Congruencias

Ingeniería informática Curso: Álgebra

Fernando Chamizo https://matematicas.uam.es/~fernando.chamizo/

Comentarios

Nos centraremos en los restos en las divisiones inexactas y veremos que en gran medida se pueden operar como si fueran números enteros. Es una abstracción y generalización de la manera en que contabilizamos las horas sin superar nunca doce en el reloj. Esta aritmética de restos permite abordar problemas de divisibilidad aparentemente complicados.

1. El anillo de clases de congruencias

Dado $m \in \mathbb{N}$ definimos la relación de equivalencia $\mathcal{R}$ en $\mathbb{Z}$

$$a\mathcal{R}b \iff m \mid a-b.$$

Es un ejercicio rutinario comprobar que realmente es relación de equivalencia. Tras el teorema de la división, escribiendo $a = mq + r$ y $b = mq + r'$, se tiene la definición alternativa

$$a\mathcal{R}b \iff a \text{ y } b \text{ dejan el mismo resto al ser divididos por } m.$$

La notación habitual para expresar la relación entre dos enteros a y b es

$$a \equiv b \pmod{m} \qquad \text{a veces abreviado como} \qquad a \equiv b \quad (m)$$

y se dice que a y b son *congruentes módulo* m. En otras palabras, una *congruencia*, indicada con $\equiv$, es una igualdad entre restos cuando se divide por un número llamado *módulo*. Como al dividir por m hay m posibles restos, el conjunto cociente $\mathbb{Z}/\mathcal{R}$ consta de m clases, concretamente de $\overline{0}$, $\overline{1}$, $\overline{2}$,..., $\overline{m-1}$. Este conjunto cociente se denota mediante $\mathbb{Z}_m$ o mediante $\mathbb{Z}/m\mathbb{Z}$. En resumen, las congruencias o las clases de $\mathbb{Z}_m$ son maneras equivalentes de expresar condiciones de divisibilidad pues

$$m \mid a-b \iff a \equiv b \pmod{m} \iff \overline{a} = \overline{b} \quad \text{en} \quad \mathbb{Z}_m.$$

Así, $n \equiv 0$ (2) y $\overline{n} = \overline{0}$ en $\mathbb{Z}_2$ son dos formas de indicar que n es par.

Ejemplo. Describir los elementos de $\mathbb{Z}_3$.

Según lo dicho, $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ donde $\overline{0}$, $\overline{1}$ y $\overline{2}$ son, respectivamente, los enteros que dejan resto 0, 1 y 2 al dividir por 3. Una descripción explícita e implícita sencilla de estas clases es:

$$\begin{aligned}
\overline{0} &= \{0, 3, 6, 9, \dots\} \cup \{-3, -6, -9, \dots\} = \{3n : n \in \mathbb{Z}\},\\
\overline{1} &= \{1, 4, 7, 10, \dots\} \cup \{-2, -5, -8, \dots\} = \{3n+1 : n \in \mathbb{Z}\},\\
\overline{2} &= \{2, 5, 8, 11, \dots\} \cup \{-1, -4, -7, \dots\} = \{3n+2 : n \in \mathbb{Z}\}.
\end{aligned}$$

Por supuesto, las clases dan lugar a una partición de $\mathbb{Z}$, en particular, son disjuntas.

Si $a_1 \equiv b_1\ (m)$ y $a_2 \equiv b_2\ (m)$, entonces $a_j = mc_j + r_j$ y $b_j = mc'_j + r_j$ (los restos coinciden), por tanto, $a_1 + a_2 - (b_1 + b_2) = m(c_1 + c_2 - c'_1 - c'_2)$, que es múltiplo de m. Con ello hemos probado que las congruencias se pueden sumar:

$$a_1 \equiv b_1 \pmod{m} \quad \wedge \quad a_2 \equiv b_2 \pmod{m} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

