TEORIA DEI NUMERI - MEDIUM 1

Note Title 9/4/2017

Ballo

- POLINOMI IN $\mathbb{Z}_p$ E AFFINI
- ESTENSIONI "PICCOLE" DI $\mathbb{Z}_p$
- RESIDUI QUADRATICI IN $\mathbb{Z}_p$
- GENERATORI E POLINOMI CICLOTOMICI (PROBABILMENTE NELLA PROSSIMA)

TEOREMA DI FERMAT (PICCOLO)

$(a,n)=1$ ⟺ MCD

$a^{\varphi(n)} \equiv 1 \pmod n$

] ALLORA IL TEOREMA DI EULERO

SE n È PRIMO SI CHIAMA FERMAT

L'IDEA È QUELLA DI PRENDERE TUTTI I RESIDUI MOD n COPRIMI CON n.

CON $n=10$

1, 3, 7, 9

È CONSIDERARE LA MAPPA

$$x \mapsto ax \pmod{n}$$

CON $(a, n) = 1$ FISSATO

SE PRENDO TUTTI I RESIDUI COPRIMI CON n E LI MOLTIPLICO PER a CI STO PERMUTANDO

$$1 \cdot 3 \cdot 7 \cdot 9 \equiv 3 \cdot 9 \cdot 1 \cdot 7 \pmod{10}$$

$$\downarrow$$

$$a \cdot 1 \cdot a \cdot 3 \cdot a \cdot 7 \cdot a \cdot 9 \pmod{10}$$

$$1 \cdot 3 \cdot 7 \cdot 9 \cdot a^4 \pmod{10}$$

$$a^4 \equiv 1 \pmod{10}$$

WILSON

p PRIMO

$$(p-1)! \equiv -1 \ (p)$$

- CON GLI INVERSI

SE FACCIO IL PRODOTTO DI TUTTI I RESTI $\neq 0 \ (p)$

ACCOPPIO (a, b) CON $a \cdot b \equiv 1 \ (p)$

TUTTI SI POSSONO ACCOPPIARE PERCHÉ $a \neq b$, TRANNE QUELLI CON

$$a^2 \equiv 1 \ (p)$$

LORO SI ACCOPPIANO DA SOLI

$a^2 \equiv 1 \ (p)$ HA SOLO ± 1 COME SOLUZIONE

$$(a-1)(a+1) \equiv 0 \ (p) \rightarrow \begin{matrix} a \equiv -1 \ (p) \\ a \equiv 1 \ (p) \end{matrix}$$

COS'HO: 1 DA SOLO, -1 DA SOLO $\Big] \ p > 2$

TUTTI GLI ALTRI ACCOPPIATI → IL LORO PRODOTTO FA 1

(È IL PRODOTTO DI TANTE COPPIE CHE FANNO 1)

$\longrightarrow \quad -1 \ (p)$

- GENERATORI (QUASI OVVIE)
- POLINOMI

CONSIDERIAMO IN $\mathbb{Z}_p$ IL POLINOMIO

$$X^{p-1} - 1$$

CHE RADICI HA? (FERMAT)

$\{1, 2, \dots, p-1\}$ SONO RADICI

$$X^{p-1} - 1 \equiv (X-1)(X-2)(X-3)\dots(X-(p-1)) \quad (p)$$

STESSO TERMINE NOTO

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

SE $p>2$ $\quad -1 \equiv (p-1)! \quad (p)$

IL PROBLEMA DI QUESTA DIMOSTRAZIONE È ☆

NON È DETTO CHE POSSIAMO SCRIVERE QUELL' UGUAGLIANZA SOLO SAPENDO CE' RADICI

$$x^2-4 \quad (15)$$

CHE RADICI HA? 2 -2 7 -7

$$x^2-4 \neq (x-2)(x+2)(x+7)(x-7) \quad (15)$$

SE CI METTO DENTRO $x=0$

$$-4 \neq 1 \quad (15)$$

IN REALTÀ ☆ HA SEMPRE SENSO MODULO p (A DOPO LO MOSTRO)

ORDINI MOLTIPLICATIVI

$\mathrm{ord}_n(a)$ il minimo $k>0$ t.c.

