A1 MEDIUM

Titolo nota 03/09/2013

POLINOMI

$$a(x) = \sum_{i=0}^{d} a_i x^i \qquad \max\{i : a_i \neq 0\} = \deg a$$

a_i: coefficienti in un anello

$\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}$ F_m $\mathbb{Z}/(m\mathbb{Z})$ $\mathbb{Z}_m$

$\mathbb{R}$ campo, $\mathbb{C}$ campo, $\mathbb{Z}$ no, F_m campo se m primo $\Leftrightarrow$ $\exists$ inversi molt. di ogni num $\neq 0$

$X^p - X$ $\mathbb{F}_p$ zero come funzione ma non come polinomio

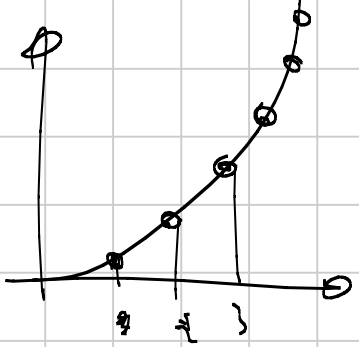
Principio di identità dei polinomi

dati $p(x)$, $q(x)$ poly. di grado $\leq d$

se $p(x_i) = q(x_i)$ per $d+1$ punti distinti

allora $p(x) = q(x)$ come polinomi

$x+y$ $x+y^2$ coincidono per ogni $x \in \mathbb{Z}$, $y = 0$



$p(x,y)$ $p(n,n^2)=0$

$(y^2-x)\cdot g(x,y)$ sono tutti

$(R[y])[x]$

$1+x+y+x^2y^2$

$1+y+1\cdot x+y^2\cdot x^2$

a_0 a_1 a_2

$p(x)$ Ruffini

$p(2)=5$ $p(4)=5$ cosa so su $p(0)$?

(coefficienti interi)

$f(x)=p(x)-5$ si annulla in $x=2$, $x=4$

$f(x)=(x-2)(x-4)q(x)$

$p(x)=(x-2)(x-4)q(x)+5$

interi

$p(0)=-2\cdot -4\cdot q(0)+5$ $p(0)\equiv 5 \bmod 8$

$a-b \mid p(a)-p(b) \quad \forall p$ coeff. interi

$4-0 \mid p(4)-p(0) = 5-p(0) \quad p(0) \equiv 5 \ (4)$

$p(0) \equiv 5 \ (2)$

$(x_0, y_0), (x_1, y_1), \dots (x_d, y_d)$ | coeff. compo

$d+1$ pti con x_i distinte

$\exists!$ $p(x)$

$(9x+3)(6x+2) =$ $\mathbb{F}_{18}$ mod 18

$= 0 \cdot x^2 + 0 \cdot x + 6$

$\deg(p \cdot q) = \deg p + \deg q \Rightarrow$ compo

- fatt. unica vale $\text{Compo}[x]$

$\text{Compo}[x, y, z, \dots]$

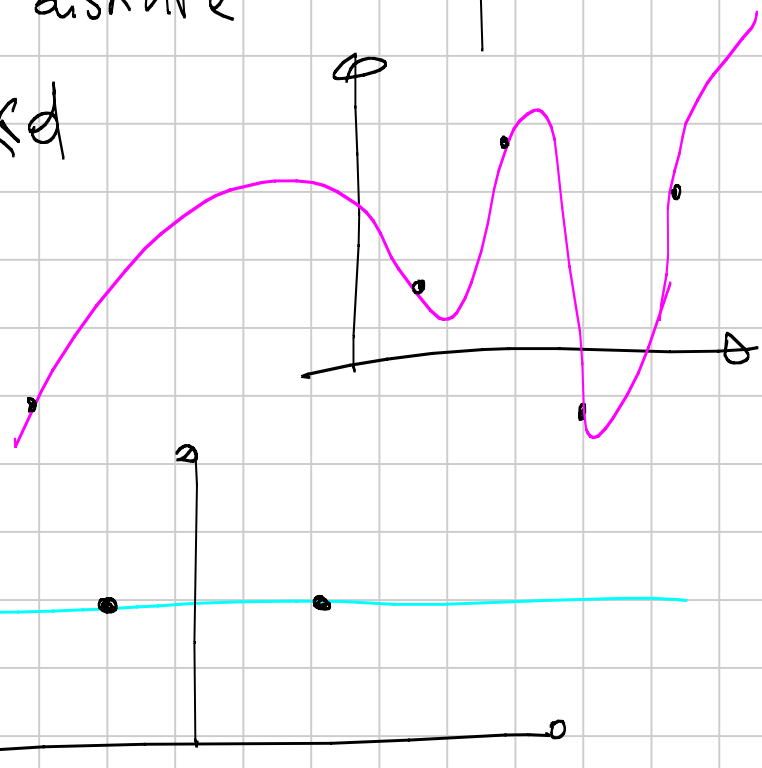
$\mathbb{Z}[x, y, z, \dots]$

Thm: Interpolazione (di Lagrange) | coeff. comp

(x_0, y_0), (x_1, y_1), -- (x_d, y_d)

$d+1$ pt con x_i distinte

$\exists!$ $p(x)$ di grado $\leq d$



Come si dimostra?

