Apunte de Teoría de Números

(cómo cocinar un problema)

Pedro Sánchez Terraf — CIEM-FAMAF

22 de octubre de 2010

1. Los ingredientes.

Vamos a estudiar Teoría de Números, es decir, las propiedades de los números enteros $\mathbb{Z}$ (también llamada *Aritmética* por los entendidos). Por ello, salvo que se indique lo contrario, cuando digamos "número" nos vamos a referir a "número entero", y todas las variables que aparezcan se moverán en $\mathbb{Z}$.

En esta sección revisaremos ciertas nociones básicas de la teoría de números que son imprescindibles para comenzar.

1.1. Divisibilidad.

La primera —y la más importante de ellas— es la de divisibilidad.

Definición 1. Diremos que a *divide a* b (sinónimos: "a es factor de b", "a es divisor b", "b es múltiplo de a", "b es divisible por a") y escribiremos "$a \mid b$" cuando exista c tal que $ac = b$.

Ejemplo 1. 3 divide a 6 pues $3 \cdot 2 = 6$. Si $4 \mid a$ entonces $2 \mid a$, pues sabemos que existe c tal que $4c = a$ y en consecuencia $2(2c) = a$. Es decir, existe un número d ($d = 2c$ en este caso) tal que $2d = a$.

Lemaa 2. *Para todos los a, b y c,*

1. *$a \mid b$ implica $a \mid bc$;*
2. *$a \mid b$ y $b \mid c$ implican $a \mid c$;*
3. *$a \mid b$ y $a \mid c$ implican $a \mid b + c$;*

Prueba. Si $a \mid b$, existe d tal que $ad = b$. Luego, $a(dc) = (ad)c = bc$ y en consecuencia, $a \mid bc$. Esto prueba la primera afirmación.

Para la segunda, por hipótesis existe d tal que $ad = b$ y un e tal que $be = c$. Entonces $c = be = (ad)e = a(de)$ y concluimos que $a \mid c$.

Por último, tenemos como hipótesis en el tercer enunciado existen d y e tales que $ad = b$ y $ae = c$. Luego

$$b + c = ad + ae = a(d + e),$$

con lo que concluimos que $a \mid b + c$. □

Ejercicio 1 (Gentile [1991])**.** Decidir si son verdaderos o falsos:

1. Si un número es divisible por 6 entonces es divisible por 3.
2. Si un número es divisible por 6 entonces no es divisible por 9
3. Si un número es par, su cuadrado es par.
4. Si el cuadrado de un número es par, el número es par.
5. $a \mid b + c$ implica $a \mid b$ ó $a \mid c$.
6. $ac \mid bc$ implica $a \mid b$.
7. $a \mid b^2$ implica $a \mid b$.
8. $a \mid a + b$ implica $a \mid b$.
9. $a^2 \mid b^2$ implica $a \mid b$.
10. $a^2 \mid b^3$ implica $a \mid b$.

Ahora enunciaremos un teorema tan conocido como útil:

Teorema 3 (Algoritmo de la división)**.** *Para todos $a \neq 0$ y b existen únicos q y r tales que*

$$b = qa + r \text{ con } 0 \leq r < |a|.$$

Decimos que q es el cociente *y r el* resto *de la división de b por a.*

Entonces, es equivalente decir que $a \mid b$ o que el resto de la división de b por a es 0.

Ejemplo 2. $14 = 4 \cdot 3 + 2$, luego 3 **no** divide a 14 por la unicidad del Algoritmo de la división. ¡Ojo! el resto de la división **nunca** es negativo, sean como sean los números a y b. El cociente de la división de -6 por 5 es -2 (¡no -1!) y el resto es 4.

1.2. mdc y mmc (ain't drugs, buddy).

Definición 4. d es el *máximo divisor común de a y b* (mdc) si $d > 0$, $d \mid a$, $d \mid b$ (es un divisor en común positivo) y cada vez que $c \mid a$ y $c \mid b$ se da $c \mid d$, para todo c. Escribiremos entonces "$d = (a; b)$". Si $(a; b) = 1$, diremos que a y b son *coprimos*. m es el *mínimo múltiplo común de a y b* (mmc) si $m > 0$, $a \mid m$, $b \mid m$ y cada vez que $a \mid c$ y $b \mid c$ se da $m \mid c$. Usamos la notación $[a; b]$ para el mínimo común múltiplo.

Nota 1. Las definiciones de mdc y mmc dadas más arriba son muy similares; en esencia son las mismas, nada más que se da vuelta la relación "$\ldots \mid \ldots$"; en otras palabras, son *duales*.

Ejemplo 3. El máximo divisor común entre 12 y 18 es $(12; 18) = 6$, pues $6 \mid 12$ y $6 \mid 18$, y todo otro divisor común, digamos, 3 ($3 \cdot 4 = 12$, $3 \cdot 6 = 18$), divide a 6. 18 y 25 son coprimos, $(18; 25) = 1$.

