlo entre 173?

***10)** ¿Cuál es el resido de $3^{10'000}$ al dividir entre 5353?

***11)** ¿Existe otro método relativamente eficiente que permite calcular el residuo de una potencia con exponente grande? Por ejemplo, ¿cuál es el residuo de 103^{784} al dividir entre 15'707?
- Para aplicar cualquier método tratado hasta ahora, necesitamos descomponer 15'707 en sus factores primos. Eso puede durar bastante tiempo. ¿Existe un método de calcularlo sin efectuar esa descomposición, y sin tener que seguir toda la secuencia de residuos hasta llegar al exponente 784 (o hasta que se repita el período)?

12) ¿Cuántas potencias de 2, menores a 1'000'000'000, dejan al dividir entre 9 un residuo de 7?

13) Demuestra o refuta:

Para todo número primo p>5 vale: $p^4 \equiv 1$ (mod.120).

14) Sea a el "gaussiano" respecto a la base b (mod.p), y c el "gaussiano" respecto a la misma base (mod.q). Encuentra una expresión generalizada que combina estas dos condiciones en un único "gaussiano".

***15)** Si $7^x \equiv 14$ (mod.23), ¿cuánto es x?

***16)** ¿Cuál es el menor número de la forma $10^n + 8$, que es divisible entre 1377?

***17.a)** ¿Existen potencias de 2 que terminan con ...1234? Si existen, ¿cuál es la menor de ellas?
b) ¿Existen potencias de 2 que terminan con ...3456? Si existen, ¿cuál es la menor de ellas?
c) ¿Existen potencias de 2 que comienzan con 1234...? Si existen, ¿cuál es la menor de ellas?

Reglas de divisibilidad "a medida"

Hemos visto que las reglas de divisibilidad conocidas, en realidad son reglas de congruencia modular. *(Vea Secundaria I, Unidad 32.)* Podemos ahora usar los mismos principios para inventar reglas nuevas.

Sumas o diferencias de cifras

Este es el principio de muchas reglas de divisibilidad. Como ejemplo, repasemos brevemente la demostración de la "regla del 11":
Sea un número ...edcba. Eso equivale a:
... + 10'000e + 1000d + 100c + 10b + a
y es congruente (mod.11) con:
... + e − d + c − b + a.
Por eso, la "suma alternando de las cifras" indica el residuo (mod.11) del número original.

Con lo que hemos aprendido en esta Unidad, entendemos mejor por qué esta demostración se aplica a números con cualquier cantidad de cifras: Los residuos de una sucesión de potencias, (mod.m), forman una sucesión periódica. Y los coeficientes 1, 10, 100, ..., por supuesto que son la sucesión de las potencias de 10. Por eso, la misma congruencia se repite para todas las cifras de un número, hasta lo infinito.

Usemos este principio para inventar una regla de divisibilidad entre 7.
Los residuos de las potencias de 10, (mod.7), son:
1, 3, 2, 6, 4, 5, 1, ... (se repite).
O usando módulos negativos:

1, 3, 2, –1, –3, –2, 1, ... (se repite).

Por tanto, un número como

... + 100'000***f*** + 10'000***e*** + 1000***d*** + 100***c*** + 10***b*** + ***a***

es congruente (mod.7) con:

... – 2***f*** – 3***e*** – ***d*** + 2***c*** + 3***b*** + ***a***.

(Y se repite el mismo período de 6 números.)

Entonces, el residuo (mod.7) de un número se encuentra, sumando la cifra de las unidades con el triple de las decenas y el doble de las centenas, restando la cifra de los millares, el triple de las decenas de millares, y el doble de las centenas de millares; después repitiendo lo mismo con los millones, y así sucesivamente.

Por ejemplo:

21: 1 + 3·2 = 7, es divisible entre 7.

999: 9 + 3·9 + 2·9 = 54 ≡ 5 (mod.7); residuo 5.

316215: 5 + 3·1 + 2·2 – 6 – 3·1 – 2·3 = –3 ≡ 4 (mod.7).

Etc.

(Si deseas, puedes verificarlo con otros números.)

Nota: *Algunos libros preuniversitarios presentan tales reglas como contenido "a memorizar para el examen". Opino que eso no vale la pena. Si entiendes los principios que se explican aquí, podrás fácilmente reconstruir esas reglas: no es otra cosa que encontrar los residuos de las potencias de 10, módulo algún divisor.*

Además, como ves en el ejemplo anterior, estas "reglas" se vuelven bastante complicadas (con pocas excepciones). Por eso, son más una curiosidad que una herramienta útil. Aplicar la regla anterior, da casi igual de trabajo como dividir el número entre 7.

(Recordarás que para números grandes, la "regla del 1001" es mucho más fácil; y ésa nos sirve para el 7, el 11 y el 13 a la vez.)

Sólo para diversión, ¿quizás querrás intentar establecer una regla similar para la divisibilidad entre 17?

Reducción sucesiva de un número

Este es un nuevo tipo de reglas. Por ejemplo para el 7:

Separa el número en dos partes: la cifra de unidades, y todo el "resto". Sustrae del "resto" el doble de las cifras de las unidades. Si quedan varias cifras, repite el proceso. Si el resultado es un múltiplo de 7, el número original también es un múltiplo de 7.

Ejemplos:

126: 12 – 2·6 = 0; es divisible entre 7.

8925: 892 – 2·5 = 882; 88 – 2·2 = 84; 84 – 2·4 = 0.
Es divisible entre 7.

1009: 100 – 2·9 = 82; 8 – 2·2 = 4.
No es divisible entre 7.

Esta regla sirve solamente para la divisibilidad, pero no para la congruencia en general. Por ejemplo con 1009, el resultado final fue 4; pero 1009 ≡ 1 (mod.7).

¿Por qué funciona esta regla?

Por ejemplo, hemos descompuesto 8925 en 10·892 + 5. En general, definimos ***n*** = 10***r*** + ***u***. Nuestra regla dice que si este número es divisible entre 7, también ***r*** – 2***u*** es divisible entre 7. Demostración:

10***r*** + ***u*** ≡ 3***r*** – 6***u*** (mod.7)

Ya que 3 y 7 son PESI, podemos aplicar una "división modular" entre 3: Si 3***r*** – 6***u*** ≡ 0 (mod.7), entonces también ***r*** – 2***u*** ≡ 0 (mod.7).

Eso es lo que había que demostrar.

¿Cómo encontramos reglas similares?

Eso es bastante fácil: Si funciona con un número en particular, lo podemos generalizar. Por ejemplo para el 7, podríamos comenzar con el número 35 y concluir que si multiplicamos el "resto" por 5 y le restamos el triple de la cifra de unidades, también tenemos una regla de divisibilidad entre 7. O sea, si ***n*** = 10***r*** + ***u***, entonces también 5***r*** – 3***u*** indica la divisibilidad entre 7. (¡Verifícalo! ¿Y puedes demostrar que funciona siempre?) - Solamente que esta "regla" resulta más complicada que una división entre 7 ...

Pero por ejemplo para una regla de divisibilidad entre 17, podríamos partir del número 51 (=17·3): El "indicador de divisibilidad" es ***r*** – 5***u***. (¡Verifica que funciona!)

Un poco más útil es una regla que permite eliminar dos o tres cifras a la vez. Para eso, separamos las *dos* o *tres* últimas cifras del número. Por ejemplo, 301 es divisible entre 43. Entonces, si definimos ***n*** = 100***r*** + ***u***, el "indicador" es ***r*** – 3***u***. Hagamos una prueba:

n = 2537: 25 – 3·37 = –86 ≡ 0 (mod.43);
y efectivamente, 2537 es divisible entre 43.

¿Puedes ver el "truco"? Podemos establecer una tal regla "fácil", si encontramos un número que termina con ...01 ó ...001, y que es divisible entre un determinado número.

Lo mismo funciona si el "número de inicio" termina con uno o varios nueves; porque podemos tratarlos como si la última cifra fuera (–1). Por ejemplo para una "regla del 13" podríamos empezar con 39 = $\overline{4(-1)}$. Entonces el "indicador" es ***r*** + 4***u***. (¡Verifícalo!)

O tenemos 7999 = $\overline{800(-1)}$ = 19 · 421. Entonces, si ***u*** significa las *tres* últimas cifras, ***r*** + 8***u*** indica si un número es divisible entre 19. (Y también entre 421, por si alguna vez necesitas una regla para ese número...) - Ejemplo:

n = 230204: 230 + 8·204 = 1862 ≡ 0 (mod.19).

(Con 1862 no sirve repetir la misma operación, porque el resultado sería mayor a 1862. Tenemos que dividirlo entre 19 para comprobar la divisibilidad.)

Para practicar: Encuentra algunas otras reglas de este tipo.

Divisibilidad en otros sistemas de numeración

Podemos aplicar los mismos principios a la numeración con otras bases. Por ejemplo, podemos establecer una regla de divisibilidad entre 41 para números en base 9:

Separamos el número en grupos de *dos* cifras; entonces tenemos:

$$\boldsymbol{n} = \ldots + 9^6\overline{\boldsymbol{hg}} + 9^4\overline{\boldsymbol{fe}} + 9^2\overline{\boldsymbol{dc}} + \overline{\boldsymbol{ba}}_{\mathbf{9}}$$

Analizando los residuos de las potencias de 81 (mod.41), encontramos que esta expresión es

congruente (mod.41) con:

$$\ldots - \overline{\boldsymbol{hg}} + \overline{\boldsymbol{fe}} - \overline{\boldsymbol{dc}} + \overline{\boldsymbol{ba}}_{\boldsymbol{9}}$$

O sea, en base 9 podemos verificar la divisibilidad entre 41, haciendo grupos de dos cifras, y sumando y restándolos alternadamente.

Una aplicación realmente útil de eso es cuando analizamos los números binarios (base 2), porque las computadoras calculan internamente en el sistema binario. Para la computadora es más rápido, aplicar una regla como ésta a los dígitos binarios de un número, en vez de realizar una división.

Por ejemplo, agrupando los dígitos binarios en grupos de cinco, tenemos el número en "base 32":

$$\boldsymbol{n} = \ldots + 32^3\,\overline{\boldsymbol{tsrqp}} + 32^2\,\overline{\boldsymbol{onmlk}} + 32\,\overline{\boldsymbol{jihgf}} + \overline{\boldsymbol{edcba}}_{\boldsymbol{2}}$$

Eso es congruente (mod.31) con:

$$\ldots + \overline{\boldsymbol{tsrqp}} + \overline{\boldsymbol{onmlk}} + \overline{\boldsymbol{jihgf}} + \overline{\boldsymbol{edcba}}_{\boldsymbol{2}}$$

Y es congruente (mod.3) y (mod.11) con:

$$\ldots - \overline{\boldsymbol{tsrqp}} + \overline{\boldsymbol{onmlk}} - \overline{\boldsymbol{jihgf}} + \overline{\boldsymbol{edcba}}_{\boldsymbol{2}}$$

Así, sumando resp. restando grupos de 5 cifras binarias, la computadora puede fácilmente calcular congruencias (mod.3), (mod.11), y (mod.31).

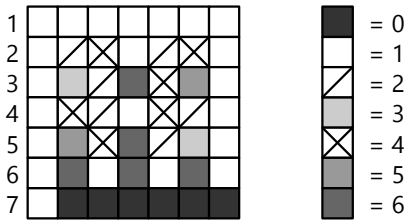
Tú mismo(a) podrás seguir explorando este tema por tu cuenta.

Ampliaciones

Los temas de esta sección son opcionales.

Arte matemático: "Tapices" modulares

Las sucesiones de los residuos de potencias (mod.***m***) se pueden representar de manera gráfica. Por ejemplo, este dibujo representa las potencias de las bases 1 a 7

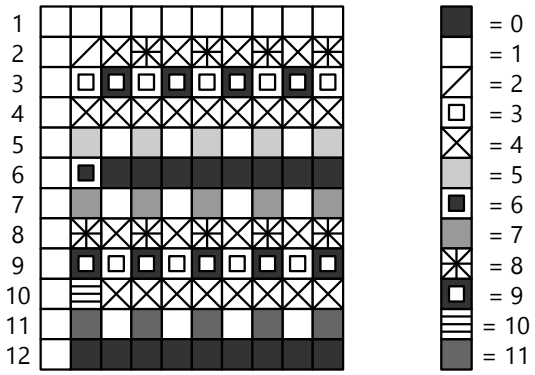


Cada fila representa las potencias de la base que se indica al margen izquierdo. El color o patrón de cada cuadrado indica el residuo correspondiente a la tabla al lado derecho.

Podríamos continuar el dibujo hacia la derecha; sabemos que después de la 6^{ta} potencia, todo se repite periódicamente. También hacia abajo podríamos continuar, y allí también hay una repetición periódica, porque 8 ≡ 1 (mod.7), entonces las potencias de 8 se comportan igual como las de 1, y así sucesivamente.

Por supuesto que tú puedes hacer tus dibujos a colores, así se verán más bonitos que estos ejemplos en el libro.

Aquí hay otro, con las potencias (mod.12):



Vemos que éste es significativamente diferente, porque 12 es un número compuesto. Por eso no aparece la franja vertical de puros "1" en el exponente ***m***–1, que es característica de los gráficos de los números primos. Hay residuos de 1 en los exponentes múltiplos de 4 = Φ(12), incluso en los múltiplos de 2; pero su franja vertical no es continua, es interrumpida por las bases que tienen un divisor común con 12.

Para hacer: Dibuja diagramas similares para otras ***m***, e investiga sus propiedades.

La conexión con los números decimales

Quizás notaste que este tema tiene mucha similitud con la investigaciones que hicimos en *Secundaria I (Unidad 46)*, acerca de los períodos de los números decimales. Y de hecho, es el mismo principio matemático. Cuando calculamos en decimales una división como 1/7, ¿qué hacemos? - Cada vez que "bajamos un cero", estamos multiplicando el residuo anterior por 10, y calculamos el nuevo residuo del resultado. Así calculamos efectivamente los residuos de las potencias de 10, (mod.7). Solamente que el resultado, el número decimal, consiste en los *cocientes*; pero dentro de la operación aparecen los residuos. Observa los números en negrita, y compáralos con el ejemplo en la sección "Reglas de divisibilidad":

```
1÷7 = 0.1428571...
10
 30
  20
   60
    40
     50
      10
       ...
```

Y si lo hacemos en otro sistema de numeración, entonces aparecen los residuos de las potencias de otra base. Por ejemplo, la misma división en base 9 produce los residuos de las potencias de 9:

```
1÷7 = 0.125125...9
10
 20
  40
   10
    20
     40    ...
```

Para hacer: Sigue explorando:
¿Cómo se relacionan las reglas acerca del orden del grupo de residuos de potencias, con las longitudes de los períodos de los números decimales?
¿Cómo se relacionan estas reglas con los divisores que producen números decimales exactos, periódicos puros, y periódicos mixtos?
¿Puedes ahora usar las propiedades de las potencias, para explicar más claramente cómo se producen los números decimales periódicos mixtos?
... y lo mismo en sistemas de numeración con otras bases.
¿Y por qué al usar un numerador distinto, a menudo el número decimal tiene la misma secuencia de cifras, solamente "rotadas" por algunas posiciones? - P.ej:

$1/7 = 0.\overline{142857}$
$2/7 = 0.\overline{285714}$
$3/7 = 0.\overline{428571}$ ... etc.

El "medio período"

Este tema encierra unos misterios, de los que podemos tocar solamente la superficie.
Explora unos casos donde el orden del grupo es par, y el divisor es primo. Por ejemplo las potencias de 10 (mod.7), ó (mod.13). En ambos casos, el orden es 6. Observa los residuos de las 3^{ras} potencias: Si usamos módulos negativos, ambos corresponden a (–1).
Explora unos casos adicionales. Bajo las condiciones mencionadas, ¿el residuo en la mitad del período siempre es (–1)?
Podemos ver aun más: A partir del (–1), se repiten todos los residuos anteriores en orden, pero con signo negativo. Por ejemplo las potencias de 10, (mod.7):

1, 3, 2, –1, –3, –2, 1, ...

Eso es lógico si consideramos que estas secuencias se producen por multiplicación repetida: Si empezamos con (–1) y efectuamos las mismas multiplicaciones, se produce la misma secuencia como si empezamos con 1, solamente con signo negativo.
En los números decimales, bajo las mismas condiciones, observamos algo similar: El período consiste en dos mitades, cuyas cifras se complementan mutuamente a 9. Por ejemplo en $1/7 = 0.\overline{142857}$:

```
142
857
999
```

Verifícalo con otros ejemplos como 1/13 ó 1/17.
Para pensar: ¿Puedes explicar esta observación, a la luz de la "regla" de que en el medio del período aparece un residuo de (–1)?

Pero todavía no hemos explicado de dónde viene ese (–1). Con el ejemplo (mod.7): El tercer residuo es $10^3 \equiv (-1)$ (mod.7). El sexto residuo es $10^6 \equiv 1$ (mod.7). 10^6 es 10^3 al cuadrado. Por la congruencia modular, lo mismo tiene que ser verdadero para los residuos; y efectivamente, $(-1)^2 = 1$.

¿Y si el divisor no es primo? - Observa las potencias de 5, (mod.12): 1, 5, 1, 5, ...
El orden es 2, pero el residuo del "medio período" es 5, no (–1). Sin embargo, sigue siendo verdad que $(5^1)^2 = 5^2$. Puedes verificar que $5^2 \equiv 1$ (mod.12). (Y también $7^2 \equiv 1$ (mod.12).)
O sea, si calculamos (mod.12), existen *cuatro* "raíces cuadradas de 1": 1; (–1); 5; y 7.
Calculando (mod.***m***), observamos lo mismo con casi todas las ***m*** compuestas: Existen más que dos números que elevados al cuadrado son congruentes con 1.

Por eso también en los números decimales, si el denominador de la generatriz es compuesto, las dos mitades del período normalmente no se complementan a 9. Por ejemplo $1/21 = 0.\overline{047619}$; y los residuos de las potencias de 10 (mod.21): 1, 10, 16, 13, 4, 19, 1, ...
Aquí no aparece el (–1) en el medio del período.

Para hacer: Plantea e investiga unas preguntas propias acerca de las "raíces cuadradas modulares".

El "teorema pequeño" de Fermat

Hemos visto que **para cada número primo *p*,** $\Phi(p) = p-1$, y por tanto $b^{p-1} \equiv 1$ **(mod.*p*) para cada base *b* < *p*.**
Eso es la primera mitad de lo que se llama "el teorema pequeño de Fermat". La otra mitad dice que también lo inverso es verdadero:

> **Si para algún número *p*, $b^{p-1} \equiv 1$ (mod.*p*) para cada base *b* < *p*, entonces *p* es primo.**

(*Demostración:* Si ***p*** es compuesto, entonces existen bases ***b*** < ***p*** que tienen un divisor común con ***p***. En las potencias de éstas no puede ocurrir ningún residuo de 1.)

Eso permite teoréticamente saber de cada número si es primo o no, sin necesidad de factorizarlo. De hecho, para la mayoría de los números compuestos, evaluar las potencias de una o dos bases ya es suficiente para descubrir que b^{p-1} no es congruente a 1 (mod.***p***), y así se sabe que ***p*** es compuesto. Por ejemplo para ***p***=9:

$2^8 = 256 \equiv 4$ (mod.9);
$3^8 = 6561 \equiv 0$ (mod.9);
$4^8 = 65536 \equiv 7$ (mod.9);
$5^8 \equiv (-4)^8 \equiv 7$ (mod.9);
$6^8 \equiv (-3)^8 \equiv 0$ (mod.9);
$7^8 \equiv (-2)^8 \equiv 4$ (mod.9).

Una prueba con cualquiera de estas bases ya revela que 9 es compuesto.
Desafortunadamente, la cosa no es siempre tan fácil. Por ejemplo, $2^{340} \equiv 1$ (mod.341); sin embargo 341 es compuesto. Se dice que "341 es un pseudoprimo de Fermat a la base 2."

Este caso todavía no es grave. Usamos 3 como base: $3^{340} \equiv 56$ (mod.341), y el impostor ya queda al descubierto.

Pero hay casos más resistentes. Por ejemplo $\boldsymbol{b}^{560} \equiv 1$ (mod.561) para *toda* base ***b*** que es PESI con 561. Sin embargo, 561 es compuesto.

Este tipo de números se llaman "números de Carmichael". Existen pocos de ellos. Sin embargo, su existencia hace que el teorema pequeño de Fermat, por sí solo, no sea lo suficientemente eficaz para detectar números primos.

Para pensar: ¿Cuál es la propiedad particular que hace que ciertos números sean "pseudoprimos", o "números de Carmichael"?

La prueba de Miller-Rabin

Esta prueba, más eficiente para detectar primos, combina el teorema pequeño de Fermat con el tema que vimos antes, el de las raíces cuadradas modulares. La prueba de Miller-Rabin escoge al azar varias bases ***b***, y evalúa con cada una de ellas:

¿Se cumple el teorema pequeño de Fermat (mod.***n***) en base ***b***? - Si no, se sabe que ***n*** es compuesto, y la prueba termina.

¿La sucesión de los residuos (mod.***n***) contiene alguna raíz cuadrada modular de 1 que no sea 1 ó (–1)? (Eso se evalúa, dividiendo el período de (***n***–1) sucesivamente en dos, hasta que su longitud se vuelve impar, o hasta que aparece un residuo de (–1).) - En caso que sí, se sabe que ***n*** es compuesto, y la prueba termina.

A menudo, una única base es suficiente para establecer que ***n*** es compuesto. Por ejemplo para el "número de Carmichael" 561, aunque parece cumplir el pequeño teorema de Fermat con la base 2, la prueba de las raíces modulares falla: $2^{280} \equiv 1$ (mod.561); $2^{140} \equiv 67$ (mod.561); entonces 67 es una raíz cuadrada de 1 (mod.561), y por tanto 561 es compuesto.

Si ***n*** ha pasado la prueba con varias bases exitosamente, se puede afirmar con *casi* 100% de seguridad que ***n*** es primo. El único problema es que queda una probabilidad mínima, aunque extremamente pequeña, de que ***n*** podría ser compuesto.

Aun así, con ***n*** muy grandes, la prueba de Miller-Rabin es enormemente más eficaz que cualquier método de factorización. Su probabilidad de fallar se puede disminuir aun más, probando con más bases. Y se puede combinar con otras pruebas, más sofisticadas, que permiten establecer con *absoluta* seguridad que ***n*** es primo, sin necesidad de conocer ninguno de sus factores. *(Vea también "Para programadores".)*

Para hacer: Este tipo de pruebas normalmente se efectúan con una computadora, y con números de cientos de cifras. Pero ¿sería factible, aplicar "a mano" una prueba de Miller-Rabin a un número de, digamos, diez cifras? ¿Cuántas multiplicaciones modulares habría que efectuar para eso, aproximadamente, si lo haces de la manera más "económica" posible? ¿Quisieras probarlo con un ejemplo?

Para programadores

PARI permite calcular el orden de un grupo de residuos de potencias, con la palabr a clave **znorder**(m).

m tiene que ser un número modular *(vea Unidad N 2)*, y sus componentes tienen que ser PESI, de otro modo la función devuelve un error.

Ejemplo:

```
> znorder(Mod(3,11))
%1 = 5
```

Para pensar: PARI no te permite calcular p.ej. directamente el orden de las potencias de 2, (mod.10):

```
> znorder(Mod(2,10))
***   at top-level: znorder(Mod(2,10))
***                 ^----------------
*** znorder: elements not coprime in
znorder:
```

El mensaje de error nos dice que los elementos (2,10) no son PESI.

¿Cómo tienes que hacerlo entonces, si quieres usar PARI para calcular el orden de una sucesión de residuos de potencias en un caso como éste?

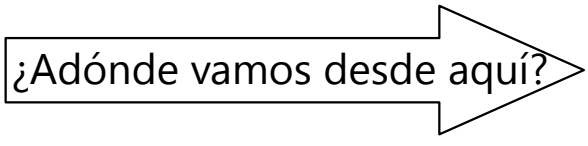
- PARI permite también probar si un número es primo, con diferentes métodos:

ispseudoprime(n) hace una prueba rápida, pero no absolutamente segura. Esa prueba combina la prueba Miller-Rabin con la prueba Lucas (un procedimiento que usa otras propiedades). Los autores de PARI dicen que esta prueba detecta correctamente todos los primos < 2^{64}, y que hasta ahora no se encontró ningún número mayor donde esta prueba hubiera dado un resultado equivocado; sin embargo se sospecha que tales números pueden existir.

isprime(n) hace una prueba más extensa, que demora más, pero que es 100% segura.

Las dos funciones mencionadas dan como resultado 1, si ***n*** es primo; 0, si ***n*** es compuesto.

primecert(n) hace la misma prueba como **isprime**(n); pero si ***n*** es primo, devuelve como resultado un vector con números que sirven como "certificado de número primo"; o sea, que permiten *demostrar* con seguridad que ***n*** es primo. (El manual de PARI describe cómo interpretar esos números, y cuáles son los principios matemáticos que lo fundamentan.)

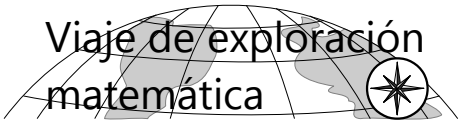


Las siguientes Unidades son opcionales. Puedes estudiarlas en cualquier orden, si deseas explorar unos temas adicionales de la teoría de números.

