3.3. Teorema chino de los restos

Teorema 3.3. *Sean m_1, m_2,..., m_k enteros coprimos dos a dos. Entonces el sistema de congruencias*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots \quad \cdots \quad \cdots\cdots\cdots \\ x &\equiv a_n \pmod{m_k} \end{aligned}$$

tiene una solución única módulo $m_1 m_2 \cdots m_k$.

Demostración. Sea $m = m_1 m_2 \cdots m_k$. Para cada $i = 1, 2, \ldots, k$ sea $M_i = m/m_i$. Entonces $\text{mcd}(M_i, m_i) = 1$ y por lo tanto existe x_i tal que de $M_i x_i \equiv 1 \pmod{m_i}$. Sea

$$x = M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_k x_k a_k.$$

Es inmediato verificar que x es solución del sistema de congruencias. Si x' es cualquier otra solución, entonces $x' \equiv x \pmod{m_i}$ para $i = 1, 2, \ldots, k$ y como los m_i son coprimos dos a dos se deduce que $x' \equiv x \pmod{m}$. □

Este teorema permite reducir la solución de ecuaciones polinómicas en congruencias de un módulo m cualquiera al caso en que el módulo sea una potencia de un primo. En efecto, si $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ es la descomposición en factores primos de m, la congruencia $P(x) \equiv 0 \pmod{m}$ es equivalente al sistema

$$\begin{aligned} P(x) &\equiv 0 \pmod{p_1^{a_1}}, \\ P(x) &\equiv 0 \pmod{p_2^{a_2}}, \\ &\cdots \quad \cdots \quad \cdots\cdots\cdots \\ P(x) &\equiv 0 \pmod{p_k^{a_k}}. \end{aligned}$$

En efecto, sea $P(x)$ un polinomio con coeficientes enteros. Si $P(x) \equiv 0 \pmod{m}$ tiene solución, evidentemente esa solución satisface también todas las congruencias del sistema. Recíprocamente, si x_i es una solución de la congruencia $P(x) \equiv 0 \pmod{p_i^{a_i}}$, entonces por el teorema chino de los restos existe un x tal que $x \equiv x_i \pmod{p_i^{a_i}}$ para $i = 1, 2, \ldots, k$, y por lo tanto $P(x) \equiv P(x_i) \equiv 0 \pmod{p_i^{a_i}}$ para $i = 1, 2, \ldots, k$ y $P(x) \equiv 0 \pmod{m}$.

3.4. Teoremas de Fermat, Euler y Wilson

Función ϕ de Euler

Si n es un número natural se define $\phi(n)$ como la cantidad de números del conjunto $\{1, 2, \ldots, n\}$ que son coprimos con n. Por ejemplo $\phi(6) = 2$ ya que de los números 1, 2, 3, 4, 5 y 6 solamente 1 y 5 son coprimos con 6.

La función ϕ es multiplicativa, es decir que:

Teorema 3.4. *Si a y b son números naturales coprimos, entonces*

$$\phi(ab) = \phi(a)\phi(b).$$

Demostración. Cada natural desde 1 hasta ab se puede escribir en la forma $qa+r$, con $0 \leq q \leq b-1$ y $1 \leq r \leq a$. Para que $qa+r$ sea coprimo con ab, debe serlo con a y con b. Pero $\text{mcd}(qa+r, a) = \text{mcd}(r, a)$, luego r debe ser coprimo con a. Hay $\phi(a)$ de estos r. Para cada uno de ellos los números r, $a+r$, $2a+r$,..., $(b-1)a+r$ son un sistema completo de residuos módulo b, ya que la diferencia de dos de ellos (diferentes) es de la forma ja, con $1 \leq j \leq b-1$, y por lo tanto no es divisible entre b. Esto significa que $\phi(b)$ de ellos son coprimos con b, y por lo tanto con ab. Esto nos da un total de $\phi(a)\phi(b)$ números coprimos con ab, entre los naturales desde 1 hasta ab. □

Si p es primo y a natural entonces los números entre 1 y p^a que no son coprimos con p^a son p, $2p$, $3p$,..., $p^{a-1}p = p^a$, que son p^{a-1}. Luego

$$\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p).$$

Usando este resultado y el hecho de que ϕ es multiplicativa, resulta que si $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ entonces

$$\begin{aligned}\phi(n) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})\cdots(p_k^{a_k} - p_k^{a_k-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Teorema 3.5 (Teorema de Euler).

