Enrique R. Aznar García
eaznar@ugr.es

LA RAÍZ CUADRADA DE UN ENTERO MÓDULO P

Sea p un primo impar y a un entero tal que $\left(\frac{a}{p}\right) = 1$. Entonces, existen exactamente dos enteros x distintos nódulo tal que $x^2 \equiv a \pmod{p}$. Para hallarlos, se puede usar fuerza bruta pero es un algoritmo lineal en p e ineficiente para valores grandes.

Si $p \equiv 3 \pmod{4}$, entonces $x = a^{(p+1)/4} \pmod{p}$ es claramente una solución ya que por el TPF se tiene $a^{(p-1)/2} \equiv 1 \pmod{p}$ y entonces
$x^2 \equiv a^{(p+1)/2} = a \cdot a^{(p-1)/2} \equiv a \pmod{p}$

Si $p \equiv 5 \pmod{8}$, como $a^{(p-1)/2} \equiv 1 \Rightarrow a^{(p-1)/4} \equiv \pm 1 \pmod{p}$

Si sale $+1$, entonces $x = a^{(p+3)/8} \pmod{p}$ es una solución.

En caso contrario, como $2^{(p-1)/2} \equiv -1 \pmod{p}$, una solución es $x = 2a(4a)^{(p-5)/8} \pmod{p}$

El caso que nos queda es $p \equiv 1 \pmod{8}$. Que es el caso que necesita de un algoritmo especial.

Hay 3 algoritmos para este caso. Uno usa el método de factorización de polinomios módulo p. Otro probabilístico debido a R. Schoff, que usa c.e. es complicado y no está clara su eficiencia. El tercer algoritmo de Tonelli y Shanks, también es probabilístico y es muy eficiente.

BASE TEÓRICA

Factorizamos $p-1=2^e\cdot q$ con q impar. Como el grupo multiplicativo $U(\mathbb{Z}_p)$ es cíclico de orden $p-1$ es isomorfo al grupo aditivo $(\mathbb{Z}_{p-1},+)$. Por tanto, su 2-subgrupo de Sylow, G, es cíclico de orden 2^e.

Si encontramos un generador z de este subgrupo, los cuadrados en G son exactamente las potencias pares de z que son exactamente los elementos de orden un divisor de $2^{e-1}q$, ya que

$$O(z^{2k})=\frac{2^eq}{(2k,2^eq)}=\frac{2^{e-1}q}{(k,2^{e-1}q)}$$

Ahora, si a es un residuo cuadrático módulo p, tenemos

$$1=\left(\frac{a}{p}\right)=a^{(p-1)/2}=(a^q)^{2^{e-1}}$$

O sea, $b=a^q \pmod p$ es un cuadrado en G y existe un entero par, k tal que

$$a^qz^k=1\in G$$

Por tanto, $x=a^{(q+1)/2}z^{k/2}\Rightarrow x^2\equiv a^{q+1}z^k\equiv a \pmod p$.

Necesitamos encontrar el generador z y el exponente par k.

INICIACIÓN DEL ALGORITMO

Para encontrar z, elegimos un n (parte probabilística del algoritmo) que no sea un residuo cuadrático entonces

$$n^{(p-1)/2}=(n^q)^{2^{e-1}}\equiv -1 \pmod p \Rightarrow O(n^q)=2^e\Leftrightarrow z=n^q$$

ALGORTIMO DE TONELLI-SHANKS

Si a es un residuo cuadrático módulo p primo tal que $p-1=2^e q$ con q impar. Queremos resolver $x^2 \equiv a \pmod{p}$

Definimos $r=a^{(q+1)/2}$, entonces $r^2=a^{q+1}=a^q a=t \cdot a$. Si $t=a^q \equiv 1 \pmod{p}$, tendríamos que r una raíz cuadrada de a módulo p.

En caso contrario, $1<e$, como $t^{2^{e-1}}=a^{q2^{e-1}}=a^{(p-1)/2}=1$, t tiene de orden un divisor de 2^{e-1}.

Si su orden es, $O(t)=2^i$, con $i \leq e-1$, entonces $t^{2^{i-1}} \equiv -1 \pmod{p}$.