$$a^k \equiv 1 \ (n)$$

$$\mathrm{ord}_n(a) \mid \varphi(n)$$

$$\mathrm{ord}_p(a) \mid p-1$$

Sia $n>1$ intero positivo p primo t.c.

$$p \mid 2^{2^n}+1$$

$$\longrightarrow 2^{n+1} \mid p-1$$

$$2^{2^n} \equiv -1 \ (p) \longrightarrow 2^{2^{n+1}} \equiv 1 \ (p)$$

$\mathrm{ord}_p(2) \mid 2^{n+1}$ → SE $\mathrm{ord}_p(2) = 2^k$ CON $k \le n+1$

$$\mathrm{ord}_p(2) \mid p-1$$

$$2^{2^k} \equiv 1 \ (p)$$

ELEVO AL $n-k$ VOLTE ↓

$$2^{2^n} \equiv 1 \ (p)$$

Assurdo! $2^{2^n} \equiv 1 \pmod p$ $2^{2^n} \equiv -1 \pmod p$

$\longrightarrow p = 2$ ($2^{2^n}+1$ È DISPARI).

PERCIÒ $\mathrm{ord}_p(2) = 2^{n+1}$

$2^{n+1} \mid p-1$

FINE DEL RIPASSO

QUANDO POSSO SCRIVERE I POLINOMI SAPENDO LE LORO RADICI?

QUALE CONDIZIONE È NECESSARIA PER SCRIVERE UN POLINOMIO $f(x)$ DI GRADO n NELLA FORMA

$$(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

IN MODO UNICO

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO

AVERE PIÙ DI n RADICI

(SENNÒ $(x-\alpha_1)\dots(x-\alpha_k)$ AVREBBE GRADO $> n$)

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO:

$a \cdot b = 0 \rightsquigarrow a = 0,\ b = 0$

✓ $\mathbb{Z}_6$

✗ $\mathbb{Z}_{15}$ $\quad 3 \cdot 5 = 0$

$\mathbb{Q}, \mathbb{C}, \mathbb{Z}$

AD ESEMPIO: I NOSTRI POLINOMI POSSONO AVERE n RADICI, DI PIÙ, DI MENO

ABBASTANZA BENE ✗

x^2-19

$\mathbb{Q}$: 0, $\pm\sqrt{19}$ IRRAZIONALE

$\mathbb{C}$: 2 $\pm\sqrt{19}$

$\mathbb{Z}_{15}$: 4 2, -2, 7, -7

$\mathbb{Z}_{17}$: 2 ± 6

$x^2-19 \equiv x^2-36 \quad (17)$

$(x-6)(x+6) \equiv 0 \quad (17)$

17 PRIMO

$\mathbb{Z}_{13}$: 0, 2

x^2-19

SUPPONIAMO a SIA UNA SUA RADICE

$a^2 \equiv 19 \ (13) \rightarrow a^2 \equiv 6 \ (13)$

$$6^{12} \equiv 6^6 \ (13)$$

$$1 \equiv 216^2 \ (13)$$

$$1 \equiv 8^2 \ (13)$$

$$1 \equiv -1 \ (13)$$

L'ASSURDO STA NELL'AVER SUPPOSTO CHE ESISTA UN α INTERO.

PRENDIAMO $x^2 - 2$ (3)

0 RADICI.

ALLORA LE CREO: NE CREO UNA (α)

$\mathbb{Z}_3$	$\mathbb{Z}_3(\alpha)$		
0	0	α	2α
1	1	$1+\alpha$	$1+2\alpha$
2	2	$2+\alpha$	$2+2\alpha$

ORA METTO LE REGOLE:

$$\alpha^2 \equiv 2 \quad (\mathbb{Z}_3(\alpha))$$

$$(a+b\alpha) + (c+d\alpha) \equiv (a+c)_{\mathbb{Z}_3} + (b+d)_{\mathbb{Z}_3}\,\alpha$$

$(a+bA)\cdot(c+dA) \overset{\text{NORMALE}}{=}$

$ac + bcA + adA + bdA^2$

$(ac + 2bd)_{\#_3} + A(bc + ad)_{\#_3}$

$+$ E . COMMUTATIVI

VORREMO CHE $\mathbb{Z}_3(A)$ AVESSE, COME $\mathbb{Z}_3$, LA LEGGE DI ANNULLAMENTO DEL PRODOTTO, OSSIA COSA CI SCONFONDE I POLINOMI!

