MCD in $\mathbb{N}$ e Polinomi

Giovanna Carnovale

October 18, 2011

1 Divisibilità e massimo comun divisore

1.1 Divisibilità in $\mathbb{N}$

In questa sezione introdurremo il concetto di divisibilità e di massimo comun divisore di due numeri naturali non nulli. Daremo inoltre due algoritmi per calcolare il massimo comun divisore.

Definizione 1.1 *Dati $a, b \in \mathbb{N}$ diremo che a divide b (in formule, $a|b$) se esiste $k \in \mathbb{N}$ tale che $ak = b$.*

Ad esempio, $4|12$ perché esiste 3 tale che $4 \cdot 3 = 12$.
La relazione $|$ è sicuramente riflessiva perché $a = a \cdot 1$ quindi $a|a$.

Esercizio 1.2 *Dimostrare che la relazione data da $|$ è una relazione transitiva su $\mathbb{N} \setminus \{0\}$ e su $\mathbb{N}$.*

Soluzione: Dobbiamo dimostrare che se $a|b$ e $b|c$ allora $a|c$. Se $a|b$ e $b|c$ allora esistono l, k in $\mathbb{N}$ per i quali $al = b$ e $bk = c$. Allora $a(lk) = (al)k = bk = c$ quindi $a|c$. □

Esercizio 1.3 *Dimostrare che la relazione $|$ è una relazione antisimmetrica su $\mathbb{N} \setminus \{0\}$ e su $\mathbb{N}$.*

Soluzione: Nel primo caso dobbiamo dimostrare che se, per $a \neq 0$, $b \neq 0$ si hanno $a|b$ e $b|a$ allora $a = b$. Se $a|b$ e $b|a$ allora esistono l, k in $\mathbb{N}$ per i quali $al = b$ e $bk = a$. Vogliamo allora dimostrare che $l = 1$ e $k = 1$. Dalle uguaglianze ottenute per a e b si ottiene: $a(lk) = (al)k = bk = a$. Quindi $a(lk) - a = 0$ ovvero $a(lk) - a(1) = a(lk - 1) = 0$. Allora, poiché $a \neq 0$, si ha $lk = 1$, ovvero $l = k = 1$. Pertanto $b = al = a \cdot 1 = a$.

Nel secondo caso, se a e b sono diversi da 0 procediamo come sopra. Se $a = 0$ ed $a|b$ allora esiste $l \in \mathbb{N}$ tale che $0 = al = b$ quindi anche $b = 0$. □

Gli esercizi 1.2 e 1.3 mostrano che $|$ è un ordinamento parziale su $\mathbb{N}$ e su $\mathbb{N} \setminus \{0\}$.

Definizione 1.4 *Un elemento $p \in \mathbb{N}$ è detto un numero primo se soddisfa le seguenti proprietà:*

- $p \neq 0, 1$
- *se $x \in \mathbb{N}$ è tale che $x|p$ allora $x = 1$ oppure $x = p$.*

Si hanno i seguenti risultati:

1. Ogni elemento non nullo di n di $\mathbb{N}$ si può scrivere come prodotto di (potenze di) numeri primi $n = p_1^{e_1} \cdots p_k^{e_k}$. Tale scrittura è unica a meno dell'ordine in cui compaiono i fattori (Teorema fondamentale dell'aritmetica o teorema della fattorizzazione unica).
2. I numeri primi sono infiniti.

Dati m, $n \in \mathbb{N}$, con fattorizzazione

$$m = p_1^{e_1} \cdots p_k^{e_k}, \quad n = q_1^{f_1} \cdots q_s^{f_s}$$

si deduce che $m|n$ se e solo se

- $\{p_1, \ldots, p_k\} \subseteq \{q_1, \ldots, q_s\}$ e
- $f_j \geq e_i$ se $q_j = p_i$.

Vale a dire: $m|n$ se e solo se

- tutti i divisori primi di m sono anche divisori di n e
- se p compare nella fattorizzazione di m con esponente e, allora p compare nella fattorizzazione di n con esponente $f \geq e$.

