


(utili x esercizi, non approfondite o dimostrate)



GENERALI

anello

$$a+b = b+a \quad \text{comm. +}$$

$$(a+b)c = a+(b+c) \quad \text{ass. +}$$

$$a+0_A = 0_A+a = a \quad \text{el. neutro +}$$

$$a+(-a) = 0_A \quad \text{opposto}$$

$$a \cdot b = b \cdot a \quad \text{comm.} \quad \text{anello commutativo}$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{ass.}$$

$$a \cdot 1_A = 1_A \cdot a = a \quad \text{el. neutro} \quad \text{anello unitario}$$

$$a(b+c) = a \cdot b + a \cdot c \quad \text{distr.}$$

N. PRIMO

$$a \in A \setminus A^\times, a \neq 0$$

$$\forall b, c \in A, a|bc \Rightarrow a|b \vee a|c$$

CAMPO

A anello comm. un.

$$\text{t.c. } \forall a \in A \setminus \{0\}$$

$$a \in A^\times$$

$$\text{noto: } \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \text{ campo}$$

$$(e, \text{ in } \mathbb{F}_p, ([a] + [b])^p = [a]^p + [b]^p)$$

Cancellazione in un anello A

$$\text{Se } a \text{ non divisore di } 0_A, ab=ac \Rightarrow b=c$$

$$(\text{in } \mathbb{Z}, \text{ se } a \neq 0)$$

$$\text{INVERTIBILI } ab=ba=1_A$$

$$\text{prop. inversi: } (ab)^{-1} = a^{-1}b^{-1}$$

EL. IRREDUCIBILE

$$a \in A \setminus A^\times \quad \forall b, c \in A,$$

$$a=bc \Rightarrow b \cdot c \in A^\times$$

$$\text{primo} \Leftrightarrow \text{irriducibile}$$

DOMINIO

A anello $\neq \{0\}$ in cui

l'unico divisore di zero è 0_A

MONDO DELLA DIVISIBILITÀ

$$(\text{div. euclidea}) \quad a, n \in \mathbb{Z}, n \neq 0 \quad \exists! q \in \mathbb{Z}, r \in \{0, \dots, |n|-1\} \\ \text{t.c. } a = qn + r \quad \text{utile! } r < n$$

$$\text{è una rel. di c.: } a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$$

DIVISIBILITÀ E CONGRUENZA MOD N

$$a|b \Leftrightarrow b = a \cdot c$$

b resto a/b

$$a \equiv_n b \Leftrightarrow n | a-b$$

$$\text{è una rel. di equivalenza} \rightarrow \text{utile!} \quad a \equiv_n b \Leftrightarrow b \equiv_n a \quad \text{simm.} \\ (n | a-b \Leftrightarrow n | b-a)$$

$$\text{nota: } a \equiv_n a', b \equiv_n b' \Rightarrow a+b \equiv_n a'+b' \\ ab \equiv_n a'b'$$

utili!!

$$1. \text{ Gauss: se } \text{MCD}(a, b) = 1$$

$$\text{allora } a|bc \Rightarrow a|c$$

$$(a, b \in \mathbb{Z}^*, c \in \mathbb{Z})$$

$$\text{lemma: se } \text{MCD}(a, b, c) = 1$$

$$\text{e } a, b | c \text{ allora } abc | c$$

TEOREMA FONDAMENTALE ARITMETICA

$$\forall a \in \mathbb{Z}^*, \quad ① \text{ l'insieme } I_a = \{p \text{ primo: } p|a\} \text{ è finito}$$

$$② a = \pm 1 \cdot \prod_p p^{v_p(a)} \quad \text{ogni numero è una combinazione di primi elevati a qualcosa)} \\ \text{uniche } \in \mathbb{N}$$

$$a \cdot b = \prod_p p^{v_p(a) + v_p(b)} = p^{v_p(a)} \cdot p^{v_p(b)} = p^{v_p(a) + v_p(b)}$$

FERMAT

$$n^p \equiv_p n \quad (p \text{ primo})$$

$$\text{quindi } n^{p-1} \equiv 1$$

$$\text{conseguenza: } [n]_p^{-1} = [n]_p^{p-2}$$

MCD

$$\delta = \text{MCD}(a, b) \quad \text{se}$$

$$① \delta | a, \delta | b$$

$$② \text{ dato } d' \in \mathbb{N} \text{ t.c. } d'|a \text{ e } d'|b \\ \text{allora } d' | \delta$$

$$\bullet \delta \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

$$\text{id Bézout } \delta = u \cdot a + v \cdot b \quad \exists u, v \in \mathbb{Z}$$

$$\text{Fibo e MCD: } \text{MCD}(F_m, F_{m+1}) = 1$$

conseguenze

$$a|b \Leftrightarrow \forall p, v_p(a) \leq v_p(b)$$

$$\text{MCD}(a, b) = \prod_p p^{\min(v_p(a), v_p(b))}$$