Ejercicio 2. Supongamos a, b y c positivos. Probar:

1. $(a; a + 1) = 1$.

2. Para todo k, $(a; ka + b) = (a; b)$. En particular, $(a; b + a) = (a; b - a) = (a; b)$.

3. $(a; b) = a$ si y sólo si $a \mid b$.

4. $(a; b) = [a; b]$ implica $a = b$.

5. *a)* (*) $(ca; cb) = c(a; b)$.
   b) $ab = (a; b)[a; b]$.
   c) $[(a; b); c] = ([a; c]; [b; c])$.

Nota 2. El requerimiento de a, b y c sean positivos no es esencial: los resultados siguen valiendo si tomamos valor absoluto en ambos miembros.

Sean ahora dos números a y b. Por el algoritmo de la división sabemos que existen q_1 y r_1 tales que $b = aq_1 + r_1$ y $0 \leq r_1 < |a|$. Ahora bien,

$$(a; b) = (a; q_1 a + r_1) = (a; r_1),$$

donde la última igualdad se da por el ejercicio 2. Si ahora hacemos la division entera de a por r_1, con cociente q_2 y resto r_2, tenemos igualmente

$$(a; b) = (a; r_1) = (r_1; a) = (r_1; r_1 q_2 + r_2) = (r_1; r_2),$$

con $0 \leq r_2 < r_1$. Si repetimos este proceso, obtendremos

$$(a; b) = (a; r_1) = (r_1; r_2) = (r_2; r_3) = \cdots, \text{ con}$$

$$r_1 > r_2 > r_3 > \cdots \geq 0$$

Eventualmente, para algún n, r_{n+1} es cero, i.e., r_n divide a r_{n-1}. Luego, por el ejercicio 2, $(a; b) = (r_{n-1}; r_n) = r_n$. Este proceso se denomina *Algoritmo de Euclides*.

Ejemplo 4. Hallemos $(324; 122)$.

$$\begin{aligned} \mathbf{324} &= \mathbf{122} \cdot 2 + 80; \\ 122 &= 80 \cdot 1 + 42; \\ 80 &= 42 \cdot 1 + 38; \\ 42 &= 38 \cdot 1 + 4; \\ 38 &= 4 \cdot 9 + 2; \\ 4 &= \mathbf{2} \cdot 2. \end{aligned}$$

Luego, $(324; 122) = 2$.

Teorema 5. *Para todos a, b existen r, s tales que $(a; b) = ra + sb$.*

Prueba. Se puede ver el resultado de dos modos.

Uno es tomar el Algoritmo de Euclides y hacerlo "marcha atrás". Sabemos que $(a; b)$ es igual a r_n. Ahora bien, $r_{n-2} = r_{n-1} q_n + r_n$, así que $r_n = r_{n-2} - r_{n-1} q_n$. Reemplazando aquí r_{n-1} por $r_{n-3} - r_{n-2} q_{n-1}$, obtenemos

$$(a; b) = r_n = r_{n-2} - r_{n-1} q_n = (-q_n) r_{n-3} + (1 - q_n q_{n-1}) r_{n-2}.$$

Retrocediendo de este modo podemos llegar a una expresión de $(a; b)$ como una *combinación lineal entera* de a y b.

Para la segunda prueba, sabemos que entre todos los números positivos de la forma $ra + sb$ existe uno mínimo $m = Ra + Sb$. Ahora bien, se puede ver que todos ellos son múltiplos de tal m. Pues si tomamos el resto β de dividir un $\alpha = r_0a + s_0b$, con r_0 y s_0 enteros, por m, tenemos

$$\beta = \alpha - qm = r_0a + s_0b - q(Ra + Sb) = (r_0 - qR)a + (s_0 - qS)b,$$

con $0 \leq \beta < m$. Por la minimalidad de m, tenemos $\beta = 0$ y en consecuencia $m \mid \alpha$. En particular, $m \mid a$ y $m \mid b$, y en consecuencia, $m \mid (a; b)$. Como además $(a; b)$ también divide a todos los números de la forma $ra + sb$, $(a; b) \mid m$. En conclusión, $m = (a; b)$. □

Nota 3. Claramente, la primera prueba es muy útil porque es constructiva, mientras que la segunda tiene una idea muy buena guardada: Todo subconjunto M de $\mathbb{Z}$ que cumpla que:

> Cada vez que $m, n \in M$, se tiene $m + n \in M$ y $m - n \in M$.

es exactamente el conjunto de múltiplos de un número (y, en particular, podemos elegir como este número al menor número positivo del conjunto). Queda la prueba como ejercicio.