1.2 Massimo comun divisore

Definizione 1.5 *Dati a, $b \in \mathbb{N}$ non entrambi nulli, l'elemento $d \in \mathbb{N}$ è detto un* massimo comun divisore *di a e b se*

1. *$d|a$ e $d|b$;*
2. *se $z|a$ e $z|b$ per qualche $z \in \mathbb{N}$, allora $z|d$.*

Ad esempio 12 è massimo comun divisore di 252 e 60. Infatti, 12 divide sia 60 che 252, i divisori di $60 = 2^3 \cdot 3 \cdot 5$ sono i numeri della forma $2^a \cdot 3^b \cdot 5^c$ con $a \leq 3$, $b \leq 1$ e $c \leq 1$, i divisori di $252 = 2^2 \cdot 3^2 \cdot 7$ sono i numeri della forma $2^s \cdot 3^t \cdot 7^r$ con $s \leq 2$, $t \leq 2$ ed $r \leq 1$. Quindi gli elementi che dividono sia 60 che 252 sono tutti e soli i numeri della forma $2^x 3^y$ con $x \leq 2$ e $y \leq 1$. Tali numeri sono tutti divisori di $12 = 2^2 \cdot 3$.

Esercizio 1.6 *Dimostrare che dati qualsiasi a, $b \in \mathbb{N}$ non nulli, il loro massimo comun divisore è unico.*

Soluzione: Se avessi d_1 e d_2 massimi comuni divisori, allora avrei $d_1|d_2$ (utilizzo la prima proprietà del massimo comun divisore applicata a d_1 e la seconda aaplicata a d_2) e $d_2|d_1$ (utilizzo la prima proprietà del massimo comun divisore applicata a d_2 e la seconda applicata a d_1). Pertanto $d_1 = d_2$. □
Denoteremo il massimo comun divisore dei due numeri a e b con il simbolo $MCD(a, b)$.

Ispirati dall'esempio appena visto, osserviamo che, $MCD(m, n)$ è il prodotto delle potenze di tutti i primi p che compaiono sia nella scomposizione di m che nella scomposizione di n, con esponente il minimo tra l'esponente di p nella scomposizione di m e l'esponente di p nella scomposizione di n.

Esercizio 1.7 *Calcolare il massimo comun divisore di* 144 *e* 9 *e dimostrare che è un massimo comun divisore.*

Esercizio 1.8 *Calcolare il massimo comun divisore di* 84 *e* 15 *e dimostrare che è un massimo comun divisore.*

Esercizio 1.9 *Siano dati* $a, b \in \mathbb{N}$ *con* $a|b$. *Dimostrare che* $MCD(a, b) = a$.

1.3 Divisione con il resto

Abbiamo introdotto il concetto di divisibilità: ora vorremmo vedere cosa si può fare quando due numeri naturali non sono uno divisore dell'altro.

Proposizione 1.10 *Dati* $a \neq 0$ *e* b *in* $\mathbb{N}$, *esitono sempre* $q, r \in \mathbb{N}$ *tali che* $0 \leq r < a$ *e* $b = aq + r$.

Dimostrazione: Se $b < a$ allora $b = 0a + b$ quindi possiamo prendere $q = 0$ ed $r = b < a$.
Sia ora $a \leq b$. Consideriamo l'insieme

$$S = \{n \in \mathbb{N} \mid n = b - ak \text{ per qualche } k \in \mathbb{N}\},$$

(Attenzione: non tutti i numeri di questa forma sono in $\mathbb{N}$, noi consideriamo *solo* i numeri nonnegativi di questa forma). Poiché $b \geq a$, $b - 1 \cdot a = b - a \in S$, che quindi non è vuoto. Per il buon ordinamento di $\mathbb{N}$, l'insieme S ammette quindi un elemento minimo m che si potrà scrivere come $m = b - ak$ per un certo k. Se prendiamo $q = k$ e $m = r$, per dimostrare l'enunciato è sufficiente mostrare che $m < a$. Se per assurdo avessimo $m \geq a$, allora $0 \leq m - a < m$ con $m - a \in S$ perché $m - a = b - a(q + 1)$. Ciò è impossibile perché m è l'elemento minimo di S. L'assurdo deriva dall'aver supposto che $m \geq a$, pertanto l'enunciato è dimostrato. □

I numeri q ed r sono detti *quoziente* e *resto* della divisione.

Esercizio 1.11 *Calcolare quoziente e resto della divisione di* b *per* a *quando:*

1. $b = 17$, $a = 3$;
2. $b = 45$, $a = 3$;
3. $b = 0$, $a = 123$.

