ALGEBRA & TEORIA DEI NUMERI

9/2/2018

Esempio 1.
Per quanti $n \in \mathbb{Z}$ si ha che $\frac{2017}{2n-3}$ è intera?

2017 è primo.

$2n-3 = \pm 1, \pm 2017$

$n = 1, 2, 1010, -1007$

Esempio 2. Stessa domanda per $\frac{2n+3}{n-1}$, $0, 2, -4, 6$ funzionano

$\frac{2n-2+5}{n-1} = 2 + \frac{5}{n-1}$. Ancora 4.

Notazione: $a \mid b$ se $\frac{b}{a}$ è intero "a divide b"

$a \mid b$, $a \mid c$ $\Rightarrow$ $a \mid b+c$: se $\frac{b}{a}$ intero e $\frac{c}{a}$ intero allora $\frac{b+c}{a}$ è intero

$a \mid xb+yc \Rightarrow \frac{xb+yc}{a} = x\frac{b}{a} + y\frac{c}{a}$

$a \mid b \Rightarrow a \mid bc$, $a \mid a$.

Esempio 3. $\frac{n^2+3n-5}{n-7}$. Tesi: $\underbrace{n-7}_{a} \mid \underbrace{n^2+3n-5}_{b}$

$n-7 \mid n-7$

$n-7 \mid n^2-7n$ (c)

$a \mid b$, $a \mid c$ $\Rightarrow a \mid b-c$

$n-7 \mid 10n-5$

$n-7 \mid 10n-70$

$n-7 \mid 65$

$$\begin{array}{r|l} m^2+3m-5 & m-7 \\ \hline m^2-7m & m+10 \\ \hline 10m-5 & \\ 10m-70 & \\ \hline 65 & \end{array}$$

Esercizio: Trovare tutte le coppie di interi x, y tali che

$$x^2-y^2=2011$$

$$(x+y)(x-y)=2011\cdot 1$$

$x=1006$ $\quad y=1005$ $\quad x=-1006$ $\quad y=1005$

$1006-1005$ $\quad -1006-1005$

$(x-\alpha) \mid P(x)$ se e solo se $P(\alpha)=0$

$$P(x)=(x-\alpha)Q(x)+P(\alpha)$$

$$x^2-3x+2=(x-2)Q(x)+P(2)$$

$4-6+2$ $\quad (x-1)$

$$x^4+3x^2+5x+1=(x-1)Q(x)+10$$

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

$$P(x)=a_n x^n+a_{n-1}x^{n-1}+\dots+a_1 x+a_0$$

$P(x)$ a coefficienti interi. Sia $P(2017)=0$. Quali valori può assumere $P(2015)$?

$2017-2015 \mid 0-P(2015) \Rightarrow 2 \mid P(2015)$

$P(x)=(x-2017)Q(x)$

$P(2015) = -2Q(2015)$

$P(x) = -2x + 4034$

— c — a —

Congruenze

$a \equiv b \pmod{m}$ "a congruo a b modulo m"

a-b è multiplo di m, $m \mid a-b$.

$143 \equiv 1733 \pmod{10}$

$3 \equiv 8 \pmod{5}$ $\quad 3 \not\equiv 8 \pmod{6}$

Operazioni

→ $a \equiv b \pmod{m} \Rightarrow a+c \equiv b+c \pmod{m}$

→ $c \equiv d \pmod{m} \Rightarrow a+c \equiv b+d \pmod{m}$

$$\frac{a+c-b-d}{m} = \frac{a-b}{m} + \frac{c-d}{m}$$

$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$ $\quad ac \equiv bd \pmod{m}$

NON POSSO DIVIDERE (o almeno non sempre)

$6 \equiv 21 \pmod{5}$

$4 \equiv 10 \pmod{6} \Longrightarrow$ ~~$2 \equiv 5 \pmod{6}$~~ $\quad 2 \equiv 7 \pmod{5}$

$$\frac{21-6}{5} = 3\,\frac{7-2}{5} \qquad \frac{10-4}{6} = 2\,\frac{5-2}{\not 3}$$

$$\frac{a-b}{m} = c\,\frac{a/c - b/c}{m}$$

Divisione solo per numeri coprimi con il modulo, altrimenti devo dividere anche il modulo.

Criteri di congruenza

mod 2: guardare l'ultima cifra se è pari o dispari.

mod 4: " le ultime 2 cifre

$72413 = 72400 + 13 \equiv 13$

mod 5: guardare l'ultima cifra

$72413 = 72410 + 3 \equiv 3 \pmod 5$

mod 3: somma delle cifre

mod 9: " " " $72413 \equiv 17 \equiv 8 \equiv -1 \pmod 9$

mod 11: $3 - 1 + 4 - 2 + 7 \equiv 0$ somma delle cifre a segni alterni

$172473 \equiv 3 - 1 + 4 - 2 + 7 - 1 \equiv 4$ partendo dalle unità

$\uparrow \times 1 - 7 + 2 - 4 + 7 - 3 \equiv -4$

$72413 \quad 7241 - 6 = 7235 \quad 723 - 10 = 713 \quad 71 - 6 = 65 \times 2$

313

33

5

Esercizio: Quando $x^2 - y^2 = k$ ha soluzione? (Per quali k)

Se k è dispari c'è sempre una soluzione.