Si $\text{mcd}(a, n) = 1$ entonces

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}.}$$

Demostración. Sean c_1, c_2,..., $c_{\phi(n)}$ los elementos de $\{1, 2, \ldots, n\}$ que son coprimos con n y pongamos $ac_i = q_i n + r_i$, para $i = 1, \ldots, \phi(n)$, con $0 \leq r_i < n$. Es claro que los restos r_i son todos diferentes, ya que $r_i = r_j \Longrightarrow ac_i = ac_j \pmod{n}$ $\Longrightarrow c_i = c_j \pmod{n}$ (por ser a coprimo con n), absurdo. Además $\text{mcd}(r_i, n) = \text{mcd}(ac_i - q_i n, n) = \text{mcd}(ac_i, n) = 1$. Se concluye que

$$\{c_1, c_2, \ldots, c_{\phi(n)}\} = \{r_1, r_2, \ldots, r_{\phi(n)}\}.$$

Pero $r_i \equiv ac_i \pmod{n}$, por lo tanto

$$c_1 c_2 \cdots c_{\phi(n)} = r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} c_1 c_2 \cdots c_{\phi(n)} \pmod{n},$$

de donde resulta $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Un caso particular importante se presenta cuando n es primo. Observe que si p es primo entonces $\phi(p) = p-1$, por lo tanto se tiene:

Teorema 3.6 (Teorema (pequeño) de Fermat). *Si p es primo y $p \nmid a$, entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Otro resultado interesante es el siguiente:

Teorema 3.7 (Teorema de Wilson). *Para cualquier primo p se cumple*

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración. Cada entero i desde 1 hasta $p-1$ tiene un (único) inverso multiplicativo en el mismo rango. Si $x^2 \equiv 1 \pmod{p}$ entonces $(x+1)(x-1) \equiv 0 \pmod{p}$, de donde los únicos que son inversos de sí mismos son 1 y $p-1$. Es decir que los enteros 2, 3,..., $p-2$ se agrupan en parejas de inversos multiplicativos y por lo tanto

$$(p-1)! \equiv 1 \cdot (p-1) \cdot 2 \cdot 3 \cdots (p-2) \equiv -1 \pmod{p}.$$

□

3.5. Lema de Hensel

El *Lema de Hensel*, también conocido como *Lema de Mihail* o *Lema de levantamiento de exponentes*, es una herramienta muy çutil para resolver problemas olímpicos de teoría de números, especialmente aquellos relacionados con congruencias.

Primero algo de notación: si p es un número primo, a y n son enteros y $n \geq 0$, escribiremos

$$p^n \parallel a$$

para indicar que $p^n \mid a$ pero $p^{n+1} \nmid a$. En otras palabras, $p^n \parallel a$ si y sólo si p^n es la mayor potencia de p que divide a a. Ejemplos: $3 \parallel 30$, $2^3 \parallel 72$, $5^4 \parallel 10000$.

Teorema 3.8. *Sean p un primo impar, a, b, n, r y s enteros, $n, r \geq 1$. Si $p^r \parallel a-b$, $p \nmid b$ y $p^s \parallel n$, entonces $p^{r+s} \parallel a^n - b^n$.*

Demostración. Primero probaremos que $p^s \parallel \frac{a^n-b^n}{a-b}$ por inducción en s. Para $s = 0$ se tiene que $p \nmid n$. Como $a \equiv b \pmod{p}$ resulta $a^j \equiv b^j \pmod{p}$ y $a^j b^{n-j-1} \equiv b^{n-1} \pmod{p}$, y sumando se tiene

$$\frac{a^n - b^n}{a-b} = \sum_{j=0}^{n-1} a^j b^{n-j-1} \equiv nb^{n-1} \not\equiv 0 \pmod{p}.$$

Supongamos ahora que $p^s \parallel \frac{a^n-b^n}{a-b}$. Pongamos $a = b + xp$. Entonces $a^{nj} \equiv b^{nj} + njb^{n(j-1)}xp \pmod{p^2}$ y se tiene

$$\begin{aligned}\frac{a^{np}-b^{np}}{a^n-b^n} &= \sum_{j=0}^{p-1} a^{nj}b^{n(p-j-1)} \equiv \sum_{j=0}^{p-1}(b^{nj}+njb^{n(j-1)}xp)b^{n(p-j-1)} \\ &\equiv pb^{n(p-1)} + pnxb^{n(p-2)}\sum_{j=0}^{p-1} j \\ &\equiv pb^{n(p-1)} + pnxb^{n(p-2)}\frac{p(p-1)}{2} \\ &\equiv pb^{n(p-1)} \pmod{p^2}.\end{aligned}$$

Por lo tanto

$$p^{s+1} \parallel \frac{a^{np}-b^{np}}{a^n-b^n}\frac{a^n-b^n}{a-b} = \frac{a^{np}-b^{np}}{a-b},$$

completando la inducción.