$a \neq 0,\ b \neq 0 \rightarrow ab \neq 0$

$a \in \mathbb{Z}_3(A)$ $\quad$ $b \in \mathbb{Z}_3(A)$

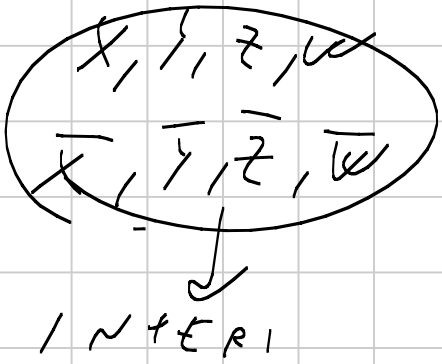
NON SONO INTERI

ASSURDO: $a \neq 0$, $b \neq 0$, $ab = 0$

$a \in b$ SONO IN $\mathbb{Z}_3(A)$

$a = (3x + y) + \alpha(3z + w)$

$b = (3\bar{x} + \bar{y}) + \alpha(3\bar{z} + \bar{w})$



$(y, w) \neq (0, 0)$

$(\bar{y}, \bar{w}) \neq (0, 0)$

$x, \bar{x}, z, \bar{z}$ CI SERVONO? NO

$3x$ SONO TUTTI INTERI

MA NON α

- SOMMA OK
- PRODOTTO PER α È OK

$3k + \alpha$ ✓

$3k \cdot \alpha$

$(3x + 3y\alpha) \cdot \alpha \rightarrow \underbrace{3x\alpha}_{0} + \underbrace{6y}_{0}$

α^2 È INTERO

$x, \bar{x}, z, \bar{z}$ via

$$(y + wx)(\bar{y} + \bar{w}\bar{x}) =$$

$$y\bar{y} + y\bar{w}\bar{x} + w\bar{y}x + 2w\bar{w} = 0$$

$$\begin{cases} x\bar{x} + 2w\bar{w} \equiv 0 \ (3) \\ y\bar{w} + w\bar{y} \equiv 0 \ (3) \\ y\bar{y} - w\bar{w} \equiv 0 \ (3) \end{cases}$$

$$\bar{w} = \frac{y\bar{y}}{w} \ (3)$$

— CASO 1

$w \equiv 0 \ (3)$ ✗

$$x\bar{x} \equiv 0 \ (3)$$

$$x\bar{w} \equiv 0 \ (3)$$

$\hookrightarrow y \equiv 0 \ (3)$

$(x + \alpha w) = 0$

$\hookrightarrow \bar{x} \equiv 0 \ (3) \quad \bar{w} = 0 \ (3)$

$(\bar{x} + \bar{w}\alpha) = 0$

CASO 2: $w \not\equiv 0 \pmod 3$

$\bar{w} \equiv \frac{y\bar{y}}{w} \pmod 3$

$\bar{x} + \alpha\bar{w} \equiv 0 \pmod 3$

$\bar{w} \equiv 0 \pmod 3$

$\bar{y} \equiv 0 \pmod 3$

$\star \quad \frac{y^2\bar{y}}{w} + w\bar{x} \equiv 0 \pmod 3$

$\bar{y}(y^2 + w^2) \equiv 0 \pmod 3$

$y^2 + w \not\equiv 0 \pmod 3$ (FERMAT)

$y^2 + w^2 \equiv y^2 - 2w^2$

$(y + \alpha w)(x - \alpha w) \equiv y^2 - 2w^2$

BISOGNA USARE CHE $x^2 - 2$ NON ABBIA RADICI PER L'ANNULLAMENTO DEL PRODOTTO

SE NON VI FIDATE PROVATE A FARE GLI STESSI CONTI CON $p = 37$ $\alpha^2 = 29$

AFFINCHÉ $y^2 - 2w^2 \equiv 0 \pmod 3 \rightarrow (y, w) = (0,0)$

SE $w \equiv 0 \ (3) \rightarrow y \equiv 0 \ (3)$

ALTRIMENTI $\left(\frac{x}{w}\right)^2 - 2 \equiv 0 \ (3)$

PRENDIAMO $p = 7$ $\quad A^2 = 2$

E CONSIDERIAMO $\mathbb{Z}_7(\sqrt{2})$.

