Seminario de problemas. Curso 2018–19

Estrategias matemáticas: congruencias

Objetivo.
Dado un entero positivo m, hacer operaciones cuando solamente nos interesa el resto del resultado al ser dividido por m.

En ese sentido, en cualquier suma $a+b$ se podrá cambiar a por $a+m$ o por $a-m$ ya que, por ejemplo, $a+b$ y $(a+m)+b$ dan el mismo resto al ser divididos por m. Algo similar ocurre con las diferencias $a-b$ y en los producto $a\cdot b$ donde también le podremos sumar/restas múltiplos de m a a o a b. Así pues, para cualquier $k\in\mathbb{Z}$, podemos cambiar a por $a-km$ en las operaciones $a\pm b$ y $a\cdot b$ anteriores (lo mismo sirve para b). A este cambio lo llamaremos *reducción* (módulo m). El algoritmo de la división asegura que cualquier entero a puede reducirse módulo m hasta un único $r\in\{0,1,\dots,m-1\}$, su resto al ser dividido entre m.

Ejemplo.
¿Cuál es el resto de dividir 2018^{10} entre 3?

Una potencia es un producto múltiple, así que como $2018=2+673\cdot 3$, en $2018^{10}=(2+673\cdot 3)\cdots(2+673\cdot 3)$ podemos reducir módulo 3 cada uno de los factores quedándonos 2^{10}. Como $2^{10}=(2^2)^5=4^5$, reduciendo el 4 módulo 3 llegamos a que 2018^{10} se reduce a 1 módulo 3. Por tanto, el resto de dividir 2018^{10} entre 3 es 1.

El que a y b den el mismo resto al ser divididos por m lo representaremos por

$$a\equiv b \pmod{m}$$

y diremos que a es *congruente* con b módulo m.

Ten siempre en cuenta...

$a\equiv b \pmod{m}$ también es lo mismo que decir que m divide a $b-a$.

Así, en el ejemplo anterior podíamos haber escrito

$$2018^{10}\equiv(2+673\cdot 3)\cdots(2+673\cdot 3)\equiv 2^{10}\equiv 4^5\equiv 1^5\equiv 1 \pmod{3},$$

y sería una solución clara y correcta.

Criterios de divisibilidad.

Conocer las potencias de 10 *módulo* m *es muy útil ya que los enteros positivos los escribimos en base* 10*:*

$$c_d 10^d + \cdots + c_1 10 + c_0.$$

- **Criterio de divisibilidad por** 3: para saber el resto que da un número al ser dividido entre 3 basta observar que $10 \equiv 1 \pmod 3$, así

$$c_d 10^d + \cdots + c_1 10 + c_0 \equiv c_d + \cdots + c_1 + c_0 \pmod 3$$

  Es decir, cualquier número da el mismo resto al ser dividido entre 3 que el que da la suma de sus cifras decimales. Por ejemplo, $2018 \equiv 2 + 1 + 8 \equiv 2 \pmod 3$.

- **Criterio de divisibilidad por** 9: análogo al anterior.

- **Criterio de divisibilidad por** 4: en este caso las potencias de 10 módulo 4 son: $10 \equiv 2, 10^2 \equiv 0, 10^3 \equiv 0, \ldots \pmod 4$. Así

$$c_d 10^d + \cdots + c_1 10 + c_0 \equiv c_1 10 + c_0 \pmod 4$$

  y el criterio nos diría que un número es divisible por 4 si y solamente si lo es el número formado por sus dos últimas cifras.

- **Criterio de divisibilidad por** 11: en este caso las potencias de 10 módulo 11 son $10 \equiv -1, 10^2 \equiv 1, 10^3 \equiv -1, \ldots \pmod{11}$. Así

$$c_d 10^d + \cdots + c_1 10 + c_0 \equiv c_0 - c_1 + c_2 - c_3 + \cdots + (-1)^d c_d \pmod{11}$$

  y el criterio nos diría que un número es divisible por 11 si y solamente si al sumar las cifras en posición par y restarle las de posición impar se obtiene un múltiplo de 11.

