Lezione 6

Prerequisiti: L'insieme dei numeri interi. Lezione 5.

Divisibilità e divisori.
Teorema di divisione euclidea.
Algoritmo delle divisioni successive.

Questa è la prima lezione dedicata all'anello dei numeri interi, del quale studieremo, in particolare, le proprietà legate alla nozione di divisibilità. Per la maggior parte queste sono note dall'aritmetica scolastica, ma qui vengono presentate all'interno di un quadro teorico e formale, nel quale esse vengono dedotte dagli assiomi dei numeri interi, oppure da proprietà valide in ogni anello commutativo (unitario). Presentiamo prima queste ultime.

Definizione 6.1 Sia A un anello commutativo, e siano $a,b \in A$. Si dice che b *divide* a (oppure che b è un *divisore* di a, oppure che a è *divisibile* per b, o che a è *multiplo* di b) se esiste $q \in A$ tale che $a = bq$. In tal caso si scrive $b \mid a$.

Esempio 6.2 (a) I divisori di 6 in $\mathbb{Z}$ sono 1, –1, 2, –2, 3, –3, 6, –6. Invece 4 non è un divisore di 6.
(b) In un anello commutativo A, lo zero divide solo se stesso: ciò è conseguenza della Proposizione 5.2 (a). In virtù della stessa proposizione, ogni elemento dell'anello divide 0.
(c) In un anello commutativo unitario, i divisori di 1 sono gli elementi invertibili. Ogni elemento invertibile divide ogni elemento dell'anello. Ogni elemento è divisore di se stesso.

Osservazione 6.3 La divisibilità definisce, su un anello commutativo A, una relazione transitiva. Infatti, per ogni $a,b,c \in A$, se $a \mid b$ e $b \mid c$, allora esistono $q,q' \in A$ tali che $b = aq, c = bq'$, e quindi $c = (aq)q' = a(qq')$, dove abbiamo applicato l'associatività del prodotto. Segue che $a \mid c$.
Se l'anello A è anche unitario, allora la relazione di divisibilità è anche riflessiva, e quindi è una relazione di *preordine*. In generale, non è una relazione d'ordine, in quanto se $1 \neq -1$ non vale la proprietà antisimmetrica: infatti si ha sempre $1 \mid -1$ e $-1 \mid 1$.

Definizione 6.4 Sia A un anello commutativo, e siano $a,b \in A$. Allora a e b si dicono *associati* se a divide b e b divide a.

Esempio 6.5 In un anello commutativo unitario A, per ogni $a \in A$, e per ogni elemento invertibile $u \in A$, a ed au sono associati. Infatti è evidente che a divide au, e, d'altra parte, $a = a1 = a(uu^{-1}) = (au)u^{-1}$, per cui au divide a. In un dominio d'integrità vale anche il viceversa.

Proposizione 6.6 *(Elementi associati in un dominio di integrità*). Sia A un dominio di integrità, siano $a,b \in A$. Allora a e b sono associati se e solo se esiste un elemento invertibile $u \in A$ tale che $b = au$ (ossia, a e b *differiscono per un fattore invertibile*).

Dimostrazione: Alla luce dell'Esempio 6.5, basta dimostrare il "solo se". Siano, dunque, a e b associati. Allora esistono $q,q' \in A$ tali che $a = bq, b = aq'$, da cui $b = (bq)q' = b(qq')$. Se b è zero, allora, in virtù della prima uguaglianza e della Proposizione 5.2 (a), anche a è zero, e dunque la tesi

è verificata per $u = 1$. Altrimenti b è un elemento regolare, e quindi cancellabile in base alla Proposizione 5.21. Allora, essendo $b1 = b(qq')$, segue che $1 = qq'$. Ciò dimostra che q' è invertibile. □

Esempio 6.7 Per ogni $a \in \mathbb{Z}$ non nullo, gli elementi associati ad *a* sono esattamente due: *a* e *–a*. Poiché 0 divide solo se stesso, in particolare è associato solo a se stesso.

