"TON" ADVANCED

Titolo nota 06/09/2011

ESERCIZIO: (IMO 6 / 2007)

SIA $S = \{ (x,y,z) \in \mathbb{Z}^3 : 0 \le x \le \ell, 0 \le y \le m, 0 \le z \le n, (x,y,z) \neq (0,0,0) \}$

QUANTI PIANI SERVONO CHE NON PASSINO PER ORIGINE TALI CHE $S \subseteq$ UNIONE PIANI?

$\ell + m + n$ BASTANO $x = 1, \dots, x = \ell$
$y = 1, \dots, y = m$
$z = 1, \dots, z = n$

K PIANI CHE VANNO BENE $(K < \ell + m + n)$

$S \subseteq$ UN PIANO

$P_i = \{ (x,y,z) : a_i x + b_i y + c_i z + d_i = 0 \}$

$VP_i = \{ \prod_{i=1}^{K} (a_i x + b_i y + c_i z + d_i) = 0 \}$

MA PIU' IN GEN, POL $f(x,y,z)$ CHE GRADO DEVE AVERE?

$g(x,y,z) = f(x+1, y, z) - f(x,y,z)$

$\deg g = \deg f - 1$

$g(0,0,0) = f(1,0,0) - f(0,0,0) = -A(0,0,0) \neq 0$

$0 \le x \le \ell - 1, \ 0 \le y \le m, \ 0 \le z \le n \quad (x,y,z) \neq (0,0,0)$

$g(x,y,z) = f(x+1,y,z) - f(x,y,z) \neq 0 = 0$

PER INDUZ. SI CONCLUDE.

COMBINATORIAL NULLSTELLENSATZ

$f(x)$ POL. DI GRADO d HA AL PIÙ d RADICI.

$f(x_1,\dots,x_n)$ $\deg f$ IN $x_i = d_i$ $f \neq 0$

se posso scegliere x_i in d_i+1 modi
riesco a non farlo annullare.

$S_1,\dots,S_n$ $|S_i| = d_i+1$ $\exists x \in S_1 \times \dots \times S_n$: $f(x) \neq 0$?

C. NSS:

$f(x_1,\dots,x_n)$ POLINOMIO DI GR. d.

$\sum a_{d_1,\dots,d_n} \cdot x_1^{d_1} \cdot \dots \cdot x_n^{d_n}$

SE ESISTE UN MONOMIO $x_1^{d_1} \dots x_n^{d_n}$ CON

$d_1 + d_2 + \dots + d_n = d$ DI COEFF. NON NULLO

ALLORA "SE POSSO SCEGLIERE x_i IN d_i+1 MODI E RIESCO A NON FARLO ANNULLARE"

[] $x^2y + y^3$ FUNZIONA MEGLIO IL Th NUOVO.

DIM $f(x_1,\dots,x_n)$

$$P_1(x_1) = \prod_{s \in S_1} (x_1 - s) \qquad P_2(x_2) = \dots$$

P_1 SI ANN. SU $S_1 \times \dots \times S_n$

P_1 HA GRADO $d_1 + 1$

CAUCHY – DAVENPORT!

$A, B \subseteq \mathbb{Z}_p$ $\quad A+B := \{ a+b \mid a \in A, b \in B \}$

$\boxed{A+B = \mathbb{Z}_p}$ OPPURE $|A+B| \geq |A| + |B| - 1$

$\prod_{c \in A+B} (x+y-c) =: f(x,y)$

$|A+B| \leq |A| + |B| - 2$

$x^{d_1} y^{d_2}$ $\quad d_1 \leq |A|-1$ $\quad d_2 \leq |B|-1$

$d_1 + d_2 = |A+B|$

$\boxed{\binom{|A+B|}{d_1}}$

ES $\quad A+A = \{ a+b \mid a, b \in A, a \neq b \}$

$A \subseteq \mathbb{Z}_p$ $\quad$ Th $\quad A+A = \mathbb{Z}_p$ OPPURE $|A+A| \geq 2|A| - 3$

CHEVALLEY WARING

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_K(x_1, \dots, x_n) = 0 \end{cases} \qquad x_i \in \mathbb{Z}_p$$

SE $n > \deg(f_1) + \dots + \deg(f_k) \Rightarrow$

SOL. AL SIST. IN $(\mathbb{Z}_p)^n$ È DIVISIBILE PER p.

OSS $1 - x^{p-1}$ È 0 SE E SOLO SE x NON LO È.

