Senior 2014 A1 Medium Simone

Titolo nota 02/09/2014

Se $p(x)$, che ha grado al più n, ha $n+1$ radici, allora $p(x) = 0$.

Supponiamo $\lambda_1, \ldots, \lambda_n$ radici distinte, allora applicando Ruffini più volte ottengo

$$p(x) = c(x-\lambda_1)\ldots(x-\lambda_n)$$

sia $\alpha \neq \lambda_i$ $\quad p(\alpha) = 0$

$$0 = c \cdot \underbrace{(\alpha - \lambda_1)}_{\neq 0} \cdot \ldots \cdot \underbrace{(\alpha - \lambda_n)}_{\neq 0}$$

quindi $c = 0$ (legge di annullamento del prodotto*)

* infatti su $\mathbb{Z}/6\mathbb{Z}$ questo non è vero: es.

$$(x-2)(x-3) \equiv x^2 - 5x \quad (6).$$

Per la dimostrazione, oltre alla legge di an. del prodotto, abbiamo usato Ruffini.

Di cosa è figlio Ruffini?

Per la divisione con resto: se $P(x)$ e $Q(x)$ sono due polinomi allora esistono (e unici) due polinomi $q(x)$ e $r(x)$ tali che $\deg(r) < \deg(Q)$

$$P(x) = q(x) \cdot Q(x) + r(x)$$

Sempre vera SE Q è MONICO

$$\begin{array}{l|l} a_n x^n + \dots + a_1 x + a_0 & x^3 + \dots + \\ \hline & a_n x^{n-3} \end{array}$$

Se Q non è monico non è detto che io lo possa fare, ma vale sempre se A è un campo ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, ...).

Oss. Quando vale la divisione con resto, vale anche Bezout (stessa dim. che in $\mathbb{Z}$) $(P(x), Q(x)) = 1$ allora esistono $a(x)$ e $b(x)$

