Congruencias

Homero Gallegos
CONACyT – Unidad Académica de Matemáticas UAZ
h.r.gallegos.ruiz@gmail.com

11 de febrero de 2015

Cálculos en MAGMA:

```
> time Max(
SequenceToSet(Divisors(31415926535897932384626433832))
meet
SequenceToSet(Divisors(271828182845904523536028747)));
13
Time: 0.050
> time GCD(31415926535897932384626433832,
271828182845904523536028747);
13
Time: 0.000
```

División con residuo:

Teorema

Sean a y b enteros, con $a \neq 0$. Entonces existen enteros únicos r y q tales que

$$b = qa + r, \quad 0 \leq r < |a|$$

Congruencias:

Decimos que a y b son *congruentes módulo* m si $m \mid a - b$. Se escribe

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

Ejemplos:

- Días de la semana
- Meses del año
- Horas del día
- $15 \equiv 1 \text{ mód } 7 \quad 10 \not\equiv 2 \text{ mód } 3$

Propiedades básicas:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Representantes de las clases:

$$\{0, 1, 2, \ldots, m-1\}$$

con el algoritmo de la división.

Más propiedades:

- Preservan sumas y productos:
  Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces
  $a + c \equiv b + d \pmod{m}$ y $ac \equiv bd \pmod{m}$.
- Si $d \mid m$ y $a \equiv b \pmod{m}$, entonces $a \equiv b \pmod{d}$
- Si $a \equiv b \pmod{m}$, entonces $na \equiv nb \pmod{nm}$
- Si $ac \equiv bc \pmod{m}$, entonces $a \equiv b \pmod{\frac{m}{\mathrm{mcd}(c,m)}}$

Cuidado con la última. $100 \equiv 60 \pmod{8}$ pero $10 \not\equiv 6 \pmod{8}$. Si $\mathrm{mcd}(c, m) = 1$ sí se puede cancelar.

Inversos $\mod m$:
Supongamos que $\mcd(a, m) = 1$, entonces por Euclides extendido

$$ax + my = 1$$

y entonces $ax \equiv 1 \pmod{m}$.
En MAGMA usa
`> XGCD(a,m)`
para obtener $\mcd(a, m), x, y$.
Nota: p primo, y $p \nmid a \Rightarrow \mcd(a, p) = 1$. Luego todo elemento $\not\equiv 0$ tiene inverso multiplicativo $\mod p$.

Exponenciación $\mod m$.
Sea n un entero positivo y $a_s \dots a_1 a_0$ su representación binaria. Por ejemplo, $n = 15$, $a_3 = a_2 = a_1 = a_0 = 1$. $15 = 1111_2$.

$$n = \sum a_i 2^i$$

Sea c otro entero. Usamos leyes de los exponentes para calcular:

$$c^n = c^{\sum a_i 2^i} = c^{a_s 2^s} \dots c^{a_2 2^2} \cdot c^{a_1 2} \cdot c^{a_0}.$$

Solo se requiere elevar al cuadrado sucesivamente para obtener las potencias:

$$c, c^2, (c^2)^2 = c^{2 \cdot 2} = c^{2^2}, (c^{2^2})^2 = c^{2^2 \cdot 2} = c^{2^3}, \dots$$

Calcula $13^{100} \pmod{81}$.
Construimos una tabla

i	$\lfloor n/2^i \rfloor$	a_i	$c^{2^i} \bmod m$
0	100	0	13
1	50	0	$13^2 = 169 \equiv 7$
2	25	1	$7^2 = 49$
3	12	0	$49^2 = 2401 \equiv 52$
4	6	0	$52^2 = 2704 \equiv 31$
5	3	1	$31^2 = 961 \equiv 70$
6	1	1	$70^2 = 4900 \equiv 40$

Entonces $13^{100} = 13^{2^2} 13^{2^5} 13^{2^6} \equiv 49 \cdot 70 \cdot 40 = 137200 \equiv 67.$

```
> n := 954680934860934509834095834098509348509384590 83;
> time 2^(n-1) mod n;

>> time 2^(n-1) mod n;
          ^
Runtime error in '^': Argument 2 (954680934860934509834095
\
82) is too large

>
```

En cambio,

```
>  n := 954680934860934509834095834098509348509384590 83;
> time Modexp(2,n-1,n);
3417344413926555387083026637859840706924868724 1
Time: 0.000
>
```

Pequeño teorema de Fermat:

Teorema

Sea p un número primo.

- *Si a es un entero y $p \nmid a$, ($a \not\equiv 0 \pmod{p}$), entonces*

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

- *Si a es cualquier entero, entonces*

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

Aplicaciones:

- Decidir que un número no es primo. Si n es un entero y a es otro con $\mathrm{mcd}(a, n) = 1$, y $a^{n-1} \not\equiv 1 \text{ mód } n$, entonces n no puede ser primo, sin necesidad de hallar factores.
- Calcular inversos. Si p es primo y $p \not| a$, entonces $a^{p-2} \equiv a^{-1}$. Calcular potencias es fácil.

