

# Quadratic Reciprocity

Universidad de Cuenca

**Optativa 6 - Criptología**

Dr. Diego Ponce

Capítulo 7

Freddy L. Abad L.

[freddy.abadl@ucuenca.edu.ec](mailto:freddy.abadl@ucuenca.edu.ec)

## CAP 7

7.1

$$\begin{aligned} * \frac{35}{53} &= (18/35) \\ &= -(9/35) \\ &= -(8/9) \\ &= -(4/9) \\ &= -(2/9) \\ &= -(1/9) \\ &= -1 \end{aligned}$$

$$\begin{aligned} \leftarrow \frac{126}{5039} &= (63/5039) \\ &= (-62/63) \\ &= (-31/63) \\ &= (1/31) \\ &= (1) \end{aligned}$$

$$\begin{aligned} * \frac{68}{1233} &= (34/1233) \\ &= (17/1233) \\ &= (12/17) \\ &= (6/17) \\ &= (3/17) \\ &= (2/17) \\ &= (-1/3) \\ &= -1 \end{aligned}$$

$$\begin{aligned} * \frac{67^2}{1297} &= (336/1297) = (68/1297) \\ &= (84/1297) = (42/1297) \\ &= (21/1297) = (6/21) \\ &= (8/21) = (4/21) \\ &= (2/21) = (1/2) = 1 \end{aligned}$$

$$\begin{aligned} * \frac{1235}{3499} &= -(1029/1235) = -(206/1029) \\ &= (103/1029) = (102/103) \\ &= (51/103) = -1/50 \\ &= -1 \end{aligned}$$

7.2

 $p \rightarrow$  es impar

$$(2/p) = (-1)^{\frac{(p^2-1)}{8}}$$

Probar: Si  $(p^2-1)/8$  es primo  $\rightarrow p \equiv 1 \pmod 8$   
 y si es impar  $p \equiv 3 \pmod 8$

$$\frac{p^2-1}{8} \equiv 1 \pmod 8$$

 $\therefore p$  debe ser impar

$$p^2 \equiv 8 \pmod 8$$

$$p^2 \equiv 1 \pmod 8$$

$$\underbrace{p \equiv 1 \pmod 8}_{\text{}} //$$

$$\frac{p^2-1}{8} \equiv 3 \pmod 8$$

$$(2n-1)^2 - 1 \equiv 3 \pmod 8$$

$$(2n-1)^2 \equiv 4 \pmod 8$$

$$2n \equiv 2 \pmod 8 \rightarrow p \text{ debe ser par}$$

$$2n \equiv 3 \pmod 8$$



7.3 Si  $p$  es primo impar

$$(3/p) = 1 \text{ si } p \equiv 1 \text{ ó } -1 \pmod{12}$$

$$(3/p) = -1 \text{ si } p \equiv 5 \text{ ó } -5 \pmod{12}$$

$$\frac{3}{p} \equiv 1 \pmod{12}$$

$$p = \frac{3}{1 \pmod{12}}$$

$$\frac{3}{p} \equiv 5 \pmod{12}$$

El valor de  $p$   
en cada caso

$$p = \frac{3}{5 \pmod{12}}$$

7.4 Cuando  $\frac{5}{p} \equiv 1$

$$\frac{5}{p} \rightarrow p \equiv 5 \text{ ó } -5 \pmod{12}$$

7.5  $p$  y  $q$   $\rightarrow$  primos distintos

$q \times a - p \times a' \rightarrow a$  y  $a'$  se ejecutan sobre los impares positivos menores de  $q$  y  $p$ .

Si  $p$  y  $q$  son impares tienen la forma  $(2n-1)$

$$q = 2n-1 \quad p = 2m-1 \quad na=x \\ ma'=y$$

$$2na - a - 2ma' - a'$$

$$2na - 2ma' = a + a'$$

$$2x - 2y = a + a'$$

Forma de un numero par ( $2z$ )

Por lo tanto, el resultado será un número

par //

LQD

7.6

$$(267980114647621) = -1$$

$$(1073899138149201) = -1$$

$$(638291631909482089) = 1$$

$$(3810026541468298937) = 0$$

$$(8377201726119372762237) = 1$$

7.7

Existe un  $n \rightarrow 1009 / n^2 - 150$

$$\frac{1009}{n^2 - 150} = 1$$

$$1009 = n^2 - 150$$

$$n^2 - 150 = 1009$$

$$n = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{150 \pm \sqrt{150^2 - 4(1)(-1009)}}{2}$$

$$n_1 = 156,44$$

$$n_2 = -6,44$$

7.8

$$p = x^2 + 1$$

$$\begin{aligned} &\rightarrow s \rightarrow p \\ &\rightarrow x \rightarrow 2 \\ &\rightarrow 17 \rightarrow p \\ &\rightarrow x \rightarrow 4 \end{aligned} \quad \left. \right\}$$

