IV SETTIMANA

L'algoritmo euclideo delle divisioni successive in $\mathbb{Z}$. Calcolo "effettivo" del MCD e di una identità di Bézout.
Scrittura di un numero intero in base b fissata, con $b \geq 2$.
Numeri primi. Teorema Fondamentale dell'Aritmetica (dimostrazione tramite il principio di induzione nella formulazione "ampia").

Coppie ordinate. Prodotto cartesiano di due insiemi. "Insiemi proiezione" di un prodotto cartesiano. Grafici.

Numeri complessi: $\mathbb{C} := \mathbb{R} \times \mathbb{R}$. Operazioni in $\mathbb{C}$: Somma, prodotto. Modulo, argomento, parte reale e parte immaginaria di un numero complesso. Coniugato e norma (di un numero complesso). Inverso moltiplicativo di un numero complesso non nullo. Forma polare di un numero complesso. Formula di A. de Moivre sulla potenza di un numero complesso.

Tali argomenti si possono trovare nei Paragrafi 4 e 5 di [FG].

* * *

[FG] Marco Fontana e Stefania Gabelli, *Insiemi, numeri e polinomi.* CISU, Roma 1989.

2 Algoritmo euclideo di divisione

In questo paragrafo intendiamo mostrare come alcune importanti proprietà dell'aritmetica elementare di $\mathbb{Z}$ traggano origine dalla validità in $\mathbb{N}$ del "Principio del Minimo" (ovvero, equivalentemente, dal "Principio del Buon Ordinamento", cfr. Teorema 1.2).

Teorema 2.1. (Algoritmo euclideo di divisione) *Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora, esistono e sono univocamente determinati due interi $q \in \mathbb{Z}$ (detto,* quoziente *) ed $r \in \mathbb{N}$ (detto* resto *) in modo tale che:*

$$a = bq + r\,, \qquad 0 \leqslant r <\mid b \mid .$$

Dimostrazione. Mostriamo, dapprima, *l'esistenza* di q ed r.

Caso 1. Supponiamo che $b > 0$. Notiamo, innanzitutto, che l'insieme:

$$S := \{a - nb\,:\; a - nb \geqslant 0,\, n \in \mathbb{Z}\}\,(\subseteq \mathbb{N})$$

è non vuoto (ad esempio, se $n' = -\mid a \mid$, allora $a - n'b \in S$). Per il "Principio del Buon Ordinamento" **(BO)** (Teorema 1.2), possiamo trovare un primo elemento nell'insieme S, che denotiamo con $r := a - qb$. Mostriamo che $r < b$. Se, per assurdo, fosse $r \geqslant b$ allora si avrebbe:

$$r - b = a - qb - b = a - (q+1)b \geqslant 0,$$

e, dunque, anche $r - b\,(< r)$ apparterrebbe ad S. Ciò contraddice la minimalità di $r \in S$.

Caso 2. Supponiamo che $b < 0$. Applichiamo il Caso 1 alla coppia di interi $a, -b$ ed avremo l'esistenza di due interi $q, r \in \mathbb{Z}$ che verificano le seguenti condizioni:

$$a = -bq + r = b(-q) + r\,, \qquad 0 \leqslant r < -b = \mid -b \mid = \mid b \mid .$$

Mostriamo, ora, *l'unicità* di q, r. Supponiamo di avere $q, q', r, r' \in \mathbb{Z}$ in modo tale che:

$$a = bq + r = bq' = r'\,, \qquad 0 \leqslant r, r' <\mid b \mid,$$

allora $(q - q')b = r' - r <\mid b \mid b$, dunque $\mid q - q' \mid\mid b \mid <\mid b \mid$, cioè $\mid q - q' \mid < 1$, ovvero $q = q'$. Da ciò segue immediatamente che anche $r = r'$. $\square$

Definizione 2.2. Dati due elementi $a, b \in \mathbb{Z}$.

