Radici quadrate Mod n

Supponiamo che la congruenza quadratica sia $x^2 \equiv 71 \pmod{77}$

in generale $x^2 \equiv y \pmod{n}$

Voglio trovare $X \equiv \sqrt{y} \bmod n$

y intero

supponiamo inoltre che $n = p \times q$ con p e q primi.

In generale la radice quadratica si può risolvere se si conosce la fattorizzazione di n; e viceversa se si conoscono tutte le soluzioni allora è facile fattorizzare n.

Cominciamo con $n = p$. Il caso più semplice è

$$\boxed{p \equiv 3 \pmod{4}}$$

(Il caso $p \equiv 1 \pmod{4}$ è più difficile)

Sia $p \equiv 3 \pmod{4}$ e voglio trovare la rad. q. di y mod p

$$x^2 \equiv y \pmod{p} \qquad x \equiv y^{\frac{p+1}{4}} \pmod{p}$$

1. Se y ha una radice quadrata mod p, allora ha due radici quadrate $= \pm x$.

sono

2. Se y non ha radici quadrate mod p allora $-y$ ha una radice quadrata mod p e le due radici di $-y$ sono $\pm x$.

Se $y \not\equiv 0 \pmod p$ allora per Fermat

$$y^{p-1} \equiv 1 \pmod p$$

per cui $x = y^{\frac{p+1}{4}}$

$$x^4 \equiv y^{p+1} \equiv y^2 y^{p-1} \equiv y^2 \pmod p$$

$$\bullet\ x^4 \equiv y^2 \pmod p$$

allora $(x^2+y)(x^2-y) \equiv 0 \pmod p$ e quindi

$$x^2 \equiv \pm y \pmod p$$

per cui almeno uno di y e $-y$ è un quadrato mod p.

Se lo sono tutti e due y e $-y$ quadrati

$$y \equiv a^2$$

$$-y \equiv b^2$$

allora $-1 \equiv \left(\frac{a}{b}\right)^2$ e -1 è un quadrato mod p

questo è impossibile x $p \equiv 3 \pmod 4$

Per cui esattamente solo uno di $-y$ e y

ha una radice quadrata mod p.

- Se y allora $y \equiv x^2$ e le due radici di y sono $\pm x$
- Se $-y$ allora $-y \equiv x^2$.

Trova la radice quadrata di

$y \bmod p = 5 \bmod 11 = x^2$ $\quad p = 11$, $p \equiv 3 \pmod 4$

allora

$\frac{p+1}{4} = 3$ calcoliamo:

$\boxed{x \equiv y^{\frac{p+1}{4}} \pmod p} \longrightarrow x \equiv 5^3 \equiv 4 \pmod{11}$

Poiché

$4^2 \equiv 5 \pmod{11}$ $\quad x^2 \equiv y$

le radici quadrate di $\underline{5 \bmod 11}$ sono $\pm 4 = x$

$y \bmod p = 2 \bmod 11 = x^2$ $\quad y \equiv 2 \bmod 11$

$x = y^{\frac{p+1}{4}}$ $\quad x \equiv 2^3 \bmod 11 \equiv 8$

$8^2 \equiv 9 \equiv -2 \pmod{11}$

allora è $\longrightarrow \boxed{x^2 \equiv -y}$ la radice quadrata di -2 sono: $\underline{\pm 8} = x$

~~2 nulla radici y. mod 11~~

Radici Quadrate

$\boxed{n = p}$

4

- 2 RADICI QUADRATE DI y (mod p)

Quindi se $x^2 \equiv y \bmod p$

con $\frac{p+1}{4}$ = intero e cioè $p \equiv 3 \pmod 4$

allora $y^{\frac{p+1}{4}} \equiv x \pmod p$

e allora $\begin{cases} \text{o } y \text{ ha 2 radici quadrate } \pm x \\ \text{o } -y \text{ ha 2 radici quadrate } \pm x \end{cases}$

Caso $\boxed{n = p \times q}$ ove $p \equiv q \equiv 3 \pmod 4$

$x^2 \equiv y \pmod n$

$\text{mcd}(y, n) = 1$

$\boxed{\text{4 RADICI QUADRATE}}$ se $y \perp n$!

se k fattori 2^k radici quadrate

e y ha radici quadrate mod n

Allora calcolare le 4 soluzioni

$\rightarrow x \equiv \pm a, \pm b$ di

di

$x^2 \equiv y \pmod n$

è computazionalmente equivalente a fattorizzare n.