$\deg(a) < \deg(q)$
$\deg(b) < \deg(P)$

$$a(x)\cdot p(x)+b(x)\,Q(x)=1.$$

Questo cosa ci dice nel caso $\mathbb{Z}[x]$

$p(x), q(x)\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$

$a,b\in\mathbb{Q}[x]$

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

$$a(x)=\frac{\bar{a}(x)}{m}\qquad b(x)=\frac{\bar{b}(x)}{n}$$

$$\bar{a}(x)\,p(x)+\bar{b}(x)\,q(x)=d\in\mathbb{Z}$$

$$\mathrm{MCD}\,\{p(n),\ q(n)\}\mid d$$

es. $p(x)=x^{2014}+x^{1000}-2$

$q(x)=x^2+1$

$$p(x)=q(x)\cdot Q(x)+a\cdot x+b$$

$$p(i)=\underbrace{\cancel{q(i)}}_{=0}\cdot Q(i)+a\cdot i+b$$

$$p(-i)=\underbrace{\cancel{q(-i)}}_{=0}\cdot Q(-i)-a\cdot i+b$$

$$\begin{cases} p(i) = ai + b \\ p(-i) = -ai + b \end{cases}$$

$p(i) = -1 + 1 - 2 = -2$

$p(-i) = -2$

$$p(x) - q(x) \cdot Q(x) = -2$$

$$MCD\left(n^{2014} + n^{1000} - 2,\ n^2 + 1\right) \Big| 2$$

$$x^{2014} + x^{1000} - 2 \equiv \quad (\text{mod } x^2 + 1)$$

$$= (-1)^{1007} + (-1)^{500} - 2 = -2$$

$$x^2 + 1 \equiv 0$$

$$x^2 \equiv -1$$

$$\frac{\mathbb{Q}[x]}{(x^2+1)} = \{ax + b\}$$

$$(ax+b)(cx+d) = ac \cdot x^2 + (bc + ad) \cdot x + bd$$

$$\equiv (bc + ad) \cdot x + (bd - ac)$$

Fatto: Se $p(x)$ è irriducibile, allora

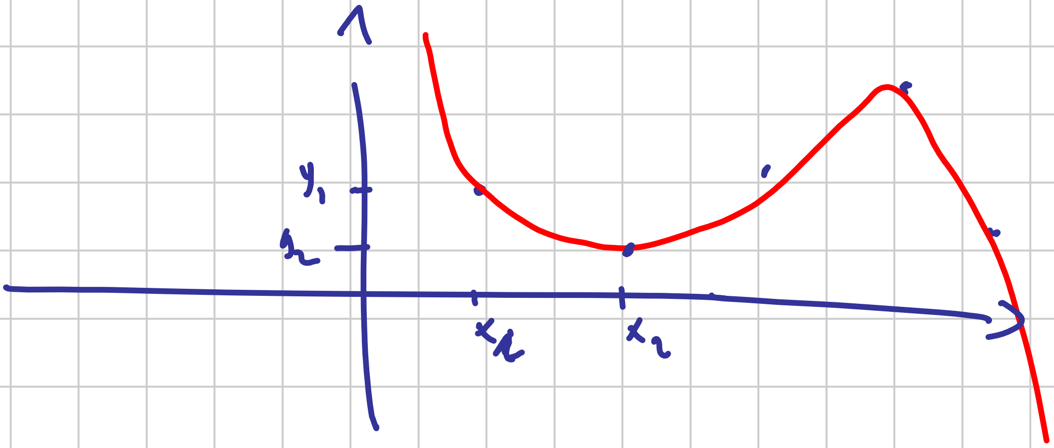
$$\frac{\mathbb{Q}[x]}{(p(x))} \text{ è un campo.}$$

Voglio trovare un polinomio "che passi dove voglio", ovvero "che ha dei valori assegnati".

ho $x_1, \dots, x_n, x_{n+1} \in A$ distinti e $y_1, \dots, y_{n+1} \in A$ non necessariamente distinti.

Q: Esiste un polinomio $p(x) \in A[x]$ tale che

$$p(x_i) = y_i \quad \forall\, i = 1, \dots, n+1$$



A: Sì, ma solo se A è un campo.

(A campo)

$$L_i(x) = \frac{(x-x_1)(x-x_2)\cdots\widehat{(x-x_i)}\cdots(x-x_{n+1})}{(x_i-x_1)(x_i-x_2)\cdots\widehat{(x_i-x_i)}\cdots(x_i-x_{n+1})}$$

L_i è un polinomio di grado n

tale che $L_i(x_j) = 0 \quad \forall j \neq i \qquad L_i(x_i) = 1$

$$p(x) = \sum_{i=1}^{n+1} y_i L_i(x) \qquad \deg(p) \leq n$$

$$p(x_j) = \sum_{i=1}^{n+1} y_i L_i(x_j) = y_j \overbrace{L_j(x_j)}^{\substack{1 \\ \shortparallel}} = y_j$$

Dim. 2

$$m \left\{ \begin{cases} \overbrace{a_n \cdot x_1^n + a_{n-1} \cdot x_1^{n-1} + \dots +}^{n} a_1 \cdot x_1 + a_0 = y_1 \\ a_n \cdot x_2^n + \dots \qquad a_1 \cdot x_2 + a_0 = y_2 \\ \vdots \qquad\qquad \vdots \\ a_n \cdot x_{n+1}^n + \text{—} \quad \text{—} \quad + a_1 \cdot x_{n+1} + a_0 = y_{n+1} \end{cases} \right.$$

$$\begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 & 1 \\ x_2^n & & & x_2 & 1 \\ \vdots & & & \vdots & \vdots \\ & & & x_n & \\ x_{n+1}^n & x_{n+1}^{n-1} & \dots & x_{n+1} & 1 \end{pmatrix} \cdot \begin{pmatrix} a_n \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_{n+1} \end{pmatrix}$$

Fatto (mistico) se ho un sistema $m \times n$ con $m \leq n$ allora ho almeno una soluzione (in genere)

Fatto 2 (ministrissimo) se ho un sistema $m \times m$ allora il sistema ha una soluzione se

$\det(M) \neq 0$.

$$\det(V) = \prod_{i<j}(x_i - x_j) \neq 0.$$

$\mathbb{Z}[x]$ $\quad p(2)=0, \quad p(0)=1$?