Un argumento similar (ejercicio) muestra que también se pueden restar y multiplicar. Entonces en $\mathbb{Z}_m$ podemos sumar, restar y multiplicar clases con las reglas:

$$\overline{a} \pm \overline{b} \text{ definido como } \overline{a \pm b} \qquad \text{y} \qquad \overline{a} \cdot \overline{b} \text{ definido como } \overline{ab}$$

(el punto del producto se suele omitir). Estas operaciones entre clases, que son conjuntos de enteros, tienen las mismas propiedades que la suma, resta y multiplicación habituales. Sin entrar en detalles, en álgebra abstracta cuando se dispone de estas operaciones y comparten las propiedades de las habituales se dice que se tiene un *anillo* (para ser más precisos, habría que añadir *conmutativo con unidad*). Así, es justo referirse a $\mathbb{Z}_m$ como el anillo de clases de congruencia.

Ejemplo. Escribir las tablas de la suma y de la multiplicación en $\mathbb{Z}_3$.

Representemos las clases como $\overline{0}$, $\overline{1}$, $\overline{2}$ y cuando nos salga $\overline{n}$ con $n \notin \{0, 1, 2\}$ lo sustituiremos por su resto al dividir por 3.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Por ejemplo, la extraña igualdad $\overline{1} + \overline{2} = \overline{0}$ solo significa que al sumar un número de la forma $3n + 1$ con otro de la forma $3n + 2$ obtenemos siempre un múltiplo de 3.

Dentro de nuestra experiencia cotidiana, la aritmética con la que sumamos las horas de un reloj es la de $\mathbb{Z}_{12}$. Por ejemplo, $\overline{5} + \overline{11} = \overline{4}$ en $\mathbb{Z}_{12}$ refleja que 5 horas después de las 11 son las 4.

El hecho de que $\mathbb{Z}_m$ tenga m elementos y estructura de anillo compatible con la de $\mathbb{Z}$ permite reducir algunos problemas de divisibilidad a un número finito de cálculos.

Ejemplo. Demostrar que para todo $n \in \mathbb{Z}$ se tiene que $n^4 - 4n^3 + 13n^2 - 18n + 20$ es divisible por 4 y determinar para qué valores de n es divisible por 3.

Podemos reducir cada coeficiente módulo 4 para obtener

$$n^4 - 4n^3 + 13n^2 - 18n + 20 \equiv P(n) \pmod 4 \qquad \text{con} \quad P(n) = n^4 + n^2 + 2n.$$

Trabajando en $\mathbb{Z}_4$ se tiene $P(\overline{0}) = P(\overline{1}) = P(\overline{2}) = P(\overline{3}) = \overline{0}$. Como se anula en todas las clases, siempre es divisible por 4. Por otro lado, módulo 3

$$n^4 - 4n^3 + 13n^2 - 18n + 20 \equiv Q(n) \pmod 3 \qquad \text{con} \quad Q(n) = n^4 - n^3 + n^2 - 1.$$

En $\mathbb{Z}_3$, $Q(\overline{0}) = \overline{-1}$, $Q(\overline{1}) = \overline{0}$ y $Q(\overline{2}) = Q(\overline{-1}) = \overline{2}$. Por tanto, es divisible por 3 si y solo si $n \in \overline{1}$, esto es, si y solo si n es de la forma $3\ell + 1$.

Las reducciones a P y Q no son estrictamente necesarias, su único propósito es operar con números más pequeños.

Ejemplo. Demostrar que para todo $n \in \mathbb{Z}$ el resto de $8n^3 - 3n^2 + 7n + 11$ al dividir por 6 es siempre 5.