Reducción del exponente en potencias modulares.

Si queremos calcular el resto de dividir a^n *entre* m*, lo mejor que nos puede pasar es que conozcamos algún exponente pequeño* d *tal que* $a^d \equiv 1 \pmod m$.

En efecto, en tal caso dividiremos n entre d, $n = cd + e$ con $0 \leq e < |d|$ y

$$a^n \equiv a^{cd+e} \equiv (a^d)^c a^e \equiv 1^c a^e \equiv a^e \pmod m.$$

Ejemplo.

¿Cuál es el resto de dividir 1492^{1969} *entre* 13*?*

Reducimos la base, $1492 \equiv 114 \cdot 13 + 10 \equiv 10 \pmod{13}$, y examinamos las potencias de 10 módulo 13 en busca de alguna relación: $10^1 \equiv 10$, $10^2 \equiv (-3)^2 \equiv 9$, $10^3 \equiv 9 \cdot 10 \equiv 9 \cdot (-3) \equiv -27 \equiv -1 \pmod{13}$, por lo que $10^6 \equiv 1 \pmod{13}$. Puesto

que $1969 = 328 \cdot 6 + 1$,

$$1492^{1969} \equiv 10^{1969} \equiv (10^6)^{328} \cdot 10 \equiv 10 \pmod{13}.$$

Sorprendentemente, a veces podemos encontrar, sin apenas hacer cálculos, exponentes d tales que $a^d \equiv 1 \pmod{m}$. Eso sí, necesitaremos que a sea primo con m. Consideramos todos los números $\{a_1, \ldots, a_d\}$ entre 1 y $m-1$ primos con m y dividimos cada $a \cdot a_i$ entre m obteniendo $a \cdot a_i = c_i \cdot m + r_i$. Ahora:

- Los números r_i son primos con m. En efecto, como a y a_i son primos con m, también así r_i.
- Los números $\{r_1, \ldots, r_d\}$ son distintos entre sí. En efecto, si $r_i = r_j$ con $i \neq j$ entonces m divide a $(c_i \cdot m + r_i) - (c_j \cdot m + r_j) = aa_i - aa_j = a(a_i - a_j)$, y por tanto m divide a $a_i - a_j$, pues a es primo con m. Sin embargo esto no es posible ya que $-(m-1) < a_i - a_j < m - 1$ y $a_i - a_j \neq 0$.

Así pues, $\{r_1, \ldots, r_d\} = \{a_1, \ldots a_d\}$ ya que el primer conjunto está contenido en el segundo y ambos tienen el mismo número de elementos. Usando esto obtenemos que $a_1 \cdots a_d \equiv r_1 \cdots r_d \equiv (aa_1) \cdots (aa_d) \equiv a^d a_1 \cdots a_d \pmod{m}$ y por tanto que m divide a $(a^d - 1)a_1 \ldots a_r$. Como $a_1 \cdots a_r$ es primo con m concluimos que m divide a $a^d - 1$, es decir,

$$a^d \equiv 1 \pmod{m}.$$

La cantidad d de enteros entre 1 y m primos con m se denota por $\phi(m)$ (*función indicatriz de Euler*).

Teorema de Euler-Fermat.
Si a es primo con m entonces $a^{\phi(m)} \equiv 1 \pmod{m}$.

En el ejemplo anterior, como 10 es primo con 13, sin hacer ninguna operación sabríamos que $10^{12} \equiv 1 \pmod{13}$. Puesto que $1969 = 164 \cdot 12 + 1$, al igual que en ejemplo obtenemos que $10^{12} \equiv 1 \pmod{13}$.

Al mínimo exponente positivo d que cumple que $a^d \equiv 1 \pmod{m}$ lo llamamos *orden multiplicativo* de a módulo m y lo denotamos por $o(a)$. Si $a^n \equiv 1 \pmod{m}$ entonces, dividiendo n entre $o(a)$, $n = c \cdot o(a) + r$ nos dice que $a^r \equiv 1 \pmod{m}$ con $0 \leq r < o(a)$. Por la minimalidad de $o(a)$, $r = 0$ y $o(a)$ divide a cualquier exponente n tal que $a^n \equiv 1 \pmod{m}$.

