Piccolo teorema di Fermat

p primo $\Rightarrow x^p \equiv x \ (p)$

Dim. Ricordiamo che se $0<i<p$ $p \mid \binom{p}{i}$ visto

Calcoliamo

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$

(Teorema del binomio di Newton)

$$\equiv_p \binom{p}{0} a^0 b^p + \cancel{\binom{p}{1} a^1 b^{p-1}} + \dots + \binom{p}{p} a^p b^{p-p}$$

$\equiv 0 \ (p)$

$$\equiv_p b^p + a^p.$$

$(a+b)^p \equiv a^p + b^p \ (p)$ se p primo

$(a+b+c)^p \equiv_p ((a+b)+c)^p \equiv_p$

$(a+b)^p + c^p \equiv a^p + b^p + c^p \pmod p$.

$(a+b+c+d+\dots+)^p \equiv a^p + b^p + c^p + \dots \ (p)$

Induzione su n

$(a_1 + a_2 + \dots + a_n)^p \equiv_p a_1^p + a_2^p + \dots + a_n^p$

$n^p \equiv \underbrace{(1+1+1+\dots+1)^p}_{n \text{ volte}} \equiv \underbrace{1^p + 1^p + \dots + 1^p}_{n}$

$\equiv \underbrace{1+1+\dots+1}_{n \text{ volte}} \equiv n \pmod p$.

Ho dimostrato $n^p \equiv n \ (p)$
$\forall n \in \mathbb{N}$.
Funziona anche per n negativo.
perché ogni $x \in \mathbb{Z}$ è congruo modulo (p) a un $n \geq 0$
(anche $0 \leq n < p$) $x \equiv n \ (p)$.

$$x^p \equiv \underbrace{x \cdot \ldots \cdot x}_{p \text{ volte}} \equiv \underbrace{n \cdot n \cdot \ldots \cdot n}_{p} = n^p \equiv n \ (p) \equiv x \ (p)$$

Quindi vale
$x^p \equiv x \ (p)$
per x sia positivo che negativo.
$x \in \mathbb{Z}$. □ piccolo teo di Fermat

p deve essere primo

Cor Se $x \not\equiv 0 (p)$
vale $x^{p-1} \equiv 1 (p)$.

Dim. So che $x^p \equiv x (p)$.
Divido la congruenza per x.
Perché lo posso fare?
$x \not\equiv 0 (p) \Rightarrow p \nmid x \Rightarrow MCD(x,p) = 1$
(p primo)
$\Rightarrow$ x ha un inverso modulo p.
$\Rightarrow$ posso dividere la congruenza

Cioè da $x^p \equiv x (p)$ $\leftarrow \forall x$
ottengo $x^{p-1} \equiv 1 (p)$ $\leftarrow x \not\equiv 0 (p)$