VALE L'ANNULLAMENTO DEL PRODOTTO?

$\sqrt{2} \equiv \pm 3 \ (7)$

$x^2 - 2 \rightarrow (x+3)(x-3)$

$(\sqrt{2}+3)(\sqrt{2}-3) = 2 - 9 = 0$

$\neq 0 \quad \neq 0$ $\qquad$ $\mathbb{Z}_7(\sqrt{2})$

$\mathbb{Z}_p(\sqrt{A})$ HA SENSO (NEL SENSO CHE È BELLO) SE E SOLO SE $x^2 - A \ (p)$ NON HA SOLUZIONI.

- SE HA SOLUZIONE K ALLORA $(K+\sqrt{A})(K-\sqrt{A}) = K^2 - A = 0$
- SE NON CE L'HA, FATE I CONTI E VIENE

COSA ABBIAMO FATTO PRIMA?

ABBIAMO VISTO LE PROPRIETÀ DEI CAMPI.

CAMPO: UN INSIEME CON DUE OPERAZIONI:

- $+$ COMMUTATIVO, ASSOCIATIVO E HA:
  - ELEMENTO NEUTRO (0)
  - INVERSO $(a \to -a)$
- $\cdot$ COMMUTATIVO, ASSOCIATIVO E HA:
  - ELEMENTO NEUTRO (1)
  - INVERSO (TUTTI TRANNE 0) $(a \to a^{-1})$

LEGGE DI ANNULLAMENTO DEL PRODOTTO

SE $a \neq 0, b \neq 0 \to ab \cdot a^{-1} \cdot b^{-1} =$

$= a \cdot a^{-1} \cdot b \cdot b^{-1} = 1 \cdot 1 = 1$ → ab HA INVERSO

(PER COMPLETEZZA DIMOSTRIAMO CHE

$$a \cdot 0 = 0$$

)

$$a \cdot (b - b) = ab - ab = 0$$

DIST.

(0 A PRIORI È SOLO L'EC. NEUTRO DEL +)

$$\mathbb{Z}_3(\sqrt{2})$$

$$a + b\sqrt{2}$$

TROVIAMO L'INVERSO

FACCIO IL CONTO

$$(a + b\sqrt{2})(c + d\sqrt{2}) =$$

$$(ac + 2bd) + \sqrt{2}(bc + ad)$$

$= 1$ $= 0$

$$bc + ad = 0 \ (3) \qquad d = -\frac{bc}{a} \ (3)$$

CASO 1: $a \equiv 0 \ (3)$

$$(b\sqrt{2}) \cdot \left(\frac{1}{b} \cdot \sqrt{2}\right) \cdot (-1) \equiv 1 \ (\mathbb{Z}/3\mathbb{Z})^*$$

$b \neq 0$

$\hookrightarrow d \equiv 2b^{-1}$

$c \equiv 0$

$(b\sqrt{2})(c + d\sqrt{2}) \equiv 1 \ (\mathbb{Z}/3\mathbb{Z})^*$

CASO 2: $a \not\equiv 0 \ (3)$

$$ac - 2b\,\frac{bc}{a} \equiv 1 \ (3)$$

$$c\left(a^2 - 2b^2\right) \equiv a \ (3)$$

$\hookrightarrow \not\equiv 0 \quad (\Leftrightarrow (a,b) \neq (0,0))$

$$c \equiv \frac{a}{a^2 - 2b^2} \ (3)$$

(ANCHE NEL CASO 1)

$$d \equiv -\frac{bc}{a} \equiv -\frac{ba}{a(a^2-2b^2)} \ (3)$$

$$\equiv -\frac{b}{a^2 - 2b^2} \ (3)$$

(ANCHE NEL CASO 1? SÌ: $a=0$ E DIVENTA $\frac{1}{2}b^{-1}$)

L'INVERSO DI $(a+b\sqrt{2})$ È

$$\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)$$

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$ (IN REAL LIFE)

(BASTAVA RAZIONALIZZARE)

CHE CAMPI CONOSCIAMO?

