

# TEORIA DEI NUMERI = problemi che

Titolo nota

21/02/2006

parlano di numeri interi

**PROBLEMA 1** Trovare i valori interi di  $n$  per cui

$$\frac{2006}{n-5} \text{ risulta a sua volta intero.}$$

Idea:  $n-5$  deve essere un DIVISORE di 2006

$$\begin{aligned} 2006 &= 2 \cdot 1003 \\ &= 2 \cdot 17 \cdot 59 \end{aligned}$$

Quali sono i divisori di 2006?

$$\begin{array}{r} 17 \cdot \\ \underline{59} \\ 1003 \\ \underline{85} \\ 1603 \end{array}$$

1, 2, 17, 59,  $2 \cdot 17$ ,  $17 \cdot 59$ ,  $2 \cdot 59$ , 2006

Ci sono quindi  $\overset{1003}{8}$  DIVISORI

Per ogni divisore ho un valore buono di  $n$

$$1 \quad n-5 = 1 \quad \Rightarrow \quad n = 6$$

$$2 \quad n-5 = 2 \quad \Rightarrow \quad n = 7$$

$\vdots$

$$2 \cdot 17 = 34 \quad n-5 = 34 \quad \Rightarrow \quad n = 39$$

Quante solus. trovo?

8

SBAGLIATO!!!

Devo aggiungere tutte le solus. che provengono dai div. negativi

$$\text{Divisore} \quad -2 \quad \quad n-5 = -2 \quad \quad n = 3$$

————— 0 ————— 0 —————

PROBLEMA 2

Stessa cosa con  $\frac{n+1}{n-5}$

$$\frac{n+1}{n-5} = \frac{n-5+6}{n-5} = 1 + \frac{6}{n-5}$$

Mi sono ricondotto a  $n-5$  divisore di 6

$$n-5 = \pm 1, \pm 2, \pm 3, \pm 6$$

$$\frac{n^2+1}{n-5}$$

Divisione di polinomi

$$\begin{array}{r|l} n^2+1 & n-5 \\ -n^2+5n & \\ \hline 5n+1 & \\ -5n+25 & \\ \hline & 26 \end{array}$$

Mi dice  $n^2+1 = (n-5)(n+5) + 26$

$$\frac{n^2+1}{n-5} = \frac{(n-5)(n+5) + 26}{n-5} = n+5 + \frac{26}{n-5}$$

$$n-5 = \pm 1, \pm 2, \pm 13, \pm 26$$

In generale

$\frac{\text{polinomio in } n}{n-5}$  intero

Si fa la divisione e rimane

..... +  $\frac{\text{numero}}{n-5}$

↑  
Guardo questo.

Trovare le soluzioni intere di

$$(x+1)(y+1) = 2xy$$

$$xy + x + y + 1 = 2xy$$

$$y(x-1) = x+1$$

$$xy - x - y - 1 = 0$$

$$y = \frac{x+1}{x-1}$$

Cerco gli  $x$  interi per cui la fras. è intero.

## TEOREMA DI RUFFINI

Dato un polinomio  $p(x)$ , se  $p(\alpha) = 0$  (cioè  $\alpha$  è radice)  
allora posso dividere

$$p(x) = (x - \alpha) q(x)$$

Cosa importante: se  $p$  ha coeff. interi e  $\alpha$  è intero,  
allora  $q(x)$  ha coeff. interi

I pol. a coeff. interi sono molto RIGIDI

Problema  $p(x)$  a coeff. interi. Supp.  $p(2006) = 0$ .

Quanto può fare  $p(2004)$ ? Può essere

$p(2004) = 7$ ? Può essere  $p(2004) = 70$ ?

Ruffini  $\Rightarrow$  posso scrivere  $p(x) = (x-2006)q(x)$

Quindi  $p(2004) = (2004-2006) \cdot q(2004)$

$$= -2 \cdot q(2004)$$

$\Rightarrow p(2004)$  <sup>INTERO</sup> DEVE ESSERE PARI

Quindi 7 non può essere, 70 forse.

