WINTER CAMP 2018 - TdN

Titolo nota 27/01/2018

NA1

$$a_{k+1}^{k} \mid C^{k} \cdot a_1 \cdots a_k$$

oss: $a_2 \mid C a_1 \Rightarrow a_k$ ha (al più) gli stessi fattori primi di Ca_1

$p_1, \dots, p_N$ sono <u>tutti</u> e soli i divisori di $a_1, a_2, a_3, \dots$

idea: guardiamo $q = p_i$

$$v_q(a_{k+1}^{k}) \le v_q(C^k) + \sum_{i=1}^{k} v_q(a_i)$$

$$k\, v_q(a_{k+1}) \le k \cdot v_q(C) + \sum v_q(a_i)$$

CLAIM: $v_q(a_{k+1}) \le v_q(C) \cdot \underbrace{\left(1 + \frac{1}{2} + \dots + \frac{1}{k}\right)}_{H_k} + v_q(a_1)$ $*$

per induzione ← fare passo iniziale

$$(k+1)\, v_q(a_{k+2}) \le (k+1) \cdot v_q(C) + \sum_{i=1}^{k+1} v_q(a_i)$$

$$\le (k+1)\, v_q(C) + \sum \left(v_q(C) \cdot H_{i-1} + v_q(a_1)\right)$$

$$\le \underbrace{v_q(c)\cdot\left(K+1+H_1+\dots+H_K\right)} + (K+1)\,v_q(a_1)$$

$$\overset{?}{\le} v_q(c)\cdot H_{K+1}\cdot(K+1)$$

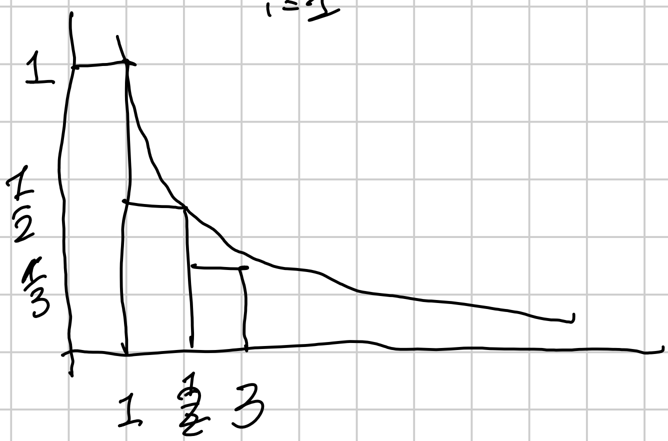
$$\sum_{i=1}^{K} H_i = \sum_{i=1}^{K}\sum_{j=1}^{i}\frac{1}{j} = \sum_{j=1}^{K}\frac{1}{j}\cdot\#\{i : i\ge j,\ i\le K\}$$

$$= \sum_{j=1}^{K}\frac{1}{j}(K-j+1) = \sum_{j=1}^{K}\frac{K+1}{j} - \sum 1 = (K+1)H_K - K$$

$$K+1+\sum H_i = (K+1)H_K - K + K+1 = (K+1)H_K + 1$$

$$H_{K+1} = \frac{(K+1)H_K+1}{K+1}$$

FATTO: $\displaystyle\sum_{i=1}^{K}\frac{1}{i} \le \log(K+1)+1$



$$\int \frac{1}{x} = \log x$$

$$\Rightarrow v_q(a_K) \le A\cdot\log(K+1)$$

Vale per tutti i p_i

$p_1 \; - \; - \; - \qquad p_N$

1
2
.
.
Alog

quanti sono i possibili a_i distinti?

$(A \cdot \log K)^N$

Dato che gli a_i sono distinti

$(A \log K)^N \geq K \leftarrow$ mi serve per poter scegliere K a_i

però per K grande, è falsa

NON C'È NESSUNA SUCCESSIONE !

$\boxed{N5}$ $\{n, \dots, n+15\}$ $A = A_n$

$$A = B \cup C \quad B \cap C = \emptyset \quad \prod_{b \in B} b = \prod_{c \in C} c$$

1° fatto: fra 16 numeri consecutivi ce n'è al massimo uno che è multiplo di 17

2° fatto: uno solo non va bene

Quindi nessuno $\quad (n \equiv 1 \pmod{17})$

Stessa cosa per ogni primo > 17.

Fattori primi possibili dei numeri $n+i$:

$2, 3, 5, 7, 11, 13$

Se m è divisibile per p^2,
allora $m+p$, $m-p$ sono per p ma non per p^2

Guardo la massima potenza di 2 (2^k) che divide uno dei numeri $n+i$.