Orden multiplicativo y su relación con la indicatriz de Euler.
Sea a un entero primo con m. Se tiene que $a^d \equiv 1 \pmod{m}$ si y solo si $o(a)$ divide a d. En particular $o(a)$ divide a $\phi(m)$.

Hay una fórmula sencilla para calcular la indicatriz de Euler. Si $m = p_1^{e_1} \cdots p_r^{e_r}$ con $p_1, \ldots, p_r$ primos distintos y $e_1, \ldots, e_r \geq 1$ entonces

$$\phi(m) = (p_1 - 1)p_1^{e_1 - 1} \cdots (p_r - 1)p_r^{e_r - 1}.$$

El -1 es especial para primos congruentes con 3 módulo 4.

Si p es un número primo congruente con 3 módulo 4 entonces no existe x tal que $x^2 \equiv -1 \pmod{p}$.

En efecto, un tal x tendría, módulo p, orden multiplicativo 4 y por lo tanto 4 dividiría a $\phi(p) = p - 1$. Sin embargo, $p - 1 \equiv 2 \pmod{4}$.

Antes de seguir conviene aprovechar un poco más que si p es primo entonces $\phi(p) = p - 1$.

Curiosidades módulo un primo p ...

- *(Pequeño Teorema de Fermat) Si p no divide a a entonces $a^{p-1} \equiv 1 \pmod{p}$.*
- *Para cualquier entero a se tiene que $a^p \equiv a \pmod{p}$.*
- *Para cualesquiera enteros a, b se tiene que $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

Es interesante observar que a y b tienen los mismos divisores comunes que b y $a - kb$ para cualquier k.

Reducir para calcular el máximo común divisor.

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a - kb).$$

Este tipo de manipulaciones puede venir bien en problemas.

Ejemplo (Problems for the mathematical olympiads, A. Negut).

Sean x, y enteros positivos tales que $3x^2 + x = 4y^2 + y$. Prueba que $x - y$ es un cuadrado perfecto.

Simplemente escribimos la relación como $3x^2 - 3y^2 + x - y = y^2$ y, factorizando, tenemos $(x - y)(3x + 3y + 1) = y^2$. Ahora vamos a fijarnos en el máximo común divisor de los factores: $d = \mathrm{mcd}(x - y, 3x + 3y + 1) = \mathrm{mcd}(x - y, 6y + 1)$. Así que d divide a $6y + 1$ pero también, por la relación, a y^2. Concluimos que $d = 1$. Al ser primos entre sí $x - y$ y $3x + 3y + 1$ y tener como producto un cuadrado, ambos son cuadrados.

Estas manipulaciones ayudan a calcular fácilmente el máximo común divisor (*Algoritmo euclídeo*). Por ejemplo, para calcular $\mathrm{mcd}(61, 24)$ observamos que

$$\underline{61} = 2 \cdot \underline{24} + 13, \quad \underline{24} = 1 \cdot \underline{13} + 11, \quad \underline{13} = 1 \cdot \underline{11} + 2, \quad \underline{11} = 5 \cdot \underline{2} + 1, \quad 2 = 2 \cdot 1 + 0$$

y así

$$\mathrm{mcd}(61, 24) = \mathrm{mcd}(24, 13) = \mathrm{mcd}(13, 11) = \mathrm{mcd}(11, 2) = \mathrm{mcd}(2, 1) = \mathrm{mcd}(1, 0) = 1.$$

De los cálculos también vemos, por sustitución regresiva, que

$$1 = 1 \cdot \underline{11} - 5 \cdot \underline{2} = 1 \cdot \underline{11} - 5(\underline{13} - 1 \cdot \underline{11}) = -5 \cdot \underline{13} + 6 \cdot \underline{11} = -5 \cdot \underline{13} + 6(\underline{24} - 1 \cdot \underline{13})$$
$$= -11 \cdot \underline{13} + 6 \cdot \underline{24} = -11(\underline{61} - 2 \cdot \underline{24}) + 6 \cdot \underline{24} = -11 \cdot \underline{61} + 28 \cdot \underline{24}.$$

Identidad de Bézout.

