

Strong Pseudoprimes & Quadratic Residues

Universidad de Cuenca

Optativa 6 - Criptología

Dr. Diego Ponce

Capítulo 6

Freddy L. Abad L.

freddy.abadl@ucuenca.edu.ec

CAP 6

6.1.

$2 \rightarrow$ paso
 $3 \rightarrow$ paso
 $5 \rightarrow$ paso
 $7 \rightarrow$ paso

$\} \text{ Alg 6.1}$

6.2.

leer $b, p, \text{base} = 2;$

int resultado = 1;

int exp = 0, c = 0;

while ($c < \exp > 0$)

{ if ($c \& 1 > 0$) {

resultado = (resultado * base) % p;

c++;

}

exp++;

base = (base * base) % p;

} if ($c == \exp$) {

System.out.println("b es un residuo cuadrático");

} else {

System.out.println("b no es un residuo cuadrático")

}

6.3.

$2 \rightarrow$ residuo cuadrático de p

$$x^2 \equiv r \pmod{p}$$

↑
coprimo

$$p = 1, 3, 5, 7, 11, 13, 17, 19, \dots$$

$$2^3 = 2 \pmod{3}$$

$$2^5 = 2 \pmod{5}$$

$$2^{11} = 2 \pmod{11}$$

$$2^{13} = 2 \pmod{13}$$

$$2^{17} = 2 \pmod{17}$$

$$2^{19} = 2 \pmod{19}$$

siempre es 2

6.4

El algoritmo es el mismo, con el cambio de base

a 3.

6.5

$$\left. \begin{array}{l} 1^2 \bmod 5 = 1 \\ 2^2 \bmod 5 = 4 \\ 3^2 \bmod 5 = 1 \\ 4^2 \bmod 5 = 1 \end{array} \right\} \{1, 4\}$$

6.6

$$\begin{aligned} 1^2 &\equiv 1 \pmod{10} & 1 \\ 2^2 &\equiv 4 \pmod{10} & 4 \\ 3^2 &\equiv 9 \pmod{10} & 9 \\ 4^2 &\equiv 16 \pmod{10} & 6 \\ 5^2 &\equiv 25 \pmod{10} & 5 \\ 6^2 &\equiv 36 \pmod{10} & 6 \\ 7^2 &\equiv 49 \pmod{10} & 9 \\ 8^2 &\equiv 64 \pmod{10} & 4 \\ 9^2 &\equiv 81 \pmod{10} & 1 \\ 10^2 &\equiv 100 \pmod{10} & 0 \\ 11^2 &\equiv 121 \pmod{10} & 1 \end{aligned}$$

↑

n^2

El patrón es que si n^2 es mayor q 100 el resultado es $n^2 - 100$ mientras que para $n^2 < 100$ su resultado siempre es n^2

6.7

$$\begin{aligned} p &= 3, 5, 7, 11, 13, 17, 19 \\ q &= 5 \end{aligned}$$

$$\left. \begin{array}{l} 3^2 \bmod 5 = 4 \\ 5^2 \bmod 5 = 0 \\ 7^2 \bmod 5 = 4 \\ 11^2 \bmod 5 = 1 \\ 13^2 \bmod 5 = 4 \\ 17^2 \bmod 5 = 4 \\ 19^2 \bmod 5 = 1 \end{array} \right\} \{1, 4\}$$

↳ El único patrón con 5.

6.8 Si $p \rightarrow$ primo y $i^2 \equiv j^2 \pmod{p}$ entonces

$$i = j \text{ ó } -j \pmod{p}$$

$$\text{Si } p | (i^2 - j^2) \rightarrow i^2 - j^2 = (i+j)(i-j)$$

como p es primo

entonces $p | (i-j)$ ó $p | (i+j)$

$$i=j$$

$$i=-j$$

entonces volviendo a reescribir

$$i = j \pmod{p} \text{ ó } i \equiv -j \pmod{p}$$

LQPD

6.9

$$645 = 3 \times 5 \times 43$$

$$b^{n-1} - 1 = \underbrace{(b^t - 1)}_{\substack{\downarrow \\ \text{Factor para 3}}} \underbrace{(b^t + 1)}_{\substack{\downarrow \\ \text{Factor para 5}}} \underbrace{(b^{2t} + 1)}_{\substack{\downarrow \\ \text{Factor para 43}}} \times \underbrace{(b^{4t} + 1)}_{\substack{\downarrow \\ \text{Factor para s}}} \dots$$

Es decir, los factores $b^{2^nt} + 1$ son divisibles para s .

En el caso de 3 y 43 únicamente se tiene 2 factores

6.10

$$n > 4 \text{ y } n = a \times b \rightarrow \frac{n}{(n-1)!}$$

① Caso : $p = \sqrt{n}$ y $n > 4$

$$p > 2 \rightarrow 2p < p^2 = n$$

entonces

$$p \leq n-1 \text{ y } 2p \leq n-1$$

$$2n = p \times 2p \mid (n-1)! - n \mid (n-1)!$$

LQPD

② Caso :

$$p < \sqrt{n} \rightarrow n/p > \sqrt{n}$$

$$\text{entonces } p \leq n-1 \text{ } n/p \leq n-1$$

$$n = p \times n/p \mid (n-1)! \rightarrow n \mid (n-1)!$$

LQPD

b.11

$$b \equiv t^2 \pmod{n}$$

$n \rightarrow$ Impar

b y $n \rightarrow$ primos relativos

$$35 \equiv t^2 \pmod{11}$$

$$t^2 \equiv 26 \pmod{11}$$

$$t^2 \equiv 35 \pmod{11}$$

$$t^2 \equiv 4 \pmod{11}$$

$$t^2 \equiv 2 \therefore \underline{\text{no es}}$$

$$\boxed{t \equiv 2}$$

Comprueba siempre y cuando "b" sea par y primo relativo de "n".

