Senior 2016 - N3 Advanced (Anèr)

Note Title 9/5/2016

- Campi finiti, qualche conto
- Vieta jumping (+ problema tostissimo)
- Successioni di Mersenne (si chiamano davvero così?)
- Esercizi vari

Dato p primo e $K \geq 2$ naturale, quanti sono i polinomi monici di grado K in $\mathbb{F}_p[x]$ irriducibili?

<u>OSS</u> Se esiste almeno un pol. $q(x) \in \mathbb{F}_p[x]$ irrid. di grado K, allora

$$\mathbb{F}_p[x] \big/ (q(x)) \text{ è un campo con } p^k \text{ elementi}$$

(È uno spazio vett. su $\mathbb{F}_p$, e ha come base $1, x, x^2, \dots x^{k-1}$

$\Rightarrow \mathbb{F}_{p^k}$ esiste!

Considero il polinomio $x^{p^k} - x \in \mathbb{F}_p[x]$

Usando i ciclotomici, ottengo la fattorizzazione

$$x^{p^k} - x = x \cdot \left(x^{p^k - 1} - 1\right) = x \cdot \prod_{d \mid p^k - 1} \Phi_d(x)$$

($\Phi_d(x)$ è il d-esimo pol. ciclotomico, e ha grado $\varphi(d)$)

OSS 1 Forse in $\mathbb{F}_p[x]$ qualcuno dei $\Phi_d(x)$ si fattorizza ulteriormente

OSS 2 $\Phi_{p^k-1}(x)$ è tra i fattori (speriamo che contenga le radici di ordine esattamente p^k-1)

Costruiamo un campo finito in cui $q(x)=x^{p^k}-x$ si fattorizza in fattori di grado 1

PASSO 1 $K_0=\mathbb{F}_p$. $q(x)=q_1^0(x)\cdot\ldots\cdot q_{m_0}^0(x)$ fatt. in irrid.

Se un fattore ha grado ≥ 2, $q_i^0(x)$, considero

$$K_0[x]\big/q_i^0(x) \doteq K_1$$

PASSO 2 K_1 (cambio lettera)

$$\underset{\substack{\uparrow\\ K_1[y]}}{q(y)} = q_1^0(y)\cdot\ldots\cdot \underset{\substack{\uparrow\\ \text{è divisibile per } (y-x)}}{\overline{q_i^0(y)}}\cdot\ldots\cdot q_{m_0}^0(y)$$

$\Rightarrow$ ho una fattorizzazione più fine. $q(y)=q_1^1(y)\cdot\ldots\cdot q_{m_1}^1(y)$

$m_1>m_0$. Prendo $q_j^1(y)$ irrid. di grado ≥ 2

$$K_2=\frac{K_1[y]}{(q_j^1(y))}\left(=K_0[x,y]\big/(q_i^0(x),q_j^1(y))\right)$$

A un certo punto ho un campo K_N in cui

$x^{p^k}-x$ si fattorizza in fattori lineari

K_N contiene come sottoinsieme le radici di $x^{p^k}-x$

La chiamo $S=\{\text{radici di } x^{p^k}-x\}\subseteq K_N$

OSS. 3 $\quad S$, come sottoinsieme di K_N, è chiuso per $+, \cdot, -$, c'è 0, se c'è t c'è t^{-1} $(t \neq 0)$.

RIVEDIAMO LA SOMMA $\quad (\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k} + \sum_{i=1}^{p^k-1} \underbrace{\binom{p^k}{i}}_{\text{multipli di } p} \cdot \alpha^i \beta^{p^k-i}$

(in K_N) $= \alpha^{p^k} + \beta^{p^k} = \alpha + \beta$

S è un campo con p^k elementi! Quasi. $x^{p^k} - x$ potrebbe avere radici doppie in K_N ...

DERIVIAMO (ma funziona davvero?)

