

# Equazioni con congruenze di grado superiore al primo

## Congruenze di II grado

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

$a \neq 0$

$p$  primo  $\neq 2$

① si moltiplica per  $4a$

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

② si somma  $b^2 - 4ac$

$$4ax^2 + 4abx + b^2 \equiv b^2 - 4ac \pmod{p}$$

$$(2ax+b)^2$$

③ Realice quadrate

$$2ax+b = \pm \sqrt{b^2 - 4ac} = \pm \sqrt{\Delta}$$

$$\text{④ } x = \frac{-b \pm \sqrt{\Delta}}{2a}$$

$$\sqrt{\Delta} \in \mathbb{R} \text{ se } \Delta \geq 0$$

Dividere per  $2a$  significa  
moltiplicare per l'inverso di  $2a$ .  
NON perché  $(2a, p) = 1$

in mod  $p$ , entro delle classi soddisfano queste condiz.

$$\text{Ex. } p=3$$

$$\begin{aligned} 0^2 &\equiv 0 \\ (\pm 1)^2 &\equiv 1 \\ \text{non c'è } \sqrt{2} \end{aligned}$$

$$p=5$$

$$\begin{aligned} 0^2 &\equiv 0 \\ (\pm 1)^2 &\equiv 1 \\ (\pm 2)^2 &\equiv 4 \\ \text{non c'è } \sqrt{3}, \sqrt{5} \end{aligned}$$

$$p=7$$

$$\begin{aligned} 0^2 &\equiv 0 \\ (\pm 1)^2 &\equiv 1 \\ (\pm 2)^2 &\equiv 4 \\ (\pm 3)^2 &\equiv 9 \equiv 2 \\ \text{non c'è } \sqrt{2} \end{aligned}$$

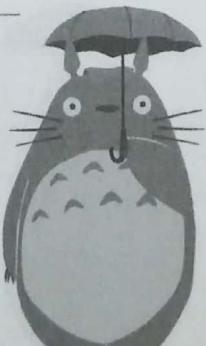
$$\text{Ex su slide}$$

Se il numero NON è primo...

• Nel caso di  $p^k \rightarrow p$ , perché  $p | p^k$  ..., right?

S

• Teorema cinese del contrario; Trasformazione in sistema con i mod fattori primi e le stesse equazioni



## Congruenze esponenziali

Ex.  $3^x \equiv 1 \pmod{7}$  calcola il periodo minimo con  
 $\min = 6 \quad \leftarrow \text{LFT}$

$$\begin{array}{c} \downarrow \\ x=0 \pmod{6} \end{array}$$

$$\begin{array}{r|rrr|rr} 3^0 & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 \\ \hline & 1 & 3 & 9 & 27 & 1 \\ 3^5 & 12 & 5 & 36 & 1 & \end{array}$$

$$3^x \equiv 5 \pmod{7}$$

guardando le tabella,  $x \equiv 5 \pmod{6}$  è soluzione

Oss. Quello che conta è il modulo FINAL

## Risoluzione di sistemi

$p$  primo

$$\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{p^2} \end{cases} \quad \begin{array}{l} \text{se c'è sol per } p^2, \rightarrow \text{allora c'è per } p, \\ \text{NON VADO IL CONTRARIO} \end{array}$$

$x \equiv c \pmod{p^2} \rightarrow x \equiv c \pmod{p}$  NON IL CONTRARIO,  
 quindi nell'es c'è soluzione se e solo se  $a \equiv b \pmod{p}$   
 ed è  $x \equiv b \pmod{p^2}$

## La funzione di Euler

(mais)

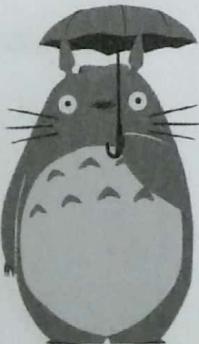
$a \in \mathbb{Z}/n\mathbb{Z}$  ha un inverso se e solo se  $(a, n) = 1$ .