DEF $F(x) := \prod_{i=1}^{k} (1 - f_i(x_1, \dots, x_n)^{p-1})$

$$\#\text{SOL} \equiv \sum_{x \in \mathbb{Z}_p^n} F(x) \equiv 0$$

$$\sum_{\lambda=1}^{p} \lambda^k \equiv 0 \pmod p$$
SE $p-1 \nmid k$

DEF AGGIUSTA I DETTAGLI

COR SE CE' UNA SOL CE N'E' UN'ALTRA.

NSS $\Rightarrow$ COR.

$x_1 = a_1, \dots, x_n = a_n$ SIA SOL.

$$\left(\prod_{i=1}^{k} (1 - f_i(x_1, \dots, x_n)^{p-1}) \right) - \prod_{i=1}^{n} (1 - (x_i - a_i)^{p-1})$$

$\downarrow$

$n \geq \deg(f_1) + \dots + \deg(f_k)$

HA GRADO $n-(p-1)$

SE NON SI ANNULLA C'HO UN'ALTRA SOLUZIONE

$x_1^{p-1} \cdot \dots \cdot x_n^{p-1}$ HA COEFF. $\neq 0$ E E' DI GR. MAX

PONENDO $S_i = \mathbb{Z}_p$ $\forall i$ E NSS. TROVO PT CON VAL $\neq 0 \Rightarrow$ NUOVA SOL.

$$x_1^d + \dots + x_{ol}^d \equiv K \pmod p$$

$$x_1^d + \dots + x_d^d \equiv K x_{d+1}^d \pmod p$$

$$\left(\frac{x_1}{x_{d+1}}\right)^d + \dots + \left(\frac{x_d}{x_{d+1}}\right)^d \equiv K$$

CON CHEVALLEY-WARING FACCIO $K \equiv -1$ (È VALIDO).

$$\left|\left\{x_1^d \mid x_1 \in \mathbb{Z}_p\right\}\right| = \frac{p-1}{MCD(p-1,d)} + 1 \geq \frac{p-1}{d} + 1$$

CAUCHY DAVENPORT A RAFFICA!

$$|A_1 + \dots + A_d| \geq |A_1| + \dots + |A_d| - d + 1$$

$$\sum_{i=1}^{k} a_i x_i^{d_i} = m \qquad \text{SI SCEGLIE } p \equiv 1 \bmod d_i$$

ES SE $a_i \not\equiv 0 \bmod p$ $\forall i$ E $\sum \frac{1}{d_i} \geq 1$

C'È SOL MOD p

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

ES $A+A = \{a+b \mid a,b \in A, a \neq b\}$

$A \subseteq \mathbb{Z}_p$ TH $A+A = \mathbb{Z}_p$ OPPURE $|A+A| \geq 2|A|-3$

ES IL PRIMO PROBL. ITA UNA SOL. CON NSS.

SAPRESTE TROVARLA?

LEMMA DEL PERMANENTE

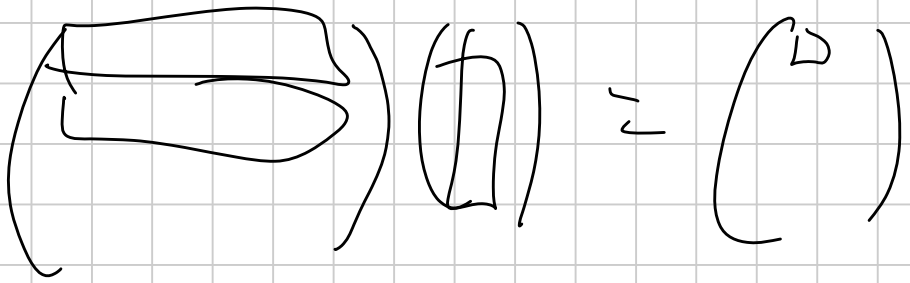
A MATRICE $n \times n$ A COEFF. IN F

b VETT. lungo n

FISSATI $S_1, \dots, S_n$ con $|S_i| = 2$

$\exists\, x \in F^n$: Ax E b hanno Π le coord. div. ($Ax - b$ ha Π coord. $\neq 0$).

A PATTO PERM $(A) \neq 0$.



$$\sum_{\sigma} a_{i,\sigma} x_{\sigma} - b_i \neq 0 \qquad \forall i$$

$$\prod_{i} \left(\sum_{\sigma} a_{i,\sigma} x_{\sigma} - b_i \right) \quad \text{HA GR. } n.$$

$$\sum_{\sigma} \prod_{i=1}^{n} a_{i,\sigma(i)} \quad \text{DETTO PERM.}$$

APPL:

WL DI UN PU^2 DI METRO PA. CO FORSE MOLTI QUANTI EL DI $(\mathbb{Q}_p)^n$ POSSO PRENDERE A CASO CHE NESSUNA SOMMA PARZIALE FACCIA 0? (non per forza distinti)

$n(p-1)$ LI TROVI.