Per dimostrare che può essere 70, basta fare in modo che

$q(2004) = -35$  Ad esempio  $q(x) \equiv -35$  (costante)

$p(x) = (x-2006) \cdot (-35) \rightarrow$  vale 0 in 2006 e  
vale 70 in 2004

## Problema

$p(x)$  coeff. interi

$$p(6) = 0$$

$$p(2006) = 0$$

Può essere  $p(2004) = 70$ ?

## Ruffini

$$p(x) = (x - 2006) q(x) \quad \leftarrow \text{ho usato solo che}$$

$$p(2006) = 0$$

Metto  $x = 6$ .

$$0 = p(6) = (6 - 2006) q(6)$$

$$\Rightarrow q(6) = 0$$

Ancora Ruffini  $\Rightarrow$

$$q(x) = (x - 6) r(x)$$

$$p(x) = (x - 2006)(x - 6) r(x)$$

$$\begin{aligned} \text{Metto } x = 2004 \Rightarrow p(2004) &= (2004 - 2006) \cdot (2004 - 6) \cdot r(2004) \\ &= (-2) \cdot 1998 \cdot r(2004) \end{aligned}$$

$p(2004)$  è per forza un multiplo di 2.1998 quindi

70 non va bene

— 0 — 0 —

Problema

$p$  coeff. interi

$$p(1) = p(3) = 7$$

Quanto può fare  $p(4) = ?$

Considero il polinomio  $q(x) = p(x) - 7$

$$q(1) = p(1) - 7 = 0$$

$$q(3) = 0$$

Ruffini:

$$q(x) = (x-1)(x-3)r(x)$$

$$p(x) - 7 = (x-1)(x-3)r(x)$$

$$p(x) = 7 + (x-1)(x-3)r(x)$$

Metto  $x = 4 \Rightarrow p(4) = 7 + (4-1)(4-3)r(4)$

INTERO





$$p(4) = 7 + 3 \cdot \text{intero}$$

I valori possibili per  $p(4)$  sono quelli della forma

$$7 + 3 \cdot \text{intero} = 7 + 3k$$

70 va bene ?

$$7 + 3k = 70, \quad 3k = 63, \quad k = 21 \quad \text{OK}$$

80 . ?

$$7 + 3k = 80, \quad 3k = 73 \quad \text{NO} \quad 73 \text{ no div.}$$

# CONGRUENZE

0

2  
4  
6

↑  
2006  
P

1

3  
5  
7

D

0

3  
6

↑  
multipli  
di 3

1

4  
7

↑  
resto 1  
nella  
div. per 3

2006

2

5  
8

RESTI NELLA  
DIV. PER 3

↑  
resto 2  
nella div.  
per 3

Multiplo di 3

$$2006 = 2004 + 2$$

0

4

↑  
MULT  
4

1

5

2

6

↑  
Pari non  
multipli di 4, 2006

3

7

Dico che  $x \equiv 1 \pmod{4}$

$x$  congruo a 1  
modulo 4

Se  $x$ , diviso per 4, dà resto 1

$$x \equiv 2 \pmod{7}$$

$x$ , diviso per 7, dà resto 2

$$2006 \equiv 2 \pmod{4}$$

$$2006 \equiv 1 \pmod{5}$$

$$2006 \equiv 2 \pmod{3}$$

$$2006 \equiv 0 \pmod{2}$$

Pari / Dispari

$$P + P = P$$

$$P \cdot P = P$$

$$P + D = D$$

$$P \cdot D = P$$

$$D + D = P$$

$$D \cdot D = D$$

Queste regole valgono anche modulo 3, 4, 5, 6, ...

$$x \equiv 2 \pmod{3}$$

$$y \equiv 2 \pmod{3}$$

$$x + y \equiv 2 + 2 \equiv 4 \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$y \equiv 3 \pmod{5}$$

$$x + y \equiv 2 + 3 \equiv 5 \equiv 0 \pmod{5}$$

Prodotto: stessa cosa!