1) caso facile

$(x_0, 1)$, $(x_1, 0)$, $(x_2, 0)$ -- $(x_d, 0)$

$L_0(x)$

$$\frac{(x-x_1)(x-x_2)\cdots(x-x_d)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_d)} = L_0(x)$$

2) $L_i(x)$ t.c. $L_i(x_j) = \begin{cases} 1 & i=j \\ 0 & \text{altrimenti} \end{cases}$

3) $\sum_{i=0}^{d} y_i L_i(x)$ funziona!

4) unicità $f(x)$, $g(x)$

$f(x) - g(x)$ ha grado $\leq d$

si annulla in $x_0, x_1, \dots x_d$

$$f(x) - g(x) = (x-x_0)(x-x_1)(x-x_2)\dots(x-x_d)\cdot q(x)$$

$$q(x) = \sum_{i=0}^{d} a_i x^i$$

a_i: incognite

$$\begin{cases} a_0 + a_1 x_0 + a_2 x_0^2 + \dots a_d x_0^d = y_0 \\ a_0 + a_1 x_1 + a_2 x_1^2 + \dots a_d x_1^d = y_1 \\ \vdots \qquad\qquad\qquad\qquad \vdots \end{cases}$$

$d+1$ eq. in $d+1$ incognite $a_0, a_1, \dots a_d$

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^d \\ 1 & x_1 & x_1^2 & & \\ 1 & x_2 & & \ddots & \\ \vdots & \vdots & & & \\ 1 & & & & x_d^d \end{bmatrix} = \text{matrice di Vandermonde}$$

$$\prod_{i<j} (x_j - x_i)$$

$$\begin{cases} x \equiv (1)\ y_0 & (3) \\ x \equiv (2)\ y_1 & (5) \\ x \equiv (5)\ y_2 & (14) \end{cases}$$

1) si risolve prima $\begin{cases} x \equiv 1 & (3) \\ x \equiv 0 & (5) \\ x \equiv 0 & (14) \end{cases}$

$5 \cdot 14 \cdot (\text{inverso di } 5 \cdot 14 \bmod 3) = L_1$

$$\sum_i y_i L_i$$

---

polinomi $\leftrightarrow$ interi

in una var.
coeff. in un campo

1) divisione TH dati $a(x), b(x)$. $\exists\ q(x), r(x)$

$$a(x) = q(x) \cdot b(x) + r(x)$$

$$\deg r < \deg b$$

$\Rightarrow$ Algoritmo di Euclide

$\Rightarrow$ Bézout

TH dati $a(x), b(x)$ senza fattori comuni

$\exists\ p(x), q(x)$ t.c.

$$a(x)p(x) + b(x)q(x) = 1$$

$a(x) \equiv b(x) \mod m(x)$

se $a(x) - b(x)$ è multiplo di $m(x)$

$x + a \mid x^m + a^m \iff m$ dispari

$x \equiv -a \quad x^m \equiv (-a)^m$ { m pari a^m ; m dispari $-a^m$

$x^m \equiv -a^m$ per m dispari

$x + a \mid x^m + a^m$

$\mathbb{Z}[x] \subseteq \mathbb{C}[x]$

$a(x) = a_d(x - x_1)(x - x_2) \cdots (x - x_d)$

x_1, x_2 complessi

$d(x) \mid a(x)$

$d(x) \cdot q(x) = a(x)$

$d(x) \mid a(x)$ se $\exists\ q(x)$ t.c.

$d(x)\,q(x) = a(x)$

1) le radici di d sono radici di a
2) se sono in $\mathbb{C}$, d, a si spezzano in fattori lineari

$$(x-x_1)(x-x_2)\cdots(x-x_d)$$

$$3(x+1) \mid 2(x^2+2x+1)$$

$$3(x+1)\cdot\frac{2}{3}(x+1) = 2(x^2+2x+1)$$

$$x^{\phi(m)} = 1$$

$$x_1, x_2 \cdots x_{\phi(m)}$$

$$x\cdot x_1,\ x\cdot x_2 \cdots x\cdot x_{\phi(m)}$$

$$x_1 \cdot x_2 \cdots x_{\phi(m)}$$

$$x^{\phi(m)} - x_1 x_2 \cdots x_{\phi(m)}$$

$\sim F_p$ funziona

$$p(x_0) = y_0$$

$$\begin{cases} p(x) \equiv y_0 & (x-x_0) \\ p(x) \equiv y_1 & (x-x_1) \\ \vdots & \\ p(x) \equiv y_d & (x-x_d) \end{cases}$$

$p(x) \quad \mod(x-a)$

$p(x) \mid x-a$

$p(x) = (x-a)q(x) + r \qquad r = p(a)$

$a+b+c \mid$

$a^3+b^3+c^3-3abc$ ribattezziamo $c=x$

$a+b+x \mid a^3+b^3+x^3-3abx$?

