PREIMO 2011 - TdN POMERIGGIO

Titolo nota 26/05/2011

5. $p = 17^{2n} + 4 \qquad p \mid 7^{\frac{p-1}{2}} + 1$

$$7^{\frac{p-1}{2}} \equiv \left(\frac{7}{p}\right) \qquad \text{Tesi} \iff \left(\frac{7}{p}\right) = -1$$

$$\left(\frac{7}{p}\right) = \begin{cases} 1, & \text{se } 7 \text{ quadr. mod } p \\ 0, & \text{se } p \mid 7 \\ -1, & \text{se } 7 \text{ non } " \quad " \end{cases}$$

Se $7 = \square$ $\quad 7 \equiv g^2 \ (p) \quad 7^{\frac{p-1}{2}} \equiv g^{p-1} \equiv 1 \ (p)$

$7 \equiv g^d \pmod p \qquad 7^{\frac{p-1}{2}} \equiv g^{d\left(\frac{p-1}{2}\right)} \equiv \left(\frac{7}{p}\right) \ (p)$

RECIPROCITÀ QUADRATICA

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

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

$$-1 \overset{?}{=} \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{17^{2n}+4}{7}\right) = \left(\frac{9^n+4}{7}\right) = \left(\frac{2^n+4}{7}\right)$$

$n \equiv 1, \quad n \equiv 2, \quad n \equiv 0 \pmod 3$

$\left(\frac{6}{7}\right) = -1 \qquad \left(\frac{5}{7}\right) = -1$

$n \equiv 2 \to \left(\frac{8}{7}\right) = 1$

Se $n \equiv 2 \pmod 3$? $\qquad 17^{2n} + 4$

$13 \mid 17^{2n} + 4$

$$4 + 17^{2n} \equiv 4 + 4^{2(3k+2)} \equiv$$

$$\equiv 4 + 4^4 \pmod{13}$$

$$1 + 4^3 = 65 = 5 \cdot 13$$

Esercizio 6

$a^n + a^{n-1} + \dots + a + 1 \mid a^{n!} + a^{(n-1)!} + \dots + a^{1!} + 1$

Dato $n \to$ infiniti valori di a

$A(x) = x^n + x^{n-1} + \dots + x + 1$

$B(x) = x^{n!} + x^{(n-1)!} + \dots + x^{1!} + 1$

$B(x) = Q(x) A(x) + R(x)$

$\deg R < \deg A \qquad$ (oppure $R = 0$).

$A(a) \mid B(a)$ per ∞ a.

$x = a \qquad B(a) = Q(a) A(a) + R(a)$

$A(a) \mid R(a)$ per ∞ a

$\Rightarrow R(a) = 0$ per a "grande".

Questo dice che il polinomio $R(x)$ è identicamente nullo

$$B(x) = Q(x)\,A(x)$$

$$C(x) = x^{c_n} + x^{c_{n-1}} + \dots + x^{c_1} + 1$$

Quando è divisibile per $A(x)$?

$$c_n = q_n(n+1) + r_n$$

$$x^{c_n} = x^{(n+1)q_n} \cdot x^{r_n} \equiv x^{r_n} \pmod{A(x)}$$

$$x^{n+1} - 1 = (x-1)\underbrace{(x^n + x^{n-1} + \dots + x + 1)}$$

È divisibile $\Leftrightarrow$ $x^{r_n} + x^{r_{n-1}} + \dots + x^{r_1} + 1 = D(x)$ è divisibile per $A(x)$

$$\deg D(x) \le n = \deg A(x)$$

$D(x) = \text{cost}\ A(x)$ $\qquad x = 1 \Rightarrow \text{cost} = 1$

Polinomi uguali $\Leftrightarrow$ $\{r_1, \dots, r_n\} = \{1, \dots, n\}$

$\{0, r_1, \dots, r_n\} = \{0, 1, \dots, n\}$

$n+1 = \text{composto} = a \cdot b$ $\qquad a, b < n$ $\qquad n+1 \neq 4$

$(n+1) \mid n!$ $\qquad r_n = 0 = r_0$

$n+1 = p > 3$

$n! = (p-1)! \equiv -1 \pmod{p}$

$1! \equiv (p-2)! \equiv 1 \pmod{p}$

Risposta $\underline{n = 1,\ n = 2}$

$A = a^n + a^{n-1} + \dots + a + 1$

$B = a^{n!} + a^{(n-1)!} + \dots + a^{1!} + 1$

$a > 1 \qquad A \mid B$

$C = a^{r_n} + a^{r_{n-1}} + \dots + a^{r_1} + 1$

$A \mid C$ somma delle cifre $= n+1$.

