Algoritmo euclideo, massimo comun divisore ed equazioni diofantee

Se a e b sono numeri interi, si dice che a divide b, in simboli: $a \mid b$, se e solo se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Si può subito notare che:

- 1 e -1 sono gli unici interi che dividano ogni intero;
- 0 è l'unico intero che sia diviso da ogni intero.
- $\forall\, a, b \in \mathbb{Z}\ \big(a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b\big)$

L'insieme dei divisori (in $\mathbb{Z}$) di un intero n si indica come $\mathrm{D}(n)$. Dunque, per ogni $n \in \mathbb{Z}$,

$$\mathrm{D}(n) := \{a \in \mathbb{Z} : a \mid n\},$$

ad esempio, $\mathrm{D}(6) = \{1, -1, 2, -2, 3, -3, 6, -6\}$.

Un *massimo comun divisore* tra a e b è poi un intero d per il quale valgano le due condizioni:

$$\begin{aligned} &\text{i.)} \quad d \mid a \ \wedge\ d \mid b; \qquad \text{e} \\ &\text{ii.)} \quad \forall\, c \in \mathbb{Z}\big((c \mid a \ \wedge\ c \mid b) \Rightarrow c \mid d\big); \end{aligned}$$

ovvero, in modo equivalente:

$$\begin{aligned} &\text{i.)} \quad d \in \mathrm{D}(a) \cap \mathrm{D}(b); \qquad \text{e} \\ &\text{ii.)} \quad \forall\, c \in \mathrm{D}(a) \cap \mathrm{D}(b),\ \ c \mid d. \end{aligned}$$

Dunque, un massimo comun divisore tra a e b è un divisore comune ad a e b che sia diviso da ogni altro divisore comune ad a e b.

Alcune osservazioni immediate sulla nozione di massimo comun divisore sono le seguenti:

- Se d è un massimo comun divisore tra a e b allora d e $-d$ sono gli unici massimi comun divisori tra a e b,

dunque: calcolare un massimo comun divisore tra due interi equivale a calcolarli tutti;

- per ogni $a, b \in \mathbb{Z}$, i divisori comuni ad a e b sono tutti e soli i divisori comuni ad $|a|$ e $|b|$; quindi i massimi comun divisori tra a e b sono tutti e soli i massimi comun divisori tra $|a|$ e $|b|$.

Quest'ultima osservazione mostra che nel calcolare massimi comun divisori tra numeri interi è sempre possibile ridursi a calcolare massimi comun divisori tra interi non negativi. Ad esempio, i massimi comun divisori tra -7811 e 8456985 sono precisamente i massimi comun divisori tra 7811 e 8456985, così come quelli tra -7811 e -8456985 o quelli tra 7811 e -8456985. Inoltre, il calcolo dei massimi comun divisori tra 0 ed un arbitrario intero è immediato, come segue da queste altre due osservazioni:

- se a e b sono interi e $a \mid b$, allora a è un massimo comun divisore tra a e b;
- in particolare, per ogni $a \in \mathbb{Z}$, si ha che a è un massimo comun divisore tra a e 0.

Pertanto:

> *Il problema di calcolare un massimo comun divisore tra numeri interi si riduce sempre al problema di calcolare un massimo comun divisore tra numeri interi positivi.*

Sino a questo momento non si è ancora stabilito se questo problema abbia sempre soluzione, cioè se, assegnati comunque due interi a e b esista un massimo comun divisore tra a e b.

Il teorema fondamentale dell'aritmetica suggerisce un metodo per calcolare un massimo comun divisore tra a e b, quello che viene insegnato sin dalla scuola elementare: supponendo, come lecito, a e b positivi, basta esprimere sia a che b come prodotti di potenze di numeri primi (positivi) a due a due distinti, con esponenti positivi:

$$\begin{aligned} a &= p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_s^{\lambda_s} \\ b &= q_1^{\mu_1} q_2^{\mu_2} \cdots q_t^{\mu_t}; \end{aligned}$$

si ottiene un massimo comun divisore tra a e b come prodotto di tutti i primi che appaiono in entrambe le fattorizzazioni (i *fattori comuni* ...), ciascuno elevato al minimo degli esponenti con cui

---

Avvertenza: Queste note integrano, ma non sostituiscono, le corrispondenti parti del libro di testo.

appare (*... col minimo esponente*). Ciò è facile da verificare (lo si faccia per esercizio) e mostra che la risposta alla domanda formulata sopra è positiva. Grazie anche alle osservazioni precedenti possiamo concludere che:

> *Se a e b sono interi allora:*
> — *se $a = b = 0$, l'unico massimo comun divisore tra a e b è 0;*
> — *altrimenti, se almeno uno tra a e b è diverso da zero, a e b hanno esattamente due massimi comun divisori, uno opposto dell'altro.*
> *In ogni caso, dunque, esiste uno ed un solo massimo comun divisore non negativo tra a e b.*

Il massimo comun divisore non negativo tra due interi a e b viene spesso indicato con il simbolo $\mathrm{MCD}(a, b)$.