Dados enteros a, b, siendo al menos uno de ellos no nulo, existen enteros s, t tales que

$$\mathrm{mcd}(a, b) = s \cdot \underline{a} + t \cdot \underline{b}.$$

La Identidad de Bézout es útil para calcular *inversos modulares*.

Inversos modulares.

Si a es primo con $m \geq 2$ siempre existe $1 \leq a' \leq m-1$ tal que $a'a \equiv 1 \pmod{m}$. Un tal número a' se puede calcular a partir del s en la Identidad de Bézout $s\underline{a}+t\underline{m} = 1$.

Esto viene muy bien para encontrar un x que cumpla un conjunto de ecuaciones del tipo

$$\left.\begin{array}{rcl} x & \equiv & a_1 \pmod{n_1} \\ x & \equiv & a_2 \pmod{n_2} \\ & \vdots & \\ x & \equiv & a_k \pmod{n_k} \end{array}\right\} \quad (*)$$

cuando $n_1, \ldots, n_k$ son primos entre sí dos a dos. La idea es primero calcular la Identidad de Bézout $s_i \frac{n_1 \cdots n_k}{n_i} + t_i n_i = 1$ y después...

Teorema chino de los restos.

Las soluciones de $(*)$ son $x_0 +$ múltiplos de $n_1 \cdots n_k$ donde

$$x_0 = a_1 s_1 \frac{n_1 \cdots n_k}{n_1} + \cdots + a_k s_k \frac{n_1 \cdots n_k}{n_k}.$$

Los inversos modulares permiten hacer más cómodas algunas cuentas. Por ejemplo, dado un número n, lo escribimos como $n = 10n' + d_0$ donde d_0 es la cifra de las unidades. Para saber si n es divisible por 13 observamos que como $10 \cdot 4 \equiv 1 \pmod{13}$ entonces $n \equiv 0 \pmod{13}$ equivale a decir que $10n' + d_0 \equiv 0 \pmod{13}$ y, multiplicando por el inverso modular de 10, esto último equivale a $n' + 4d_0 \equiv 0$. Por ejemplo, para saber si 26234 es múltiplo de 13 calculamos los números $2639, 299, 65, 26$ y vemos que como 26 es múltiplo de 13, también así 2639.

El inverso modular de a es único (si lo tomamos en $\{1, \ldots, m-1\}$) debido a que $aa' \equiv 1, aa'' \equiv 1 \pmod{m}$ implica que $a'' \equiv (aa')a'' \equiv a'(aa'') \equiv a' \pmod{m}$, por lo que $a' = a''$. También es claro que si a' es el inverso modular de a entonces a lo será de a'. Cuando multipliquemos entre sí módulo m todos los elementos en $\{1, \ldots, m-1\}$ primos con m, cada uno desaparecerá con su inverso modular, a no ser que él mismo sea su propio inverso modular (piensa en $m - 1 \equiv -1 \pmod{m}$).

De hecho, dado p primo, los únicos a que son sus propios inversos modulares son los que cumplen que $a^2 \equiv 1 \pmod{p}$, es decir, p divide a $(a+1)(a-1)$. Como $1 \leq a \leq p-1$ esto implica que o bien $a = 1$ o bien $a = p-1$. Por tanto hemos demostrado el siguiente resultado:

Teorema de Wilson.
Sea p un número primo. Se tiene que $(p-1)! \equiv -1 \pmod{p}$.

Ejemplo (American Regions Mathematics League, 2002).
Sae a el entero tal que $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{22} + \frac{1}{23} = \frac{a}{23!}$. Calcular el resto de dividir a entre 13.

