Álgebra Abstracta y Codificación

Clase 4: GCD y Aritmética modular

by

Mauro Artigiani

19 agosto 2020

Máximo común divisor

Máximo común divisor

Sean n y m dos naturales. El máximo común divisor de n y m, denotado con $\gcd(n, m)$ es el natural más grande que divide ambos.

Máximo común divisor

Sean n y m dos naturales. El máximo común divisor de n y m, denotado con $\gcd(n, m)$ es el natural más grande que divide ambos. $\gcd$ viene del inglés “greatest common divisor”.

Máximo común divisor

Sean n y m dos naturales. El máximo común divisor de n y m, denotado con $\gcd(n, m)$ es el natural más grande que divide ambos. gcd viene del inglés “greatest common divisor”.

De la definición sigue que, para todos $n \in \mathbb{N}$, se tiene $\gcd(n, 0) = n$.

Por convención, decidimos que $\gcd(0, 0) = 0$.

Algoritmo euclidiano

Hemos visto en clase el siguiente resultado:

Proposición

Sean n y m dos números naturales. Entonces

$$\gcd(n, m) = \begin{cases} n, & \text{si } m = 0; \\ \gcd(m, r), & \text{si } n = mq + r, \text{ con } 0 \leq r < m. \end{cases}$$

Podemos entonces calcular de manera algorítmica el gcd entre dos números. El hecho que $r < m$ implica que el algoritmo termina (dando el resultado correcto) en un tiempo finito.

Algoritmo euclidiano

Por ejemplo, sean $n = 7007$ y $m = 1991$. Se tiene

$$\begin{aligned}
7007 &= 3 \cdot 1991 + 1034, \\
1991 &= 1 \cdot 1034 + 957, \\
1034 &= 1 \cdot 957 + 77, \\
957 &= 12 \cdot 77 + 33, \\
77 &= 2 \cdot 33 + 11, \\
33 &= 3 \cdot 11 + 0.
\end{aligned}$$

Entonces sabemos que:

$$\gcd(7007, 1991) = \gcd(1991, 1034) = \gcd(1034, 957) = \\ \gcd(957, 77) = \gcd(77, 33) = \gcd(33, 11) = \gcd(11, 0) = 11.$$

Algoritmo euclidiano

El algoritmo euclidiano hace más que encontrar el $\gcd$:

Teorema (Identidad de Bézout)

Sean n y m dos números naturales, no ambos 0. Entonces el $\gcd(n, m)$ es el número *positivo* más pequeño contenido en el conjunto

$$A = \{nx + my, x, y \in \mathbb{Z}\}.$$

Algoritmo euclidiano

Antes de ver la demostración, vemos como el algoritmo euclidiano nos permite encontrar x y y.

$$\begin{aligned} 7007 &= 3 \cdot 1991 + 1034, \\ 1991 &= 1 \cdot 1034 + 957, \\ 1034 &= 1 \cdot 957 + 77, \\ 957 &= 12 \cdot 77 + 33, \\ 77 &= 2 \cdot 33 + 11. \end{aligned}$$

Entonces

$$\begin{aligned} 11 &= 77 - 2 \cdot 33 \\ &= 77 - 2(957 - 12 \cdot 77) = 25 \cdot 77 - 2 \cdot 957 \\ &= 25(1034 - 957) - 2 \cdot 957 = 25 \cdot 1034 - 27 \cdot 957 \\ &= 25 \cdot 1034 - 27(1991 - 1034) = 52 \cdot 1034 - 27 \cdot 1991 \\ &= 52(7007 - 3 \cdot 1991) - 27 \cdot 1991 = 52 \cdot 7007 - 183 \cdot 1991. \end{aligned}$$

Es decir $x = 52$ y $y = -181$.