(a) Diremo che a *divide* b (oppure che b *è divisibile per* a), in breve scriveremo "$a \mid b$", se esiste un elemento $c \in \mathbb{Z}$ in modo tale che $ac = b$. Se ciò non accade, diremo che a *non divide* b, e scriveremo "$a \nmid b$". Notiamo che:

(a1) $\quad x \mid x\,, \qquad x \mid 0\,, \qquad 1 \mid x\,, \qquad$ per ogni $x \in \mathbb{Z}$;

(a2) $0 \mid x \;\Leftrightarrow\; x = 0$;
(a3) $x \mid 1 \;\Leftrightarrow\; x = \pm 1$;
(a4) $a \mid b$ e $b \mid a \;\Leftrightarrow\; a = \pm b$;
(a5) $a \mid b$ e $b \mid c \;\Rightarrow\; a \mid c$;
(a6) $z \mid a$ e $z \mid b \;\Leftrightarrow\; z \mid ax + by$, presi comunque $x, y \in \mathbb{Z}$;
(a7) $a \mid b \;\Leftrightarrow\; ac \mid bc$, per ogni $c \in \mathbb{Z}$.

(b) Se a e b non sono contemporaneamente nulli, si chiama *un Massimo Comun Divisore* di a, b (in breve, MCD(a, b)) un intero $d \in \mathbb{Z}$ tale che:

(MCD1) $d \mid a$, $d \mid b$;
(MCD2) $d' \in \mathbb{Z}$, $d' \mid a$, $d' \mid b \;\Rightarrow\; d' \mid d$.

Notiamo che se $a = 0$ e $b \neq 0$, allora b (ovvero, $-b$) è un Massimo Comun Divisore di 0 e b.
Infine, osserviamo che MCD$(0, 0)$ *non* è definito, in quanto ogni intero $x \in \mathbb{Z}$ è tale che $x \mid 0$ (e, quindi, non esiste un intero "massimo con tale proprietà", cioè non esiste un intero che verifica anche la proprietà **(MCD2)**).

(c) Se a, b non sono entrambi nulli, diremo che a e b sono *relativamente primi* (ovvero, *coprimi*) se MCD$(a, b) = 1$. □

Teorema 2.3. *Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esiste sempre un Massimo Comun Divisore d di a e b in $\mathbb{Z}$. Se d_1 e d_2 sono due Massimi Comun Divisori di a e b allora $d_1 = \pm d_2$.*
Il Massimo Comun Divisore d di a e b esiste ed è univocamente determinato in $\mathbb{N}$ *(in tal caso, esso è il più grande tra i divisori positivi comuni ad a e b, quindi la scrittura $d :=$ MCD(a, b) ha un significato univoco) ed esso coincide con il minimo intero positivo nell'insieme:*

$$S_{a,b} := \{ax + by \;\mid\; x, y \in \mathbb{Z},\, ax + by > 0\}.$$

Dimostrazione. Sia $d := ax_0 + by_0$ il minimo intero (positivo) dell'insieme non vuoto $S_{a,b}$. Mostriamo che, preso comunque $z := ax + by \in \mathbb{Z}$, con $x, y \in \mathbb{Z}$ (dove z può anche non appartenere ad $S_{a,b}$), allora $d \mid z$. Possiamo, ovviamente, supporre che $z \neq 0$. Per il Teorema 2.1, possiamo trovare $q, r \in \mathbb{Z}$, in modo tale che:

$$z = dq + r, \qquad 0 \leqslant r < d,$$

ovvero,

$$ax + by - (ax_0 + by_0)q = r \;\text{ cioè }\; a(x - x_0q) + b(y - y_0q) = r$$

dunque se $r > 0$ allora $r\,(< d) \in S_{a,b}$. Per la minimalità di d possiamo concludere che $r = 0$, ovvero che $d \mid z$. In particolare, $d \mid a$ (per $x = 1$ e $y = 0$) e $d \mid b$ (per $x = 0$ e $y = 1$), (proprietà **(MCD1)** per d).
Per terminare la dimostrazione che d è un MCD di a e b, mostriamo che d verifica anche la proprietà **(MCD2)**. Se $d' \mid a$ e $d' \mid b$, allora è subito visto dalla definizione di divisibilità che $d' \mid a\alpha + b\beta$, presi comunque $\alpha, \beta \in \mathbb{Z}$.