□

Esempi Trovare gli $x \in \mathbb{Z}$ tali che

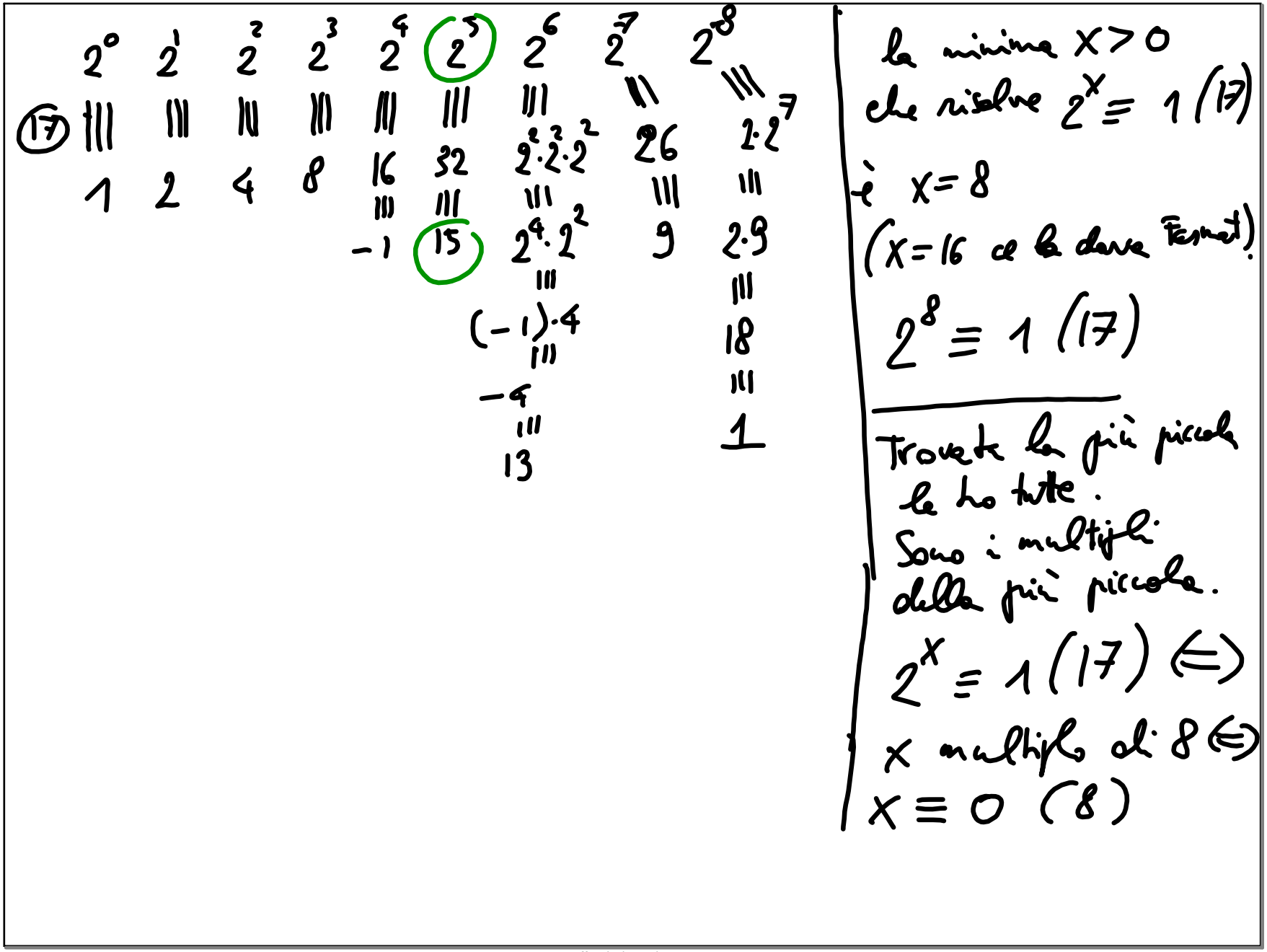
$2^x \equiv 1 \ (17)$.

Congruenza esponenziale: la x sta in esponente.
(La riconduco a una congruenza $x \equiv b \ (c)$).

— Piccolo teo di Fermat ci fornisce una soluzione: $x = ?$ $x = 16$
17 primo $\Rightarrow 2^{17-1} \equiv 1 \ (17) \Rightarrow 2^{16} \equiv 1 \ (17)$.
Però non è detto che sia la minima soluzione.

— Trovare la minima soluzione

La minima x è zero. A parte zero, $0 < x \leq 16$.
Le provo tutte
(in realtà vedremo che basta provare i divisori di 16).
Per ora le provo tutte.


2^0 2^1 2^2 2^3 2^4 2^5 2^6 2^7 2^8
(17)
1 2 4 8 16 32 26 $2\cdot 2^7$
-1 15 9 $2\cdot 9$
$(-1)\cdot 4$ 18
-4 1
13
la minima $x>0$ che risolve $2^x \equiv 1\ (17)$
è $x=8$
(x=16 se la dava Fermat)
$2^8 \equiv 1\ (17)$
Trovate la più piccola le ho tutte.
Sono i multipli della più piccola.
$2^x \equiv 1\ (17) \Leftrightarrow$
x multiplo di 8 $\Leftrightarrow$
$x \equiv 0\ (8)$

dic 1-14:41

Def La minima $x > 0$:

$$2^x \equiv 1 \ (17)$$

si chiama ordine di 2 mod 17.

che in questo caso è $\boxed{8}$

$$8 = O_{17}(2) = \text{ordine di } 2 \text{ mod } 7.$$

Def La min. $x > 0$

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

si chiama

ordine di a mod n.

Se n è primo Fermat ci fornisce una soluzione x che però non è detto sia la minima.