Multiplicando por 23! obtenemos $a = 23! + \frac{23!}{2} + \frac{23!}{3} + \cdots + \frac{23!}{22} + \frac{23!}{23}$. Módulo 13 todos estos sumandos son nulos excepto $\frac{23!}{13}$ que es congruente con $12! \cdot 10!$ módulo 13. Usando el Teorema de Wilson y observando que el inverso modular de $11 \equiv -2 \pmod{13}$ es $-7 \equiv 6 \pmod{13}$ mientras que el de 12 es -1, el resto de dividir a entre 13 es congruente con -6 módulo 13. Por tanto ese resto es 7.

Ten siempre en cuenta...
Las igualdades entre números enteros deben mantenerse módulo cualquier m. Esto permite algunas veces deducir que ciertas igualdades no son posibles.

Algunos problemas acerca de números enteros requieren de esta observación.

Ejemplo (Rusia, 1997).
Encuentra las parejas de primos p, q tales que $p^3 - q^5 = (p+q)^2$

En este caso tenemos mezcladas diferentes potencias, pero lo primero que sí que es claro es que $p > q$. Vamos a reducir usando algún módulo pequeño, por ejemplo 3, a ver qué pasa. Inicialmente obviamos el caso en que $p = 3$ o $q = 3$. Usando el Pequeño Teorema de Fermat tenemos que $p - q \equiv (p+q)^2 \pmod{3}$. Así, si $p \equiv q \pmod{3}$ entonces $0 \equiv q^2 \not\equiv 0 \pmod{3}$, lo que no es posible. Por tanto $p \not\equiv q \pmod{3}$. Pero en este caso $(p+q)^2 \equiv 0 \pmod{3}$ mientras que $p - q \not\equiv 0 \pmod{3}$, lo que nuevamente no es posible. Así que no queda más remedio que o bien $p = 3$ o bien $q = 3$. Como $3^3 - 2^5 < 0$, la única posibilidad es $q = 3$. En este caso $p^3 - 243 = p^2 + 6p + 9$ implica que p divide a 252, por lo que solamente puede ser $p = 7$.

Cuando aparezcan cuadrados o sumas de cuadrados conviene tener en cuenta que, módulo m, puede no haber muchos cuadrados.

Restos cuadráticos...

- Los cuadrados módulo 3 son solamente 0 y 1.
- Los cuadrados módulo 4 son solamente 0 y 1.
- La suma de dos cuadrado módulo 4 nunca es 3.
- Los cuadrados módulo 8 son solamente 0, 1 y 4.
- ... muchas otras observaciones de este tipo que se te ocurran.

Problemas bastante complicados pueden abordarse con esta sencilla observación.

Ejemplo (Korea, 1997).

Encuentra todos los enteros x, y, z que cumplen $x^2 + y^2 + z^2 - 2xyz = 0$.

La ecuación es

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

Si x, y, z son impares entonces el lado derecho sería impar pero el izquierdo sería par, así que al menos uno de los enteros x, y, z es par, y por lo tanto $2xyz$ es múltiplo de 4. Puesto que los cuadrados módulo 4 son 0 y 1, la ecuación obliga a que x, y, z sean pares.

Escribamos $x = 2x_1$, $y = 2y_1$, $z = 2z_1$. La ecuación queda $16x_1y_1z_1 = 4(x_1^2 + y_1^2 + z_1^2)$, y simplificando,

$$4x_1y_1z_1 = x_1^2 + y_1^2 + z_1^2.$$

En este punto nos damos cuenta de que podemos repetir el razonamiento anterior, y que así $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$ para ciertos x_2, y_2, z_2. Reiterando el mismo argumento con estos x_2, y_2, z_2 y con los sucesivos que obtengamos, al final llegamos a que x, y, z son divisibles por infinitas potencias de 2. Esto solo lo cumplen $x = 0, y = 0, z = 0$.

Otros problemas relativos a ecuaciones con números enteros (*ecuaciones diofánticas*) se basan en pícaras factorizaciones.