Il metodo di calcolo di un massimo comun divisore tra due interi a e b appena ricordato è molto rapido ed efficace nel caso in cui a e b siano numeri di valore assoluto sufficientemente piccolo da renderne semplice la scomposizione in fattori primi. Quando si ha a che fare con numeri più grandi questo metodo risulta invece spesso impraticabile, dal momento che non sono noti metodi che permettano di scomporre in tempi ragionevolmente brevi numeri interi arbitrari; anzi, il calcolo dei fattori primi di un intero può rivelarsi di estrema complessità computazionale.

Per questo è molto importante disporre di un metodo alternativo, quello fornito dall'algoritmo euclideo, che ora illustreremo e che si dimostra essere invece molto efficiente. Per semplificare la discussione, introduciamo una definizione. Per ogni $a, b \in \mathbb{Z}$ chiamiamo *combinazione lineare di a e b a coefficienti in $\mathbb{Z}$* ogni numero intero che si possa scrivere come $\alpha a + \beta b$ per opportuni $\alpha, \beta \in \mathbb{Z}$. In altri termini, una combinazione lineare di a e b (a coefficienti in $\mathbb{Z}$; talvolta lasceremo sottintesa questa specificazione) è la somma di un multiplo di a per un multiplo di b. Ad esempio, sono combinazioni lineare di a e b i numeri $3a + 7b$, $15a - 2b$, $-19b$.

Lemma 1. *Siano $a, b, c \in \mathbb{Z}$. Se c divide a e b allora c divide ogni combinazione lineare di a e b a coefficienti in $\mathbb{Z}$.*

Dimostrazione — Se $c \mid a$ e $c \mid b$, esistono interi h e k tali che $a = hc$ e $b = kc$. Scelti comunque $\alpha, \beta \in \mathbb{Z}$ si ha allora $\alpha a + \beta b = \alpha(hc) + \beta(kc) = (\alpha h + \beta k)c$, dunque c divide $\alpha a + \beta b$. □

Un caso particolare del precedente lemma è il punto centrale del ragionamento che suggerisce e giustifica l'algoritmo euclideo:

Lemma 2. *Siano $a, b, q, r \in \mathbb{Z}$ tali che $a = bq + r$. Allora i divisori comuni ad a e b sono tutti e soli i divisori comuni a b e r. In particolare, i massimi comun divisori tra a e b sono precisamente i massimi comun divisori tra b e r.*

Dimostrazione — Sia c un divisore comune a b e r. Poiché a è combinazione lineare di b e r, allora $c \mid a$ per il Lemma 1. Dunque c è un divisore comune ad a e b. Abbiamo così provato l'inclusione

$$\mathrm{D}(a) \cap \mathrm{D}(b) \supseteq \mathrm{D}(b) \cap \mathrm{D}(r).$$

Per provare l'inclusione opposta, osserviamo che $r = a - bq$ è combinazione lineare di a e b, quindi, come per il passaggio precedente, ogni divisore comune ad a e b divide r ed è così un divisore comune a b e r. Abbiamo ora dimostrato l'uguaglianza $\mathrm{D}(a) \cap \mathrm{D}(b) = \mathrm{D}(b) \cap \mathrm{D}(r)$, cioè che a e b da una parte e b ed r dall'altra hanno gli stessi divisori comuni, quindi anche gli stessi massimi comun divisori. □

Supponiamo ora di voler calcolare un massimo comun divisore tra due interi a e b; come visto sopra possiamo supporre che essi siano entrambi positivi. Possiamo ovviamente anche supporre $a \geq b$, infatti se $a < b$ basta scambiare tra loro a e b, dal momento che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$.

Come sappiamo, si può effettuare la divisione aritmetica (con resto) di a per b. Esistono dunque (e sono univocamente determinati) due numeri naturali q (il quoziente) e r (il resto) tali che

$$a = bq + r \qquad \text{e} \qquad r < b.$$

Il Lemma 2 mostra che vale l'uguaglianza $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$. Possiamo dunque tradurre il nostro problema originale (calcolare un massimo comun divisore tra a e b) con il problema, simile,

di calcolare un massimo comun divisore tra b e r. Il vantaggio di questa riformulazione consiste in questo, che se consideriamo la "grandezza" dei due numeri a e b come misura (grossolana!) della difficoltà del nostro problema (nel senso che è, probabilmente, più facile calcolare un massimo comun divisore tra due numeri più piccoli piuttosto che tra due numeri più grandi), allora l'aver sostituito la coppia (b, r) alla coppia (a, b) ha semplificato il problema, perché $b < a$ e $r < b$.