El enunciado se traduce en

$$8n^3 - 3n^2 + 7n + 11 \equiv 5 \pmod 6.$$

Pasando todo a un miembro y reduciendo los coeficientes módulo 6 equivale a $P(n) \equiv 0$ (6) con $P(n) = 2n^3 - 3n^2 + n$. Comprobando $P(\overline{0}) = P(\overline{1}) = \cdots = P(\overline{5}) = \overline{0}$ en $\mathbb{Z}_6$ se termina la demostración. Una forma alternativa y truculenta de proceder, que evita las evaluaciones anteriores, es factorizar $P(n) = n(n-1)(2n-1)$. Siempre es par porque $n(n-1)$ es producto de dos números consecutivos y es divisible por 3 porque cada clase de $\mathbb{Z}_3$ anula un factor.

Una aplicación de las congruencias, hoy en día casi lúdica, es un tratamiento generalizado de las *reglas de divisibilidad* en términos de las cifras. Dado $n \in \mathbb{N}$ llamemos c_0 a la cifra de las unidades, c_1 a la de las decenas, c_2 a la de las centenas, etc. Se tiene

$$n = 10^k c_k + 10^{k-1} c_{k-1} + \cdots + 10c_1 + c_0.$$

Como $\overline{10} = \overline{1}$ en $\mathbb{Z}_3$, se deduce $\overline{n} = \overline{c_k + \cdots + c_1 + c_0}$. En particular, se deduce la conocida regla de que un número es divisible por 3 si y solo si la suma de sus cifras lo es. El procedimiento se puede aplicar sucesivamente y en el caso de no divisibilidad da el resto. Por ejemplo, el número $n = 73499875$ cumple $\overline{n} = \overline{52} = \overline{5+2}$. Entonces el resto al dividir n por 3 es el mismo que el de 7, que es 1.

La misma regla se aplica para la divisibilidad por 9 porque $\overline{10}$ también es $\overline{1}$ en $\mathbb{Z}_9$. Por cierto, esta regla es la base de la llamada *regla del nueve* que sabían todos los escolares cuando las calculadoras no eran tan comunes como ahora.

Por el teorema fundamental de la aritmética, las reglas de divisibilidad tienen interés para primos y potencias de primos (por ejemplo, un número es divisible por 12 si y solo si lo es por 2^2 y por 3). Con esta restricción, quizá conozcas las reglas para 2, 3, 4, 5, 8, 9 y 11. El resto de los casos responden a un marco teórico similar, pero se vuelven complicadas para hacer cálculos mentales, por ello no son tan conocidas.

Ejemplo. Crear una regla de divisibilidad por 37 en términos de las cifras.

Se tiene $\overline{10}^1 = \overline{10}$, $\overline{10}^2 = \overline{26} = \overline{-11}$ (pasamos a negativos solo para que salgan números menores) y $\overline{10}^3 = \overline{1}$ en $\mathbb{Z}_{37}$, por tanto, $\overline{10}^{3j+1} = \overline{10}$, $\overline{10}^{3j+2} = \overline{-11}$ y $\overline{10}^{3j} = \overline{1}$. Con la notación anterior:

$$\overline{n} = \overline{c_0 + 10c_1 - 11c_2 + c_3 + 10c_4 - 11c_5 + \dots}$$

Es decir, si agrupamos las cifras de n de tres en tres (completando con ceros a la izquierda si es necesario), n será divisible por 37 si y solo si la suma de los final de cada grupo más 10 veces la suma de los de en medio, menos 11 veces la de los primeros es divisible por 37. Por ejemplo, al aplicar esta regla a $n = 98172285$ hacemos la subdivisión $|098|172|285|$ y se deduce

$$n \equiv 5 + 2 + 8 + 10(8 + 7 + 9) - 11(2 + 1 + 0) \pmod{37}.$$

Al operar el segundo miembro se obtiene 222. Si no está claro que este número es divisible por 37, aplicamos de nuevo el procedimiento para obtener $2 + 10 \cdot 2 - 11 \cdot 2 = 0$.