Vogliamo CONTARE quante sono le classi con queste proprietà

Abbiamo esaminato due casi:

1-  $n = p$  (nr. primo)

2-  $n = p^k$  (potenza di un nr. primo)



Caso(1): Le classi cercate sono tutte quelle  $\neq 0 \pmod{p-1}$

Caso(2): Le classi cercate sono tutte tranne quelle dei nr. che hanno MCD con  $p > 1$ , quindi quelle dei nr. DIVISIBILI per  $p$

Dovendo perciò eliminare  $p^{k-1}$  classi,  $p^k - p^{k-1} = p^{k-1}(p-1)$

Caso generale - Teorema cinese

$$n = p^a q^b \quad p, q \text{ primi}$$

Vedi slide

$$\text{Il nr. di sistemi è } (p^a - p^{a-1})(q^b - q^{b-1}) = \\ p^{a-1} q^{b-1} (p-1)(q-1)$$

Generalizzazione: se  $n = p$  (primo), allora  $\phi(n) = \phi(p) = p-1$

ANALOGIA CON L'PT

o Dim per l'orale? Key be better times o

Periodo minimo divisore di  $\phi(n)$  ( $\phi(p) \rightarrow p-1$ )

s: calcolo a mano?

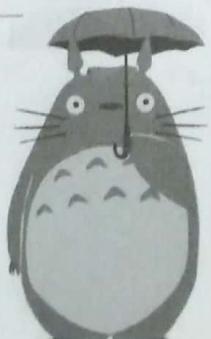
Trucco EX.  $z^x \equiv 8 \pmod{16}$ , voglio Trovare il periodo

$$z^1 \equiv 2 \quad z^2 \equiv 4 \quad z^3 \equiv 8 \quad z^4 \equiv 16 \equiv 5 \quad z^5 \equiv 32 \equiv 1 \quad \text{STOP}$$

il periodo deve per forza essere un

DIVISORE di  $p-1$ , qui ndi: 1, 2, 4, 8, 16

guarda agli esercizi: 122, 16-03



# Polinomi

$A[x]$  A insieme di coefficienti

Oss. Nell'insieme  $A[x]$  si possono fare somme e moltiplicaz.

I gradi di un polinomio è il massimo intero  $n$  per cui  $a_n \neq 0$

Note: NON si definisce (solitamente) il grado del polinomio 0

$$\deg(f+g) \leq \max\{\deg f, \deg g\}$$

$$\deg(fg) \leq \deg f + \deg g$$

Oss. Se  $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ , allora  $\deg(fg) = \deg f + \deg g$

Se  $f \in A[x]$ , l'inverso è un polinomio  $g$  tale che  $f \cdot g = 1$ .

Questo è possibile solo se  $\deg(f) = \deg(g) = 0$ , cioè solo

~~se non c'è la  $x$  (polinomi "costanti")~~

Note In  $\mathbb{Z}$  solo 1 e -1 hanno un inverso.

## Divisione euclidea aka divisione con resto

Numeri interi

$$a = q b + r$$

q quoziente, r resto

$$0 \leq r < |b|$$



Polinomi

$$f = qg + r$$

resto "piccolo":  $\deg r < \deg g$   
oppure  $r = 0$

**Prop.** Dati  $f, g \in K[x]$  con  $g \neq 0$ , esistono e sono unici due polinomi  $q, r \in K[x]$  con:

- $f = qg + r$
- $\deg r < \deg g$  oppure  $r=0$

**Dim.** su slide

L'algoritmo di Euclide è applicabile anche ai polinomi

### Ripasso! Algoritmo di Euclide

$$|a| = |b|q + r_1$$

$$|b| = r_1 q_1 + r_2$$

$$r_1 = r_2 q_2 + r_3$$

...

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

$$r_{n-1} = r_n q_n + 0$$

$$r_n = \text{MCD}(|a|, |b|)$$

!!!

Ogni polinomio  $f(x) \in K[x] \neq 0$  si scrive in modo unico (e meno di fattori costanti) come prodotto di polinomi irriducibili

Analogie Tra polinomi irriducibili e nr. primi

Teorema di Ruffini !!!