Divisione tra polinomi in $(\mathbb{R}[a,b])[x]$

$\underbrace{a^3+b^3+x^3-3abx}_{p(x)} = (a+b+x)\,q(x) + r(x)$

$r = p(-a-b)$

$a^3+b^3+(-a-b)^3-3ab(-a-b) =$

$= a^3+b^3-a^3-3a^2b-3ab^2-b^3+3ab(a+b) =$

$= 0$

Oss: quando faccio $a(x) : b(x)$

$a(x) \mid b(x)$

se $b(x)$ è monico, allora arrivo alla fine

senza dover fare divisioni

⇒ funziona anche in $\mathbb{Z}$, (e in un anello generico)

e $q(x)$, $r(x)$ hanno coefficienti nell'anello

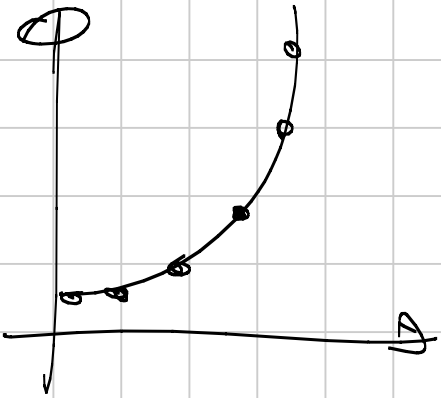
$ax^3+3x^2+3x+1 \;\big|\; bx+1$

$ax^3+\frac{a}{b}x^2$

//

non sempre funziona

$p(x,y)$ per ogni $n \in \mathbb{N}$



$p(n, n^2) = 0$

Th $p(x,y) = (y-x^2) \cdot$ polinomio (x,y)

1) $p(z, z^2)$ polinomio nella sola z

si annulla per ogni $z = 1, 2, 3, \ldots \in \mathbb{N}$ (Hp)

⇒ $p(z, z^2)$ è il polinomio 0

2) Guardiamo x "coefficiente", y "indeterminata"

$(\mathbb{C}[x])[y]$

$y-x^2$ è un poly. di primo grado in y

Ruffini!

$p(x,y) = q(x,y) \cdot (y-x^2) + r(x,y)$

grado 1 in y ; grado 0 in y

per Ruffini, è $p(x, x^2)$ = 0

polinomio in (x,y) perché $y - x^2$ è monico $\Rightarrow$ non servono divisioni

---

$x^3 + 1$

Qual è il resto della divisione $x^{2013} + x^{1000} + x + 1$ per $x^3 + 1$?

$x^3 \equiv -1$

$(x^3)^{roba} \equiv (-1)^{roba} \equiv -1$

$x^{2013} = (x^3 + 1)\, x^{2010} - x^{2010}$

congruenze $\Leftrightarrow$ somme/sottrazioni multipli

$x^{2013} + x^{1000} + x + 1 \equiv -1 + x \cdot x^{\overset{-1}{111999}} + x + 1 \equiv \quad (x^3 + 1)$

$\equiv -1 - x + x + 1 = 0$

---

congruenze modulo $x^3 - x + 2$: faccio i conti normalmente, tutte le volte che trovo x^3 lo rimpiazzo con $x - 2$

ogni $f \in \mathbb{R}[x]$ ha un "rappresentante privilegiato" modulo (x^3-x+2) del tipo ax^2+bx+c

$$\frac{\mathbb{R}[x]}{(x^3-x+2)} = \{\text{classi di resto dei polinomi mod } x^3-x+2\}$$

Se il polinomio $p(x)$ è irriducibile in $F(x)$ (F campo) allora $\dfrac{F(x)}{(x^3-x+2)}$ è un campo

Dim: Bézout

$$a(x)p(x) + (x^3-x+2)q(x) = 1$$

$$a(x)p(x) \equiv 1 \pmod{x^3-x+2}$$

Irriducibili in $\mathbb{C}[x]$: solo i polinomi di grado 1!

$$p(x) = a(x-x_1)(x-x_2)\cdots(x-x_d)$$

Irriducibili in $\mathbb{R}[x]$?

$$(x-x_0)(x-x_1)\cdots(x-x_r)\,(x-c_1)(x-\bar{c}_1)(x-c_2)(x-\bar{c}_2)\cdots(x-c_s)(x-\bar{c}_s)$$

Ruffini

- grado 1
- grado 2 con $\Delta < 0$

$$\frac{\mathbb{R}[x]}{(x^2+1)}$$

$$(a+bx) \cdot (c+dx)$$

$$(a+bx)(c+dx) = ac + bcx + adx + bdx^2$$
$$\equiv (ac - bd) + (bc + ad)x$$

$$\frac{\mathbb{Q}[x]}{(x^3-x+2)} = \{ ax^2+bx+c \,;\, a,b,c \in \mathbb{Q} \}$$

(campo)

perché lui è irriducibile?