2. Ecuaciones con congruencias

Una pregunta algebraica natural es si, además de sumar, restar y multiplicar, se puede dividir en $\mathbb{Z}_m$. Para dividir entre $\overline{a}$ esta clase debe tener un *inverso* (multiplicativo) módulo m. Es decir, la ecuación $\overline{a}\,\overline{x} = \overline{1}$ debe tener solución en $\mathbb{Z}_m$ que llamaremos $\overline{a}^{-1}$. En términos de divisibilidad significa que m divide a $1 - ax$ y el problema se traduce en que $ax + my = 1$ debe tener solución $x, y \in \mathbb{Z}$. Con lo que sabemos de las ecuaciones diofánticas lineales, concluimos

$$\overline{a} \text{ invertible } \mathbb{Z}_m \iff \overline{a}\,\overline{x} = \overline{1} \text{ tiene solución en } \mathbb{Z}_m \iff \operatorname{mcd}(a, m) = 1.$$

La primera equivalencia es simple notación. Además, según lo anterior, podemos calcular el inverso $\overline{a}^{-1} = \overline{x}$ hallando una solución $ax + my = 1$ con el algoritmo de Euclides. Cuando m es pequeño, es más rápido buscar tal solución "a ojo". El subconjunto de elementos de $\mathbb{Z}_m$ con inverso lo denotaremos mediante $\mathbb{Z}_m^*$. Con símbolos:

$$\mathbb{Z}_m^* = \left\{\overline{n} \in \mathbb{Z}_m \,:\, \exists \overline{n}^{-1}\right\} = \left\{\overline{n} \in \mathbb{Z}_m \,:\, \operatorname{mcd}(n, m) = 1\right\}.$$

Claramente $\overline{0} \notin \mathbb{Z}_m^*$ excepto en el caso tonto $m = 1$ en el que solo hay una clase y $\overline{0} = \overline{1}$.

Ejemplo. Describir explícitamente $\mathbb{Z}_{12}^*$ y hallar el inverso de sus elementos.

Sabemos que $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \ldots, \overline{11}\}$. Eliminando de esta lista los que tienen factores comunes con 12 se sigue $\mathbb{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Este conjunto contiene también a los inversos de sus elementos porque $(\overline{n}^{-1})^{-1} = \overline{n}$. Comprobando los productos de dos elementos hasta obtener $\overline{1}$ se consiguen las igualdades:

$$\overline{1} = \overline{1} \cdot \overline{1} = \overline{5} \cdot \overline{5} = \overline{7} \cdot \overline{7} = \overline{11} \cdot \overline{11}.$$

Es decir, cada elemento de $\mathbb{Z}_{12}^*$ es su propio inverso.

Comentario. Se puede probar que esta peculiaridad de que cada elemento coincida con su inverso ocurre en $\mathbb{Z}_m^*$ si y solo si m divide a 24, es decir, para $m \in \{1, 2, 3, 4, 6, 8, 12, 24\}$.

Veamos un ejemplo en el que no hay casualidades ni cálculos a ojo.

Ejemplo. Calcular el inverso de $\overline{100}$ en $\mathbb{Z}_{433}$.

Siguiendo el esquema antes mencionado, si hallamos una solución de $100x + 433y = 1$ se tiene $\overline{100}\,\overline{x} = \overline{1}$ y $\overline{x}$ es el inverso buscado. Utilizando el algoritmo de Euclides y la tabla:

$$\begin{aligned} 100 &= 433 \cdot 0 + 100 \\ 433 &= 100 \cdot 4 + 33 \\ 100 &= 33 \cdot 3 + 1 \\ 33 &= 1 \cdot 33 + 0 \end{aligned}$$

	0	4	3	33
1	0	1	4	**13**
0	−1	0	−1	−3

Por tanto, $100 \cdot 13 + 433(-3) = 1$ y se concluye $\overline{100}^{-1} = \overline{13}$. Nótese que solo necesitamos el número en negrita, la última fila de la tabla nos la podemos ahorrar si no queremos comprobar la solución de $100x + 433y = 1$.

