angela.veronese@sns.it

PORDENONE, 2 febbraio 2017

INSIEMI NUMERICI

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ $\quad +, \cdot$

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$ $\quad +, -, \cdot$ } TEORIA dei NUMERI

$\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z} \}$ $\quad +, -, \cdot, :$

$\mathbb{R} = \{0, 1, 2, \frac{1}{2}, \frac{3}{4}, \sqrt{2}, \pi, \sqrt{3}, \dots\}$] ALGEBRA

($\mathbb{C}$ numeri complessi $a + ib$, $a, b \in \mathbb{R}$, $i^2 = -1$)

NUMERI INTERI $\mathbb{Z}$

· Divisione con resto

$a, b \in \mathbb{Z}$, $b \neq 0$

Esistono $q, r \in \mathbb{Z}$ tali che $a = q \cdot b + r$, $0 \leq r < b$

Esempi: $a = 24$, $b = 5$ $\quad 24 = 5 \cdot 4 + 4$

$a = -24$ $\quad b = 5$ $\quad -24 = 5 \cdot (-5) + 1$

Se $r = 0$, $b \mid a$.

· Fattorizzazione in primi.

Esercizio: $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. Dimostriamo che $\sqrt{2}$ non si può scrivere come a/b, con $a, b \in \mathbb{Z}$.

Per assurdo, $\sqrt{2} = a/b$. Allora $b \cdot \sqrt{2} = a \Rightarrow 2b^2 = a^2$.

$a = 2^{c_1} \cdot d_1$, d_1 dispari $\qquad b = 2^{c_2} \cdot d_2$, d_2 dispari.

Sostituendo trovo: $2(2^{c_2} \cdot d_2)^2 = (2^{c_1} \cdot d_1)^2$

$$2^{2c_2+1} \cdot d_2^2 = 2 \cdot 2^{2c_2} \cdot d_2^2 = 2^{2c_1} \cdot d_1^2$$

$2c_2 + 1 = 2c_1$ ASSURDO.

Esercizio: Per quali $n \in \mathbb{Z}$, l'espressione $\frac{12}{n+4}$ è un numero intero?

Vuol dire che $n+4 \mid 12$. Quindi

$n+4 = 1, 2, 3, 4, 6, 12, -1, -2, -3, -4, -6, -12$. Ricavo n.

Esercizio: Quante sono le coppie (x,y) di interi tali che $x^2 - y^2 = 2017$?

$x^2 - y^2 = (x-y)(x+y) = 2017$ (2017 è primo)

Allora $x+y$ è un divisore di 2017.

$\begin{cases} x+y = 1 \\ x-y = 2017 \end{cases}$ $\begin{cases} x+y = 2017 \\ x-y = 1 \end{cases}$ $\begin{cases} x+y = -1 \\ x-y = -2017 \end{cases}$ $\begin{cases} x+y = -2017 \\ x-y = -1 \end{cases}$

Risolvo i sistemi e trovo le soluzioni.

Per casa: Dimostrare che $x^2 - y^2 = 2018$ non ha soluzioni (x,y) intere.

$*$ $a, b \rightarrow MCD(a,b) = (a,b)$

Come calcolo l'MCD?

1° MODO: uso la fattorizzazione

$(120, 396)$ $120 = 2^3 \cdot 3 \cdot 5$ $396 = 2^2 \cdot 3^2 \cdot 11$

$$MCD(120, 396) = 2^2 \cdot 3 = 12$$

2° MODO: sfruttare il fatto che: $c \mid a, \; c \mid b \Rightarrow c \mid a+b, \; c \mid a-b$
$c \mid a+nb$

$$(120, 396) = (120, 396-120) = (120, 276) = (120, 156) =$$
$$= (120, 36) = (120 - 36 \cdot 3, 36) = (12, 36) = 12.$$

Esercizio: Per quali valori di $n \in \mathbb{Z}$, $\dfrac{12n+6}{4n+5}$ è intero?