Sia  $f(x) \in K[x]$ , allora  $a \in K$  è una radice di  $f(x)$  se e solo se  $x-a \mid f(x)$

**Dim.** Esegui la divisione euclidea di  $f(x)$  per  $x-a$ :

- $f(x) = q(x)(x-a) + r(x)$   $\deg r < \deg$  divisore si, oppure  $r=0$
- $\downarrow \deg = 1$      $\downarrow$  costante ha grado 0, perciò  
 $r = \text{costante}$  (oppure 0)  
 (che può essere  $= 0 \neq 0$ )



Sostituisco in  $x=a$ :

$$f(a) = q(a)(a-a) + r \rightarrow f(a) = r$$

QUINDI  $r=0$  (resto zero  $\Rightarrow x-a \mid f(x)$ )  $\Leftrightarrow \underline{f(a)=0}$

- che è l'enunciato del teorema

**Prop.** Un polinomio  $f \in K[x]$  di grado  $n$  ha al più  $n$  radici.

**Dim. Induzione su  $n$**

Caso base  $n=0$

se  $f=0$ , tutti gli elementi di  $K$  sono radici

$f=c \neq 0$ , NNESSUN elemento di  $K$  è radice

Passo induttivo  $n \rightarrow n+1$

Supponiamo che  $f = \underline{n+1}$

Mo' dove c'è:

- $f$  non ha NESSUNE radice, QUINDI  $0 < n+1$  OR
- $f$  ha almeno una radice  $a$ , QUINDI (RUFFINI)  $f(x)$  è divisibile per  $x-a$ :  
 $f(x) = q(x)(x-a)$   
gradi  $n+1$      $n$      $1$

Supponiamo che  $b$  sia una radice di  $f(x)$ , cioè  $\underline{f(b)=0}$

$$q(b)=0 \quad \textcircled{1}$$

$$\text{Mo' } 0 = f(b) = q(b)(b-a) \rightarrow b-a=0 \quad \textcircled{2}$$

①  $b$  è una radice del polinomio  $q$ , di grado  $n$ .

Per ipotesi induttiva,  $q$  ha non più di  $n$  radici

$\Rightarrow$  non più di  $n$  possibilità

②  $b=a \Rightarrow 1$  possibilità

① + ② = al più  $n+1$  possibilità



In un campo  $\mathbb{K}$  con infiniti elementi, vale il principio delle identità dei polinomi.

In campi con elementi finiti, come  $\mathbb{Z}/p\mathbb{Z}$ , il principio delle identità NON VALE.

**Teorema di Wilson:**  $p$  primo, allora  $(p-1)! \equiv -1 \pmod{p}$

## Numeri complessi $\mathbb{C}$

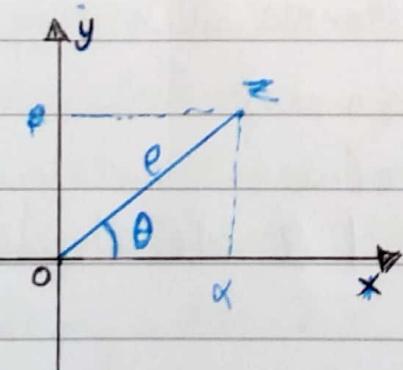
27-04

i elementi tale che  $i^2 = -1$ . Si possono risolvere eq. con discriminante ( $\Delta$ ) negativo.

Forme  $\alpha + i\beta$

## Coordinate polari

$$z = \alpha + i\beta$$



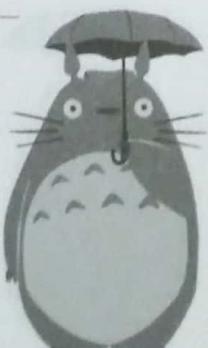
$\rho$ : lunghezza del vettore  $\vec{Oz}$

Teo. di Pitagora  $\rho = \sqrt{\alpha^2 + \beta^2}$

$\theta$ : angolo che  $\vec{Oz}$  forma con l'asse x  
(senso antiorario)

Le coordinate polari di  $z$  sono  $(\rho, \theta)$  e si chiamano  
modulo di  $z$  ( $\rho$ )

argomento di  $z$  ( $\theta$ )