A menudo cuando se trabaja en $\mathbb{Z}_m$ se prefiere representar las clases por números entre 0 y $m - 1$, como hemos hecho hasta ahora. Sin embargo, el algoritmo de Euclides puede dar lugar a números negativos. Basta reemplazarlos por su resto si se sigue esta preferencia.

Ejemplo. Calcular el inverso de $\overline{199}$ en $\mathbb{Z}_{426}$.

Procedemos como antes,

$$\begin{aligned} 199 &= 426 \cdot 0 + 199 \\ 426 &= 199 \cdot 2 + 28 \\ 199 &= 28 \cdot 7 + 3 \\ 28 &= 3 \cdot 9 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

	0	2	7	9	3
1	0	1	2	15	**137**
0	−1	0	−1	−7	−64

que lleva a $199 \cdot (-137) + 426 \cdot 64 = 1$. Esto es, $\overline{199}^{-1} = \overline{-137}$. Lo habitual es sustituir $\overline{-137}$ por $\overline{289}$, que es la misma clase porque $-137 + 426 = 289$.

Parece natural generalizar la ecuación que define el inverso y plantearse ecuaciones lineales con el lenguaje de las congruencias o de las clases:

$$ax \equiv c \pmod{m} \qquad \text{o, equivalentemente,} \qquad \overline{a}\,\overline{x} = \overline{c} \quad \text{en} \quad \mathbb{Z}_m.$$

Estas ecuaciones también equivalen a que $c - ax$ es divisible por m, entonces todo lo que hay que hacer es resolver $ax + my = c$ en enteros y olvidarse de y. En particular, existe solución si y solo si $d = \mathrm{mcd}(a, m)$ divide a c.

Hay un pequeño detalle a tener en cuenta y es que la fórmula de la solución general de las ecuaciones diofánticas lineales da $x = cx_0/d + mt/d$ con $t \in \mathbb{Z}$. Si $d = 1$ todas estas soluciones son congruentes módulo m, pero si $d > 1$ obtenemos las d soluciones no congruentes:

$$\frac{cx_0}{d} + \frac{m}{d} \cdot 0, \quad \frac{cx_0}{d} + \frac{m}{d} \cdot 1, \quad \dots \dots \quad , \frac{cx_0}{d} + \frac{m}{d} \cdot (d-1).$$

Otra manera de verlo es decir que $ax \equiv c\ (m)$ equivale a $a/d \cdot x = c/d\ (m/d)$ y cada clase de $\mathbb{Z}_{m/d}$ es la unión de d clases de $\mathbb{Z}_m$. Por ejemplo, en $\mathbb{Z}_2$ la clase $\overline{0}$ son los pares que es unión de las clases $\overline{0}$ y $\overline{2}$ de $\mathbb{Z}_4$, los múltiplos de cuatro y los múltiplos pares de un número impar.

Ejemplo. Resolver $\overline{32}\,\overline{x} = \overline{58}$ en $\mathbb{Z}_{70}$.

La ecuación diofántica asociada es $32x + 70y = 58$. Primero hallamos $\mathrm{mcd}(32, 70)$, que resulta ser 2, y calculamos con la tabla (x_0, y_0) tal que $32x_0 + 70y_0 = 2$:

$$\begin{aligned} 32 &= 70 \cdot 0 + 32 \\ 70 &= 32 \cdot 2 + 6 \\ 32 &= 6 \cdot 5 + 2 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

	0	2	5	3
1	0	1	2	**11**
0	−1	0	−1	−5

Con lo que $(x_0, y_0) = (11, -5)$ satisface $32x_0 + 70y_0 = 2$. De nuevo, y_0 y la última fila de la tabla son irrelevantes para nuestros propósitos. Aquí $d = 2$ y se obtienen las soluciones no congruentes

$$\frac{cx_0}{d} + \frac{m}{d} \cdot 0 = \frac{58 \cdot 11}{2} \qquad \text{y} \qquad \frac{cx_0}{d} + \frac{m}{d} \cdot 1 = \frac{58 \cdot 11}{2} + \frac{70}{2}.$$