Non esiste perché $p(0)=1 \Rightarrow a_0 = 1$

ma allora $p(2)$ e' dispari

$$a_n \cdot 2^n + \dots + a_1 \cdot 2 + a_0 = 2 \cdot \text{roba} + a_0 = \text{dispari!}$$

se $p(x) \in \mathbb{Z}[x]$ $\quad a-b \mid p(a) - p(b)$

$$p(a) - p(b) = a_n \cdot (a^n - b^n) + a_{n-1} \cdot (a^{n-1} - b^{n-1}) \dots$$

$$\dots + a_1 (a-b)$$

$$a-b \mid a^m - b^m \quad \forall m \quad \Rightarrow \quad a-b \mid p(a) - p(b).$$

Ricordatevi l'esercizio.

Es. Sia $p(x) \in \mathbb{Z}[x]$. dimostra che

(i) sia $Q(x) = \overbrace{P(P(\ldots(P(x))))}^{k} - x$. Se $Q(n) = 0$ allora $P(P(n)) = n$ $(n \in \mathbb{N})$

(ii) IMO 2006/5

Dim. $a - b \mid P(a) - P(b)$

(prendo $b = P(a)$)

$$a - P(a) \mid P(a) - P(P(a))$$

$$P(a) - P(P(a)) \mid P(P(a)) - P(P(P(a)))$$

$$a - P(a) \mid P(a) - P(P(a)) \mid P(P(a)) - P(P(P(a))) \mid P^{(3)}(a) - P^{(4)}(a)$$

$$\ldots \quad \_\_ \mid P^{(k)}(a) - P^{(k+1)}(a)$$

Se $Q(a) = 0 \iff P^{(k)}(a) = a$

$$P^{(k+1)}(a) = P(P^{(k)}(a))$$

$$a - P(a) \mid P(a) - P(P(a)) \mid \ldots\ldots \mid a - P(a)$$

sono uguali

$$|a - P(a)| \leq |P(a) - P(P(a))| \leq \ldots\ldots \leq |a - P(a)|$$

Quindi $a - P(a) = \pm (P(a) - P(P(a)))$

caso 1 $\quad a-\cancel{P(a)} = -\cancel{P(a)}+P(P(a)) \Rightarrow P(P(a))=a$ ok.

caso 2 $\quad a-P(a) = P(a)-P(P(a))$

$$P(a)-P(P(a)) = \pm\left(P(P(a)) - P(P(P(a)))\right)$$

caso 2.1 $\quad P(a) - \cancel{P(P(a))} = -\cancel{P(P(a))} + P(P(P(a)))$

$$P(P(a)) \overset{d}{=} P(P(P(P(a))))$$

$$\overbrace{P\ldots}^{k} P(a) = P(\overbrace{P\ldots P}^{k+2} P(a))$$

$$a = P(P(a))$$

caso 2.2 $\quad P(a)-P(P(a)) = P(P(a)) - P(P(P(a)))$

caso 2.2.2. ..... 1. $\quad P^{(r)}(a) = P^{(r+2)}(a)$

applico P $k-r$ volte ad ambo i membri e ottengo $P^{(k)}(a) = P^{(k+2)}(a)$

cioè $a = P(P(P^{(k)}(a))) =$

$= P(P(a))$

caso II $\quad$ se non ci sono cambi di segni

$$P(a)-a = P(P(a)) - P(a) = P(P(P(a))) - P(P(a)) \,\_\_\_ \,\_\_\_$$

$$= P(a)-a$$

ma allora $P^{(r)}(a) = a_r \quad a_r$ è prog. aritmetica

$a_k = a_0 \Rightarrow a_r \equiv a_0 = a \Rightarrow a_1 - a_0 = 0$

$P(a) - a = 0$

$P(a) = a \Rightarrow P(P(a)) = a.$

Parte (ii) $Q_k(x) = P^{(k)}(x) - x$ (con k fissato).

Dimostrare che $Q(x)$ ha al più n radici intere, dove $n = \deg(P)$

(i) ci dice che $Q_k(n) = 0 \Rightarrow Q_2(n) = 0$

in particolare n° radici di $Q_k \leq$ numero di radici di Q_2.