Unidad N 6 - Residuos cuadráticos y problemas relacionados

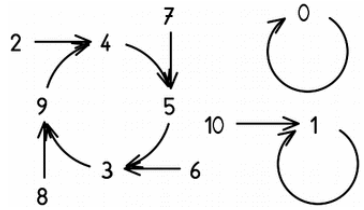
Prerrequisitos:
- Concepto de residuo cuadrático *(Secundaria I, Unidad 37).*

Nota: *Los temas de esta Unidad son opcionales; no figuran en los currículos escolares usuales.*

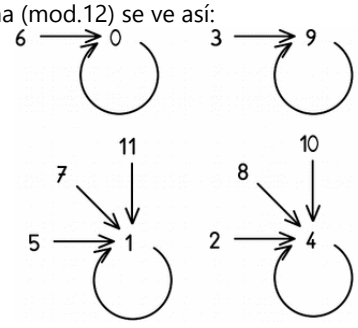


Diagramas de cuadrados modulares

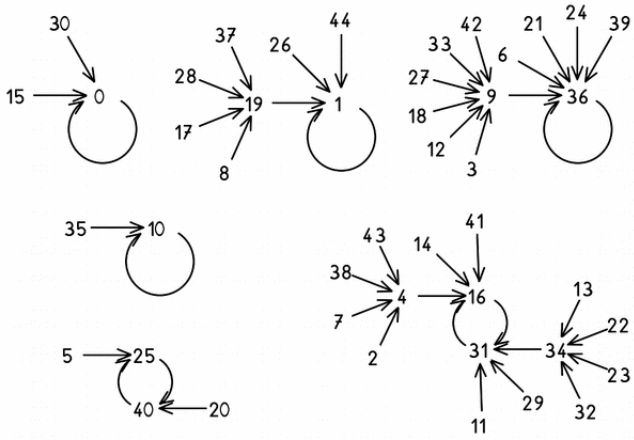
En el siguiente diagrama, la flecha significa "elevar al cuadrado, (mod.11)":



Vemos que de cada número sale una flecha, porque todos los números se pueden elevar al cuadrado. Pero no todos los números reciben flechas, sino solamente los que son residuos cuadráticos (mod.11); porque los otros no tienen raíz cuadrada modular. En este diagrama, todos los números con excepción del cero tienen *dos* raíces modulares, las cuales se complementan a 11.
Es interesante también que los números 4, 5, 3, 9, forman una secuencia cíclica, o sea se repite periódicamente.
El diagrama (mod.12) se ve así:



Aquí notamos que la mayoría de los números tienen *cuatro* raíces modulares.
Al examinar números mayores, aparecen patrones más aventurosos. El siguiente es el diagrama (mod.45):



Construye tus propios diagramas con otros números, e investiga las propiedades que revelan. Examina especialmente las diferencias entre los diagramas para números primos, para números que son el doble de un número primo, y para números compuestos. Quizás encuentras unas leyes matemáticas interesantes.

Aquí unas preguntas concretas para investigar:
1) ¿Por qué, si ***m*** es compuesto, existen menos residuos cuadráticos (mod.***m***) diferentes que si ***m*** es primo?
2) ¿Por qué, si ***m*** es compuesto, muchos números tienen más que dos raíces cuadradas (mod.***m***)? ¿y por qué, si ***m*** es primo, no tienen más que dos?
3) Demuestra o refuta: "Si ***r*** es un residuo cuadrático (mod.***m***), y (–1) es un residuo cuadrático (mod.***m***), entonces (–***r***) es un residuo cuadrático (mod.***m***)."
4) Igualmente: "Si ***r*** es un residuo cuadrático (mod.***m***), y (–1) no es un residuo cuadrático (mod.***m***), entonces (–***r***) tampoco es un residuo cuadrático (mod.***m***)."
5) ¿En qué se distinguen aquellos números primos ***m*** donde (–1) es un residuo cuadrático (mod.***m***)?

Cuadrados que repiten su propia raíz

6) $25^2 = 625$; en el cuadrado (625) se repite la raíz entera (25). ¿Existen otros números donde sucede lo mismo? ¿quizás aun con más que dos cifras? ¿Cuántas cifras puede un tal número tener, a lo máximo? ¿Cómo se pueden encontrar tales números de una manera sistemática?

Dos otros problemas

7) ¿En qué sistema de numeración es 11572 un cuadrado perfecto?

***8)** Christian Goldbach conjeturó que cada número compuesto impar se puede escribir como la suma de un número primo más el doble de un cuadrado perfecto:

$9 = 7 + 2\cdot1^2$, $15 = 7 + 2\cdot2^2$, $21 = 3 + 2\cdot3^2$, etc.

Pero la conjetura resultó falsa. ¿Cuál es el menor número compuesto impar que no se puede escribir de esta manera? *(Podrías necesitar una computadora...)*

Sherlock Numbers y los cuatro residuos

VI

El detective revisó su lista. 811 obviamente era demasiado pequeño. El siguiente número en la lista era 6047. "Ahora, ¿cómo sabré si este número puede producir un residuo de 622? ¿Probar con todos los divisores en el rango? No tengo tiempo para eso ..."

Pero pronto se le ocurrió una idea. Parecía que la visita donde el Dr.Raíz había reactivado sus neuronas matemáticas. "Le *resto* 622, entonces el resultado debe ser un múltiplo del divisor. Y un número no puede ser múltiplo de muchos números a la vez ... así reduciré las opciones para el divisor."

Dicho y hecho. 6047 – 622 = 5425. "Ahora, que el calculador me busque los divisores de 5425."

Salió: 1, 5, 7, 25, 31, 35, 155, 175, 217, 775, 1085, 5425.

"A ver, con 5 no puede dar un residuo de 622. Con 7 tampoco.

... "Con 775 sí funcionaría ... pero es demasiado grande para ser usado en una prueba de división aquí. No funciona con este número. El siguiente primo en la lista:"

13901 – 622 = 13279.

Sus divisores: 1, 7, 49, 271, 1897, 13279.

Pero aquí tampoco se encontró un divisor adecuado que pudiera producir un residuo de 622. Numbers siguió probando con los siguientes números ...

Por fin exclamó: "¡Productos y cocientes! ¡Los primos en esta lista están *lejos* del tamaño requerido para una solución! ¿Por qué no me di cuenta antes? Para que un número tenga un factor menor en el rango de 622, ¡tendría que ser por lo menos 622 al cuadrado! Otra vez a hacer trabajar el calculador."

Esta vez hizo una búsqueda de primos mayores – pero siempre cumpliendo las condiciones, por supuesto. La nueva lista se veía así:

390893, 422309, 432781, 438017, 445871, 464197, 472051, 495613, 524411, 534883, 540119, 555827, 589861, 595097, 602951, 634367, 657929, 660547, 665783, 673637, 684109, 699817, 705053, 707671, 723379, 731233, 736469, 739087, 752177, 770503, 775739, 778357, 786211, ...

Y nuevamente a examinar los números, si alguno de ellos cumplía las condiciones.

390893 – 622 = 390271

Sus divisores: 1, 7, 127, 439, 889, 3073, 55753, 390271

"Una división entre 889 sí podría producir un residuo de 622 – pero otra vez, 889 ya es demasiado grande para la prueba de divisiones."

422309 – 622 = 421687

Sus divisores: 1, 7, 107, 563, 749, 3941, 60241, 421687

Y otra vez no se encontró ningún divisor adecuado.

432781 – 622 = 432159

Los divisores: 1, 3, 7, 13, 21, 39, 91, 273, 1583, 4749, 11081, 20579, 33243, 61737, 144053, 432159

"¡Tantos divisores, pero no funciona con ninguno! Todos son demasiado pequeños, o demasiado grandes. Eso se hace más largo de lo que pensé..."

Pero algo más se le ocurrió a Sherlock. "¿No me dijo el buen doctor que en la prueba de división se divide entre números *primos*? Ese calculador me da muchos divisores que no son primos, así que de todos modos no sirven. Tengo que reprogramarlo para que me dé solamente los factores primos. Bueno, esa no es mi profesión, así que no podré evitar equivocarme de vez en cuando." – Y el detective empezó a preguntarse si no debía haber encargado este trabajo al matemático, aun con el riesgo de entregarle unos datos confidenciales.

Pero ahora, por lo menos resultaron menos números para comprobar:

445871 – 622 = 445249 = 7· 63607 (Obviamente no funciona.)

464197 – 622 = 463575 = 3·5·5·7·883 (¿Podría funcionar con el 883? – Pero no, es demasiado grande.)

Y así continuó el detective, hasta que por fin encontró una solución:

778357 – 622 = 777735 = 3·3·3·5·7·823

¡...y 823 era un número que todavía podía aparecer en la prueba de división aquí!

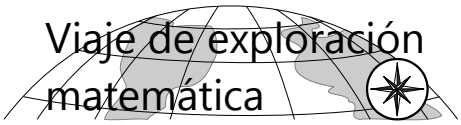
Desafío a los lectores:

Como ves, eso no se podría haber calculado "a mano" ... o solamente con ***mucha*** *perseverancia. Pero si el último residuo hubiera sido más pequeño – si hubiera sido, digamos, 36 en vez de 622 –, ¿podrías en ese caso tú mismo encontrar la solución?*

Unidad N 7 - Tripletos pitagóricos y ladrillos de Euler

Prerrequisitos:

Nota: *Los temas de esta Unidad son opcionales; no figuran en los currículos escolares usuales.*



Tripletos pitagóricos

Según el teorema de Pitágoras, en un triángulo rectángulo con catetos **a**, **b** e hipotenusa **c**, se cumple que $\mathbf{a^2 + b^2 = c^2}$. Ahora es un desafío interesante, descubrir qué triángulos rectángulos existen donde todos los lados son números enteros, como p.ej. 3, 4 y 5 ($3^2 + 4^2 = 5^2$). Tales grupos de tres lados "enteros" se llaman "tripletos pitagóricos".

a) Demuestra que todos los múltiplos de un tripleto pitagórico son también tripletos pitagóricos. O sea, si 3, 4, 5 es un tal tripleto, entonces lo son también p.ej. 6, 8, 10 ó 12, 16, 20.

b) Encuentra más tripletos pitagóricos. Después de demostrar a), podemos limitarnos a tripletos sin divisores comunes. Esos se suelen llamar "tripletos primitivos". - ¿Puedes descubrir un método para encontrar un número ilimitado de tales tripletos?

***c)** ¿Puedes incluso encontrar una fórmula generalizada que describe *todos* los tripletos pitagóricos posibles?

***d)** En un triángulo rectángulo e isósceles, la hipotenusa mide igual como un cateto multiplicado por la raíz cuadrada de 2. Entonces, si encontramos un tripleto pitagórico donde los catetos miden aproximadamente lo mismo, tendremos una aproximación racional a la raíz de 2.
- Por ejemplo, 20, 21, 29 es un tripleto pitagóricos, entonces la raíz de 2 se encuentra entre 29/20 y 29/21, o sea, en aproximadamente 58/41. (Efectivamente, esta aproximación es correcta hasta tres decimales.) ¿Cómo se pueden encontrar otros tripletos que dan una aproximación aun más exacta? - Lo mismo para la raíz de 3, de 5, etc. ...

- ¿Existe algún tripleto donde los catetos son *exactamente* iguales? ¿O puedes demostrar que no existe?

Ladrillos de Euler

e)** Un "ladrillo pitagórico" es un prisma rectangular cuyos lados tienen medidas de números enteros, y donde también todas las diagonales laterales tienen medidas enteras. Se llaman también "ladrillos de Euler", porque Leonardo Euler describió este problema en detalle. En otras palabras, si los aristas miden ***a, b, c, entonces es $\boldsymbol{a}^2 + \boldsymbol{b}^2 = \boldsymbol{d}^2$, $\boldsymbol{a}^2 + \boldsymbol{c}^2 = \boldsymbol{e}^2$, $\boldsymbol{b}^2 + \boldsymbol{c}^2 = \boldsymbol{f}^2$, donde ***d***, ***e***, ***f*** son también números enteros. ¿Puedes encontrar "ladrillos pitagóricos"? ¿y un método o una fórmula para encontrarlos?

*****f)** ¿Existen también "ladrillos pitagóricos" donde además la *diagonal espacial* (la que pasa por el centro del ladrillo) tiene una medida entera? (Se llaman también "ladrillos de Euler perfectos".) ¿O se puede demostrar que no existen? - Según las informaciones que me son accesibles, este problema todavía no fue solucionado por nadie. Entonces, ¡si lo solucionas, eres un verdadero genio!

Unidad N 8 - Ecuaciones diofánticas cuadráticas y superiores

Prerrequisitos:
- Introducción a las ecuaciones diofánticas *(Secundaria I, Unidad 35).*
- Operaciones con expresiones algebraicas y con ecuaciones
- Te ayudará si antes realizaste unas investigaciones acerca de temas relacionados, como por ejemplo: Residuos cuadráticos; Sumas de cuadrados; Tripletos pitagóricos *(Unidades N 6, N 7)*.

Nota: *Los temas de esta Unidad son opcionales; no figuran en los currículos escolares usuales.*

Como hemos visto, las ecuaciones diofánticas lineales normalmente no son muy difíciles. En cambio, las ecuaciones diofánticas de segundo grado pueden presentar dificultades inesperadas. Los problemas acerca de los tripletos pitagóricos y ladrillos pitagóricos *(vea N 7)*, son ejemplos de ecuaciones diofánticas de segundo grado.
Los siguientes ejemplos ampliarán un poco este tema:

a) ¿Encuentras todas las soluciones de esta ecuación diofántica?

$$x^2 + 720 = y^2$$

(Recuerda que todas las soluciones tienen que ser números naturales.)
¿Cómo puedes proceder para estar seguro de que hayas encontrado *todas* las soluciones?

b) ¿Cuántas soluciones tiene esta ecuación diofántica?

$$28x + 25 = y^2$$

¿Puedes describir el conjunto solución completo con una fórmula generalizada?

c) Lo mismo para la siguiente ecuación diofántica:

$$8x + 45 = y^2$$

d) Un número, escrito en un determinado sistema de numeración, es **136**. En un sistema con otra base, el mismo número se escribe **514**. ¿Cuál es el número en el sistema decimal, y cuáles son las bases de los otros sistemas de numeración?
(¿Encuentras un procedimiento abreviado, con el cual no necesitas probar todas las posibilidades? - ¿Cuántas soluciones puedes encontrar?)

e) ¿Cuántas soluciones de la siguiente ecuación diofántica encuentras?

$$a^2 + ab + b^2 = c^2$$

– ¿Encuentras una "receta" generalizada para encontrar *todas* las soluciones?

***f)** ¿Encuentras (por lo menos) una solución de esta ecuación diofántica? $61x^2 + 1 = y^2$

- Recuerda que el cero no es ningún número natural; de otro modo existiera una solución demasiado fácil...
(Advertencia: Aquí no llegarás a la meta probando al azar.)

***g)** Si tienes una solución de una ecuación diofántica de la forma $ax^2 + 1 = y^2$, ¿cómo puedes encontrar otras soluciones de una manera sistemática?

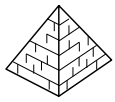
****h)** ¿Encuentras un procedimiento general para solucionar ecuaciones diofánticas de la forma

$$ax^2 + b = y^2 \quad ?$$

¿O por lo menos de la forma $ax^2 + 1 = y^2$?

i) ¿Qué otras formas de ecuaciones diofánticas cuadráticas encuentras? Plantea algunas, e intenta resolverlas.

Un poco de historia



El problema f) alcanzó fama histórica. El matemático francés Pierre de Fermat propuso este problema en el año 1657, y sus contemporáneos demoraban aproximadamente un año para solucionarlo. Recién 70 años más tarde encontró Leonardo Euler unas pautas para un procedimiento generalizado para solucionar ecuaciones diofánticas de la forma $ax^2+1=y^2$; este método fue completado por Lagrange en 1766.
(La mayoría de los matemáticos se hicieron famosos por los problemas que resolvieron. Fermat es una excepción: su fama se basa más que todo en los problemas sin resolver que él dejó a la posteridad. Con sus problemas proveyó trabajo para los matemáticos después de él, durante trescientos años.)
- Lo que los matemáticos europeos de aquel tiempo no sabían, era que el matemático hindú Brahmagupta ya en el año 628 propuso y resolvió ecuaciones de este tipo, incluída la de nuestro problema. Y ya en 1150, Bhaskara II había encontrado un procedimiento general aun más sencillo que el de Lagrange.

Sherlock Numbers y los cuatro residuos

VII

Apresuradamente, Sherlock Numbers se dirigió al cuartel general de la policía, a buscar al inspector Cuadrícula. Con él tenía algo de confianza, ya que le habia asistido un poco en unos casos anteriores.

– "Me han encargado de buscar a un cierto 778357. ¿Por casualidad fue reportado como desaparecido durante los últimos meses?"

El inspector se puso a rebuscar los registros. "Sí, existen dos personas que corresponden a ese número", dijo por fin. "Pero no hay ningún reporte al respecto. Le puedo dar las direcciones, si es que no las usará para propósitos ilícitos."

– "Por supuesto que no", se rió Numbers. "Al contrario, es para *impedir* unos propósitos ilícitos."

– "Aquí tiene."

Para tener un pretexto, Numbers se proveyó de unas invitaciones a un Club de Primos fundado el año anterior, y se puso a hacer averiguaciones en las direcciones indicadas. Encontró a ambos 778357 en casa, en buen estado, y no notó nada sospechoso. En ambos casos, los vecinos confirmaron que las personas en mención no se habían ausentado por un tiempo prolongado últimamente.

"Tengo que admitir que me equivoqué", dijo Numbers para sí mismo. "Pero no me atrevo a dudar de la precisión del calculador. El Dr.Raíz suele usar equipos de buena calidad. Mas bien ... él me dijo que pueden existir varias soluciones. Tendré que buscar entonces la siguiente solución."

Así que, otra vez a hacer trabajar el calculador. La nueva lista de números primos se extendió a más allá de un millón. Y después de otro tiempo de trabajo arduo, que no relataré en detalle, el detective perseverante encontró la siguiente solución:

$1'294'103 - 622 = 1'293'481 = 7 \cdot 257 \cdot 719$

... y el factor 719 puede producir un residuo de 622, y también aparecer en una prueba de división para este número.

"Qué atrevidos, secuestrar a un número en el rango millonario", pensó Numbers. Y se dirigió nuevamente a la oficina del inspector Cuadrícula para solicitar información.

– "¿No vino ya hace unos días por un asunto similar?", preguntó el inspector. "¿Qué es eso de buscar desaparecidos que no han desaparecido?"

– "De haber desaparecido alguien, de eso no tengo dudas", respondió Numbers. "Solamente acerca del número exacto existen unas inseguridades. Espero estar en lo cierto esta vez; pero sinceramente, no se lo puedo garantizar."

– "Es como la última vez", dijo del inspector, después de consultar los registros. "La persona existe, pero no figura como desaparecido. No vaya a causar falsas alarmas, por favor."

– "Descuide, inspector, descuide", lo tranquilizó el detective. "Mis métodos son discretos. De matemática discreta, para decir así. No estoy alarmando a nadie, ni siquiera a la policía. Todavía no."

Problemas diversos

(Para 1) a 3): Letras distintas significan cifras distintas.)

1) ¿Cuáles números cumplen $\overline{abcd}_{\mathbf{8}} = \overline{efg}_{\mathbf{9}}$?

2) ¿y cuáles cumplen $\overline{abc}_{\mathbf{6}} = \overline{def}_{\mathbf{12}}$?

3) $\overline{abc}_{\mathbf{8}} + \overline{bca}_{\mathbf{8}} + \overline{cab}_{\mathbf{8}} = \overline{defg}_{\mathbf{8}}$ $(\boldsymbol{a}<\boldsymbol{b}<\boldsymbol{c})$

4) Encuentra la menor solución posible para:
$123_{\boldsymbol{x}} + 442_{\boldsymbol{y}} = 964_{\boldsymbol{z}}$

***5)** Halla $\boldsymbol{x}$, $\boldsymbol{y}$, en: $198_{\boldsymbol{x}} + 449_{\boldsymbol{y}} = 713_{\boldsymbol{x}}$

6) ¿Cuál es el significado de cada una de las letras en "matematica", sabiendo que
$\overline{matematica}_{\boldsymbol{6}} = \overline{maattaai}_{\boldsymbol{6}} \cdot \overline{mat}_{\boldsymbol{6}}$?

***7)** Un número $\overline{a0bc}$ es igual a $\overline{bc} \cdot \overline{bac}$.
La suma de todos sus divisores es igual a $\overline{a} \cdot \overline{ac} \cdot \overline{bac}$.
Si a esta suma le restamos el número mismo, obtenemos $\overline{ab} \cdot \overline{abc}$. ¿Cuál es el número?

8) Resuelve: $\overline{cabe}^2 = \overline{162bcdec}$

***9)** Encuentra números naturales $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, de manera que $2^{\boldsymbol{a}} \cdot 9^{\boldsymbol{b}} \cdot \boldsymbol{c} = \boldsymbol{a}^{\boldsymbol{c}} \cdot 10\boldsymbol{b}$.

10) Encuentra un tripleto pitagórico ($\boldsymbol{a}^2 + \boldsymbol{b}^2 = \boldsymbol{c}^2$), donde $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} = 1000$.

11) Los números de Kaprekar son cuadrados perfectos que se pueden separar en dos grupos de igual cantidad de dígitos, que juntos suman su raíz. Por ejemplo:

$\sqrt{2025} = 20 + 25 = 45$.

Nota: *Aquí no se requiere que las cifras sean distintas; en un número se pueden repetir cifras iguales.*

a) Encuentra números de Kaprekar con 6 dígitos.
$\left(\sqrt{\overline{abcdef}} = \overline{abc} + \overline{def}\right)$

b) Si permitimos grupos con diferente número de dígitos, ¿existen números de Kaprekar con 5 dígitos?
$\left(\sqrt{\overline{abcde}} = \overline{ab} + \overline{cde}\text{ , ó }\overline{abc} + \overline{de}\right)$

Ecuaciones diofánticas de grado superior

1. (Investigación preliminar)
En las ecuaciones diofánticas cúbicas, encontrarás que casi siempre te conducen a estas factorizaciones conocidas:

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$
$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

Investiga entonces primero unas propiedades de los números de la forma $a^2 \pm ab + b^2$:
a) Haz una lista de tales números. Después observa: ¿Cuáles números se pueden expresar de esta forma? O sea, ¿cómo puedes predecir si un número determinado se puede expresar en la forma $a^2 \pm ab + b^2$, o no?
b) ¿Puedes encontrar alguna relación llamativa entre los números de la forma $a^2 + ab + b^2$, y los de la forma $a^2 - ab + b^2$?
c) En la *Unidad A 9* hemos examinado las propiedades de los números que son la suma de dos cuadrados perfectos ($a^2 + b^2$). Allí encontramos que el conjunto de estos números es cerrado respecto a la multiplicación. O sea, el producto de dos números de la forma $a^2 + b^2$ es a su vez un número de la forma $a^2 + b^2$; y cada número de la forma $a^2 + b^2$ o es el producto de dos de esos números, o es primo. Los números que examinamos ahora, ¿tienen una propiedad similar? *¿Puedes demostrarlo?

2. Residuos cúbicos:
Resuelve algunas ecuaciones diofánticas de la forma $ax + b = y^3$, para diversas a y b. Por ejemplo:
$10x + 7 = y^3$, $9x + 1 = y^3$, $9x + 4 = y^3$, etc.
En otras palabras, estamos investigando en qué casos es b un residuo cúbico módulo a.

3. Resuelve unas ecuaciones diofánticas de la forma:
$x^3 + a = y^3$.
¿Para cuáles a hay una solución? ¿Para cuáles no?
¿Encuentras alguna a para la cual existen dos o más soluciones? - La respuesta está relacionada con el siguiente problema (4).
Investiga también las mismas preguntas para la ecuación $x^3 + y^3 = a$.

4. Investiga la ecuación $x^3 + y^3 = z^3 + v^3$. Intenta descubrir una estrategia práctica para encontrar soluciones.
Este problema originó una anécdota acerca de la vida del matemático indio Srinivasa Ramanujan (1887-1920). Su talento matemático fue descubierto por el matemático inglés G.H.Hardy, y Hardy lo trajo a Inglaterra para trabajar con él. Pero después de pocos años, Ramanujan se enfermó gravemente. Un día, Hardy fue a visitarlo en el hospital. Al verlo, le dijo: "Llegué en un taxi con el número 1729. Un número bastante aburrido." – Ramanujan respondió: "¿Aburrido? ¡Es un número muy interesante! Es el menor número que se puede expresar de dos maneras como la suma de dos cubos perfectos."
– O sea, es la primera solución de nuestro problema. Desde entonces, los matemáticos llaman a estos números los "números de taxi". (¿Ya encontraste los números x, y, z, v, cuyos cubos de dos en dos suman 1729?) Ahora puedes investigar cómo encontrar otros "números de taxi".
El problema se puede ampliar: ¿Cuáles números se pueden expresar de *tres* maneras como la suma de dos cubos? - ¿Cuáles números se pueden expresar de dos maneras como la suma de dos *cuartas potencias*? - Etc.

***5. El problema de los tres cubos**
¿Cuáles números naturales a se pueden expresar como la suma de tres cubos perfectos?
O sea, $x^3 + y^3 + z^3 = a$.
Este problema es más interesante cuando permitimos que x, y, z sean también números negativos, o cero. Puedes probar con todas las a en orden: 1, 2, 3, 4, ...
Encontrarás que para muchas a se puede encontrar una solución relativamente fácil (con $|x|$, $|y|$, $|z|$ todas < 20).
Además existe una clase específica de números a, para los cuales no existe ninguna solución. *¿Cuál es la característica particular de esos números? ¿Puedes demostrarlo?
Y finalmente, hay unos números a que tienen solución, pero solamente con números muy grandes. El primero de ellos es el 30. Por mucho tiempo era desconocido si existe una solución para los números 33 y 42. Recién en el año 2019 se encontraron soluciones para esos números, con la ayuda de 500'000 computadoras unidas en red. La solución para el 42 es:
$(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42$
Los matemáticos conjeturan que deben existir soluciones para todas las a que no están en la categoría de las "imposibles" (vea la pregunta anterior). Pero todavía nadie logró demostrarlo.

6. Encuentra soluciones para esta ecuación diofántica:

$$x^2 + y^3 = z^4$$

¿Encuentras un procedimiento o una fórmula que describe las soluciones?

7. Investiga esta ecuación diofántica:

$$x^3 + y^2 = z^3$$

Se pueden encontrar tres clases de soluciones. Una de ellas permite encontrar infinitas soluciones de una manera muy fácil. La segunda y la tercera clase son más difíciles de encontrar; y necesitas para ellas las propiedades que descubriste en el problema 1.

