WC 2016 TdN

Titolo nota

N4

- $f(n)$ CHE VALORI ASSUME mod p?

$p \mid ab \to p \mid a \vee p \mid b$

$f(n)^2 - f(n) \equiv 0 (p) \to f(n) \equiv 0 (p) \vee f(n) - 1 \equiv 0 (p)$

$$f(n) \equiv 0 \ (p) \quad \vee \quad f(n) \equiv 1 \ (p)$$

$$f(0) \equiv 0 \ (p) \qquad f(1) \equiv 1 \ (p)$$

LEMMA $\sum_{j=0}^{p-1} x^k \equiv 0 \ (p) \iff p-1 \nmid k$

$k \geq 1$

$\equiv -1 \ (p)$ ALTRIMENTI

ESISTE UN GENERATORE mod p

$\exists\, g \mid \mathrm{ord}_p(g) = p-1$.

$g^k \not\equiv 1 \pmod p \quad \forall\, 1 \le k \le p-2$

$X \mapsto g \cdot x$

$a \to g \cdot a$

$b \to g \cdot b$

$\exists E \quad g \cdot a \equiv g \cdot b \ (p) \quad p \mid g(a-b) \quad p \nmid g$

$a \equiv b \ (p)$

$1 \le k \le p-2 \qquad \sum_{x=0}^{p-1} x^k \equiv \sum_{x=0}^{p-1} (gx)^k \quad (p)$

$\sum_{x=0}^{p-1} x^k \equiv g^k \sum_{x=0}^{p-1} x^k \quad (p)$

$$g^k \not\equiv 1 \pmod{p}$$

$$\underbrace{(g^k - 1)}_{\neq 0} \left(\sum_{x=0}^{p-1} x^k \right) \equiv 0 \pmod{p}$$

$$\sum_{x=0}^{p-1} x^k \equiv 0 \pmod{p}$$

$p-1 \mid k \Rightarrow x^k \equiv 1 \quad (x,p)=1$

$$\sum_{k=0}^{p-1} x^k \equiv p-1 \quad (p)$$

PER FERMAT

$x^{p-1} \equiv 1 (p)$

$\forall x \in (x,p)=1$

$x^{k+p-1} \equiv x^k \quad (p) \qquad p \in \mathbb{R} \; k \geq 1$

$$\sum_{x=0}^{p-1} x^k \equiv 0 \ (p) \quad \text{SE} \quad 1 \le k \le p-2$$

$\Big\|$ POSSO SOSTITUIRLO mod p

$$\sum_{x=0}^{p-1} x^{k+p-1} \equiv \sum_{x=0}^{p-1} x^k \equiv 0 \ (p)$$

IN GENERALE: $\sum_{x=0}^{p-1} x^{n(p-1)+k} \equiv 0 \ (p)$

Con $p-1+k$.

$$\sum_{x=0}^{p-1} f(x) \quad (p)$$

Supponiamo $\deg f < p-1$

$$f(x) = a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \dots + a_0$$

$$\sum_{x=0}^{p-1} f(x) = \sum_{x=0}^{p-1} \left(\sum_{i=1}^{p-2} a_i x^i \right) + \sum_{x=0}^{p-1} a_0 \quad (p)$$

$F(x)$

$$\sum_{i=1}^{p-2} \left(\sum_{x=0}^{p-1} a_i x^i \right) + \sum_{x=0}^{p-1} a_0 \quad (p)$$

LEMMA

DATO CHE $i \leq p-2$

SE $i \geq 1$ ALLORA

$$\sum_{x=0}^{p-1} a_i x^i \equiv 0 \quad (p)$$

$$\sum_{i=1}^{p-2} \binom{p}{i} \overset{\text{LEMMA}}{\equiv} 0 + \sum_{i=0}^{0} \left(\sum_{x=0}^{p-1} a_0 \right)$$

$$\| \quad \| \quad |$$

$$0 \quad (p)$$

↳ $p \cdot a_0 \equiv 0 (p)$

CONCLUSIONE: $\sum_{x=0}^{p-1} f(x) \equiv 0 \ (p)$

$f(x) \equiv 0 \vee f(x) \equiv 1 \pmod p \quad \forall x$

$f(0) = 0, \quad f(1) \equiv 1.$

$\overline{F} \equiv f \pmod p$

$\overline{F}(x)$

$f(0) + f(1) + f(2) + \dots + f(p-1) \equiv 0 +$

$f(1) + \dots + f(p-1) \leq p-1$

b VALORI $\equiv 1 \pmod p \qquad 1 \leq b \leq p-1$

$0 \equiv \sum_{x=0}^{p-1} f(x) \equiv b \pmod p$

$S \in \deg p < p-1$

ASSURDO!