# Relazioni con coordinate cartesiane

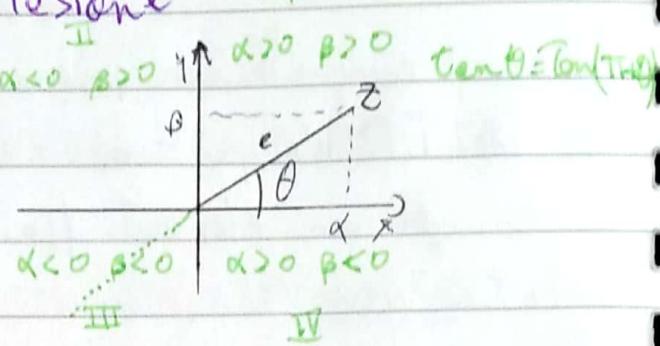
$$x = \rho \cos \theta$$

$$y = \rho \sin \theta$$

$$z = \rho \cos \theta + i \sin \theta$$

$$\rho = \sqrt{x^2 + y^2}$$

$\theta = \arctan \frac{y}{x} \rightarrow$  per capire il quadrante, guardare il segnale di  $y$



La corrispondenza  $(\rho, \theta) \leftrightarrow (x, y)$  è BIUNIVOCÀ, tranne in  $(0,0)$ :  $\rho = 0$  ma  $\theta$  qualsiasi cosa  $\rightarrow$  NON si stilizzano per l'origine

coordinate polari del prodotto  $(e^{i\theta}, \rho_1)$

Si moltiplica le lunghezze, si somma l'angolo

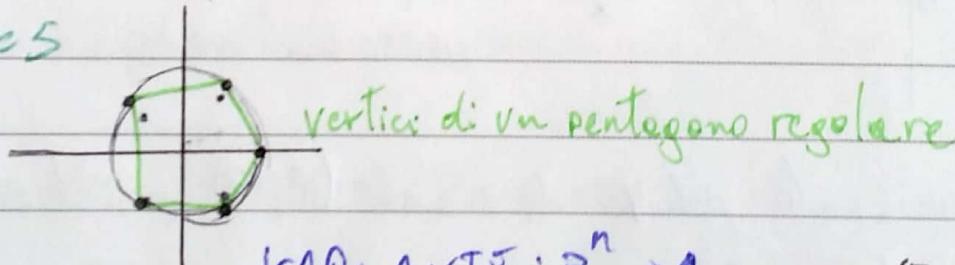
## Equazioni particolari in $\mathbb{C}$

$$z^n = 1 \quad \text{sol. in } \mathbb{R} = 1 (+ -1 \text{ se n pari})$$

sol. in  $\mathbb{C} \rightarrow$  rappresentazione grafica:

- Dividere  $2\pi$  per  $n$ , questo è il  $\theta$  delle soluzioni.  $\rho = 1$

es.  $n=5$



VARIANTE:  $z^n = a$   $a = (3, \tau)$

$$z^n = (\rho^n, n\theta)$$

DEF. MIA

$$\begin{cases} \rho^n = 3 \\ n\theta = \tau + 2k\pi \end{cases} \rightarrow \rho = \sqrt[n]{3} \quad \theta = \frac{\tau}{n} + \frac{2k\pi}{n}$$

le sol. sono sempre i vertici di una figura regolare ma con un offset di  $\frac{\tau}{n}$



# Teorema fondamentale dell'algebra

Ogni polinomio  $f(x) \in \mathbb{C}[x]$  di grado  $\geq 1$  ha almeno una radice complessa

Oss. Non vale per i polinomi  $\in \mathbb{Q}[x]$  o in  $\mathbb{R}[x]$

## Conseguenze

I polinomi IRRIDUCIBILI in  $\mathbb{C}$  sono solo quelli di grado 1

## Il coniugio dei numeri complessi:

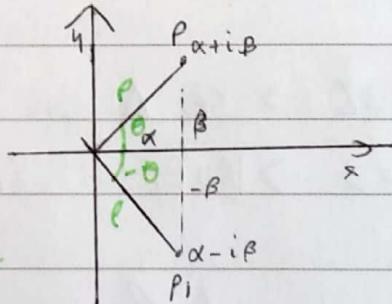
coniugio: funzione  $\mathbb{C} \rightarrow \mathbb{C}$   $z \mapsto \bar{z}$

definito così: se  $z = \alpha + i\beta$ , allora  $\bar{z} = \alpha - i\beta$

il coniugio è la simmetria rispetto all'asse delle  $x$ .