Ejemplo (Olimpiada matemática de Polonia).

Encuentra las soluciones enteras de la siguiente ecuación

$$x^2(y-1) + y^2(x-1) = 1.$$

Realizamos el cambio $x = u+1$, $y = v+1$ de modo que la ecuación se transforma en $(u+1)^2v + (v+1)^2u = 1$ y en el lado izquierdo ya no hay término independiente. Es decir, $u^2v + 2uv + v + v^2u + 2uv + u = 1$. Si uv fuese -1 entonces el lado izquierdo valdría -4, por lo que si le sumamos 4 podremos factorizarlo mediante el factor $uv + 1$. Es decir, $5 = u^2v + 4uv + v^2u + u + v + 4 = (uv + 1)(u + v + 4)$. Ahora el problema e mucho más sencillo ya que uno de los factores debe ser ± 1 y el otro

± 5. Por tanto hay cuatro posibles sistemas de ecuaciones:

$$\left.\begin{array}{rcl} u+v &=& 1 \\ uv &=& 0 \end{array}\right\}, \quad \left.\begin{array}{rcl} u+v &=& -9 \\ uv &=& 2 \end{array}\right\}, \quad \left.\begin{array}{rcl} u+v &=& -3 \\ uv &=& 4 \end{array}\right\}, \quad \left.\begin{array}{rcl} u+v &=& -5 \\ uv &=& -6 \end{array}\right\}.$$

Las soluciones para (u, v) son $(0, 1), (1, 0), (-6, 1), (1, -6)$, por lo que las soluciones para (x, y) son las parejas $(1, 2), (-5, 2), (2, 1), (2, -5)$.

Problemas más complicados requieren entender mejor qué potencias de un número primo pueden dividir a otros números.

Dado p un número primo sea $v_p(a)$ el mayor exponente v tal que p^v divide al entero a. Por ejemplo $v_2(40) = 3$ ya que $40 = 2^3 \cdot 5$. También sería cierto que $v_5(40) = 1$ y que $v_7(40) = 0$.

Dado un primo p que divide a $x - y$ pero que no divide ni a x ni a y vamos a intentar encontrar qué potencia de p divide a $x^n - y^n$. Inicialmente asumimos que p es primo con n. Recordamos que

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}).$$

Como p divide a $x - y$ entonces $x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} \equiv nx^{n-1} \not\equiv 0 \pmod{p}$ ya que n y x son primos con p. Así que en este caso $v_p(x^n - y^n) = v_p(x - y)$. Ahora abordamos el caso en que p divide a n. Escribimos $n = p^e N$ con N primo con p, así $v_p(x^n - y^n) = v_p((x^{p^e})^N - (y^{p^e})^N) = v_p(x^{p^e} - y^{p^e})$ debido al caso inicial que hemos desarrollado. Ahora escribimos $x = y + Kp^v$ con $v \geq 1$ y observamos que

$$\begin{aligned} x^p - y^p = (y + Kp^v)^p - y^p &= \binom{p}{1} y^{p-1} K p^v + \binom{p}{2} y^{p-2} (Kp^v)^2 + \cdots + \binom{p}{p} (Kp^v)^p \\ &= p^{v+1} \left(y^{p-1} K + \binom{p}{2} y^{p-2} K^2 p^{v-1} + \cdots + \binom{p}{p} K^p p^{pv-v-1} \right), \end{aligned}$$

de donde, si $p \neq 2$, la máxima potencia de p que lo divide es p^{v+1} ya que p divide a todos los sumandos del paréntesis excepto al primero. Esto nos dice que $v_p(x^p - y^p) = v_p(x - y) + 1$. Reiterando llegamos a que

$$v_p(x^n - y^n) = v_p(x^{p^e} - y^{p^e}) = v_p(x^{p^{e-1}} - y^{p^{e-1}}) + 1 = \cdots = v_p(x - y) + v_p(n).$$

Lema LTE (Lifting The Exponent).