$C = c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0$

$c_n + \dots + c_0 = n+1$

$\{ x = x_n a^n + x_{n-1} a^{n-1} + \dots + x_1 a + x_0 \}$ (x divisibile per A)

Quanto può essere AL MINIMO $c_n + \dots + c_0$.

Posto sottomo $x_i < a$

$x_n \geq a \qquad x_n = a + y_n \qquad c_n a^n = a^{n+1} + a^n y_n$

$\downarrow$

1

$x_i \geq a \qquad i < n$

$x_i = a + y_i$

$x_i a^i + x_{i+1} a^{i+1}$

$= y_i a^i + (x_{i+1} + 1) a^{i+1}$

N° con somma di cifre minore

$\bar{e} \quad < a (a^n + a^{n-1} + \dots + 1)$

$= aA$

$A, 2A, \dots (a-1)A.$

$\boxed{C = A}$

PROBLEMA 8

$x^2 = y^p + 1$ $\quad$ x, y INT. POS

TH $\quad 2 \mid y \quad \Leftrightarrow \quad p \mid x \qquad 3^2 = 2^3 + 1$

$$(x+1)(x-1) = y^p$$

y DISP. $\Rightarrow$ x È PARI

$(x+1, x-1) = 1$ $\quad$ $x+1$ e $x-1$ PDT P-E SUI.

$$x^2 = (y+1)(y^{p-1} - y^{p-2} + \dots + 1)$$

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

$p \nmid x \Rightarrow \quad (y+1, y^{p-1} - y^{p-2} + \dots + 1) = 1$

$y + 1 = s^2 \qquad x^2 = y^p + 1$

$$X^2 - d y^2 = 1$$

$s^2 - y \cdot 1^2 = 1 \qquad x^2 - y \cdot (y^{\frac{p-1}{2}})^2 = 1$

$$\boxed{(s + \sqrt{y})^n (s - \sqrt{y})^n = 1^n}$$

$a^2 - y b^2 = 1$ allora $\forall n$: $a + \sqrt{y}\, b = (s + \sqrt{y})^n$

$$x + \sqrt{y}\cdot y^{\frac{p-1}{2}} = (s+\sqrt{y})^n$$

$$\boxed{x = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} y^i s^{n-2i}} \qquad s^2 = y+1$$

$$\sqrt{y}\, y^{\frac{p-1}{2}} = \sqrt{y}\cdot \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i+1} y^i s^{n-2i-1}$$

s È DISPARI, x È DISPARI, y È PARI

$$0 \equiv n\cdot s^{n-1} \qquad (2)$$

$n = 2m$

$$x + \sqrt{y}\cdot y^{\frac{p-1}{2}} = \left[(s+\sqrt{y})^2\right]^m$$

$$= \left[s^2 + y + 2\sqrt{y}\cdot s\right]^m$$

$$y^{\frac{p-1}{2}} = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2i+1} (s^2+y)^{m-2i-1} (2s)^{2i+1} y^i$$

$\Rightarrow s \mid y^{\frac{p-1}{2}}$ $\qquad s^2 = y+1$

ESEMPI: F_n, $2^n - 1$

INCISO: a_n SEQ. DI FIBONACCI SE $(a_n, a_m) = a_{(n,m)}$

$x^2 - d y^2 = 1$ PELL

y_n LA SUCC. DELLE SOL. ALLA PELL: È UNA SEQ. DI FIBONACCI!

PROBLEMA 7:

a) $x^3 + 51x$ $\qquad 51 \mid (x^3+51x) - (y^3+51y)$

$51 \mid x^3 - y^3$

$51 = 17 \cdot 3$

$x^3 \equiv y^3 \pmod{17}$

$(x^3)^{11} \equiv (y^3)^{11} \pmod{17}$

$x^{33} \equiv y^{33}$

$x \equiv y \pmod{p}$.