Siano $a_1, a_2, a_3, \dots, a_{n+1}$ radici distinte di $Q_2(x)$

$$a_1 - a_2 \mid P(a_1) - P(a_2) \mid P(P(a_1)) - P(P(a_2))$$

Sappiamo che $P(P(a_1)) = a_1$ e $P(P(a_2)) = a_2$

$$a_1 - a_2 \mid P(a_1) - P(a_2) \mid a_1 - a_2$$

Quindi, di nuovo $a_1 - a_2 = \pm (P(a_1) - P(a_2))$

I $\quad a_1 - a_2 = P(a_1) - P(a_2) \rightsquigarrow a_1 - P(a_1) = a_2 - P(a_2)$

II $\quad a_1 - a_2 = P(a_2) - P(a_1) \rightsquigarrow a_1 + P(a_1) = a_2 + P(a_2)$

Considero $\quad h(x) = x - P(x) \qquad (n > \not{1})$

e $\quad g(x) = x + P(x)$

Presi $a_i, a_j \Rightarrow$ $h(a_1) = h(a_j)$ oppure

$g(a_1) = g(a_j)$.

$h(a_j) - h(a_1) = 0 \qquad a_j = a_1$

$g(a_j) - g(a_1) = 0 \qquad h(x) - h(a_1)$

wlog $h(a_2) \neq h(a_1)$

ma allora $g(a_2) = g(a_1)$.

$\forall a_i \quad g(a_i) = g(a_2)$

opp' $h(a_i) = h(a_2)$

$\exists j$ t.c. $h(a_j) = h(a_2)$ e $g(a_j) \neq g(a_2)$

$h(a_j) = h(a_2) \neq h(a_1)$

$$g(a_3) \neq g(a_2) = g(a_1)$$

$p(p(x))$ ha grado n^2 !! **ACHTUNG !**

Fattorizzazioni

1 - radici razionali
2 - Eisenstein
3 - Lemma di Gauss
4 - modulo p

$p(x) \in \mathbb{Z}[x]$

Radici razionali

$$p(x) = a_n x^n + \dots + a_1 x + a_0$$

se $r = \frac{p}{q}$ $(p,q)=1$ è radice di $p(x)$, allora $p \mid a_0$ e $q \mid a_n$.

$$0 = p(r) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0$$

$$0 = a_n p^n + a_{n-1} p^{n-1} \cdot q + \dots + a_1 p \cdot q^{n-1} + a_0 \cdot q^n$$

mod q $\quad 0 = a_n \cdot p^n + 0 \qquad q \mid a_n \cdot \cancel{p^n} \qquad q \mid a_n$

mod p $\quad 0 = a_0 \cdot q^n \qquad p \mid a_0 \cdot \cancel{q^n} \qquad p \mid a_0$

Guardo il polinomio mod p

$$A(x) = P(x) \cdot Q(x)$$

$$\overline{A}(x) = \overline{P}(x) \cdot \overline{Q}(x)$$

Se $\overline{A}$ è irriducibile, anche A lo è

Crit. Eisenstein sia $q(x) \in \mathbb{Z}[x]$ $\deg(q) = n$

tale che $p \nmid a_n$, $p \mid a_i$ $\forall\, 0 \leq i \leq n-1$ $p^2 \nmid a_0$

$\Rightarrow$ $q(x)$ è irriducibile.

Dim. $(\mathbb{F}_p)$ $\overline{q}(x) = a_0' \, x^n$

supp che $q(x) = a(x) \cdot b(x)$

$$a_0 x^n = \overline{q}(x) = \overline{a}(x)\,\overline{b}(x)$$

$\Downarrow$ fatt. unica

$\overline{a}(x) = \alpha x^k$ $\overline{b}(x) = \beta x^{n-k}$ $(\alpha\beta = a_0)$

$$a(x) = \tilde{\alpha} x^k + \dots \alpha_1 x + \alpha_0$$

$p \mid \alpha_0$ e $p \mid \beta_0$

$$b(x) = \tilde{\beta} x^{n-k} + \dots \beta_1 x + \beta_0$$

$$a(x) \cdot b(x) = x^n \cdot \tilde{\alpha}\tilde{\beta} + \quad \dots + (\alpha_1\beta_0 + \alpha_0\beta_1)\, x + \alpha_0\beta_0$$

$p^2 \mid \alpha_0 \beta_0 = a_0$ Assurdo!