7.9

a entero  
p primo

$$p / x^2 + ay^2$$

$$x^2 + ay^2 = (x + c + ay)(x - c - ay)$$

$$\text{Se cumple para todo } c = \sqrt{2xy} \left(\frac{a}{2}\right)$$

$$c = \sqrt{xya}$$

$$xya = -a \bmod p$$

$$xy = -1 \bmod p.$$

$a, x, y$  deben ser enteros y  $p$  debe ser primo UQ9D

7.10  $p = 2m + 1 \rightarrow$  Número impar primo  
 $3, 5, 7, 13$

$$10^m - 1 \equiv 2m + 1$$

$$10^m \equiv 2(m+1)$$

$$\frac{10^m}{2} \equiv m+1$$

$$5(10^{m-1}) \equiv m+1$$

$$10^{m-1} \equiv \frac{m+1}{5}$$

∴ Cumple cuando  $p=5$ , LQQ.D

7.11 a) m divide  $n^{\phi(m)/2} - (n/m)$

$$m=3 \quad \text{y} \quad n=5$$

$$5^{2/2} - \frac{5}{3}$$

$$5 - \frac{5}{3}$$

$$m \mid 5 - \frac{5}{3}$$

$\Rightarrow$  Número racional | m no divide a este resultado

b) m divide  $n^{\phi(m)/2} - \frac{n}{m}$

como  $\phi(m) = m-1 \rightarrow$  Obtenemos el mismo resultado a demostrar que en a

c) Si  $\frac{n}{m} = 1$

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

Para que  $\frac{n}{m}$ , n debe ser igual a m y ya que no cumple con el enunciado del Ej. por ende no existe un t que cumple la congruencia

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

7.12  $n \rightarrow$  es pseudo ríos cuadrado

7.13 la probabilidad de elegir un número cuadrado o pseudo-cuadrado depende del algoritmo implementado para realizar esta función

7.14 Cuadrados perfectos hasta 1 millón  
1000

Pseudo cuadrado perfectos hasta 1 millón  
1000

7.15 public int[] ~~verificar Pseudocuadrado~~ (int n, int p)  
{  
    n = n % p;  
    if (n == 0)  
        return 0;  
    if (n < 0)  
        return (n + 1) % p;  
    else  
        return n / 2 % p;  
}

7.16 Si  $p$  es impar, entonces  $\frac{p^2 - 1}{8}$  es impar  
sí y solo si  $p \equiv 3 \pmod{8}$  o  $-3 \pmod{8}$

$$\textcircled{1} \quad \frac{p^2 - 1}{8} = \frac{q - 1}{8} = \frac{1}{8} = 1 \rightarrow \text{Impar}$$

$$\textcircled{2} \quad \frac{p^2 - 1}{8} = \frac{(-3)^2 - 1}{8} = \frac{8}{8} = 1 \rightarrow \text{Impar}$$

7.17 Si  $p$  y  $q$  son impares entonces

$$\frac{(p-1)(q-1)}{4}$$

$$p = 2m + 1 \quad q = 2n + 1 \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{Forma impar}$$

$$\frac{(2m+1-1)(2n+1-1)}{4} = \frac{4mn}{4} = mn \rightarrow \text{Si } p \text{ y } q \text{ son impares se cumple}$$

7.18

Probar  $\frac{3}{m} = 1$  si y solo si  $m \equiv \pm 1 \pmod{12}$

$m$  no es múltiplo de 203.

$p = 12m + 1 \rightarrow$  Por Corolario 7.5

$$3 \times 1, 3 \times 3, \dots, 3 \times (4m-1)$$

$$3 \times (8m+1), 3 \times (8m+3), \dots, 3 \times (10m-1)$$

$$3 \times (4m+1), 3 \times (4m+3), \dots, 3 \times (8m-1)$$

$$\frac{3}{p} = 1 \text{ si y solo si } p \equiv 1 \text{ o } -1 \pmod{12}$$

$\frac{1}{4}$

Por Corolario 7.6

$$\rightarrow \frac{3}{p} = -1 \text{ si y solo si } p \equiv 5 \text{ o } -5 \pmod{12}$$

QED

7.19

$$\frac{7}{p} = 1$$

Condiciones para que sea un Número de Jacobi.

$$-\frac{7}{28} = \frac{p}{28} \rightarrow 7 \equiv p \pmod{28}$$

$$-\frac{1}{28} = 1 \quad y \quad \frac{0}{28} = 0$$

$$-\frac{2p}{28} = \frac{p}{28}$$

$$\text{Si } 28 = \pm 1 \pmod{28}$$

Las condiciones anteriores deben darse para encontrar las clases de residuo  $p$  del símbolo de Legendre  $\frac{7}{p} = 1$

7-20

porque en el Algoritmo 7.9 es necesario el Algoritmo 1.7 para encontrar los cuadrados perfectos

No se utiliza directamente la función pero se b puede localizar en QUAD-REC-WOP.

$$\text{if } (n-1) \times (p-1) \bmod 8 = 4$$

$$\text{legendre} = 1 \times \text{legendre}$$

$$\text{temp} = n$$

$$n = p \bmod n$$

$$p = \text{temp}$$

y

Algoritmo 7.9

while  $b \neq 0$

$\rightarrow \text{temp} = b$   
     $\rightarrow b = a \bmod b$   
     $\rightarrow a = \text{temp}$

y

Algoritmo 1.7.

Aquí se puede notar el encadenamiento de los temas.

Loop

Freddy L. Abad L.

freddy.abad@ucienca.edu.pe