La identidad de Bézout

Demostración

Empezamos notando que, si tomamos $x = 0, y = 1$ o $x = 1, y = 0$, se tiene $n, m \in A$ y por eso A contiene elementos positivos.
Llamamos $d = nx + my$ el número positivo más pequeño en A.
Cualquier divisor común de n y m va a dividir también $d = nx + my$, y por eso tenemos

$$\gcd(n, m) \leq d.$$

La identidad de Bézout

Demostración

Ahora, sea $c = nx' + my' \in A$ otro elemento. Por división euclidiana, tenemos

$$c = qd + r, \qquad 0 \leq r < d.$$

Acordándonos que $d = nx + my$, obtenemos $r = n(x' - qx) + m(y' - qy)$. Es decir: $r \in A$. Siendo $0 \leq r < d$ y d el mínimo, necesariamente $r = 0$. Entonces $d \mid c$. Pero c era un elemento cualquiera de A. Entonces en particular $d \mid n$ y $d \mid m$. Por eso

$$d \leq \gcd(n, m). \quad \square$$

Aritmética modular

Aritmética modular

Hemos visto en la clase pasada que dos enteros a y b son congruentes módulo m, por un entero $m \geq 2$ si

$$m \mid (a - b).$$

La relación ser congruente módulo un entero m es una relación de equivalencia en $\mathbb{Z}$ cuyas clases de equivalencia son

$$\mathbb{Z}_m = \{[0]_m, \ldots, [m-1]_m\}.$$

Aritmética modular

Hemos visto en la clase pasada que dos enteros a y b son congruentes módulo m, por un entero $m \geq 2$ si

$$m \mid (a - b).$$

La relación ser congruente módulo un entero m es una relación de equivalencia en $\mathbb{Z}$ cuyas clases de equivalencia son

$$\mathbb{Z}_m = \{[0]_m, \ldots, [m-1]_m\}.$$

Queremos definir las dos operaciones de suma y múltiplicación en $\mathbb{Z}_m$. Esto se puede hacer así:

$$[x]_m + [y]_m = [x+y]_m, \qquad [x]_m \cdot [y]_m = [xy]_m.$$

Aritmética modular

$$[x]_m + [y]_m = [x+y]_m, \qquad [x]_m \cdot [y]_m = [xy]_m.$$

hay un problema: $[x]_m$ significa la clase de equivalencia de x, y lo mismo vale para $[y]_m$.

Aritmética modular

$$[x]_m + [y]_m = [x + y]_m, \qquad [x]_m \cdot [y]_m = [xy]_m.$$

hay un problema: $[x]_m$ significa la clase de equivalencia de x, y lo mismo vale para $[y]_m$. Entonces podríamos elegir otros representantes en cada clase de equivalencia. Debemos mostrar que el resultado no depende de cuales representantes elegimos.

Aritmética modular

$$[x]_m + [y]_m = [x + y]_m, \qquad [x]_m \cdot [y]_m = [xy]_m.$$

hay un problema: $[x]_m$ significa la clase de equivalencia de x, y lo mismo vale para $[y]_m$. Entonces podríamos elegir otros representantes en cada clase de equivalencia. Debemos mostrar que el resultado no depende de cuales representantes elegimos. Sean $[x]_m = [x']_m$ y $[y]_m = [y']_m$. Por definición, $m \mid (x - x')$. Entonces existe un entero a tal que $x' = x + am$. De manera similar existe un entero b tal que $y' = y + bm$. Se tiene

$$x'y' = (x + am)(y + bm) = xy + (ay + bx + abm)m,$$

y entonces $[xy]_m = [x'y']_m$ como queríamos.

Aritmética modular

$$[x]_m + [y]_m = [x+y]_m, \qquad [x]_m \cdot [y]_m = [xy]_m.$$

hay un problema: $[x]_m$ significa la clase de equivalencia de x, y lo mismo vale para $[y]_m$. Entonces podríamos elegir otros representantes en cada clase de equivalencia. Debemos mostrar que el resultado no depende de cuales representantes elegimos. Sean $[x]_m = [x']_m$ y $[y]_m = [y']_m$. Por definición, $m \mid (x - x')$. Entonces existe un entero a tal que $x' = x + am$. De manera similar existe un entero b tal que $y' = y + bm$. Se tiene

$$x'y' = (x+am)(y+bm) = xy + (ay + bx + abm)m,$$

y entonces $[xy]_m = [x'y']_m$ como queríamos.
La demostración que la suma es *bien definida*, es decir no depende de que representantes utilizamos para calcularla, es un ejercicio.