1.4 L'algoritmo di Euclide

Abbiamo già visto un algoritmo per calcolare il massimo comun divisore di due numeri naturali, tramite fattorizzazione dei due numeri dati. L'algoritmo di scomposizione di un numero nei suoi fattori primi è però piuttosto lungo. Introdurremo ora un nuovo algoritmo, molto meno complesso, per calcolare il massimo comun divisore di due numeri naturali, basato sulla divisione con il resto ed il principio di buon ordinamento. Tale algoritmo prende il nome di *Algoritmo di Euclide*.

Dati due numeri $a \leq b$, interi positivi, se $a = b$ allora $MCD(a, b) = MCD(a, a) = a$.
Se invece $a \neq b$ allora $a < b$ ed esistono q_1, $r_1 \in \mathbb{N}$ con $0 \leq r_1 < a$ tali che

$$b = aq_1 + r_1.$$

Se $r_1 = 0$, allora $a|b$ e $MCD(a, b) = a$.
Se $r_1 \neq 0$, allora esistono q_2, $r_2 \in \mathbb{N}$ con $0 \leq r_2 < r_1$ tali che

$$a = q_2 r_1 + r_2$$

(divisione di a per r_1).
Se $r_2 = 0$ allora r_1 è il MCD di a e b. Infatti, $r_1|a$ perché $r_1 q_2 = a$ e $b = (q_2 r_1)q_1 + r_1 = r_1(q_2 q_1 + 1)$, cioè $r_1|b$. Sia $z \in \mathbb{N}$ con $zm = a$ e $zn = b$ un divisore comune di a e di b. Allora

$$zn = b = (zm)q_1 + r_1, \text{ quindi } r_1 = (n - mq_1)z$$

cioè $z|r_1$. Quindi $MCD(a, b) = r_1$ e ci si ferma.
Se invece $r_2 \neq 0$, allora esistono q_3, $r_3 \in \mathbb{N}$, con $0 \leq r_3 < r_2$ per i quali

$$r_1 = q_3 r_2 + r_3$$

(divisione di r_1 per r_2).
Se $r_3 = 0$ allora, come sopra si dimostra che $r_2 = MCD(a, b)$.
Se invece $r_3 \neq 0$, iteriamo il procedimento dividendo r_2 per r_3, e cosi via. Il procedimento ha termine per il principio del buon ordinamento perché $a > r_1 > r_2 > \cdots$. L'ultimo resto non nullo ottenuto per divisioni successive è il massimo comun divisore di a e b.

Esempio 1.12 *Calcolare mediante l'algoritmo di Euclide il massimo comun divisore di* 74 *e* 14.
Abbiamo

$$74 = 14 \cdot 5 + 4$$

quindi $q_1 = 14$ *e* $r_1 = 4 \neq 0$.

$$14 = 4 \cdot 3 + 2$$

quindi $q_2 = 3$ *e* $r_2 = 2 \neq 0$.

$$4 = 2 \cdot 2 + 0$$

quindi $q_3 = 2$ *e* $r_3 = 0$. *L'ultimo resto non nullo, cioè* 2 *è* $MCD(74, 14)$.

Esercizio 1.13 *Calcolare, utilizzando l'algoritmo di Euclide, il MCD delle coppie di numeri degli esercizi della sezione precedente.*

2 Polinomi

Sia S l'insieme $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oppure $\mathbb{C}$.
Un polinomio a coefficienti in S nell'indeterminata X è un'espressione della forma

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

con $a_i \in S$ (gli a_i sono detti i *coefficienti di* $p(X)$). Il polinomio nullo è il polinomio che ha tutti i coefficienti nulli e lo denoteremo con 0. Il grado di un polinomio non nullo $p(X)$ è il massimo numero n per il quale $a_n \neq 0$ (cioè l'esponente della potenza più alta di X che compare con coefficiente non nullo) e sarà denotato con $\deg(p(X))$. Un polinomio di grado zero è anche detto polinomio costante. Denoteremo con il simbolo 1 il polinomio costante con $a_0 = 1$.