Utilizando que $29 \cdot 11 \equiv 39\ (70)$ y $29 \cdot 11 + 35 \equiv 4\ (70)$ se sigue que las soluciones son $x \equiv 39\ (70)$ y $x \equiv 4\ (70)$ o, equivalentemente, $\overline{x} = \overline{39}, \overline{4}$ en $\mathbb{Z}_{70}$.

Si a y m son coprimos, $d = 1$ y solo aparece la solución correspondiente a cx_0.

Ejemplo. Resolver $7x \equiv 36 \pmod{52}$.

Es fácil ver sin el algoritmo de Euclides que $\mathrm{mcd}(7, 52) = 1$ (porque 7 es primo y $7 \nmid 52$). En cualquier caso, debemos llevarlo a cabo para hallar una solución de $7x + 52y = 1$:

$$\begin{aligned} 7 &= 52 \cdot 0 + 7 \\ 52 &= 7 \cdot 7 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

	0	7	2	3
1	0	1	7	**15**
0	−1	0	−1	−2

De esta forma, $(x_0, y_0) = (15, -2)$ satisface $7x_0 + 52y_0 = 1$. Con ello, la única solución es $x \equiv 36 \cdot 15\ (52)$ y al calcular el resto de $36 \cdot 15 = 540$ para tener números más pequeños, se sigue $x \equiv 20\ (52)$.

A veces se presenta el problema de resolver simultáneamente ecuaciones lineales con respecto a diferentes módulos. El resultado fundamental es el *teorema chino del resto* que afirma que dados m_1 y m_2 números naturales coprimos, para cada $a_1, a_2 \in \mathbb{Z}$ existe $b \in \mathbb{Z}$ tal que se verifica

$$x \equiv a_1 \pmod{m_1} \quad \wedge \quad x \equiv a_2 \pmod{m_2} \iff x \equiv b \pmod{m_1 m_2}.$$

De hecho se puede tomar (ejercicio) $b = a_1 m_2 y_0 + a_2 m_1 x_0$ donde (x_0, y_0) una solución entera de $m_1 x_0 + m_2 y_0 = 1$. No entraremos en detalles porque no se incluye este importante resultado en el temario, aunque tiene aplicaciones prácticas. El nombre proviene de que lo emplearon matemáticos chinos de la antigüedad, posiblemente con el motivo inicial de elaborar calendarios.

3. El teorema de Euler-Fermat

Se define la *función φ de Euler* como la función

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N} \qquad \text{dada por} \qquad \varphi(m) = |\mathbb{Z}_m^*|.$$

Según lo que sabemos, $\varphi(m)$ cuenta los números $1 \leq n \leq m$ con $\operatorname{mcd}(n, m) = 1$. Así, con un poco de trabajo se tiene $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

Ejemplo. Demostrar que si p es primo $\varphi(p) = p - 1$ y, en general, $\varphi(p^k) = p^k - p^{k-1}$ para $k \in \mathbb{N}$.

Lo primero se verifica porque $1, 2, \ldots, p-1$ no pueden tener ningún factor común con p porque p solo es divisible por p y por 1. Este argumento también funciona para la segunda parte si excluimos los múltiplos de p entre 1 y p^k que son $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$.

Una consecuencia del teorema chino del resto es $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$ cuando m_1 y m_2 son coprimos (también se puede obtener con otros métodos elementales). Combinando este resultado con el ejemplo anterior y el teorema fundamental de la aritméticas, se obtiene la fórmula

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_1} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \qquad \text{para} \quad m > 1$$

donde $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es la descomposición en factores primos de m.

Ejemplo. Calcular $\varphi(700)$.