$p-1$ VOLTE $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $p-1$ VOLTE $\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$n(p-1)+1$ NON SI PUÒ!

ES CON CAUCHY-CARNICA

MA SI PUÒ FARE DI PIÙ

PRENDIAMO $n(p-1)$ VETTORI $v_1, \dots, v_{n(p-1)}$

$$\begin{pmatrix} (v_1) & v_2 & \cdots & v_{n(p-1)} \\ (v_1) & \cdot & & \vdots \\ \vdots & & & \\ (v_1) & v_2 & \cdots & v_{n(p-1)} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{n(p-1)} \end{pmatrix}$$

$\neq$ COORD. PER COORD. $\begin{pmatrix} v+1 \\ v+2 \\ \vdots \\ v+p-1 \end{pmatrix}$

$$\begin{pmatrix} (v) \\ (v+1) \\ \vdots \\ (v+1) \end{pmatrix}$$

$$\begin{pmatrix} w \\ w \\ \vdots \\ w \end{pmatrix}$$

$$\begin{pmatrix} (v+1) \\ (v+2) \\ \vdots \\ (v+p-1) \end{pmatrix}$$

E SE PERM $(\pi) = 0$?

$$\prod_{n} \left(\sum_{j} a_{ij} x_j - b_i \right) - \lambda \prod_{j} (1 - x_j)$$

$$\sum_{\sigma} \prod_{n} a_{i,\sigma(i)} = 0$$

$\left(V_1 \dots V_{n(p-1)}\right)\left(\quad\right) \overset{t}{\underset{\text{COORD.}}{\quad}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 2 \\ 2 \\ \vdots \\ p-1 \\ \vdots \\ p-1 \end{pmatrix}$

$V_1, \dots, V_{n(p-1)}$

C.W $\Rightarrow$) se nessuna somma fin. è zero, le somme parziali sono suriettive (1)

NSS $\Rightarrow$) se $\mathrm{PERM}(\Pi) \neq 0$ le som. sono surj

NSS $\Rightarrow$) se $\mathrm{PERM}(\Pi) = 0$ ALLORA c'è somma fin $= 0$.

GRAFI $(?,2,2)$

G grafo finito V VERTICI E LATI

$(p-1)|V| \leq |E|$

OGNI VERTICE HA AL PIÙ $2p-1$ VICINI (GRADO $\leq 2p-1$)

TH. ESISTE SOTTOGRAFO p-REGOLARE.

X_e e $\in E$ le variabili

$$\prod_{v \in V}\left[1-\left(\sum_{e \text{ "PASSA PER } v\text{"}} X_e\right)^{p-1}\right] - \prod_{e \in E}(1-X_e)$$

$$v \in V \left\{ \sum_{e \text{ "PASSA PER } v\text{"}} X_e^{p-1} = 0 \right.$$

TROVO S. GRAFO p-REG.

TR ERDÖSS-GINZBURG-ZIV

PRESI $2p-1$ INTERI (NON PER FORZA DISTI.)

NE POSSO SCEGLIERE p LA CUI SOMMA

È MULTIPLA DI p. C.V. C.D. $\Sigma \alpha_1 + \dots + \alpha_p^{p-1}$

AND NOW FOR SOMETHING

COMPLETELY DIFFERENT!

$\Phi_n(X) = \prod_{\omega \text{ rad. prim. } n\text{-esima di unità}} (X-\omega)$

Φ_n È MONICO CON COEFF. INTERI

$\prod_{d|n} \Phi_d(X) = X^n - 1$

$X^n - 1 \qquad nX^{n-1} \qquad p|n \cdot nX^{n-1} \equiv 0$

$p \nmid n$

$-(X^n-1) + \frac{X^n}{n} \cdot nX^{n-1} = 1$ NON HA FATTORI DOPPI

RIDURSI MOD DA INF. SU COSA DEVE ESSERE FATTA UNA FATT. IN $\mathbb{Z}$.

CRIT. DI EISENSTEIN

$X^n + a_{n-1}X^{n-1} + \dots + a_0 = f(X)$ $p|a_i$ $\forall i$ IL POL.

$p^2 \nmid a_0$ $\Rightarrow$ È IRR.