$b \not\equiv 0 \pmod p$

PERCIÒ $\deg f \geq p-1$.

UN ESEMPIO: $f(x) = x^{p-1}$

PER FERMAT $\equiv 0,1 \pmod{p}$

N 6

IDEA: CONSIDERIAMO x TALE CHE $\mathrm{Ord}_p(x) = q$ CON q PRIMO GRANDE.

LEMMINO: $\forall q$ PRIMO ESISTONO INFINITI PRIMI $p \equiv 1 \pmod{q}$.

OSSERVAZIONE:

SE $p \mid 1 + x + x^2 + \dots + x^{q-1} \rightarrow p = q$ oppure $q \mid p-1$.

$$(x^q - 1) \equiv (x-1)(1 + x + \dots + x^{q-1})$$

SE $p \mid 1 + x + \dots + x^{q-1} \rightarrow x^q \equiv 1 \pmod{p}$

ORA:

- $ord_p(x) \mid p-1$
- $ord_p(x) \mid q$ (qui)

$ord_p(x) = q \to q \mid p-1$

$ord_p(x) = 1 \to x \equiv 1 (p)$

$x^1 \equiv 1 (p) \to x \equiv 1 (p)$

$p \mid 1 + x + \dots + x^{q-1} \to p \mid q \to p = q$

IN GENERALE SE

$x^n \equiv 1 (p)$

$ord_p(x) \mid n$

SUPPONIAMO ESISTA UN NUMERO FINITO DI PRIMI $\equiv 1 \pmod{q}$ (OPPURE ZERO)

E CONSIDERIAMO: $S = \left(\prod_{p \equiv 1 \pmod{q}} p\right) \cdot q$

OPPURE $S = q$ SE NON CI SONO $p \equiv 1 \pmod{q}$

$1+s+s^2+s^3+\dots+s^{q-1} > 1$

PERCHÉ $s \geq q$.

↓

HA DEI FATTORI PRIMI. ↳ PONIAMO PROPRIO DI QUESTI MA:

- SE $p \mid s \rightarrow p \nmid 1+s+\dots+s^{q-1}$

$s \equiv 0 \pmod{p} \rightarrow 1+s+\dots+s^{q-1} \equiv 1 \pmod{p}$

- SE $p \nmid s$: ALLORA $p \mid q$ OPPURE $p \equiv 1 \pmod q$.

ASSURDO! p DIVIDEREBBE s.

PRENDIAMO $p \equiv 1 \pmod q$ E SIA α UN ELEMENTO DI ORDINE q MOD p.

VOGLIAMO DIMOSTRARE CHE α È LIBERO DA p PER $p > C$ DOVE C È COSTANTE

$$\alpha^q - 1 \equiv 0 \ (p)$$

SUPPONIAMO PER ASSURDO ESISTANO i, j, k TALI CHE $p \mid \alpha^i + \alpha^j - \alpha^k$

$$\alpha^i + \alpha^j \equiv \alpha^k \pmod{p}$$

SUPPONIAMO $i \leq j$

$$\alpha^i \left(1 + \alpha^{j-i}\right) \equiv \alpha^k \pmod{p}$$

ELEVIAMO ALLA q.

$$\alpha^{iq} \left(1 + \alpha^{j-i}\right)^q \equiv \alpha^{kq} \pmod{p}$$

$\equiv 1$ ← $\alpha^{iq} \equiv 1 \pmod{p}$

$\equiv 1$ ↓

$$(1+x^{j-i})^q \equiv 1 \ (p)$$

VOGLIAMO SUPPORRE $0 \leq j-i \leq q-1$.

$x^{j-i} \equiv x^{j-i-q}$ PERCHÉ $x^{-q} \equiv (x^q)^{-1} \equiv 1 (p)$

QUINDI SE $j-i \geq q$, ALLORA $x^{j-i} \equiv x^{j-i-q} \ (p)$. A $j-i$ POSSO TOGLIERE q.

