PREIMO 2006 N - Matt.

Titolo nota 22/05/2006

$$\frac{2^a - 2^b}{2^c - 2^d} = n$$

$$2^a - 2^b = n\left(2^c - 2^d\right)$$

$$\cancel{2^b}\left(2^{a-b} - 1\right) = n \cdot \cancel{2^d}\left(2^{c-d} - 1\right) \implies b = \phi$$

$$a - b = x \qquad c - d = y$$

$$2^x - 1 = 11 \cdot (2^y - 1)$$

$$2^x + 10 = 11 \cdot 2^y \qquad x > 1 \implies y = 1$$

$$x = 1$$

$\equiv 3 \ (4)$ se $x \geq 2$

$\equiv 3 \cdot 3$ se $y \geq 2$

$$2^x - 1 = 11 \cdot (2^y - 1)$$

Quando $11 \mid 2^x - 1$? Quando $10 \mid x$

$$2^{p-1} \equiv 1 \quad (p)$$

Quando $\mathrm{ord}_{11}(2) \mid x$

$$\mathrm{ord}_{11}(2) = 10$$

$$2^{10} - 1 = 1023 = 11 \cdot 3 \cdot 31$$

$\mathrm{ord}_{11}(2)$

1

2

5

10

$$2^{20} - 1 = (2^{10} - 1)(2^{10} + 1)$$

$2^y - 1 \equiv 0 \ (3) \iff y$ pari

$2^y - 1 \equiv 0 \ (31)$

$$\mathrm{ord}_{31}(2) \mid y$$

$$\mathrm{ord}_{31}(2) = 5$$

$$2^x y = 3^x - 1 = (3-1)\underbrace{(3^{x-1} + 3^{x-2} + \dots + 1)}_{(3+1)3^{x-2} + (3+1)3^{x-4} \dots}$$

$$8(3^{x-2} \dots + 1)$$

$$(9^{\frac{x-2}{2}} + \dots + 1)$$

$$x^5$$

$$\sum_{i=0}^{2^n-1} 3^i = d \cdot 2^{n+1} \qquad n \geq 2$$

$$1 + 3 + 3^2 + 3^3 = 40$$

$$\sum_{i=0}^{2^{n+1}-1} 3^i = \sum_{i=0}^{2^n-1} 3^i + 3^{2^n}\left(\sum_{i=0}^{2^n-1} 3^i\right) = \left(\sum^{2^n-1} 3^i\right)(1+3^{2^n})$$

$$3^x - 1 = 2^x \cdot y$$

$$3^{x-1} + \cdots + 1 = 2^{x-1} \cdot y$$

$$\underbrace{1 + 3 + \cdots + 3^{2^n - 1}}_{2^{n+1}} \cdot \underbrace{+ \cdots + 3^k} \qquad k < 2^{n+1} - 1$$

$(1,1)$

$(2,2)$

$2x \geq 2^{x-1} \qquad x \leq 4 \qquad (4,5)$

$(3^x - 1)$ Max potenza di 2 che lo divide

Risposta: scrivo $x = 2^a \cdot d$.

dispari

La max potenza è $\begin{cases} a+2 & \text{se } a \geq 1 \\ 1 & \text{se } a = 0 \end{cases}$

$\boxed{\text{Caso } a = 0}$ x = dispari $3^x \equiv (-1)^x \equiv -1 \quad (4)$

$3^x - 1 \equiv 2 \quad (4)$ Max potenza è 1

$a=1$ $$3^{2d}-1=(3^2)^d-1$$

$$=\underset{\overset{\shortparallel}{8}}{(3^2-1)}\Big(\underbrace{(3^2)^{d-1}+\dots+1}_{d \text{ termini dispari}}\Big)$$

$\Rightarrow$ dispari

$$3^{2^a d}-1=\left(3^{2^a}\right)^d-1=\left(3^{2^a}-1\right)(\dots\dots)$$

dispari

Vero per $a \Rightarrow$ vero per $a+1$

$$3^{2^{a+1}}-1=3^{2\cdot 2^a}-1=\left(3^{2^a}-1\right)\left(3^{2^a}+1\right)$$

div. per 2^{a+2} esatt.

