Congruencias

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

4 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
>
```