Finalmente, como $a^n - b^n = \frac{a^n-b^n}{a-b}(a-b)$ es claro que $p^{r+s} \parallel a^n - b^n$. □

Corolario 3.9. *Sean p un primo impar, a, b, n, r y s enteros, $n, r \geq 1$ y n impar. Si $p^r \parallel a+b$, $p \nmid b$ y $p^s \parallel n$, entonces $p^{r+s} \parallel a^n + b^n$.*

Demostración. Basta observar que si n es impar entonces $a + b = a - (-b)$ y $a^n + b^n = a^n - (-b)^n$. □

Para $p = 2$ el lema de Hensel como lo hemos enunciado no es cierto, por ejemplo $2 \parallel 3 - 1$ y $2 \parallel 2$, pero $2^3 \parallel 3^2 - 1^2$. Sin embargo vale un resultado similar:

Teorema 3.10. *Sean a, b, n, r y s enteros, $n, r, s \geq 1$. Si $2^r \parallel \frac{a^2-b^2}{2}$, $2 \nmid b$ y $2^s \parallel n$, entonces $2^{r+s} \parallel a^n - b^n$.*

Demostración. Primero probaremos que $2^{s-1} \parallel \frac{a^n-b^n}{a^2-b^2}$ por inducción en $s \geq 1$. Para $s = 1$ se tiene que $n = 2m$, con m impar. Como $2 \mid \frac{a^2-b^2}{2}$ debe ser $a \equiv b \pmod 2$, de donde $a^{2j} \equiv b^{2j} \pmod 2$ y $a^{2j}b^{2m-2j-1} \equiv b^{2m-1} \pmod 2$, y sumando se obtiene

$$\frac{a^{2m}-b^{2m}}{a^2-b^2} = \sum_{j=0}^{m-1} a^{2j}b^{2m-2j-1} \equiv mb^{2m-1} \equiv 1 \pmod 2,$$

o sea que $2^0 \parallel \frac{a^n-b^n}{a^2-b^2}$. Supongamos ahora que $p^{s-1} \parallel \frac{a^n-b^n}{a^2-b^2}$. Como a y b son impares y n es par se tiene $a^n \equiv b^n \equiv 1 \pmod 4$ y por tanto $a^n + b^n \equiv 2 \pmod 4$, es decir que $2 \parallel a^n + b^n$. Entonces

$$p^s \parallel \frac{a^n-b^n}{a^2-b^2}(a^n+b^n) = \frac{a^{2n}-b^{2n}}{a^2-b^2},$$

completando la inducción.

Finalmente, como $a^n - b^n = 2\frac{a^n-b^n}{a^2-b^2}\frac{a^2-b^2}{2}$ es claro que $p^{r+s} \parallel a^n - b^n$. □

3.6. Problemas

Problema 3.1. Un número se escribe con cien ceros, cien unos y cien doses, en algún orden. ¿Puede ser un cuadrado perfecto?

Problema 3.2. Pedro multiplicó dos enteros de dos cifras cada uno y codificó los factores y el producto con letras, usando letras iguales para dígitos iguales y letras diferentes para dígitos diferentes. Entonces le mostró al maestro su trabajo: $AB \cdot CD = EEFF$. Pero el maestro le contestó: Revisa lo que hiciste, pues cometiste un error. ¿Cómo supo eso el maestro?

Problema 3.3. Permutando las cifras del número

$$122333444455555666666777777777$$

¿podrá obtenerse un cuadrado perfecto?

Problema 3.4. Determine todos los valores de k para los cuales el número $111\ldots1$, compuesto por k unos, es un cuadrado perfecto.

Problema 3.5. ¿Alguno de los números que se pueden obtener permutando las cifras de 86420 es un cuadrado perfecto?