Denoteremo con $S[X]$ l'insieme dei polinomi a coefficienti nell'insieme S. In $S[X]$ possiamo introdurre operazioni di somma e prodotto: dati

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{j=0}^{n} a_j X^j$$

$$q(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 = \sum_{j=0}^{m} b_j X^j$$

avremo

$$p + q = \sum_{j=0}^{\max\{m,\, n\}} (a_j + b_j) X^j$$

$$pq = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) X^j$$

(qui se $k > m$, $b_k = 0$ ed analogamente per a_j). Tali operazioni godono delle seguenti proprietà:

1. $p + q = q + p$ per ogni p, $q \in S[X]$ (proprietà commutativa della somma);
2. $(p + q) + r = p + (q + r)$ per ogni p, q, $r \in S[X]$ (proprietà associativa della somma);
3. $0 + p = p$ per ogni $p \in S[X]$ (esistenza dell'elemento neutro per la somma);
4. dato $p \in S[X]$ esiste $q = -p \in S[X]$ tale che $q + p = 0$ (esistenza dell'elemento opposto);
5. $(pq)r = p(qr)$ per ogni p, q, $r \in S[X]$ (proprietà associativa del prodotto);

6. $p(q+r) = pq + pr$ per ogni p, q, $r \in S[X]$ (proprietà distributiva);
7. $pq = qp$ per ogni p, $q \in S[X]$ (proprietà commutativa del prodotto);
8. $1a = a$ per ogni $p \in S[X]$ (esistenza dell'elemento neutro per il prodotto);
9. $\deg(p+q) = \max(\deg p, \deg q)$ per ogni p, $q \in S[X]$ p, $q \neq 0$;
10. $\deg(pq) = \deg(p) + \deg(q)$ per ogni p, $q \in S[X]$, p, $q \neq 0$;
11. Dati p, $q \in S[X]$, se $pq = 0$ allora $p = 0$ e/o $q = 0$ ($S[X]$ è privo di divisori dello 0);
12. $p(X)q(X) = 1$ se e solo se $p(X) = p_0$, $q(X) = q_0$ hanno grado 0 e $p_0 q_0 = 1$ in S.

Le proprietà 1.2.3.4.5.6 ci dicono che $S[X]$ è un *anello*, unite alla 8. ci dicono che $S[X]$ è un *anello unitario*, e unite alla 7. ci dicono che $S[X]$ è un *anello commutativo unitario*.

Anche in $S[X]$ è possibile effettuare la divisione con il resto:

Proposizione 2.1 *Dati f, $g \in S[X]$ con $S = \mathbb{C}, \mathbb{R}, \mathbb{Q}$ e $g \neq 0$ esistono sempre due polinomi q, r con $r = 0$ oppure $\deg r < \deg g$ per i quali $f = gq + r$.*

Esempio 2.2 *Calcolare quoziente e resto dei due polinomi $f = 3X^3 - 2X^2 + X + 4$ e $g = X^2 - 1$ in $\mathbb{Q}[X]$.*

Soluzione: Costruiamo, termine per termine il polinomio q, a partire dal grado più alto:

$$\begin{array}{l|l} 3X^3 - 2X^2 + X + 4 & X^2 - 1 \\ \hline & 3X + \cdots \end{array}$$

Abbiamo posto $3X$ perché $\tilde{f} = f - (3X)g = f - 3X^3 + 3X$ ha grado minore o uguale a 2, e quindi abbiamo "diminuito" il grado di f.

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X + \cdots \end{array}$$

Qui abbiamo scritto sotto f, il polinomio $(3X)g$ incolonnato in modo da avere termini dello stesso grado nella stessa colonna. Ora *sottraiamo* alla riga corrispondente ad f la riga corrispondente a $(3X)g$:

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X - 2 \\ & -2X^2 & +4X & +4 & \end{array}$$

e ripetiamo l'operazione. Abbiamo aggiunto un -2 perché $\tilde{f} - (-2)g$ ha grado minore o uguale ad 1. Scriviamo ora sotto la riga del polinomio $\tilde{f} = f - (3X)g$ il polinomio $(-2)g$.

$$\begin{array}{llll|l} 3X^3 & -2X^2+ & X+ & 4 & X^2 - 1 \\ \hline 3X^3 & & -3X & & 3X - 2 \\ & -2X^2 & +4X & +4 & \\ & -2X^2 & & +2 & \end{array}$$

e sottraiamo alla riga del polinomio $\tilde{f}$ il polinomio $(-2)g$ ottenendo $f-(3X-2)g$:

$$\begin{array}{cccc|c} 3X^3 & -2X^2+ & X+ & 4 & X^2-1 \\ \hline 3X^3 & & -3X & & 3X-2 \\ & -2X^2 & +4X & +4 & \\ & -2X^2 & & +2 & \\ & & 4X & +2 & \end{array}$$

Ora $q = 3X - 2$ ed $r = 4X + 2$.

Diremo che il polinomio g divide il polinomio f se il resto della divisione di f per g è 0. In tal caso diremo anche che g è un *fattore* di f.