Vuol dire che $4n+5 \mid 12n+6$, cioè $(12n+6, 4n+5) = 4n+5$.

$$(12n+6, 4n+5) = (4n+5, 12n+6-(4n+5)) = (4n+5, 8n+1) =$$
$$= (4n+5, 8n+1-(4n+5)) = (4n+5, 4n-4) =$$
$$= (4n+5, -9) = 4n+5$$

significa che $4n+5 \mid 9 \rightarrow 4n+5 = 1, 3, 9, -1, -3, -9$
$n = -1, 1, -2.$

Esercizio: Dimostrare che $x^2 = 3y^2 + 1001$ non ha soluzioni (x,y) intere.

Riscrivo: $3y^2 = x^2 - 1001$ Devo essere $3 \mid x^2 - 1001$ $3 \mid 999$

Devo avere $3 \mid x^2 - 2$.

Dividiamo x per 3: $x = 3 \cdot q + r$ $r = 0, 1, 2$

$x^2 = \underline{9q^2 + 6qr} + r^2$ $3 \mid x^2 - 2 \Rightarrow 3 \mid r^2 - 2 = \begin{cases} -2 \\ -1 \\ 2 \end{cases}$ Nessuno è multiplo di 3!

$\Rightarrow$ L' equazione iniziale non ha soluzioni.

* ~~A~~ volte è comodo lavorare con i resti di una divisione...

CONGRUENZE

$$a \equiv b \pmod m \qquad m \in \mathbb{Z}^{\geq 2}$$

Diciamo che a e b sono congrui modulo m se ~~d~~ danno lo stesso resto nella divisione per m.

Esempi:
- $a \equiv 0 \pmod m$ significa $m \mid a$
- $36 \equiv 12 \pmod 8$
- $-3 \equiv 7 \pmod 5$

Le congruenze (mod m) si possono sommare, sottrarre e moltiplicare. (NON DIVIDERE)

$\rightarrow$ Esercizio di prima: $3y^2 = x^2 - 1001$

Se sono uguali, allora sono congrui modulo 3

$$0 \equiv x^2 - 2 \pmod 3$$
$$x^2 \equiv 2 \pmod 3$$

$$x \equiv 0, 1, 2 \pmod 3 \quad \Rightarrow \quad x^2 \equiv 0, 1, 1 \not\equiv 2 \pmod 3$$

Esercizio: Una sequenza di 100 cifre comprese tra 0 e 8 è multipla di 3 se letta in base 10, è multipla di 4 se letta in base 9 ed è multipla di 5 se letta in base 11. Quanto vale, al massimo, la somma delle cifre?

* NOTA: criteri di divisibilità

CRITERIO DIVISIBILITÀ PER 3

$3 \mid a$ se e solo se $3 \mid$ ~~l~~ somma delle cifre

Perché? $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$

$$3 \mid a \iff a \equiv 0 \pmod 3 \iff a_k \cdot \underbrace{10^k}_{1 \bmod 3} + \dots + a_1 \cdot \underbrace{10}_{=1 \bmod 3} + a_0 \equiv 0 \pmod 3$$

$$\iff a_k + \dots + a_1 + a_0 \equiv 0 \pmod 3$$

POLINOMI

Un polinomio è: $p(x) = \underbrace{a_n}_{\text{coefficiente direttivo}} x^{\overset{= \text{grado di } p(x)}{n}} + a_{n-1}x^{n-1} + \dots + a_1 x + \underbrace{a_0}_{\text{termine noto}}$, $a_n \neq 0$

$a_n, a_{n-1}, \dots, a_0 \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$

Se $a_n = 1$, diciamo che $p(x)$ è monico.

* VALUTAZIONE

- $p(0) = a_0$
- $p(1) = a_n + a_{n-1} + \dots + a_0$

* DIVISIONE (con resto)

$a(x)$, $b(x) \neq 0$ polinomi

Esistono unici $q(x)$, $r(x)$ tali che

$$a(x) = q(x) \cdot b(x) + r(x) \qquad \text{grado}(r(x)) < \text{grado}(b(x))$$

Esercizio: $p(x)$ a coefficienti interi. Sappiamo che $p(2) = -1$, $p(3) = 5$.
Quali sono i possibili valori per $p(4)$?