Ejemplo 5. Retomamos el ejemplo anterior; como indica el teorema, retrocedemos cada paso del cálculo del mdc. Para ello, despejamos cada una de las relaciones:

$$2 = 38 - 4 \cdot 9 \tag{1}$$
$$4 = 42 - 38 \cdot 1 \tag{2}$$
$$38 = 80 - 42 \cdot 1 \tag{3}$$
$$42 = 122 - 80 \cdot 1 \tag{4}$$
$$80 = 324 - 122 \cdot 2. \tag{5}$$

Reemplazamos el 4 de la ecuación (1) por su expresión en (2) y, agrupando convenientemente, dejamos afuera el 42 y el 38:

$$2 = 38 - (\underline{42 - 38 \cdot 1}) \cdot 9 = 42 \cdot (-9) + 38 + 38 \cdot 9 = 42 \cdot (-9) + 38 \cdot 10.$$

Reemplazamos en esta última expresión el 38 usando la ecuación (3), y dejamos afuera el 80 y el 42:

$$2 = 42 \cdot (-9) + (\underline{80 - 42 \cdot 1}) \cdot 10 = 80 \cdot 10 + 42 \cdot (-19).$$

Reemplazamos el 42 esta vez, usando (4), sacamos el 122 y el 80:

$$2 = 80 \cdot 10 + (\underline{122 - 80 \cdot 1}) \cdot (-19) = 122 \cdot (-19) + 80 \cdot 29.$$

Y repetimos esto usando (5):

$$2 = 122 \cdot (-19) + (\underline{324 - 122 \cdot 2}) \cdot 29 = 324 \cdot 29 + 122 \cdot (-77)$$

con lo que $(324; 122) = 324 \cdot 29 + 122 \cdot (-77)$.

Ejercicio 3. Encontrar r y s tales que $234r + 128s = (234; 128)$.

Ejercicio 4. Intentar nuevamente el grupo de ejercicios 5 de la página 3.

Ejercicio 5. Suponga que dispone de un recipiente de 19 litros, otro de 3 litros y otro, más grande, de tamaño desconocido.

1. ¿Cómo haría para dejar 14 litros de agua en el recipiente grande?
2. Suponiendo que la capacidad del recipiente grande es un número entero de litros, explique un procedimiento para averiguarla.
3. ¿Como haría para dejar 14 litros en el de 19, suponiendo que no dispone del grande?

Ejercicio 6. (*) Si $a \mid bc$ y $(a; c) = 1$, entonces $a \mid b$.

1.3. Los hijos de los tíos.

Como se sospecha por el título, trabajaremos con los primos.

Definición 6. p es *primo* si y sólo si $p \neq 1$ y los únicos divisores positivos de p son 1 y $|p|$ (el valor absoluto de p). Llamaremos p_n al n-ésimo primo positivo. Por ejemplo, $p_1 = 2$, $p_2 = 3$, $p_5 = 11$, etcétera.

Teorema 7. *Todo número mayor que 1 es primo o divisible por algún primo.*

Prueba. La prueba es por inducción. Como la hipótesis habla de números mayores a 1, tomaremos como caso base a $n = 2$. El resultado vale para 2, pues se da la primera posibilidad (el teorema dice que se debe dar *alguna* de ellas). Supongamos el resultado válido para todos los $n < k$ y lo probemos para $n = k$. Si k es primo, ya está. Si no, tiene algún divisor positivo distinto de 1 y k, digamos d. Pero como $1 < d < k$, d cumple con la conclusión del teorema por hipóteis inductiva. Luego d es primo (y en consecuencia k tiene a d como divisor primo) o d tiene un divisor primo c. Ahora tenemos $c \mid d$ y $d \mid k$, y por el lema 2, $c \mid k$ y c es un divisor primo de k. Por el principio de inducción queda completa la prueba. □

Teorema 8 (Euclides)**.** *Existen infinitos primos positivos.*

Prueba. Tomemos los primeros N primos positivos $p_1, \ldots, p_N$. Luego, el número

$$Q := \prod_{i=1}^{N} p_i + 1 = p_1 \ldots p_N + 1$$

no es divisible por p_i con i entre 1 y N. Luego, por el teorema 7, tenemos que o bien Q es primo (mayor a todos los p_i y por ende distinto) o es divisible por un primo, que por la observación anterior debe ser también mayor que todos los p_i. Concluimos que hay más de N primos positivos, y como N era arbitrario, deducimos que hay infinitos primos. □

Nota 4. Falta decir arriba que existe *algún* primo positivo (¿por qué?).

Ejercicio 7. Si p es primo y no divide a a, entonces $(a; p) = 1$.