Sumas y diferencias de cuadrados perfectos

¿Puedes demostrar las siguientes afirmaciones (o encontrar un contraejemplo)?

a) La diferencia de dos cuadrados perfectos *no sucesivos* nunca es un número primo.
(P.ej. 100 – 49 = 51, 51 = 3 · 17.
Pero 36 – 25 = 11 primo; 25 y 36 son los cuadrados de dos números sucesivos; por tanto el teorema no se aplica a este caso.)

b) La suma de un cuadrado *par* con un cuadrado *impar* es un número primo, si es que los dos cuadrados son primos entre sí.
(P.ej. 25 + 4 = 29 primo, 100 + 49 = 149 primo.
Pero 36 + 81 = 117 = 9 · 13, porque 36 y 81 tienen el 9 como divisor común.)

c) Todas las sumas de dos cuadrados *impares* son divisibles entre 2, pero no entre 4.
(P. ej. 25 + 9 = 34, 34 es par, pero no es divisible entre 4.)

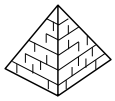
d) Todas las diferencias de dos cuadrados *impares* son divisibles entre 8.
(P.ej. 49 – 25 = 24, 24 es divisible entre 8.)

e) Como seguramente sabes, la suma de dos cuadrados perfectos ($\boldsymbol{a}^2 + \boldsymbol{b}^2$) no se puede factorizar en el caso general. Sin embargo, existe una ley acerca de las multiplicaciones y divisiones entre números que son sumas de dos cuadrados, y es la siguiente:
El conjunto de los números naturales que se pueden representar como suma de dos cuadrados perfectos, es un grupo cerrado respecto a la multiplicación.

En otras palabras:
(1) El producto de dos números que son sumas de dos cuadrados, es a su vez la suma de dos cuadrados.
(2) Un número que es suma de dos cuadrados, o es el producto de dos números que son sumas de cuadrados, o es primo.
(Para que esta ley tenga aplicación universal, se debe incluir entre los números "sumas de cuadrados" también los mismos cuadrados perfectos, p.ej. 25 = 25+0.)
El desafío: Demostrar la validez universal de esta ley, de manera matemática-algebraica.
Pauta adicional y nota histórica: Demostrar el enunciado (1) es relativamente fácil; lo descubrió Brahmagupta en la India en el siglo VII. Solamente hay que multiplicar algebraicamente dos sumas de cuadrados, y transformar el resultado de manera adecuada para que se pueda expresar como la suma de dos cuadrados perfectos. - Su inverso (2), en cambio, no es tan fácil de demostrar. Por primera vez lo hizo el suizo Leonardo Euler en el siglo XVIII. Entonces, si logras demostrarlo, ya estás en camino de ser un genio.

f) *Desafío adicional:* Demostrar que el producto de dos sumas de cuadrados perfectos, se puede representar como suma de dos cuadrados perfectos *de dos maneras distintas* como mínimo.
Por ejemplo: 5=1+4, 13=4+9, 5·13 = 65. Ahora, 65 = 1+64 = 16+49 (dos maneras distintas de representar 65 como suma de dos cuadrados perfectos).
(Euler usó esta propiedad para comprobar de una manera bastante rápida si un número es primo.)

Un poco de historia



La ecuación diofántica $\boldsymbol{x}^3 + \boldsymbol{y}^3 = \boldsymbol{z}^3$ no tiene solución. Es un caso particular del "Último teorema de Fermat". Después de su muerte, se encontró que Pierre de Fermat (1607-1655) había escrito en el margen de una página de su ejemplar de la "Aritmética" de Diofanto:
"No se puede descomponer un cubo en una suma de dos cubos, ni una cuarta potencia en una suma de dos cuartas potencias, ni una potencia superior en una suma de dos potencias del mismo exponente. Encontré una demostración verdaderamente maravillosa de ello, pero desafortunadamente no cabe en este margen."

Esa pequeña nota mantuvo ocupados a los matemáticos durante trescientos años. Muchos intentaron reconstruir la demostración de Fermat, pero no lo lograron. A lo máximo pudieron demostrar el teorema para ciertos exponentes específicos, pero no de manera general. Recién en 1994, Andrew Wiles pudo demostrarlo. Pero su demostración hace uso de unas herramientas de matemática avanzada que Fermat no pudo conocer.
Sigue siendo un problema sin resolver, cómo se puede demostrar este teorema con los conocimientos matemáticos que estaban disponibles en los tiempos de Fermat. Sin embargo, algunos matemáticos sospechan que quizás en realidad Fermat no tenía tal demostración; o que su demostración era errónea.

La "Aritmética" de Diofanto

Las ecuaciones diofánticas se llaman así según el libro "Aritmética" de Diofanto, que contiene muchas ecuaciones de este tipo. Solamente que hoy en día entendemos con "ecuaciones diofánticas" las que exigen *números naturales* como soluciones; mientras que las ecuaciones originales de Diofanto se resuelven en los *números racionales* (fracciones) positivas.
En su obra, Diofanto comienza con ecuaciones determinadas, lineales y cuadráticas, con métodos similares a las que seguimos usando hoy en día en el álgebra escolar. Después procede a las ecuaciones indeterminadas, o "diofánticas".
Normalmente, Diofanto presenta para cada ecuación un razonamiento que produce una única solución. Es tarea del estudiante, entender y generalizar este razonamiento para poder encontrar otras soluciones. A diferencia de los matemáticos actuales, Diofanto todavía no exigía que se describan *todas* las soluciones, ni mucho menos que se *demuestre* que las soluciones están completas.
Algunos ejemplos:

Libro II, Problema 11:
Son dados dos números a y b. Encuentra x, tal que $x+a$ y $x+b$ sean cuadrados perfectos.

Solución según Diofanto:
Establecemos las dos ecuaciones:

$x+a = y^2$ Restamos la segunda ecuación de la

$x+b = z^2$ primera, y obtenemos:

$a - b = y^2 - z^2 = (y+z)(y-z)$

Descomponemos $a - b$ en dos factores. Así tenemos $(y+z)$ y $(y-z)$. Eso nos permite calcular y y z.
(Este es uno de los pocos problemas donde Diofanto presenta una solución generalizada.)

Libro II, Problema 14:
Es dado un número a. Descompón a en dos sumandos, de manera que a cada uno de ellos se le puede sumar el mismo cuadrado, y el resultado es a su vez un cuadrado.
Solución según Diofanto:

$$x + y = a$$
$$x + u^2 = z^2$$
$$y + u^2 = v^2$$

Escoge arbitrariamente dos números b, c. Entonces es:
$u^2 + 2bu + b^2 = (u+b)^2 = z^2$
$u^2 + 2cu + c^2 = (u+c)^2 = v^2$
De ahí, $x = 2bu + b^2$, $y = 2cu + c^2$. Y su suma:
$x + y = 2u(b+c) + b^2 + c^2 = a$.
Despeja u; entonces con las ecuaciones anteriores se pueden calcular las otras incógnitas.
Nota: Puedes investigar cómo hay que escoger b, c, para obtener una solución en números naturales, según el entendimiento actual de una ecuación diofántica. ¿O existe otra estrategia mejor, si las soluciones deben ser números naturales?

Libro II, Problema 20:
Encuentra dos números, de manera que cualquiera de ellos, sumado al cuadrado del otro, resulta en un cuadrado.
Solución según Diofanto:

$$x^2 + y = z^2$$
$$x + y^2 = u^2$$

Asume que $y = 2x + 1$; con eso se cumple la primera ecuación. Sustituyendo y en la segunda ecuación, resulta: $4x^2 + 5x + 1 = u^2$.
Definimos (arbitrariamente) $u = 2x - 2$, y sustituimos. Resulta una ecuación lineal donde se puede despejar x (en este caso, $x = \frac{3}{13}$.)

Libro II, Problema 26:
Encuentra dos números, de manera que su producto sumado a cualquiera de ellos resulta en un cuadrado; y que la suma de las raíces de estos cuadrados es un número dado, por ejemplo 6.
Solución según Diofanto:

$$xy + x = z^2$$
$$xy + y = u^2$$
$$z + u = 6$$

Definimos $y = 4x - 1$; entonces la primera ecuación es:
$x(4x - 1) + x = (2x)^2 = z^2$
(Nota: y tiene que definirse de tal manera que xy es igual a un cuadrado menos x.)
Entonces la segunda ecuación es: $4x^2 + 3x - 1 = u^2$.
Según la tercera ecuación, $u = 6 - z = 6 - 2x$.
Entonces también: $u^2 = (6 - 2x)^2$.
Por tanto $4x^2 + 3x - 1 = (6 - 2x)^2$, $x = \frac{37}{27}$.

Libro III, Problema 6:
Encuentra tres números cuya suma es un cuadrado, y que también las sumas de cada dos de ellos es un cuadrado.
Solución según Diofanto:

$$x + y + z = t^2$$
$$x + y = u^2$$
$$x + z = v^2$$
$$y + z = w^2$$

Ya que $x + y = u^2$, definimos $z = 2u + 1$. Así se cumple la primera ecuación, y $t = u + 1$.
Definimos además $w = u - 1$. Entonces, según la última ecuación, $y = u^2 - 4u$. Con eso, la segunda ecuación requiere $x = 4u$.
Ahora, $x + z = 6u + 1 = v^2$. O sea, v^2 es un cuadrado que deja un residuo de 1 al dividirlo entre 6; por ejemplo 121. En este caso, $u = 20$, y así se calculan todas las otras incógnitas.

Libro IV, Problema 4:
A un cuadrado y a su raíz se suma el mismo número, y los resultados son nuevamente un cuadrado y su raíz, respectivamente.
Solución según Diofanto:

$$x^2 + y = z^2$$
$$x + y = z$$

Definimos $y = 3x^2$. Así se cumple la primera ecuación, y $z = 2x$. Entonces la segunda ecuación es $3x^2 + x = 2x$, $x = \frac{1}{3}$.)

Libro IV, Problemas 8 y 9:
8) A un cubo y a su raíz se suma el mismo número, y los resultados son nuevamente un cubo y su raíz, respectivamente.
9) A un cubo y a su raíz se suma el mismo número, y en los resultados es al revés. (O sea, la *segunda* suma es un cubo, y la *primera* suma es su raíz.)

Libro VI, Problema 16:
Encuentra un triángulo rectángulo con lados racionales, de manera que también la bisectriz de uno de sus ángulos agudos tiene una longitud racional.

Trata de resolver tú mismo(a) los últimos tres problemas. Investiga también para los otros problemas: ¿Cómo puedes generalizar el procedimiento dado por Diofanto, de manera que puedes encontrar otras soluciones? ¿Y cuáles de estos problemas se pueden resolver en números enteros?

Unidad N 9 - Problemas diversos

Prerrequisitos:
- Teoría de números (prácticamente el bloque entero).

Esta Unidad es opcional. Pero puede ser interesante y divertido, ocuparse con algunas de las curiosidades matemáticas que se presentan en los problemas de investigación.

Problemas cerrados

1) ¿Cuál es el primer número triangular que tiene más de 500 divisores?

2) Encuentra todas las fracciones con numerador 1 y un denominador < 10'000, en cuya representación decimal se repite un período de exactamente 15 cifras.

3) Divisibilidad sucesiva
Entre los números de 10 a 19 se encuentra exactamente uno que es divisible entre 10; uno que es divisible entre 11; uno que es divisible entre 12; etc, hasta 19. (Lógico...) – Lo mismo vale para los números de 11 a 20, porque 20 es nuevamente divisible entre 10.
Ahora la pregunta: *¿Dónde se encuentran los siguientes diez números sucesivos que cumplen la misma condición?*
La respuesta varía, según la definición exacta de la condición:
a) ¿Cuáles son los siguientes diez números consecutivos que cumplen la condición *en orden* – o sea, donde el *primero* de ellos es divisible entre 10, el siguiente entre 11, el siguiente entre 12, etc. hasta 19?
b) ¿Cuáles son los siguientes diez números consecutivos. donde *cada uno* de ellos es divisible entre uno de los números de 10 a 19, pero *no necesariamente en orden*? (Una tal sucesión son los números de 11 a 20, porque empieza con un múltiplo de 11, y termina con un múltiplo de 10. ¿Dónde se encuentra la siguiente?)
c) ¿Cuáles son los siguientes diez números consecutivos que juntos contienen múltiplos de todos los números de 10 a 19, pero sin la condición de que *cada uno* de los diez números tenga que ser uno de esos múltiplos? – O sea, esos diez números podrían por ejemplo contener un número que es divisible entre 13 y también entre 15; mientras que otro de los diez números (o varios de ellos) no es divisible entre ninguno de los números de 10 a 19. Pero *en conjunto* deben contener múltiplos de todos los números de 10 a 19.

4) Factorización grande
Descompón 281474976710655 en factores primos. "¡A mano!"
En serio. Pero no estoy planeando obligarte a calcular divisiones por el resto de tu vida (o diferencias de cuadrados, si aplicas el método de Fermat). Por eso te doy una pauta adicional: El sucesor de nuestro número, o sea 281474976710656, es igual a 2^{48}. El problema principal consiste entonces en descubrir cómo esta pauta te facilita la tarea enormemente.

5) Multiplicación idéntica *(Problema semi-cerrado)*
a) ¿Cuál es el mayor número natural que se puede multiplicar por 17, de manera que el producto termina con el número original completo?
Por ejemplo, el 5 es un tal número: $5 \cdot 17 = 85$, termina con 5. El siguiente número con la misma propiedad es 25, porque $25 \cdot 17 = 425$, termina con 25. Ahora, ¿cuál es el *mayor* número con esta propiedad?
(¿O quizás no existe uno "mayor"? ¿Podrían encontrarse tales números arbitrariamente grandes?)
- Exigimos además que el número no termine con cero. De otro modo podríamos simplemente añadir ceros para construir soluciones "mayores", p.ej. 500000.
b) Después de solucionar a), debes ahora poder deducir la ley generalizada que te permite encontrar números con la misma propiedad para otros factores de multiplicación. O sea, donde el número original no debe multiplicarse por 17, sino por 126, por 193, etc.
c) Investiga ahora problemas similares donde el producto termina con una versión ligeramente alterada del número original. Por ejemplo:
¿Cuál es el mayor número que se puede multiplicar por 8, tal que el producto termine con el número original, disminuido en 1?
¿Cuál es el mayor número que se puede multiplicar por 382, tal que el producto termine con el número original, aumentado en 1?
¿Encuentras aquí también una ley o un procedimiento generalizado?

6) Números al revés
a) Set pregunta: "¿De cuál número es su doble igual a su triple, escrito al revés?"
Después de pensar un tiempo, Anita responde: "Tres. Su doble es 6, escrito al revés es 9, y éso es el triple de 3."
Set queda sorprendido, después ríe y dice: "Verdad, se puede entender así. Pero yo no lo quise decir de esta manera. Estuve pensando en un número de varias cifras, y escribir sus cifras en el orden invertido. Por ejemplo si el número fuera 12, su doble sería 24, escrito al revés es 42, entonces 42 tendría que ser el triple de 12. Solamente que en este caso no es cierto, porque no es la solución."
Eso es más difícil. Anita demora bastante tiempo calculando. ¿Encuentras una solución?
b) Amplía el problema. Por ejemplo: ¿De cuál número es su cuádruple igual a su séptuple, escrito al revés?
¿De cuál número es su triple igual al número mismo, escrito al revés? - Etc.
¿Cuáles son las menores soluciones que encuentras? ¿y hay soluciones mayores, o sea con más cifras?
¿Para cuáles casos hay soluciones, para cuáles no?

Criptogramas difíciles

Los criptogramas son operaciones "cifradas", donde cada cifra de 0 a 9 es representada por un símbolo o una letra particular. Aquí una vez más las "reglas del juego":

1. Dentro de un mismo criptograma – aun si contiene varias operaciones –, símbolos iguales significan cifras iguales, y símbolos distintos significan cifras distintas. La tarea consiste en descubrir cuál símbolo significa cuál cifra, de manera que todas las operaciones son correctas.
2. De un criptograma a otro, el significado de los símbolos puede cambiar. Por ejemplo, si el criptograma no.5 contiene la letra B, y el criptograma no.9 contiene también una letra B, esa letra no necesariamente significa la misma cifra en ambos criptogramas. – En otras palabras: Cada criptograma es un problema independiente de los demás. Pero si un mismo criptograma contiene varias operaciones, ésas forman un único problema, como se describió en la Regla 1.
3. Ningún número (entero) comienza con cero. (Pero *en el interior* de un número, o en su fin, sí pueden ocurrir ceros.)
4. Los criptogramas no son álgebra. Por ejemplo "AB" no significa "A multiplicado por B". Significa un número de dos cifras; una cifra es A y la otra es B.
5. Los matemáticos verdaderos demuestran su habilidad al resolver los criptogramas a mano (sin calculadoras, computadoras, etc).

Aquí siguen entonces los criptogramas difíciles:
[EDIT !!]

a) OGIRAD ÷ O = GIRADO

b) AJ x ERROR = JAJAJA

c) △ ▽ ◁ x △ ▽ ◁ = **▲▼▲** ▷ ▽ **▼**
▲▼▲ + ▷ ▽ **▼** = △ ▽ ◁

d) ABC + ABC = DEF
ABC + DEF = GHI
(¡Este criptograma tiene <u>cinco</u> soluciones correctas!)

e)
SABES
+ SUMAR
NUMERO
(Este criptograma tiene dos soluciones correctas.)

Esta es una variación un poco más difícil de un criptograma "clásico", que se puede encontrar en muchos libros de matemática recreativa:

SEND
+ MORE
MONEY

El cuento dice que un joven se mudó a otra ciudad para estudiar, mientras que su padre pagaba por su mantenimiento. Pero el estudiante no sabía controlar sus gastos, y así se quedó pronto sin dinero. Por eso envió este telegrama a su padre ("Send more money" = "Envía más dinero"), y con eso le señaló también el monto exacto que esperaba recibir. No se sabe si el padre realmente premió las capacidades matemáticas de su hijo con este monto.

f) SU : LA = O.$\overline{\text{REPITO}}$ ...
Este es el primer criptograma con un número decimal. Dos notas acerca de este caso:
1. El número decimal es periódico. O sea, REPITO se repite infinitamente.
*2. Según la Regla 3, ningún número **entero** comienza con cero. Pero eso no aplica a números decimales. O sea, en este ejemplo, O podría ser cero..*

g) MUS x ASNO = SUMSUM

h)
⊖ ◑ ▽ x ⊗ ◫ △ ⊠
◪ ⊠ ◔ ⊠
◑ △ ▽ ◪
▽ ▽ ⊗ ◑
▽ ⊠ ▽ ◪ ▽ ⊠

i) ◫ ◨ ÷ ⊟ ⬓ = ◰,◱ ⊠ ◰ ◧ ⬒ . . .
Nota: Recuerda que en los criptogramas, un número decimal sí podría comenzar con cero.

j) ⧖ ∩ ⧠ ⧠ U □ x ○ = □ U ⧠ ⧠ ∩ ⧖

k) $\frac{A}{BC} + \frac{D}{AF} + \frac{F}{AB} = A$

Y porque fue tan bonito, aquí otro ejemplo del mismo tipo:

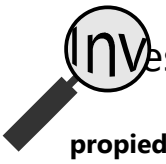
l) $\frac{☺}{⊖\ ◨} + \frac{☺}{◨\ ⊖} + \frac{⊖}{◨\ ⊠} = ◨$

m) Y aquí viene el "aumento". Los verdaderos investigadores y aficionados a la matemática calculan también la raíz cuadrada a mano, con lápiz y papel (¿o sabes hacerlo en la cabeza, como Leonardo Euler?). Entonces, ¡mucha suerte al calcular algo como 90 raíces cuadradas!

$\sqrt{\text{TE}}$ = E.VAINILLA . . .

Repito aquí la nota anterior: En un criptograma, un número decimal sí puede comenzar con cero.

Y, por si acaso: Recordarás que la representación decimal de una raíz cuadrada inexacta *no* es periódica.



7) Unas propiedades de potencias superiores

¿Puedes demostrar las siguientes afirmaciones (o encontrar un contraejemplo)?

a) Cada potencia a^{4k+1} termina con la misma cifra como la base a (para todos los números naturales a y k).

(Ejemplos: $17^5 = 1419857$, termina en 7.
$4^{13} = 67108864$, termina en 4.)

b) Para todos los números primos $p > 3$ vale: $p^{2k} - 1$ es divisible entre 24 (para todos los números naturales k).

(Ejemplos: $7^6 - 1 = 117648 = 24 \cdot 4902$.
$13^4 - 1 = 28560 = 24 \cdot 1190$.)

8) Factorización según Fermat

Pierre de Fermat (1601-1665) era un abogado francés aficionado a la matemática, que hizo muchos descubrimientos novedosos para su tiempo. Entre otros, descubrió un método alternativo de descomponer un número natural en factores primos. Este método se basa en la factorización $a^2 - b^2 = (a+b)(a-b)$: Si quiero factorizar el número n, solamente tengo que averiguar si puedo representar n como una diferencia de cuadrados, y si puedo, entonces he encontrado una factorización.

Fermat encontró maneras de aplicar este método de una manera bastante eficaz, más eficaz que la factorización "normal" dividiendo entre cada número primo. Unos matemáticos del siglo 20 siguieron perfeccionando este mismo método, especialmente para poder factorizar números muy grandes con programas de computadora. Este tema sigue siendo un tema de investigación importante para los matemáticos actuales.

Seguiremos los pasos de Fermat en esta investigación ...

a) Se trata entonces de descubrir si n es una diferencia de cuadrados: $n = a^2 - b^2$. En otras palabras, de revisar los cuadrado mayores a n (a^2), para ver si su diferencia con n es un cuadrado perfecto ($a^2 - n = b^2$). - Practica este método con algunos números, p.ej. 2077, 2059, 2279.

b) ¿Encuentras una manera práctica de calcular estas diferencias, sin tener que calcular cada cuadrado aparte?

c) ¿Y encuentras una manera práctica de averiguar si estas diferencias son cuadrados perfectos? (sin tener que sacar la raíz cada vez)

***d)** ¿Es necesario probar con *cada* cuadrado > n, o podemos excluir de antemano ciertos números para reducir el trabajo?

e) ¿En qué casos duraría demasiado, encontrar los factores con este método?

- Si no lo descubres, intenta con 2249. Después factorízalo con el método normal (dividiendo entre cada número primo en orden). Explica por qué en este caso la factorización normal es más rápida.

***f)** Ahora, desafortunadamente no podemos saber de antemano cual método es mejor para un número dado, porque esto depende de sus factores que todavía no conocemos. Una alternativa consistiría entonces en usar ambos métodos paralelamente: el método de Fermat para encontrar los factores grandes, y el método normal para encontrar los factores pequeños.

Usando el resultado de la pregunta e), establece una regla que nos diga hasta donde debemos usar el método de Fermat, y hasta donde usar la factorización normal, para reducir el trabajo al mínimo posible, y sin embargo asegurar que no pasemos por alto ningún factor – o sea, que podemos saber también cuando hemos terminado la búsqueda de factores, en el caso de que se trata de un número primo.

g) Usando los resultados de arriba, factoriza de la manera más eficaz que puedas:

136517, 180787, 141226, 166601, 190747, 191761

h) Anota cualquier otra observación o descubrimiento que hiciste acerca de este tema. (Todavía existen más maneras de optimizar este método de factorización...)

9) Cómo alegrar a un matemático

Un matemático se alegra cuando encuentra un número que es divisible entre la suma de sus cifras. Por lo menos, eso es lo que dijo uno de ellos. Si eso es verdad, entonces los matemáticos deben ser personas alegres, porque existen muchos números con esta propiedad.

Un ejemplo: La suma de las cifras de 48 es 4 + 8 = 12; y 48 es divisible entre 12.

Existen diversas preguntas que se pueden investigar acerca de estos números y sus propiedades. Por ejemplo:

a) ¿Cómo se pueden encontrar estos números de una manera relativamente fácil?

b) Demuestra o refuta la siguiente afirmación: "Si un número n es divisible entre la suma de sus cifras, entonces el número $10n$ también es divisible entre la suma de sus cifras."

c) Parece que estos números se acumulan en ciertas regiones. Por ejemplo, ocho de los diez números de 1008 a 1017 son divisibles entre la suma de sus cifras. ¿Encuentras otras "regiones" donde se encuentran muchos de estos números?

d) Por el otro lado, también existen intervalos bastante largos de números sucesivos, de los cuales *ninguno* es divisible entre la suma de sus cifras. ¿Encuentras tales intervalos? ¿Y puedes descubrir unas propiedades particulares de esos intervalos?

***e)** En general, ¿cuán frecuentes son estos números? ¿Puedes hacer unas predicciones acerca de ello, aun sin hacer una tabla completa de los números? ¿Y cómo se reparten estos números en la recta numérica? – Por ejemplo, en los números primos podemos observar

que con números mayores se vuelven menos frecuentes: De 1 a 1000 hay 168 números primos. En el siguiente millar hay todavía 135 de ellos; en el tercer millar hay 127. Continuando así, se encuentran de vez en cuando unas excepciones; o sea millares que contienen más números primos que el anterior; pero la tendencia general es decreciente. Después de 43'000, todos los millares contienen menos que 100 primos.
¿Existen propiedades similares en los números que son divisibles entre la suma de sus cifras?
f) Investiga las mismas preguntas, y otras similares, también para sistemas de numeración con otras bases: ¿Valen allí las mismas leyes? ¿O cambian las condiciones en ciertos sistemas de numeración? ¿Existen bases en las cuales hay más de estos números que en otras?
g) ... y cualquier otra propiedad que puedes encontrar.
¡Que la investigación te dé alegría!