È possibile che si abbia $r = 0$. In questo caso, $b \mid a$ e quindi b è un massimo comun divisore tra a e b. Se invece $r > 0$, possiamo ripetere per b e r il procedimento effettuato per a e b: dividendo b per r otteniamo,

$$b = rq_1 + r_1 \qquad \text{e} \qquad r_1 < r,$$

dove, ancora, $q_1, r_1 \in \mathbb{N}$ e i massimi comun divisori tra r e r_1 sono i massimi comun divisori tra b e r, quindi tra a e b. Se $r_1 = 0$ (cioè se $r \mid b$), allora r è un massimo comun divisore tra a e b, in caso contrario possiamo effettuare un'altra divisione, quella tra r e r_1, ottenendo $q_2, r_2 \in \mathbb{N}$ tali che:

$$r = r_1q_2 + r_2 \qquad \text{e} \qquad r_2 < r_1,$$

se $r_2 = 0$ allora r_1 è il massimo comun divisore cercato, altrimenti si proseguirà dividendo r_1 per r_2.

Dovrebbe essere a questo punto chiaro il procedimento: ad ogni passo si verifica se il resto r_t dell'ultima divisione effettuata: $r_{t-2} = r_{t-1}q_t + r_t$, è 0; in questo caso il penultimo resto r_{t-1} (vale a dire, l'ultimo resto diverso da 0, o, ancora, l'ultimo divisore) è il massimo comun divisore positivo tra a e b, se invece $r_t \neq 0$ si effettua un'altra divisione, tra il divisore r_{t-1} ed il resto r_t della divisione precedente.

È ancora da chiarire un solo punto, cioè se questo procedimento termina, ovvero se, iterando questo procedimento, si perviene ad una divisione con resto 0. La risposta è affermativa. Infatti, la sequenza dei resti ottenuti nelle successive divisioni è strettamente decrescente:

$$b > r > r_1 > r_2 > r_3 > \cdots \geq 0$$

e una sequenza strettamente decrescente di numeri naturali minori di b può avere al più b termini, dal momento che l'insieme $\{n \in \mathbb{N} \mid b \geq n\}$ ha b elementi. Dunque $r_t = 0$ per qualche $t < b$. Pertanto l'algoritmo termina, fornendo un massimo comun divisore tra a e b, dopo al più b divisioni (ad essere pedanti, si dovrebbe specificare che, affinché tutto ciò che è stato appena scritto abbia senso in ogni caso, si devono sottintendere le posizioni $r_0 := r$ e $r_{-1} := b$).

Notiamo che l'algoritmo euclideo appena descritto fornisce un'altra dimostrazione, costruttiva, dell'esistenza di un massimo comun divisore tra due arbitrari interi.

Possiamo riassumere la discussione precedente e schematizzare l'algoritmo euclideo per la ricerca di un massimo comun divisore come segue:

Assegnati due numeri interi a e b, si intende calcolare un massimo comun divisore d tra a e b.

① se uno tra a e b è 0, si pone d uguale all'altro e l'algoritmo termina. Altrimenti:

② si sostituiscono a e b con $|a|$ e $|b|$, nell'ordine;

③ se $a < b$ si scambiano tra loro a e b;

④ a partire dalla divisione di a per b si effettuano divisioni aritmetiche successive, come sopra specificato, finché non si ottenga 0 come resto:

$$\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
r &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{t-3} &= r_{t-2}q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1}q_t + r_t \\
r_{t-1} &= r_tq_{t+1} + 0
\end{aligned}$$

dove $b > r > r_1 > r_2 > \cdots > r_t > 0$. A questo punto, si pone $d = r_t$ e l'algoritmo termina.

Anche se non essenziali per la comprensione dell'algoritmo, si possono fare alcune osservazioni marginali. Innanzitutto, il passo ② non è necessario in senso stretto, dal momento che è possibile effettuare divisioni aritmetiche anche tra interi negativi, o tra un positivo e un negativo. Tuttavia, è consigliabile eseguirlo per evitare inutili complicazioni di calcolo. Anche il passo ③ si sarebbe potuto omettere dalla descrizione dell'algoritmo, per un motivo di tipo diverso. Infatti, se a e b sono positivi e $a < b$, allora la divisione aritmetica di a per b fornisce quoziente 0 e resto a. Dunque se eseguiamo il passo ④ dell'algoritmo senza aver prima scambiato tra loro a e b, la prima divisione (di a per b) fornisce $r = a$ e quindi la seconda, quella tra b e $r = a$, è precisamente quella da cui saremmo partiti se avessimo eseguito il passo ③. Ciò mostra che l'unico scopo del passo ③ è quello di evitare una divisione inutile (ancorché banale).