Proposición 9. *$p \neq 1$ es primo si y sólo si para todos a y b, se da*

$$p \mid ab \Rightarrow p \mid a \text{ ó } p \mid b.$$

Prueba. ($\Leftarrow$) Supongamos que p **no** es primo; luego existen c y d tales que $c, d < p$ y $p = cd$. Luego $p \mid cd$ pero no valen $p \mid c$ ni $p \mid d$.
($\Rightarrow$) Supongamos que $p \nmid a$. Luego, por el ejercicio 7 tenemos $(a; p) = 1$. Por el teorema 5, existen r y s tales que $ra + sp = 1$. Multiplicando ambos miembros por b, obtenemos $rab + sbp = b$. Como p divide al primer miembro, también divide al segundo, así que tenemos lo que queríamos ($\leftarrow$ ¡y esto es una prueba del ejercicio 6!). □

Teorema 10 (Fundamental de la Aritmética, TFA)**.** *Todo entero mayor que 1 se factoriza en primos positivos en forma única.*

Prueba. Primero debemos aclarar qué se quiere decir con que la factorización es *única*. La idea es que las siguientes factorizaciones del número 12, por ejemplo, sean las mismas:

$$2 \cdot 2 \cdot 3,\ 2 \cdot 3 \cdot 2,\ 3 \cdot 2 \cdot 2,$$

o sea, que aparezcan los mismos factores igual cantidad de veces. Por el teorema 7 y usando inducción puede verse que todo número puede expresarse como producto de primos. Probemos por inducción en la cantidad *mínima* de factores primos de n que la factorización es única. Así, supongamos que todos los números con una factorización en l factores primos o menos se factoriza de manera única y sea n con dos factorizaciones

$$n = p_1 \cdots p_{l+1} \text{ y } n = p'_1 \cdots p'_m.$$

Si $m \leq l$, listo. Si no, como p_{l+1} divide a $n = p'_1 \cdots p'_m$, debe dividir a alguno de los p'_i, digamos p'_r. Pero entonces $p_{l+1} = p'_r$ y podemos simplificar.

$$p_1 \cdots p_l = \frac{n}{p_{l+1}} = p'_1 \cdots p'_{r-1} p'_{r+1} \cdots p'_m.$$

Por hipótesis inductiva los p'_i $(i \neq r)$ son exactamente los p_i $(i \neq l+1)$ en algún orden, y multiplicando de nuevo por p_{l+1} obtenemos el resultado. □

Ejercicio 8. Probar que todo primo mayor a 3 se puede escribir de la forma $6k + 1$ o $6k + 5$. Demostrar que $\{3, 5, 7\}$ forman la única terna de *primos consecutivos* (i.e., cuya diferencia es 2).

1.4. No ser incongruente.

Definición 11. Diremos que *a es congruente a b módulo m* y escribimos "$a \equiv b \mod (m)$" si y sólo si $m \mid a - b$.

Lemaa 12. *Se cumplen las siguientes propiedades de la congruencia módulo:*

1. $a \equiv a \mod (m)$*;*
2. $a \equiv b \mod (m)$ *si y sólo si* $b \equiv a \mod (m)$*;*
3. $a \equiv b \mod (m)$ *y* $b \equiv c \mod (m)$ *implican* $a \equiv c \mod (m)$*;*

es decir, "... es congruente a ... módulo m" es una relación de equivalencia.

Prueba. Para la primera, por definición de congruencia módulo basta ver que $m|a-a=0$, pero como todo m divide a cero ($m \cdot 0 = 0$), el resultado es siempre válido.

Para la segunda, supongamos que $a \equiv b \mod (m)$, es decir, $m \,|\, a-b$. Pero esto último significa que existe algún k tal que $a-b=km$. Luego $b-a=-(a-b)=-km=(-k)m$, y tenemos que $m \mid b-a$. Por definición, obtenemos $b \equiv a \mod (m)$.

Dejamos la tercera como ejercicio. □

Lemaa 13. *Supongamos* $a \equiv b \mod (m)$ *y* $c \equiv d \mod (m)$. *Tenemos:*

1. $a+c \equiv b+d \mod (m)$, *y*
2. $ac \equiv bd \mod (m)$.

I.e., la congruencia módulo preserva las operaciones aritméticas.

Prueba. Probamos sólo la primera de ellas. Si $m \mid a-b$ y $m \mid c-d$, m divide a la suma de ambos números, esto es, $m \mid a-b+c-d$. Reordenando tenemos $m \mid a+c-(b+d)$, que era lo que queríamos probar. □

Ejercicio 9. Sean a, b y m como en el lema. Ver que para todo $c > 0$,

$$a^c \equiv b^c \mod (m)$$

(Ayuda: Inducción).

Ejemplo 6. Para ver la utilidad del uso de las congruencias módulo, calculemos cuál es la cifra de las unidades u del desarrollo decimal de 9999^{9999}. Sabemos que la cifra de las unidades de un número es su resto en la división por 10, así que $9999^{9999} \equiv u \mod (10)$. Pero $9999 \equiv -1 \mod (10)$ (pues $10 \mid 9999-(-1)=10000$), y luego $-1=(-1)^{9999} \equiv u \mod (10)$. Ahora, el único número entre 0 y 9 que sea congruente a -1 módulo 10 es 9, y en conclusión $u=9$.