La dimostrazione del prossimo enunciato è lasciata al lettore.

Corollario 6.8* In un anello commutativo unitario, due elementi sono associati se e solo se hanno gli stessi divisori e gli stessi multipli.

Proposizione 6.9 *(Proprietà della divisibilità rispetto alla somma ed al prodotto)* Sia *A* un anello commutativo. Allora, per ogni $a, b, c \in A$,

(a) se *a* divide *b* e *c*, allora *a* divide $b + c$ e $b - c$;
(b) se *a* divide *b* e $b + c$, allora *a* divide *c*;
(c) se *a* divide *b*, allora *a* divide *bc*.

Dimostrazione: (a) Se *a* divide *b* e *c*, allora esistono $q, q' \in A$ tali che $b = aq, c = aq'$, per cui, in virtù della proprietà distributiva, si ha $b + c = aq + aq' = a(q + q')$. Ciò prova che *a* divide $b + c$. Poiché, inoltre, $b - c = aq - aq' = a(q - q')$, si ha anche che *a* divide $b - c$.
(b) Basta applicare la parte (a) dell'enunciato, osservando che $c = (b + c) - b$.
(c) Se $b = aq$, con $q \in A$, allora $bc = (aq)c = a(qc)$, e quindi *a* divide *bc*.

Dedichiamo il resto della lezione ai numeri interi.

Diamo, anzitutto, un fondamentale teorema.

Teorema 6.10 *(Teorema di divisione euclidea)* Siano $a, b \in \mathbb{Z}$, ove $b \neq 0$. Allora esistono, e sono univocamente determinati, $q, r \in \mathbb{Z}$ tali che

(i) $a = bq + r$;
(ii) $0 \leq r < |b|$.

I numeri *q* ed *r* si dicono, rispettivamente, *quoziente* e *resto* della *divisione (euclidea)* di *a* per *b*. I numeri *a* e *b* si dicono, rispettivamente, *dividendo* e *divisore*.

Dimostrazione: Supponiamo dapprima che $b > 0$. Consideriamo l'insieme

$$X = \{a - bx \geq 0 \mid x \in \mathbb{Z}\}.$$

Questo insieme è non vuoto. Infatti, se $a \geq 0$, allora $0 \leq a = a - b0 \in X$. Altrimenti, essendo $b \geq 1$, si ha $0 \leq (1 - b)a = a - ba \in X$. Inoltre *X* è un sottoinsieme di $\mathbb{N}$. Quindi, per il principio del minimo (assioma di buon ordinamento), *X* possiede un minimo *r*. Allora, per qualche $q \in \mathbb{Z}$, $r = a - bq \geq 0$. Valgono dunque la (i) e la prima disuguaglianza della (ii). Resta da verificare che $r < |b|$, ossia $r < b$. Supponiamo per assurdo che $r \geq b$. Allora $0 \leq r - b = a - b(q + 1)$. Quindi $r - b \in X$, pur essendo $r - b < r = \min X$. Ciò fornisce la contraddizione cercata. Supponiamo ora che sia $b < 0$. Allora $-b > 0$ e quindi esistono, come abbiamo appena dimostrato, $q, r \in \mathbb{Z}$ tali che si abbia

$a = -bq + r$ (ossia $a = b(-q) + r$) e $0 \le r < |-b| = |b|$. Ciò conclude la dimostrazione dell'esistenza di $q, r \in \mathbb{Z}$ verificanti la (i) e la (ii).
Proviamo ora l'unicità. Siano $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tali che $q = q_i, r = r_i$ con $i = 1, 2,$ verificano la (i) e la (ii). Allora, in particolare,

$$bq_1 + r_1 = bq_2 + r_2, \tag{1}$$

da cui $b(q_1 - q_2) = r_2 - r_1,$ e, pertanto, supponendo che sia $r_2 \ge r_1,$

$$|b||q_1 - q_2| = |b(q_1 - q_2)| = r_2 - r_1 \le r_2 < |b|.$$

Ma allora $0 \le |q_1 - q_2| < 1,$ e quindi, essendo $q_1 - q_2$ intero, segue che $|q_1 - q_2| = 0,$ cioè $q_1 = q_2$. Dalla (1) segue allora che $r_1 = r_2$. Ciò prova l'unicità del quoziente e del resto. □

Osservazione 6.11 Nelle ipotesi del Teorema 6.10, *b* divide *a* se e solo se il resto della divisione di *a* per *b* è zero.