Rational root theorem: in $\mathbb{Z}[x]$

se un polinomio ha radici razionali p/q,

allora p | termine noto, q | coeff. grado massimo

(Achtung: no radici $\neq$ irriducibile in generale)

$$\underbrace{(x^2+1)}\underbrace{(x^2+5)}$$

Irriducibile $\stackrel{\text{def}}{=}$ non posso scriverlo come $a(x)b(x)$ (con a,b non costanti)

$\mathbb{F}_7$, 5 no residuo quadratico

x^2-5 irriducibile in $\mathbb{F}_7$

$$\frac{\mathbb{F}_7[x]}{(x^2-5)} = \{ a+bx \ ; \ a,b \in \mathbb{F}_7 \}$$

Faccio i conti normalmente, quando ho x^2 lo rimpiazzo con 5

Invece di x, posso chiamarlo "$\sqrt{5}$"

Fibonacci:

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+1} = F_n + F_{n-1} \end{cases}$$

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

Cosa succede ai Fibonacci mod p?

1) se 5 è un residuo quadratico, allora $\exists$ a classe di resto t.c. $a^2 = 5$

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

es. $p=11$, $4^2 = 5$

2) se 5 non è res. quadratico,

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

Fate i conti sostituendo $(\sqrt{5})^2$ con 5

3) $p=5$

Corollario

$\forall n,\ F_{n+p} \equiv F_{n+1}$ per i primi di Tipo 1

$\Rightarrow$ periodo (un divisore di) $p-1$

Tipo 2 Abbiamo aggiunto $\sqrt{5}$; non vale più piccolo th. Fermat per gli "oggetti" che abbiamo aggiunto

$$y^p - y \in \left[\frac{F_p[x]}{(x^2-5)}\right][x]$$

$0, 1, 2, \dots p-1$

$\sqrt{2}$ $\longrightarrow$ radice dell'equazione $x^2-2=0$

"$-\sqrt{2}$" $\longleftarrow$

$\sqrt{2}$ $\quad -\sqrt{2}$

Qual è il resto mod 5 di

$$\left\lfloor (\sqrt{2}+1)^{2013} \right\rfloor ?$$

$$Q_{2013} = \left[(\sqrt{2}+1)^{2013} + \underbrace{(-\sqrt{2}+1)^{2013}}_{\text{piccolissimo}} \right] = \left\lfloor (\sqrt{2}+1)^{2013} \right\rfloor$$

piccolissimo $\Leftrightarrow$ $-0,000\dots01$

$a_0 = \dots$

$a_1 = \dots$

$a_{n+1} = ?\,a_n + ?\,a_{n-1}$ $\qquad a_{2013} = ?\,\lambda_1^{2013} + ?\,\lambda_2^{2013}$

Lavoriamo al contrario!

$$a_n := (\sqrt{2}+1)^n + (-\sqrt{2}+1)^n$$

$a_0 = 2$

$a_1 = 2$

$a_{n+1} = 2 \cdot a_n + 1 \cdot a_{n-1}$

$$\begin{vmatrix} a_n & a_{n+1} \end{vmatrix} = \begin{vmatrix} a_n & a_{n+1} \end{vmatrix}$$

$$(x-1)^2 = 2$$

$$x^2 - 2x - 1 = 0$$

$$\cos(15^\circ) + \cos(30^\circ) + \cos(45^\circ) + \dots + \cos(315^\circ)$$

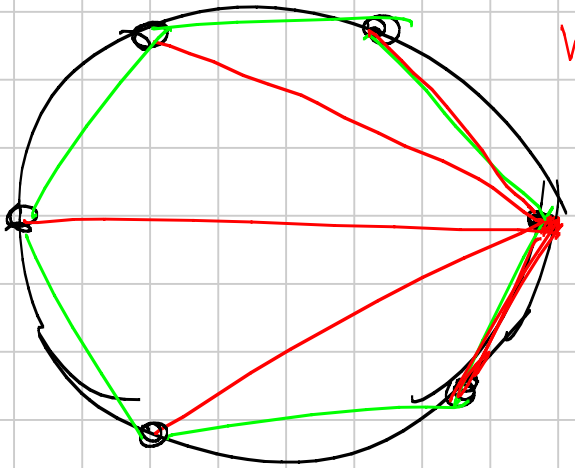
$$\cos x + \cos 2x + \dots + \cos(nx) +$$

$$+ i\sin x + i\sin 2x + \dots + i\sin(nx)$$

$$= e^{ix} + e^{2ix} + \dots e^{nix} = \frac{1 - e^{nix}}{1 - e^{ix}} e^{ix}$$

$$\Rightarrow \cos x + \dots + \cos nx = \mathrm{Re}\left[\frac{1+e^{nix}}{1-e^{ix}}\, e^{ix}\right]$$