Teo $a^x \equiv 1 \ (p)$ ⇕ $x \equiv 0$ (ordine di a mod p)

Es $2^x \equiv 1 \ (17)$ ⇕ $x \equiv 0 \ (8)$

funziona anche per $x<0$ però che vuol dire?

$2^{-8} \equiv 1 \ (17)$

chi è 2^{-8} ?

non è $\frac{1}{2^8} \notin \mathbb{Z}$

Per convenzione quando lavoro mod p

2^{-1} non è $\frac{1}{2}$ ma è un inverso di 2 mod p.

$2^{-1} \underset{(17)}{\equiv} 9 \qquad 2 \cdot 9 \equiv 1 \ (7)$

dic 1-14:49

mod 17. $2 \cdot 9 \equiv 18 \ (17)$

$\Rightarrow 2^{-1} \equiv 9$. (un inverso di 2 mod 17)

$2^{-n} \equiv (2^{-1})^n \equiv 9^n$.

Con queste convenzioni

$2^8 \equiv 1 \ (17)$ Sperimentalmente

$2^{16} = 2^8 \cdot 2^8 \equiv 1 \cdot 1 \equiv 1 \ (17)$

$2^{8k} = \underbrace{2^8 \cdot \ldots \cdot 2^8}_{k} \equiv 1 \ (17)$

per $k<0$? $k=-1$

$2^{-8} = (2^{-1})^8 = 9^8 \equiv 1$

$2^n \cdot 2^{-n} = 2^n \cdot (2^{-1})^n$

$= 2^n \cdot 9^n \equiv (2 \cdot 9)^n \equiv 18$

$\equiv (1)^n \equiv 1$.

$\forall n \rightarrow$ $2^n \cdot 2^{-n} \equiv 1 \ (17)$

$1 \equiv 2^8 \cdot 2^{-8} \equiv 1 \cdot 2^{-8} \equiv 2^{-8}$ (17)

$1 \equiv 2^{-8} \ (17)$

dic 1-14:53

In generale:

Se $a^x \equiv 1 \ (p)$

$\Rightarrow$ anche $\boxed{\bar{a}^x \equiv 1 \ (p)}$.

dove $\bar{a}^x = (\text{inverso di } a \bmod p)^x$

$= (a^{-1})^x$.

Def: Se $a \cdot b \equiv 1 \ (p)$

Scrivo $\bar{a}^1$ invece di b

e scrivo $\bar{a}^m$ invece di b^m.

Esempio

$2 \cdot 9 \equiv 1 \ (17)$

Quindi scrivo $2^{-1} = 9$

$2^{-4} = 9^4$.

Dim. $1 \equiv (a \cdot \bar{a}^1)^x \equiv a^x \cdot \bar{a}^x \equiv 1 \cdot \bar{a}^x \equiv \bar{a}^x \ (p)$. $\square$

dic 1-14:58

Es $2^{67} \equiv \square \ (17)$

$\overset{?}{\equiv}$

So che se $x \equiv 0 \ (8)$
$2^x \equiv 1 \ (17)$.
So anche che se $x \not\equiv 0 \ (8)$
$2^x \not\equiv 1 \ (17)$?

Sì.

$67 = 8 \cdot 8 + 3$

$67 = \underset{3}{\underline{|8}}$
$\quad\ \ 8$

$2^{67} \equiv 2^{8\cdot 8+3} \equiv 2^{8\cdot 8} \cdot 2^3$

$\equiv (2^8)^8 \cdot 2^3 \equiv 1 \cdot 2^3 \equiv 2^3 \not\equiv 1 \ (17)$

perché 8 era la più piccola x tale che $2^x \equiv 1 \ (17)$.

$2^{67} \equiv 2^3 \equiv 8 \ (17)$.

Sapendo che $2^{k8} \equiv 1 \ (17)$

So calcolare 2^x $\forall x$.

(1) Se $x \equiv 0 \ (8) \Rightarrow 2^x \equiv 1 \ (17)$

(2) Se $x \not\equiv 0 \ (8)$

Scrivo $x = 8 \cdot q + r$, $0 \le r < 8$

$$2^x = 2^{8 \cdot q + r} = (2^8)^q \cdot 2^r \equiv (1)^q \cdot 2^r \equiv 2^r \ (17).$$

$\not\equiv 1$ a meno che $r = 0$ cioè $x \equiv 0 \ (8)$.