Osservazione più rilevante, a proposito del passo ④, è che, come abbiamo già detto, l'algoritmo terminerà dopo al più $|b|$ divisioni.

Come esempio di applicazione dell'algoritmo euclideo, supponiamo di voler calcolare il massimo comun divisore positivo d tra 2547 e -7431. Passando ai valori assoluti dei due numeri considerati, e tenendo conto che $2547 < 7431$, procediamo come al passo ④ dopo aver posto $a = 7431$ e $b = 2547$. Eseguiamo dunque le divisioni:

$$
\begin{aligned}
7431 &= 2547[2] + 2337 \\
2547 &= 2337[1] + 210 \\
2337 &= 210[11] + 27 \\
210 &= 27[7] + 21 \\
27 &= 21[1] + 6 \\
21 &= 6[3] + 3 \\
6 &= 3[2]
\end{aligned}
$$

Come evidenziato dalle frecce in colore, ogni divisione successiva alla prima ha per dividendo e per divisore il divisore ed il resto della divisione precedente. Come si può capire, è importante, eseguendo l'algoritmo, non confondere i ruoli tra i successivi divisori (indicati sopra come $b, r, r_1, \ldots$) ed i successivi quozienti (indicati come $q, q_1, q_2, \ldots$). I primi vanno riutilizzati nella divisione seguente, i secondi no. Allo scopo di evitare questa possibile confusione può essere utile adottare qualche artificio grafico. In questo caso, i quozienti sono stati scritti tra parentesi quadre.

Tornando al nostro specifico esempio, poiché l'ultimo resto non nullo è 3, concludiamo che 3 è un massimo comun divisore tra 2562 e -7491.

Un'ulteriore osservazione su questo algoritmo è che esso può essere reso ancora più efficace da una piccola modifica. Infatti, l'algoritmo si basa su una ripetuta applicazione del Lemma 2, e nell'enunciato del Lemma 2 non è richiesto che gli interi q ed r siano proprio il quoziente ed il resto della divisione aritmetica di a per b. Ora, è possibile effettuare un altro tipo di divisione tra interi che rispetti la condizione "$a = bq + r$" dell'ipotesi del Lemma 2:

Lemma 3 (Divisione euclidea). *Siano $a, b \in \mathbb{Z}$. Se $b \neq 0$ esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $|r| \leq |b|/2$.*

Dimostrazione — Assegnati a e b come richiesto dall'enunciato, effettuiamo la divisione aritmetica tra a e b. Otteniamo così $\bar{q}, \bar{r} \in \mathbb{Z}$ tali che $a = b\bar{q} + \bar{r}$ e $0 \leq \bar{r} < |b|$. Se $\bar{r} \leq |b|/2$, allora abbiamo concluso la ricerca di q e r: basterà porre $r = \bar{r}$ e $q = \bar{q}$, a questo punto avremo $a = bq + r$ e $|r| = r \leq |b|/2$, come richieso dall'enunciato.

Se invece $\bar{r} > |b|/2$, allora si ha $|b| - \bar{r} < |b| - \big(|b|/2\big) = |b|/2$. In questo caso, poniamo $r := \bar{r} - |b|$. Poiché $\bar{r} < |b|$ si ha allora $r < 0$, e quindi $|r| = -r = |b| - \bar{r} < |b|/2$. Dunque la condizione $|r| \leq |b|/2$ è soddisfatta. Inoltre $\bar{r} = |b| + r$, dunque

$$a = b\bar{q} + \bar{r} = b\bar{q} + \big(|b| + r\big) = bq + r,$$

avendo posto $q = \bar{q} + 1$ se $b > 0$ (e quindi se $|b| = b$) e $q = \bar{q} - 1$ se $b < 0$. Con questa scelta di q e r le condizioni richieste dall'enunciato sono soddisfatte, e così il lemma è dimostrato. □

Ad esempio la divisione aritmetica di 14 per 5 dà quoziente 2 e resto 4; la divisione euclidea appena introdotta dà quoziente 3 (aumentato di 1 rispetto al precedente, perché il divisore 5 è positivo) e resto -1: infatti $14 = 5[3] + (-1)$.