Es

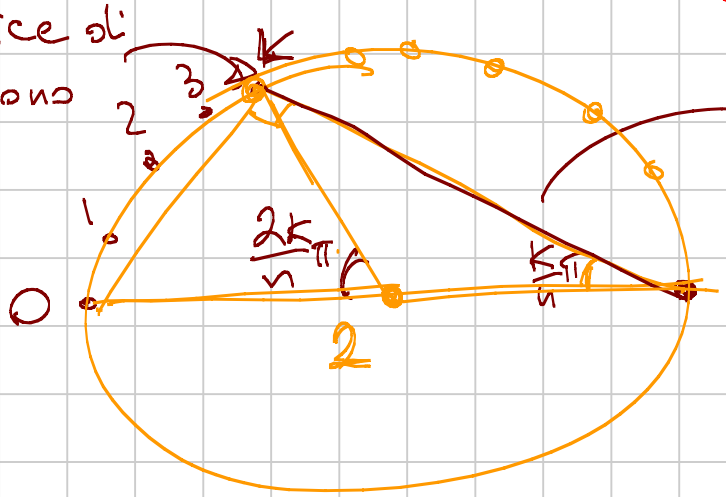


n-agono regolare in cerchio di raggio 1

Diagonali che partono da un vertice;

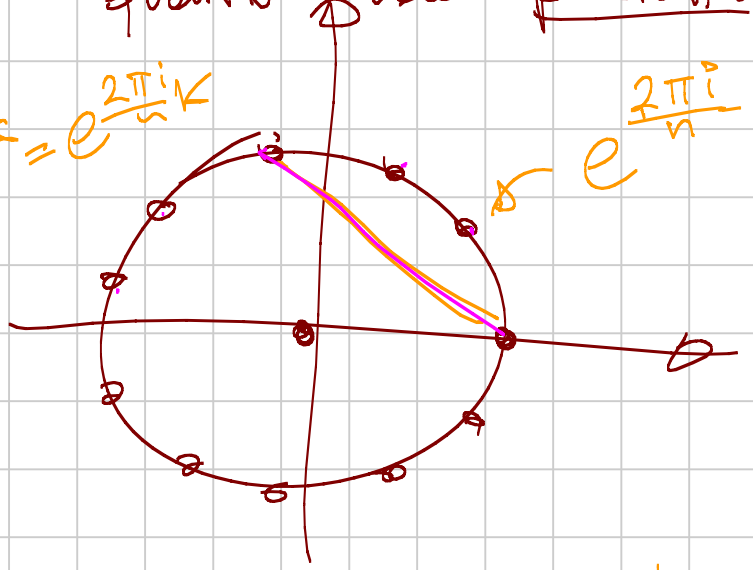
Quanto vale la somma delle loro lunghezze?

k-vertice di un n-agono



$$\Rightarrow 2\cdot\cos\frac{k}{n}\pi$$

Es quanto vale prodotto delle diagonali?



$$w^k = e^{\frac{2\pi i}{n}k} \qquad e^{\frac{2\pi i}{n}} = w$$

$$|w^k - 1|$$

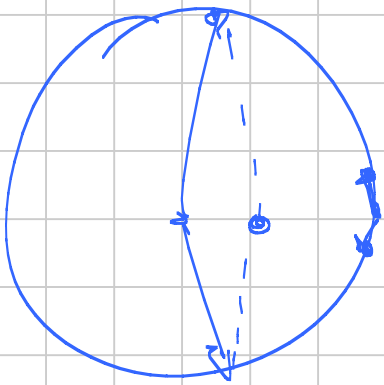
$$\prod_{k=1}^{n-1} |w^k - 1| = \left|\prod_{k=1}^{n-1} (w^k - 1)\right| = n$$