Funziona $\quad$ Sia $q(x)$ un polinomio a coeff. in K $(=K_N)$

$$q(x) = (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_m) \qquad \alpha_i \in K$$

- Se α è radice doppia di q, allora α è radice di q', altrimenti no

$$q'(x) = \sum_{i=1}^{m} \cdot \prod_{\substack{j=1 \\ j\neq i}}^{m} (x-\alpha_j)$$

tutti gli addendi si annullano in $\alpha = \alpha_1$ (wlog), tranne

(forse) $\prod_{j=2}^{m} (x-\alpha_j)$. Questo si annulla sse $\alpha = \alpha_j$ per qualche $j \geq 2$

REGOLA DI LEIBNITZ $\quad (fg)' = f'g + fg'$ segue dalla def. di der. di un polinomio $\left(\sum a_i x^i\right)' = \sum i a_i x^{i-1}$

$$\left(x^{p^k} - x\right)' = p^k \cdot x^{p^k-1} - 1 = -1 \quad (\text{perché } p = 0 \text{ in } K_N)$$

(Da questo punto $K_N = S$, basta ricostruirlo ...)

Le radici di $x^{p^k} - x$ contenute in $\Phi_{p^k-1}(x)$ hanno ordine esattamente $p^k - 1$, le altre no.

Prendiamone una, diciamo α.

$\mathbb{F}_p[\alpha] = \left\{ \begin{matrix} \text{tutti gli el. di } K_N \text{ esprimibili come} \\ \text{pol. calcolati in } \alpha \text{, con coeff. in } K_0 \end{matrix} \right\}$

$= K_N$ perché contiene $1, \alpha, \alpha^2, \dots \alpha^{p^k-2}$

α ha un polinomio minimo, chiamiamolo $q(x)$.
Che grado ha q? k.
Infatti $1, \alpha, \alpha^2, \dots \alpha^{\deg q - 1}$ sono una base di
K_N su K_0 (verificatelo...)

q è un polin. di grado k, ed è irriducibile su $\mathbb{F}_p$
perché è il pol. minimo di α su $\mathbb{F}_p$.

Ugualmente, se α è radice di $\Phi_d(x)$ con $d \mid p^k - 1$
$d \neq p^k - 1$, allora $\alpha^{\boxed{p^h - 1}} = 1$ per qualche $h < k$ $(h \mid k)$ falso

$K_0[\alpha]$ contiene al massimo α^{p^h} elementi, è un campo pure lui, ma è più piccolo di K_N falso falso

$\Rightarrow \dim K_0[\alpha] / \mathbb{F}_p = [K_0[\alpha] : \mathbb{F}_p] \leq h < k$

il pol. minimo di α ha grado al massimo h

<u>OSS</u> Ciò che è falso, a volte è vero. Ci sono alcuni
$d \mid p^k - 1$ con $d \nmid p^h - 1$ per alcun $h \mid k$ e
ci sono altri d per cui $\exists\, h \mid k$ per cui $d \mid p^h - 1 \mid p^k - 1$

$\Phi_d(x)$ ha come radice α. Se d è del primo tipo, allora $\underbrace{K_0[\alpha]}_{\text{è un campo}}$ è tutto K_N, altrimenti no.

Fatto: Un sottoanello di un campo finito è un campo (finito)

$\beta \in$ sottoanello, $\beta \neq 0$ $\beta, \beta^2, \beta^3, \dots$ sono tutti nel sottoanello.

Pigeonhole + il campo è finito $\Rightarrow \beta^n = \beta^m \quad m < n$

$\beta^{n-m} = 1 = \beta \cdot (\beta^{n-m-1}) \qquad \frac{1}{\beta}$ è nel sottoanello

Facciamo ordine • $x^{p^n} - x$ ha delle radici, che sono tutti (e soli) gli elementi di K_N.