Esempio 6.12 Eseguiamo la divisione euclidea dei numeri 16 e –16 per i numeri 5 e –5, secondo tutte le possibili combinazioni.

$$16 = 5 \cdot 3 + 1$$
$$16 = (-5) \cdot (-3) + 1$$
$$-16 = 5 \cdot (-4) + 4$$
$$-16 = (-5) \cdot 4 + 4$$

Per ottenere il quoziente della prima abbiamo calcolato $\left[\frac{16}{5}\right] = 3$, ove le parentesi indicano la parte intera. La seconda è stata ottenuta, semplicemente, cambiando il segno al quoziente della prima. La terza è stata ottenuta cambiando il segno al resto e al quoziente della prima, e poi sottraendo un'unità al quoziente: $-16 = 5 \cdot (-3) - 1 = 5 \cdot (-4) + 5 - 1$. Infine, la quarta è stata ottenuta dalla terza cambiando il segno al quoziente.

Veniamo ora alla definizione di un concetto, tanto noto quanto importante, dell'aritmetica dei numeri interi.

Definizione 6.13 Siano $a, b \in \mathbb{Z}$. Allora si dice *massimo comune divisore* di *a* e *b* ogni numero intero *d* tale che

(a) $d \mid a$ e $d \mid b$;

(b) per ogni $e \in \mathbb{Z}$ tale che $e \mid a$ ed $e \mid b,$ si ha che $e \mid d$.

Da questa definizione segue immediatamente il

Corollario 6.14 Siano $a, b \in \mathbb{Z}$. Allora *b* divide *a* se e solo se *b* è massimo comune divisore di *a* e *b*. In particolare, se $a = 0,$ un massimo comune divisore di *a* e *b* è *b*.

Proposizione 6.15 *(Lemma di Bézout)* Siano $a, b \in \mathbb{Z}.$ Allora esiste un massimo comune divisore *d* di *a* e *b*. Inoltre esistono $s, t \in \mathbb{Z}$ tali che

$$sa + tb = d. \tag{2}$$

Tale uguaglianza si dice *identità di Bézout*, I numeri *s,t* si dicono *coefficienti di Bézout* di *a* e *b*.

Dimostrazione: Se $a = 0,$ allora *b* è un massimo comune divisore di *a* e *b*, e si può prendere $s = 0, t = 1.$ Supponiamo allora che *a* non sia nullo. Sia

$$X = \{ax + by > 0 \mid x, y \in \mathbb{Z}\}.$$

Allora X è un sottoinsieme di $\mathbb{N}$. Inoltre non è l'insieme vuoto. Infatti, se $a > 0$, allora $a1 + b0 = a \in X,$ e se $a < 0$, allora $a(-1) + b0 = -a \in X.$ Per il principio del minimo, l'insieme X ammette un minimo *m*. Siano $s, t \in \mathbb{Z}$ tali che $as + bt = m.$ Proviamo che *m* è un massimo comune divisore di *a* e *b*. Per provare che *m* divide *a* e *b*, utilizziamo il teorema di divisione euclidea. Siano *q* ed *r* il quoziente ed il resto della divisione di *a* per *m*. Allora $r < m$ e

$$r = a - mq = a - (as + bt)q = a(1 - sq) + b(-tq).$$

Se fosse $r > 0,$ allora si avrebbe $r \in X$, e quindi $m \le r,$ il che costituisce una contraddizione. Quindi $r = 0$, il che prova che *m* divide *a*. Analogamente si prova che *m* divide *b*.
Supponiamo ora che $e \in \mathbb{Z}$ sia tale che $e \mid a$ ed $e \mid b.$ Allora, in base alla Proposizione 6.9 (c), *e* divide *as* e *bt* e quindi, per la Proposizione 6.9 (a), *e* divide $as + bt = m.$ Ciò prova che *m* soddisfa le condizioni della Definizione 6.13, ed è dunque un massimo comune divisore di *a* e *b*. □