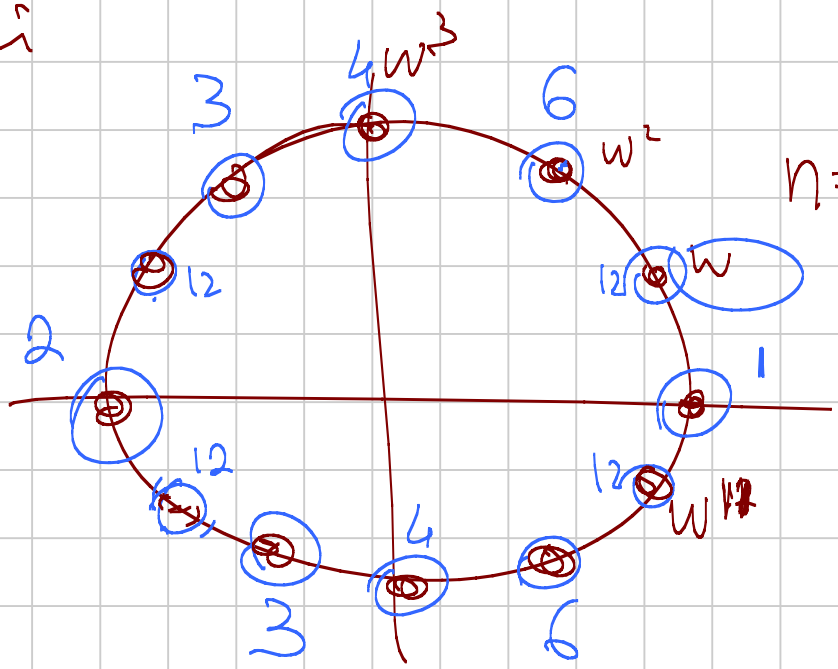
Chi è $\prod_{k=1}^{n-1}(x-w^k)$? è $\frac{(x^n-1)}{x-1} = 1+x+x^2+\dots+x^{n-1}$

Chi è $\prod_{k=1}^{n-1}(1-w^k)$? è $1+1+\dots+1 = n$

$$\prod_{k=1}^{n-1} 2\cos\frac{2\pi k}{n} = n$$

Ciclotomici





$w^{12}=1$

$a5+b12=1 \Rightarrow 1=(w^5)^a\cdot(w^{12})^b = w^{5a+12b}=w$

$$x^{12}-1=(x^4)^3-1=(x^4-1)(x^8+x^4+1)$$

$$=(x-1)(1+x+x^2+\dots+x^{11})$$

$$=(x^6-1)(x^6+1)$$

$$(x-1)(x^5+x^4+\dots)$$

$\Phi_1(x) = (x-1)$ ← radice con periodo 1 $w^0 = 1$

$\Phi_2(x)$ $(x+1)$ ← radice con periodo 2, $w^6 = -1$

$\Phi_4(x) = (x+i)(x-i) = x^2+1$ ← radici con periodo 4 $w^3 = i$, $w^4 = -1$

x^2+x+1 — 3, 6

$\Phi_{12}(x) = (x-w)(x-w^5)(x-w^7)(x-w^{11})$ — 12

Formalmente,

$$\Phi_n(x) := \prod_{\substack{w \text{ radice} \\ n\text{-esima primitiva} \\ \text{di } 1}} (x-w) = \prod_{\substack{(k,n)=1 \\ k=1,2,\dots n}} \left(x - e^{\frac{2\pi i}{n}\cdot k}\right)$$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

$$(x^6-1) = (x-1)\,(x+1)\,(x^2+x+1)\,(x^2-x+1)$$

$$\Phi_1(x)\quad \Phi_2(x)\quad \Phi_3(x)\quad \Phi_6(x)$$

1) i $\Phi(x)$ hanno tutti coeff. interi

Dim: induzione estesa!

Supponiamo che tutti fino a $n-1$ abbiano coeff. interi

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) = \Phi_1(X)\,\Phi_d(X) \cdots \Phi_{\frac{n}{d}}(X)\,\Phi_n(X)$$

divisore, monico, a coeff. interi per hp. induttiva

$$\Rightarrow \Phi_n(X) = \frac{X^n - 1}{\text{roba (monica)}}$$

$\Phi_1(X)$ $\Phi_2(X)$ $\Phi_4(X)$

$$X^{12} - 1 = (X^6 - 1)(X^6 + 1) = (X^2 - 1)(X^4 + X^2 + 1)(X^2 + 1) \cdot$$

$$\cdot (X^4 - X^2 + 1) = \Phi_{12}(X)$$

$$(X^2 + X + 1)(X^2 - X + 1)$$

$\Phi_3(X)$ $\Phi_6(X)$

Fatto: sono irriducibili sui razionali

$$a(X) \cdot b(X) \quad a, b \in \mathbb{Q}[X]$$

Fatto falso: i coeff. sono solo $-1, 0, 1$

(se andate alla lezione scorsa, controesempi)

$$\Phi_m(X) = \varphi(n)$$

In particolare, $\boxed{\sum_{d \mid n} \varphi(d) = n}$

Pol. ciclotomici si possono usare per dimostrare che $\exists$ infiniti primi t.c. $p \equiv 1 \ (n)$ per ogni n