Ejercicio 10. Probar las siguientes propiedades de la congruencia módulo.

1. Si $n \mid m$, se da $a \equiv b \mod (m) \Rightarrow a \equiv b \mod (n)$.
2. $ac \equiv bc \mod (m)$ y $(c;m)=1$ implica $a \equiv b \mod (m)$.
3. $a \equiv b \mod (m) \Rightarrow (a;m)=(b;m)$.

2. Recetario.

2.1. Reglas de divisibilidad.

Repasemos brevemente los criterios de divisibilidad más conocidos, y algunos no tanto. Todos son consecuencia directa de los resultados ya vistos.

Divisibilidad por potencias de 2 y de 5.

Fácilmente, para todo número n tenemos $n=10q+u$ con $0 \leq u \leq 9$ por el Algoritmo de la división. Como el primer sumando es divisible por 2 y por 5, tenemos que n es divisible por 2 o por 5 si y sólo si u (la cifra de las unidades de n) es divisible por ellos. En general, y con la misma prueba (tomando resto módulo 10^r) se demuestra que un número es divisible por 2^r ó 5^r si y sólo si el número formado por sus últimas r cifras lo es.

Divisibilidad por 7.

Un número n es múltiplo de 7 si y sólo si lo es el número formado por las cifras de n sin las unidades, restándole el doble de las unidades. Es decir, si $n = 10q + u$, $7 \mid n$ si y sólo si $7 \mid q - 2u$. Para verlo, tenemos

$$10q + u \equiv 0 \quad \text{mód } (7),$$

que es equivalente a

$$3q + u \equiv 0 \quad \text{mód } (7)$$

lo cual sucede si y sólo si

$$6q + 2u \equiv 2u - q \equiv 0 \quad \text{mód } (7)$$

(para la parte ($\Leftarrow$) uso que $(2; 7) = 1$). Por último, la última igualdad se da si y sólo si

$$q - 2u \equiv 0 \quad \text{mód } (7).$$

Ídem... por 3, 9 y 11.

¿Por qué funcionan los criterios de divisibilidad por dichos números? Vamos a ver el del 9. Sabemos que $10 \equiv 1 \mod (9)$. Luego, por el ejercicio 9, $10^n \equiv 1 \mod (9)$ para todo n. Ahora bien, si $\overline{d_n d_{n-1} \dots d_1}$ es un número de n cifras,

$$\overline{d_n d_{n-1} \dots d_1} = 10^n d_n + 10^{n-1} d_{n-1} + \dots + 10 d_2 + d_1 \equiv d_n + d_{n-1} + \dots + d_2 + d_1 \quad \text{mód } (9).$$

Luego, todo número es congruente a la suma de sus cifras, módulo 9 (y también vale módulo 3 por el ejercicio 10.1).

El criterio para 11 puede obtenerse fácilmente considerando que $10 \equiv -1 \mod (11)$ y, en consecuencia,

$$10^n \equiv 1 \quad \text{mód } (11) \text{ si } n \text{ es par, y } \; 10^n \equiv -1 \quad \text{mód } (11) \text{ si } n \text{ es impar.}$$

Ejercicio 11. Demostrar que $\overline{d_n d_{n-1} \dots d_1}$ es divisible por 13 si y sólo si $d_1 - 3d_2 - 4d_3 - d_4 + 3d_5 + 4d_6 + \dots$ lo es.

Ejercicio 12. Hallar un criterio semejante al anterior para 7 y para 17.

2.2. Testeo de restos.

Un método muy bueno para ver si una ecuación en $\mathbb{Z}$ tiene solución o no es fijarse en el comportamiento de dicha ecuación en las distintas congruencias.

Ejemplo 7. Demostrar que $3x^2 + 2 = y^2$ no admite soluciones enteras.

Basta fijarse que la misma ecuación *no tiene soluciones módulo 3*. ¿Por qué? Si X e Y cumplieran dicha ecuación, tendríamos

$$3 \cdot X^2 + 2 = Y^2,$$

e inmediatamente (por el lema 13 y el ejercicio 9),

$$3 \cdot X^2 + 2 \equiv 2 \equiv Y^2 \quad \text{mód } (3), \tag{6}$$

pues $3 \equiv 0 \mod (3)$. Pero un número arbitrario es congruente a 0, 1 ó 2 módulo 3, así que su cuadrado será congruente a 0, 1 o 4; como este último es congruente a 1, se deduce que todo cuadrado perfecto es congruente a 0 ó a 1 módulo 3. Pero esto contradice claramente la ecuación (6), así que por lo tanto no existe y tal que $3x^2 + 2 = y^2$.

En el razonamiento anterior se aprecia el uso de lo que se conoce por *residuo cuadrático*. Diremos que r es residuo cuadrático módulo m si y sólo si existe a tal que $r \equiv a^2 \mod (m)$. Podemos concluir que 0 y 1 son residuos cuadráticos módulo 3, y el 2 no.