$f(X) = g(X)^{\alpha} \cdot h(X)^{\beta}$

$f(X) \equiv g(X) \cdot h(X) \quad (\mod p)$

$g(X) = X^{\alpha} + p(\dots) \qquad h(X) = X^{\beta} + p(\dots)$

$\Phi_p(X) = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \dots + 1$

$X = Y + 1 \qquad \dfrac{(Y+1)^p - 1}{Y} = Y^{p-1} + \sum_{i=1}^{p-1} Y^{i-1} \binom{p}{i}$

$\Phi_p(X)$ È IRRIDUCIBILE.

$\Phi_n(X) = f(X) g(X) \qquad p \nmid n$

ω RAD. DI f

$\boxed{\Phi_n(X) = f(X) g(X)}$ VALE IN $\mathbb{F}_p$

$\omega = f(\alpha)^p = f(\alpha^p) \qquad (\alpha+\beta)^p = \alpha^p + \beta^p$

α RAD. DI $f(X) \Rightarrow \alpha^p$ RAD. DI $f(X)$ IN $\mathbb{C}$. $\forall p \nmid n$

$\alpha \qquad \alpha^k = \alpha^{p_1 \cdot p_2 \cdots p_r}$

α rad. $f \Rightarrow \alpha^{p_1}$ rad. $f \Rightarrow (\alpha^{p_1})^{p_2}$ rad. $f \dots \Rightarrow \alpha^k$ rad. f.

$\Rightarrow \Phi_n(X)$ IRR.

$\boxed{(X-\omega)\cdot(X-\omega^p)\cdot\dots\cdot(X-\omega^{p^K})} \qquad K = \operatorname{ord}_n(p) - 1$

come si conta p. modulo p.

a INTERO $\quad \Phi_n(a) \quad p \mid \Phi_n(a)$

$p \nmid n \quad x^n - 1$ NON HA RADICI DOPPIE

a è UNA RADICE DI $x^n - 1$.

$\mathrm{ord}_p(a) \mid n \quad a^d \equiv 1 \quad d < n$

$\Rightarrow \quad x - a \mid x^d - 1 \quad x - a \mid \Phi_n(x)$

$(x^d - 1)\ \Phi_n(x) \mid x^n - 1 \Rightarrow \mathrm{ord}_p(a) = n$

$\mathrm{ord}_p(a) = n \Rightarrow \Phi_n(a) \equiv 0 \pmod p$

$p \mid n \quad n = p \cdot d \quad a^d \equiv 1 \pmod p$

$\Phi_n(x) \mid \dfrac{x^{dp} - 1}{x^d - 1} \qquad p \mid \dfrac{a^{dp} - 1}{a^d - 1}$

$n = p^k \cdot s \quad (n, s) = 1$

$\mathrm{ord}_p(a) < s \quad s = \mathrm{ord}_p(a) \cdot r \quad r \geq 1$

$\Phi_n(x) \mid \dfrac{x^{p^k \cdot \mathrm{ord}_p(a) \cdot r} - 1}{x^{p^k \cdot \mathrm{ord}_p(a)} - 1}$

$\boxed{n \geq p^k \cdot \mathrm{ord}_p(a)} \qquad p \,\|\, \Phi_n(a)$.

$a \quad n$ INT. POS. $\quad p$ T.C. a HA ORD $n \bmod p$,

$\Phi_n(a) = \pm p \qquad p \leq n$

$\boxed{|\Phi_n(a)| \leq \ldots}$

$a \geq 3$

$$\left| \prod_{\substack{\omega \text{ rad.} \\ \text{prim}}} (a-\omega) \right| = \prod |a-\omega| \geq 2^{\phi(n)} \geq n$$

ASSURDO.

COR $\exists$ inf. primi $\equiv 1 \pmod n$

SUPP. CHE CI SIANO FIN. $P = \prod_{p \equiv 1 (n)} p$

$\exists\, p$ primo, t.c. $\Phi_n(P) = n \Rightarrow p \equiv 1 (n)$

$\Rightarrow p \mid P$

$x^{p-1} - 1$ HA TT. LE RAD MOD p (SI CP. IN FATT. LIN.)

$\Phi_{p-1}(X)$ HA TT. RAD MOD p $\quad \Phi_{p-1}(X) \mid x^{p-1} - 1$

α rad. di $\Phi_{p-1}(X)$ IN $\mathbb{F}_p$

$p \nmid p-1$ $\quad \text{ord}_p(\alpha) = p-1$ $\quad x^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(X)$

ES p PRIMO $\exists q$ t.c. p NON È UN RESIDUO p-ESIMO IN $\mathbb{Z}_q$

$p \nmid n^p \pmod q$ NON HA SOL

ITA 6 ANNI IGNOTO