---

n fissato

Fatto 1) esistono ∞ primi t.c.

$$p \mid \Phi_n(a)$$ per qualche a intero

$$p_1 \cdot p_2 \cdot p_3 \cdots p_u = b$$

$$\Phi_n(b) = b^n + \cdots \pm 1 \equiv 1 \ (p_i)$$

assurdo

In generale, $\forall$ f polinomio a coeff. interi, esistono ∞ primi che dividono $f(a)$ per qualche $a \in \mathbb{N}$

---

2) $p \mid \Phi_n(a) \Rightarrow p \equiv 1 \ (n)$

$p \nmid n$ voglio dire che $p \nmid a^d - 1$ per ogni $d \mid n$

Se $p \mid a^d - 1$, $a^d \equiv 1 \mod p$

$$p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/d} - 1} = 1 + a^d + \cdots + a^{n - n/d} \equiv n/d$$ assurdo!

Ora, $p \mid a^n - 1$ $p \nmid a^k - 1$ $\forall k \mid n$

$\Rightarrow \operatorname{ord}_p(a) = n$ $\quad n \mid p - 1 \Rightarrow p \equiv 1 \ (n)$

Lemma di Gauss $\mathbb{Z}[X]$

$p(x)$ a coefficienti interi,

$p(x) = a(x)\,b(x) \qquad a(x), b(x) \in \mathbb{Q}[X]$

Allora $p(x) = c(x)\,d(x) \quad c(x), d(x) \in \mathbb{Z}[x]$

$$x^2 - 4 = (x-2)(x+2) = \underbrace{(3x-6)} \cdot \underbrace{\left(\frac{1}{3}x + \frac{2}{3}\right)}$$

$$(9x^2 - 4) = (3x-2)(3x+2)$$

$x^5 + x^4 + 1$ irriducibile (su $\mathbb{Q}$)

$$(x^2 + ax + 1)(x^3 + bx^2 + cx + 1)$$

$$(x^2 + ax - 1)(x^3 + bx^2 + cx - 1)$$

---

dato $f(x)$ a coeff. interi, definiamo

$\mathrm{mcd}(a_0, a_1, \dots a_n) =: c(f) \qquad f = \sum_{i=0}^{d} a_i x^i$

$$c(f\cdot g) = c(f)\cdot c(g)$$

$$\sum f_i g_{k-i}$$

$$f = c(f)\cdot f'$$

f': coeff. interi, contenuto 1

$$g = c(g)\cdot g'$$

$$c(f\cdot g) = c\Big(c(f)\,c(g)\,f'g'\Big) = c(f)\,c(g)\,c(f'g')$$

Mi manca da dimostrare che se

$$c(f') = c(g') = 1 \Rightarrow c(f'g') = 1$$

$p \mid c(f'g') \Leftrightarrow$ ogni coeff. di $f'g'$ è multiplo di p

$f'g' \equiv 0 \mod p$

f', g' non sono il polinomio 0

(idea: coeff. di grado più alto!)

$f' = ax^d + \dots \qquad g' = bx^D + \dots$

$\boxed{a\cdot b}\, x^{d+D}$ $\square$

Dim. Lemma di Gauss:

$$p(x) = f(x)\,g(x) = \frac{a(x)}{m} \cdot \frac{b(x)}{n} \qquad (*)$$

(f, g: razionali; $a(x), b(x)$: coeff. interi; m, n: den. comuni)

$$m \cdot n \cdot p(x) = a(x) \cdot b(x)$$

$$m \cdot n \cdot c(p) = c(a) \cdot c(b)$$

posso supporre 1

$$\Rightarrow m \cdot n = c(a) \cdot c(b)$$

$$(*) \quad p(x) = \frac{a(x)\,b(x)}{mn} = \frac{a(x)}{c(a)} \cdot \frac{b(x)}{c(b)}$$

coeff. interi

Idea da tenere a mente: proiettare modulo p e cercare un assurdo

---

Criterio di Eisenstein

$f \in \mathbb{Z}[x]$

$$f = 1 \cdot x^d + a_{d-1} \cdot x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$$

$a_{d-1}, \dots, a_2, a_1$: multipli di p

a_0: multiplo di p ma non di p^2

$$p \,\|\, a_0$$

Allora f irriducibile

Dim: proietta modulo p!