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Z}_p(\sqrt{\Delta})$

p: PRIMO

$x^2 - \Delta$ NO SPL. (p)

CHE PROPRIETÀ HANNO I POLINOMI A COEFFICIENTI IN UN CAMPO?

$a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$

$a_n \neq 0$

POSSO MOLTIPLICARE PER a_n^{-1} TUTTO:

A MENO DI COSTANTI MOLTIPLICATIVE, TUTTI I POLINOMI SONO MONICI.

(I.E.: II $X+1$ DIVISO $2X$ È ANTIPATICO:

$X+1 = 2X\,p(x) + q(x)$

$q(x)$ HA SEMPRE GRADO ≥ 1.

(UNO SPERA IN UN RESTO PIÙ PICCOLO)

NEI CAMPI, SE HO $p(x)$ E $q(x)$ POSSO FARE LA DIVISIONE EUCLIDEA.

IN $\mathbb{Z}$ 439

$$7x^8 + 23x^6 + x - 1 \quad \text{DIVISO}$$

$$13x^4 + 7x - 1$$

$$(13x^4 + 7x - 1) \cdot \left(\frac{7x^8}{13x^4}\right)$$

$$\left(Cx^4\right)$$

FACCIO LA DIVISIONE EUCLIDEA TRA

$$\left(p(x) - q(x) \cdot Cx^4\right) \Big/ q(x)$$

QUINDI SI OTTIENE UN RESTO:

$$p(x) = q(x) \cdot \bar{q}(x) + r(x)$$

$r(x) = 0$

$\deg r < \deg p$

(FUNZIONA ANCHE IN $\mathbb{Z}$ SE $q(x)$ È MONICO)

IN UN CAMPO, $f(x)$ DI GRADO n, QUANTE RADICI PUÒ AVERE?

AL MASSIMO n

VEDIAMO SE VALE RUFFINI.

SE $f(\alpha)=0 \rightarrow f(x)=(x-\alpha)\,g(x)$

FACCIAMO LA DIVISIONE EUCLIDEA TRA

$f(x) \,/\, (x-\alpha)$

$$f(x)=g(x)(x-\alpha)+r(x)$$

deg 1 — $r(x)$ HA GRADO 0

r

$\downarrow \alpha$

$$0=f(\alpha)=g(\alpha)\cdot 0+r$$

$r=0. \rightarrow$ RUFFINI

$$f(x)=(x-\alpha)\,g(x)$$

INDUZIONE!

Hp. Ind. OGNI POLINOMIO DI GRADO n HA AL PIÙ n RADICI

$$f(x) = (x-a)\cdot g(x)$$

$f(x)$: ? → deg n

$(x-a)$: AL PIÙ 1 RADICE

$g(x)$: → deg $n-1$ → AL PIÙ $n-1$ RADICI

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO !!!

SE α È RADICE DI $p(x)\,q(x)$,

ALLORA α È RADICE DI $p(x)$ O DI $q(x)$.

(FATE IL PASSO BASE)

[NON INTERROGHIAMOCI SUL GRADO DI 0, DICIAMO CHE NON HA GRADO]

VOGLIAMO LA FATTORIZZAZIONE UNICA.

(A MENO DI COSTANTI $\neq 0$)

INVERTIBILI

ASSUMIAMO QUINDI MONICI.

CI SONO DUE TIPI DI POLINOMI:

- FATTORIZZABILI IN 2 o + POLINOMI: $f(x) = p(x)q(x)$
- IRRIDUCIBILI.

OGNI POLINOMIO SI SCRIVE COME PRODOTTO DI FATTORI IRRIDUCIBILI

SI VA PER INDUZIONE:

f

- IRRIDUCIBILE ✓
- $f = p(x) \cdot q(x)$ — $p(x)$: IRRIDUCIBILE …; $q(x)$: IRRIDUCIBILE …

PER COME HO DEFINITO IRRIDUCIBILE (A UNA CERTA ARRIVO A GRADO 0)

IN $\mathbb{Z}$ $\quad x^2 - 4 \equiv (x-2)(x+2)$

$\mathbb{Z}_7$

$(x-7)(x+7)$

IN UN CAMPO È DAVVERO UNICA?