PERCIÒ PONIAMO $J-i = n$ CON $0 \leq n \leq q-1$

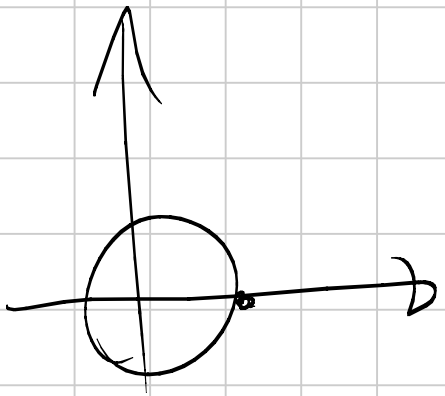
$$x^q - 1 \equiv 0 \ (p)$$

$$(x^N + 1)^q - 1 \equiv 0 \ (p) \quad \text{CON } 0 \leq N \leq q-1$$

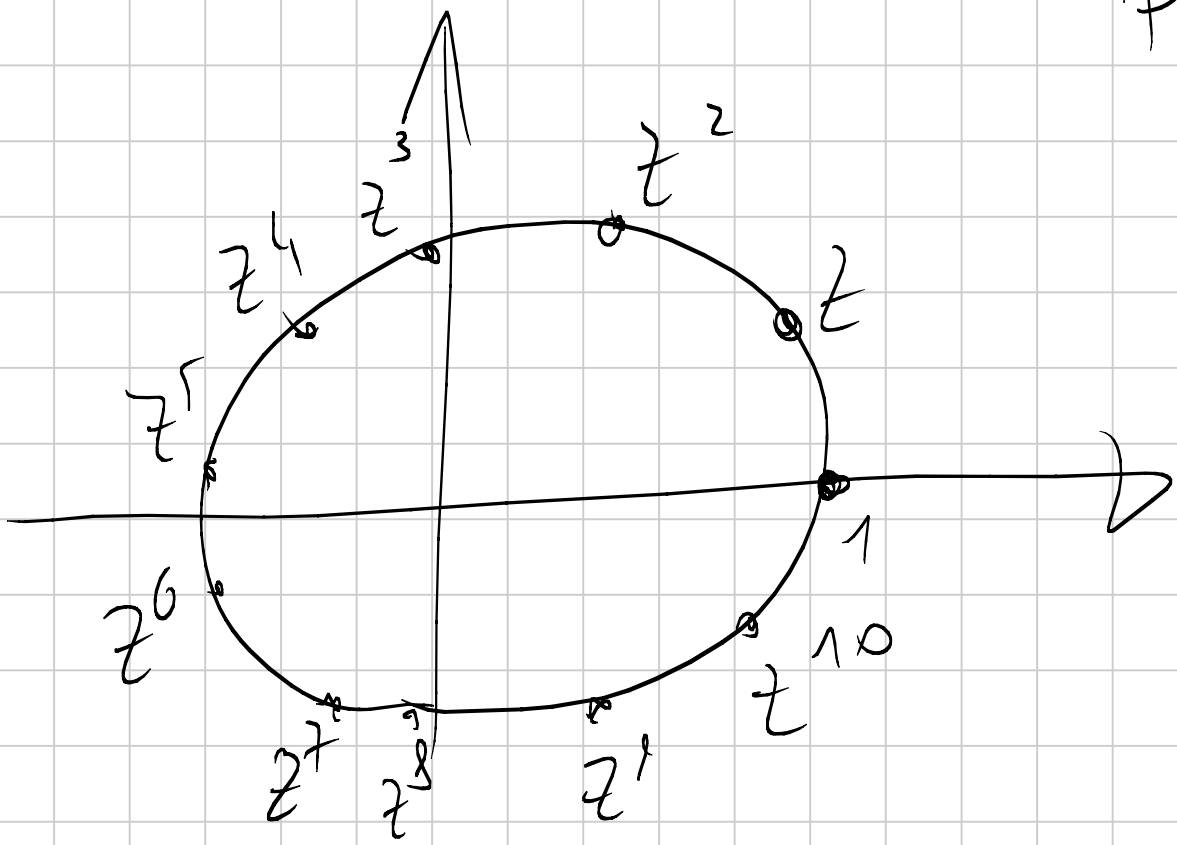
$x^9 - 1$ E $(x^N + 1)^9 - 1$ NON HANNO RADICI COMUNI IN $\mathbb{C}$.