$$x \equiv 2 \pmod{5}$$

$$y \equiv 3 \pmod{5}$$

$$x \cdot y \equiv 2 \cdot 3 \equiv 6 \equiv 1 \pmod{5}$$

$$2006 \equiv 2 \pmod{3}$$

$$2006 \cdot 2006 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$$

$$2006^2$$

$$2006^3 \equiv 2006^2 \cdot 2006$$

$$\equiv 1 \cdot 2 \equiv 2 \pmod{3}$$

$$2006^4 \equiv 2006^3 \cdot 2006 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$$

$$2006^n \equiv \begin{cases} 2 \pmod{3} & n \text{ dispari} \\ 1 \pmod{3} & n \text{ pari} \end{cases}$$

In part.

$$2006^{2006} \equiv 1 \pmod{3}$$

### Criteri di congruenza

$$72568 \equiv \quad \quad \quad \pmod{3}$$

Somma cifre = 28 non multiplo di 3  $\Rightarrow$  numero non multiplo di 3.

$$1 \equiv 1 \pmod{3}$$

$$10 \equiv 1 \pmod{3}$$

$$100 \equiv 1 \pmod{3}$$

$$1000 \equiv 1 \pmod{3}$$

Tutte le potenze di  
10 sono  $\equiv 1 \pmod{3}$

$$72568 = \boxed{8} + \boxed{6} \cdot 10 + \boxed{5} \cdot 10^2 + \boxed{2} \cdot 10^3 + \boxed{7} \cdot 10^4$$

$$\equiv 8 + 6 \cdot 1 + 5 \cdot 1 + 2 \cdot 1 + 7 \cdot 1$$

$$\equiv 8 + 6 + 5 + 2 + 7 = 28 \equiv 1 \pmod{3}$$

Ogni numero è congruo (mod 3) alla somma delle sue cifre

Cong. Ogni numero è congruo (mod 9) alla somma delle cifre

$$1 \equiv 1 \pmod{9}$$

$$10 \equiv 1 \pmod{9}$$

$$10^2 \equiv 1 \pmod{9}$$

$$\vdots$$
$$10^k \equiv 1 \pmod{9}$$

$\Rightarrow$  stessa dim. di prima

Per 11: 7 5 6 9 4

$$4 - 9 + 6 - 5 + 7 = 17 - 14 = 3 \quad \text{non \u00e9 div. per 11}$$

$$75694 \equiv 3 \pmod{11}$$

$$1 \equiv 1 \pmod{11}$$

$$10 \equiv -1 \pmod{11}$$

$$10^2 \equiv (-1) \cdot (-1) \equiv 1 \pmod{11}$$

$$10^3 \equiv -1 \pmod{11}$$

⋮

$$10^k \equiv \begin{cases} 1 & k \text{ pari} \\ -1 & k \text{ dispari} \end{cases}$$

$$\begin{array}{cccccccc} & & & & & & & -1 \\ & & & & & & 9 & 10 \\ 0 & 1 & 2 & 3 & \dots & & & \\ 11 & 12 & 13 & & & & & \end{array}$$

$$4 \cdot 1 + 9 \cdot 10 + 6 \cdot 10^2 + 5 \cdot 10^3 + 7 \cdot 10^4 \equiv$$

$$4 + 9(-1) + 6 \cdot 1 + 5(-1) + 7 \cdot 1$$

Somma a segni alterni

$$95788 \equiv 3 \pmod{5}$$

basta vedere l'ultima  
cifra

$$957\boxed{88} \equiv 88 \pmod{4}$$

basta vedere le ultime 2  
cifre

$$95788 = 88 + 957 \cdot 100$$

$$\downarrow \quad \cdot \quad \downarrow$$

$$\equiv 88 + 957 \cdot 0$$

$$\equiv 88 \pmod{4}$$

$$100 \equiv 0 \pmod{4}$$



Trovare le soluzioni intere di

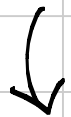
$$x^2 - y^2 = 2006200626 \quad \leftarrow \text{NO SOL.}$$

$$x^2 - y^2 = 2006200625 \quad \leftarrow \text{SI SOL.}$$

Come sono i quadrati modulo 4?