(4BIS)

PRINCIPIO $n = pq$ dispari e $p \equiv q \equiv 3 \pmod 4$

$y \perp n$ e ha radici quadrate mod n

Trovare le 4 soluzioni $\boxed{x = \pm a, \pm b}$ di

$$x^2 \equiv y \pmod n$$

è computazionalmente equivalente a fattorizzare n

date le soluzioni si fattorizza semplicemente

e viceversa dato la fattorizzazione si trovano semplicemente le soluzioni

Esempio $p=7;\ q=11$

$n=77=7\times 11$

$7\equiv 11\equiv 3 \pmod 4$

$y=71$

$$\boxed{x^2=71 \pmod{77}}$$

$$\begin{cases} x^2\equiv 71\equiv 1 \pmod 7 \\ x^2\equiv 71\equiv 5 \pmod{11}\end{cases}$$

teorema del resto cinese

allora

$$x\equiv \pm 1 \pmod 7$$
$$x\equiv \pm 4 \pmod{11}$$

infatti $1^{\frac{7+1}{4}}\equiv x\equiv y^{\frac{p+1}{4}}$

$1^1\equiv x^2$

$x\equiv \pm 1 \pmod 7$

$$x\equiv 5^{\frac{11+1}{4}}\equiv 5^3\equiv 4 \pmod{11}$$
$$x^2\equiv 4^2 \pmod{11}$$

allora $x\equiv \pm 4 \mod 11$

e quindi le 4 radici sono

$$\begin{cases} x\equiv \pm 1 \pmod 7 \\ x\equiv \pm 4 \pmod{11}\end{cases}$$

ict CONSULTING

Soluz.

altro

(A) $x \equiv 1 \pmod 7$; $x \equiv 4 \pmod{11}$ → 15

(B) $x \equiv 1 \pmod 7$; $x \equiv -4 \pmod{11}$ → 29

(C) $x \equiv -1$ 〃 $x \equiv 4$ 〃 → −29

(D) $x \equiv -1$ 〃 $x \equiv -4$ 〃 → −15

(mod 77)

---

teorema del resto cinese p e q primi dispari

p>q $\begin{cases} x \equiv a \bmod q \\ x \equiv b \bmod p \end{cases}$

caso (A) $x \equiv 1 \bmod 7$ $b=1$ $p=7$

$x \equiv 4 \bmod 11$ $a=4$ $q=11$

		0	1
		1	0
1	$11 = 1 \times 7 + 4$	−1	1
2	$7 = 1 \times 4 + 3$	2	−1
3	$4 = 1 \times 3 + 1$	−3	2
4	$3 = 3 \times 1 + 0$	11	−7

p<q

la prima $x = atp + bsq$

mcd(p,q) = 1

$tp + sq = 1$

$-3 \cdot 7 + 2 \cdot 11 = 1$

$x = -4 \cdot 3 \cdot 7 + 1 \cdot 2 \cdot 11 = -62 = 15 \bmod 77$

$-84 + 22$

CONSULTING

7

la seconda $X \equiv 1 \mod 7$ $b=1$

$X \equiv -4 \mod 11$ $a=-4$

$-3 \cdot 7 + 2 \cdot 11 = 1$

$X \equiv 4 \times 3 \times 7 + 1 \times 2 \times 11 = 106 \mod 77$

$84 + 22 = 29 \mod 77$

$X = 29$

la terza $X \equiv -1 \mod 7$ $b=-1$

$X \equiv 4 \mod 11$ $a=4$

$-3 \cdot 7 + 2 \cdot 11$

$-4 \times 3 \times 7 - 1 \times 2 \times 11 = -106 \mod 77$

$- \qquad = -29 \mod 77$

$X = -29$

la quarta $b=-1$

$a=-4$

$4 \times 37 - 1 \times 2 \times 11 = 62 \mod 77$

$84 - 22 = -15 \mod 77$

ok!