Problema 3.6. Halle todos los enteros positivos n tales que $n! + 5$ sea un cubo perfecto.

Problema 3.7. Si m y n son enteros tales que $m^2 + n^2$ es múltiplo de 3, pruebe que tanto m como n son múltiplos de 3.

Problema 3.8. Hallar el menor entero positivo x tal que $21x \equiv 2 \pmod{37}$.

Problema 3.9. Si x, y, z son enteros tales que $x^2 + y^2 = z^2$, pruebe que al menos uno de ellos es múltiplo de 3.

Problema 3.10. Si tres números primos mayores que 3 están en progresión aritmética, pruebe que la razón (o diferencia común) de la progresión es múltiplo de 6.

Problema 3.11. Se tienen 7 números enteros tales que la suma de 6 cualesquiera de ellos es divisible entre 5. Pruebe que los 7 números son múltiplos de 5.

Problema 3.12. Resuelva el sistema de congruencias

$$\begin{aligned} 2x &\equiv 3 \pmod{5}, \\ 3x &\equiv 5 \pmod{7}, \\ 5x &\equiv 7 \pmod{11}. \end{aligned}$$

Problema 3.13. Si x, y, z son enteros tales que $x^2+y^2+z^2$ es múltiplo de 4, pruebe que tanto x, y, z son los tres pares.

Problema 3.14. (OMCC 2014/6) Un entero positivo n es *divertido* si para todo d divisor positivo de n, $d+2$ es un número primo. Encuentre todos los números divertidos que tengan la mayor cantidad posible de divisores.

Problema 3.15. Pruebe que $2222^{5555}+5555^{2222}$ es divisible entre 7.

Problema 3.16. Determine el valor de d si el número

$$\underbrace{888\cdots888}_{50\ 8's}d\underbrace{999\cdots999}_{50\ 9's}$$

es divisible entre 7.

Problema 3.17. ¿Qué resto se obtiene al dividir $2^{3^{2011}}$ entre 17?

Problema 3.18. Pruebe que para todo natural n se cumple $\sum_{d|n}\phi(d)=n$.

Problema 3.19. ¿Cuál es la cifra de las unidades de $\underbrace{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}_{2015\ 7's}$?

Problema 3.20. Halle las tres últimas cifras de $2003^{2002^{2001}}$.

Problema 3.21. Pruebe que existe n tal que 3^n tiene al menos 2011 ceros consecutivos.

Problema 3.22 (IMO 2005/4). Considere la sucesión a_1, a_1,... definida por

$$a_n=2^n+3^n+6^n-1$$

para todos los n enteros positivos. Halle todos los enteros positivos que son coprimos con todos los términos de la sucesión.

Problema 3.23. Pruebe que, dado cualquier natural N, existe n tal que 2^n tiene al menos N ceros consecutivos.

Problema 3.24. (IMO 2009/1) Sea n un entero positivo y sean a_1, a_2,..., a_k ($k\geq 2$) enteros distintos del conjunto $\{1,2,\ldots,n\}$ tales que n divide a $a_i(a_{i+1}-1)$ para $i=1,2,\ldots,k-1$. Demostrar que n no divide a $a_k(a_1-1)$.

Problema 3.25. Halle el menor entero positivo n tal que $2^{2007}\mid 17^n-1$.

Problema 3.26. (Rusia 1996) Supongamos que $a^n+b^n=p^k$, donde a, b, y k son enteros positivos, p es un primo iompar y $n>1$ es un entero impar. Pruebe que n debe ser una potencia de p.

Problema 3.27. (IMO 1990/3) Halle todos los enteros positivos n tales que $\frac{2^n+1}{n^2}$ es entero.

Problema 3.28. (ORP 2004, 2N P2) Encontrar todos los valores enteros positivos de k, n y p primo que satisfacen la ecuación $5^k - 3^n = p^2$.

Problema 3.29. (OMCC 2001/3) Encontrar todos los números naturales N que cumplan las dos condiciones siguientes:

- Sólo dos de los dígitos de N son distintos de 0 y uno de ellos es 3.
- N es un cuadrado perfecto.

Problema 3.30. (IMO 2000/5) ¿Existe un entero positivo n que tenga esactamente 2000 divisores primos y que divida a $2^n + 1$?

Problema 3.31. (IMO 2003/6) Sea p un número primo. Demostrar que existe un primo q tal que, para todo entero n, el número $n^p - p$ no es divisible por q.