PER ASSURDO:

$$\prod_{i=1}^{n} p_i(x) = \prod_{i=1}^{m} q_i(x)$$

p_i RIDUCIBILI — q_i IRRIDUCIBILI

- VORREI ANNULLARCI CON UN K, MA, AD ESEMPIO, IN $\mathbb{Q}$ x^2+1 NON HA RADICI

SUPPONIAMO CHE $p_1(x)$ NON SIA NESSUN $q_i(x)$.

$p_1(x)$ DIVIDE $\prod p_i(x)$

$p_1(x)$ DIVIDE $\prod q_i(x)$

PER LA DIVISIONE EUCLIDEA:

TT $q_i(x) = g(x) \cdot p_1(x)$

SE $p_1(x)$ DIVIDE $a(x) \cdot b(x)$

VOGLIAMO MOSTRARE CHE $p_1(x) \mid a(x)$

OPPURE $p_1(x) \mid b(x)$

$$a(x) = p_1(x) \cdot \alpha(x) + r_a(x)$$

$$b(x) = p_1(x) \cdot \beta(x) + r_b(x)$$

$$p_1(x) \mid \left(p_1(x)\cdot\alpha(x) + r_a(x)\right)\left(p_1(x)\cdot\beta(x) + r_b(x)\right) = p_1(x)\left(p_1(x)\alpha(x)\beta(x) + r_a(x) + r_b(x)\right) + r_a(x) r_b(x)$$

$$\longrightarrow p_1(x) \mid r_a(x) r_b(x)$$

$\deg = k$ $\quad \deg < k \quad \deg < k$

USIAMO BÉZOUT

(FIGLIO DELL'ALGORITMO DI EUCLIDE)

$$p_1(x) = r_0(x) \cdot v_1(x) + u_1(x)$$

$$r_0(x) = u_1(x) \cdot v_2(x) + u_2(x)$$

$$u_1(x) = u_2(x) \cdot v_3(x) + u_3(x)$$

...

...

$$u_j(x) = u_{j+1}(x) \cdot v_{j+2}(x) \quad \underline{\neq 0}$$

PER QUESTIONI DI GRADO

(PASSAGGIO PRIMA...)

$$u_{j-1}(x) = u_j(x) \cdot v_{j+1}(x) + u_{j+1}(x)$$

$$u_{j+1}(x) = u_{j-1}(x) - u_j(x) \cdot v_{j+1}(x)$$

$$u_j(x) = u_{j-2}(x) - u_{j-1}(x) \cdot v_j(x)$$

...

$$u_2(x) = r_0(x) - v_2(x) \cdot u_1(x)$$

$$u_1(x) = p_1(x) - v_1(x) \cdot r_0(x)$$

QUINDI:

$$M_{j+1}(x) = a(x) \cdot p_1(x) + b(x) V_0(x)$$

È VERO CHE M_{j+1} DIVIDE M_j?

★ M_{j+1} DIVIDE M_j

QUINDI

M_{j-1}

...

DIVIDE $V_0(x)$ E $p_1(x)$

QUINDI $M_{j+1}(x) = 1$ (o COSTANTE)

$= p_1(x) \cdot$ (COSTANTE

QUESTIONE DI GRADO

$= p_1(x)$: $V_0(x)$ NON È MULTIPLO DI M_{j+1}

A MENO CHE $V_0(x) = 0$

(MA ALLORA $p_1(x) \mid a(x)$)

$= 1$

$$p_1(x)\cdot a(x) + r_a(x)\cdot b(x) = 1$$

Hp. $p_1(x) \mid r_a(x)\ r_b(x)$

MOLTIPLICHIAMO PER $r_b(x)$

$$p_1(x)\cdot a(x)\cdot r_b(x) + r_a(x)\cdot r_b(x)\cdot b(x) = r_b(x)$$

MULT. DI p_1 — MULT. DI p_1 — MULT. DI p_1 QUINDI $\equiv 0$.