10) Una misteriosa secuencia de cifras

Haz el siguiente ***experimento:*** Comienza con cualquier número natural, pero que no sea divisible entre 7. Duplica este número y escribe el resultado debajo, pero dos columnas más a la derecha. Repite este proceso 20 a 30 veces. Después suma todos estos números, columna por columna, tal como están escritos. (Puedes omitir los últimos dígitos donde la sucesión se interrumpió.) Por ejemplo, empezando con 41:

```
        41
          82
           164
             328
               656
                1312
                  2624
                    5248
                     10496
                       20992
                         41984
                           83968
                             ...
_____________________________
      418367346938775510201...
```

Elimina la primera y la última cifra de tu resultado. Después compáralo con la siguiente sucesión de cifras:

```
10204081632653061224489795918367346938775
5102040... (se repite)
```

Encontrarás que tu resultado está contenido completamente en esta sucesión.
Intenta con algunos otros números de inicio (pero que no sean divisibles entre 7). No importa con qué número comienzas, ¡siempre sale un trozo de esta misma secuencia! *(Si comienzas con un número de una única cifra, tienes que rellenar las columnas vacías con ceros. Por ejemplo empezando con 1: 1020408...)*
Este experimento se puede presentar como un truco: Escribe la secuencia misteriosa sobre una tira de papel y une el final con el principio. Pide al público que efectúe la operación de arriba. Después muestra tu tira de papel en el lugar correspondiente, y declara que ya sabías el resultado de antemano.

Ahora las preguntas de investigación:
a) ¿Por qué funciona este experimento? ¿Cuáles son las propiedades matemáticas especiales de esta secuencia de cifras?
b) Hemos excluido los números divisibles entre 7, porque ésos tienen otro efecto. Analiza ahora qué sucede si comienzas con un número divisible entre 7. ¿Puedes de allí sacar más conclusiones?
c) La secuencia misteriosa aparece también en un contexto distinto; o sea, se la puede producir con una operación distinta. ¿Con cuál? - Eso es quizás más fácil de descubrir si sigues analizando las secuencias que resultan de los números divisibles entre 7.
d) Otra observación interesante es que las cifras de la segunda mitad de la sucesión (a partir de 8979...) complementan las cifras de la primera mitad a 9. ¿Por qué sucede eso? ¿Y cómo se relaciona eso con la operación mencionada en c)?
e) Investiga también otras sucesiones similares. Por ejemplo, ¿qué sucede si triplicas o cuadruplicas el número inicial, en vez de duplicarlo? ¿Qué sucede si trasladas los resultados de las duplicaciones una única columna hacia la derecha, en vez de dos? - Etc.
- Si descubres los principios matemáticos detrás de esta sucesión, podrás tú mismo encontrar muchas otras variaciones.

11) Otra propiedad sorprendente de las potencias superiores

a) Se escoge de manera aleatoria un número natural ***n***. ¿Cuál es la probabilidad de que 2^n, escrito en cifras, comience con la cifra 1? ¿Puedes dar un valor aproximado de esta probabilidad? ¿O encuentras incluso una expresión matemática que describe esta probabilidad *exactamente*?
- Cuidado con conclusiones apresuradas. La probabilidad no es $^1/_{10}$ ... y tampoco es $^1/_9$.
b) ¿Cuánto es esta probabilidad, si en vez de las potencias de 2 usamos las potencias de 3, o de alguna otra base?
c) ¿Y cuánto es la probabilidad de que estas potencias comiencen con la cifra 2, con 3, con 4, etc.?
d) Amplía esta investigación para otras secuencias de números, por ejemplo los cuadrados perfectos, cubos perfectos, y otros ...

12) Progresiones aritméticas de números primos

¿Cómo se pueden encontrar progresiones aritméticas largas que contienen únicamente números primos?
La secuencia de los números primos se ve bastante "desordenada". A pesar de eso, ¿se pueden encontrar dentro del conjunto de los números primos tales secuencias "ordenadas", aritméticas? ¿Y cuán largas podrían ser esas progresiones aritméticas?
Este es un ejemplo:

11, 41, 71, 101, 131, ...

Vemos que la diferencia entre un miembro y el siguiente siempre es 30. Todos los cinco números son

primos. Pero el siguiente miembro, 161, ya no es primo ($161 = 7 \cdot 23$).
Entonces, aquí unas preguntas como incentivo a la investigación:
a) ¿Cuáles son las primeras progresiones aritméticas de seis, siete, ocho, ... número primos?
b) ¿Cómo se pueden encontrar tales secuencias de manera eficaz?
c) ¿Cuáles números son prácticos como diferencias entre los miembros de una tal secuencia? ¿y cuáles no sirven para este propósito?
d) ¿Qué relación matemática existe entre esa diferencia de un miembro al siguiente, y el número máximo de miembros primos en la secuencia?

13) Primo, dos, tres, cuatro...

Observa los números sucesivos **13, 14, 15**: El primer número es primo (13). El siguiente número es el doble de un número primo (14 = 2 x 7). El tercer número es el triple de un número primo (15 = 3 x 5). – Otra sucesión con las mismas propiedades es **37, 38, 39**:

37 es primo.
38 = 2 x 19.
39 = 3 x 13.

a) ¿Cuál es la siguiente sucesión de tres números con las mismas propiedades? ¿Y después?
b) En vez de probar con todos los números primos si son el inicio de una tal sucesión, ¿existe una manera más eficaz de buscar tales sucesiones? – por ejemplo excluyendo de antemano todos los números con determinadas características? ¿Qué características serían ésas?
c) ¿Existen también sucesiones similares de *cuatro* números? O sea, que después del tercer número sigue un cuarto número que es el cuádruple de un número primo? – ¿Cuál es la primera sucesión de este tipo con cuatro números?
***d)** ¿Pueden existir sucesiones arbitrariamente largas de este tipo (aunque sea con números muy, muy grandes)? ¿Cómo podrías encontrarlas?
Si sabes programar en PARI, escribe un programa que encuentra tales sucesiones de una manera eficaz.

14) Progresiones aritméticas de cuadrados perfectos

Como último desafío, nos preguntamos si existen *cuadrados perfectos* que forman una progresión aritmética. Por supuesto que no tienen que ser cuadrados sucesivos; de esa manera sería imposible. Pero con cuadrados que están espaciados un poco más, ¿quizás sería posible?
El siguiente ejemplo muestra que si es posible, por lo menos si nos contentamos con tres miembros:

$49,\ 169,\ 289 \quad (= 7^2,\ 13^2,\ 17^2)$

es una P.A. con diferencia 120.
Investiga entonces las siguientes preguntas (y otras que se te ocurren acerca del tema):
a) Encuentra un método eficaz de encontrar tales progresiones aritméticas.
b) Si tienes conocimientos de programación, haz una búsqueda con tu método, con la ayuda de la computadora.
c) ¿Cuántos miembros puede tener una P.A. de cuadrados perfectos, a lo máximo? ¿o pueden ser arbitrariamente largas?

15) Fracciones egipcias

Hace tres mil años ya, los antiguos egipcios calculaban con fracciones. Pero ellos no las escribían con numerador y denominador. Solamente sabían escribir fracciones con un numerador de 1: 1/2, 1/3, 1/4, etc. - Otras fracciones las escribían como sumas de tales fracciones. Pero además seguían la regla extraña que todos los sumandos en esta suma tenían que ser *distintos*. Por ejemplo para escribir 3/4 no podían escribir 1/4 + 1/4 + 1/4, porque aquí tenemos sumandos iguales. Tenían que escribir 1/2 + 1/4. Y 2/3 tenían que escribir como 1/2 + 1/6. En sus jeroglíficos tenían un signo especial que significaba "fracción". Entonces p.ej. un 6 junto con ese signo significaba 1/6.
Esta manera de escribir fracciones no es sencilla. Por ejemplo, ¿cómo escribirías 3/7 "en egipcio"? ¿o 8/11? (La manera más sencilla de escribir 8/11 es:
1/2 + 1/6 + 1/22 + 1/66.)
De hecho, los antiguos egipcios necesitaban la ayuda de un especialista cuando necesitaban calcular con fracciones. Uno de esos especialistas escribió un libro entero solamente acerca de cómo escribir las fracciones con denominadores hasta 100.
Imagínate entonces que eres un egipcio de los tiempos antiguos, que está aprendiendo a escribir fracciones. Inténtalo primero con los fáciles, antes de pasar a los difíciles. Cuando tienes un poco de práctica, entonces intenta encontrar para cada fracción la versión *más sencilla*. Es que siempre existen varias posibilidades. Por ejemplo 2/3 es no solamente 1/2 + 1/6. Es también 1/3 + 1/4 + 1/12; pero eso es más complicado.
Incluso podríamos discutir cuál es la versión "más sencilla". Por ejemplo 4/13 = 1/4 + 1/26 + 1/52, pero también 4/13 = 1/6 + 1/13 + 1/26 + 1/39. La primera versión tiene menos sumandos; pero en la segunda, el máximo denominador es 39, mientras que en la primera es 52, un número mayor. Podemos entonces definir que la versión "más sencilla" es la que tiene menos sumandos; o también, la que tiene los denominadores menores. ¿O quizás aquella donde la *suma* de los denominadores es menor?

Bien, aquí siguen unas preguntas concretas para investigar:
a) Investiga unos tipos particulares de fracciones. Por ejemplo todas las fracciones con un numerador de 3; o todas las fracciones con un denominador de 11. ¿Encuentras alguna regularidad interesante, que te permite calcular metódicamente cómo escribir todas las fracciones de esta clase "en egipcio"?
b) ¿Existen numeradores resp. denominadores "fáciles" y "difíciles"? O sea, ¿es para ciertos numeradores resp. denominadores más fácil que para otros, encontrar la manera "egipcia" de escribir la fracción?

c) Las fracciones propias con denominador 12 tienen la propiedad interesante de que todas pueden escribirse "en egipcio" con denominadores menores a 12:

2/12 = 1/6	7/12 = 1/3 + 1/4
3/12 = 1/4	8/12 = 1/2 + 1/6
4/12 = 1/3	9/12 = 1/2 + 1/4
5/12 = 1/4 + 1/6	10/12 = 1/2 + 1/3
6/12 = 1/2	11/12 = 1/2 + 1/4 + 1/6

¿Encuentras otros denominadores con la misma propiedad? ¿Cómo se pueden encontrar tales denominadores de manera sistemática?

d) ¿Existen fracciones que tienen una única descomposición "egipcia"? ¿O hay siempre varias soluciones? ¿Pueden incluso existir infinitas soluciones para una fracción dada? - Fundamenta tus conclusiones.

e)** ¿Pueden todas las fracciones con numerador ***n descomponerse en una suma "egipcia" con ***n*** o menos sumandos? ¿Puedes demostrar esta conjetura, o refutarla?

f) Plantea e investiga más preguntas acerca de las fracciones egipcias.

****g)** ¿Todas las fracciones con numerador 4 se pueden escribir "en egipcio" con *tres* sumandos?

(Según la información que tengo, hasta la fecha todavía nadie resolvió este problema.)

***16) Problemas sin resolver

En la teoría de números existe una gran cantidad de problemas que se enuncian fácilmente, pero que hasta la fecha nadie pudo resolver. A continuación presentaré algunos de ellos, para los curiosos y atrevidos:

a) Los siguientes números son primos:

$1^1 + 1 = 2$, $2^2 + 1 = 5$, $4^4 + 1 = 257$.

¿Existen otros números primos de la forma $\boldsymbol{x^x} + 1$?

b) ¿Son el 8 y el 9 los únicos números sucesivos que ambos son potencias?

c) ¿Existen "números de taxi" de grado 5? - O sea, ¿tiene solución la siguiente ecuación diofántica?

$$\boldsymbol{a}^5 + \boldsymbol{b}^5 = \boldsymbol{c}^5 + \boldsymbol{d}^5$$

d) ¿Siempre existe por lo menos un número primo entre dos cuadrados perfectos sucesivos?

e) ¿Hay infinitos números primos en la secuencia de Fibonacci?

f) ¿Existen tres números enteros (no necesariamente positivos) $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$, de manera que $(\boldsymbol{x} + \boldsymbol{y} + \boldsymbol{z})^3 = \boldsymbol{xyz}$?

g) ¿Existen dos números naturales $\boldsymbol{x}$ y $\boldsymbol{n}>7$, de manera que $\boldsymbol{n}! = \boldsymbol{x}^2 - 1$?

Para $\boldsymbol{n}\leq 7$ existen varias soluciones:

$4! = 24 = 5^2–1$, $5! = 120 = 11^2–1$, $7! = 5040 = 71^2–1$.

h) ¿Existen infinitos cuadrados perfectos que contienen solamente dos cifras distintas? - tales como $88^2=7744$, $173^2=29929$, $235^2=55225$, $3114^2=9696996$, etc.

i) ¿Existe un "cuadrado mágico de cuadrados perfectos" de 3x3 ? O sea, un cuadrado mágico de 3x3 cuadros, donde cada entrada es distinta y es un cuadrado perfecto.

***17) La conjetura de Collatz

El siguiente problema fue propuesto por primera vez en 1937 por Lothar Collatz:

Construimos una secuencia de números según la siguiente "receta": Comenzamos con un número natural $\mathbf{n_1}$. Si este número es par, le sigue el número $\mathbf{n_2 = n_1 / 2}$. En cambio, si $\mathbf{n_1}$ es impar, el siguiente número será $\mathbf{n_2 = 3n_1 + 1}$. - A este número $\mathbf{n_2}$ le aplicamos otra vez la misma receta, y así sucesivamente.

Por ejemplo, si comenzamos con el número 23, resulta la siguiente secuencia:

23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1.

(Después del 1 ya no tiene sentido continuar, porque se siguen repitiendo los mismos números 1, 4, 2, 1, 4, 2, 1, ...)

Ahora la pregunta es, ¿si cada secuencia de este tipo necesariamente nos lleva alguna vez al número 1? ¿O existe algún número $\mathbf{n_1}$ cuya "secuencia Collatz" *nunca* llega al 1?

- Unas ideas para la investigación:

a) ¿Cómo podríamos representar gráficamente estas "secuencias Collatz"? (p.ej. las mismas secuencias como una familia de curvas; o la longitud de cada secuencia en relación con su número inical; o un "árbol" que combine todas las secuencias posibles; etc...)

b) ¿Existe alguna fórmula "directa" (más o menos...) para calcular directamente un número $\mathbf{n_a}$ (con cualquier **a**) a partir del número $\mathbf{n_1}$? ¿Qué propiedades del número $\mathbf{n_1}$ tendríamos que saber para poder hacer esto?

c) ¿Qué estrategias podríamos aplicar para llegar quizás a una demostración de que siempre se llega al 1 (o a encontrar un contraejemplo)?

d) Nota que pueden existir dos tipos de contraejemplos (si los hay): O una secuencia infinita donde los números siguen aumentando infinitamente; o una secuencia periódica que vuelve al número inicial sin llegar al 1. - ¿Podemos descartar de antemano una de estas posibilidades, o son ambos posibles?

Si se admiten también números negativos, entonces existe efectivamente un contraejemplo periódico:

–5, –14, –7, –20, –10, –5, ...

Entonces no podemos excluir de antemano esta posibilidad.

Sherlock Numbers y los cuatro residuos

VIII

Numbers se dirigió al lugar, acompañado de su amigo Less, por si hubiera alguna complicación. Ya habían preguntado a varios vecinos. Algunos dijeron recordar a la persona que buscaban. "Sí, allí vive", dijo una señora. "Un chico solitario. Habla poco, y parece que no tiene amigos." – Nadie lo había visto durante los últimos dos meses.

Numbers instruyó a Less: "Ahora quédate aquí, fuera de la vista. Yo iré solo. Después, si todo está bien, volveré acá. Si voy hacia el otro lado y no vengo acá, llama inmediatamente al inspector, puede haber peligro. Cuida los datos que te di." – Enseguida, el detective se acercó a la casa misma. Se veía vieja y oscura. En una ventana opaca colgaba un letrero descolorido: "Se alquilan habitaciones".

Un anciano abrió la puerta.

– "¿El señor 1'294'103?"

– "Ah, el joven", respondió el anciano. "No se encuentra."

– "¿Cuándo lo podré encontrar, por favor? Tengo un encargo para él."

– "Déjelo conmigo no más, yo se lo voy a entregar."

– "Prefiero hablar con él personalmente. ¿Cuándo estará de regreso?"

– "Eso no lo sé. Se fue de viaje, y no dijo nada más."

– "¿Hace tiempo?"

– "Un buen tiempo, sí."

– "¿Más de un mes?"

– "Sí, sí, por lo menos cuatro semanas."

– "Pero debe haberle dejado una dirección, algún dato de contacto..."

– "Nada. Así son los primos, hacen lo que quieren. Qué voy a decirle, es una persona adulta, puede ir adonde quiere."

– "¿Entonces usted no es un pariente suyo?"

– "Soy el dueño de esta casa, y no tengo por qué meterme en la vida de mis inquilinos."

– "¿No tiene entonces ni la menor indicación adónde podría haberse ido?"

– "Ya se lo dije. Yo no pregunto a la gente de dónde son, quiénes son, qué hacen. Se van, y no les pregunto a dónde. ¿Para qué? No soy como algunos que se pasean por todo el vecindario, preguntando por la gente."

– "Lo siento haberle molestado. Buenas tardes."

Y Numbers continuó caminando por la calle, alejándose de Less. Éste, alarmado, llamó a Cuadricula. No fue fácil convencer al inspector. "El hombre no ha sido visto desde hace dos meses", insistió Less. "Y Numbers tiene pruebas matemáticas de que su desaparición está relacionada con el caso del 622. Por favor, inspector, yo conozco a Numbers. Cuando él dice que algo es serio, lo es."

Numbers intentó alejarse de la vista de la casa lo más rápido posible, pero sin dar señas de estar sospechando algo. Dobló en un callejón, llegó a una avenida bastante transitada, se mezcló entre los transeúntes, entró en una tienda y salió con su abrigo invertido. Aun con todas estas precauciones se sintió intranquilo. Una banda capaz de asesinar a un testigo en la misma puerta de la comisaría, no era de tomar en poco.

Y de hecho, a pocos pasos de la salida de otro callejón angosto, se dio cuenta de que alguien entró al mismo callejón detrás de él. De reojos pudo reconocer a un hombre que ya le había seguido en la avenida. Numbers logró salir del callejón, y rápidamente dobló la esquina. Pero en la otra calle también estaba un hombre caminando detrás de él con una actitud sospechosa. Numbers estaba todavía mirando por todos lados para encontrar un camino de escape, cuando los sucesos se sobresaltaron.

Su perseguidor salió del callejón, se volteó para buscar a Numbers con su mirada, y por poco se chocó con el hombre que caminaba en la calle. Los dos se agarraron y empezaron a pelearse. Entonces salió un tercer hombre del callejón, y también se metió en la pelea. Numbers aprovechó la oportunidad para alejarse lo más que pudo. Antes de doblar la siguiente esquina, todavía pudo ver que los dos desconocidos arrastraron a su primer perseguidor en la dirección opuesta.

Unidad N 10 - Los números transfinitos de Cantor

Prerrequisitos:
- Números naturales, racionales, y reales *(Secundaria I, Unidad 30)*.

Nota: *Los temas de esta Unidad son opcionales; no figuran en los currículos escolares usuales.*

Comparar conjuntos infinitos entre sí

En esta Unidad seguiremos unos razonamientos del matemático Georg Cantor. Entraremos al ámbito de lo infinito, y allí encontraremos muchos misterios y paradojas.
Empecemos con una pregunta sencilla:
¿De cuáles hay más: Números naturales, o números naturales pares?
Probablemente dirás que los números pares son solamente la mitad de los números naturales; y por tanto los números naturales son más. En un intervalo *finito*, eso es cierto. Por ejemplo del 1 al 10 hay 10 números naturales, pero solamente 5 números pares.
Pero cuando entramos al ámbito de lo infinito, las cosas cambian de manera sorprendente. Llamemos N al conjunto de los números naturales, y P al conjunto de los números positivos pares. Entonces podemos definir la siguiente correspondencia entre sus miembros:

1 2 3 4 5 6 7 8 9 ...
↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕
2 4 6 8 10 12 14 16 18 ...

O sea, para cada número natural existe un número par correspondiente, que es el doble del número. Esta correspondencia continúa hasta lo infinito, porque para *cada* número natural existe otro que es su doble.
Por tanto, *la cantidad de números pares positivos es la misma como la cantidad de números naturales.* En otras palabras, los dos conjuntos son *de la misma "clase de infinidad"*.

Otro ejemplo:
¿De cuáles hay más: Números naturales, o cuadrados perfectos?
Nuevamente, según nuestra intuición diríamos que los cuadrados perfectos son "mucho menos". Pero al comparar los conjuntos *infinitos*, podemos hacer la misma clase de correspondencia como antes:

1 2 3 4 5 6 7 8 9 ...
↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕
1 4 9 16 25 36 49 64 81 ...

Así que también la cantidad de cuadrados perfectos, es de la misma "clase de infinidad" como los números naturales.

Otro ejemplo:
¿De cuáles hay más: Números naturales, o números primos?
Ya te puedes imaginar lo que viene...

1 2 3 4 5 6 7 8 9 ...
↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕
2 3 5 7 11 13 17 19 23 ...

Pero quizás protestarás: "Esta correspondencia no es válida. No hay ningún método para calcular, por ejemplo, cuál es el número primo no. 587'388."
Pero eso no es necesario. Podemos simplemente asignar a cada número primo su "número de orden"; no hay necesidad de una correspondencia matemática directa. Solamente necesitamos demostrar dos cosas:
1) *Que con los números primos se puede formar una sucesión ordenada.* - Eso es lógico: se pueden ordenar de menor a mayor, y ya tenemos una sucesión ordenada.
2) *Que la sucesión es infinita.* Eso lo demostró Euclides hace más de 2000 años. *(Vea Secundaria I, Unidad 37.)*
Cantor llamó a las sucesiones que cumplen estas condiciones, "sucesiones infinitas enumerables". En estas sucesiones, se puede asignar a cada miembro un "número de orden" natural. Por tanto, todas las sucesiones de esta clase son de la misma "clase de infinidad" como los números naturales.

Este es un primer resultado importante de los razonamientos de Cantor:
En cada sucesión infinita enumerable, la cantidad de sus miembros es igual a la cantidad de los números naturales.

Para practicar:
Las siguientes sucesiones, son infinitas enumerables o no?
1) Los cubos perfectos
2) Los múltiplos de 5 (5; 10; 15; 20; ...)
3) Los divisores de 1200
4) La sucesión de Fibonacci (1; 1; 2; 3; 5; 8; 13; ...)
5) Los números naturales que contienen cada una de las cifras de 1 a 9 exactamente una vez

La cantidad de números racionales

Hasta ahora hemos encontrado conjuntos finitos, y conjuntos infinitos enumerables. ¿Existen también conjuntos infinitos que no son enumerables?
¿Qué tal los números racionales? ¿Seguramente hay más números racionales que naturales? - Sabemos que los números racionales no se pueden ordenar de menor a mayor, porque son "densos". O sea, entre dos números racionales cualesquieras, siempre se pueden encontrar infinitos otros números racionales.
Veremos los razonamientos de Cantor acerca de este tema.

Cada número racional se puede representar como una fracción. Las fracciones, aunque no se pueden ordenar de menor a mayor, pero se pueden ordenar en una tabla de dos dimensiones, donde las columnas se ordenan por numeradores y las filas por denominadores:

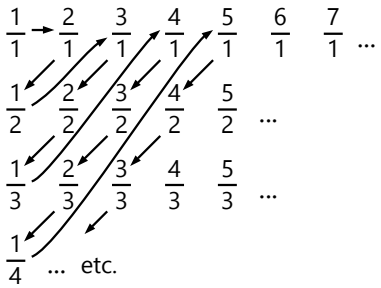
$$\frac{1}{1}\ \ \frac{2}{1}\ \ \frac{3}{1}\ \ \frac{4}{1}\ \ \frac{5}{1}\ \ \frac{6}{1}\ \ \frac{7}{1}\ \cdots$$

$$\frac{1}{2}\ \ \frac{2}{2}\ \ \frac{3}{2}\ \ \frac{4}{2}\ \ \frac{5}{2}\ \cdots$$

$$\frac{1}{3}\ \ \frac{2}{3}\ \ \frac{3}{3}\ \ \frac{4}{3}\ \ \frac{5}{3}\ \cdots$$

$$\frac{1}{4}\ \ \ldots \text{ etc.}$$

Ahora, Cantor tuvo la idea genial de recorrer esta tabla en forma "triangular", así:



Eso nos da la siguiente sucesión:
$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{4}{2},$ etc.
Si continuamos este proceso hasta lo infinito, estamos efectivamente recorriendo la tabla entera. Y con eso tenemos una sucesión ordenada, que nos permite asignar un "número de orden" a cada fracción.
¡Así que ***también los números racionales son enumerables***! O sea, la cantidad de números racionales es también de la misma "clase de infinidad" como los números naturales.

Nota: Uno podría objetar que esta secuencia contiene la misma fracción repetidas veces, porque p.ej. $\frac{1}{2} = \frac{2}{4}$. Pero si corregimos eso y omitimos las fracciones equivalentes, entonces obtenemos una sucesión con "*menos*" miembros, no con más. Entonces eso no afecta el argumento principal, de que no existen "más" números racionales que naturales.

El conjunto de los números reales

¿Podemos hacer algo similar con los números reales? La mayoría de éstos ya no se pueden representar como fracciones. Si queremos representar todos los números reales de una misma forma, solamente podemos hacerlo en forma de números decimales infinitos (y la mayoría de ellos no periódicos).
Algunos números irracionales tienen una representación alternativa que permite calcularlos; por ejemplo $\sqrt{13}$, π, cos 11°, etc. También un número como 0.3030030003... tiene una "ley" que nos permite predecir cómo continúa, aunque no es periódico. Pero muchos números reales no se pueden representar de manera "finita", y no se pueden definir de una manera que permitiría calcularlos; o sea son números "no calculables".
¿La infinidad de estos números se puede ordenar en una tabla, de manera similar como lo hemos hecho con las fracciones? - Si lo intentas por un tiempo, verás que probablemente es imposible. (¡Una tal tabla tendría que tener una infinidad de dimensiones!)