Supponiamo che $\underline{n} = p \times q$ primi distinti $p \equiv q \equiv 3 \pmod 4$

avremo le 4 soluzioni

$$\begin{cases} x = \pm a \\ x = \pm b \end{cases} \quad \text{di } x^2 \equiv y \pmod n$$

ma

$$\left.\begin{array}{l} \sigma \begin{cases} a \equiv b \pmod p \\ a \equiv -b \pmod q \end{cases} \\ \text{ovvero} \\ \sigma \begin{cases} a \equiv b \pmod q \\ a \equiv -b \pmod p \end{cases} \end{array}\right\} \text{Risulta ora}$$

ad esempio $n = 77$

$\underline{x^2 \equiv 71 \bmod 77}$ $\quad p = 7 \quad q = 11$

ho 4 soluzioni $\begin{cases} x = \pm 15 \\ x = \pm 29 \end{cases}$ $\quad 15^2 \equiv 29^2 \equiv 71 \pmod{77}$ $\quad \dfrac{b = 15}{\underline{a = 29}}$

sappiamo che $\begin{cases} 15 \equiv 29 \bmod 7 \equiv 1 \bmod 7 \\ 15 \equiv -29 \bmod 11 \equiv 4 \bmod 11 \end{cases}$

Allora $p \mid (a-b)$ e $q \nmid (a-b)$ oppure l'altro!

QUINDI $\underline{\text{mcd}[(a-b), n] = p}$ **BINGO!**

$a - b = 29 - 15 \equiv 14 \bmod 77 \quad 14 = 2 \times 7 \quad n = 7 \times 11$ Primo Base della fattorizzazione

Crittosistema di Rabin

$n = p \times q \qquad p = 3\,;\ q = 19 \qquad n = 57$

$p, q \equiv 3 \pmod 4$

Alice cifra $P = 7$ e manda

$$C \equiv P^2 \equiv 49 \pmod{57}$$

Bob conosce p e q e decifra

$$a^2 \equiv 49 \equiv 11 \mod 19$$

$$b^2 \equiv 49 \equiv 1 \mod 3$$

$$\begin{cases} a = 11^{\frac{19+1}{4}} \equiv 11^5 \equiv 7 \mod 19 \\ b = 11^{\frac{3+1}{4}} \equiv 1 \mod 3 \end{cases}$$

$$\pm a \equiv \pm 7 \pmod{19}$$

$$\pm b \equiv \pm 1 \pmod 3$$

$$p^{-1} = 3^{-1} \mod 19 \equiv 3^{17} \equiv 13 \pmod{19}$$
$$\equiv -6$$

$$q^{-1} \equiv 19^{-1} \mod 3 \equiv 19 \equiv 1 \pmod 3$$

$x_1 \begin{cases} a = 7 \\ b = 1 \end{cases} \qquad k = (a-b)\,p^{-1} \mod q = 6 \cdot 13 \equiv 78$
$\equiv 2 \mod 19$

②

$x_1 = b + pk = 1 + 3\cdot 2 \equiv 7 \mod 57$

$x_1 \equiv 7$

$x_2 \begin{cases} a = 7 \\ b = -1 \end{cases}$ $\quad k \equiv 8\cdot 13 \equiv 104 \equiv 9 \mod 19$

$x_2 = b + pk \equiv -1 + 3\times 9 \equiv 26 \pmod{57}$

infatti $26^2 \equiv 49 \pmod{57}$

$x_3 \begin{cases} a = -7 \\ b = 1 \end{cases}$ $\quad k \equiv (-8)\cdot 13 \equiv 11\cdot 13 \equiv 143 \equiv$

$\equiv 10 \mod 19$

$x_3 = 1 + 3\times 10 \equiv 31 \mod 57$

$31^2 \equiv 49 \mod 57$

$x_4 \begin{cases} a = -7 \\ b = -1 \end{cases}$ $\quad k \equiv (-6)\cdot 13 \equiv 13\cdot 13 \equiv 169 \equiv 17 \pmod{19}$

$\left.\begin{array}{l} x_4 = -1 + 3\times 17 \equiv 50 \\ 50^2 \equiv 49 \mod 57 \end{array}\right\} \mod 57$

allora delle 4 soluzioni

$[7, 26, 31 (\equiv -26), 50 (\equiv -7)] \mod 57$

solo 7 è una lettera $0 \le 7 \le 25$

le altre Bob le scarta.

ok!

Simboli di Legendre e di Jacobi

$x^2 \equiv a \pmod p$ ha soluzione?
esistono le radici quadrate di a?