Possiamo eseguire l'algoritmo euclideo per la ricerca di un massimo comun divisore effettuando quest'ultimo tipo di divisioni anziché quelle aritmetiche. Uno svantaggio (se così si può dire, anche questo sarebbe evitabile) è che eseguiremo divisioni anche tra numeri negativi, un significativo vantaggio è che la successione dei resti r, r_1, $r_2, \dots$ verificherà le condizioni:

$$|r| \leq |b|/2; \quad |r_1| \leq |r|/2 \leq |b|/4; \quad |r_1| \leq |r_2|/2 \leq |b|/8; \dots,$$

che, per dirla in termini informali, garantiscono che la successione dei resti decrescerà, nella maggior parte dei casi, più rapidamente di quanto non accadeva con la versione originaria dell'algoritmo. Ciò significa che possiamo aspettarci di dover effettuare meno divisioni, e quindi di terminare più rapidamente l'algoritmo.

A titolo di esempio, si possono confrontare il procedimento seguito prima per il calcolo del massimo comun divisore tra 7431 e 2547 con una versione dello stesso calcolo eseguito effettuando divisioni euclidee anziché aritmetiche:

$$\begin{aligned}
7431 &= 2547[2] + 2337 \\
2547 &= 2337[1] + 210 \\
2337 &= 210[11] + 27 \\
210 &= 27[7] + 21 \\
27 &= 21[1] + 6 \\
21 &= 6[3] + 3 \\
6 &= 3[2]
\end{aligned}
\qquad\qquad
\begin{aligned}
7431 &= 2547[3] + (-210) \\
2547 &= (-210)[-12] + 27 \\
-210 &= 27[-8] + 6 \\
27 &= 6[4] + 3 \\
6 &= 3[2]
\end{aligned}$$

Esercizio. Si sarebbero potute eseguire le divisioni nella colonna di sinstra, senza alterare il risultato finale, tralasciando i segni 'meno' dei divisori, e quindi assicurando che tutte le divisioni fossero tra numeri positivi. Ad esempio, dopo la prima divisione: $7431 = 2547[3] + (-210)$, la seconda avrebbe potuto essere $2547 = 210[12] + 27$. Basandosi sul Lemma 2 e su osservazioni precedenti, spiegare perché questa procedura è sempre lecita.

Equazioni diofantee

Oltre al calcolo dei massimi comun divisori, l'algoritmo euclideo permette di risolvere un altro importante problema. Un'equazione diofantea è un'equazione in cui appaiano solo indeterminate e numeri interi che si intenda risolvere in $\mathbb{Z}$, cioè per la quale siano ammesse come soluzioni solo numeri interi.

Ci occupiamo qui di un particolare tipo di equazione diofantea: quella cosiddetta lineare a due indeterminate, cioè una equazione diofantea della forma

$$ax + by = c, \tag{‡}$$

dove a, b e c sono numeri interi. Risolvere l'equazione (‡) significa dunque trovare le coppie di *interi* (u, v), che rendano vera l'uguaglianza se sostituiti a x e y, cioè tali che $au + bv = c$. Osserviamo subito che è possibile che la (‡) non ammetta soluzioni. Ad esempio, per $a = b = 0$ e $c = 1$ otteniamo l'equazione $0x + 0y = 1$ che, ovviamente, non ammette soluzioni. Facendo uso della terminologia introdotta sopra, è chiaro che (‡) ammette soluzioni (intere) se e solo se c è combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. Ciò permette di dimostrare la prima importante osservazione su questo genere di equazioni.

Lemma 4. *Siano $a, b, c \in \mathbb{Z}$, e sia d un massimo comun divisore tra a e b. Se d non divide c, allora l'equazione diofantea $ax + by = c$ non ammette soluzioni.*

Dimostrazione — Supponiamo che l'equazione abbia soluzioni. Allora esistono $u, v \in \mathbb{Z}$ tali che $au + bv = c$, dunque c è combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. Dal Lemma 1 segue allora che d divide c. Dunque, se supponiamo che d non divida c dobbiamo trarre la conclusione che la nostra equazione non ha soluzioni. □

Ad esempio, l'equazione diofantea $2x + 6y = 3$ non ha soluzioni. Ovviamente ciò significa che l'equazione non ha soluzioni intere; essa ha ovviamente soluzioni razionali (cioè in $\mathbb{Q}$), ad esempio $(0, 1/2)$ o $(1, 1/6)$, ma nessuna di esse è data da due numeri interi.

