CONGRUENCIA LA UNIDAD

Nº inscripción :00/2000/3213.-Sección 1
R.P.I.- VA-2060

PROCEDIMIENTOS PARA CONOCER LOS CUADRADOS QUE GENERAN COMO RESTO LA UNIDAD

Además de 1^2 y $(N-1)^2$,para todo "N" impar, compuesto ,positivo ,han de existir como mínimo 2 cuadrados que generen " 1 " como resto cuadrático .

Para su cálculo empleamos 4 procedimientos :

a).- Calculándolo en función de los cuadrados que generan como resto N – 1.

b).- Hallando la diferencia entre dos cuadrados ,que tienen como característica común ,tener como congruencia sus respectivas bases , módulo N.

c).- En función de 1^2 ó $(N-1)^2$.

d).- En función de los cuadrados de Fermat .

Método " a "

$N = x \cdot y$ $\qquad$ $N = a^2 + b^2$

planteamos la ecuación indeterminada,

$$N c - b = e \cdot a$$

elevamos al cuadrado , ponemos " b al cuadrado " , en función de " a al cuadrado " ,dividimos por " a^2 "

$$N \frac{N c^2 - 2 c b + 1}{a^2} - 1 = e^2 \text{ , recordemos que , } N = a^2 + b^2$$

podríamos pensar que " a " tiene algún factor común con " N " , en este caso ,lo tendría también " b ". Dividiríamos " a " " b " , por el factor , y " N " por el cuadrado del mismo.

Según lo arriba expuesto ,

$$e^2 \equiv (N-1) \pmod{N}$$

Empleando el mismo planteamiento :

$$N d - a = f b \qquad \frac{N d - a}{b} = f$$

1

$f^2 \equiv (N-1) \pmod{N}$; es decir que $e \cdot f^2 \equiv 1 \pmod{N}$

Método " b "

Para todo $N = x \cdot y$, se trata de buscar 2 parejas de números consecutivos que tengan como factores entre otros , " x " e " y " .

$N = x \cdot y$ $\quad a x + 1 = b y$ $\quad d x = e y + 1$

$(b y)^2 \equiv b y \pmod{N}$ $\quad (d x)^2 \equiv dx \pmod{N}$

$(b y - dx) \equiv 1 \pmod{N}$

Método " c "

Este método es valido para cualquier resto cuadrático .

$N = X \cdot Y$ $\quad C^2 \equiv R \pmod{N}$ $\quad (N + C)^2 \equiv R \pmod{N}$

se trata de encontrar otros cuadrados que generen el mismo resto cuadrático. Le llamaremos C (1) ,

$C(1) = (b X - C)^2 \equiv R$ $\quad b X$ puede ser < ó ´> que N

$(N + C)^2 - (b X - C)^2 = N d$, elevamos al cuadrado ,

$N^2 + 2 C N - b^2 X^2 + 2 b X C = N d$

para que sea válida ,tiene que darse que .

$(2 b X C - b^2 X^2) \equiv 0 \pmod{N}$

como quiera que,

$(2 b X C - b^2 X^2) = (b X - C)^2 - C^2$

$(b X - C)^2 \equiv R \pmod{N}$

empleando el mismo proceso,

$(a Y + C) \equiv R \pmod{N}$

Método " d "

En función de los cuadrados de Fermat :

$N = x \cdot y$ $\quad C(1)^2 - N = C(2)^2$ $\quad b \cdot N - C(1) = a \cdot C(2)^2$

“ a^2 “ es congruente “ 1 “ , módulo “ N “

EJEMPLO : N = 617 x 101 = 206^2 + 141^2 = 174^2 + 179^2

Método “a”

62.317 c - 141 = 206 e

e = 5747

62.317 d - 179 = 174 f

f = 12534 5747 x 12534 ≡ 56.763 (mod.62317)

$56.763^2 \equiv 1$ (mod.62.317)

206

105	1
35	69
7	55
1	155
141	19

Método “b”

617 a + 1 = 101 b b=336 336 x 101 = 33936

617 a = 101 b + 1 a= 46 46 x 617 = 28382

$33936 - 28382 = 5554$; $5554^2 \equiv 1$ (mod. 62317)

Método “c”

617 a - 2 = 101 b b = 562 (562 x 101) + 1 = 56.763

$56.763^2 \equiv 1$ (módulo 62.317)

Método “d”

62317 b - 258 = 359 a a = 5554

$5554^2 \equiv 1$ (mód. 62.317)

3