Se $p \equiv 3 \pmod 4$ [non vale per l'altra classe di $p>2$: $p \equiv 1 \pmod 4$]

allora $$s \equiv a^{\frac{p+1}{4}} \pmod p$$

Se a ha una radice quadrata, allora s è una di quelle e $s^2 \equiv a \pmod p$.
Altrimenti se
$$s^2 \not\equiv a \pmod p$$
a non ha radici quadrate.

<u>Proposizione</u> per $p>2$ <u>qualsiasi</u>!!

Sia p un primo dispari e $a \not\equiv 0 \pmod p$ intero. Allora

Fermat: elevando (1) al quadrato $a^{p-1} \equiv 1 \pmod p$

$$(1) \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

la congruenza
$$x^2 \equiv a \pmod p$$

ha soluzione, se e solo se:

$$(2) \quad a^{\frac{p-1}{2}} \equiv +1 \pmod{p}$$

Per dimostrare la (2). Sia α una radice primitiva modulo p, $\alpha \in \mathbb{Z}_p^*$. Allora

$$a \equiv \alpha^j \pmod{p}, \text{ per certi } j$$

<u>Se</u> $a^{\frac{p-1}{2}} \equiv 1$, allora

$$\alpha^{\frac{j(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} \equiv 1$$

Infatti $\quad j\frac{(p-1)}{2} \equiv 0 \pmod{(p-1)}$

e cioè j è PARI: $j = 2k$ $(k = 1, 2, 3 \dots)$

$$a \equiv \alpha^j \equiv (\alpha^k)^2 \pmod{p}$$

e cioè a è un quadrato mod p.

$$x^2 \equiv a \pmod p$$

Come si trova?

$p \equiv 3 \pmod 4$ oppure $p \equiv 1 \pmod 4$

a è un residuo quadratico ha radice

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

-1 non ha rq

$$a^{\frac{p+1}{4}} = s \quad \text{se} \quad s^2 \equiv a \pmod p \text{ ok}$$

altrimenti a non è residuo (e lo è $-a$)

Come si trova?

$p = 11$

$$x^2 \equiv 2 \pmod{11}$$

$$2^{\frac{11+1}{4}} = 2^3 \equiv 8 \bmod 11$$

$$8^2 \equiv 64 \equiv 9 \equiv -2$$

$$-2 \Rightarrow \equiv -8 \bmod 11 \equiv 3$$

$$3^2 \equiv 9 \bmod 11 \equiv -2$$

Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a \text{ è residuo quadratico mod } p \\ -1 & \text{se } a \text{ è un nonresiduo mod } p \end{cases}$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

$$\left(\frac{1}{p}\right) \equiv 1 \mod p$$

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \mod 8 \\ -1 & \text{se } p = \pm 3 \mod 8 \end{cases}$$

Simboli di Legendre

$p>0$ e $a \not\equiv 0 \pmod p$ intero $\Big\{ >0$ se $p|a$

simbolo di Legendre di a e p

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{se } x^2 \equiv a \pmod p \text{ \underline{HA} SOLUZIONE} \\ -1, & \text{se '' '' \underline{NON HA} ''} \end{cases}$$

LEGENDRE

Proprietà

1. se $a \equiv b \not\equiv 0 \pmod p$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{(uguaglianza)}$$

2. se $a \not\equiv 0 \pmod p$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

3. se $ab \not\equiv 0 \pmod p$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

4.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

---

e poi

$$\left(\frac{1}{p}\right) = 1 \quad \text{e} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \bmod 8 \\ -1 & \text{se } p \equiv \pm 3 \bmod 8 \end{cases}$$

<u>Esempio</u> sia $p=11$. $p \equiv 3 \pmod 4$

$\boxed{a \not\equiv 0, \bmod p}$ $x^2 \equiv a \pmod p$

$a \in \mathbb{Z}_{11} = \{0, \underline{1}, 2, \underline{3}, \underline{4}, \underline{5}, 6, 7, 8, \underline{9}, 10\}$