Ejercicio 13. Encontrar los residuos cuadráticos módulo 4, 5, 7 y 8

En general, se puede hablar de un residuo r cúbico, cuártico, ..., módulo m si existe un a tal que $r \equiv a^3 \mod (m)$, $r \equiv a^4 \mod (m)$, ..., respectivamente.

2.3. Cantidad de cifras de un número entero.

Sabemos que un número entero n tiene c cifras si y sólo si $10^{c-1} \leq n < 10^c$. Por ejemplo, 34 (con 2 cifras) satisface $10^{2-1} = 10 \leq 34 < 100 = 10^2$. Luego, usando logaritmos podemos obtener la cantidad de cifras de número arbitrario. Supongamos

$$10^{c-1} \leq n < 10^c.$$

Si tomamos logaritmo en base 10 a cada miembro, obtenemos,

$$c - 1 = \log\left(10^{c-1}\right) \leq \log(n) < \log\left(10^c\right) = c,$$

es decir,

$$c - 1 \leq \log(n) < c,$$

donde $\log(\cdot)$ es el logaritmo decimal. Resumiendo, c es la parte entera de $\log(n)$ más 1, $\lfloor \log(n) \rfloor + 1$. Todo esto sirve de igual modo para cualquier base si reemplazamos cada "10" por la base en cuestión y el logaritmo decimal por el logaritmo en dicha base.

Podemos recordar las propiedades del logaritmo que serán muy útiles. Para todos a, b y c positivos,

- $\log_a(1) = 0$.
- $\log_a(a) = 1$.
- $\log_a(b) + \log_a(c) = \log_a(bc)$.
- $\log_a(b^c) = c \cdot \log_a(b)$.

Ejercicio 14.

1. ¿Cuantas cifras tiene $1234567^{1234567}$? (Se puede usar calculadora.)
2. Encontrar la cantidad de cifras de $16^{100000!}$ en base 2 (**no** se puede usar calculadora).

2.4. Forma factorizada de múltiplos y divisores.

Una vez que tenemos el teorema de factorización única en primos, podemos expresar a los múltiplos y divisores de un número cualquiera de una manera muy práctica. Para facilitar las cuentas, lo haremos para naturales exclusivamente. Supongamos que nuestro n es igual a

$$p_1^{e_1} p_2^{e_2} \cdots = \prod_{p_i} p_i^{e_i},$$

donde el producto corre sobre *todos* los primos (¿Cómo? Así, por ejemplo: 12 es igual a $2^2 \cdot 3^1$, pero también es igual a

$$2^2 \cdot 3^1 \cdot 5^0 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = \cdots .$$

Es decir, puedo poner tantos primos p_j como quiera mientras sus exponentes e_j sean nulos. Fin del paréntesis.) y supongamos que $d \mid n$. Luego, si la factorización de d es

$$p_1^{f_1} p_2^{f_2} \cdots = \prod_{p_i} p_i^{f_i},$$

debemos tener $f_i \leq e_i$ para todo i, pues como $p_i^{f_i}$ divide a n, tenemos que $p_i^{f_i}$ divide a $p_i^{e_i}$ y esto sólo es posible si $f_i \leq e_i$.

Un resultado inmediato (usando combinatoria y el **TFA**) es que el número total de divisores de n como arriba es

$$(e_1 + 1)(e_2 + 1) \cdots = \prod_i (e_i + 1).$$

Ejercicio 15. 1. ¿Cuántos divisores tiene 10! ?

2. Hallar los menores números con exactamente 3, 4, 5 y 8 divisores positivos.

3. Demostrar que un número positivo es un cuadrado perfecto si y sólo si tiene una cantidad impar de divisores positivos.

4. Llamemos $\tau(n)$ a la cantidad de divisores de n. Luego, el producto de los divisores positivos de n es $\sqrt{n^{\tau(n)}}$. En símbolos,

$$\prod_{d|n} d = \sqrt{n^{\tau(n)}}.$$

2.5. Expresión polinómica de números

Una de las herramientas básicas que tenemos en $\mathbb{Z}$ es que podemos expresar los números en forma bonita usando algunos trucos.

Aplicando el Algoritmo de la división para $a = 2$, sabemos que para cualquier número n existen q y r tales que $n = 2q + r$ con $0 \leq r < 2$. Pero esta última condición quiere decir que $r = 0$ ó $r = 1$, así que todo número puede ser escrito de la forma $2k$ ó $2k+1$ (¡y sólo una!) para algún k. Análogamente, todo número puede ser escrito de la forma $3k$, $3k+1$ ó $3k+2$ para algún k. También pueden probarse estas afirmaciones por inducción.