Cantor encontró una demostración ingeniosa de que eso efectivamente es imposible:
Supongamos que *fuera* posible, poner todos los números reales en una secuencia ordenada. Entonces (con tiempo y espacio infinitos ...) podríamos escribir estos números uno debajo del otro, como números decimales infinitos.
En esta tabla infinita de cifras, trazamos la diagonal, y marcamos todas las cifras que se encuentran en ella:

0.037800348380009...
0.040506022000324...
0.902570800671342...
0.777777000333333...
0.904022381672345...
...

Estas cifras, en este orden, forman también un número real. (0.04272... en el ejemplo.) A partir de este número construimos uno nuevo, alterando cada cifra según una regla fija. Por ejemplo, remplazamos cada cero por un 9, y todas las otras cifras remplazamos por ceros:

0.937800348380009...
0.000506022000324...
0.900570800671342...
0.777077000333333...
0.904002381672345...
...

Este nuevo número comienza entonces con 0.90000...

¿Se encuentra este nuevo número en nuestra lista infinita original? - Vamos a ver. ¿Puede ser igual al primer número? Pero la primera cifra de nuestro número es diferente de la primera cifra del primer número en la lista, porque la hemos cambiado al propósito. Aunque todas las otras cifras del primer número fueran iguales al número nuevo, en la primera cifra difieren.
¿Puede el número nuevo ser igual al segundo número en la lista? - No, porque su *segunda* cifra es diferente de la segunda cifra del segundo número.
¿Puede el número nuevo ser igual al número en la posición 3078 de nuestra lista? - No, porque su 3078ª cifra es diferente de la 3078ª cifra del número en la posición 3078.
Y así sucesivamente, hasta lo infinito: Cada número en la lista tiene por lo menos una cifra que es *diferente* del nuevo número que hemos construido.
Por tanto, nuestra lista *no puede contener todos los números reales*: Acabamos de construir un número que no está en la lista.
Pero eso es una contradicción contra nuestra suposición inicial; porque hemos asumido que nuestra lista de números reales es completa. Ahora hemos demostrado que no lo es. Por tanto, es imposible definir una sucesión ordenada que contenga *todos* los números reales.

En otras palabras: ***El conjunto de los números reales no es enumerable.*** La cantidad de los números reales es de una "clase de infinidad" diferente de la cantidad de los números naturales.

Reseña biográfica

Georg Cantor (1845 – 1918) es conocido como el fundador de la teoría de los conjuntos. Como hemos visto en esta Unidad, este tema va mucho más allá de lo que se enseña en la escuela. Cantor desarrolló su teoría en primer lugar para estudiar conjuntos *infinitos*, y para poder identificar, clasificar y relacionar diferentes clases de "infinidades".
Cuán profundo era este tema para Cantor, demuestra la siguiente anécdota: Entre colegas conversaban de cómo se imaginaban un conjunto. El matemático Richard Dedekind dijo: "Yo me imagino un conjunto como una bolsa cerrada con objetos dentro." A lo cual Cantor respondió con un gesto teatral: "Para mí, ¡un conjunto es *un abismo*!"
Pocos matemáticos tuvieron que luchar contra tanta oposición como Cantor. Muchos de sus colegas rechazaban sus ideas por su novedad; el eminente matemático Henri Poincaré las llamó "una enfermedad de la cual la matemática se recuperará dentro de pocos años." Su anterior profesor en la universidad, Leopold Kronecker, lo calumniaba públicamente, e hizo todo lo posible para impedir la publicación de sus obras.
Cantor respondió a estos ataques: "*La esencia de la matemática radica en su libertad*". O sea, cuando alguien impide la publicación de una nueva teoría matemática, está atacando no solamente a su autor. Está atacando la *libertad* de la matemática, y con eso pone en peligro el desarrollo científico. Eso es de mucha actualidad hoy en día, donde los resultados de muchas investigaciones son censurados porque contradicen la política de los gobiernos del mundo.
- Además de la enemistad de sus colegas, Cantor sufría del trastorno bipolar. Durante la segunda mitad de su vida tenía frecuentes crisis nerviosas de tanta intensidad que tuvo que ser hospitalizado.
Cantor seguía trabajando en la fundamentación lógica de su teoría, aun durante sus tiempos de enfermedad. Solamente su confianza en Dios le mantuvo firme a través de todas estas dificultades.
Efectivamente, Cantor estaba convencido de que la teoría de los conjuntos infinitos fue una revelación de Dios, y de que él, Cantor, fue llamado por Dios para dar a conocer esta teoría al mundo. Como lema para su última publicación escogió las palabras del Señor Jesús (citadas de manera inexacta): "El tiempo llegará cuando estas cosas, que ahora están escondidas ante ustedes, serán traídas a la luz." (según Marcos 4:22, o quizás pensó en 1 Corintios 4:5.)
El pensamiento de Cantor se enfocaba principalmente en lo infinito como una característica de Dios. Él razonó que la mente de Dios es infinita; y por eso, la infinidad de los números existía desde el inicio. Solamente por eso podemos nosotros pensar en números concretos, finitos; y solamente por eso podemos seguir contando y confiar en que los números continúan; porque son "como huellas en el camino preexistente", trazado por la infinidad en la mente de Dios.
Muchos matemáticos opinaban que lo infinito no existe en realidad; que es solamente una hipótesis o una posibilidad imaginaria. Cantor revolucionó esta manera de pensar. Primeramente, porque él declaró que lo infinito existe de hecho (y dijo que eso era porque Dios existe). Y con su teoría demostró matemáticamente que existen muchas diferentes clases o cualidades de infinidad, todas distintas entre sí. Una pequeña parte de eso hemos estudiado en esta Unidad.
Cantor descubrió también que deben existir otras "infinidades" que no se pueden definir con claridad, o que conducen a paradojas cuando uno intenta tratarlas matemáticamente. A esas infinidades las llamó "absolutos", y dijo que se encontraban más allá del alcance de la matemática: "El verdadero infinito o Absoluto, que está en Dios, no permite ninguna determinación."

Los primeros números transfinitos

Cantor definió una nueva clase de números para expresar las distintas "clases de infinidades" que había descubierto. A la cantidad de los números naturales llamó $\aleph_0$ (álef-cero).

A la cantidad de los números reales, Cantor la llamó $\aleph_1$ (álef-uno).
($\aleph$ (álef) es la primera letra del alfabeto hebreo.)
Estos son los primeros dos "números transfinitos", o sea, números que describen "infinidades".

Sherlock Numbers y los cuatro residuos

IX

Fue una hora más tarde. "Menos mal que no haya sido una falsa alarma", dijo el inspector. "Pero usted tuvo razón, Numbers. El hombre estaba armado."
– "Y gracias a su pronta y sabia decisión de mandar a unos agentes encubiertos, me tiene aquí con vida", respondió el detective.
– "Pero ¿cómo supiste que estabas en peligro?", intervino Less.
– "Hubo suficientes motivos para sospechar del anciano que me habló en la puerta. Debe ser un cómplice. Primero y ante todo, ¿cómo no se va a inquietar si su inquilino desaparece sin advertencia, por más de un mes y sin signo de vida alguno? Pero a él no le importó en absoluto.
Segundo, debe haberme observado tocando las puertas de otras casas en el vecindario. Hizo un comentario al respecto, que sonaba como una amenaza velada.
Además, las contradicciones en sus declaraciones. Dijo no saber nada acerca de sus inquilinos. Sin embargo, sabía que el desaparecido es un número primo. Eso es un hecho que los primos no suelen divulgar. Y el anciano tampoco pudo haberlo calculado, porque eso es bastante difícil con números de esta magnitud. Aun más para alguien que dificulta tanto en la matemática, que cree que cuatro semanas son más que un mes."
– "No lo veo tan concluyente", dijo el inspector, "pero el hecho es, sus sospechas resultaron fundamentadas. Ahora, por favor explíqueme esto. Me parece chino."
Y le alcanzó el papel que Less le había entregado media hora antes, siguiendo las instrucciones de Numbers. En él estaba escrito:

"Residuos encontrados o testificados:
8 (divisor 11)
6 (divisor 7)
12 (divisor 17)
622 (divisor primo, < $\sqrt{n}$).
n = 811 + 1309k (Teorema chino de los residuos).
Primera solución:
n_1 = 778'357; 778'357÷ 823 = 945, R.***622***
(descartada porque se encontró presente.)
Segunda solución:
n_2 = 1'294'103; 1'294'103 ÷ 719 = 1799, R.***622***
No fue visto desde hace dos meses.
Rastrear divisores 7, 11, 17, 719."

– "Según el Dr.Raíz, de hecho ***es*** chino", respondió Numbers. "Mi amigo Less ya le habrá contado cómo me encontré con los tres primeros residuos. Mi análisis químico demostró que deben estar relacionados con el caso del 622; o sea, procedieron del mismo dividendo. Los cálculos demuestran que los números 778'357 y 1'294'103 dejan efectivamente estos residuos, incluido el 622, cuando se les aplican pruebas de división entre números primos.
Esta tarde, sus vecinos nos confirmaron que el segundo de ellos está desaparecido desde hace dos meses. Pero sospechosamente, el hecho no se reportó a la policía. Tratándose de este número particular, eso refuerza mi teoría de que su desaparición está relacionada con el caso del 622, y de los otros tres residuos. Y tratándose de este número, sabemos ahora que en el caso del 622, el divisor fue 719. Por tanto, sugiero rastrear los divisores mencionados, para ubicar el laboratorio clandestino y al desaparecido 1'294'103. Opino que eso pertenece a las competencias de la policía, y que con eso concluye mi contribución a este caso."
Algún tiempo después, Numbers y Less fueron satisfechos al enterarse de que el operativo policial había sido exitoso, y el desaparecido 1'294'103 había sido liberado. Y con eso termina la historia de los cuatro residuos – casi.

X

Un sorprendido Dr.Raíz abrió la puerta de su casa. El inspector Cuadrícula y su ayudante le saludaron. "Quisiéramos felicitarle por su contribución a la solución del caso del 622. De parte de la Policía Nacional, le entregamos este reconocimiento" – y colocaron una medalla de honor en sus manos.
– "Pero por qué ... yo no sé ... no tuve nada que ver con ningún caso ... seguramente es una confusión ..." dijo el erudito.
Detrás de los policías apareció el rostro de Sherlock Numbers. "Decidí dejarla para usted. Si no hubiera sido por su valiosa lección de matemática y su calculador, yo no hubiera sido capaz de resolver ese caso."
El doctor seguía confundido. – "¿Cuál lección?"
– "El problema de los residuos que le traje esa vez. El teorema chino."
– "Así que ... ¿eso fue ... ?"
– "Mi pista en el caso del 622."
– "¡Pero mi querido Numbers! ¿Por qué no me lo dijo? Mi nuevo calculador programable de último modelo hubiera encontrado las primeras cinco soluciones en menos de cuarenta y siete segundos. Pero de todos modos ... el problema tiene cierto interés matemático. Pienso hacerme cargo de generalizarlo. Por si se le presentase otro caso similar..."

Anexo A: Solucionario del Bloque V – Teoría de números

Unidad N 1 - Números defectivos, perfectos, y abundantes

Investigación:

1, 2, 3) La pregunta 3) nos conduce a unas propiedades que son clave también para resolver las preguntas 1) y 2). Recomiendo examinar el cociente $\frac{\sigma(n)}{n}$. Si este cociente es igual a 2, tenemos un número perfecto; y si es mayor a 2, tenemos un número abundante. Ahora, este cociente puede descomponerse según los factores primos de n. Sea la factorización de $n = p^a + q^b + \ldots + z^k$. Entonces

$$\frac{\sigma(n)}{n} = \frac{1+p+p^2+\ldots+p^a}{p^a} \cdot \frac{1+q+q^2+\ldots+q^b}{q^b} \cdot \ldots \cdot \frac{1+z+z^2+\ldots+z^k}{z^k}.$$

Ahora puedes examinar:

- Para un factor primo p determinado, ¿cuál es el máximo valor posible del cociente $\frac{1+p+p^2+\ldots+p^a}{p^a}$?
- Si tenemos un número n dado, ¿cómo cambia su cociente $\frac{\sigma(n)}{n}$, si multiplicamos n por uno de sus factores primos?
- ¿y cómo cambia $\frac{\sigma(n)}{n}$, si multiplicamos n por un número primo que no es uno de sus factores?

Los resultados de estos razonamientos deben ser suficientes para resolver las preguntas 1) y 3). – Ahora, el resultado de 3) sugiere que todos los números abundantes se pueden construir a partir de ciertos "números abundantes primitivos" (y números perfectos). Llamamos "número abundante primitivo" a un número que es abundante, pero que no es múltiplo de ningún otro número abundante. Ahora, ¿se pueden encontrar números sucesivos entre los múltiplos de los números abundantes primitivos? Si es que existen, ¿cómo los podemos encontrar? – Con eso encontrarás la respuesta a la pregunta 2).

4, 5) Aquí también puede ayudar el cociente $\frac{\sigma(n)}{n}$.

¿Qué propiedades tiene que cumplir la factorización de n, para que este cociente sea exactamente 2? ¿o exactamente 3, para un número "doblemente perfecto"?

*****6)** Ya es un desafío interesante, encontrar números amistosos. En este caso no basta con estudiar el cociente $\frac{\sigma(n)}{n}$. Tenemos que considerar adicionalmente la diferencia $\sigma(n) - n$. ¿Quién sabe, si encuentras alguna propiedad interesante, o una fórmula?

Para la pregunta sin resolver, obviamente no se pueden dar pautas, ya que todavía nadie sabe cómo resolverla ...

****7)** En la pregunta 4) ya habrás descubierto que para un número perfecto, las sumas de potencias $(1+p+p^2+\ldots)$, $(1+q+q^2+\ldots)$, etc, deben *en conjunto* contener los mismos factores primos como las potencias p^a, q^b, etc. Pero cada suma de potencias es PESI con la potencia correspondiente; entonces sus factores deben distribuirse entre las potencias de los *otros* factores.

Para números perfectos pares, eso se puede alcanzar fácilmente, porque uno de los factores es 2. La siguiente fórmula fue conocida ya por Euclides:

$$\frac{\sigma(n)}{n} = \frac{1+2+2^2+\ldots+2^a}{2^a} \cdot \frac{1+q}{q} = \frac{2^{a+1}-1}{2^a} \cdot \frac{1+q}{q} = 2$$

Esto se cumple si q es primo, y $2^{a+1} - 1 = q$.

Entonces: $\underline{n = 2^a \cdot (2^{a+1} - 1)}$ es un número perfecto, si $2^{a+1} - 1$ es primo.

Así, los primeros números perfectos son:

$a = 1$, $2 \cdot 3 = 6$

$a = 2$, $4 \cdot 7 = 28$

(Con $a=3$ no funciona, porque $2^4-1=15$ es compuesto.)

$a = 4$, $16 \cdot 31 = 496$

$a = 6$, $64 \cdot 127 = 8128$ ... etc.

Euler demostró que esta fórmula describe *todos* los números perfectos pares:

Todo número par n se puede escribir de la forma:

$n = 2^k m$, de manera que m es impar.

Definimos $q = 1+2+4+\ldots 2^k = 2^{k+1} - 1$.

Entonces, por la fórmula, $\sigma(n) = q \cdot \sigma(m)$.

Ahora, si n es un número perfecto, $2n = \sigma(n)$.

Y de acuerdo a cómo definimos m, q:

$2n = 2^{k+1} m = (q+1)m = \sigma(n)$.

Juntándolo con la primera ecuación:

$q \cdot \sigma(m) = (q+1)m = qm + m \quad | - qm$

$q \cdot (\sigma(m) - m) = m$

O sea, $\sigma(m) - m$, la suma de los divisores propios de m, es a su vez un divisor propio de m. Eso es posible solamente si existe un único divisor propio; o sea m es primo y entonces $\sigma(m) - m = 1$, $q = m$.

Pero en este caso, n tiene la forma $2^k (2^{k+1} - 1)$, o sea está incluido en los números descritos por la fórmula. No existen otros números perfectos *pares*.

- Ahora, el caso de los números perfectos *impares* es completamente distinto. Probando, verás pronto que su estructura tiene que ser mucho más complicada que la de los números perfectos pares.

Unidad N 2 - División modular, y otros temas de congruencia modular

Tablas de multiplicación modular – Para practicar:

1.a) 30÷6 = 5, **b)** 896÷14 = 64

2.a) MCD(44; 143) = 11.

b) Ninguna. MCD(56; 208) = 8; pero 100 no es ningún múltiplo de 8. La ecuación es equivalente a 0 ≡ 4 (mod.8).

División modular – Para practicar:

3) 4, 4) 5, 5) 2,

6) 3 (se puede dividir de frente, ya que 3 y 11 son PESI).

7) C.S.={3; 7; 11} - equivalente a 3÷1 (mod.4).

8) 70 - Se puede calcular 1÷13 (mod.10), y multiplicar el resultado por 10.

9) 18x ≡ 3 (mod.31); x = 26 (; 57; 88; ...)

10) 29x ≡ 11 (mod.90); x = 19

11) 101, 12) C.S. = {9; 26; 43; 60; 77; 94; 111}
Se simplifica con 7: 13x ≡ 15 (mod.17).

13) 803 - Se puede usar el módulo negativo, la ecuación equivale a: –3x ≡ 594 (mod.1001). Eso se puede dividir directamente:
594÷(–3) = –198 ≡ 803 (mod.1001).

Investigación: Ecuaciones diofánticas lineales

No puedo dar una pauta sin descubrir a la vez un procedimiento concreto. Por eso, solamente una pauta muy general: Si no quieres probar todas las posibilidades, entonces tienes que encontrar una forma de reducir la ecuación con números grandes a una con números menores. Y posiblemente hay que hacer eso repetidas veces.

Por si decidiste rendirte, y buscar en la literatura para saber cómo lo hacen los "profesionales": El tema está relacionado con encontrar el *valor recíproco modular* de un número, y con el *algoritmo de Euclides extendido*.

Otros problemas:

14) Que un número "termine con 7", significa que es un número de la forma 10x + 7. Se trata entonces de resolver la ecuación diofántica 10x + 7 = 13y.
Resulta x = 11, y = 9, y "el número", de forma generalizada, es 117 + 130k.
En el intervalo de 1000 a 2000, la primera solución es 1027, la última 1937, en total 8 soluciones.

15) 588 = $2^2 \cdot 3 \cdot 7^2$. Buscamos entonces los números que no contienen ninguno de los factores primos 2, 3, ó 7. En cada intervalo de 42 números, ésos son 12 números.
1000 ÷ 42 = 23 R.34; lo más práctico es calcular con 24 intervalos completos y después examinar aparte los 8 números que sobran, de 3000 a 3008. Entre ésos hay 3 que son PESI con 588 (3001, 3005, 3007). Entonces, entre 2000 y 3000 hay 24·12 – 3 = 285 números PESI con 588.

16) Si "exactamente la décima parte" es un número entero, entonces el número buscado es un múltiplo de 10. Lo llamamos 10x. Este número es igual al cuadrado de su raíz, más el residuo: $10x = y^2 + x$.
Restamos x por ambos lados: $9x = y^2$.
Entonces todos los múltiplos de 3 son posibles valores para y. Verificamos cuántos de esos son efectivamente soluciones:

y = 3, x = 1, $10 = 3^2 + 1$.

y = 6, x = 4, $40 = 6^2 + 4$.

y = 9, x = 9, $90 = 9^2 + 9$.

y = 12, x = 16, $160 = 12^2 + 16$.

y = 15, x = 25, $250 = 15^2 + 25$.

y = 18, x = 36, $360 = 18^2 + 36$.

y = 21, x = 49, $490 = 22^2 + 6$. *(¡no es solución!)*

Vemos que a partir de aquí, la condición ya no se cumple, porque existe un cuadrado perfecto más cercano que hace que el residuo sea menor a x. Eso continúa así con todos los y > 21. Hay un total de 6 soluciones.

17) $\overline{ab}_{12} \cdot \overline{cd}_{12} = \overline{ce}_{12} \cdot \overline{bf}_{12} = 1000_{12}$

Viendo el producto final, sabemos que ninguno de los números involucrados contiene un factor primo que no sea 2 ó 3.

Ahora hay diversos caminos para llegar a la solución.

Podríamos concentrarnos en las cifras de las unidades: Tanto $b \cdot d$ como $e \cdot f$ son múltiplos de 12; pero además sabemos que ninguna de estas letras significa cero.

Pero sugiero que será más eficaz, examinar primero la c, porque ambas multiplicaciones contienen un número que empieza con c. Si c fuera 1, esos números serían 16 y 18. (Son los únicos de 13 a 23 que contienen solamente factores 2 y 3.) Si c fuera 2, ¿cuáles serían esos números? ¿Y si c fuera 3? - Verás que para muchos valores de c, ni siquiera hay una solución. Entonces usa aquellos valores de c que sí son posibles, calcula los otros factores de las multiplicaciones para cada caso, y evalúa cuál de ellos corresponde con la ecuación dada.

Unidad N 3 - El teorema chino de los residuos

Para practicar:

1) n ≡ 77 (mod.90), 2) n ≡ 279 (mod.322),

3) n ≡ 5 (mod.8),

4) indefinido. (Podría ser 7, 18, ó 29.)

5) Podemos calcular con n – 1, y entonces simplificar con el MCD (=7): (n – 1)/7 ≡ 2 (mod.4), (n – 1)/7 ≡ 3 (mod.7). Resultado final: n ≡ 71 (mod.196).

6) No hay solución. Según la primera ecuación, n ≡ 1 (mod.3); según la segunda ecuación, n ≡ 2 (mod.3).

7) n ≡ 706 (mod.990).

8) $n \equiv 204$ (mod.525), 9) $n \equiv 221$ (mod.280)
(calcula con $(n-4)/7$ para simplificar)
10) Contradicción (mod.19); no hay solución.
11) $n \equiv 96$ (mod.252). (La primera condición es redundante, porque está implicada en la tercera.)
12) $n \equiv -1 \equiv 209$ (mod.210); $n_2 = 419$
13) Expresamos el tiempo t en el momento descrito:
Ana: $t = 161x$; Braulia: $t = 168y + 168/12$;
Carla: $t = 184z + 184/4$. O sea:
$t \equiv 0$ (mod.161); $t \equiv 14$ (mod.168); $t \equiv 46$ (mod.184).
$t = 3542$; $x = 22$; $y = 21$; $z = 19$.
14.a) 47; b) 299 - La condición implica que $n \equiv 2$ (mod.3), y $n \equiv 3$ (mod.4), entonces $n \equiv 11$ (mod.12). Además, $n-1$ no puede ser ningún múltiplo de algún número de 3 a 12. Para a) basta con evaluar los números $\equiv 11$ (mod.12) para encontrar la solución.
Para b) es más rápido razonar que n tiene que ser el producto de dos primos > 12. Evaluando esos productos (mod.12) encontramos que 13·23=299 es el menor de ellos, y cumple también la otra condición.

Unidad N 4 - La función Φ de Euler

Viaje de exploración:

3 y **5)** La afirmación 5) es correcta. Verifica mediante la fórmula dada en el viaje guiado:
Si un número n se multiplica por un factor primo p que ya está en n, $\Phi(n)$ se multiplica por p. Si n se multiplica por un factor primo q que no está en n, entonces $\Phi(n)$ se multiplica por $q \cdot \frac{q-1}{q} = q-1$. Así o así, $\Phi(n)$ se multiplica por un número entero.
Eso responde a la vez a la pregunta 3).

"Dos preguntas":

7) Una posibilidad de razonar es ésta:
Supongamos que n contiene los dos factores primos distintos p y q. Al excluir los números divisibles entre p, separamos todos los números de 1 a n en dos "clases": los que son $\equiv 0$ (mod. p), y los que no lo son.
Obviamente, p y q son PESI, ya que ambos son primos.
Ahora, el teorema chino nos dice que dentro del intervalo [1; pq] existe cada combinación posible de un residuo (mod. p) con un residuo (mod. q), exactamente una vez.
Por tanto, en este intervalo hay exactamente q números que son múltiplos de p. Y entre ésos hay un único número, o sea 1/q de ellos, que es también múltiplo de q. O sea, un número que es $\equiv 0$ (mod. p), y también $\equiv 0$ (mod. q).
Y los que quedan, o sea que no son múltiplos de p, son $pq - q = q(p-1)$ números.
Ya que en el intervalo [1; pq] hay p múltiplos de q, $(p-1)$ de ellos están entre "los que quedan". Eso es exactamente 1/q de su cantidad de $q(p-1)$.
Con eso, la demostración ya está casi concluida. Solamente falta añadir que necesariamente, n es un múltiplo de pq (ya que hemos definido p, q como factores primos de n). Por tanto, la misma distribución proporcional aplica al entero intervalo [1; n].
Y podemos aplicar el mismo razonamiento a otros factores adicionales de n.

Para practicar:

***10.a)** C.S.={5; 8; 10; 12}
b) C.S.={11; 22}
c) C.S.={35; 39; 45; 52; 56; 70; 72; 78; 84; 90}
d) No hay solución. *(El valor de $\Phi(x)$ siempre es par; excepto $\Phi(2)=1$. ¿Puedes explicar por qué?)*
- Ecuaciones como éstas se pueden resolver, intentando construir x "al revés". Por ejemplo, si $\Phi(x) = 24$, entonces $x = 24 \cdot \frac{p}{p-1} \cdot \frac{q}{q-1} \cdot \frac{r}{r-1} \cdot \ldots$
Una solución es válida, si x contiene exactamente los factores primos p, q, r, ..., y ningún otro. – La elección de esos factores es limitada, ya que $p-1$, $q-1$, etc, tienen que ser divisores de 24 (en este ejemplo).