Divido $p(x)$ per $(x-2)(x-3)$:

$$p(x) = (x-2)(x-3)\,q(x) + r(x) \qquad \text{grado}(r) < 2$$

$r(x) = ax + b$

Calcoliamo: $p(2) = -1 = \cancel{(2-2)(2-3)q(2)} + r(2) = 2a+b$
$p(3) = 5 = \cancel{(3-2)(3-3)q(3)} + r(3) = 3a+b$

$$\begin{cases} 2a+b = -1 \\ 3a+b = 5 \end{cases} \qquad a = 6 \qquad b = -13$$

$$p(x) = (x-2)(x-3)\,q(x) + 6x - 13$$

$$p(4) = (4-2)(4-3)\,q(4) + 11 = 2 \cdot \underbrace{q(4)}_{\text{può assumere qualsiasi valore } \in \mathbb{Z}} + 11$$

$\Rightarrow$ I valori possibili per $p(4)$ sono tutti gli interi della forma $2n + 11$.

* α, $p(x)$ tali che $p(\alpha) = 0$. Diciamo che α è RADICE di $p(x)$.

Se $p(x)$ ha radice α, divido per $(x - \alpha)$

$p(x) = q(x)(x-\alpha) + r$ $\quad r$ costante

$p(\alpha) = 0 = r \quad \Rightarrow \quad p(x) = q(x)(x-\alpha)$

grado $(p) = n \qquad$ grado $(q) = n-1$

Questo ci dice che se grado$(p) = n$, e $p \neq 0$, allora $p(x)$ ha $\leq n$ radici.

- Se $p(x)$ ha grado $\leq n$ e si annulla in $n+1$ punti distinti, allora $p = 0$.
- Se $p(x)$ e $q(x)$ hanno grado $\leq n$ e coincidono in $n+1$ punti distinti, allora $p(x) = q(x)$.

Infatti $r(x) = p(x) - q(x)$ ha grado $\leq n$ e $n+1$ radici distinte.

Esercizio: $p(x)$ è monico di grado 6. $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 4$, $p(5) = 5$, $p(6) = 6$.
Calcolare $p(7)$. $\quad$ ($p(7) \neq 7$).

* RELAZIONI RADICI COEFFICIENTI

Esempi:

1) $p(x) = x^2 + ax + b \qquad x_1, x_2$ radici

$$p(x) = (x-x_1)(x-x_2) = x^2 - (x_1+x_2)x + x_1x_2$$

$$x_1 + x_2 = -a \quad , \quad x_1x_2 = b$$

2) $p(x) = x^3 + ax^2 + bx + c \qquad x_1, x_2, x_3$

$$\stackrel{!}{=} (x-x_1)(x-x_2)(x-x_3)$$
$$= x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - x_1x_2x_3$$

$$x_1 + x_2 + x_3 = -a$$
$$x_1x_2 + x_2x_3 + x_3x_1 = b$$
$$x_1x_2x_3 = -c$$

Esercizio: $x^2 + 5x - 7$, α, β radici. Quanto fa $\alpha^2 + \beta^2$?

$\alpha + \beta = -5$, $\quad \alpha\beta = -7$

$$(\alpha+\beta)^2 = 25 = \alpha^2 + \beta^2 + 2\alpha\beta = \alpha^2 + \beta^2 - 14$$

Ricavo: $\alpha^2 + \beta^2 = 25 + 14 = 39$.

* Trovo un polinomio che abbia α^2 e β^2 come radici.

$$(x-\alpha^2)\cdot(x-\beta^2) = x^2 - \alpha^2 x - \beta^2 x + \alpha^2\beta^2$$
$$= x^2 - (\alpha^2+\beta^2)x + (\alpha\beta)^2 = x^2 - 39x + 49.$$