- Se $\alpha \in K_N \quad K_0[\alpha] \subseteq K_N$ è un sottocampo.
- Poiché $|K_n| = p^k$, $|K_0[\alpha]| = p^h$ con qualche $h \mid k$
- Se $h < k$, allora $\alpha \in \mathbb{F}_{p^h} = \{ \text{el. } \beta \in K_N : \beta^{p^h} = \beta \}$
  - allora il pol. min. di α ha grado $< k$ (ha grado h)
- Se $h = k$, allora il pol. min. di α ha grado k
- α è radice di $\Phi_d(x)$ per qualche $d \mid p^k - 1$
- Se $\Phi_d(x) \mid x^{p^h} - x$ per qualche $h < k$, siamo nel 1° caso, altrimenti nel secondo.

- $\Phi_d(x)$, se $d \nmid p^h - 1$ per alcun $h < k$, si fattorizza in pol. irr. su $\mathbb{F}_p$ di grado k (tutti distinti)

Successioni di Mersenne (o di MerSam)

$a_0, a_1, a_2, \dots$ succ. di numeri naturali si dice di MerSam se $\forall\, m, n \in \mathbb{N}$

$$a_{(m,n)} = (a_m, a_n)$$

(variante: a_n a valori in un anello in cui il m.c.d. è ben definito)
Esempio: $K[x]$

Esempi ① $a_n = n^K$ (K naturale)

② $a_n = K^n - 1$ $K \geq 2$ fissato

③ $a_n = x^n - 1$ nei polinomi $\mathbb{Q}[x]$

Facciamolo • Se $m \mid n$, $(K^m - 1) \mid (K^n - 1)$ (NOTO)

$\Rightarrow K^{(m,n)} - 1$ divide $(K^m - 1, K^n - 1)$ (idem con X)

• Suppongo $m > n$. Se $d = (K^m - 1, K^n - 1)$ $m = bn + c$, $c < n$

$$d \mid (K^m - 1) - \underbrace{(K^m - K^c)}_{K^c \cdot (K^{bn} - 1) \text{ è un multiplo di } K^n - 1} = K^c - 1$$

quindi $d \mid K^c - 1$ $d \mid (K^n - 1, K^c - 1)$

$\dots \Rightarrow d \mid K^{(m,n)} - 1$ (idem con X)

④ Successioni per ricorrenza opportune (a valori interi)

$a_0 = 0$ $a_1 = a$ $a_{n+2} = b\, a_{n+1} + a_n$

qui ci va $+1$

con b e c coprimi (OSS. Il caso $a=1$ è quello interessante)

(Caso particolare: $a_n = F_n$ numeri di Fibonacci)

- Se $m | n$, allora $a_m | a_n$: ragioniamo modulo a_m

$0, 1, b, \ldots \qquad a_k \; a_{k+1} \qquad a_h \; a_{h+1}$

$\exists\, k, h \leq a_m^2 + 1$ per cui $a_k \equiv a_h$. $a_{k+1} \equiv a_{h+1}$ mod m $\Rightarrow$ .... eccetera

OSS $a_m \equiv 0 \quad (a_m) \qquad a_{m+1} \equiv l \quad (a_m)$

allora da a_m ad a_{2m} ripeto gli stessi resti mod (m) visti da a_0 a a_m, ma moltiplicati per l $\Rightarrow a_{2m} \equiv l \cdot a_m \equiv 0 \quad (a_m)$

DOMANDA Esistono altri a_i multipli di a_m, ma con $m \nmid i$? No, perché l (e in generale a_{km+1}) sono coprimi con a_{km} che è multiplo di a_m $\Rightarrow$ a_{km+1} è invertibile mod (a_m) $\Rightarrow$ Se a_i è multiplo di a_m, allora anche $a_{i \bmod (m)}$ lo è. Facciamo che b era >0, otteniamo un assurdo perché a_n è crescente in n (il caso $b<0$ comunque è trattabile...)

- $m | n \Rightarrow a_m | a_n$ fatto $\qquad a_{(m,n)} | (a_m, a_n)$

- Abbiamo dimostrato che i multipli di a_m sono tutti e soli gli a_{km}. Similmente (stesso procedimento), se $d > 0$ e $d \mid a_m$ ma $d \nmid a_1, a_2, \dots a_{m-1}$ allora i multipli di d sono a_{km}.