Demostración: Sea a un entero no divisible por p. Entonces $\mathrm{mcd}(a, p) = 1$. Considera el conjunto

$$\{1, \ldots, p-1\}$$

y multiplica todo por a:

$$\{a, 2a, \ldots, (p-1)a\}.$$

Nota que en este nuevo conjunto, ningún número es divisible entre p. Además, si $ia \equiv ja \pmod{p}$, podemos multiplicar por un inverso de a para ver que $i \equiv j$. Es decir, no hay forma de que dos elementos diferentes del conjunto dejen el mismo residuo.

En otras palabras:

$$\{1, \ldots, p-1\} \equiv \{a, 2a, \ldots, (p-1)a\}.$$

Por las propiedades:

$$a^{p-1} 1 \cdot 2 \ldots (p-1) \equiv 1 \cdot 2 \ldots (p-1),$$

y como $1, \ldots, p-1$ son cancelables, obtenemos

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

La segunda parte es fácil si $p \mid a$, y en otro caso, sólo multiplicamos por a.

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

Teorema chino del residuo. (TCR)

Teorema

Sean m_1, m_2 *enteros con* $\mathrm{mcd}(m_1, m_2) = 1$. *Sean* a_1, a_2 *enteros. El sistema de congruencias simultáneas:*

$$\begin{aligned} t &\equiv a_1 \pmod{m_1} \\ t &\equiv a_2 \pmod{m_2} \end{aligned}$$

tiene solución y es única módulo $m_1 \cdot m_2$.

Demostración (algoritmo):
Usa Euclides extendido:

$$1 = xm_1 + ym_2.$$

Multiplica por a_1 y reduce mód m_1:

$$a_1 = a_1xm_1 + a_1ym_2 \equiv a_1ym_2 \pmod{m_1}.$$

Lo mismo con a_2:

$$a_2 \equiv a_2xm_1 \pmod{m_2}.$$

Entonces

$$t = a_1ym_2 + a_2xm_1$$

es solución.

Si t' es otra solución, entonces $t' - t$ es divisible entre m_1 y m_2. Como $\mathrm{mcd}(m_1, m_2) = 1$, entonces $m_1 \cdot m_2 \mid t' - t$. Es decir,

$$t' \equiv t \pmod{m_1 \cdot m_2}.$$

```
> m1:= 151; // Los modulos
> m2:= 878;
> GCD(m1,m2); // Checar condicion del mcd
1
> g,x,y:=XGCD(m1,m2);  // Euclides extendido
> g;
1
> x;
157
> y;
-27
> a1:=10;   // Valores ai
> a2:=87;
> t:= a1*y*m2 + a2*x*m1;  // Formulita
1825449
> t mod (m1*m2); // Reduccion.
101935
```

MAGMA tiene la función CRT (Chinese Remainder Theorem)

```
> CRT([a1,a2],[m1,m2]);
101935
```

Teorema de Euler:
Para un entero mayor que 1 definimos:

$$\varphi(n) := \#\{0 \leq a < n \mid \mathrm{mcd}(a, n) = 1\}.$$

Propiedades:

- Si p es primo: $\varphi(p) = p - 1$,
- Si p es primo y n positivo: $\varphi(p^n) = p^{n-1}(p-1)$,
- Si m, n son tales que $\mathrm{mcd}(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

Las primeras dos son ejercicios fáciles de demostrar, la tercera es una aplicación del TCR y las propiedades de mcd.
Con estas propiedades, se puede calcular $\varphi(n)$ a partir de la factorización en primos de n. No se conoce un método para hacerlo sin la factorización.

Teorema de Euler

Teorema

Sea n un entero > 1, y a un entero cualquiera tal que $\mathrm{mcd}(a, n) = 1$. Entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Es pues, una generalización del Pequeño teorema de Fermat, y se demuestra de una forma similar.

Teorema

Sea $n = pq$ un entero producto de dos números primos distintos p y q. Sean e, d enteros tales que $ed \equiv 1 \pmod{\varphi(n)}$.
($\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$) Entonces

$$a^{de} \equiv a \pmod{n}.$$

Demostración: Queremos ver que $n \mid a^{de} - a$. Como n es producto de primos distintos, basta ver que p y q dividen a $a^{de} - a$. Si , $p \nmid a$, por el pequeño teorema de Fermat:

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

Notemos que $ed \equiv 1 \pmod{\varphi(n)}$ implica que $p-1 \mid ed-1$, y luego, existe un k tal que $(p-1)k = ed-1$ así que $1 \equiv (a^{p-1})^k = a^{(p-1)k} = a^{ed-1} \pmod{p}$.
Entonces

$$a^{ed} \equiv a \pmod{p}$$

Si $p \mid a$, entonces $a \equiv 0 \pmod{p}$ y luego $a^{ed} \equiv a \pmod{a}$.
Los mismos argumentos funcionan con q, así que tanto p como q dividen a $a^{ed} - a$, y por tanto $n = pq \mid a^{ed} - a$, es decir,

$$a^{ed} \equiv a \pmod{n}.$$