Ahora, si $b=z^{2^{e-i-1}}$, entonces $O(b^2)=O(z^{2^{e-i}})=2^i$ y satisface que $b^{2^i} \equiv -1 \pmod{p}$. Por tanto,
$(tb^2)^{2^{i-1}} \equiv (-1)(-1)=1 \pmod{p} \Rightarrow O(tb^2) \leq 2^{i-1} \leq 2^{e-2}$
O sea, $t_1=tb^2$ tiene de orden un divisor de 2^{i-1} que es menor o igual que que 2^{e-2}.

Si definimos $r_1=rb$, se mantiene la relación invariante $r_1^2 \equiv t_1 a$ ya que
$r_1^2=r^2 b^2=tab^2=t_1 a$

Si el orden de t_1 es cero, $t_1 \equiv 1 \pmod{p}$ y tendríamos una raíz cuadrada módulo. En caso contrario, repetimos el argumento. Como en cada paso del algoritmo se baja al menos una unidad en el exponente, Como mucho en e iteraciones se encuentra una raíz cuadrada y se resuelve la ecuación $x^2 \equiv a \pmod{p}$.

EJEMPLO 1

Para resolver $y^2 \equiv 145 \pmod{p}$ con $p = 1492556235563626978475467978606060 7237$, primero comprobamos que p es primo porque encontramos que 2 es un elemento primitivo. Después comprobamos que 145 es un residuo cuadrático módulo p porque

$$\left(\frac{145}{p}\right) = 1$$

Por tanto la congruencia tiene dos soluciones y existen dos raíces cuadradas de 145 módulo p.

Como $p \equiv 5 \pmod{8}$, son fáciles de hallar sin necesidad del algortimo de Tonelli-Shanks.

Como $145^{(p-1)/4} \equiv 1 \pmod{p}$, una de las raíces es

$$y_1 = 145^{(p+3)/8} \equiv 776852700273444030245998870798631 9554 \pmod{p}$$

y la otra es su opuesto modular

$$y_2 = p - y_1 = 715703535290182948229469107807428 7683$$

Como $5^3 + 4 * 5 = 145$, hemos encontrado dos puntos de la c.e. $y^2 = x^3 + 4x$ módulo p

$$\begin{cases} Q_1 = (5, 7768527002734440302459988707986319554) \\ Q_2 = (5, 7157035352901829482294691078074287683) \end{cases}$$

EJEMPLO 2

Para resolver $y^2 \equiv 145 \pmod{p}$ con $p = 1492556235563626978475467978606060727 3$, primero comprobamos que p es primo porque encontramos que 3 es un elemento primitivo. Comprobamos que 145 es un residuo cuadrático módulo p porque de nuevo $\left(\frac{145}{p}\right) = 1$

Por tanto la congruencia tiene dos soluciones y existen dos raíces cuadradas de 145 módulo p.

Como $p \equiv 1 \pmod{8}$, tenemos que usar el algoritmo de Tonelli-Shanks. Para eso extraemos las potencias de dos

$$p - 1 = 2^3 * 186569529445453372309433497325757590 9$$

El algoritmo como mucho tiene 3 pasos, $e = 3$, $q = 1865695294454533723094334973257575909$

Para iniciar, necesitamos un no residuo cuadrático módulo p, el primero que se encuentra es $n = 3$ ya que $\left(\frac{3}{p}\right) = -1$. Entonces, un generador del 2-subgrupo de Sylow, $G \cong \mathbb{Z}_{2^3} = \mathbb{Z}_8$, es

$$z = n^q \equiv 4666375454944377570433408908093471653 \pmod{p}$$

Ahora calculamos, $a^q \equiv 1 \pmod{p}$. Como sale uno hemos acabado y la raíces cuadradas de 145 módulo p son

$$y_1 = 145^{(q+1)/2} \equiv 1452088723950244542247243880610248122 3 \pmod{p}$$

y su opuesto modular $y_2 = p - y_1 = 4046751161338243622822409799581260 50$

Como $5^3 + 4 * 5 = 145$, hemos encontrado dos puntos de la c.e. $y^2 = x^3 + 4x$ módulo p

$$\begin{cases} Q_1 = (5, 14520887239502445422472438806102481223) \\ Q_2 = (5, 404675116133824362282224097995812605 0) \end{cases}$$

Enrique R. Aznar García
eaznar@ugr.es