Investigación: Números aleatorios PESI

a) Un método seguro, pero tedioso, es el siguiente: Examinamos para cada número de 1 a 50 aparte, cuál es la probabilidad de que ése y un segundo número son PESI. Si el primer número es 1, esa probabilidad es 1 (un evento seguro), porque todos los números son PESI con 1. Si el primer número es 2, los números son PESI si el segundo es impar; entonces la probabilidad es 1/2. Si el primer número es 3, entonces son PESI si el segundo número no es divisible entre 3 (¿cuántos de esos números hay de 1 a 50?). Etc.
Sigue examinando los números de esta manera, y haz una tabla de las probabilidades correspondientes, desde 1 hasta 50. ¿Cómo puedes ahora con la ayuda de esta tabla calcular la probabilidad final, según las leyes del cálculo de probabilidades?
Al elaborar esta tabla, puedes hacer unas observaciones que te facilitarán el trabajo. Por ejemplo verás que para ciertos grupos de números resultan exactamente las mismas probabilidades. ¿Para cuáles? ¿Por qué? – Examina números primos y compuestos por separado. ¿Qué podemos decir acerca de las probabilidades en el caso de números primos? ¿Y con números compuestos?
Ves que todos estos razonamientos están relacionados con la función phi de Euler, $\phi(n)$.
b) Si seguiste las pautas acerca de la pregunta **a)**, entonces ya tienes casi todas las herramientas necesarias para generalizar el problema. Como ya se mencionó en el problema, probablemente no encontrarás ninguna fórmula exacta. Pero las propiedades de la función $\phi(n)$ para diversas n te dan unas pautas para encontrar por lo menos una aproximación.
Una pauta adicional: Si n es grande, entonces podemos suponer que para muchos "primeros números" ***a,*** la

probabilidad de sacar un segundo número tal que sean PESI, es *aproximadamente* $\boldsymbol{\phi(a) / a}$ **.** (Piensa por qué ... y cuán grande o cuán pequeño puede ser el error que resulta si calculamos así.)

Otro razonamiento posible – quizás más sencillo que el anterior:

Si sacamos dos números naturales al azar, ¿cuál es la probabilidad de que *ambos* son divisibles entre 2? ¿y que *ambos* son divisibles entre 3? Etc ... Así puedes hacer una colección de aquellos casos donde los dos números *no* son PESI. Ahora solamente tienes que combinar estos casos de la manera correcta. Por ejemplo, ¿Qué pasa con los números que tienen tanto el 2 como el 3 como divisores comunes?

Y para que puedas comprobar si estás más o menos cerca del valor correcto: Si $\boldsymbol{n}$ es muy, muy grande ("tiende a infinito"), entonces la probabilidad de que dos números naturales de 1 a $\boldsymbol{n}$ sean PESI, se acerca a $\frac{6}{\pi^2}$. Pero para demostrar eso, y para entender lo que tiene que ver el número π aquí, se requieren unos conocimientos más avanzados.

Acerca de la pregunta adicional, cómo se puede deducir la variante "con devolución" desde la variante "sin devolución", y viceversa:

Las dos variantes se distinguen solamente en un grupo específico de eventos, que en una de las variantes está excluido y en la otra variante está incluido: los casos donde se sacan dos números iguales. Por supuesto que dos números iguales no son PESI. Estos casos pertenecen entonces todos a los eventos "no favorables" y no cuentan para la probabilidad total. Solamente incrementan el número total de los "eventos posibles", en la variante donde los incluimos.

¿Qué sucede con el "error", o sea la diferencia entre las dos probabilidades según las dos variantes, cuando $\boldsymbol{n}$ se vuelve muy grande?

Unidad N 5 - Congruencia modular en potencias

La longitud del período - Para pensar:

1) Todas las potencias de 5 contienen como único factor primo el 5 (repetidas veces). Por eso no es posible que alguna de ellas sea divisible entre 7.

Si la base fuera 7, entonces *todas* las potencias serían divisibles entre 7 (excepto el 1); entonces todos los residuos a partir de 7^1 serían cero.

***2)** La idea clave es que *cada* residuo posible pertenece a un grupo del mismo orden, porque cada residuo posible define una secuencia con la misma longitud de período.

Tomando el ejemplo de las potencias de 2, (mod. 7):

Si comenzamos con el residuo 4, y multiplicamos sucesivamente por 2, resulta la secuencia:

4, 1, 2, 4, ...

Es una secuencia con período 3, y es equivalente a la original. - Comencemos ahora con el residuo 3:

3, 6, 5, 3, ...

Otra vez resulta una secuencia con período 3; pero esta secuencia contiene ahora los residuos que *no* pertenecen a la secuencia original.

Generalizado:

Si $\boldsymbol{x}$ no es un residuo de $\boldsymbol{b^k}$ (mod.$\boldsymbol{m}$), entonces $\boldsymbol{bx}$, $\boldsymbol{b^2x}$, $\boldsymbol{b^3x}$, etc, tampoco son residuos de $\boldsymbol{b^k}$ (mod.$\boldsymbol{m}$).

Pero si $\boldsymbol{n}$ es el orden del grupo, entonces $\boldsymbol{b}^n \equiv 1$ (mod.$\boldsymbol{m}$); y entonces $\boldsymbol{b}^n\boldsymbol{x} \equiv 1\cdot\boldsymbol{x} \equiv \boldsymbol{x}$ (mod.$\boldsymbol{m}$). Por tanto, si comenzamos una secuencia de residuos con $\boldsymbol{x}$, el grupo resultante tiene el mismo orden como el grupo que comienza con 1.

De esta manera, el grupo de todos los residuos posibles (cuyo orden es Φ($\boldsymbol{m}$)), se puede particionar en subgrupos de los que cada uno consiste en una secuencia de residuos definidos por algún residuo $\boldsymbol{x}$. Ya que el orden de todos esos subgrupos es igual, su orden tiene que ser un divisor de Φ($\boldsymbol{m}$).

3) El 6 contiene los factores primos 2 y 3. El 24 contiene los mismos factores primos, y ningún otro. Por eso, si multiplicamos el 6 suficientes veces, en algún momento la potencia contiene los factores 2 y 3 por lo menos tantas veces como los contiene el 24; y a partir de ese momento, todas las potencias sucesivas serán divisibles entre 24.

Para practicar:

4) Φ(16) = 8; $8934 \equiv 6$ (mod.8); $13^6 \equiv \underline{\mathbf{9}}$ (mod.16)

Para calcular el último paso, se puede comenzar con $13^3 = 2197 \equiv 5$ (mod.16), y elevarlo al cuadrado:

$25 \equiv 9$ (mod.16).

5) Eso equivale a pedir el residuo (mod.100). Calculamos con Φ(100/MCD(100; 12)) = Φ(25) = 20;

$12^{777} \equiv 12^{17}$ (mod.100).

Podemos calcular el residuo de 12^{16}, elevando sucesivamente al cuadrado:

$12^2 \equiv 44$; $44^2 \equiv 36$; $36^2 \equiv 96 \equiv (-4)$;

$(-4)^2 \equiv 16$ (mod.100). Con una multiplicación más llegamos a 12^{17}: $16\cdot12 \equiv \underline{\mathbf{92}}$ (mod.100).

(Nota: A veces un módulo negativo facilita el cálculo; $(-4)^2$ es más fácil que 96^2.)

6) $63 = 3\cdot3\cdot7$; $6561 = 3^8$. Puesto que 63 contiene el 3 como factor primo, sus potencias mayores son divisibles entre 3^8; el residuo es cero.

7) Φ(1953) = 1080; eso es mayor a 813, por lo cual no nos ayuda. Tenemos las siguientes opciones:

a) Examinar la sucesión de los residuos. En este caso tenemos suerte: $5^6 = 15'625 \equiv 1$ (mod.1953), entonces el orden es 6. $813 \equiv 3$ (mod.6); entonces la respuesta es $5^3 = 125$.

b) Por si eso no hubiera funcionado, podríamos examinar los residuos según cada factor de 1953:

(mod.9): El orden es 6; $5^3 \equiv 8$ (mod.9).

(mod.7): El orden es 6; $5^3 \equiv 6$ (mod.7).

(mod.31): El orden es 3; $5^0 \equiv 1$ (mod.31).

Buscamos un número que cumple con estas tres congruencias, y encontramos que es el 125.

8) 173 ≡ 1 (mod.172). Por tanto, los residuos de todas sus potencias también son iguales a 1.

9) 172 ≡ (–1) (mod.173). Por tanto, la sucesión de los residuos es: 1, –1, 1, –1, ...; la respuesta es –1.

***10)** Aquí el orden del grupo es tan grande que el método 7.a) no nos sirve. Intentamos por factores (7.b):

$\Phi(53) = 52$; $3^{10'000} \equiv 3^{16}$ (mod.53) ≡ 16

$\Phi(101) = 100$; $3^{10'000} \equiv 3^0$ (mod.101) ≡ 1.

Tendrás que probar un poco hasta encontrar un número que cumple con las dos congruencias. *(¿O resolviste el problema de investigación en la Unidad N2? Entonces podrás hacerlo de una manera más sistemática.)*

***11)** Con un divisor tan grande, realmente no hay ningún método "rápido". Pero el siguiente es mucho más eficiente que calcular la entera secuencia de residuos:

Calculamos $103^2 = 10609 \equiv 10609$ (mod.15707).

Elevamos este resultado al cuadrado:

$103^4 = 10609^2 \equiv 10226$ (mod.15707).

(Admito, eso también es bastante trabajo si queremos calcularlo "a mano". Pero verás que tenemos que hacer eso mucho menos que 784 veces.)

Lo elevamos nuevamente al cuadrado:

$103^8 \equiv 10226^2 \equiv 9577$ (mod.15707)

$103^{16} \equiv 9577^2 \equiv 5756$ (mod.15707)

$103^{32} \equiv 5756^2 \equiv 5473$ (mod.15707)

... y asi sucesivamente hasta llegar a 103^{512}.

Ahora, 784 = 512+256+16. Por tanto:

$103^{784} = 103^{512} \cdot 103^{256} \cdot 103^{16}$,

y los residuos de todas estas potencias ya los tenemos en nuestra lista. Entonces nos falta multiplicar ésos, y calcular nuevamente su residuo (mod.15707). Por si quieres verificar tu resultado, es 1018.

Este método permite efectuar la operación entera con 11 multiplicaciones modulares.

Eso funciona con todo exponente, porque cada número natural se puede representar como una suma de potencias de 2. (Eso corresponde a representar el exponente en el sistema binario.)

12) El rango indicado comprende las potencias de 2 hasta 2^{29}. *(Lo podemos averiguar fácilmente así: 2^{10} es un poco mayor a 1000; entonces 2^{30} es un poco mayor a 1'000'000'000.)*

El orden del grupo es 6, y el primer residuo de 7 ocurre en 2^4. Entonces, nuestra pregunta equivale a:

¿Cuántos números de la forma 4 + 6***k*** hay de 1 a 29?

Y encontramos que son 5.

13) $\Phi(8) = 4$; $\Phi(3) = 2$; $\Phi(5) = 4$.

El orden del grupo de los residuos es 4, o un divisor de 4, (mod.8), (mod.3), y (mod.5). Por tanto, el orden es 4 también (mod.8·3·5 = 120). Esto significa que en cada 4^{ta} potencia se repite el residuo de 1, para todas aquellas bases que son PESI con 2, con 3 y con 5. Todos los primos > 5 cumplen con esta condición; por tanto la afirmación es verdadera.

**** Investigación adicional:*** De hecho, esas potencias son incluso ≡ 1 (mod.240). ¿Puedes fundamentar por qué?

14) Tenemos dos períodos que se repiten, de longitud ***a*** y de longitud ***c***. Ambos *juntos* se repiten después de MCM(***a***; ***c***). Y si el primero es una congruencia (mod.***p***) y el segundo una congruencia (mod.***q***), entonces la combinación de ambos es una congruencia (mod. MCM(***p***; ***q***)), según el teorema chino de los residuos. Por tanto:

El "gaussiano" respecto a la base ***b*** (mod MCM(***p***; ***q***)) es igual a MCM(***a***; ***c***).

(Este es el principio que se aplicó en la resolución del problema 13.)

***15)** Este es un problema de encontrar un "logaritmo modular"; y desafortunadamente no existe ningún método eficiente para eso. Tenemos que examinar la secuencia de residuos, que es:

1, 7, 3, 21, 9, ...

El matemático atento se detiene aquí y observa que 9 ≡ (–14) (mod.23). Si investigaste en el viaje de exploración las propiedades de esas secuencias respecto a módulos negativos (o si estudiaste este tema en la sección "Ampliaciones"), entonces sabes cómo aprovechar este dato: Si el orden del grupo es 22, entonces $7^{11} \equiv (-1)$ (mod.23); y entonces $7^4 \cdot 7^{11} \equiv (-14)\cdot(-1) \equiv 14$ (mod.23); por tanto ***x*** = 4+11 = 15.

Solamente falta verificar si efectivamente $7^{11} \equiv (-1)$ (mod.23). (El orden podría ser 11, y en este caso el residuo 14 no existiría, o sea no habría solución.)

***16)** Similar a 15). Si $10^{\boldsymbol{n}} + 8$ es divisible entre 1377, entonces $10^{\boldsymbol{n}} \equiv (-8)$ (mod.1377). Ya que $1377 = 3^4 \cdot 17$, podemos proceder por factores:

$10^6 \equiv (-8)$ (mod.17), y el orden es 16. Entonces:

n ≡ 6 (mod.16).

$10^8 \equiv (-8)$ (mod.81), y el orden es 9. Entonces:

n ≡ 8 (mod.9).

La menor ***n*** que cumple las congruencias es 134.

(Nota: 81 es 9·9, y el orden (mod.9) es 1. Así podemos saber anticipadamente que el orden (mod.81) no puede ser mayor a 9.)

***17.a)** $2^{\boldsymbol{x}} \equiv 1234$ (mod.10'000)

Comenzamos con los residuos (mod.10), que deben ser iguales a 4. Vemos que ***x*** ≡ 2 (mod.4).

Ahora solamente tenemos que examinar 2^2, 2^6, 2^{10}, etc. Los residuos (mod.100) de esta secuencia son:

4, 64, 24, 84, 44, 4, ...

El residuo 34 no aparece. Por tanto, no hay solución.

(Más rápido lo hubiéramos visto si hubiéramos pasado primero a los residuos (mod.20). Ésos son 4, 4, 4, ...; pero 1234 ≡ 14 (mod.20).)

b) Procedemos como antes: $2^{\boldsymbol{x}} \equiv 6$ (mod.10), entonces ***x*** ≡ 0 (mod.4).

Los residuos de las potencias 2^4, 2^8, 2^{12}, ... (mod.100):

16, **56**, 96, ...

El orden es 20 (eso ya lo hemos visto en a), donde el 4 se repitió en 2^{22}). Entonces $\boldsymbol{x} \equiv 8$ (mod.20).

Examinamos entonces 2^8, 2^{28}, etc. (mod.1000). Para avanzar de un miembro al siguiente, podemos multiplicar por 576, porque $2^{20} \equiv 576$ (mod.1000):

256, **456**, 656, 856, 56, 256, ...

(Podríamos habernos detenido en 456, porque allí ya vemos que los residuos (mod.200) se repiten, y así podríamos deducir ya que el orden es 20·5 = 100.)

Entonces $\boldsymbol{x} \equiv 28$ (mod.100).

Seguimos con el proceso (mod.10000); la nueva sucesión es:

5456, 1456, 7456, **3456**, ...

El residuo 3456 corresponde a 2^{328}; ésa es la solución.

c) ¡Este problema nos lleva a un tema completamente diferente! No daré la solución aquí, pero unas pautas:

Un método tentativo podría consistir en encontrar una aproximación, y desde allí encontrar otra aproximación más cercana. Por ejemplo:

$2^{10} = 1024$

$2^{20} = 1048576$

$2^{30} = 1073741824$

Vemos que las 4 cifras del inicio aumentan poco a poco. Siguiendo esta sucesión, ¿quizás llegamos a 1234? - Pero 2^{80} comienza con 1208, mientras que 2^{90} comienza con 1237. Hemos "saltado" una solución posible.

Pero podemos observar lo siguiente: 2^7 comienza con 128. 2^{110} comienza con 129. Entonces, si multiplicamos por 2^{103} (103 = 110–7), obtenemos una potencia que comienza con unas cifras sólo ligeramente mayores que la original. Por ejemplo, $2^{80} \cdot 2^{103} = 2^{183}$ = 1225... Ya estamos más cerca. Pero si multiplicamos otra vez por 2^{103}, el resultado ya se hace demasiado grande.

Pero quizás encontramos otros "multiplicadores" que permiten aproximarnos con aun más precisión ... hasta que lo logramos.

Por el otro lado, calcular con potencias tan grandes es tedioso; aun si usamos aproximaciones y calculamos por ejemplo solamente las 10 primeras cifras. Nos facilitamos el trabajo si calculamos con *logaritmos (vea Unidad A 17)*.

¿Cómo representarías $2^{\boldsymbol{x}}$ con un logaritmo?

¿Cómo representarías "un número que comienza con 1234" con un logaritmo?

¿Y cómo representarías con logaritmos el proceso de aproximación que acabamos de describir?

¿Cuál debe ser la precisión de los logaritmos, para poder encontrar una solución con seguridad? O sea, ¿con cuántos dígitos decimales tenemos que calcular?

Limitando así la precisión, ¿hay una forma de representar este problema como una ecuación diofántica?

Sigue investigando...

Solamente una nota adicional: Al usar logaritmos, esto se convierte en un problema de números irracionales. Básicamente se trata de encontrar un múltiplo de un número irracional, cuya parte fraccionaria debe encontrarse dentro de cierto intervalo estrecho. Por ejemplo, es un problema similar al siguiente:

"Encuentra un número natural $\boldsymbol{k}$, de manera que $\boldsymbol{k}\sqrt{2}$ difiera en menos de 0.00001 de un número entero."

O, en un nivel superior:

"Encuentra tu número de teléfono como cifras sucesivas en los dígitos decimales de π."

Es un teorema de la teoría de números, que esta clase de problemas siempre tiene solución – incluso infinitas soluciones. Parece bastante obvio: En los números irracionales no hay periodicidad. Entonces, si repetimos la misma operación infinitas veces, es de asumir que en los resultados, cualquier combinación finita de cifras aparecerá alguna vez. (Pero eso es todavía lejos de ser una demostración rigurosa del teorema ...)

Unidad N 6 - Residuos cuadráticos y problemas relacionados

Diagramas de cuadrados modulares:

1, 2) Las dos preguntas son relacionadas entre sí. Si la mitad de los residuos posibles tienen una raíz modular, entonces distribuyendo todos los residuos "equitativamente" entre ellos, les toca dos raíces a cada residuo. Pero si solamente un cuarto de los residuos tienen una raíz modular, entonces les toca cuatro raíces a cada uno de ellos.

¿Y por qué hay menos residuos cuadráticos distintos si $\boldsymbol{m}$ es compuesto? - Para que dos cuadrados $\boldsymbol{a}^2$, $\boldsymbol{b}^2$ tengan el mismo residuo (mod.$\boldsymbol{m}$), su diferencia tiene que ser un múltiplo de $\boldsymbol{m}$. Pero $\boldsymbol{a}^2 - \boldsymbol{b}^2 = (\boldsymbol{a}+\boldsymbol{b})(\boldsymbol{a}-\boldsymbol{b})$. Si $\boldsymbol{m}$ es primo, eso es un múltiplo de $\boldsymbol{m}$ solamente si $\boldsymbol{a}+\boldsymbol{b} = \boldsymbol{m}$, o sea $\boldsymbol{b} \equiv (-\boldsymbol{a})$ (mod.$\boldsymbol{m}$). Por eso, un mismo residuo cuadrático puede ocurrir solamente dos veces en los cuadrados de los números de 1 a $\boldsymbol{m}$.

(Para el otro factor, si $\boldsymbol{a}-\boldsymbol{b} = \boldsymbol{m}$, entonces $\boldsymbol{a} \equiv \boldsymbol{b}$ (mod.$\boldsymbol{m}$); eso no crea ninguna ocurrencia "nueva".)

En cambio, si $\boldsymbol{m}$ es compuesto, entonces sus factores podrían repartirse entre $\boldsymbol{a}+\boldsymbol{b}$ y $\boldsymbol{a}-\boldsymbol{b}$. Por ejemplo si $\boldsymbol{m}$=12, podría ser $\boldsymbol{a}+\boldsymbol{b} = 6$, $\boldsymbol{a}-\boldsymbol{b} = 2$. Eso crea posibilidades adicionales para residuos repetidos.

3, 4) Un cuadrado multiplicado por un cuadrado da un cuadrado. Un cuadrado multiplicado por un número que no es un cuadrado, da un número que no es un cuadrado. (Puedes verificarlo examinando lo que sucede con los factores primos: En un cuadrado perfecto, los exponentes de *todos* sus factores primos son pares.)

Lo mismo aplica en la aritmética modular. Por tanto, si

(–1) y ***r*** son cuadrados perfectos (mod.***m***), entonces su producto (–***r***) también es un cuadrado perfecto (mod.***m***). Lo mismo aplica al producto de dos residuos cuadráticos cualesquieras (mod.***m***). En cambio, el producto de un residuo cuadrático por un número que no es residuo cuadrático, no es un residuo cuadrático.
Además, si ***m*** es primo, entonces el producto de dos números que *no* son residuos cuadráticos, da un residuo cuadrático. (¿Puedes demostrarlo?)

5) Si (–1) es un residuo cuadrático, entonces cada residuo cuadrático ***r*** tiene su "complemento" (–***r***). Entonces, la cantidad de todos los residuos cuadráticos distintos (con excepción del 0) es par. Con ***m*** primo, eso es posible solamente si ***m***–1 es un múltiplo de 4.

Cuadrados que repiten su propia raíz
Con números de dos cifras, tenemos que calcular (mod.100): $n \equiv n^2$ (mod.100); entonces

$$n^2 - n = n(n-1) = 100k.$$

Ya que ***n*** es un número de 2 cifras, no puede ser un múltiplo de 100. Por el otro lado, ***n*** y ***n***–1 son PESI; entonces cada uno de ellos tiene que contener un factor distinto de 100. Existe una sola forma de descomponer 100 en dos factores que son PESI: 100 = 4·25. Entonces quedan las dos posibilidades:
$n \equiv 0$ (mod.25), y $n-1 \equiv 0$ (mod.4); o viceversa.
Según el teorema chino, para ambos hay una única solución. Para el primer caso es ***n***=25; la otra solución es ***n***=76.
El mismo razonamiento funciona para números de tres cifras (1000 = 8·125), de cuatro (10000 = 16·625), etc. Por tanto, para cualquier cantidad de cifras, siempre existen exactamente dos soluciones.
Además, por la congruencia (mod.100), para *todo* número que termina en 25 resp. 76 (y sólo para ellos), su cuadrado también termina en 25 resp. 76 Eso significa que las soluciones de tres y más cifras también tienen que terminar con 25 resp. 76. (Para tres cifras, son 625 y 376.) Igualmente sabemos ahora que las soluciones de cuatro cifras tienen que terminar con 625 y 376, respectivamente; y así sucesivamente. Eso facilita la búsqueda de soluciones mayores.

Dos otros problemas:

7) Sabemos: La base ***b*** > 7; 2 es un residuo cuadrático (mod.***b***); y nuestro número es un poco mayor a b^4, entonces su raíz un poco mayor a b^2.
El menor número > 7 donde 2 es un residuo cuadrático, es 14. Pero 11572_{14} no es un cuadrado perfecto. Con la siguiente base,17, sí funciona.
- Para hacer la evaluación, se puede simplemente convertir 11572 al sistema decimal y sacar la raíz. Alternativamente, definimos que $11572 = (b^2 + r)^2 = b^4 + 2rb^2 + r^2$, donde ***r*** es una de las raíces modulares de 2 (mod.***b***). Entonces tiene que cumplirse: $2r = 15_b$, y $r^2 = 72_b$. Este método es un poco más rápido.

*8) Aquí se llega a la meta solamente probando con mucha paciencia. O escribiendo un programa para que la computadora lo haga.
Si decides hacer una lista de todas las combinaciones de $2n^2$ más un número primo, de paso podrás apreciar que $2n^2+29$ es primo para toda ***n*** de 1 a 28. O sea, $2n^2+29$ es un "polinomio generador de primos". Este es otro tema interesante de investigación: ¿Encuentras otros polinomios generadores de primos?
Esto es un script de PARI que usa "fuerza bruta" (probando todo con todos los números), para encontrar los que no cumplen con la conjetura:

```
EncuentraNoSol(n) = {
  forstep (i=9, n, 2,
    if (ispseudoprime(i)==0,
      b = sqrtint(i\2);
      haySol=0;
      for (n=1, b,
        if (ispseudoprime(i-n*n*2)==1,
          haySol=n;    \\ Hay solución.
          break
        );
      );
      if (haySol==0,
        print ("Sin solucion: ", i)
      );
    );
  );
  print ("Hecho hasta ", n);
}

EncuentraNoSol(1000000);
```

(Resultado: En el rango hasta un millón hay dos números que no cumplen con la conjetura.)

Unidad N 7 – Tripletos pitagóricos y ladrillos de Euler

Tripletos pitagóricos:
b), *c) Si el cuadrado mayor es la *suma* de los menores, entonces cada uno de los menores es la *diferencia* entre el mayor y el otro. Te ayudará entonces, aplicar tus conocimientos acerca de las propiedades de las diferencias de cuadrados.
Los tripletos se pueden clasificar, por ejemplo, según la diferencia entre el cateto mayor y la hipotenusa. Podrás encontrar toda una sucesión de tripletos donde esa diferencia es 1: 3,4,5; 5,12,13; 7,24,25; .... ¿cómo continúa? - Y lo mismo con una diferencia de 2: 8,15,17 ... ¿cómo continúa aquí?
¿y qué otras diferencias son posibles?
- Para los curiosos voy a descubrir aquí la respuesta a la pregunta *c), porque es un poco difícil que lo encuentres por ti mismo(a). Todo par de números a, b (a<b) genera un tripleto pitagórico de la forma:
$b^2 - a^2$, $2ab$, $b^2 + a^2$. Verifícalo, y sigue investigando.
***d)** Por supuesto que la aproximación es óptima

cuando la diferencia entre los catetos es 1. ¿Cómo puedes encontrar tripletos con esta propiedad? Y si conoces uno de estos tripletos, ¿encuentras quizás un procedimiento que te permite deducir otros a base del primero?

***e)** Si en las preguntas anteriores te limitaste a los tripletos "primitivos" (o sea, donde los lados son PESI), entonces no olvides que ahora para el prisma necesitarás probablemente también tripletos generados mediante la multiplicación ("amplificación") de los "primitivos".