Dim (contrassa) $a(x)\, b(x) = p(x)$

$a(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \dots + \alpha_0$

$b(x) = \beta_{n-k} \dots + \beta_0$

$a_0 = \alpha_0 \beta_0$ $p \mid a_0$ ma $p^2 \nmid a_0 \Rightarrow$ WLOG $p \mid \alpha_0$, $p \nmid \beta_0$

$a_1 = \alpha_0 \beta_1 + \beta_0 \alpha_1 \rightsquigarrow p \mid \alpha_1$

$a_2 = \alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0$ $p \mid \alpha_2$

$a_3 = \alpha_0 \beta_3 \dots \alpha_3 \beta_0$ $(p \mid \alpha_n)$

$a_k = \alpha_0 \beta_k + \dots + \alpha_{k-1} \beta_1 + \alpha_k \beta_0$

$a_{n-1} = \alpha_{k-1} \beta_{n-k} + \alpha_k \beta_{n-k-1}$

$a_n = \alpha_k \beta_{n-k}$

ma $p \nmid a_n \Rightarrow$ assurdo!

Eisenstein plus Se $p \mid a_i$ $\forall\, i \leq k$ e $p^2 \nmid a_0$ allora $p(x)$ ha un fattore irriducibile di grado almeno $k+1$.

Dim. $\overline{p}(x) = \overline{a}_n x^n + \dots \overline{a}_{k+1} x^{k+1} = x^{k+1} r(x)$

$\overline{p}(x) = \overline{a}_1(x) \cdot \overline{a}_2(x) \dots \cdot \overline{a}_s(x)$

devo distribuire i fattori di x^{k+1} tra tutti gli $\overline{a}_i$. Supp. per assurdo che $\deg(\overline{a}_i) \leq k$

$\overset{wlog}{\Rightarrow}$ $x \mid \bar{a}_1(x)$, $x \mid \bar{a}_2(x)$

$\Rightarrow$ termine noto di a_1 e di a_2 è divisibile per p $\Rightarrow$ Assurdo perché altrimenti $p^2 \mid a_0$.

$\boxed{\text{IMO } 1993-1}$ $x^n + 5x^{n-1} + 3$ è irriducibile per $n > 1$.

Eisenstein plus con $p = 3$ $k = n-2$

$\Rightarrow$ c'è un fattore irrid di grado almeno $n-1$

ma allora
- $x^n + 5x^{n-1} + 3$ è irrid. (ok)
- $x^n + 5x^{n-1} + 3 = (x - \xi)(\overset{n-1}{\cdot} \quad)$

Per il criterio della radice razionale $\xi \mid 3$

$\xi = \pm 1$ $\xi = \pm 3$ ma $p(\xi)$ è dispari

$p(x) = x^3 + x^2 + x + 2$

(A)^{V} non divide il polinomio $x^{2014} - x^{1997} + 2$

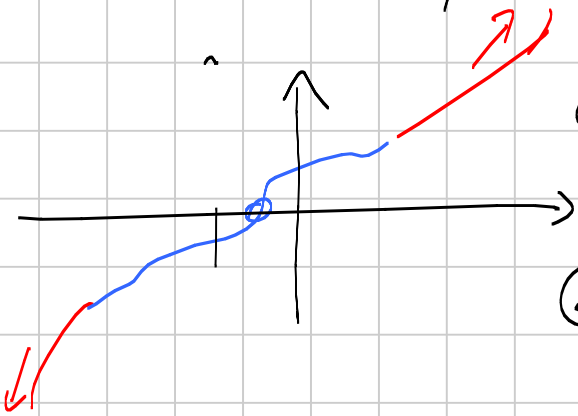
(B)^{V} Ha due radici comp. con. con $Re > 0$

(C)^{F} Ha una radice con $Im > 3/2$ $|\xi_1| < \sqrt{2}$

(D)^{V} Tutte le sue radici (ev. complesse) hanno mod > 1

(E)^{V} Ha un'unica radice reale.