- $k \geq 4$
- $2^k \| n+i$

Nell'insieme A ci sono:

- esattamente un numero divisibile esattamente per 8
- " 2 num. " " per 4
- " 4 num. " " per 2

$$8 \cdot 4^2 \cdot 2^4 = 2^3 \cdot 2^4 \cdot 2^4 = 2^{11}$$

Allora $k \leq 11$, infatti se $k > 11$
$n+i \in B$
la potenza di 2 in C non può bilanciare 2^k,
Quindi la massima potenza di 2 che può dividere $\prod(n+i)$ è 2^{22}.

Altri primi:

$p = 3$ al massimo 6 fattori divisibili per 3.

Certamente $k \geq 2$

Se $k \geq 3$ 1^0 numero div. esattamente per 3^2

4 num. " " " 3.

$3^2 \cdot (3)^4 = 3^6 \Rightarrow k \leq 6$

⋮

$p = 13$ al max 2 numeri divisibili per 13

Almeno uno dei due div. esattamente per 13

L'altro pure (altrimenti non divide in parti uguali

$$n^{16} \leq \prod_{i=0}^{15} (n+i) \leq 2^{22} \cdot 3^{12} \cdot 5^6 \cdot 7^4 \cdot 11^2 \cdot 13^2$$

$$2^{22} \cdot 3^{12} = 2^{16} \cdot 2^6 \cdot 3^{12} < 2^{16} \cdot 3^4 \cdot 3^{12}$$

$$= (6)^{16}$$

$5^6 < 7^6 \quad 11^2 < 7^3 \quad 13^2 < 7^3$

$$5^6 \cdot 7^4 \cdot 11^2 \cdot 13^2 < 7^{16}$$

$$n \leq 2 \cdot 3 \cdot 7 = 42$$

Visto che ci sono numeri primi grandi per $17 \leq m \leq 43$

$n \geq 2$ non va bene

$n = 1$ il prodotto di tutti i numeri è $16!$

che però non è un quadrato

(basta considerare il primo 13)

Impossibile che $\prod_{b \in B} b = \prod_{c \in C} c$.

$\boxed{N6}$ Esistono infinite terne (a,b,p) t.c. $0<a\leq b<p$

e $p^5 \mid (a+b)^p - a^p - b^p$

Oss Un fattore p è gratis:

$$(a+b)^p - a^p - b^p = p \cdot \underbrace{q(a,b)}_{\text{coefficienti interi}} = p \cdot b^p \cdot r(a/b)$$

Oss. 2 $$(a+b)^7 - a^7 - b^7 = 7\,ab(a+b)\left(a^2+ab+b^2\right)^2$$
$$= 7b^7\, x(x+1)(x^2+x+1)^2 \qquad x := a/b$$

$$r(x) = \frac{(x+1)^p - x^p - 1}{p}$$

Fatto $s(x) \in \mathbb{C}[x]$. $\quad d(x)^2 \mid s(x) \iff$
$$d(x) \mid \left(s(x),\ s'(x)\right)$$

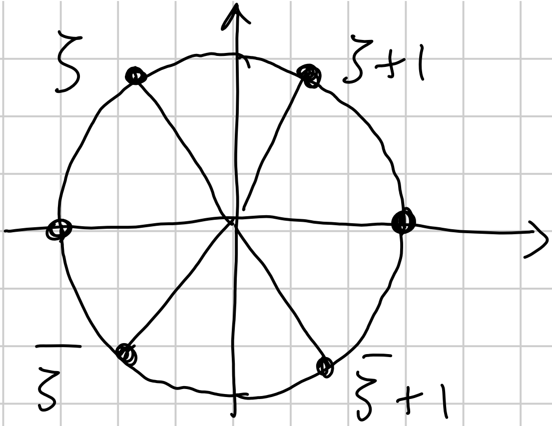
$$s(x) = d(x)^m \cdot e(x) \qquad s'(x) = m\,d(x)^{m-1}e(x) + d(x)^m e'(x)$$

Criterio della derivata

$$\left(p\,r(x),\ p\,r'(x)\right) = \left((x+1)^p - x^p - 1,\ \cancel{p}(x+1)^{p-1} - \cancel{p}x^{p-1}\right)$$

$$= \left((x+1)x^{p-1} - x^p - 1,\ (x+1)^{p-1} - x^{p-1}\right)$$

$$= \left(\underbrace{x^{p-1} - 1}_{\substack{\text{radici} = \\ \text{radici dell'unità} \\ \text{ordine} \mid p-1}},\ \underbrace{(x+1)^{p-1} - \cancel{x^{p-1}} + \cancel{x^{p-1}} - 1}_{\substack{\text{radici} = \\ \{\zeta \,:\, \zeta+1 \text{ sia radice} \\ \text{dell'unità di ordine} \\ \text{che } \mid p-1\}}}\right)$$