Vedremo come l'algoritmo euclideo permette non solo di dimostrare che vale anche l'implicazione inversa di quella stabilita nel Lemma 4, cioè, nelle stesse notazioni, che se d divide c, allora l'equazione diofantea $ax + by = c$ ammette soluzioni, ma anche di trovare queste soluzioni.

A questo scopo, iniziamo a considerare un caso banale, quello in cui almeno uno tra i coefficienti a e b è 0. Se $a = 0$, allora l'equazione (‡) si riduce a $by = c$. Dire che questa ha una soluzione intera equivale a dire che b divide c. Inoltre, b è un massimo comun divisore tra $a(= 0)$ e b, quindi è vero, in questo caso, che l'equazione data ammette soluzioni se (e solo se, in accordo col Lemma 4) un massimo comun divisore tra a e b divide c. Naturalmente, sempre in questo caso, è semplicissimo determinare le soluzioni, qualora ne esistano: se $b \neq 0$ esse sono tutte (e sole) le coppie $(n, c/b)$ al variare di n in $\mathbb{Z}$, mentre ogni coppia di numeri interi è soluzione se $b = 0$.

In modo analogo si ragiona se $b = 0$.

Supponiamo allora che sia a che b siano diversi da zero. Eseguiamo le divisioni successive previste dall'algoritmo euclideo:

$$\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
r &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{t-3} &= r_{t-2}q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1}q_t + r_t \\
r_{t-1} &= r_tq_{t+1}
\end{aligned}$$

Allora r_t è uno dei due massimi comun divisori tra a e b; poniamo $d := r_t$. Per risolvere l'equazione diofantea (‡) proveremo prima a risolvere l'equazione diofantea

$$ax + by = d. \tag{†}$$

Come già osservato, risolvere quest'ultima equivale ad esprimere d come combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. La divisione in cui $d = r_t$ appare come resto permette di esprimere d come combinazione lineare dei due resti precedenti, r_{t-1} e r_{t-2}, infatti da $r_{t-2} = r_{t-1}q_t + d$ traiamo $d = r_{t-2} + [-q_t]r_{t-1}$. La divisione precedente, $r_{t-3} = r_{t-2}q_t + r_{t-1}$, fornisce poi r_{t-1} come combinazione lineare di r_{t-3} e r_{t-2}, dando $r_{t-1} = r_{t-3}+[-q_{t-1}]r_{t-2}$. Se sostituiamo questa espressione per r_{t-1} nella espressione trovata prima per d otteniamo $d = r_{t-2} + [-q_t]r_{t-1} = r_{t-2} + [-q_t]\big(r_{t-3} + [-q_{t-1}]r_{t-2}\big) = [-q_t]r_{t-3} + [1 + q_tq_{t-1}]r_{t-2}$, ed esprimiamo così d come combinazione lineare di r_{t-2} e r_{t-3}, i due resti precedenti r_{t-1}. Questi passaggi dovrebbero essere sufficienti a comprendere l'intero procedimento. Per comodità di espressione poniamo $r_0 := r$, $r_{-1} := b$ e $r_{-2} := a$. Ad ogni passo d è espresso come combinazione lineare (a coefficienti in $\mathbb{Z}$) di due "resti" con pedici consecutivi, diciamo r_i e r_{i+1}; dalla divisione di r_{i-1} per r_i si ottiene $r_{i+1} = r_{i-1} + [-q_{i+1}]r_i$. Sostituendo nell'espressione di d r_{i+1} con, appunto, $r_{i-1} + [-q_{i+1}]r_i$ si può scrivere d come combinazione lineare di r_{i-1} e r_i, i due "resti" precedenti, nell'ordine, r_i e r_{i+1}. Questo passaggio può essere reiterato finché non si ottenga un'espressione di d come combinazione lineare di $a = r_{-2}$ e $b = r_{-1}$, cioè due interi α e β tali che $\alpha a + \beta b = d$. Allora α e β forniscono una soluzione dell'equazione (†). Da questa si trae facilmente una soluzione per l'equazione (‡). Infatti, avendo assunto per ipotesi che d divida c, si ha $c = dh$ per un opportuno $h \in \mathbb{Z}$. Allora, ponendo $u := h\alpha$ e $v := h\beta$, si ha

$$au + bv = ah\alpha + bh\beta = h(\alpha a + \beta b) = hd = c,$$

quindi u e v forniscono una soluzione di (‡).