$x^a \equiv y^a \pmod{p}$ $\qquad (a, p-1)=1$

Fie: $ab \equiv 1 \pmod{p-1}$

$x^{ab} \equiv y^{ab} \Rightarrow x \equiv y$

$d \mid a, \quad d \mid p-1$

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

$$x^3 + 51x \equiv y^3 + 51y \pmod{n}$$

$$\Downarrow$$

$$x \equiv y \pmod{n}$$

VALE PER $n = p_1^{a_1} \cdots p_n^{a_n}$

SE E SOLO SE VALE PER OGNI $p_i^{a_i}$

$x^3 + 51x$ È BUONA mod p^k ?

BUONA mod $p^k \Rightarrow$ BUONA mod p.

$$x^3 + 51x \equiv y^3 + 51y \pmod{p}$$

$$x^3 - y^3 + 51(x-y) \equiv 0$$

$$(x-y)\left(x^2 + xy + y^2 + 51\right) \equiv 0 \pmod{p}$$

$$x - y \not\equiv 0 .$$

$$x^2 + xy + y^2 \equiv -51$$

$$\boxed{\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 \equiv -51} \pmod{p}$$

$u = x + \frac{y}{2}$ $\qquad$ y

$$u^2 + \frac{3}{4}y^2$$

$-51+v^2$ HA $\frac{p+1}{2}$ VALORE

$-\frac{3}{4}y^2$ HA $\frac{p+1}{2}$ VALORI

C: $C \equiv v^2 - 51$ PER QUALCHE v

$C \equiv -\frac{3}{4}y^2$ PER QUALCHE y

$0 \equiv v^2 - 51 + \frac{3}{4}y^2 \pmod p$

$x \equiv v - \frac{y}{2} \pmod p$

$$\boxed{\left(x+\frac{y}{2}\right)^2 + \frac{3}{4}y^2 \equiv -51}$$

$$\left(x+\frac{y}{2}\right)^2 \equiv \left(-\left(x+\frac{y}{2}\right)\right)^2$$

$$x' \equiv -x-y$$

$$\left(x'+\frac{y}{2}\right)^2 \equiv \left(-x-y+\frac{y}{2}\right)^2 \equiv \left(-x-\frac{y}{2}\right)^2$$

p^k - BUONA $\Rightarrow$ $p = 3, 17$

SE È p^k - BUONA $k \geq 2$

$\Rightarrow$ È p^2 - BUONA! $\quad X = 51 \quad y = 0$

$$p^2 \mid (51)^3 + 51 \cdot 51 - (0^3 + 51 \cdot 0)$$

$$p^2 \nmid 51$$

$X^3 - 51^2 X \qquad (51, 0)$

$3^k, 17^k \rightsquigarrow 3^3, 17^3$

$17 \equiv -1 \pmod 3$

$X^3 + 2010\,X$

X^3 NON È BIG. POI $2010 \equiv 1 \pmod 3$

(LEGA FORTUNA) $2010 = 2 \cdot 5 \cdot 3 \cdot 67$

$aX^3 + bX$ biyettiva mod 67

$a X^3 + bX \qquad p \equiv 1 \pmod 3$

$$\sum_{X=1}^{p} (aX^3 + bX)^{\frac{p-1}{3}} \equiv \sum_{X=1}^{p} X^{\frac{p-1}{3}} \pmod p$$

$$\sum_{X=1}^{p} g(X) = \sum_{X=1}^{p} a^{\frac{p-1}{3}} \cdot X^{p-1} + r(X)$$

$\deg(r) < p-1 \qquad \sum_{X=1}^{p} r(X) \equiv 0 \pmod p$

$$\sum_{X=1}^{p} a^{\frac{p-1}{3}} X^{p-1} \equiv 0 \pmod p$$

$$(p-1)\, a^{\frac{p-1}{3}} \pmod p$$

$$\Downarrow$$

$a \equiv 0 \pmod p$

$67 \mid a \qquad 67 \nmid b$

$x = \frac{2010}{67} \qquad y = 0$

$67 \mid a \qquad 67 \nmid b$

(a,b) BUONA MOD 67^K

(INDUZ SU K).

$$67^K \mid aX^3 + bX - (ay^3 + by)$$

$$\Rightarrow 67 \mid X - y$$

(ESERCIZIO)