  $d = (a_m, a_n)$: i suoi multipli sono tutti gli

  a_{kh} per qualche h fissato, K variabile.

  h deve però dividere m e n $\Rightarrow h \mid (m, n)$

  $\Rightarrow d \mid a_{(m,n)}$

Lemma utile: Se $(a_0), a_1, a_2, \dots$ è una success. di Mersenne, e $K > 0$, $m > 0$, allora

$$\left(\prod_{i=1}^{K} a_i \right) \Bigg| \left(\prod_{i=m+1}^{m+K} a_i \right)$$

Esempio $a_i = i$: $K! \mid (m+1) \cdot \dots \cdot (m+K)$

vero perché il rapporto è $\binom{m+K}{K}$ che è intero

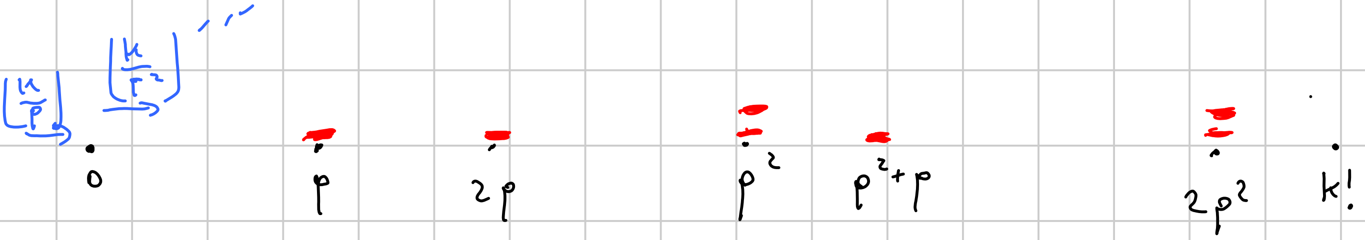
Domanda di Andrea: È sempre vero, data (a_n) di Mersenne, che, per ogni K e per ogni N

$$m.c.d \left\{ \prod_{i=m+1}^{m+K} a_i \right\}_{m \geq N} = \prod_{i=1}^{K} a_i \quad ?$$

DIM lemma utile: Scelgo p primo e stimo le valutazioni p-adiche a sinistra e a destra.

RICORDO

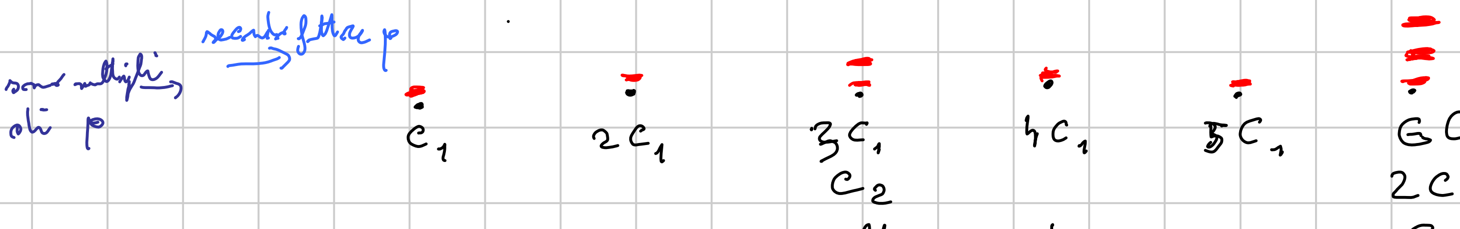
$$v_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \dots$$



OSS Fissato $d > 0$, esiste c t.c. gli a_i multipli di d sono esattamente quelli per cui i è un multiplo di c

DIM Come fatto prima (è una ridef. equivalente di successione di Mersenne)

Come sarà ora il disegno?



c_1 t.c. a_{kc_1} sono i multipli di p

c_2 t.c. // // p^2

c_3 // // p^3

(c_2 è multiplo di c_1)

$$v_p\left(\prod_{i=1}^{k} a_i\right) = \left\lfloor \frac{k}{c_1} \right\rfloor + \left\lfloor \frac{k}{c_2} \right\rfloor + \dots$$