La factorización en primos de 700 es $2^2 \cdot 5^2 \cdot 7$. Según la fórmula anterior $\varphi(700)$ es igual a $(2^2 - 2^1)(5^2 - 5^1)(7 - 1) = 240$.

Comentario. Al igual que otras funciones que dependen de la factorización, el comportamiento de la función φ es errático y da lugar a problemas abiertos. Por ejemplo, es una cuestión sin resolver si para cada $n \in \mathbb{N}$ siempre existe otro $m \in \mathbb{N}$ distinto con $\varphi(n) = \varphi(m)$, violando así de manera drástica la inyectividad. Por otro lado, se sabe que φ en promedio es aproximadamente lineal. Concretamente, el valor medio de $\varphi(1), \ldots, \varphi(N)$ dividido entre N tiende a $3/\pi^2$ cuando $N \to \infty$.

El *teorema de Euler-Fermat* o *congruencia de Euler-Fermat* afirma:

$$\textit{Si } a \textit{ y } m \textit{ son coprimos entonces } a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Esta es la base de uno de los criptosistemas más famosos. Por otro lado, parte de la seguridad informática se basa en que con los conocimientos actuales es difícil recuperar el exponente a partir del residuo de una potencia.

Comentario. Dados a y m coprimos la fórmula $f(\overline{n}) = \overline{a}^n$ define una función $\mathbb{Z}_{\varphi(m)} \longrightarrow \mathbb{Z}_m^*$. Si m es enorme hay buenos algoritmos para evaluar $f(\overline{n})$, sin embargo, dado $f(\overline{n})$ se desconocen algoritmos adecuados para recuperar un posible $\overline{n}$. Si $\overline{n}$ representa un *password* podríamos guardar $f(\overline{n})$ en una base de datos y usarla para comprobar la identidad de un usuario y en caso de que la base de datos fuera asaltada el atacante no podría averiguar el *password*. Al problema de "invertir" f se le conoce como *problema del logaritmo discreto* porque el análogo en $\mathbb{R}$ tiene fácil solución con logaritmos: si $f(x) = a^x$ entonces a partir de $y = a^x$ se obtiene x con la fórmula $x = \log_a y$ donde $\log_a$ es el logaritmo en base a.

Cuando $m = p$ primo se tiene $a^{p-1} \equiv 1\ (p)$ si $p \nmid a$. Este es el llamado *pequeño teorema de Fermat*. El caso $p \mid a$, que falla porque $0 \not\equiv 1$, se vuelve cierto si multiplicamos por a. Así se obtiene otra versión del pequeño teorema de Fermat:

$$\textit{Si } a \in \mathbb{Z} \textit{ y } p \textit{ es primo entonces } a^p \equiv a \pmod{p}.$$

Con estos resultados se pueden calcular a mano algunos restos de potencias que operadas darían lugar a números inimaginablemente grandes.

Ejemplo. Calcula el resto al dividir 2^{1945} por 103.

El número 103 es primo porque si no lo fuera su menor factor primo tendría que ser menor que 11 (ya que $11^2 > 103$) y ninguno de los primos en este rango (que son 2, 3, 5 y 7) divide a 103. Por tanto, $\varphi(103) = 102$ y se cumple $2^{102} \equiv 1\ (103)$. El cociente y el resto al dividir 1945 entre 102 son 19 y 7 (en realidad solo nos interesa el último) y se obtiene

$$2^{1945} = 2^{19\cdot 102+7} = \left(2^{102}\right)^{19} \cdot 2^7 \equiv 1^{19} \cdot 2^7 = 128 \equiv 25 \pmod{103}.$$

En suma, el resto es 25.

Ejemplo. Demostrar que 188 divide a $19^{2025} + 13^{2026}$.