¿Cómo puedes transformar ("amplificar") dos tripletos pitagóricos distintos, de manera que ambos tienen un cateto de la misma longitud? Ese cateto sería entonces uno de los lados del prisma. Los otros catetos serán los otros dos lados. – El gran arte consiste en conseguir que esos otros dos catetos sean *también* los catetos de un "triángulo pitagórico". En este caso completaste un ladrillo.

- *Nota:* Todavía no se encontró una fórmula similar a la de *c), que describiría todos los ladrillos de Euler. Pero se encontraron fórmulas que describen ciertas clases de ellos.

Unidad N 8 - Ecuaciones diofánticas cuadráticas y superiores

Investigación

a) 720 es la diferencia de dos cuadrados perfectos. ¿Qué sabemos acerca de tales diferencias? ¿y qué podemos hacer con el 720 para encontrar los cuadrados que generan esta diferencia?

b) y **c)** Estas dos ecuaciones describen residuos cuadráticos (mod.28), resp. (mod.8). ¿Qué sabes acerca de los residuos cuadráticos? ¿Cómo te ayuda eso para resolver estas ecuaciones? (Básicamente se trata de sacar raíces cuadradas modulares; ya nos hemos encontrado anteriormente con este tema.)

d) Si no ves ninguna luz en el camino, recuerda cual es el tema: Ecuaciones diofánticas de segundo grado.

- Si ya tienes la ecuación, pero sigues sin ver la luz: Este problema es un "caso feliz", porque se puede transformar la ecuación de una manera bastante sencilla, hasta que se pueda usar un método parecido al problema a). Si esto no fuera posible, el problema sería bastante más difícil.

e) Las diferencias de cuadrados perfectos pueden servir aquí también. - Si eso no ayuda, espera hasta el apartado "Ecuaciones diofánticas de grado superior"; allí regresamos a números de la forma $\boldsymbol{a}^2 + \boldsymbol{ab} + \boldsymbol{b}^2$.

***f)** y ***g)** Ecuaciones como las aquí mencionadas se llaman "Ecuaciones de Pell". Entonces, si realmente quieres echar a perder la emoción de la investigación propia (o si ya has investigado por demasiado tiempo), puedes buscarlo en un libro sobre teoría de números o en internet.

****h)** Ésta es realmente difícil. Históricamente, fue necesario el genio de Leonardo Euler para resolverla. Él descubrió cómo se pueden usar las soluciones de una ecuación de Pell para deducir las soluciones de la ecuación más generalizada $\boldsymbol{ax^2 + b = y^2}$.

Problemas diversos:

1) Podemos dar primero un límite inferior y superior para las soluciones: $\overline{\text{abcd}}_{\boldsymbol{8}}$ es *a lo mínimo* $1023_{\boldsymbol{8}} = 531 = 650_{\boldsymbol{9}}$. Y $\overline{\text{efg}}_{\boldsymbol{9}}$ es *a lo máximo* $876_{\boldsymbol{9}} = 717 = 1324_{\boldsymbol{8}}$.

Con eso ya sabemos que $\boldsymbol{a}=1$, y $\boldsymbol{e} \geq 6$.

Ahora hay que probar sistemáticamente con todos los números que tienen cifras distintas en el uno o en el otro sistema de numeración. (Hay 11 soluciones.)

2) Similar al anterior. Adicionalmente, ya que 12 es un múltiplo de 6, sabemos: $\boldsymbol{f} = \boldsymbol{c}+6$ (porque $\boldsymbol{f} \equiv \boldsymbol{c} \pmod 6$, pero no pueden ser iguales). Y por la misma razón, $\boldsymbol{b}$ tiene que ser impar. Entonces $\boldsymbol{b}=3$ ó $\boldsymbol{b}=5$, porque el 1 ya está ocupado por la $\boldsymbol{a}$. Con esta ayuda debes encontrar fácilmente las cuatro soluciones.

3) Observa los tres sumandos: Su suma es igual a $(\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c})\cdot 111_{\boldsymbol{8}}$. $(\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c})$ es a lo máximo $5+6+7 = 18 = 22_{\boldsymbol{8}}$. Ahora solamente falta averiguar cuál de los números de $10_{\boldsymbol{8}}$ hasta $22_{\boldsymbol{8}}$, al multiplicar por $111_{\boldsymbol{8}}$, produce cuatro cifras diferentes en el resultado.

4) Lo escribimos con álgebra:

$\boldsymbol{x}^2 + 2\boldsymbol{x} + 3 + 4\boldsymbol{y}^2 + 4\boldsymbol{y} + 2 = 9\boldsymbol{z}^2 + 6\boldsymbol{z} + 4 \quad | -3$

$\boldsymbol{x}^2 + 2\boldsymbol{x} + 1 + 4\boldsymbol{y}^2 + 4\boldsymbol{y} + 1 = 9\boldsymbol{z}^2 + 6\boldsymbol{z} + 1 \quad | -3$

$(\boldsymbol{x} + 1)^2 + (2\boldsymbol{y} + 1)^2 = (3\boldsymbol{z} + 1)^2$

Se trata entonces de encontrar un tripleto pitagórico que cumple esta condición; y además $\boldsymbol{z} \geq 10$ (por las cifras dadas).

***5)** Aquí no hay una salida fácil como en 4). Pero después de transformar la ecuación, se puede llegar a:

$\boldsymbol{x}\,(3\boldsymbol{x} - 4) = 2\boldsymbol{y}^2 + 2\boldsymbol{y} + 7$.

Ahora podemos sustituir $\boldsymbol{y}$ sucesivamente por los números de 10 en adelante, y ver con cuál de ellos el lado derecho se puede factorizar de una manera que corresponde al lado izquierdo.

6) Examinamos las *primeras* cifras de cada número:

$\overline{\text{ma}}... \cdot \overline{\text{ma}}... = \overline{\text{ma}}...$ - Eso es posible solamente si $\boldsymbol{m}=1$, $\boldsymbol{a}=0$. - Examinamos ahora las últimas cifras:

$...\overline{0\text{i}} \cdot ...\overline{0\text{t}} = ...\overline{\text{c}0}_{\boldsymbol{6}}$. Entonces $\boldsymbol{i} \cdot \boldsymbol{t} = 2 \cdot 3$ ó $4 \cdot 3$. Pero $\boldsymbol{c}$ no puede ser 1; por tanto solamente $4 \cdot 3$ es posible. Prueba con $\boldsymbol{i}=3$, $\boldsymbol{t}=4$, y con $\boldsymbol{i}=4$, $\boldsymbol{t}=3$.

***7)** $\overline{\text{bac}}$ es un divisor de $\boldsymbol{n}$ y de $\sigma(\boldsymbol{n})$. Eso permite analizar los factores primos posibles de $\boldsymbol{n}=\overline{\text{a0bc}}$.

El factor 2 necesariamente tiene que aparecer, porque con solamente factores impares no se puede lograr una combinación así. Por el otro lado, el factor 5 no puede aparecer, porque entonces los números terminarían con 0. Pero en la primera multiplicación, $\boldsymbol{c} \cdot \boldsymbol{c}$ termina con $\overline{\boldsymbol{bc}}$. (Si $\boldsymbol{c}=0$, sería $\overline{\boldsymbol{cc}}$.) - Así sabemos a la vez que $\boldsymbol{c}=6$.

Si $\boldsymbol{n}$ contiene 2^2 ó 2^5, entonces $\sigma(\boldsymbol{n})$ contiene el factor 7.

(Y también 3^2, si es 2^5.) - No puede ser 2^3 ni 2^7, porque se produciría un factor 5. - 2^4 y 2^6 son improbables, porque se producirían factores primos grandes (31 resp. 127).
Prueba entonces cuáles combinaciones de los factores 2, 7, y posiblemente el 3 u otros, pueden producir un número $\overline{ba6}$ que es un divisor de $\overline{a0b6}$ y de $\sigma(\overline{a0b6})$. Lo demás se dará por sí solo.

8) Las cifras dadas ya permiten deducir que $\overline{ca}$ = 40. Entonces el cuadrado termina con 4; por tanto ***e***=2 u 8. Eso da $\overline{ec}$ = 24 ó 84. Con eso quedan muy pocas posibilidades para $\overline{be}$; hay que probarlas.
Alternativamente, podemos continuar la operación de sacar la raíz cuadrada: tenemos $2\overline{bcd}$ ÷ 800, y eso puede dar solamente 2 ó 3.

9)** Ambos lados de la ecuación deben contener los mismos factores primos. Por tanto, ***a y ***b*** deben juntos contener los factores 2 y 3; y ***c*** debe contener el factor 5. Y ninguno de los números ***a***, ***b***, ***c*** puede ser grande, porque cada uno aparece en un exponente. Hay que probar unas combinaciones sensatas.

10) Puedes probar con tripletos "pequeños", si la suma de alguno de ellos da un divisor de 1000; entonces puedes multiplicar los números por el factor correspondiente. - O si conoces la fórmula general de los tripletos pitagóricos, puedes establecer una ecuación y verás que ésa requiere una factorización de 1000.

11.a) Como ecuación: $1000\cdot\overline{abc} + \overline{def} = (\overline{abc} + \overline{def})^2$
Restamos por ambos lados $(\overline{abc} + \overline{def})$, para poder factorizar ambos lados:

$$999\cdot\overline{abc} = (\overline{abc} + \overline{def})^2 - (\overline{abc} + \overline{def})$$
$$= (\overline{abc} + \overline{def}) \cdot (\overline{abc} + \overline{def} - 1)$$

Ahora se trata de encontrar unos valores para $\overline{abc} + \overline{def}$, que permiten que el producto al lado derecho sea un múltiplo de 999. Descubre tú mismo(a) cómo hacer eso.

b) De manera similar puedes resolver esto también.

Ecuaciones diofánticas de grado superior:

1.a) Examina las descomposiciones de esos números en factores primos. Encontrarás que siempre aparece una misma clase de factores primos; y hay otra clase de factores primos que nunca aparecen.

b) Si hiciste unas colecciones lo suficientemente grandes, habrás notado que ambas fórmulas describen *exactamente el mismo conjunto de números*.
O sea, para cada número de la forma $\boldsymbol{a}^2 + \boldsymbol{ab} + \boldsymbol{b}^2$ se pueden encontrar dos números ***c***, ***d***, de manera que el número es igual a $\boldsymbol{c}^2 - \boldsymbol{cd} + \boldsymbol{d}^2$. Y viceversa.
¿Puedes demostrarlo algebraicamente?
Y si los números ***a*** y ***b*** son dados, ¿cómo exactamente puedes encontrar ***c*** y ***d***?

c) Efectivamente aplica la misma propiedad. Y existe también para estos números una identidad similar a la identidad de Brahmagupta *(vea Unidad N 8)*. Si examinas algunos ejemplos con números, quizás la puedes encontrar. Eso ya demuestra la primera parte del teorema: El producto de dos números de la forma $\boldsymbol{a}^2 + \boldsymbol{ab} + \boldsymbol{b}^2$ es a su vez un número de la misma forma (y existen *dos* pares de números ***a***, ***b*** que lo describen). - Lo inverso es más difícil de demostrar; habría que encontrar algún método de reducción a números menores.

2) Coleccionando suficientes ejemplos, te darás cuenta de algunos patrones regulares. Para ciertas ***a*** existen muchos residuos cúbicos distintos; o sea, hay soluciones para muchas ***b*** distintas. Para otras ***a*** existen pocos residuos cúbicos, y para muchas ***b*** no hay solución. ¿Qué tienen en común las ***a*** donde eso es el caso?
Como en los residuos cuadráticos, encontrarás que aquí también hay unas simetrías; pero son distintas de las simetrías de los residuos cuadráticos. ¿Puedes explicar por qué?

3) Ahora ya tienes una oportunidad para aplicar los conocimientos que adquiriste al investigar el problema 1. Para que exista una solución, la ***a*** tiene que ser una diferencia de dos cubos (resp. una *suma* de dos cubos, en el caso de la segunda ecuación). Entonces aplican las factorizaciones que mencionamos en el problema 1. Ya debes conocer ahora varias propiedades que el factor grande tiene que cumplir. Entonces te falta solamente investigar cómo se relaciona el factor grande con los factores pequeños ($\boldsymbol{x}+\boldsymbol{y}$ resp. $\boldsymbol{x}-\boldsymbol{y}$).
Para encontrar los casos con dos o más soluciones, para al problema 4.

4) La pauta para **3.** aplica aquí también. Realmente, este problema es equivalente a la pregunta cómo se pueden encontrar los casos donde las ecuaciones del problema 3 tienen dos soluciones.
Nota además, que la ecuación se puede transformar así: $\boldsymbol{x}^3 - \boldsymbol{v}^3 = \boldsymbol{z}^3 - \boldsymbol{y}^3$. Entonces obtenemos al mismo tiempo los números que se pueden expresar de dos maneras como la *diferencia* de dos cubos.

5) Para descubrir cuáles son los números "imposibles", investiga los residuos cúbicos módulo 9. Existen muy pocos de ésos. Sumando tres de ellos, existen algunos residuos módulo 9 que no pueden salir como resultado; ésos son los números imposibles.
Si deseas unos desafíos que quizás puedes resolver todavía sin computadora, intenta encontrar soluciones para el 78, el 79, y el 51. Los números ***x***, ***y***, ***z*** para el 78 y para el 79 tienen dos cifras; para el 51 tienen tres cifras.
Una primera estrategia puede consistir en calcular $\boldsymbol{a}+\boldsymbol{x}^3$ y $\boldsymbol{a}-\boldsymbol{x}^3$ para $\boldsymbol{x}$ = 0, 1, 2, 3, etc, y examinar cada resultado para ver si puede ser la suma de dos cubos (vea problema 3). Si lo es, entonces encontraste una solución.
¿Quizás encuentras una manera de mejorar esta estrategia?

6) Hay diferentes maneras de describir las soluciones.
Es recomendable transformar la ecuación así:

$$\boldsymbol{y}^3 = \boldsymbol{z}^4 - \boldsymbol{x}^2 = (\boldsymbol{z}^2 + \boldsymbol{x})(\boldsymbol{z}^2 - \boldsymbol{x})$$

Ahora podemos analizar los factores al lado derecho. ¿Qué condiciones tienen que cumplir para que su

producto sea un cubo perfecto?
Una solución obvia es que el factor mayor sea el cuadrado del menor; o sea $(z^2 + x) = (z^2 - x)^2$; entonces $y = z^2 - x$. ¿Cómo podemos encontrar números que cumplen esta condición?
Pero existen otras variaciones. Si y es un número compuesto, entonces existen más formas de descomponer y^3 en factores.
Otra estrategia, menos obvia, es la siguiente: Buscamos primero tres números que cumplen:

$$a^2 + b^2 = c^4$$

Éstos se pueden encontrar, analizando las propiedades de los tripletos pitagóricos *(vea Unidad N 7)*.
Multiplicamos la ecuación entera por b^4, y tenemos:

$$(ab^2)^2 + (b^2)^3 = (bc)^4$$

... y entonces $x = ab^2$, $y = b^2$, $z = bc$.

7) La clase "fácil" de soluciones se puede encontrar de una manera similar a la última estrategia descrita para el problema 6.
Las otras clases de soluciones se encuentran, transformando la ecuación así:

$$y^2 = z^3 - x^3 = (z - x)(z^2 + zx + x^2)$$

Ahora existen dos posibilidades para que el lado derecho sea igual a un cuadrado perfecto:
a) Ambos factores son cuadrados perfectos.
b) Ambos factores son cuadrados perfectos, multiplicados por un mismo factor común. (En este caso, ¿cuán grande puede ser ese factor común a lo máximo?)
Para ambos casos, descubre qué condiciones tienen que cumplir los números x, z, y cómo se pueden entonces encontrar tales números.

- Una vez que encuentras una solución, puedes desarrollar infinitas soluciones a partir de ésta, puesto que la ecuación no contiene ninguna constante: solamente necesitas multiplicar las soluciones de la manera correcta. (De una manera parecida a los tripletos pitagóricos, pero no exactamente igual.) - Solamente que aun de las soluciones "fundamentales" o "primitivas" existen todavía infinitas ...

Sumas y diferencias de cuadrados perfectos:
a) ¿Cómo se puede transformar algebraicamente una diferencia de dos cuadrados perfectos?
b) Aquí será más difícil llegar a la meta con álgebra. Es bastante difícil expresar algebraicamente que un número es primo, o que dos números son PESI. Mejor colecciona primero unos ejemplos; después analiza.
c), d) Aquí es más fácil, traducir las propiedades dadas al lenguaje del álgebra. – También pueden ayudarte los resultados de la *Unidad N 6* sobre los residuos cuadráticos.

e) Algebraicamente, el producto de dos sumas de cuadrados es:
$(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$
Ahora, el "truco" consiste en añadir, y enseguida sustraer, el producto $2abcd$:
... $= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + 2abcd - 2abcd$
Si ordenas los términos de manera apropiada, vas a tener la suma de dos cuadrados. Y si descubres una segunda manera de ordenar los términos, entonces ya respondiste la pregunta **f)** también.
Esa es la famosa "Identidad de Brahmagupta", que ahora te faltan solamente dos pasos para descubrirla.
***)** *Para seguir investigando:* Si conoces dos descomposiciones de un número en sumas de dos cuadrados perfectos, ¿cómo puedes usar ese dato para factorizar el número? Por ejemplo, sabiendo que $31373 = 38^2+173^2 = 82^2+157^2$, ¿puedes con la ayuda de este dato factorizar 31373?

Unidad N 9 - Problemas diversos

Problemas cerrados:

1) Los números triangulares tienen la forma $n\cdot(n+1)/2$. Para que tengan muchos divisores, tanto n como $n+1$ deben tener una variedad de factores primos.
Podemos primero intentar estimar el tamaño aproximado de nuestro número. Por ejemplo, un número con 9 factores primos distintos, cada uno una vez, tendría $2^9 = 512$ divisores. El menor de esos es $2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23 = 223'092'870$. En este caso, $n \approx 21'000$. - Pero si elevamos los factores menores a potencias mayores, podemos obtener un número menor que también tiene 512 divisores; por ejemplo $2^7\cdot3^3\cdot5\cdot7\cdot11\cdot13 = 17'297'280$. En este caso, $n \approx 6000$.
Entonces, hay que buscar dos números sucesivos, aproximadamente en el rango entre 6000 y 21'000, que tengan únicamente factores primos pequeños. (Los matemáticos llaman a esos números "números suaves".)
Puedes pensar cómo crear un script de PARI que haga eso. ¿O quieres intentarlo "a mano"? - Una idea sería, coleccionar todos los números entre 6000 y 21'000 (aproximadamente) que tengan solamente factores primos hasta 23, o hasta 29, y después buscar si hay dos sucesivos entre ellos. - O podemos coleccionar los números que tengan solamente uno, dos, tres, o al máximo cuatro factores primos pequeños distintos; y después evaluar si el antecesor o el sucesor de uno de esos números es también un "número suave". - O podemos asumir que nuestro número contiene como mínimo los factores 2^3 y 3^2. (Si no tuviera éstos, sería muy improbable que sea "pequeño" y sin embargo tenga muchos divisores.) Entonces existen dos posibilidades: n (ó $n-1$) contiene ambos factores, entonces n (resp. $n-1$) es un múltiplo de 72. O los factores se reparten entre n y $n-1$; en este caso esos

dos números son congruentes a ±8 resp. ±9 (mod.72). Repasa todos los números desde 6000 en adelante que cumplen estas condiciones, y descarta de antemano los que contienen factores primos grandes.
Con cualquiera de estas estrategias, necesitarás mucha paciencia. Y al encontrar un "candidato", por supuesto que hay que evaluar si el número triangular correspondiente tiene realmente más que 500 divisores.
¿Quizás escribir un script de PARI da menos trabajo?
Sigue investigando ...

2) Sea ***d*** el denominador; entonces el orden de los residuos de las potencias de 10 (mod.***d***) es 15. Por tanto, ***d*** es un divisor de $10^{15} - 1$.

Pero ***d*** no debe ser divisor de $10^3 - 1$ ni de $10^5 - 1$, porque en este caso el orden sería 3 resp. 5.
Aplicando cocientes notables *(Unidad A 9)*, se factoriza:

$10^{15} - 1 = (10^5-1)(10^{10} + 10^5 + 1)$
$= (10-1)(10^4+10^3+10^2+10+1)(10^{10} + 10^5 + 1)$
$= 9 \cdot 11111 \cdot 10000100001,$

y también:

$10^{15} - 1 = (10^3-1)(10^{12} + 10^9 + 10^6 + 10^3 + 1)$
$= (10-1)(10^2+10+1)(10^{12}+10^9+10^6+10^3+1).$
$= 9 \cdot 111 \cdot 1001001001001.$

Ya que 111 y 11111 son PESI, 111 tiene que ser un divisor de 10000100001, y viceversa. Eso nos permite factorizar más completamente:

$10^{15}-1 = 9 \cdot 111 \cdot 11111 \cdot 90090991.$

Pero $111 = 3 \cdot 37$, y $11111 = 41 \cdot 271$.
(Puede ser interesante saber que 41 y 271 son los únicos denominadores primos que producen números decimales con un período de 5 cifras.)
Entonces:

$10^{15}-1 = 3 \cdot 3 \cdot 3 \cdot 37 \cdot 41 \cdot 271 \cdot 90090991.$

Adicionalmente, $(10^{15}-1)\cdot(10^{15}+1) = 10^{30}-1$, y por el "pequeño teorema de Fermat" sabemos que eso es divisible entre 31. Entonces, ó $10^{15}-1$ ó $10^{15}+1$ es divisible entre 31. Efectivamente:

$10^{15}-1 = 3 \cdot 3 \cdot 3 \cdot 37 \cdot 41 \cdot 271 \cdot 31 \cdot 2906161.$

El último factor, 2906161, es demasiado grande para factorizar "a mano", entonces nos quedamos aquí.
(Comprobando con computadora, resulta que 2906161 es primo.)
Entonces, ***d*** es cualquier producto de algunos de estos factores, que no sea divisor de 999 ni de 99999. Por ejemplo:

$3^3 \cdot 41 = 1107$ $3^3 \cdot 271 = 7317$
$37 \cdot 41 = 1507$ $3 \cdot 31 = 93$ ... etc.

Completa tú mismo(a) la tabla con los que sean menores a 10'000. (¡El 31 solo también cumple!)
- Y casi terminamos. Solamente que el problema no especifica si también valen los números periódicos *mixtos*. En caso que sí, entonces hay que añadir todos los productos de los anteriores por 2 y por 5 (con tal que sean menores a 10'000). Por ejemplo:

$2^3 \cdot 1107 = 8856$ $5 \cdot 1107 = 5535$
$2 \cdot 1507 = 3014$ $2^3 \cdot 5^2 \cdot 31 = 6200$ ... etc.

3) Divisibilidad sucesiva

a) Esta pregunta podrás responder con bastante facilidad, si observas dónde se encuentra el múltiplo de 10, de 11, etc, *anterior* al número que es miembro de la sucesión que buscamos. ¿Qué propiedades debe tener entonces ese "múltiplo anterior"?

b) Aquí puedes acercarte a la meta, si tratas de descubrir en qué orden pueden presentarse los múltiplos. Por ejemplo, ¿es posible que después de un múltiplo de 12 sigue directamente un múltiplo de 15? ¿o de 16? Con estos razonamientos puedes limitar las posibilidades para el orden de los múltiplos. Después, para cada una de estas posibilidades (o para grupos de posibilidades similares) puedes buscar la sucesión correspondiente con los números menores.
Eso puede ser un poco difícil. En vez de buscar la sucesión completa, puede ser más fácil pensar, por ejemplo, qué condiciones tiene que cumplir el *primer* número de la sucesión. Si hiciste la investigación de la *Unidad N 2* acerca de las ecuaciones diofánticas lineales con coeficientes grandes, entonces verás que aquí tenemos un problema similar, solamente un poco más complejo.

c) Puedes proceder de manera similar como en la pregunta b). Solamente tendrás que pensar adicionalmente, cuáles "combinaciones" de divisibilidad serán las más probables. Por ejemplo, ¿cuál es más probable: que un número de la sucesión sea a la vez un múltiplo de 13 y de 17; o que un número sea a la vez un múltiplo de 10 y de 15? – Será aconsejable buscar primero las combinaciones más probables.

4) Factorización grande:

Por supuesto que puedes probarlo también dividiendo. Los primeros cinco o seis factores primos son bastante fáciles de descubrir. Pero después la cosa se vuelve más difícil.
La pauta en el problema te dice que el número a descomponer se puede escribir como $\boldsymbol{x}^{48} - 1$ (y en este caso sabemos que $\boldsymbol{x} = 2$). ¿Recuerdas unas leyes acerca de productos y cocientes notables?
Sin embargo, *un* factor importante no encontrarás de esa manera, y por eso te ayudo un poco más. El "pequeño teorema de Fermat" *(vea Unidad N 5, "Ampliaciones")* nos dice que $2^{96}-1$ tiene que ser divisible entre 97. Por el otro lado, $2^{96} - 1 = (2^{48} + 1) \cdot (2^{48} - 1)$. O sea, el factor primo 97 tiene que estar escondido en *uno* de los dos paréntesis. Con eso existe una probabilidad de 50% de que $2^{48} - 1$ es divisible entre 97.

5) Multiplicación idéntica

a) Llamemos al número original ***n***, y al producto P. Si P "termina con ***n***", entonces P–***n*** tiene que terminar con tantos ceros como ***n*** tiene cifras. El problema nos dice que P = 17***n***. Entonces P–***n*** = 16***n***. Con eso sabemos que 16***n*** tiene que ser un múltiplo de una potencia de 10. ¿Con cuál número - que no termine con cero – podemos multiplicar 16, para obtener la mayor posible potencia de 10 (o un múltiplo de ella)? La ***n*** que buscamos, tendrá que ser entonces un múltiplo de ese

número. - ¿Y cuántos dígitos puede entonces tener n, a lo máximo? - Con eso tienes todas las condiciones necesarias para encontrar la mayor n posible.

b) Llamemos f al factor de multiplicación. Entonces es $P = nf$, y $P-n = n\cdot(f-1)$. Usemos todos los razonamientos que en a) hicimos respecto a la multiplicación por 16, y apliquémoslos a la multiplicación por $f-1$. (¿Hay soluciones para todas las f ?)

c) De manera similar como en a): Si el producto tiene que terminar con el número original *menos 1*, entonces $n\cdot(f-1)$ es un múltiplo de una potencia de 10, *menos 1*. O sea, es un número que termina en ...9999. Y para un número *aumentado* en 1, $n\cdot(f-1)$ tiene que terminar en ...0001.