QUINDI: SE $p_1(x) \mid a(x)\cdot b(x) \rightarrow$
$p_1(x) \mid a(x)$, $p_1(x) \mid b(x)$

IRRIDUCIBILE

$$p_1(x) \mid \prod_{i=1}^{m} q_i(x) = q_1(x)\cdot \prod_{i=2}^{n} q_i(x)$$

$p_1(x)$ { DIVIDE $q_1(x)$ (IRRIDUCIBILE) $\rightarrow p_1(x) = q_1(x)$

DIVIDE $\prod_{i=2}^{m} q_i(x)$ { $q_2(x)$ / $\prod$ }

QUINDI CON $q_i(x) = p_1(x)$

$$p_1(x) \cdot \prod_{i=2}^{n} p_i(x) = p_1(x) \cdot \prod_{\substack{i=1 \\ i \neq K}}^{m} q_i(x)$$

VORREMMO CHE $p_1(x)$ ANDASSE VIA

IL PROBLEMA SONO COSE TIPO

$$p_1^2 \cdot p_2 = p_1 \cdot p_2^2$$

RACCOGLIAMO $p_1(x)$

$$p_1(x)\left(\prod p_i(x) - \prod q_i(x)\right) = 0$$

$$= 0$$

ANNULLAMENTO DEL PRODOTTO,

MA L'ABBIAMO SOLO SUI COEFFICIENTI,

MA SUI POLINOMI È DIVERSO:

BASTA IL TERMINE DI GRADO MASSIMO

O COME POLINOMIO!

POSSO QUINDI DIRE

$$\prod_{i=2}^{n} p_i(x) = \prod_{\substack{i=1 \\ i \neq j}}^{m} q_i(x)$$

TEOREMA (LO DIMOSTRIAMO ALLA # LEZIONE)

OGNI CAMPO FINITO AMMETTE UN GENERATORE.

OVVERO UN ELEMENTO y CHE HA ORDINE MOLTIPLICATIVO = # ELEMENTI INVERTIBILI

L'ORDINE MOLTIPLICATIVO IN CAMPO K DI x È IL MINIMO INTERO POSITIVO n T.C. $x^n = 1$ (IN K).

$1, y^1, y^2, \dots, y^{s-1}$ DOVE s È IL NUMERO DI ELEMENTI INVERTIBILI ($|K| - 1$) SONO TUTTI

GLI ELEMENTI DEL CAMPO TRANNE ZERO.

(INFINITI NO, TIPO $\mathbb{Q}$).

ESERCIZI TIPO TEORICI.

DIMOSTRARE CHE IN $\mathbb{Z}_p(\sqrt{\alpha})$ CON $X^2-\alpha$ SENZA RADICI IN $\mathbb{Z}_p$ VALE

$$x^{p^2-1} \equiv 1 \quad \left(\mathbb{Z}_p(\sqrt{\alpha})\right| \quad \forall x \neq 0.$$

CONSIDERIAMO:

$x \in \mathbb{Z}_p(\sqrt{\alpha})$

$x \neq 0$

$x \mapsto \alpha x$ (PERMUTAZIONE)

$x \mapsto \alpha x$

$y \mapsto \alpha y$

$0 \mapsto 0$

$x \neq y \rightarrow \alpha x \neq \alpha y$

PERCHÉ POSSO MOLTIPLICARE PER α^{-1}

LE FUNZIONI INIETTIVE SU INSIEMI FINITI SONO (SULLO STESSO)
PERMUTAZIONI

$$\prod_{\substack{x \neq 0 \\ x \in \mathbb{Z}_p(\sqrt{a})}} (a x) = a^{|\mathbb{Z}_p(\sqrt{a})|-1} \cdot \prod_{\substack{x \neq 0 \\ x \notin \mathbb{Z}_p(\sqrt{a})}} x$$

$$a^{p^2-1} \equiv 1 \quad (\mathbb{Z}_p(\sqrt{a}))$$

WILSON

$$\prod_{\substack{x \neq 0 \\ x \in \mathbb{Z}_p(\sqrt{a})}} x$$

CONSIDERIAMO IL POLINOMIO:

$$X^{p^2-1} - 1 \quad \text{IN} \quad \mathbb{Z}_p(\sqrt{a})$$

HA p^2-1, TUTTI E SOLI GLI EL. INVERTIBILI.