Sea p un número primo y sean $v_p(a)$ el mayor exponente v tal que p^v divide a a, n un entero positivo y a, b enteros no divisibles por p:

- Si p divide a $a - b$ pero p no divide a n entonces $v_p(a^n - b^n) = v_p(a - b)$.
- Si $p \neq 2$ y p divide a $a - b$ entonces $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$.
- Si $p = 2$ divide a $a - b$ y también divide a n entonces $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$.
- Si $p = 2$ y 4 divide a $a - b$ entonces $v_2(a^n - b^n) = v_2(a - b) + v_2(n)$.

Como consecuencia, también es cierto:

- Si n es impar, no es divisible por p pero p divide a $a+b$ entonces $v_p(a^n+b^n) = v_p(a+b)$.
- Si n es impar $p \neq 2$ y p divide a $a+b$ entonces $v_p(a^n+b^n) = v_p(a+b)+v_p(n)$.

Ejemplo (T. Shin).

Calcula el menor entero positivo n_1 tal que $n = n_1^2$ cumpla que $7^n \equiv 1 \pmod{6^9}$.

Aquí el problema es que las potencias modulares módulo 6^9 son complicadas de calcular a mano. Usamos otra estrategia. Decir que $7^n \equiv 1 \pmod{6^9}$ es lo mismo que decir que $7^n \equiv 1 \pmod{2^9}$ y $7^n \equiv 1 \pmod{3^9}$. Usamos el LTE para hacernos una idea. Para $p = 3$, $9 \leq v_3(7^n - 1^n) = v_3(7-1)+v_3(n) = 1+2v_3(n_1)$. Así pues, el mínimo exponente de 3 en n_1 es 4. También observamos que n no puede ser impar ya que $7^n \equiv 1 \pmod{2^9}$ implica que el orden multiplicativo de 7 divide a n y a $\phi(2^9) = 2^8$, por lo que n es par. Así $9 \leq v_2(7^n-1^n) = v_2(7-1)+v_2(7+1)+v_2(n)-1 = 1+3+2v_2(n_1)-1$ implica que el mínimo exponente de 2 en n_1 es 3. Por tanto, el mínimo n_1 posible es $n_1 = 2^3 3^4 = 648$.

Ejemplo (Rusia, 1996).

Encuentra todos los enteros positivos n para los cuales existen enteros positivos x, y, k tales que $\text{mcd}(x, y) = 1$, $k > 1$ *y* $3^n = x^k + y^k$.

Es sorprendente la cantidad de información que puede proporcionar el LTE en esta situación. Primero observamos que, por supuesto, $x + y$ es impar o de lo contrario $x^k + y^k$ sería par. También es cierto que k es impar (basta examinar la ecuación en módulo 3). Ahora nos preguntamos por sus divisores primos. Sea p primo impar divisor de $x + y$ (esto implica que no puede dividir ni a x ni a y ya que $\text{mcd}(x, y) = 1$). Tenemos que $v_p(3^n) = v_p(x + y) + v_p(k)$. Por tanto, si $p \neq 3$ entonces p no divide ni a $x+y$ ni a k, es decir, $x+y = 3^m$, $k = 3^e$ para ciertos m, e con $e \geq 1$ y $n = m + e$. Esto nos lleva a

$$(x + y)3^e = 3^n = x^{3^e} + y^{3^e}.$$

Inmediatamente vemos que esta relación no es muy natural ya que el lado de la derecha tenderá a ser mucho mayor que el de la izquierda. Así que el problema pasa a ser un problema de acotaciones. Si lo piensas con cuidado verás que las únicas soluciones para (x, y, e) son $(1, 2, 1)$ y $(2, 1, 1)$, las cuales se corresponden con las soluciones $(1, 2, 3)$ y $(2, 1, 3)$ para (x, y, k).

Referencias

1. J. Stevens: *Olympiad Number Theory Through Challenging Problems.*
2. T. Andreescu, D. Andrica, I. Cucurezeanu: *An Introduction to Diophantine Equatiosn. A problem-based approach.* Birkhäuser, 2010.