Ejercicio 16. Probar:

1. Todo número se escribe únicamente de la forma $3k - 1$, $3k$ ó $3k + 1$.

2. Todo número se puede escribir de la forma $2k$, $3k$, $6k + 1$ ó $6k - 1$.

Ejercicio 17. El producto de dos números consecutivos es par.

Las expresiones $2k+1$, $3k$ son ejemplos de *polinomios (lineales)* en la variable k. Resulta que muchos problemas, una vez planteados en forma algebraica, hablan de algún polinomio. Y muy frecuentemente, su solución involucra una *factorización* inteligente del mismo. Por ejemplo, al polinomio

$$p(x) := x^2 - 1$$

se lo puede pensar en la forma

$$p(x) := (x+1)(x-1),$$

usando distributividad. La utilidad de la segunda expresión es que está puesta en forma de producto, y como en Aritmética la noción más importante es la de divisibilidad, las descomposiciones en productos juegan un papel muy importante.

Ejemplo 8. Para ningún n, $2^n + 1$ es un cubo.

La expresión que aparece en este problema —$(2^n + 1)$— no es un polinomio, puesto que tiene una variable en el exponente. Pero pensando un poco más, el problema nos pide ver que dicha expresión nunca será un cubo perfecto. Por un momento supongamos que sí es el caso, que existe x tal que $2^n + 1 = x^3$. ¡Ahora sí tenemos un polinomio! Si pasamos ahora el 1 restando, la afirmación del problema es:

El polinomio $x^3 - 1$ nunca vale una potencia de 2.

Lo próximo es obvio luego de la introducción. Factorizamos el polinomio:

$$x^3 - 1 = (x-1)(x^2 + x + 1) \stackrel{?}{=} 2^n.$$

Pero $x^2+x+1 = x(x+1)+1$ y para todo x esto será impar por el ejercicio 17. Ahora bien, el único factor impar de 2^n es 1, así que $x^2 + x + 1 = 1$ y esto sólo sucede con $x = 0, -1$. Sin embargo, para estos valores, $x^3 - 1$ es negativa, así que no puede ser potencia de dos.

Terminanos con un resultado muy útil cuando llega la hora de factorizar polinomios de grado mayor que 2.

Proposición 14. *Sean a_i, $i = 0, \ldots, n$ enteros. Si c es una raíz del polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ (es decir, si $p(c) = 0$) entonces $c \mid a_0$.*

Sabemos que en tal caso (haciendo la división de polinomios) existe un polinomio $q(x)$ (con coeficientes no necesariamente enteros) tal que $p(x) = (x-c)q(x)$.

Demostración. Como $p(c) = 0$, podemos escribir:

$$-a_0 = a_1 c + \cdots + a_n c^n,$$

luego de pasar a_0 restando. Ahora bien, el lado derecho es divisible por c, así que también debe serlo el lado izquierdo. □

Ejercicio 18. Sea p como antes. Si $p(\frac{r}{s}) = 0$ con $(r; s) = 1$, entonces $r \mid a_0$ y $s \mid a_n$.

Ejercicio 19. Probar que

$$\sqrt[3]{2 + \frac{10}{9}\sqrt{3}} + \sqrt[3]{2 - \frac{10}{9}\sqrt{3}}$$

es un entero.

3. ¡A cocinar!

Aquí sigue un *pot-pourri* (¿un guiso?) de problemas para entretenerse. Están ordenados cronológicamente, por número de envío y por nivel (en ese orden de prioridad). El número romano corresponde al "año OMA", y el número de tres cifras siguiente indica el nivel (las centenas) y el número de envío (el resto). Por ende, los problemas con "resto" más alto son más difíciles.

XII-228 Hallar el menor entero positivo n tal que el número

$$N = 100000 \cdot 100002 \cdot 100006 \cdot 100008 + n$$

sea un cuadrado perfecto.

XII-328 ¿Para qué valores enteros de x es $x^4 + 6x^3 + 11x^2 + 3x + 31$ un cuadrado perfecto?

XIII-107 Con los dígitos del 1 al 9 inclusive se forman tres números A, B y C de tres dígitos distintos cada uno, usándose los nueve dígitos. ¿Se puede lograr que ninguno sea múltiplo de 3?

XIII-207 Hallar todos los números de 3 dígitos tales que al elevarlos al cuadrado tienen las tres últimas cifras iguales y en el mismo orden que el número original.

XIII-216 Hallar el menor múltiplo de 999, mayor que 999 que tiene todos sus dígitos impares.

XIII-220 Determinar todos los enteros x tales que $x^2 - 19x + 96$ sea un cuadrado perfecto.

XIII-223 ¿Es posible escribir los 11 números desde 1985 a 1995 en algún orden de modo que el número de 44 cifras que se obtiene sea primo?

XIII-307 Hallar el resto de dividir $\overbrace{11\ldots1}^{1995}$ por 1001.