Risolvere i quadrati $\not\equiv 0 \bmod 11$ sono

$$x^2 \equiv a \not\equiv 0 \pmod p$$

- $\underline{x^2 \equiv 1 \pmod{11}}$ OK HA radici ± 1 <u>OK!</u>
- $x^2 \equiv 2 \pmod{11}$ $s = 2^{\frac{11+1}{4}} \equiv 2^3 \equiv 8 \pmod{11}$
  $s^2 = 64 \bmod 11 \equiv 9 \not\equiv 2$ non ha soluzione <u>NO</u>
- $\underline{x^2 \equiv 3} \pmod{11}$ $s = 3^3 \equiv 27 \equiv 5 \pmod{11}$
  $s^2 = 25 \bmod 11 \equiv 3$ <u>OK</u>! HA SOLUZIONE
- $\underline{x^2 \equiv 4} \pmod{11}$ $s = 4^3 \equiv 2^6 \equiv 64 \pmod{11} \equiv 1$
  <u>OK</u>! HA SOLUZIONE
- $\underline{x^2 \equiv 5} \pmod{11}$ $s = 5^3 \equiv 125 \equiv 4$
  $s^2 \equiv 16 \bmod 11 = 5$ <u>OK</u>!
- $x^2 \equiv 6 \pmod{11}$ NO
- $x^2 \equiv 7$ " NO
- $x^2 \equiv 8$ " NO
- $\underline{x^2 \equiv 9}$ " OK! SI
- $x^2 \equiv 10$ " NO

I quadrati mod 11 sono: 1, 3, 4, 5, 9.

Allora risulta che (6 e 7 non sono residui quadratici) 5

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = (-1)(-1) = +1$$

(e $6\times7=42$) e quindi

$$\frac{42}{11} = +1 = \left(\frac{9}{11}\right)$$ in quanto $42 \equiv 9 \pmod{11}$

e allora

$$\left(\frac{6}{11}\right)\left(\frac{7}{11}\right) = \left(\frac{42}{11}\right).$$ c.v.d.

Simboli di Jacobi

n <u>INTERO DISPARI COMPOSTO</u> $a \not\equiv 0 \pmod n$

e $mcd(a,n)=1$ $(a \perp n)$. Sia:

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$$

allora

$$\left(\frac{a}{n}\right) = \underbrace{\left(\frac{a}{p_1}\right)^{b_1}\left(\frac{a}{p_1}\right)^{b_2}\cdots\left(\frac{a}{p_r}\right)^{b_r}}_{\text{simboli di Legendre}}$$

Simbolo di Jacobi

$n = 135 = 3^3 \cdot 5$

$$\left(\frac{2}{135}\right) = \left(\frac{2}{3}\right)^3\left(\frac{2}{5}\right) = (-1)^3(-1) = +1$$

$\left.\begin{array}{l} x^2 \equiv 2 \pmod 3 \\ x^2 \equiv 2 \pmod 5 \end{array}\right\}$ <u>non</u> ha <u>soluzioni</u> $s = 2^1 \equiv 2 \rightarrow s^2 = 4 \neq 2$; $s = 5 \rightarrow s^2 = 25 \equiv 0 \not\equiv 2 \pmod 5$

Ma anche $x^2 \equiv 2 \pmod{135}$ non ha soluzioni in quanto con CRT fallisce (2 non ha soluzioni mod 5)

quindi

$$\left(\frac{2}{135}\right) = +1$$

Jacobi

135 composto

NON SIGNIFICA CHE $x^2 \equiv 2 \pmod{135}$ HA SOLUZIONI

Se invece $= -1$ ALLORA NON HA SOLUZIONE!

TEOREMA n dispari JACOBI

1. Se $a \equiv b \pmod{n}$ e $\mathrm{mcd}(a,n)=1$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

2. Se $\mathrm{mcd}(ab,n)=1$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

3. $$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

4. $$\left(\frac{2}{n}\right) = \begin{cases} +1 & \text{se } n \equiv 1 \text{ o } 7 \pmod{8} \quad (\pm 1) \\ -1 & \text{se } n \equiv 3 \text{ o } 5 \pmod{8} \quad (\pm 3) \end{cases}$$

5. $$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{se } m \equiv n \equiv 3 \pmod{4} \\ +\left(\frac{n}{m}\right) & \text{altrimenti} \end{cases}$$

LEGGE DELLA RECIPROCITA' QUADRATICA Gauss 1796

NOTA In genere non è vero che per n composto come in Legendre

PER n COMPOSTO $\Rightarrow$ JACOBI $\left(\frac{a}{n}\right) \equiv (-1)^{\frac{n-1}{2}}$ (Solovay–Strassen)

Legge della Reciprocità Quadratica

LAW of QUADRADIC RECIPROCTY

$p, q > 2$ primi dispari

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) =$$

$$= \begin{cases} -\left(\frac{p}{q}\right) & \text{se } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{altrimenti} \end{cases}$$