Supponiamo $f(x) = a(x) \cdot b(x)$

mod p $\rightarrow$ $x^d = \bar{a}(x) \cdot \bar{b}(x)$

$\frac{1}{t} x^c \cdot t x^{d-c}$

$a(x) = a_c x^c + a_{c-1} x^{c-1} + \dots + a_1 x + a_0$

$\cancel{\neq}\ 0 \quad 0 \quad 0 \quad 0$

$b(x) = b_{d-c} x^{d-c} + b_{d-c-1} x^{d-c-1} + \dots + b_1 x + b_0$

$\cancel{\neq}\ 0 \quad 0 \quad 0 \quad 0$

$p_0 = a_0 \cdot b_0$ multiplo di p^2

$\uparrow$ mult p $\quad \uparrow$ mult p

assurdo

ES $\Phi_p(x)$ irriducibile per p primo

$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x^1 + 1 = \frac{x^p - 1}{x - 1}$

Trick: cambio di var $y \rightarrow \frac{x+1}{x-1}$

$a_d x^d + \dots$

$b_D x^D + \dots$

$a_d b_D x^{d+D} + \dots$

$a^3+b^3+c^3-3abc$

$a^3+b^3+c^3-3abc = (a+b+c)(\text{roba})$

$\text{roba} = \underset{\parallel}{A}\cdot(a^2+b^2+c^2) + \underset{\parallel}{B}\cdot(ab+bc+ca)$

$1 \qquad\qquad -1$

Polinomi di Chebyshev

$\cos(x) = \cos(x)$

$\cos(2x) = 2\cos^2(x)-1$

$\cos(3x) = \cos(2x+x) = \cos 2x \cdot \cos x - \sin 2x \sin x$ (*) =

(*) $= 2\sin x \cos x \cdot \sin x = 2\cos x(1-\cos^2 x) =$

$= (2\cos^2 x - 1)\cos x - 2\cos x(1-\cos^2 x) =$

$= 2\cos^3 x - \cos x - 2\cos x + 2\cos^3 x =$

$= 4\cos^3 x - 3\cos x$

$\cos(nx)$ è un polinomio in $\cos x$

$\cos(nx) = T_n(\cos(x))$ per un opportuno T_n

$T_0(x) = 1$

$T_1(x) = x$

$T_2(x) = 2x^2 - 1$

$T_3(x) = 4x^3 - 3x$

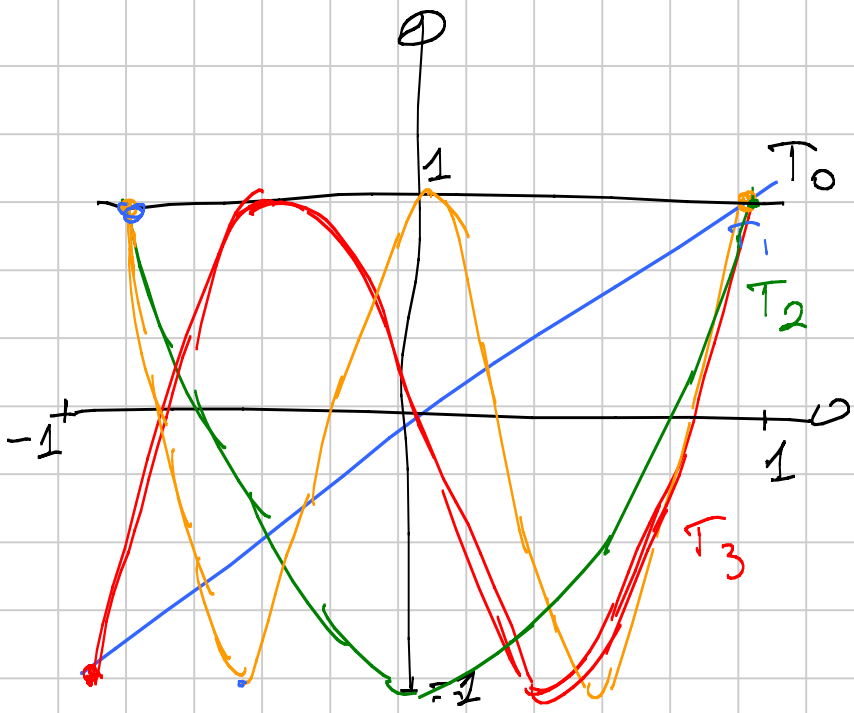
In gen $T_{n+1} = 2x\,T_n(x) - T_{n-1}(x)$

$\cos((n+1)x) = 2\cos x \cos nx - \cos((n-1)x)$

(Werner)

$\cos((n+1)x) + \cos((n-1)x) = 2\cos x \cos nx$

$\cos x$: semi differenza; nx: semi somma



$T_n(x) = \cos n \cdot (\cos^{-1} x)$

Quando $\cos n\vartheta = \begin{cases} 1 \\ -1 \end{cases}$?

$$n\vartheta = k \cdot \pi \qquad \vartheta = \frac{k}{n}\pi$$

$\cos^{-1} x$ varia fra 0 e π quando x varia fra -1 e 1

$$\cos^{-1}\left(\frac{k}{n}\pi\right)$$

Thm: ogni altro polinomio di grado n con coeff. dom. 2^{n-1} "cosca fuori" da $[-1, 1]$