Aritmética modular

En $\mathbb{Z}_m$ se puede siempre restar, pero no siempre se puede dividir.

Aritmética modular

En $\mathbb{Z}_m$ se puede siempre restar, pero no siempre se puede dividir.

Teorema

En $\mathbb{Z}_m$ un elemento $[x]_m$ tiene un *inverso* si y solo si $\gcd(x, m) = 1$.

Demostración

Si $[x]_m$ tiene un inverso, digamos $[y]_m$, entonces $xy \equiv 1 \pmod{m}$. Es decir, $xy = 1 + am$. Cualquier divisor d de x y m divide también $xy - am = 1$, lo que implica $\gcd(x, m) = 1$.

Aritmética modular

En $\mathbb{Z}_m$ se puede siempre restar, pero no siempre se puede dividir.

Teorema

En $\mathbb{Z}_m$ un elemento $[x]_m$ tiene un *inverso* si y solo si $\gcd(x, m) = 1$.

Demostración

Si $[x]_m$ tiene un inverso, digamos $[y]_m$, entonces $xy \equiv 1 \mod m$. Es decir, $xy = 1 + am$. Cualquier divisor d de x y m divide también $xy - am = 1$, lo que implica $\gcd(x, m) = 1$.
Si sabemos que $\gcd(x, m) = 1$, por la identidad de Bézout sabemos que existen a y b enteros tales que $ax + bm = 1$, es decir $ax \equiv 1 \mod m$ y a es el inverso de x módulo m. □

La función φ de Euler

Pregunta

¿Cuántos son los elementos invertibles en $\mathbb{Z}_n$?

La respuesta es la función φ de Euler:

$$\varphi(n) = |\{1 \leq k \leq n, \gcd(k,n) = 1\}|.$$

La función φ de Euler

Pregunta

¿Cuántos son los elementos invertibles en $\mathbb{Z}_n$?

La respuesta es la función φ de Euler:

$$\varphi(n) = |\{1 \leq k \leq n, \gcd(k, n) = 1\}|.$$

Teorema

La función φ de Euler satisface:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

donde el producto es sobre todos los primos p que dividen n.

La demostración será un ejercicio (guiado).

El teorema chino del resto

Supongamos querer resolver el sistema de congruencias

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

con $\gcd(n, m) = 1$, es decir n y m *primos entre sí*.

El teorema chino del resto

Supongamos querer resolver el sistema de congruencias

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

con $\gcd(n, m) = 1$, es decir n y m *primos entre sí*.
Si existe una solución x, también $x + mn$ será una solución. Del otro lado, si x y y son dos soluciones, se tiene $x \equiv y$ tanto módulo m que módulo n. Siendo n y m primos entre sí, esto implica $x \equiv y$ módulo mn. Es decir: si la solución existe será una clase de congruencia módulo mn.

El teorema chino del resto

Supongamos querer resolver el sistema de congruencias

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

con $\gcd(n, m) = 1$, es decir n y m *primos entre sí*.
Si existe una solución x, también $x + mn$ será una solución. Del otro lado, si x y y son dos soluciones, se tiene $x \equiv y$ tanto módulo m que módulo n. Siendo n y m primos entre sí, esto implica $x \equiv y$ módulo mn. Es decir: si la solución existe será una clase de congruencia módulo mn.
¿Cómo mostrar que existe siempre una solución?

El teorema chino del resto

Acabamos de demostrar que

$$\begin{aligned} \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ [x]_{mn} &\mapsto ([x]_m, [x]_n), \end{aligned}$$

es injectiva. Dado que $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, la aplicación es también sobreyectiva, y por eso existe siempre una solución.

Teorema chino del resto

Sean n y m dos enteros primos entre sí. El sistema de congruencias

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n}, \end{cases}$$

tiene solución para cualesquiera a y b enteros. La solución es única módulo nm.