SUPPONIAMO:

$$\begin{cases} z^9 - 1 = 0 \rightarrow |z| = 1 \\ (z^N + 1)^9 - 1 = 0 \rightarrow |z^N + 1| = 1 \end{cases}$$

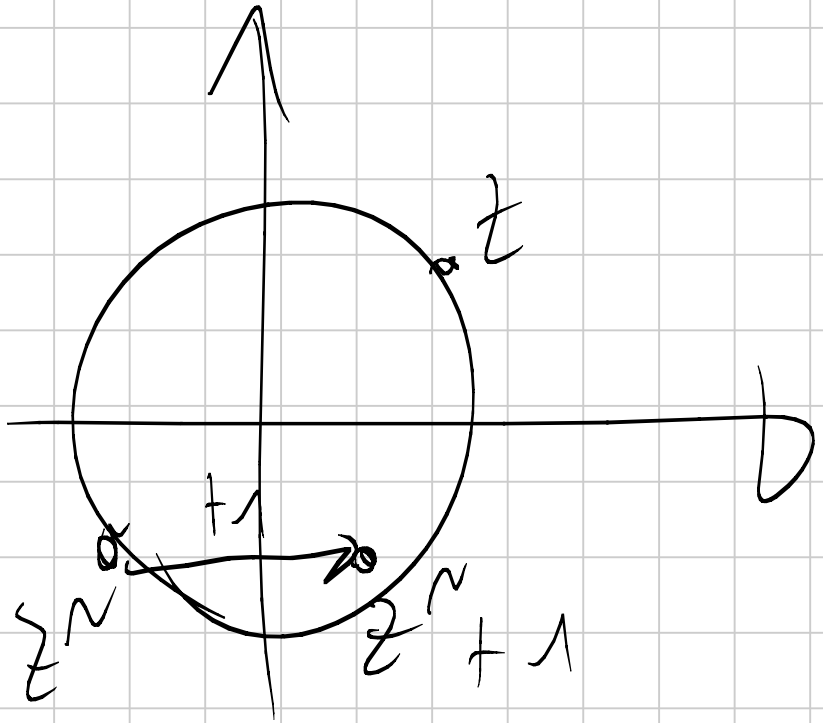


z^N DOVE STA?



PER $q = 11$,

z^N SARÀ IN UNO DI QUESTI VERTICI.



$a+ib$

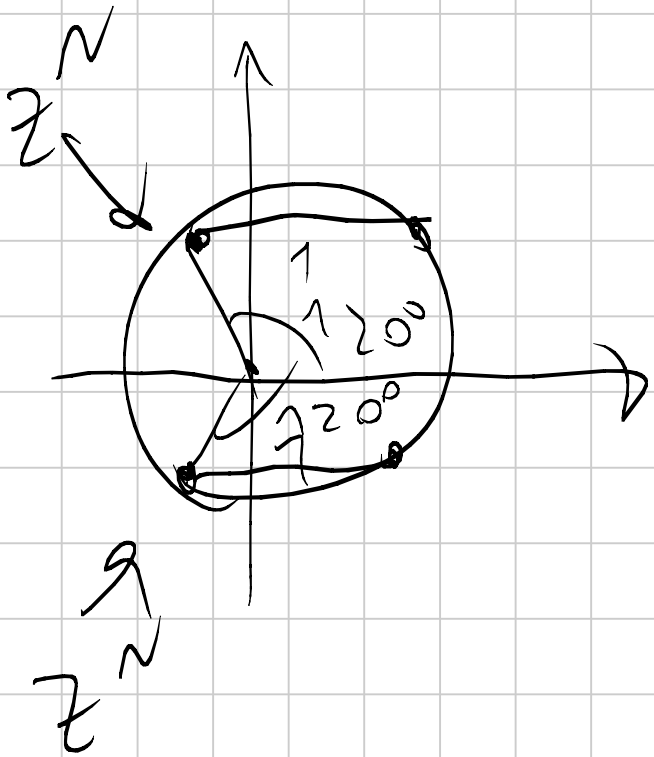
$a^2+b^2=1$

$(a+1)+ib \to$

$(a+1)^2+b^2=1$

$a^2=(a+1)^2 \Rightarrow a=-\frac{1}{2}$

$b=\pm\frac{\sqrt{3}}{2}$



$$z^3 = 1$$

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

$$\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)^3 = 1$$

$(z^N)^3 = 1$ MA $z^9 = 1$.