Esercizio 2.3 *Calcolare quoziente e resto della divisione di f per g con*

1. $f = 6X^5 - 12X^3 + X-$, $g = 2X^3 - 3$ *in* $\mathbb{Q}[X]$;
2. $f = 6X^5 - 12X^3 + X-$, $g = 2X + 1$ *in* $\mathbb{Q}[X]$;
3. $f = X^3 - \sqrt{2}X + 1$, $g = X - \sqrt{3}$ *in* $\mathbb{R}[X]$;
4. $f = X^2 - iX + 2$, $g = \sqrt{3}X - 2i$ *in* $\mathbb{C}[X]$.

Ad un elemento $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in S[X]$ possiamo associare la *funzione polinomiale*

$$\begin{array}{rccc} \psi_f\colon & S & \longrightarrow & S \\ & z & \mapsto & a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \end{array}$$

Se $f = g \in S[X]$, allora la funzione ψ_f è uguale alla funzione ψ_g, vale a dire, per ogni $z \in S$, $\psi_f(z) = \psi_g(z)$. Se $f \in S[X]$ è un polinomio costante a_0, allora ψ_f è la funzione costante che associa a tutti i valori di S il valore a_0. Infine, per ogni coppia $f, g \in S[X]$ e per ogni $z \in S$ si ha: $\psi_{f+g}(z) = \psi_f(z) + \psi_g(z)$; $\psi_{fg}(z) = (\psi_f(z))(\psi_g(z))$.
Una *radice* di $f = a_0 + a_1X + \cdots + a_nX^n \in S[X]$ è un elemento $z \in S$ per il quale $\psi_f(z) = 0$. Sfruttando la divisione con il resto otteniamo il seguente risultato, noto come Teorema di Ruffini:

Teorema 2.4 *Sia $f \in S[X]$ non nullo e sia $z \in S$. Allora z è una radice di S se e soltanto se $(X - z)$ è un fattore di f.*

Dimostrazione: La divisione con il resto di f per $(X - z)$ dà

$$f = q(X - z) + r$$

con $r = 0$ oppure $\deg r < \deg(X - z) = 1$, cioè $r = r_0$ è un polinomio costante oppure è 0.
Se z è una radice di f, allora la funzione $\psi_f = \psi_{q(X-z)+r_0} = \psi_q\psi_{(X-z)} + \psi_{r_0}$ si annulla in z, ovvero $\psi_q(z)(z - z) + r_0 = r_0 = 0$, quindi il resto della divisione di f per $(X - z)$ è nullo ed $(X - z)$ divide f.

Se $(X - z)$ divide f allora $f = (X - z)q$, quindi $\psi_f = \psi_{(X-z)q} = \psi_{(X-z)}\psi_q$. Calcolando il valore di questa funzione in z vediamo che z è una radice di f. $\square$

Il teorema di Ruffini ci aiuta nella ricerca delle radici di polinomi di grado superiore al secondo, se ne conosciamo almeno una radice, come nel seguente esempio:

Esempio 2.5 *Calcolare le radici reali del polinomio:* $f = X^3 - 3X^2 - 13X + 15$.

Soluzione: Poiché la somma dei coefficienti di questo polinomio è zero, 1 è una radice di f. Per il teorema di Ruffini $f = (X - 1)q$ per qualche polinomio $q \in \mathbb{R}[X]$. L'algoritmo di divisione ci fornisce $f = (X - 1)(X^2 - 2X - 15)$. Con la formula di risoluzione delle equazioni di secondo grado troviamo altre due radici: -3 e 5.

Esercizio 2.6 *Trovare le radici reali dei polinomi:* $f = X^3 - 6X^2 - 9X + 14$ *e* $g = X^3 - 10X^2 - 23X - 12$.

Come conseguenza del Teorema di Ruffini e della formula del grado di un prodotto di polinomi abbiamo il seguente corollario:

Corollario 2.7 *Ogni polinomio di grado n ha al più n radici.*

In particolare, una conseguenza del Teorema di Ruffini e del Teorema fondamentale dell'algebra (ogni polinomio non costante di $\mathbb{C}[X]$ ha una radice in $\mathbb{C}$) è il seguente Teorema:

Teorema 2.8 *Ogni elemento f di $\mathbb{C}[X]$ ammette una fattorizzazione del tipo $f = c_0(X - c_1)\cdots(X - c_n)$ dove i $c_j \in \mathbb{C}$ per $j > 0$ sono tutti e soli gli zeri di f.*