ALGEBRA & TEORIA DEI NUMERI

1/2/2019

- Polinomi a coefficienti interi
- Congruenze

$a \mid b$ a divide b b/a è intero

$a^2 - b^2 = (a-b)(a+b)$

$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$

Se n è dispari

$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \dots + b^{n-1})$

$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

$a-b \mid a^n - b^n$ per ogni n

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

$\boxed{a-b \mid P(a) - P(b)}$

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

$= a_n (a^n - b^n) + a_{n-1} (a^{n-1} - b^{n-1}) + \dots + a_1 (a-b)$

$3 \mid 6 \quad 3 \mid 9 \Rightarrow 3 \mid 6+9$

Se $P(a) = 0$ allora $(x-a) \mid P(x)$

$x^2 - 3x + 2 \qquad x-1 \mid x^2-3x+2$

$(x-1)(x-2)$

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

$P(x) = (x-a)Q(x) + R = (x-a)Q(x) + P(a) = P(x)$

$a \mid b \quad a \mid c \implies a \mid xb + yc$

Esempio: Per quali n $\dfrac{n^2+3n-5}{n-7}$ è intero?

$$\begin{cases} n-7 \mid n^2+3n-5 \\ n-7 \mid n^2-7n \end{cases}$$

$n-7 \mid 10n-5$

$n-7 \mid 10n-70$

$n-7 \mid 65$

Es: $\dfrac{21n+4}{14n+3}$ è irriducibile per ogni n

$a \mid 21n+4$

$a \mid 14n+3$

$a \mid 7n+1 \leftarrow$

$a \mid 14n+2$ $\qquad a \mid 1.$

Congruenze

$a \equiv b \pmod n$ "a congruo a b modulo n"

se $n \mid b-a$ $\qquad 3 \equiv 14 \pmod{11}$

$3 \equiv 25 \pmod{11}$

$a \equiv b \pmod{m}$ $\quad a+c \equiv b+d \pmod{m}$ $\quad a \cdot c \equiv bd \pmod{m}$

$c \equiv d \pmod{m}$ $\quad a-c \equiv b-d \pmod{m}$

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

$2 \equiv 5 \pmod{3}$

$12 \equiv 42 \pmod{10}$

$4 \equiv 14 \pmod{10}$

Criteri di Congruenza

mod 2 guardare l'ultima cifra

mod 3 somma delle cifre $\quad 4571 \equiv 2 \pmod{3}$

$4571 \Rightarrow 17 \Rightarrow 8 \equiv 2 \pmod{3}$

mod 4 guardare le ultime 2 cifre $\quad 45 \cdot 100 + 71 \equiv 3 \pmod{4}$

mod 5 ultima cifra $\quad 4571 = 457 \cdot 10 + 1 \equiv 1 \pmod{5}$

mod 9 somma delle cifre

mod 11 somma delle cifre a segni alterni partendo dalle unità $\quad 4 - 5 + 7 - 1 = 5$

$1 - 7 + 5 - 4 = -5 \leftarrow$

$-5 \equiv -5 + 11 = 6 \pmod{11}$

$5^{240} \mod 3$ $\quad 3 \mid 5^{240} - 1$

$!!! \quad 2^{240} \equiv (-1)^{240} \equiv 1 \pmod{3}$

mod 3

$2^2 \equiv (-1)^2 \equiv 1$

$\boxed{\begin{matrix} 0 \\ 1 \end{matrix}}$

mod 4

x	x^2
0	0
1	1
2	0
3	1

$4k+2$

0
1

mod 8

x	x^2
0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

0
1
4

—— o —— o ——

Esercizi

1. $x^3 - 1 = p$ o $x^3 + 1 = p$

$(x-1)(x^2+x+1) = p$ $\quad x=2$ $\quad (7,8)$

$(1,2)$.

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

3

1

2. $n^{n+1} + 1$

$(n+1)(n^n - n^{n-1} + \dots + 1)$

$n^{n-1}(n-1) + n^{n-3}(n-1) + \dots$

3. $n^{23} + 23^n$ è multiplo di 4

$n^{23} + 23^n \equiv n^{23} + (-1)^n \pmod 4$

n dispari $n^{23} \equiv 1 \pmod 4$

$n \equiv 1 \pmod 4$

4. n dispari, allora $11 \mid 2^{3n+1} + 3^n + 5^{2n}$

$2^{3n+1} + 3^n + 5^{2n} \equiv 2 \cdot 8^n + 3^n + 3^n \pmod{11}$

$2\left((-3)^n + 3^n\right) \equiv 2\left(-3^n + 3^n\right) \equiv 0 \pmod{11}$

5. a = somma delle cifre di posto dispari

b = " " " " " pari

$a+b$ è multiplo di 9

$a-b$ è multiplo di 11

$|a-b| \geq 11$ 19, 8 10989

$a+b > 27$

10989 ~~10098~~

99999

6. $a+b$ $1a-6b$ $8a-13b$

$a-6b \equiv a-6b+7b \equiv a+b \pmod 7$

$8a-13b \equiv a+b \pmod 7$

$\frac{30 \cdot 31}{2} = 15 \cdot 31$

7. $2^x + 1 = 3^y$ (4)

$x = 0$ $\quad 1 + 1 = 3^y$

$x = 1$ $\quad 2 + 1 = 3^1$ ✓ $\quad (1,1)$

$(3,2)$

$x \geq 2$

$3^y \equiv 1 \pmod 4$ $\quad y$ é par $\quad y = 2k$

$2^x = 3^{2k} - 1 = (3^k + 1)(3^k - 1)$

4 $\quad$ 2 $\quad x = 3$

$k = 1 \Rightarrow y = 2$