possiamo anche scrivere il coniugio con le coordinate polari:  $z \mapsto (r, \theta)$   $\bar{z} \mapsto (r, -\theta)$

$$\bar{z+w} = \bar{z} + \bar{w}$$

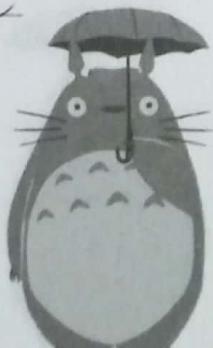


## Polinomi a coefficienti reali

30-04

Sia  $f(x) \in \mathbb{R}[x]$  ( $\subseteq \mathbb{C}[x]$ ). Se  $\alpha \in \mathbb{C}$  è una radice di  $f(x)$ , allora anche  $\bar{\alpha}$  lo è.

dim sul slide



## Polinomi irriducibili in $\mathbb{R}[x]$

I polinomi che non presentano radici reali di  $\deg(f) < 0$  sono irriducibili in  $\mathbb{R}[x]$ .

Se  $d = \deg(f(x)) > 2$ , allora  $f$  è riducibile. Dim sussiste

Note: Per arrivare ad alcune fattorizzazioni in  $\mathbb{R}$  si deve essere per  $\mathbb{C}$ , per poi moltiplicare le radici coniugate per ottenere polinomi reali di grado 2.

## Polinomi irriducibili in $\mathbb{Q}[x]$ (coeff. razionali)

Ci sono polinomi irriducibili di QUAISIASI grado  $n \geq 1$ . In particolare

$\deg = 2 \rightarrow$  se  $\Delta$  non è un quadrato perfetto  $\rightarrow$  IRRIDUCIBILE

$\deg = 3 \rightarrow$  (RUFFINI)  $f(x)$  deve avere una radice razionale

## Lemme di Gauss

Se  $f(x) \in \mathbb{Z}[x]$  e ci sono due polinomi  $g(x), h(x) \in \mathbb{Q}[x]$  tali che  $f(x) = g(x)h(x)$ , allora ci sono anche dei polinomi  $g'(x), h'(x) \in \mathbb{Z}[x]$  dello stesso grado di  $g$  e  $h$  tali che

$$f(x) = g'(x)h'(x)$$



In sostanza, si possono eliminare i denominatori di  $g(x)$  e  $h(x)$  moltiplicando per costanti opportune

per passare a un polinomio  $\in \mathbb{Z}[x]$  faccio il mcm dei coefficienti.

## • COMBINATORIA .

Principio di inclusione - esclusione :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Applicazioni: nr. divisibili:

### Combinazioni con ripetizione

Distribuire 10 pelline in tre scatole, mettendone almeno una in scatola. Quante sono le combinazioni possibili?

30

• 3 pelline a scatola :  $10 - 3 \Rightarrow$  lo collocare

$$n = 3 \text{ (scatole)}$$

$$k = 7 \text{ (pelline)}$$

$$\frac{(n+k-1)!}{k!(n-1)!} = \frac{(3+7-1)!}{7!(3-1)!} = \frac{9!}{7!2!} = 36$$

permutazioni  $n!$

se non conta l'ordine  $\binom{n}{r} \binom{r}{k} = \frac{n!}{k!(n-k)!}$

Tutti i sottoinsiemi:  $2^n$

• Teorema cinese del resto f DIM

• Algoritmo di Euclide applicato a polinomi

• MCD polinomi (Ascoli)

• Cose di combinatoria - Sottinsiemi

• Formula ricorsiva Fibonacci

Combinatore asf!

## Ricorsive - Fibonacci

Successione definite come esponenziali

$$F_n = \alpha^n \quad \alpha = \sqrt[2]{\alpha^{n-1} + \alpha^{n-2}} \rightarrow \alpha^2 = \alpha + 1$$

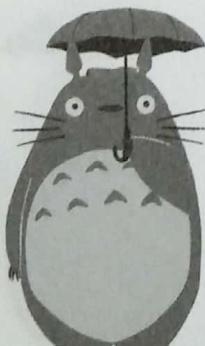
Radici  $\alpha = \frac{1 \pm \sqrt{5}}{2}$  queste però non appartengono agli stessi nr di Fibonacci,

quindi abbiamo:

$$\alpha \alpha^n + b \beta^n \Rightarrow \text{mettiamo a sistema con } F_0 = 0 \text{ e } F_1 = 1, \\ \text{unica soluzione } a = \frac{1}{\sqrt{5}}, b = -\frac{1}{\sqrt{5}}$$