Sui reali qualsiasi polinom. di grado dispari (a coeff. reali) si annulla almeno una volta.



(I) So che $p(x)$ ha almeno una radice reale.

(II) tutti i coeff. positivi

$\Rightarrow$ $p(x) > 0$ se $x > 0$ (non ha radici positive)

(III) $p(x) = (x+1)(x^2+1) + 1$

$p(-1) = 1$ $\qquad$ $p\left(-\frac{3}{2}\right) = \left(-\frac{1}{2}\right)\left(\frac{9}{4}+1\right) + 1 < 0$

ho una radice $r \in \left(-\frac{3}{2}, -1\right)$

Se $x < y < -1$ $\qquad$ $x+1 < y+1 < 0$

$x^2 > y^2$

$(x+1)(x^2+1) < (y+1)(x^2+1) < (y+1)(y^2+1)$

$p(x)$ è crescente per $x \leq -1$. $\rightarrow$ ha un'unica radice reale

$D(x^n) = n x^{n-1}$

$D(a_n x^n + \cdots + a_1 x + a_0) = a_n \cdot n \cdot x^{n-1} + \cdots + a_1$

Lemma: $p'(x) \geq 0$ in $[a,b]$ $\iff$ $p(x)$ e' crescente in $[a,b]$

$$p(x) = x^3 + x^2 + x + 2$$

$$p'(x) = 3x^2 + 2x + 1 = (x+1)^2 + 2x^2 > 0 \text{ sempre}$$

$\Rightarrow$ $p(x)$ e' crescente sempre.

Lemma ($p(x)$ ha radici doppie $\iff$ $(p(x), p'(x)) \neq 1$)

$$D(p \cdot q)(x) = D(p)(x) \cdot q(x) + p(x)\, D(q)(x).$$

$p(x)$ ha un'unica radice reale $r \in \left(-\frac{3}{2}, -1\right)$.

ξ_1, ξ_2 le radici complesse $\xi_1 = \overline{\xi_2}$

$r, \xi_1, \overline{\xi_1}$

relazioni di Viète (rad. coeff)

$$(x-r)(x-\xi_1)(x-\overline{\xi_1}) = x^3 + x^2 + x + 2$$

$$r + \xi_1 + \overline{\xi_1} = -1$$

$$2 \operatorname{Re} \xi_1 = -1 - r \in \left(0, \tfrac{1}{2}\right)$$

$$\operatorname{Re} \xi_1 \in \left(0, \tfrac{1}{4}\right)$$

$$r\xi_1\overline{\xi_1} = -2 \qquad |\xi_1|^2 = -\frac{2}{r} \in \left(\frac{4}{3}, 2\right)$$

$$|\xi_2| = |\xi_1| \in \left(\sqrt{\frac{4}{3}}, \sqrt{2}\right)$$

$$q(x) = x^{2014} - x^{1997} + 2 =$$

$$= (x^{17} - 1)(x^{1997}) + 2 \quad > 4$$

$$-\frac{3}{2} < r < -1 \qquad r^{17} < -1$$

$$r^{1997} < -1$$

$$x^{17} - 1 < -2$$

$$\cancel{x}^{1997} < -1$$

$$(x^{17} - 1)x^{1997} > 2$$

$q(x) > 0$ per $x < 0$

se $x \geq 1$ $\quad x^{2014} > x^{1997} \Rightarrow q(x) > 2$

se $x < 1$ $\quad x^{1997} < 1$

$$x^{2014} - x^{1997} + 2 > 0 - 1 + 2 > 1.$$

~

Polinomi ciclotomici

Radici dell'unità sono numeri complessi tali che $z^n = 1$ per qualche n.