ORA: SE $9 > 3$ E $N < 9$ ALLORA

9 E 3N SONO COPRIMI.

$N \neq 0$.

$3 < 9$, $N < 9 \Rightarrow (3N, 9) = 1$

$z^{3N} = 1$ $z^9 = 1$

$\exists a, b$ $3Na - 9b = 1$

$$1 = \frac{\left(z^{3N}\right)^{q}}{\left(z^{9}\right)^{b}} = z^{3Nq-9b} = z$$

$$1^9 - 1 = 0 \quad \checkmark$$

$$\left(1^N + 1\right)^9 - 1 = 0 \quad \times$$

$N=0$ $\begin{cases} x^{q-1}-1=0 \\ z^q-1=0 \end{cases}$ NO SOLUZIONE

PERCIÒ $x^q-1 \in (x^N+1)^q-1$ SONO COPRIMI $\forall\, 0 \le N \le q-1$.

QUINDI ESISTONO PER BÉZOUT

POLINOMI A COEFFICIENTI INTERI $f_n(x)$ E $g_n(x)$ TALI CHE

$$f_n(x)\left(x^{q-1}\right)+g_n(x)\left(\left(x^n+1\right)^q-1\right)=C_n$$

CON C_n INTERO POSITIVO

PERCIÒ VALUTANDO IN α:

$$f_n(x)(x^q-1)+g_n(x)\left((x^n+1)^q-1\right)=C_n$$

$$p \mid x^q-1, \quad p \mid (x^n+1)^q-1 \Rightarrow p \mid C_n.$$

PERCIÒ $p \leq C_n$

ALLORA, DATO n, C_n NON DIPENDONO DA p MA SOLO DA q, IN PARTICOLARE $\max\{C_0, C_1, \dots, C_{q-1}\}$ DIPENDE SOLO

DA q. MA $p \leq \max\{c_0, \dots, c_{q-1}\}$

r E q NON DIPENDONO DA p PERCHÉ

$$0 \leq r \leq q-1$$

ASSURDO! MI BASTA PRENDERE $p > \max$

N5 Idea fondamentale:

$$n = (p_1 p_2 \cdots p_k)^A$$

$$m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \qquad b_i < A$$

$$\phi(n) \longleftrightarrow \phi\left(\frac{n}{m}\right)$$

Qual è la relazione?

$$\phi(n) = (p_1 p_2 \cdots p_k)^{A-1} (p_1 - 1) \cdots (p_k - 1)$$

$$\frac{n}{m} = p_1^{A-b_1} \cdots p_k^{A-b_k}$$

$$\varphi\left(\frac{n}{m}\right) = p_1^{A-b_1-1} \cdots p_k^{A-b_k-1} (p_1-1) \cdots (p_k-1)$$

$$\varphi\left(\frac{n}{m}\right) = \frac{\varphi(n)}{m}$$

Secondo passo

$$n = (p_1 \cdots p_k)^A$$

Altro primo : $q \neq p_1, \ldots, p_k$

tale che $q-1$ sia "del tipo precedente"

$$q-1 = p_1^{b_1} \cdots p_k^{b_k}$$

$$\phi\left(\frac{n\,q}{q-1}\right) = \phi\left(\frac{n}{q-1}\right)\phi(q)$$

$$= \frac{\phi(n)}{q-1}\cdot(q-1) = \phi(n)$$

x abbastanza grande:

Voglio che siano almeno 2016 numeri primi q

$$x < q < 2x$$

$\{p_1, \dots, p_k\}$ = numeri primi $< x$

$$n = (p_1 \cdots p_k)^A$$

con A abbastanza grande:
tutti i numeri $< x$ sono divisori di n.

$$\frac{n}{q-1} \cdot q$$

Perché $\frac{q-1}{2} < x$ $q-1$ ha solo fattori primi $< x$

Uso la formula

$$\phi\left(\frac{n}{q-1}\, q\right) = \frac{\phi(n)}{q-1} \cdot (q-1) = \phi(n)$$

$$S = \{11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71\}$$

$|S| = 11$ $\qquad 2^{11} > 2016$

$$n = (2 \cdot 3 \cdot 5 \cdot 7)^A$$

$$n \to n \prod_{q \in T} \frac{q}{q-1}$$

$T \subseteq S$