$(n+1)^2 - (n-1)^2 = 4n \Rightarrow$ multipli di 4 ✓

x	x^2	y^2	k
0	0	0	0
1	1	1	3
2	0		1
$3 \equiv -1$	1		0

$\Rightarrow$ non posso avere $\equiv 2 \pmod 4$

$x^2 - y^2 \equiv k \pmod 4$

$0 - 0 \equiv 0$

$0 - 1 \equiv -1 \equiv 3$

$1 - 0 \equiv 1$

$1 - 1 \equiv 0$

Se $k \equiv 2 \bmod 4$ non posso avere soluzioni

— o — o —

mod 3		mod 4		mod 8		
x	x^2	x	x^2	x	x^2	
0	0	0	0	0	0	
1	1	1	1	1	1	
2	1	2	0	2	4	←
		3	1	3	1	
				4	0	
				$-3 \equiv 5$	1	
				$-2 \equiv 6$	4	←
				$-1 \equiv 7$	1	

— o — o —

Esercizio un po' più difficile

$3^a - 2^b = 1$ $\quad (1,1), (2,3)$

$3^0 - 2^b = 1 \Rightarrow \cancel{2^b = 0}$

1

$3^a - 2^0 = 1 \Rightarrow \cancel{3^a = 2}$

$a, b > 0$

→ 1
2
1
2
1
2

b dispari

mod 3: $-2^b \equiv 1 \bmod 3$

$2^b \equiv 2 \bmod 3$

$b = 2k+1$

$3^a = 2^{2k+1} + 1$ ← non funziona

mod 4: Se $b = 1 \Rightarrow 3^a = 2 + 1 \Rightarrow a = 1$ $\quad (1,1)$

Se $b > 1$: $3^a \equiv 1 \bmod 4 \Rightarrow (-1)^a \equiv 1 \bmod 4$

a pari

$a = 2k$

$3^{2k} - 2^b = 1 \Rightarrow 3^{2k} - 1 = 2^b$

$(3^k+1)(3^k-1) \Rightarrow k = 1 \Rightarrow a = 2$

$4 \quad 2$

$b = 3$

Quindi $(1,1)$ e $(2,3)$ sono le uniche soluzioni.

Esercizio 1. (IMO 1959, 1)

$\frac{21n+4}{14n+3}$ è irriducibile per ogni n

$a \mid 21n+4$
$a \mid 14n+3$
$\Rightarrow a \mid 7n+1 \Rightarrow a \mid 14n+2$

$a \mid 1 \rightarrow a = 1 \; (\neq -1)$

Esercizio 2.

Non ce ne sono. $\bmod 4$: $n^2 \equiv 0, 1$ $\quad 34 \equiv 2 \pmod 4$

Esercizio 3

$p(1) = p(3) = 7$. Possibili valori di $p(4)$?

$q(x) = p(x) - 7$. $\quad q(x) = (x-1)(x-3)Q(x)$

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

$p(4) = 3 \cdot XQ(4) + 7 \qquad p(4) = 3t + 7 = 35 + 1$

$p(4)$ può essere qualunque numero congruo a 1 mod 3

— o — o —

Esercizio 4.

$p(x) = (x-1)(x-2)(x-3)Q(x) + 1$. Se $p(n) = 4$:

$4 = (n-1)(n-2)(n-3)Q(n) + 1$

$3 = (n-1)(n-2)(n-3)Q(n)$ impossibile.

— o — o —

Esercizio 5.

$c = d = 0$

8 a b 3 1 7 6 1 8 8 6 4 9 5 5 1 8 1 9 4 0 1 2 8 0 0 0 0 0 0 0

$a + b + 4 \equiv 0 \mod 9$

8 a b 3 1 7 6 1 8 8 6 4 9 5 5 1 8 1 9 4 0 1 2 8

$8 - a + b - 1 + 7 - 6 + 1 - 6 + 4 - 9 + 1 - 8 + 1 - 3 + 0 - 1 + 2 - 8$

$-a + b - 2 \equiv 0 \mod 11$

$b - a \equiv 2 \mod 11 \qquad b = a + 2$

$2a + 6 \equiv 0 \mod 9$

$2a = 12 \Rightarrow a = 6 \quad b = 8$

— c — o —

Esercizio 6.

$7 \mid 3^{2m+1} + 2^{m+2}$

mod 7: $3 \cdot 3^{2m} + 4 \cdot 2^m \equiv 3 \cdot 9^m + 4 \cdot 2^m \equiv 3 \cdot 2^m + 4 \cdot 2^m \equiv 7 \cdot 2^m \equiv 0$.

Esercizio 7.

fabiomarconi94@hotmail.it

$2018!$ ha meno di $2018 \cdot 4$ cifre

$a_1 \leq 2018 \cdot 4 \cdot 9$ ha 5 cifre

$a_2 \leq 45$

$a_3 = 9 \Rightarrow a_{10} = 9$