È VERO CHE:

$$X^{p^2-1} - 1 = \prod_{\alpha \text{ INVERTIBILE}} (X - \alpha) \quad ?$$

QUANDO LE RADICI IN UN CAMPO DI UN POLINOMIO SONO TANTE QUANTE IL SUO GRADO SÌ.

OGNI $X - \alpha$ DIVIDE $X^{p^2-1} - 1$

QUINDI:

$\prod_{\alpha \text{ INVERTIBILE}} (X - \alpha)$ DIVIDE $X^{p^2-1} - 1$ PERCHÉ GLI $X - \alpha$ SONO IRRIDUCIBILI

HA GRADO $p^2 - 1$

VISTO CHE SONO MONICI:

$$\prod_{\alpha \text{ INVERTIBILE}} (X - \alpha) = X^{p^2-1} - 1$$

$X = 0 \rightarrow (-1)^{p^2-1} \cdot \prod_{\alpha \text{ INVERTIBILE}} \alpha = -1$

□

SIA $p > 5$ PRIMO E SIA $F_0 = 0$, $F_1 = 1$,

$$F_{n+2} = F_{n+1} + F_n$$ (FIBONACCI),

SI MOSTRI CHE $p \mid F_{p^2-1}$

CONSIDERIAMO $\mathbb{Z}_p(\sqrt{5})$

CASO I: $x^2 - 5$ (p) HA SOLUZIONE

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

$a + b\sqrt{5}$ CON a, b RAZIONALI NON CON DENOMINATORI MULTIPLI DI p, HA SENSO VEDERLI COME NUMERI MODULO p, PONENDO

$$\sqrt{5} = k \quad \text{t.c.} \quad p \mid k^2 - 5$$

PROBLEMA 1: k o $-k$?

$p = 7$ $\qquad 4+\sqrt{2}$ — $4+3$, $4+4$

$$(a+b\sqrt{\alpha})(c+d\sqrt{\alpha}) =$$

$$= ac + \alpha bd + \sqrt{\alpha}(bc+ad)$$

$$\equiv K^2 \ (p)$$

MOTIVO CRUCIALE: QUANDO FACCIO $(a+b\sqrt{\alpha})(c+d\sqrt{\alpha}) = x+y\sqrt{\alpha}$

SE NEL FARE I CONTI $y \equiv 0 \ (p)$,

POSSO SCEGLIERE INDIFFERENTEMENTE $\sqrt{\alpha}$ (k o $-k$)

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{p^2-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p^2-1}\right) \equiv$$

$$K^2 \equiv 5 \ (p)$$

$$\equiv \frac{1}{K}\left(\left(\frac{1+K}{2}\right)^{p^2-1} - \left(\frac{1-K}{2}\right)^{p^2-1}\right) \equiv$$

$\hookrightarrow (\wedge(p-1))^{\wedge(p+1)}$ FERMAT

$$\equiv \frac{\wedge}{\chi}\,(1-1) \equiv 0 \pmod{p}$$

- II CASO: $\mathbb{Z}_p(\sqrt{5})$ ESISTE ED È UN CAMPO

a^{p^2-2} È L'INVERSO DI a

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{p^2-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p^2-1}\right) \equiv 0 \quad \left(\mathbb{Z}_p(\sqrt{5})\right)$$

$\left(\frac{1+\sqrt{5}}{2}\right)$ $\left(\frac{1-\sqrt{5}}{2}\right)$ ↓ 1 ↓ 1

(ES. PER CASA: PROVATE A VEDERE SE IN $\mathbb{Z}_p(\sqrt{5})$ BECCO

$$\left(\frac{1+\sqrt{5}}{2}\right)^{p+1} = \pm 1$$

(MA ANCHE SOLO CON IL + FORSE)

ESERCIZI PER CASA / CAMERA

1] $a_0 = 2, \quad a_{n+1} = 2a_n^2 - 1$

SE $p \mid a_n \longrightarrow 2^{n(n+3)} \mid p^2 - 1$

2] SIA IN $\mathbb{Z}_p$ CHE IN $\mathbb{Z}_p(A)$, OGNI VALORE È ASSUNTO DA: $\qquad$ (n FISSATO)

$$X_1^n + \dots + X_n^n$$