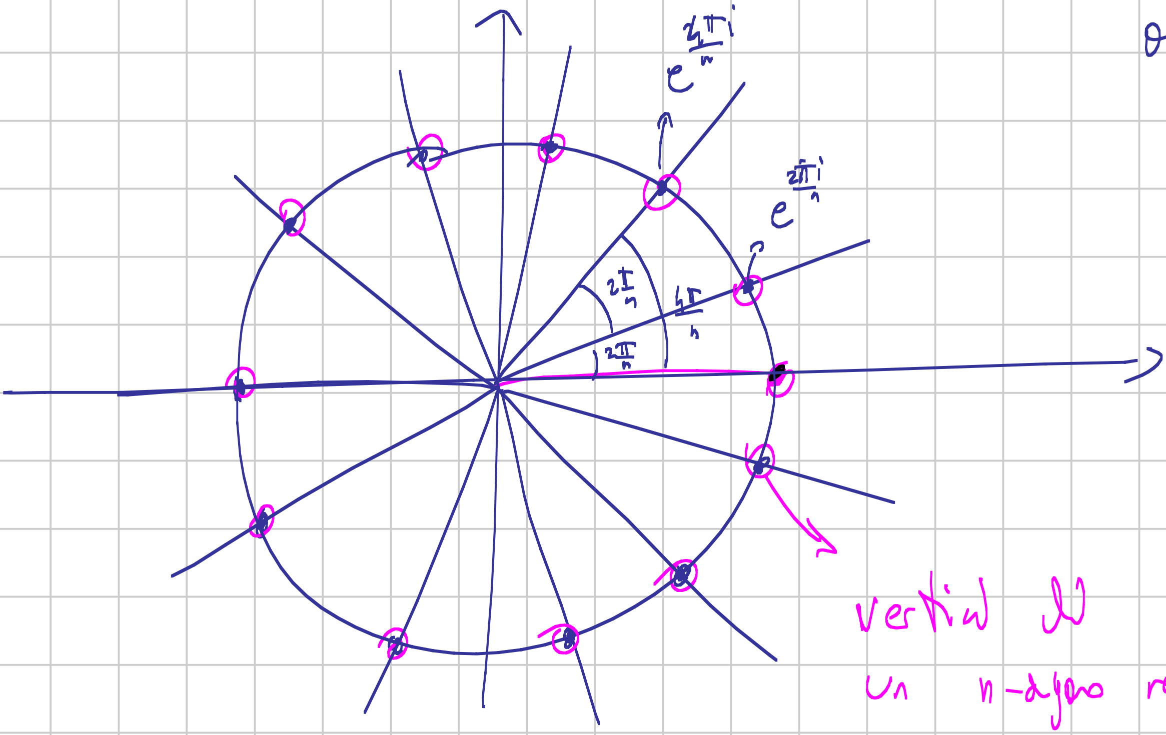
$$z = \rho \cdot e^{i\theta}$$

$$\rho = 1$$

$$z^n = \rho^n \cdot e^{in\theta} = 1 \qquad e^{in\theta} = 1 \iff n\theta = 2\pi k$$

$$\theta = \frac{2\pi k}{n}$$

$k = 1, \dots, n$



$$\xi_1, \dots, \xi_n \qquad \xi_k = e^{\frac{2k\pi i}{n}}$$

$$x^n = 1 \qquad p(x) = x^n - 1 = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n)$$

$n=6$ $\quad \xi_1 = e^{i\frac{2\pi}{6}} = e^{i\frac{\pi}{3}} = \cos\frac{\pi}{3} + i\,\text{sen}\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$

	$\wedge 2$	$\wedge 3$	$\wedge 4$	$\wedge 5$	$\wedge 6$
ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	1
ξ_2	ξ_4	1	ξ_2	ξ_4	1
ξ_3	1	ξ_3	1	ξ_3	1
ξ_4	ξ_2	1	ξ_4	ξ_2	1
ξ_5	ξ_4	ξ_3	ξ_2	ξ_1	1

e' anche radice 3_a

e' anche radice 2_a

$\xi_5 = (\xi_1)^{-1} = \overline{\xi_1}$

e' anche radice 3_a

$$(\xi_i)^3 = (\xi_1^{\,i})^3 = \xi_1^{\,i\cdot 3} = \xi_1^{\,(i\cdot 3)_6} = \xi_{(i\cdot 3)_6}$$

Se $(k,n)=1$ allora $\xi_k, \xi_k^2, \dots, \xi_k^n$ sono tutti distinti e sono tutte le radici n-esime dell'unità!