La successione è quindi definita come

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



## UTILITIES:

$$\text{LFT: } a^{(p-1)} \equiv 1 \pmod{p} \quad a^x \equiv 1 \pmod{p} \quad x \equiv 0 \pmod{p-1}$$

ATTENZIONE! Vale solo per i primi

## ARITMETICA MODULARE

Opera solo con i primi

Per Trovare une sol. di un sistema fai l' MCM

### Teorema cinese applicazione

$$n_1 k = n_2 k + b - a$$

$$\begin{cases} x \equiv a \pmod{n_1} \\ x \equiv b \pmod{n_2} \end{cases} \quad n_1 k = b - a \pmod{n_2}$$

$$\text{sol } x \equiv x_0 \pmod{\text{lcm}(n_1, n_2)}$$

$$x_0 + S \cdot \text{lcm}(n_1, n_2)$$

### • Counting •

$\text{MCD}(x, n) \leq x \quad \text{mcm}(4, n) \leq q \quad \text{quanti } n \text{ esistono?}$

Scomposizione di  $x$  e  $y$ . Per ogni fattore, si prenda l'esp.  
nel mcm di  $x$  e  $y$  e si sottrae quello del mcd se presente.

Si moltiplicano fra loro i nr. ottenuti

## Criterio di irriducibilità di Eisenstein

Sia  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  a coefficienti interi e supponiamo che esiste un primo  $p$  tale che:

i.  $p \nmid a_n$ ,  $p \mid a_{n-1}, p \mid \dots, p \mid a_1$ ,  $p \nmid a_0$

ii.  $p^2 \nmid a_0$

allora  $f(x)$  è irreducibile

## Principio di inclusione-esclusione

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

## Funzione di Eulero

$\phi(n)$  indica il nr. degli interi positivi < n e coprimi con n

$$x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^{\phi(p)} \equiv 1 \pmod{p} \text{ (generalizzazione)}$$

## Teorema cinese del resto

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \begin{array}{l} m, n \text{ coprimi} \\ \text{sol comune} \\ x = a + mk = b + nh \\ \text{risolvibile solo se } \frac{m}{\text{lcm}} \mid b - a \end{array}$$

## Piccolo Teorema di Fermat

$$\begin{aligned} x^{p-1} &\equiv 1 \pmod{p} \\ x^p &\equiv x \pmod{p} \end{aligned}$$



## Tipologie di esercizi - congruenze

$$(\alpha + x)^n \equiv b \pmod{n} \rightarrow \alpha + x \equiv b \pmod{n}$$

NR. complessi:

$\frac{\text{espr}}{m} = \alpha + bi \rightarrow \text{espr} = (\alpha + bi) (m)$ , poi raccogli  
su  $a$  e  $b$  e vai a tentativi

## DIOFANTEO - minimo

Trovare minimo  $n \geq k$  tale che  $n = \beta x + \gamma y$  ha soluzione.  
 $\text{lcm}(\beta, \gamma) \rightarrow$  moltiplica finché non  $i \geq k$ . ecco  $n$ .

Sottoinsiemi pari e dispari

$n$  dispari: a ogn' insieme pari corrisponde il compl. oligo  
pari  $\frac{2^n}{2} = 2^{n-1}$  gli pari  $\frac{2^n}{2} = 2^{n-1}$   $[2^{n-1}]$

$n$  pari: fassene: conti con il coeff binomiale  
Viene sempre  $2^{n-1}$

## Teorema di Eulero

Abbiamo tre casi:

1.  $n \equiv p \rightarrow$  Tutte le classi diverse da  $\bar{0} \rightarrow (p-1) \rightarrow [p^1 - p^0]$
2.  $n \equiv p^K \rightarrow p^N - p^{K-1}$
3. Caso generale  $\rightarrow$  Si applica il teorema cinese e si scrive  $n$  come prodotto di primi. Si procede come 2. e si moltiplicano i risultati.

**ANALOGIA CON LFT:** se  $(x, p) = 1 \rightarrow x \in I(p)$   
se  $(x, n) = 1 \rightarrow x^{(q^n)} \in I(n)$

## TEOREMA DI RUFFINI

Sia  $f(x) \in K[x]$ .

Allora  $\alpha \in K$  è una radice

della  $f(x)$  se e solo se  $x-\alpha | f(x)$

← DIM P5