$\equiv 2 \ (4)$ guadagno 2

Max potenza di 7 che divide $5^x - 1$

$7 \mid 5^x - 1 \iff 6 \mid x$

$5^6 - 1$ max potenza $= 1$

$5^6 = 1 + 7y \qquad 7 \nmid y$

$(5^6)^7 = (1 + 7y)^7 = 1 + 7^2 y + \binom{7}{2}(7y)^2 + \dots$

$7^2 \parallel (5^6)^7 - 1$

$7^{k+1} \parallel (5^6)^{7^k} - 1$

$(5^6)^{7^k} = 1 + 7^{k+1} t \qquad 7 \nmid t$

$(\qquad)^7 = (\qquad)^7 = 1 + 7^{k+2} t +$

$$(5^6)^{7^k a} - 1 \qquad 7 \nmid a$$

$$(5^6)^{7^k} = 1 + 7^{k+1} y$$

$$(\quad)^a = (1 + 7^{k+1} y)^a = 1 + 7^{k+1} a y + \ldots$$

$$n^8 - n^2 = p^5 + p^2$$

$$\cancel{n^2}(n+1)\underbrace{(n^2-n+1)(\cancel{n-1})(n^2+n+1)}_{\text{al massimo 1 fattore } p} = p^2(p+1)(p^2-p+1)$$

$2n$

$MCD(\times\ \times) \leq 2n$

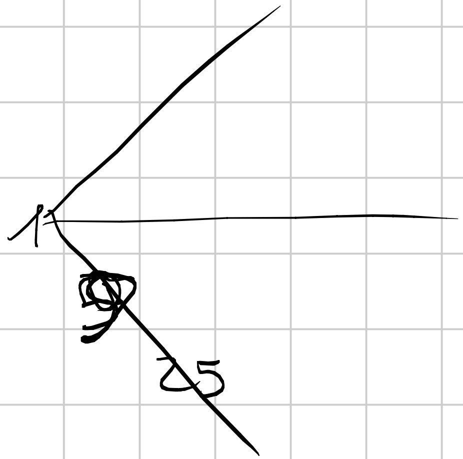
$$a \mid bc,\quad (a,b)=1 \Rightarrow a \mid c$$

$$n < p < n^2$$

$p \mid n+1$ $\quad p > n \quad \Longrightarrow \quad \boxed{p = n+1}$

$p = 3$ $\quad n = 2$ UNICA SOL.

Trovare per quali p esiste una semiretta destra che non contiene multipli di p.



$$4n^2+5n+2+k$$

$$4n^2+5n+2+k \not\equiv 0 \ (p)$$

$$(4n+1)(n+1) \not\equiv -k-1 \ (p)$$

Se esistono a e b, $a \neq b$ tali che

$$(4a+1)(a+1) \equiv (4b+1)(b+1) \ (p)$$

$$4(a+b)\cancel{(a-b)}+5\cancel{(a-b)}\equiv 0 \ (p)$$

$$(a+b)\equiv -\frac{5}{4} \ (p) \iff p\neq 2$$

$$4\equiv 0 \qquad 5\equiv 0 \ (2) \text{ imp.}$$

Domanda $p > 2$

$\exists$ polinomi di II grado surg. / iniettivi mod p ?

$ax^2 + bx + c$ $\quad p \nmid a$

NO e i valori presi (l'immagine) è ~~fatta~~ da $\frac{p+1}{2}$ elementi

$$x^2 + bx + c = (x+\alpha)^2 + \beta$$

k^2

$(-k)^2$

Immagine pol. = B + residui quadratici mod p

$$\frac{p-1}{2} + 1$$

0 è residuo quadr.

$x^2 \equiv a \quad (p)$

$y^2 \equiv a \quad (p)$

$x^2 - y^2 \equiv 0 \quad (p)$

$p \mid (x+y)(x-y)$

$\rightarrow p \mid x-y \rightsquigarrow x \equiv y$

$\rightarrow p \mid x+y \rightsquigarrow x \equiv -y$

$$ax^2 + bx + c = \frac{1}{4a}\left(4a^2x^2 + 4abx + 4ac \overset{\pm b^2}{} \right)$$

$$\frac{1}{4a}\left[(2ax+b)^2 + (4ac - b^2)\right]$$

— o — o —

Ex. $\boxed{x^3 + 2 \quad (\text{mod } 2003) \quad \text{SURG ?}}$

$(\text{mod } p)$