Se  $x$  è pari  $x^2$  è multiplo di 4  $\Rightarrow x^2 \equiv 0 \pmod{4}$

Se  $x$  è dispari  $x^2 \equiv 1 \pmod{4}$



$$x \equiv 1 \rightarrow x^2 = 1 \cdot 1 \equiv 1 \pmod{4}$$

$$x \equiv 3 \rightarrow x^2 = 3 \cdot 3 = 9 \equiv 1 \pmod{4}$$

$$x \text{ dispari} \Rightarrow x = 2k+1, \quad x^2 = 4k^2 + 4k + 1$$

I quadrati, modulo 4, possono essere solo  $\equiv 0$  o  $\equiv 1$

$$x^2 + y^2 \equiv \begin{cases} 0+0 & \equiv 0 \\ 0+1 & (1+0) \equiv 1 \\ 1+1 & \equiv 2 \end{cases}$$

$\Rightarrow$  La somma di quadrati non può essere  $\equiv 3 \pmod{4}$

$$x^2 + y^2 = 200675864 \boxed{27}$$

**ACHTUNG!**

$\uparrow$   
 $\equiv 3 \pmod{4}$

Non può essere

Se fosse stato  $\equiv 0, 1, 2$  poteva essere, ma non era detto.

$$x^2 - y^2 \equiv \dots \boxed{26} \equiv 2 \pmod{4} \text{ non può essere.}$$

$$x^2 - y^2 \equiv \begin{array}{l} \diagup \quad 0-0 \equiv 0 \\ \diagdown \quad 1-0 \equiv 1 \\ \diagup \quad 0-1 \equiv 3 \\ \diagdown \quad 1-1 \equiv 0 \\ \hline 0 \qquad \qquad 0 \end{array}$$

Non può essere  $\equiv 2 \pmod{4}$

$$x^2 + y^2 \equiv \dots \underbrace{030}_{\text{Mostro}} \leftarrow \text{Mod 4 è 2, che può essere somma di 2 quadrati (1+1)}$$

Mod 8

$x^2$  cosa può essere?

$x$  pari

$$x^2 \equiv \begin{array}{l} 0 \\ 4 \end{array} \pmod{8}$$

$x$  dispari

$$x^2 \equiv 1 \pmod{8}$$

$$x \equiv \begin{array}{l} / \\ / \\ / \\ / \end{array} \begin{array}{l} 1 \\ 3 \\ 5 \\ 7 \end{array}$$

Facciamo i quadrati e vediamo che viene sempre 1 (8)

$$\begin{aligned} (2k+1)^2 &= 4k^2 + 4k + 1 = 4(k^2 + k) + 1 \\ &= 4k(k+1) + 1 \end{aligned}$$

uno dei 2 fattori è pari  
multiplo di 8

$x^2 + y^2$  quando può essere  $\equiv 2 \pmod{4}$ . Solo se  $x$  e  $y$  sono dispari (1+1)

Modulo 8

$$\text{disp}^2 + \text{disp}^2 \equiv 1 + 1 \equiv 2 \pmod{8}$$

Può funzionare

solo se la somma  $e \equiv 2 \pmod{8}$

.....

$$030 \equiv 030 \equiv 6 \pmod{8}$$

IMPOSSIBILE

2000...06  
k zeri

può essere un  
quadrato perfetto?

$$\equiv 2 \pmod{4} \Rightarrow \text{NO}$$

500...06

stessa cosa!

600...0065

$$\equiv 1 \pmod{4} \text{ forse si può!!!}$$

Mod 3      ↓      è       $6+6+5 \equiv 5 \equiv 2 \pmod{3}$

Può un quadrato essere  $2 \pmod{3}$

$$x \equiv \begin{cases} 0 & \rightarrow x^2 \equiv 0 \\ 1 & \rightarrow x^2 \equiv 1 \\ 2 & \rightarrow x^2 \equiv 4 \equiv 1 \end{cases} \pmod{3} \Rightarrow 2 \text{ non può essere}$$

$$\text{dispari}^4 \equiv 1 \quad (16)$$

$$x^3 \equiv \begin{matrix} 0 \\ -1 \\ 1 \end{matrix} \quad (7)$$

$$x^3 \equiv \begin{matrix} 0 \\ -1 \\ 1 \end{matrix} \quad (9)$$