Proposizione 6.16 Siano $a, b \in \mathbb{Z}$ e sia *d* un massimo comune divisore di *a* e *b*. Allora i massimi comuni divisori di a e *b* sono *d* e $-d$.

Dimostrazione: È chiaro che, se *d* verifica le condizioni (a) e (b) della Definizione 6.13, lo stesso vale per $-d$: ciò segue infatti dal Corollario 6.8. Quindi $-d$ è un massimo comune divisore di *a* e *b*. Viceversa, sia δ un massimo comune divisore di *a* e *b*. Allora, poiché δ verifica la condizione (a), è un divisore comune di *a* e *b;* pertanto, siccome *d* verifica la (b), si ha che $\delta \mid d$. Scambiando i ruoli di δ e *d* si deduce che $d \mid \delta.$ Dunque δ e *d* sono numeri interi associati. Se sono distinti, segue, alla luce dell'Esempio 6.7, che $\delta = -d$. □

Chiaramente, ogni massimo comune divisore di due interi non entrambi nulli è non nullo (vedi l'Esempio 6.2 (b)). Si ha allora il seguente

Corollario 6.17 Due numeri interi non entrambi nulli hanno esattamente due massimi comuni divisori, che sono uno l'opposto dell'altro.

Nota Indicheremo con $\mathrm{MCD}(a, b)$ il massimo comune divisore positivo di due numeri interi *a* e *b* non entrambi nulli.

Mostriamo ora un procedimento per ottenere un massimo comune divisore di due interi non nulli assegnati, detto *algoritmo delle divisioni successive.*

Siano $a, b \in \mathbb{Z}$, entrambi non nulli. Si comincia effettuando la divisione con resto di *a* per *b*:

1) $a = bq_1 + r_1$ $\qquad (0 \le r_1 < |b|)$

Se $r_1 \neq 0,$ si prosegue effettuando la divisione con resto di b per r_1:

2) $b = r_1 q_2 + r_2$ $\qquad (0 \le r_2 < r_1)$

Se $r_2 \neq 0,$ si prosegue effettuando la divisione con resto di r_1 per r_2.

3) $r_1 = r_2 q_3 + r_3$. $\qquad (0 \le r_3 < r_2)$

Fintanto che non si trova un resto nullo, si va avanti, ricorsivamente, effettuando ogni volta la divisione del penultimo resto per l'ultimo resto trovato. In questo modo, il passo *i*-esimo fornisce l'uguaglianza:

i.) $r_{i-2} = r_{i-1} q_i + r_i$ $\qquad (0 \le r_i < r_{i-1})$

In base a quanto osservato a margine delle uguaglianze 1.), 2.), 3.), …*i*.), (e che deriva dalla condizione (ii) del Teorema 6.10), si conclude che la sequenza dei resti è *strettamente decrescente*:

$$r_1 > r_2 > r_3 > \cdots > r_i > \cdots$$

Poiché questi numeri sono tutti maggiori o uguali a zero, necessariamente, prima o poi, si deve pervenire allo zero, si deve trovare, cioè, un resto $r_n = 0$. Quindi il nostro procedimento si conclude con le seguenti due uguaglianze:

n–1.) $r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$ $\qquad (0 \le r_{n-1} < r_{n-2})$

n.) $r_{n-2} = r_{n-1} q_n$

Si prova allora che r_{n-1} è un massimo comune divisore di a e b; infatti vale la seguente

Proposizione 6.18 Un massimo comune divisore di due numeri interi non nulli (che non siano uno divisore dell'altro) è l'ultimo resto non nullo che compare nel relativo algoritmo delle divisioni successive.