Abbiamo in questo modo provato che l'equazione diofantea (‡) ammette soluzioni se $d \mid c$. Ricordandoci del Lemma 4 possiamo dunque concludere col seguente teorema:

Teorema 5 (Teorema di Bézout). *Siano $a, b \in \mathbb{Z}$, e sia $d = \mathrm{MCD}(a, b)$. Allora l'equazione diofantea $ax + by = c$ ammette soluzioni (in $\mathbb{Z}$) se e solo se d divide c.*

Il Teorema di Bézout è spesso citato, in modo equivalente, anche in questa forma:

Teorema 5*. *Siano $a, b \in \mathbb{Z}$, e sia $d = \mathrm{MCD}(a, b)$. Allora l'insieme $\{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$ delle combinazioni lineari di a e b a coefficienti in $\mathbb{Z}$ coincide con l'insieme $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$ dei multipli di d in $\mathbb{Z}$.*

Come già per la ricerca di un massimo comun divisore, grazie all'algoritmo euclideo, non solo abbiamo stabilito esattamente quando un'equazione diofantea del tipo a noi considerato ammette soluzioni, ma abbiamo anche individuato un metodo (piuttosto efficace) per determinarne una nel caso esista.

Ad esempio, supponiamo di voler trovare soluzioni dell'equazione diofantea

$$74x + 22y = 10.$$

In questo caso è evidente che $\mathrm{MCD}(74, 22) = 2$; poiché 2 divide 10 siamo certi che l'equazione ammette soluzioni. Benché già conosciamo il massimo comun divisore 2, per trovare una soluzione mediante l'algoritmo euclideo bisogna eseguire le divisioni successive:

$$\begin{aligned} 74 &= 22[3] + 8 \\ 22 &= 8[2] + 6 \\ 8 &= 6[1] + 2 \\ 6 &= 2[3] \end{aligned}$$

sino ad ottenere 2 come ultimo resto non nullo. Da queste uguaglianze ricaviamo:

$$\begin{aligned} 8 &= 74 + 22[-3] \\ 6 &= 22 + 8[-2] \\ 2 &= 8 + 6[-1] \ . \end{aligned}$$

A questo punto possiamo esprimere 2 come combinazione lineare di 74 e 22, mediante successive sostituzioni:

$$\begin{aligned} 2 &= 8 + 6[-1] \\ &= 8 + \big(22 + 8[-2]\big)[-1] && \text{(sostituendo 6)} \\ &= 8 + 22[-1] + 8[2] && \text{(eseguendo i calcoli \dots)} \\ &= 8[3] + 22[-1] && \text{(\dots e raccogliendo i coefficienti di 8 e 22)} \\ &= \big(74 + 22[-3]\big)[3] + 22[-1] && \text{(sostituendo 8)} \\ &= 74[3] + 22[-9] + 22[-1] && \text{(eseguendo i calcoli \dots)} \\ &= 74[3] + 22[-10] && \text{(\dots e raccogliendo i coefficienti di 22 e 74).} \end{aligned}$$

Abbiamo così ottenuto l'espressione di 2 cercata. Questa mostra che la coppia $(3, -10)$ è soluzione dell'equazione diofantea $74x + 22y = 2$. Moltiplicando per 5 (cioè per $10/2$) si ottiene $74[15] + 22[-50] = 10$, dunque la coppia $(15, -50)$ è soluzione della nostra equazione diofantea $74x + 22y = 10$.

Alcune annotazioni: come è chiaro, il procedimento effettuato si sarebbe potuto semplificare in almeno due modi:

- avremmo potuto effettuare divisioni euclidee anziché aritmetiche, risparmiando qualche passaggio. In questo caso specifico, dividendo 22 per 8 avremmo potuto scrivere $22 = 8[3] + (-2)$ piuttosto che $22 = 8[2] + 6$, risparmiando sia una divisione che una sostituzione nella seconda parte dell'algoritmo. Per quest'ultima avremmo infatti ottenuto: $-2 = 22 + 8[-3] = 22 + \big(74 + 22[-3]\big)[-3] = 22[10] + 74[-3]$ e quindi $10 = 22[-50] + 74[15]$, moltiplicando per $-5 = 10/(-2)$.
- avendo osservato che 2 divide 74, 22 e10, avremmo potuto semplificare l'equazione dividendo tutti i coefficienti per 2 e ottenendo $37x + 11y = 5$, un'equazione equivalente alla precedente. Avremmo poi proceduto con calcoli analoghi a quelli effettuati sopra, ma facilitati perché applicati a numeri già divisi per due.