ESEMPIO

7411 è un residuo quadratico modulo 9283?

sia 7411 e 9283 sono primi $\equiv 3 \bmod 4$

allora $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right) =$

ma $1872 = 2^4\, 3^2\, 13$

$$= -\left(\frac{2}{7411}\right)^4 \left(\frac{3}{7411}\right)^2 \left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right)$$

$(-1)^4 (-1)^2$

$\left(\frac{2}{7411}\right)=-1$ 7411 mod 8 ≡ 3 $\left(\frac{3}{7411}\right)=-1$ $3^{7410} \bmod 7411 \equiv 3^{3705} \equiv$

$\equiv 7410 \equiv -1$

oppure

$1872 = 12^2 \times 13$

$(-1)^4=1$ $(-1)^2=1$

$$-\left(\frac{4}{7411}\right)^2\left(\frac{3}{7411}\right)^2\left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right)$$

mcd(12, 7411) = 1

$\boxed{\text{per } b \text{ primo con } p}$ (6) $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$

$$-\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1$$

essendo $\left(\frac{1}{p}\right)=1$ allora 7411 non è residuo quadratico

---

$$(4)\ \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

$$(5)\ \left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}\left(\frac{n}{m}\right)$$

6 TER

JACOBI

se $\left(\frac{a}{n}\right) = +1$, non è detto che a è un quadrato mod n !

se $\qquad = -1$, allora è certo che a non è un quadrato mod n

---

Calcolare $\left(\frac{107}{137}\right)$ $\qquad$ $137 = p$, $107 = q$

$\left(\frac{107}{137}\right) = +\left(\frac{137}{107}\right) =$ $\qquad$ $p \equiv 137 \equiv 1 \pmod 4 \not\equiv 3$, $q = 107 \equiv 3 \pmod 4$

$= \left(\frac{30}{107}\right) =$ $\qquad$ $137 \equiv 30 \pmod{107}$

$= \left(\frac{2}{107}\right)\left(\frac{15}{107}\right) =$

$= (-1)\left(\frac{15}{107}\right) =$ $\qquad$ visto che $\left(\frac{2}{107}\right) = -1$ dato $107 \equiv 3 \pmod 8$

$= \left(\frac{107}{15}\right) =$ visto che $107 \equiv 15 \equiv 3 \pmod 4$

$= \left(\frac{2}{15}\right) =$ visto che $107 \equiv 2 \pmod{15}$

$= +1$ $\qquad$ visto che $15 \equiv 7 \pmod 8$, $7 \not\equiv 3$

allora visto che 137 è primo 107 è un quadrato mod 137.

Mentre $\left(\frac{2}{15}\right) = 1$ <u>NON</u> vuol dire che 2 è quadrato mod 15 $15 = 3 \times 5$ composto (infatti NON è) se $n=pq$ e $\left(\frac{a}{n}\right)=-1$ allora a NON è quadrato mod n

Mentre se $\left(\frac{a}{n}\right)=1$ forse? a è quadrato mod n

QUADRATIC RESIDUOSITY PROBLEM

Poiché

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$ allora ci sono due possibilità!

o

(1) $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$ NO SOLUTION

o

(2) $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=+1$ SOLUTION

nel caso (1) a non essendo soluzione mod p, allora non può essere per il CRT soluzione mod $(p \times q)$.

nel caso (2) CRT ci dà la soluzione mod $(p \times q)$

~~Esercizi~~ SIMBOLI DI LEGENDRE e JACOBI

1

$n = 15$. Mostrare che

$$\left(\frac{2}{n}\right) \not\equiv 2^{\frac{(n-1)}{2}} \pmod n$$

si ha che

$$\left(\frac{2}{15}\right) = 1$$ dato che $15 \bmod 8 = 7$

e che $2^7 \bmod 15 = 8$ c.v.d.