b.12

$$b^{(n-1)/2} \equiv 1 \pmod{n} - b \quad y \quad n \text{ impares y primos}$$

$$\frac{n-1}{2} \equiv 1 \rightarrow b \text{ debe ser primo e impar de la forma } 2p+1$$

$$n-1 \equiv 2$$

$$n \equiv 3 \quad n = 2p+1 \rightarrow \text{forma impar}$$

$$2p+1 = 3$$

$$p = 1 \rightarrow 2p = 2 \quad y \quad n \geq 3$$

∴ Si $n=3$ y b cumple que sea primo e impar entonces se cumple la igualdad a demostrar.

b.13

b y n son primos relativos

$$b \equiv t^2 \pmod{n}$$

$$n \rightarrow \text{dnde } a \quad b^{\frac{(n-1)}{2}} \equiv -1$$

$$b^{\frac{(n-1)}{2}-1}$$

$$\text{Utilizando el resultado de } \frac{26^5 - 1}{11} = \underbrace{1080125}_{\text{entero}} \rightarrow \text{entero}$$

6.11

en donde $b=26$

$n=11 \rightarrow$ verificar que al ser primo relativo se cumple

$$\frac{b^{\frac{(n-1)}{2}} - 1}{n} \rightarrow \text{es entero}$$

6.14

$$b^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n} \Rightarrow S(n)$$

→ Encontrar n para que $S(n)$ -es \Rightarrow $\frac{\phi(n)}{2} = 1$

$$\phi(n) = n - 1$$

$$\frac{(n-1)}{2} \neq 1$$

$$n \neq 3$$

∴ Cuando n no sea congruente con $3S(n)$
⇒ falso

6.15

$$S(n) \quad n=18 \quad \phi(18) = 6$$

$$\phi(18) = 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1$$

$$\therefore \phi(18) = 6$$

$$S(18)$$

$$S(18) = b^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$$

$$17^{\frac{6}{2}} \equiv 1 \pmod{18} \equiv 7$$

$$13^{\frac{6}{2}} \equiv 1 \pmod{18} \equiv 7 \quad \text{No cumple}$$

$$11^{\frac{6}{2}} \equiv 1 \pmod{18} \equiv 7$$

6.16

Si. $b^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$ entonces

$$b \equiv (b^k)^2 \pmod{n}$$

$$k \equiv \frac{\phi(n)+2}{4} \rightarrow \phi(n) \equiv 4k-2$$

$$b^{\frac{(4k-2)/2}{2}} \equiv 1 \pmod{n}$$

$$b^{2k} - b \equiv 1 \pmod{n}$$

$$-b \equiv b^{2k} \pmod{n}$$

$$b \equiv (b^k)^2 \pmod{n}$$

□ Q.D.

6.17

Probar: $s(n)$ es verdadero si y solo si 4 divide a $\phi(n)$

$$11^4 \equiv 1 \pmod{9} \equiv 7 \quad \therefore \text{no cumple}$$

Como se puede ver en este problema y en el 6.15

$s(n)$ no cumple si $\phi(n)$ es múltiplo de 4 .

$$2^{170} \equiv 1 \pmod{341} \rightarrow \text{Sí cumple}$$

Sí y solo si $\phi(n)$ no es divisible para 4 .

6.18

$$s(n) = b^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$$

$$\prod_{n \geq 3} s(n) \mid s(n)$$

$\forall n \geq 3$ como se demostró en 6.14 $s(n)$ es falso cuando n no sea congruente a 3 .

Entonces para que $s(n)$ sea Verdadero, $n \geq 3$

6.19

Prueba: $s(n)$ se cumple si y solo si $\prod_{n \geq 3} s(n)$ no es congruente con $1 \pmod{n}$

$$\phi(n) = 11, 16, 9, 8, 7, 6, 5, 4, 3, 2, 1 = 4$$

$$\prod_{n \geq 3} s(n) = 11 \times 7 \times 5 \times 1 = 385$$

$$5^{4/2} = 1 \pmod{12} = 1 \pmod{12} \rightarrow \text{LQD}$$

6.20

n compuesto hasta 30 , $s(n)$ es verdadero

$s(n)$ es verdadero para todo $(\forall n \geq 3 \wedge n < 30)$

6.21

p, q son primos impares distintos

$$\frac{n}{p}, \frac{n}{q} \quad n = pq \quad n = x^2 - y^2 \quad x = \frac{a+b}{4} \quad y = \frac{a-b}{4}$$

$$\therefore n = \frac{(x-y)(x+y)}{pq} \quad n = \left(\frac{a+b}{4} - \frac{a-b}{4}\right) \left(\frac{a+b}{4} + \frac{a-b}{4}\right)$$

$$n = \left(\frac{b-a}{4}\right) \left(\frac{a+b}{4}\right) \quad \therefore \text{divide } \frac{1}{4}n.$$