Dimostrazione: Proviamo che, con le notazioni introdotte sopra, il resto r_{n-1} verifica le condizioni (a) e (b) della Definizione 6.13.
Dall'uguaglianza *n*.) segue che $r_{n-1} \mid r_{n-2}$. Allora, in base alla Proposizione 6.9 (a) e (c), r_{n-1} divide entrambi gli addendi a secondo membro della *n*–1.). Dalla Proposizione 6.9 (a) segue dunque che r_{n-1} divide l'intero secondo membro, cioè $r_{n-1} \mid r_{n-3}$. Procedendo in questo modo, risalendo la sequenza dei passi dell'algoritmo, si giunge a concludere che $r_{n-1} \mid r_3$, $r_{n-1} \mid r_2$; allora dalla 3.) si deduce che $r_{n-1} \mid r_1$ e, quindi, dalla 2.), si ricava che $r_{n-1} \mid b$, e dalla 1.), infine che $r_{n-1} \mid a$. Ciò prova che r_{n-1} verifica la condizione (a) della Definizione 6.13.
Sia ora e un divisore comune di a e b. Allora, per la Proposizione 6.9 (c), $e \mid bq_1$; d'altra parte, poiché $e \mid a,$ in virtù della Proposizione 6.9 (b), dalla 1.) segue che $e \mid r_1$. Analogamente, dalla 2.) si deduce che $e \mid r_2,$ e quindi, dalla 3.) segue che $e \mid r_3$. Procedendo in questo modo, discendendo i

passi dell'algoritmo, si giunge a concludere, in base alla n–1.), che $e \mid r_{n-1}$. Con ciò è provato che r_{n-1} verifica anche la condizione (b) della Definizione 6.13, il che conclude la dimostrazione. □

Esempio 6.19 Determiniamo un massimo comune divisore di $a = 255$ e b = 87 con l'algoritmo delle divisioni successive.

1.) $255 = 87 \cdot 2 + 81$
2.) $87 = 81 \cdot 1 + 6$
3.) $81 = 6 \cdot 13 + 3$
4.) $6 = 3 \cdot 2$

Segue che 3 è un massimo comune divisore di 255 e 87. In base alla Proposizione 6.16, l'altro massimo comune divisore è –3. Si ha $\mathrm{MCD}(255,87) = 3$.
Rappresentiamo ora 3 nella forma 255s + 87t, per opportuni numeri interi s e t. Dalla 3.) si ricava

$$3 = 81 - 13 \cdot 6 . \tag{3}$$

Lo scopo sarà raggiunto se riusciremo a rappresentare 81 e 6 in funzione di 255 e 87. A tal fine possiamo utilizzare la 2.)

$$6 = 87 - 81, \tag{4}$$

e la 1.)

$$81 = 255 - 87 \cdot 2 \tag{5}$$

Sostituendo ora la (5) nella (4) si ottiene

$$6 = 87 - (255 - 87 \cdot 2),$$

cioè

$$6 = 87 \cdot 3 - 255 . \tag{6}$$

Sostituendo la (6) e la (5) nella (3)

$$3 = 255 - 87 \cdot 2 - 13 \cdot (87 \cdot 3 - 255) ,$$

ossia

$$3 = 255 \cdot 14 + 87 \cdot (-41) .$$

Questa è una rappresentazione del tipo cercato (s = 14, t = –41).

Definizione 6.20 Due numeri interi si dicono *coprimi* (o *relativamente primi*) se gli unici loro divisori comuni sono 1 e −1.

Corollario 6.21 Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Allora a e b sono coprimi se e solo se $\mathrm{MCD}(a,b) = 1$.

Dimostrazione: Il "solo se" è banale conseguenza della Definizione 6.20. Per il "se" basta osservare che, se 1 è un massimo comune divisore di due interi, allora ogni divisore comune di questi interi divide 1, ed è quindi uguale ad 1 o a –1. □

La coprimalità di due interi si può caratterizzare tramite il Lemma di Bézout.