ζ rispetta $\zeta^3=1$

$(\zeta^2+\zeta+1=0)$

Radici comuni $\iff$ ζ radice di $r(x)$

$\iff$ ζ radice di $x^{p-1}-1$

$\iff$ $3 \mid p-1$

Conclusione parziale $3 \mid p-1 \implies r(\zeta)=r(\bar\zeta)=0$

$$\implies (x-\zeta)(x-\bar\zeta) \mid r(x)$$

$$\implies x^2+x+1 \mid r(x)$$

Non solo: per il criterio della derivata,

$$(x^2+x+1)^2 \mid r(x)$$

$$\xrightarrow[r(x)]{\text{def di}} \quad (a+b)^p-a^p-b^p = p\cdot(a^2+ab+b^2)^2\, t(a,b)$$

Ci basterebbe quindi trovare a,b "piccoli" t.c.

$$p^2 \mid a^2+ab+b^2$$

Ambizione: cerchiamo a,b t.c. $p^2=a^2+ab+b^2$

Passo 1: $a^2+ab+b^2\equiv 0\ (p)$

$p\equiv 1\ (3) \implies$ esiste ω mod p t.c. $\omega\not\equiv 1\ (p)$

ma $\omega^3\equiv 1\ (p)$

$$a^2+ab+b^2 = (a-\omega b)(a-\omega^2 b)$$

Voglio a,b t.c. $a \equiv \omega b \pmod p$

Lemma (Thue) Dato $K \not\equiv 0\ (p)$ esistono $x,y \in \mathbb{Z}$

t.c. $y \equiv Kx \mod p \qquad 0 < |x|, |y| < \sqrt{p}$

[Sketch: $y_1 - Kx_1 \equiv y_2 - Kx_2 \ (p)$]

$\rightsquigarrow$ trovo a,b con $|a|, |b| < \sqrt{p}$ e t.c.

$$p \mid \underbrace{a^2+ab+b^2}_{<3p} \in \{p, \cancel{2p}\}$$

$$2p = a^2+ab+b^2 \xrightarrow{\text{mod } 2} ab+a+b \equiv 0 \ (2)$$

$(a+1)(b+1) \equiv 1 \ (2)$

a,b pari $\Rightarrow 4 \mid a^2+ab+b^2$ NO

$$a^2+ab+b^2 = p \Rightarrow p^2 = (a^2+ab+b^2)^2$$
$$= c^2+cd+d^2$$

$$c = a^2-b^2, \quad d = 2ab+b^2$$

$$(A^2+B^2)(C^2+D^2) = (AC+BD)^2+(AD-BC)^2$$

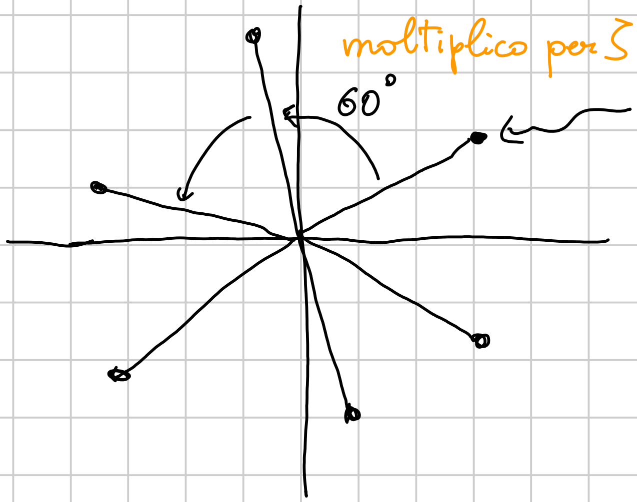
$$(A+Bi)(A-Bi)(C+Di)(C-Di)$$

$$a^2+ab+b^2 = (a-\xi b)(a-\bar{\xi} b)$$

$$(a^2+ab+b^2)^2 = (a-\xi b)^2(a-\bar{\xi} b)^2$$

$$= \left[a^2 - 2ab\zeta + \underbrace{\zeta^2}_{-\zeta-1} b^2 \right] \cdot \text{coniugato}$$

$$= \left[(a^2 - b^2) - \zeta(b^2 + 2ab) \right] \cdot \text{coniugato}$$



$c - d\zeta$ norma $= p^2$

Moltiplicando $a - b\zeta$ per $(-\bar{\zeta})^i$ (i opportuno)

posso assumere che a, b (o c, d) abbiano i segni che voglio

$p^2 = c^2 + cd + d^2$, posso assumere $c, d > 0$

$> \max\{c^2, d^2\} \Rightarrow \max\{c, d\} < p$

[Bisogna controllare $cd \neq 0$: facile!]