A diferencia de las potencias de 10, desafortunadamente, no podemos generalizar una factorización completa de este tipo de números. Por eso no podemos decir a primera vista con qué número multiplicar $f-1$ para obtener un tal número. Pero podemos usar un procedimiento que se puede llamar "división desde el final". En el primer ejemplo, $f-1 = 7$. La división es ...9999 ÷ 7. La cifra final del dividendo es 9, entonces el cociente tiene que terminar con 7, porque 7·7 = 49:

```
...9999÷7=...7
    −49
..9995
```

El residuo termina con 5, entonces la siguiente cifra del cociente es también 5:

```
...9999÷7=...57
    −49
..9995
   −35
.9996
```

El nuevo residuo termina con 6. 7·8=56, entonces la siguiente cifra del cociente es 8; tenemos ...857. Así podemos continuar hasta ... ¿hasta dónde? Descubrir eso será tu tarea. Solamente quiero mencionar que cada cociente parcial ya es una solución:

$7 \cdot 8 = 56$, termina con $6 = 7 - 1$.
$57 \cdot 8 = 456$, termina con $56 = 57 - 1$.
$857 \cdot 8 = 6856$, termina con $856 = 857 - 1$.

De manera similar en el segundo ejemplo:

```
...0001÷381=...2021
   −381
..99962
   −762
.9992
  −762
.9923      etc.
```

Si generalizas este problema, verás que para ciertos valores de f no hay solución. ¿Para cuáles? ¿Y con cuál otro tema conocido está relacionado este problema?

6) Números al revés

a) Hay varias maneras de resolverlo. Probablemente lo más práctico es mediante ecuaciones diofánticas. Asumiendo que "el doble" y "el triple" tienen dos cifras:

$2\overline{ab} = 3\overline{ba}$ ... lo que equivale a:

$$20a + 2b = 30b + 3a$$
$$17a = 28b$$

Tenemos ahora la restricción adicional de que a, b tienen que ser cifras de 1 a 9. Vemos inmediatamente que bajo esta condición no hay solución.

Con tres cifras, la ecuación resulta en que la cifra de las decenas tendría que ser negativa: no hay solución. (Compruébalo.) Razonando un poco, podemos ver aun sin ecuación, que la condición no se puede cumplir si la cifra de las decenas debe ser la misma en el "doble" como en el "triple".

Con cuatro cifras tenemos:

$$2000a + 200b + 20c + d = 3000d + 300c + 30b + 3a$$
$$1997a + 170b = 2998d + 280c$$

Ahora nos ayuda el pequeño "truco" de escribir la ecuación (mod.10):

$$7a \equiv 8d \pmod{10}$$

Eso se cumple solamente si a es par. Por ejemplo para $a=2$, $d=3$ v $d=8$. (Repasa la *Unidad N 2* sobre "división modular", y completa las correspondencias entre a y d.)

La ecuación inicial nos dice adicionalmente que $2a \approx 3d$, ya que a, b, c, d son pequeños. Los únicos números de 1 a 9 que cumplen ambas condiciones, son $a=6$, $d=4$. Remplazamos en la ecuación anterior:

$$11982 + 170b = 11992 + 280c$$
$$170b = 10 + 280c$$
$$17b = 1 + 28c$$

... y esto sí tiene una solución con números de 1 a 9.

Ahora debes ser capaz de completar el cálculo, y de buscar soluciones con más cifras, y de investigar las ampliaciones sugeridas en b). (Algunas no tienen solución en absoluto.)

Cuando llegues al caso de "un número que es igual a su cuádruple escrito al revés", compara la solución con la del problema original en a). Quizás puedes observar algo interesante.

Investigación

7) Unas propiedades de potencias superiores

a) Esta pauta es trivial a este nivel, pero quizás la necesitas: ¿Qué significa exactamente, expresado algebraicamente, que "dos números terminan con la misma cifra"?

La expresión **"4k + 1"** señala que existe una *repetición periódica*: Cada cuatro potencias se repiten las mismas cifras finales. Sobre eso aprendiste algo en este bloque. Solamente falta aplicar esta propiedad en el contexto del problema planteado aquí.

b) Aparentemente, esta propiedad aplica solamente a potencias con exponentes *pares*. ¿Qué propiedades particulares tienen esas potencias "pares", a diferencia de las "impares"?

- ¿Por qué el teorema vale solamente para números primos? Y: ¿Realmente es *necesario* que sean números primos?

- En el nivel de *Secundaria I (Unidad 34)* hemos investigado acerca de las reglas de divisibilidad para números compuestos. Ahora solamente tienes que "descomponer" una tal regla "compuesta", y falta poco para llegar a la solución.

8) Factorización según Fermat:

a) No debe ser difícil seguir las instrucciones. Pero para el caso de que necesites ayuda, usemos el primer ejemplo (2077): Buscamos el siguiente cuadrado perfecto; en este caso $46^2 = 2116$. La diferencia con nuestro número es 2116 – 2077 = 39; no es ningún cuadrado perfecto. Lo intentamos entonces con el siguiente cuadrado perfecto (47^2), etc. En algún momento encontrarás una diferencia b^2 que es un cuadrado perfecto. Entonces es $2077 = a^2 - b^2 = (a+b)(a-b)$.

b) Si seguimos la sucesión de los cuadrados perfectos en orden, ¿conoces una ley matemática que te dice cómo progresa esta sucesión?

c) También las *diferencias* siguen la sucesión de los cuadrados perfectos, solamente en pasos distintos. Aun así, puedes aplicar unas leyes acerca de esa sucesión.

– Además, quizás conoces algunas propiedades de los cuadrados perfectos que te ayudan a distinguir rápidamente si un número dado puede ser un cuadrado perfecto o no.

***d)** La pauta anterior te ayudará aquí también: Entre las diferencias que encuentras, habrá algunas que no tienen las propiedades típicas de los cuadrados perfectos. Podemos excluir ésas de antemano. Y esa clase de diferencias ocurrirán con cierta regularidad ... (Otra palabra clave en este contexto: ¡"Residuos cuadráticos"!)

e) El ejemplo 2249 ya te habrá dado la respuesta.

Aquí otro caso, un poco diferente: Intenta con este método encontrar factores de 210. ¿Por qué no funciona en este caso?

***f**) Para cada uno de los dos métodos tenemos que encontrar una manera de medir su "eficiencia". O sea, una fórmula que nos dice cuántos factores posibles podemos encontrar, resp. excluir, con cada operación. Así tendremos una relación matemática entre la cantidad de operaciones que efectuamos, y la cantidad de factores que eso permite encontrar, resp. excluir. (El mismo número n también aparecerá en esta relación.) ¿Dónde tenemos que colocar entonces el límite donde nos detenemos con el método corriente de dividir, y comenzamos con el método de Fermat, para que esa relación sea óptima?

g), h) Existen varias otras formas de hacer que este método sea más eficiente. Algunas de ellas se investigaron recién en el siglo 20. Puedes seguir investigando; quizás descubres una novedad.

Según sé, la siguiente mejora ya fue descrita por el mismo Fermat:

Supongamos que los primeros dos factores que podemos encontrar, son u y v. Si $u < v$, entonces podemos definir la proporción entre u y v como $p = v:u$ (o sea, $v = up$), y nuestro número n es entonces $n = u \cdot v = u^2 \cdot p$. ($p$ no es un número entero.)

Ahora, si podemos aproximar p con una fracción con numerador y denominador pequeños, digamos $p \approx f \div g$, entonces es $v \cdot g \approx u \cdot f$. Eso significa que podemos construir un número que tiene dos factores aproximadamente iguales: $(v \cdot g) \cdot (u \cdot f) = n \cdot g \cdot f$. Pero si un número tiene dos factores aproximadamente iguales, entonces encontraremos ésos muy rápidamente con el método de Fermat.

En realidad no podemos saber de antemano cuál es la proporción p. Pero podemos experimentar. Por ejemplo, si tratamos de descomponer $3n$ en vez de n, entonces encontraremos rápidamente aquellos factores que están aproximadamente en una proporción de 1:3. Si descomponemos $15n$, entonces encontraremos rápidamente los factores que tienen entre sí aproximadamente una de las proporciones 3:5 ó 1:15. Etc ... (sigue investigando ...)

9) Cómo alegrar a un matemático:

Estos números fueron descritos por primera vez por el matemático indio D.R.Kaprekar. Los llamó en el idioma sanscrito "números harshad". ("harshad" = "que causa alegría"). De allí el título especial de este problema.

a) Intenta clasificar los números que deseas investigar, y sepáralos en subconjuntos de números que tienen ciertas propiedades particulares en común.

Puesto que la suma de las cifras está relacionada con el residuo del número al dividirlo entre 9, se recomienda investigar aquellos números en conjunto que son congruentes entre sí (mod. 9).

O puedes directamente unir en conjuntos aquellos números que tienen la misma suma de sus cifras. ¿Dónde se ubican los números que tienen la misma suma de cifras? ¿Y cuáles de ésos pueden ser divisibles entre esa suma de cifras? – O quizás es más práctico, plantear la pregunta al revés. Por ejemplo: ¿En cuáles múltiplos de 7 es posible que la suma de sus cifras sea 7?

Con esta clase de preguntas podrás limitar las posibilidades, de manera que ya no tendrás que examinar muchos números directamente, para saber si son "números harshad" o no.

b) Todos los divisores de n son también divisores de $10n$. Entonces, la conclusión es bastante obvia.

c) ¿Cuándo tenemos una mayor probabilidad de que un número es divisible entre la suma de sus cifras: si esa suma es pequeña, o si es grande? ¿Dónde es más probable que encontremos números con una tal suma de cifras?

d) Ya habrás notado que una porción bastante grande de los números harshad son múltiplos de 9. (Por si todavía no descubriste eso, piensa ahora por qué eso es así.) Entonces tendrás que fijarte particularmente en esos números, si quieres encontrar un intervalo largo sin números harshad.

***e)** Será difícil, predecir una tendencia general en la frecuencia de los números harshad, y/o fundamentar lógicamente la existencia de una tal tendencia. Pero las respuestas a las preguntas c) y d) muestran que existen ciertos "patrones" de áreas donde los números harshad son frecuentes, resp. poco frecuentes.

Si quieres describir estos "patrones" más exactamente, quizás te ayudará imaginarte cómo se ve generalmente la función "suma de las cifras". Respectivamente, cómo puedes descubrir cuántos números en un intervalo dado tienen una suma de cifras dada. ¿Y cuál es la

probabilidad de que un número con una suma de cifras ***n*** es divisible entre ***n*** (expresada como función de ***n***)? – Haz unas predicciones para varias ***n*** en un intervalo específico. Después verifica tus predicciones con un conteo exacto. Si para ciertas ***n*** tu predicción estuvo muy lejos de la realidad, entonces trata de descubrir por qué. ¿Quizás tienen esas sumas "especiales" de cifras unas propiedades que no tomaste en consideración?

f) La "regla del 9" tiene su correspondencia en los sistemas de numeración con otras bases. *(Vea Unidad N 5)* Ya hemos visto que esa regla influencia la distribución de los números harshad. Por lo demás, puedes hacer razonamientos similares como en las investigaciones con el sistema decimal.

Un caso interesante es el sistema binario. Parece que allí valen unas leyes distintas. Quizás te ayuda hacer unos razonamientos adicionales acerca de la divisibilidad de las potencias de 2; o mejor dicho, acerca de los *residuos* de las potencias de 2, módulo ***n***.

10) Una misteriosa secuencia de números:

¿Qué es lo que hace la operación de "duplicar y sumar"? - En el fondo, estamos calculando *la suma de una progresión geométrica*. El desplazar cada número dos columnas hacia la derecha, tiene el efecto de dividirlo entre 100. Y si antes de eso lo duplicamos, en el efecto final lo dividimos entre 50. O sea, estamos calculando la suma de una P.G. con $q = {}^{1}/_{50}$. Y el problema original sugiere que debemos imaginarnos la P.G. como infinita. Entonces, su suma es: $\frac{a}{1-\frac{1}{50}} = a\left(1\frac{1}{49}\right)$. - Con eso ya deberías encontrar la operación por la que se pregunta en **c)**.

Pero con eso todavía no hemos explicado por qué resulta siempre la misma secuencia, independientemente del número inicial.

- Esperemos todavía un poco con eso, y por mientras daré una pauta acerca de la pregunta **d)**:

Si nuestra secuencia misteriosa debe ser realmente "universal", entonces debe valer también para números iniciales *negativos*. En este caso tenemos que *sustraer* las duplicaciones - ¿de qué? - De cero, por supuesto. Pero para no tener que hacer una operación sin sentido, nos imaginamos que hay un 1 delante de todos los ceros. Entonces se ve así (empezando con 1:

```
(1)000000000000...
 -1
   -2
     -4
       -8
        -16
          -32
            -64  ...
-------------------
  897959183673 ...
```

... y eso es efectivamente la segunda mitad de nuestra sucesión misteriosa. Junto con cualquier número inicial, nuestra sucesión contiene también los resultados para el número negativo correspondiente; y eso requiere que las cifras de las dos mitades se complementan a 9.

Pero vamos ahora a la pregunta principal, la pregunta **a)**. Entendemos a estas alturas que la pregunta es equivalente a: ***¿Por qué en los múltiplos de una fracción, en representación decimal, se repite la misma secuencia de cifras como en la fracción original?***

Porque esto es lo que sucede con los múltiplos de 1/49, como hemos examinado. Y vemos lo mismo, por ejemplo, en 1/13:

1÷13 = 0.076923...
3÷13 = 0.230769...
4÷13 = 0.307692...
... etc.

Al examinar cómo se forman las representaciones decimales de las fracciones (Secundaria I, Unidad 46), hemos visto que esto está relacionado con los residuos que resultan en las divisiones sucesivas. Y éstos, a su vez, están relacionados con los residuos de las potencias *(Unidad N 5)*. Examinémoslo en el ejemplo de la división entre 13:

```
1÷13 = 0.076923...
-91
  90
 -78
  120
 -117
    30
   -26
     40
    -39
      1   ...
```

... y en consecuencia:

$10^0 \equiv 1 \pmod{13}$
$10^1 \equiv 10 \pmod{13}$
$10^2 \equiv 9 \pmod{13}$
$10^3 \equiv 12 \pmod{13}$
$10^4 \equiv 3 \pmod{13}$
$10^5 \equiv 4 \pmod{13}$
$10^6 \equiv 1 \pmod{13}$
... etc.

Ahora, si comenzamos la división con algún otro número, pero que dé uno de los residuos en la tabla arriba, entonces necesariamente se repetirá la misma secuencia de residuos. Por ejemplo si dividimos 9÷13, recibiremos los residuos 9, 12, 3, 4, 1, 10, ... y en consecuencia también las mismas cifras en el resultado: 692307...

Con esto debes estar en condiciones de despejar el misterio del problema inicial por completo.

11) Otra propiedad sorprendente de las potencias superiores:

a) Calcula las potencias de 2 hasta 2^{20}, y cuenta cuántas de ellas comienzan con 1. Así ya notarás que una proporción sorprendentemente grande de esos números comienza con 1. ¿Por qué es eso así?

Podemos acercarnos a una explicación, si primero consideramos que en el intervalo entre dos números ***a*** y ***2a*** tiene que existir exactamente una potencia de 2. (Piénsalo. ¿Puedes demostrar que efectivamente es

así?) – Si definimos ***a*** como una potencia de 10, entonces el intervalo desde ***a*** hasta ***2a*** corresponde exactamente a los números con una determinada cantidad de cifras, que comienzan con 1. (Para matemáticos exactos: Rigurosamente tendríamos que hablar del intervalo semiabierto ***[a; 2a[*** ; o sea, con ***a*** incluida y ***2a*** excluida.) Si por ejemplo ***a*** = 10'000, entonces tenemos los números de 10'000 hasta 20'000, o sea los números con cinco cifras que comienzan con 1. Y efectivamente existe en este intervalo exactamente una potencia de 2: $16'384 = 2^{14}$.

¿Dónde se encuentra en este caso la siguiente potencia de 2? – El doble de un número de 10'000 a 20'000 cae en el intervalo de 20'000 a 40'000. Y la siguiente potencia de 2 después de ésa tiene que encontrarse entre 40'000 y 80'000. Para cada potencia de 2 que comienza con 1, existe otra que comienza con 2 *ó con 3*; y otra que comienza con una de las cifras 4, 5, 6, ó 7. O sea, las potencias de 2 que comienzan con 1, ocurren con la misma frecuencia como aquéllas que comienzan con 2 ó con 3 – *juntas*. Y con la misma frecuencia como aquéllas que comienzan con 4, 5, 6, ó 7 *juntas*. Eso nos da una primera explicación por qué tantas de esas potencias comienzan con 1. Estas relaciones pueden ayudarnos también a encontrar una *aproximación* al valor de esta frecuencia o probabilidad.

Todavía no digo nada acerca de su valor *exacto*. A eso llegaremos a continuación en el punto **b)**.

b) Para las potencias de 3 no podemos hacer exactamente los mismos razonamientos como antes. Caminaremos ahora por un camino distinto; uno que se puede aplicar a potencias de cualquier base.

Imagínate las potencias de 3 como puntos marcados en la recta numérica. Son distribuidos de manera "exponencial": Al inicio hay muchos puntos bastante cercanos los unos a los otros; pero a medida que avanzamos, se vuelven más escasos. Así es difícil calcular la probabilidad de que uno de esos puntos caiga dentro de un intervalo determinado. Sería mucho más práctico si tuviéramos una distribución uniforme.

Podemos lograr eso, si aplicamos a nuestra recta numérica una transformación matemática específica. Buscamos una transformación que hace que nuestros "puntos de potencias" se encuentren a distancias iguales de, digamos, 1 cm entre sí. Después de esta transformación habrán cambiado las distancias entre *todos* los números. Al inicio de la recta, los números naturales se encuentran ahora a distancias bastante grandes; y mientras que el tamaño de los números aumenta, las distancias entre ellos se reducen. A 1 cm del origen encontramos el número 3; a 2 cm se encuentra el 9; a 3 cm el 27; y así sucesivamente. Podemos describir esta transformación con exactitud matemática.

Ahora que los "puntos de potencias" están uniformemente distribuidos, podemos calcular las probabilidades de que uno de ellos caiga dentro de determinados intervalos: Las proporciones entre esas probabilidades son iguales a las proporciones entre las longitudes de los intervalos correspondientes. ¿Puedes ahora calcular cuál porción de nuestra recta "transformada" es ocupada por números que comienzan con 1, en proporción a los otros números?

c) Si pudiste seguir los razonamientos de **b)** hasta el final, entonces esta pregunta ya no es difícil. Solamente te falta calcular las porciones que los números con 2, con 3, etc, ocupan en la "recta numérica transformada".

d) Aquí también te ayudarán las pautas acerca de la pregunta **b)**. Solamente que con otras clases de sucesiones tendremos que aplicar otras clases de transformaciones.

Nota: Este problema está muy relacionado con la "Ley de Benford", formulada en 1938 por el físico Frank Benford (aunque ya había sido observada por Simon Newcomb en 1881). Esta ley dice que en colecciones de números que ocurren de una manera "natural", una proporción relativamente grande de los números comienzan con 1, y solamente una proporción pequeña comienzan con 9. Eso se puede observar por ejemplo en colecciones de constantes de la física; en datos de población; en las longitudes de ríos; en la cantidad de páginas de libros; etc. La ley se cumple con tanto mayor precisión, cuanto mayor es la gama de magnitudes que abarcan los números; o sea, cuando el rango de los números es desde muy pequeños hasta muy grandes. Efectivamente, la probabilidad estadística de que los números de tales colecciones comienzan con 1, es la misma como la que resulta en la pregunta **a)** de nuestro problema.

Sigue investigando ...

12) Progresiones aritméticas de números primos

En la sucesión que se dio como ejemplo, el sexto número es un múltiplo de 7. ¿Cómo se podría encontrar una sucesión donde se siguen más números que no son múltiplos de 7; o que no contienen ningún múltiplo de 7 en absoluto? – Y el mismo razonamiento se puede hacer para otros divisores posibles.

¿Qué condiciones tiene que cumplir entonces el primer número de la sucesión? ¿Y la diferencia entre un miembro y el siguiente?

Con eso ya hemos cumplido muchas condiciones. Pero ¿qué si se nos mete un múltiplo de 11, ó de 13, en medio de la secuencia? - Recuerda la congruencia modular: Si los miembros se siguen en progresión aritmética, entonces también sus residuos (mod.11), (mod.13), etc, forman una P.A. Sabiendo eso, puedes examinar el primer número de la secuencia, y desde allí predecir dónde ocurrirá el primer múltiplo de 11, el primer múltiplo de 13, etc. Y eso a la vez te permite decir qué clases de números son aptos para iniciar tu secuencia, y cuáles no.

Por supuesto que nunca podemos cumplir de antemano todos estos criterios completamente y a la perfección. Es por eso que a la búsqueda tiene que añadirse la perseverancia (o la ayuda de la computadora). Tenemos que elegir cierto número de criterios que creemos poder cumplir, y después examinar todas las secuencias que cumplen con estos criterios.

13) Primo, dos, tres, cuatro

Por si ya descubriste las propiedades matemáticas de esta clase de secuencias, solamente me queda desearte mucha perseverancia al buscar.
Por si no, aquí una pequeña ayuda para empezar: El planteamiento nos da unos datos obvios acerca de la divisibilidad de los números en la secuencia: El primero es primo, el segundo divisible entre 2, el tercero divisible entre 3, etc. – Pero al mismo tiempo tenemos un dato un poco menos obvio acerca de algunas clases de números que *no* pueden ocurrir en la secuencia. Con eso puedes excluir muchas "regiones" donde no necesitas buscar. (El principio es similar al que se tiene que aplicar en el problema anterior.)

14) Progresiones aritméticas de cuadrados perfectos
a) Por una vez voy a proceder al revés: Te presento unos resultados, y te lo dejo a ti encontrar el camino para calcularlos.
En aproximadamente una hora, usando un método más o menos eficaz, encontré "a mano" las siguientes progresiones:

1, 25, 49 (= 1^2, 5^2, 7^2)

... y todos sus múltiplos:

4, 100, 196 (= 2^2, 10^2, 14^2)

9, 225, 441 (= 3^2, 15^2, 21^2)

... etc. (Como con los tripletos pitagóricos, si hemos encontrado una sucesión "primitiva", todas las sucesiones cuyas raíces son múltiplos de las raíces "primitivas", forman también una P.A.)

49, 169, 289 (= 7^2, 13^2, 17^2)

49, 289, 529 (= 7^2, 17^2, 23^2)

289, 625, 961 (= 17^2, 25^2, 31^2)

529, 1369, 2209 (= 23^2, 37^2, 47^2)

2401, 3721, 5041 (= 49^2, 61^2, 71^2)

Acerca del método, solamente una pauta: Una clave consiste en factorizar la diferencia entre los cuadrados, y después analizar qué conclusiones podemos sacar de estas factorizaciones, y cómo encontrar factores que cumplen con las condiciones dadas.
c) Hay un límite de la longitud de una tal P.A, y el límite es bastante pequeño. ¡Quizás logras demostrarlo?

15) Fracciones egipcias
La idea clave para este tema entero consiste en examinar qué es lo que pasa exactamente al sumar las "fracciones egipcias". Después se trata de encontrar algo como una "operación inversa" de ese proceso.
Al sumar fracciones, todos los sumandos tienen que amplificarse a un denominador común. Y después se requiere que la suma se pueda simplificar, de tal manera que obtengamos el resultado deseado, "nuestra" fracción que queremos descomponer en fracciones egipcias. ¿Cuál sería este proceso "al revés"? ¿Y qué te dice eso acerca de las descomposiciones posibles de una fracción?
Como en casi todos los problemas con fracciones, el tema de los múltiplos y divisores es esencial aquí.

16) Problemas sin resolver
a) La mayor dificultad de este problema está en el enorme tamaño de los números involucrados. Pero ¿qué clases de números se pueden siquiera considerar para que sean nuestra x? Si investigas un poco, descubrirás que son mucho menos de lo que uno pensaría a primera vista.
Si solucionaste la pregunta anterior: ¿Cuáles leyes matemáticas permiten limitar el conjunto de los factores primos posibles de $x^x + 1$, de manera que quizás se pueden determinar estos factores aun con x un poco mayores?
- Estas pautas no son nada más que unos intentos de adentrarse al problema. Recuerda que se trata de un problema no resuelto; entonces tienes que encontrar tus propias pautas.
b) Lo dicho arriba aplica también aquí. No tiene mucho sentido dar pautas acerca de un problema no resuelto.
¿Se puede atacar desde el lado de la aritmética modular? - investigando cómo se pueden encontrar dos potencias cuyos residuos difieren en 1 para todos los divisores?
¿o se pueden investigar los múltiplos de los logaritmos de los números naturales, para encontrar dos que estén muy cerca?
¿o existe otro acceso novedoso que tú vas a descubrir?
- Un detalle: Tanto las bases como los exponentes de las dos potencias, en caso de existir, serán PESI. ¿Por qué?
c) Como vez, aun los "números de taxi" siguen teniendo sus preguntas abiertas.
No más pautas ahora; estamos en territorio poco explorado ...

Unidad N 10 - Los números transfinitos de Cantor

Comparar conjuntos infinitos entre sí – Para practicar:

1) Sí, 2) Sí, 3) No (es un conjunto finito), 4) Sí,
5) No (es un conjunto finito).