Tenemos la descomposición en factores primos $188 = 2^2 \cdot 47$ que implica $\varphi(188) = 2 \cdot 46 = 92$. Procediendo como antes, empleando $2025 = 22 \cdot 92 + 1$,

$$19^{2025} + 13^{2026} = \left(19^{92}\right)^{22} \cdot 19^1 + \left(13^{92}\right)^{22} \cdot 13^2 \equiv 19 + 13^2 \pmod{188}$$

donde se ha usado el teorema de Euler-Fermat para la congruencia. Un cálculo muestra $19 + 13^2 = 188$ y se deduce el resultado.

Ya hemos visto que el pequeño teorema de Fermat es una consecuencia directa del teorema de Euler-Fermat. La prueba de este último no es complicada, pero sí lo suficientemente ingeniosa como para sea injusto proponerla sin indicaciones.

Ejemplo (Teórico). Si $a \in \mathbb{Z}$ y $m \in \mathbb{N}$ son coprimos, comprobar que la función $f : \mathbb{Z}_m^* \longrightarrow \mathbb{Z}_m^*$ dada por $f(\overline{n}) = \overline{a}\,\overline{n}$ es biyectiva. Deducir de ello que si P es el producto de las clases de $\mathbb{Z}_m^*$ entonces $P = \overline{a}^{|\mathbb{Z}_m^*|}P$ en $\mathbb{Z}_m$ y, de aquí, el teorema de Euler-Fermat.

Es biyectiva porque su inversa es $g(\overline{n}) = \overline{a}^{-1}\overline{n}$. Al ser biyectiva, lo único que hace es reordenar las clases y entonces el producto P de los elementos de $\{\overline{n} \in \mathbb{Z}_m^*\}$ es igual al de los elementos de $\{\overline{a}\,\overline{n} \,:\, \overline{n} \in \mathbb{Z}_m^*\}$. Como hay $|\mathbb{Z}_m^*|$ elementos en estos conjuntos la clase $\overline{a}$ aparecerá multiplicada por sí misma $|\mathbb{Z}_m^*|$ veces, de modo que $P = \overline{a}^{|\mathbb{Z}_m^*|}P$ en $\mathbb{Z}_m$. Ahora bien, al ser P producto de clases invertibles, es también una clase invertible y multiplicando por su inverso se concluye $1 = \overline{a}^{|\mathbb{Z}_m^*|}$ en $\mathbb{Z}_m$ que con el lenguaje de congruencias es $1 \equiv a^{\varphi(m)}\ (m)$.

Los ejemplos anteriores pueden dar la falsa impresión de que el cálculo de restos de potencias grandes requiere conocer la factorización, para hallar $\varphi(m)$, y la casualidad de que el exponente tenga resto pequeño al dividir por $\varphi(m)$. Sin estos requerimientos el cálculo puede resultar más tedioso, pero factible sin apelar al teorema de Euler-Fermat y bastante eficiente con un ordenador. Si el exponente es potencia de dos, se procede elevando sucesivamente al cuadrado y si no lo es, se expresa como una suma de potencias de dos (que es lo mismo que escribirlo en base 2). El siguiente ejemplo ilustra el algoritmo, el cual es usado ampliamente en informática.

Ejemplo. Hallar el resto de 17^{48} al dividir por 211.

Aquí el Teorema de Euler-Fermat no sería de utilidad porque $48 < \varphi(211)$. Se tiene $17^2 = 289 \equiv 78\ (211)$ y elevando al cuadrado de nuevo $17^4 \equiv 78^2 = 6084 \equiv 176 \equiv -35\ (211)$. Procediendo de la misma forma tres veces más: $17^8 \equiv 35^2 \equiv -41\ (211)$, $17^{16} \equiv 41^2 \equiv -7\ (211)$, $17^{32} \equiv 49\ (211)$. Pasando a base dos, $48 = 2^5 + 2^4 = 32 + 16$ y los cálculos anteriores implican $17^{48} \equiv 49(-7) \equiv 79\ (211)$, así que el resto buscado es 79.