Proposizione 6.22 *(Corollario al Lemma di Bézout*). Siano $a,b \in \mathbb{Z}$. Allora *a* e *b* sono coprimi se e solo se esistono $s,t \in \mathbb{Z}$ tali che

$$sa + tb = 1. \tag{3}$$

Dimostrazione: Il "solo se" è il Lemma di Bézout per $d = 1$. Proviamo il "se". Detto *d* un comune divisore di *a* e *b*, si ha che *d* divide *a* e *b*, e quindi, se esistono $s,t \in \mathbb{Z}$ verificanti la (3), *d* divide 1. Quindi $d \in \{1,-1\}$. □

Esempio 6.23 Si ha $\text{MCD}(15,17) = 1$, e, in effetti, $15 \cdot 8 - 17 \cdot 7 = 120 - 119 = 1$.

Proposizione 6.24 Siano $a,b,c \in \mathbb{Z}$. Se $a \mid bc$, e *a* e *b* sono coprimi, allora $a \mid c$.

Dimostrazione: In virtù della Proposizione 6.22, esistono $s,t \in \mathbb{Z}$ tali che $sa + tb = 1$. Segue che

$$c = 1 \cdot c = (sa + tb)c = sac + tbc,$$

ma, per ipotesi, *a* divide questa somma, e quindi $a \mid c$. □

Dal Lemma di Bézout e dalla Proposizione 6.22 segue facilmente:

Corollario 6.25 Se *a* e *b* sono numeri interi non entrambi nulli, e $d = \text{MCD}(a,b)$, allora i numeri $\frac{a}{d}$ e $\frac{b}{d}$ sono coprimi.

Osservazione 6.26 In base al Corollario 6.25, è quindi possibile, data una frazione $\frac{a}{b}$, in cui *a* e *b* sono interi, e *b* non è nullo, trovare una frazione equivalente nella quale il numeratore ed il denominatore sono coprimi (una cosiddetta *frazione ridotta ai minimi termini*): basta sostituire *a* e *b*, rispettivamente, con $\frac{a}{d}$ e $\frac{b}{d}$.

Invertendo le relazioni di divisibilità nella definizione di massimo comune divisore si ottiene la seguente:

Definizione 6.27 Siano $a,b \in \mathbb{Z}$. Allora si dice *minimo comune multiplo* di *a* e *b* ogni numero intero *h* tale che

(a) $a \mid h$ e $b \mid h$;

(b) per ogni $k \in \mathbb{Z}$ tale che $a \mid k$ ed $b \mid k$, si ha che $h \mid k$.

Esercizio 6.28* Provare che, se $a,b \in \mathbb{Z}$ sono interi non entrambi nulli, allora $\frac{ab}{\text{MCD}(a,b)}$ è un minimo comune multiplo di *a* e *b*.

Esercizio 6.29* Provare l'enunciato analogo alla Proposizione 6.16 per i minimi comuni multipli.

Nota Una volta stabilito che, per ogni coppia di interi *a, b* entrambi non nulli, esistono esattamente due minimi comuni multipli, che sono uno l'opposto dell'altro, indicheremo con $\mathrm{mcm}(a,b)$ quello positivo.

Le definizioni di massimo comune divisore e di minimo comune multiplo si estendono, in maniera ovvia, al caso in cui al posto di *a* e *b* abbiamo *r* numeri interi $a_1,...,a_r$.

Esercizio 6.30* Sia *b* un intero maggiore di 1. Provare che, per ogni intero positivo *n*, esistono e sono univocamente determinati un numero naturale *N* ed interi $a_0,...,a_N$, tali che

(i) $0 \le a_i \le b-1$ per ogni *i*,

(ii) $a_N \neq 0$,

(iii) $n = \sum_{i=0}^{N} a_i b^i$.

La $(N+1)$-upla $a_N...a_0$ si dice *rappresentazione di n in base b.*