OSS Nell'intervallo $m+1, \dots, m+k$, ci sono almeno

$\left\lfloor \frac{K}{c_i} \right\rfloor$ multipli di c_i, quindi

la sequenza $a_{m+1}, \dots, a_{m+K}$ contiene almeno

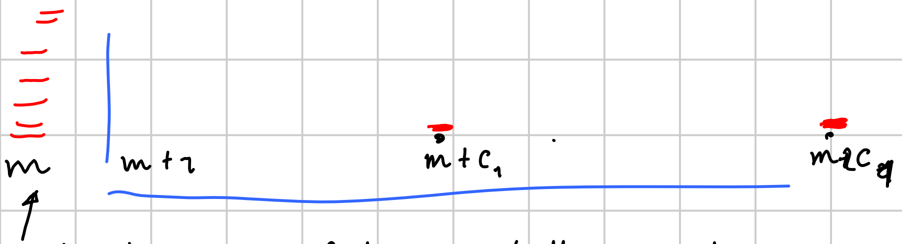
$\left\lfloor \frac{K}{c_1} \right\rfloor$ multipli di p, almeno $\left\lfloor \frac{K}{c_2} \right\rfloor$ multipli di p^2,

$$\dots \Rightarrow v_p\left(\prod_{i=m+1}^{m+K} a_i\right) \geq \sum \left\lfloor \frac{K}{c_i} \right\rfloor$$

□

Torniamo alla domanda di prima

Sia c un multiplo di tutti i $c_i < K$. Sia $m > N$ e $m \equiv 0 \pmod{c_i}$. Allora



qui ho tantissimi fattori p, tutti sprecati

Funzione $f : \{\text{primi}\} \to \{\text{primi}\}$ $\quad f(p)$ = il più piccolo primo $> p$

$$a_n = f(p_1)^{\alpha_1} \cdot \ldots \cdot f(p_k)^{\alpha_k} \quad \text{se } n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$$

Questa è di Mersenne, ma 2 non compare mai.

La risposta alla domanda di Andrea è SÌ !!!

Esercizi

- p primo dispari, allora $\prod_{k=1}^{p-1} k^{2k-p+1}$ è intero
- $c_n = n(n+1)$; $l, m, k > 0$ per cui $m+k+1$ è primo $> l+1$. Allora

$$(c_1 \cdot \ldots \cdot c_\ell) \mid \left[(c_{m+1} - c_k) \cdot \ldots \cdot (c_{m+\ell} - c_k)\right]$$

Classici da Vieta jumping (o quasi)

- $x, y > 0$ interi $\frac{x^2+y^2+1}{xy}$ è intero, allora vale 3 (già visto ...)

- $x, y, z \geq 0$ interi, $(xy+1)(yz+1)(zx+1)$ è un quadrato. Allora i tre fattori sono quadrati.

- $n > 0$ tale che $2 + \sqrt{12n^2+1}$ è intero; allora è un quadrato

Variante: $p \equiv -1 \pmod 4$ $2 + \sqrt{4pn^2+1}$ intero; allora è un quadrato (wow!).

Pubblicità: Volete un problema di TdN da risolvere ma non sapete dove trovarlo? Consultate il PEN (Problems in Elementary Number theory).

Altra pubblicità (proposta da Federico e modificata da cip999)

Auguriamo un oro alle IMO al formulatore della congettura sulle successioni di MerSam che si è rivelata vera:

VIOLA ORO, ORO ALLE IMO!!!...

#CIP999OROPURELUI

VIETA JUMPING / DISCESA INFINITA

$\frac{x^2+y^2+1}{xy}$ intero $\Rightarrow$ è 3

<u>oss</u> Se $x=y=1$ allora viene 3
$x=2 \quad y=1$ //

Facciamo che viene K

$x^2+y^2+1-Kxy=0$ lo vedo come pol. in x

$x^2-ky\cdot x+y^2+1=0$ ha due radici:
una è x_1 (quella della coppia (x_1,y) da cui parto)
l'altra è $x_2=\frac{y^2+1}{x_1}>0$ x_2 è intera perché

$x_2=ky-x_1$. Speranza: $x_2<x_1$

Basta (forse) $x_1>y$ perché allora (forse) $x_2\leq y$ ...