Una cosa molto importante da chiarire è che la soluzione trovata non è l'unica. Infatti, come è immediato verificare, per ogni intero k si ha $74(15 + 22k) + 22(-50 - 74k) = 10$, il che fornisce infinite soluzioni alla nostra equazione. In effetti, in generale, *ogni equazione diofantea del tipo che stiamo considerando (cioè lineare a due indeterminate) ha infinite soluzioni se ne ha almeno una.* Detto in altri termini: ha nessuna o infinite soluzioni. Ciò si può far seguire dalla teoria delle equazioni congruenziali lineari ad una indeterminata, che viene trattata in altre note. Ci limitiamo qui a stabilire il nesso tra equazioni diofantee e equazioni congruenziali:

Lemma 6. *Siano $a, b, c, u \in \mathbb{Z}$. Allora u è soluzione dell'equazione congruenziale $ax \equiv c \pmod{b}$ se e solo se esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione dell'equazione diofantea $ax + by = c$.*

Dimostrazione — Se u è soluzione di $ax \equiv c \pmod{b}$, allora b divide $au - c$, quindi $au - c = bk$ per un opportuno $k \in \mathbb{Z}$. Ma allora $au - bk = c$, dunque, ponendo $v = -k$, si ha $au + bv = c$, il che significa che (u, v) è soluzione di $ax + by = c$. Viceversa, se esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione di $ax + by = c$, cioè tale che $au + bv = c$, allora b divide $bv = au - c$, dunque $au \equiv c \pmod{b}$ e u è soluzione di $ax \equiv c \pmod{b}$. □

Possiamo concludere, grazie al Lemma 6, che il problema di risolvere l'equazione diofantea $ax + by = c$ è equivalente al problema di risolvere l'equazione congruenziale $ax \equiv c \pmod{b}$. Infatti, ogni soluzione (u, v) della prima fornisce immediatamente la soluzione u della seconda; viceversa, se u è soluzione della seconda, allora non solo esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione della prima, ma tale v è facile da determinare: basta risolvere l'equazione (ad una sola indeterminata) $au + by = c$.

A titolo di esempio, torniamo alla nostra equazione $74x + 22y = 10$. Come abbiamo visto, la coppia $(15, -50)$ ne fornisce una soluzione. Allora 15 è soluzione dell'equazione congruenziale $74x \equiv 10 \pmod{22}$. Utilizzando questa informazione, dalla teoria delle equazioni congruenziali deduciamo che l'insieme di tutte le soluzioni di $74x \equiv 10 \pmod{22}$ è $[15]_{11} = [4]_{11} = 4 + 11\mathbb{Z} = \{4 + 11k \mid k \in \mathbb{Z}\}$. Pertanto le soluzioni (intere) di $74x + 22y = 10$ saranno tutte e sole le coppie (u, v) tali che $u = 4 + 11k$ e v sia soluzione di $74u + 22y = 10$, vale a dire: $v = (10 - 74u)/22$. Svolgendo tutti i calcoli, si ottiene $(10 - 74u)/22 = \big(5 - 37(4 + 11k)\big)/11 = -13 - 37k$, quindi l'insieme delle soluzioni della nostra equazione è

$$\big\{(4 + 11k, -13 - 37k) \,\big|\, k \in \mathbb{Z}\big\}.$$

Per $k = 0$ troviamo così la soluzione $(4, -13)$, mentre la soluzione $(15, -50)$ che avevamo calcolato sopra si ottiene per $k = 1$.

Va infine menzionata una importante applicazione del Teorema di Bézout. Due interi a e b si dicono *coprimi* se e solo se $1 = \mathrm{MCD}(a, b)$. È evidente che questa condizione equivale a richiedere che non esista alcun numero primo che divida sia a che b. Il Teorema di Bézout ha questo caso particolare (anch'esso talvolta chiamato Teorema di Bézout, in effetti il Teorema 5 si può dedurre da questo enunciato):

Corollario 7. *Siano $a, b \in \mathbb{Z}$. Allora a e b sono coprimi se e solo se esistono $u, v \in \mathbb{Z}$ tali che $au + bv = 1$.*

Dimostrazione — Per il Teorema 5, esistono $u, v \in \mathbb{Z}$ tali che $au + bv = 1$ se e solo se $\mathrm{MCD}(a, b)$ divide 1. Poiché i soli divisori di 1 sono 1 e -1, questa condizione equivale a $\mathrm{MCD}(a, b) = 1$, cioè a richiedere che a e b siano coprimi. □

Proposizione 8. *Siano a e b due interi coprimi. Per ogni $c \in \mathbb{Z}$, se $a \mid bc$ allora $a \mid c$.*

Dimostrazione — Per il Teorema di Bézout (o per il Corollario 7) si ha $1 = au + bv$ per opportuni $u, v \in \mathbb{Z}$. Moltiplicando per c otteniamo $c = acu + bcv$. Dunque c è combinazione lineare di a e bc; poiché a divide a e, per ipotesi, bc allora il Lemma 1 prova che a divide c. □