ATTENTI!

anche se $17 \equiv 0 \ (17)$

$2^{17} \not\equiv 2^0 \equiv 1 \ (17)$, ma $2^{17} \equiv 2^{16} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \ (17)$

dic 1-15:18

Esercizi Trovare $\forall x \in \mathbb{Z}$

$2^x \equiv 15 \quad (17)$.

Sol: Scrivo 15 come 2^{qualcosa} mod 17

$15 \equiv 2^5 \quad (17)$.

$2^x \equiv 15 \equiv 2^5 \quad (17)$.

2 è divisibile mod 17. Divido per 2^5. (Moltiplico per $(2^{-1})^5 \equiv 9^5$)

ottengo: $2^x \cdot 2^{-5} \equiv 2^5 \cdot 2^{-5} \quad (17)$

$2^{x-5} \equiv 1 \quad (17)$

$x-5 \equiv 0 \quad (8)$

$x \equiv 5 \quad (8)$.

sapere che

$2^y \equiv 1 \ (17) \iff y \equiv 0 \ (8)$

Soluzione: $2^x \equiv 15 \ (17) \iff x \equiv 5 \ (8)$ cioè $x = 5 + k8$

dic 1-15:20

Oss p primo $a \not\equiv 0 \ (p)$

il minimo x tale che

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

deve essere un divisore di $(p-1)$

(Fermat $\Rightarrow a^{p-1} \equiv 1 \ (p)$)

Dim $(p-1) \equiv x \cdot q + r$ (x: min. soluzione)

$$a^{p-1} \equiv a^{x \cdot q + r}$$

$$\equiv (a^x)^q \cdot a^r \equiv$$

$$\equiv 1 \cdot a^r$$

Fermat: $a^{p-1} \equiv 1 \ (p)$

$\| \quad a^r$

quindi $a^r \equiv 1 \ (p)$

ma $0 \leq r < x$

quindi $r = 0$. cioè $x \mid p-1$.

Esercizio Organizzo torneo di Calcio

5 Squadre. Tutti contro tutti. Squadre = {1,2,3,4,5}

Quante giornate servono?

1 giorno giocano: (1,5), (2,4), 3 riposa

2 giorno gioca: ?(2,5), (3,4), 1 riposa

i giorno giocano x contro y sse $x+y \equiv i \ (5)$

e inoltre $x \neq y$.

Dimostro che funziona. Dimostro che

in ogni giornata ci sono 4 squadre giocano e 1 riposa.

Nel giorno i chi riposa? Quella (X) che non è

congrua a nessuno di 1,2,3,4,5 mod(i) tranne eventualmente

se stessa.

x sicuramente è $\equiv$ a un elemento di {1,2,3,4,5}

OSS X riposa $\Leftrightarrow$

$X + X \equiv i \pmod 5$

$\Leftrightarrow 2X \equiv i \pmod 5$

Bisogna dimostrare che dati X ce ne è 1 sola tra $1,2,\dots,5$.

Inverso di 2 mod 5

$(2,5) = 1$ esiste inverso di 2.

$2 \cdot 3 \equiv 1 \pmod 5$

$2X \equiv i \pmod 5$

$\cdot 3$

$X \equiv 3i \pmod 5$.

ES nel giorno $i = 4$

riposa $3i \equiv 3 \cdot 4 \equiv 12 \equiv 2$

riposa $X = 2$.

ES non è vero che nessuno riposa 2 volte.

Con 6 squadre?

$2X \equiv i \pmod 6$

può avere più soluzioni

dic 1-15:42

$2 \cdot 6 \equiv 6 \pmod 6$

$2 \cdot 3 \equiv 6 \pmod 6$

2 soluzioni di $2 \cdot x \equiv 6 \pmod 6$
in $\{1,2,3,4,5,6\}$.

sia la 6 che la 3 riposano
nella giornata 6. Bisogna cambiare regola.
Il problema è che 6 è pari e non c'è l'inverso di 2.

dic 1-15:49

Torneo a 6 squadre
la faccio giocare in 5 giornate!
Come? Metto la 6 a parte.
organizzo il torneo a 5 squadre $\{1,2,3,4,5\}$
in 5 giornate. Come prima.
La 6 rientra in gioco, giocando ogni volta
con quella che riposava nel torneo a 5.