$x_2=\frac{y^2+1}{x_1}\leqslant\frac{y^2+1}{y+1}\leqslant y$ con $=$ sse $y=1$
$x_1=y+1=2$

Quindi mi riduco quasi sempre a una coppia con una delle comp. invariata e l'altra diminuita, a meno che non capiti una di queste:

- $x=y$ $\Rightarrow$ si finisce in fretta
- $x=2$ $y=1$ $\Rightarrow$ viene 3

PEN A 1 $(xy+1)(yz+1)(zx+1)$ è un $\square$, con $x,y,z \geq 0$. Allora i 3 fattori sono quadrati.

Idea Se uno tra x,y,z è 0, allora la tesi è vera.

Idea Se $\overset{\text{wlog}}{x=y}$, allora x deve essere 0 o il prodotto non è un $\square$. Possiamo supporre $x<y<z$, $z \geq 2$ (anzi, $x \geq 1$ altrimenti concludo ...)

Vorrei passare da $(z,y,x) \longrightarrow (t,y,x)$ con t più piccolo di z

OSS (Differenza dal problema precedente) Stavolta il polinomio interessante

$$(xy+1)(yz+1)(zx+1)-k^2$$

non è monico in z (se xy divide gli altri coeff.... ma non c'è da sperarci)

Idea Cerchiamo un polinomio di 2° grado in t, monico, nelle variabili x,y,z,t, con $\Delta =$ un parente di $(xy+1)(yz+1)(zx+1)$, simmetrico in x,y,z,t

Magia (fare un po' di tentativi)

$$x^2+\overbrace{y^2+z^2+t^2}^{U}+a\overbrace{\sum_{sym} xy}^{V}+b\overbrace{\sum_{sym} xyz}^{W}+\overbrace{c\,xyzt}^{P}$$

$$+d\overbrace{\sum_{sym} x}^{S}+\overbrace{e}^{N}$$

qui sym è da intendersi "cum grano salis"

OSS Δ ha solo monomi di grado pari.

Δ è un polinomio in U, V, W, P, S, N (quasi vero)

(Qui non so se si può fare qualche altra considerazione

$$\underbrace{\sum t^2}_{4 \text{ termini}} - 2\underbrace{\sum xy}_{6 \text{ termini}} - 4xyzt - 4$$

$$\Delta_t = 4(xy+1)(yz+1)(zx+1)$$

Parto da $(x,y,z) \rightsquigarrow (x,y,t)$. Vorrei le seguenti cose:

- $t < z$
- $t \geq 0$
- $(xt+1)$, $(yt+1)$ e $(xy+1)$ non sono tutti quadrati.
- $(xt+1)(yt+1)(xy+1)$ è un $\square$

$$= (x+y-z-t)^2 - 4xy - 4zt - 4xyzt - 4 = 0$$

$$(x+y-z-t)^2 = 4(x\underline{y}+1)(z\underline{t}+1) \quad \text{e cicliche (magia)}$$

$$\square = 4(y\overline{z}+1)(x\underline{t}+1)$$

$$\square = 4(z\underline{x}+1)(y\underline{t}+1)$$

$zt+1 \geq 0 \quad t \geq -\frac{1}{z}$ ma è intero $\Rightarrow t \geq 0$

Almeno un _ non è $\square \Rightarrow t \geq 1$

Anzi, almeno due _, in particolare almeno uno tra $(xt+1)$ e $(yt+1)$ non è un $\square$

Speranza: $t < z$ (almeno una delle due radici)

Il termine noto di rispetto a t è

$$\cancel{z^2} > x^2 + y^2 + \cancel{z^2} - 2xy - 2yz - 2xz - 4 = t_1 \cdot t_2$$

batte

batte

ok (uso che z è il più grande)