~~Risolvere~~

Mostrare che

$$\left(\frac{3}{65537}\right) = -1$$

Si ha che

$$\left(\frac{3}{65537}\right) = \left(\frac{65537}{3}\right) =$$ dato che $65537 \bmod 4 = 1$

$= \left(\frac{2}{3}\right)$ dato che $65537 \bmod 3 = 2$

$= -1$ dato che $3 \bmod 8 = 3$

ESERCIZIO

Quali delle congruenze seguenti ha soluzione? (2)

(a) $x^2 \equiv 123 \pmod{401}$

(b) $x^2 \equiv 43 \pmod{179}$

(c) $x^2 \equiv 1093 \pmod{65537}$

401, 179 e 65537 sono PRIMI

(a) $\left(\frac{123}{401}\right) \overset{+}{=} \left(\frac{401}{123}\right) = \left(\frac{32}{123}\right) = \left(\frac{2}{123}\right)^5 = (-1)^5 = -1$

$123 \bmod 8 = 3$

con dispari $=123$, $\mathrm{mcd}(123, 401) = 1$

$123 \bmod 4 = 3$; $401 \equiv 32 \bmod 4$

$401 \equiv 32 \pmod{123}$

nessuna soluzione!

(b) $43 \bmod 4 = 3$, $179 \bmod 4 = 3$; $179 \equiv 7 \bmod 43$; $7 \bmod 4 = 3$, $43 \bmod 4 = 3$; $43 \bmod 7 = 1$

$$\left(\frac{43}{179}\right) = -\left(\frac{179}{43}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1$$

$\left(\frac{1}{7}\right) \equiv 1 \equiv 1 \equiv 1$

c'è UNA SOLUZIONE!

(c) $1093 \bmod 4 = 1$

$$\left(\frac{1093}{65537}\right) = \left(\frac{65537}{1093}\right) = \left(\frac{2}{1093}\right)\left(\frac{525}{1093}\right) = -\left(\frac{1093}{525}\right)$$

$\left(\frac{1050}{1093}\right) =$

$1093 \bmod 8 \equiv 5 \to -1$

$1093 \bmod 4 = 1$

$65537 \bmod 4 = 1$

$$= -\left(\frac{43}{525}\right) = \left(\frac{525}{43}\right) = -\left(\frac{9}{43}\right) = -1$$

$525 \bmod 43 = 9$

$\left(\frac{9}{43}\right) \equiv 9^{21} \equiv 1 \pmod{43}$

$1093 \bmod 525 = 43$

nessuna soluzione!

$401 = p$ 3

(a) $\left(\frac{123}{401}\right) = +\left(\frac{401}{123}\right) =$ essendo $123 \equiv 3 \pmod 4$ e $401 \equiv 32 \not\equiv 3 \pmod 4$

$= \left(\frac{32}{123}\right)$ essendo $401 \equiv 32 \bmod 123$

$= \left(\frac{2}{123}\right)^5 = (-1)^5 = -1$

essendo $123 \bmod 8 = 3$

Nessuna soluzione

$179 = p$

(b) $\left(\frac{43}{179}\right) = -\left(\frac{179}{43}\right) =$

$43 \bmod 4 = 3 = 179 \bmod 4$

$= -\left(\frac{7}{43}\right) =$ $179 \equiv 7 \pmod{43}$

$= \left(\frac{43}{7}\right) =$ $7 \bmod 4 = 3 = 43 \bmod 4$

$= \left(\frac{1}{7}\right) = 1$ $43 \bmod 7 = 1$ e $\left(\frac{1}{7}\right) = 1$

$1^{\frac{7+1}{4}} = 1^2 = 1$ $7 \equiv 3 \pmod 4$

c'è soluzione

(c) 65537 primo

$$\left(\frac{1093}{65537}\right) = \left(\frac{65537}{1093}\right) =$$ 65537 = 1 mod 4
1093 = 1 mod 4

$$= \left(\frac{1050}{1093}\right) =$$ 65537 mod 1093 = 1050

$$= \left(\frac{2}{1093}\right)\left(\frac{525}{1093}\right) =$$ 1050 = 2 x 525

$$= (-1)\left(\frac{525}{1093}\right) =$$ essendo 1093 mod 8 = 5

$$= -\left(\frac{1093}{525}\right) =$$ essendo 1093 mod 4 = 1
525 mod 4 = 1

$$= -\left(\frac{43}{525}\right) =$$ 1093 mod 525 = 43

$$= -\left(\frac{525}{43}\right) =$$ 525 mod 4 = 1:
43 mod 4 = 3

$$= -\left(\frac{9}{43}\right) = -1$$ 525 mod 43 = 9

in quanto $\left(\frac{9}{43}\right) \Rightarrow 9^{21} \equiv 1 \pmod{43}$

NESSUNA SOLUZIONE!