XIII-310 ¿Para cuántos enteros n la fracción $\frac{n^2-3}{n^2-1}$ es reducible?

XIII-323 Para cada entero positivo n sea $p(n)$ el número de pares ordenados (x, y) de enteros positivos tales que $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$. Ejemplo: $p(2) = 3$.

1. Determinar $p(n)$ para todo n y calcular $p(1995)$.

2. Determinar todos los n tales que $p(n) = 3$.

XIII-325 Hallar el menor número natural que es suma de 9 naturales consecutivos, es suma de 10 naturales consecutivos y además es suma de 11 naturales consecutivos.

XV-107 La Asociación Vida Silvestre de Saladillo tiene 50 miembros. El sábado cada uno de los presentes plantó 17 árboles y el domingo cada uno de los presentes plantó 20 árboles. En total se plantaron 1545 árboles. ¿Cuántos de los miembros de la Asociación faltaron el sábado y cuántos faltaron el domingo?.

XV-124 Hallar todos los cuadrados perfectos que tienen el primer dígito (de la izquierda) igual a 1 y todos los restantes dígitos iguales a 4.

XV-204 Hallar todos los números naturales $n < 1000$ tales que n^2 termina en 44.

XV-210 Sea $p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots$ el producto de todos los números primos hasta 1997 y $q = 3 \cdot 5 \cdot 7 \cdot 11 \cdots$ el producto de todos los números impares hasta 1997. Hallar la penúltima cifra de la derecha del producto pq.

XV-217 Hallar números naturales tales que

$$\frac{97}{19} = 5 + \cfrac{1}{x + \cfrac{1}{y + \cfrac{1}{z}}}.$$

XV-221 Demostrar que para todos a, b el número $c = a^3b - ab^3$ es múltiplo de 6.

XV-227 Si a, b y c son números enteros tales que $ab-(a+b) = 19$ y $bc-(b+c) = 97$, hallar todos los posibles valores de $ca - (c + a)$.

XV-230 Sea n un número natural con cuatro o más divisores naturales [distintos]. De todos los divisores de n, se consideran los cuatro más pequeños: $a < b < c < d$. Hallar todos los n tales que

$$n = a^2 + b^2 + c^2 + d^2.$$

ACLARACIÓN: 1 es el divisor positivo más pequeño de n.

XV-305 ¿Cuántos números enteros entre 1 y 1000 inclusive pueden descomponerse en suma de un múltiplo positivo de 7 más un múltiplo positivo de 4?

XV-317 Hallar todos los números naturales n tales que $\left[\frac{n^2}{5}\right]$ es primo.

XV-322 Hallar el último dígito antes de la cola de ceros del número

$$19! + 20! + 21! + \cdots + 96! + 97!$$

XV-326 Sea p un primo, $p = 3k + 2$ para un valor entero k. Demostrar que si p divide a $a^2 + ab + b^2$ para ciertos enteros a y b, entonces p divide a a y p divide a b.

XVI-106 De los 999 números:

$$\text{mdc(1;1998), mdc(2;1998), mdc(3;1998), } \ldots \text{, mdc(999,1998),}$$

¿cuántos son mayores que 19?

XVI-107 Hay cinco montones de piedras. Se quita $\frac{1}{5}$ de las piedras del primer montón y se agregan al segundo montón. Luego se quita $\frac{1}{5}$ de las piedras que hay ahora en el segundo montón y se agregan al tercer montón. A continuación, se quita $\frac{1}{5}$ de las piedras que hay ahora en el tercer montón y se agregan al cuarto montón. Finalmente, se quita $\frac{1}{5}$ de las piedras que hay ahora en el cuarto montón y se agregan al quinto montón. De este modo todos los montones finalizan con 124 piedras cada uno. ¿Cuántas piedras había inicialmente en cada montón?

XVI-301 Hallar todos los números enteros n tales que $\frac{n+98}{n+19}$ es un número entero.

Cuenca 1995 – 2 Sea $a_1, \ldots, a_n$ una sucesión de enteros entre 2 y 1995 tal que

1. cada par de elementos a_i son coprimos.

2. cada a_i es primo o es producto de primos distintos.

Determinar el menor valor posible de n para que la sucesión contenga necesariamente por lo menos un número primo.

Sel-IberoXXI Un número natural n es atrevido si la suma de las cifras de 3^n es mayor o igual que la suma de las cifras de 3^{n+1} (ejemplos: 2 y 11). Demostrar que hay infinitos números atrevidos.

Referencias

[1991] E. Gentile: "Aritmética Elemental en la Formación Matemática". *Ed. OEA*.

[1979] G.H. Hardy, E.M. Wright: "An Introduction to the Theory of Numbers". Quinta edición. *Oxford Sci. Publ.*

[1965] N. Jacobson: "Lectures in Abstract Algebra". Vol **1**, pp. 114–120. *D. Van Nostrand, Inc.*