$$\xi_k^{\,s} = e^{\frac{2\pi i s k}{n}} = 1$$

$$\frac{\cancel{2\pi} sk}{n} = \cancel{2\pi} s$$

$sk = n s$ $\qquad n \mid sk \Rightarrow n \mid s$

$\Rightarrow s \geq n$

Se $(k,n)=1 \Rightarrow \text{ord}(\xi_k) = n$

Se $(k,n) = 1$ $\Rightarrow$ $\operatorname{ord}(\xi_k) = n$ $\Rightarrow$ rad. primitive sono $\phi(n)$

Se $(k,n) = d$ $\Rightarrow$ $\operatorname{ord}(\xi_k) = \frac{n}{d}$ $\Rightarrow$ rad. con ordine $\frac{n}{d}$ $\varphi(\frac{n}{d}$

$$\frac{\cancel{2\pi}\, j k}{n} = \cancel{2\pi}\, s \qquad j\frac{k}{d} = \frac{n}{d} s \qquad \frac{n}{d} \mid j \cdot \frac{k}{d}$$

$$\Downarrow$$

$$\frac{n}{d} \mid j$$

$(k,n) = d$ $\qquad dk'$ t.c. $(k', \frac{n}{d}) = 1$ $\qquad \varphi(\frac{n}{d})$

$\Downarrow$

$(\frac{k}{d}, \frac{n}{d}) = 1$

radici n-esime $= n = \sum_{d|n}$ radici n-esime che hanno ordine $\frac{n}{d}$ $= \sum_{d|n} \varphi(d)$

$$\Phi_n(x) = \prod_{(k,n)=1} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

$$\deg(\Phi_n) = \varphi(n)$$

$$x^n - 1 = \prod_{k=1}^{n} \left(x - e^{\frac{2\pi i k}{n}}\right) = \prod_{d|n} \prod_{(k', \frac{n}{d})=1} \left(x - e^{\frac{2\pi i k'}{n/d}}\right)$$

$$= \prod_{d|n} \Phi_{\frac{n}{d}}(x)$$

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$$

$$\Phi_6(x) = x^2 - x + 1 .$$

$$(x^3+1)\cancel{(x^3-1)} = x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$$

$$= (x-1)(x+1)(x^2+x+1)\,\Phi_6(x)$$

$$= \cancel{(x^3-1)}(x+1)\,\Phi_6(x)$$

$$\Phi_6(x) = \frac{x^3+1}{x+1} = x^2 - x + 1$$

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)} = \frac{x^{15} - 1}{(x^5 - 1)(x^2 + x + 1)} =$$

$$= \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = ?$$

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

$$\mu(n) = \begin{cases} 1 & \text{se } n=1 \\ 0 & \text{se } n \text{ non è sq.free} \\ (-1)^k & \text{se } n = p_1 p_2 \cdots p_k \end{cases}$$

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

$$\left(\text{se } h(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} h(d)\,\mu\!\left(\frac{n}{d}\right) \right)$$

Es. Fissato n, esistono infiniti primi $p \equiv 1 \ (n)$

Dim. Sia $a > 1$ a multiplo di n, consideriamo $p \mid \Phi_n(a)$ $\quad p \nmid n$

$$\Phi_n(a) \equiv 0 \quad (p)$$

$$a^n - 1 \equiv 0 \quad (p)$$

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

supponiamo $\mathrm{ord}_p(a) = d$

$$a^d \equiv 1 \quad \text{con } d < n$$

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

$$\equiv \frac{n}{d} \quad (p)$$

assurdo se $p \nmid n$

$$\Phi_n(a) \cdot (a^d - 1) \mid a^n - 1 \qquad p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^d - 1}$$

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

$p \equiv 1 \ (n)$.

$q \mid \Phi_n(pn)$ $\quad$ $\Phi_n(qpn)$.

Consid.

$q \mid \Phi_n(pa)$ $\quad$ $\mathrm{ord}_q(pa) = n$

a multiplo di $n \Rightarrow p \nmid n$.

$p \mid \Phi_n(a)$.