Dunque, in particolare, $d' \mid d$ (prendendo $\alpha = x_0$ e $\beta = y_0$).
Se d_1 e d_2 sono due Massimi Comun Divisori di a e b, allora dal fatto che d_1 è un MCD di a e b e che d_2 è un divisore di a e b, ricaviamo che $d_2 \mid d_1$. Analogamente, dal fatto che d_2 è un MCD di a e b e che d_1 è un divisore di a e b, ricaviamo che $d_1 \mid d_2$. Pertanto, da **(a4)**, possiamo concludere che $d_1 = \pm d_2$. $\square$

Osservazione 2.4. Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, da quanto precede segue immediatamente che:

$$\mathrm{MCD}(a, b) = \mathrm{MCD}(\mid a \mid, \mid b \mid) .$$

Corollario 2.5. ***(Identità di Bézout** (1730–1783)) Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esistono $x, y \in \mathbb{Z}$ in modo tale che:*

$$\mathrm{MCD}(a, b) = ax + by .$$

Osservazione 2.6. Si noti che gli elementi $x\ y \in \mathbb{Z}$ nella identità di Bézout non sono univocamente determinati. Ad esempio, se $a := 9$, $b := 6$, allora $\mathrm{MCD}(9, 6) = 3$ ed ad esempio $1 \cdot 9 + (-1) \cdot 6 = 3 = (-1) \cdot 9 + 2 \cdot 6$.

Corollario 2.7. ***(Lemma di Euclide,** IV–III Sec. A.C.) Siano $a, b, c \in \mathbb{Z}$. Allora:*

$$\mathrm{MCD}(a, b) = 1 \ \ e \ \ a \mid bc \quad \Rightarrow \quad a \mid c .$$

Dimostrazione. Dal Corollario 2.5 sappiamo che esistono $x, y \in \mathbb{Z}$ con $1 = ax + by$. Pertanto, $c = c \cdot 1 = acx + bcy$. Inoltre, per ipotesi, esiste un intero $k \in \mathbb{Z}$ in modo tale che $ak = bc$. Sostituendo abbiamo $c = acx + aky = a(cx + ky)$, da cui ricaviamo che $a \mid c$. $\square$

Definizione 2.8. Dati due elementi $a, b \in \mathbb{Z}$. Si chiama *minimo comune multiplo di a, b* (in breve, $\mathrm{mcm}(a, b)$) un intero $h \in \mathbb{Z}$ tale che:

(mcm1) $a \mid h$, $b \mid h$;

(mcm2) $h' \in \mathbb{Z}$, $a \mid h'$, e $b \mid h' \ \Rightarrow \ h \mid h'$.

Notiamo che, dalle proprietà della relazione di divisibilità, discende immediatamente che $\mathrm{mcm}(a, 0) = \mathrm{mcm}(0, b) = \mathrm{mcm}(0, 0) = 0$.

Osservazione 2.9. Dati comunque $a, b \in \mathbb{Z}$, se h_1 e h_2 sono due minimi comuni multipli di a e b allora $h_1 = \pm h_2$. Pertanto, un minimo comune multiplo h di a e b, se esiste, esso è univocamente determinato in $\mathbb{N}$ (in tal caso esso coincide con il minimo tra tutti gli interi positivi che seguono a e b e che somo multipli sia di a che di b, quindi la scrittura $h := \mathrm{mcm}(a, b)$ ha un significato univoco). Il prossimo risultato mostra l'esistenza del $\mathrm{mcm}(a, b)$, per ogni coppia di elementi $a, b \in \mathbb{Z}$. E' ovvio, da quanto precede, che $\mathrm{mcm}(a, b) = \mathrm{mcm}(\mid a \mid, \mid b \mid)$.

Teorema 2.10. *Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esiste ed è univocamente determinato in* $\mathbb{N}$ il $\mathrm{mcm}(a,b)$ *e risulta:*

$$\mathrm{MCD}(a,b) \cdot \mathrm{mcm}(a,b) = \mid ab \mid \ .$$

In particolare, se $a, b \in \mathbb{N}^+$, *allora* $\mathrm{MCD}(a,b) \cdot \mathrm{mcm}(a,b) = ab$.

Dimostrazione. Per le Osservazioni 2.9 e 2.4 non è restrittivo supporre che $a > 0$, $b > 0$. Sia $d := \mathrm{MCD}(a,b)$. Allora, esistono $\alpha, \beta, x, y \in \mathbb{Z}$ in modo tale che:

$$a = d\alpha\,, \quad b = d\beta\,, \quad \text{e} \quad d = ax + by\,.$$

Poniamo $m := \frac{ab}{d} \in \mathbb{N}$. Allora abbiamo che $m = a\beta = b\alpha$ e quindi che $a \mid m$ e $b \mid m$ (proprietà **(mcm1)**). Sia ora h' un multiplo comune di a e b, cioè $a \mid h'$ e $b \mid h'$, ovvero $h' = a\alpha' = b\beta'$, per una qualche coppia $\alpha', \beta' \in \mathbb{N}$. Notiamo che:

$$\frac{h'}{m} = \frac{h'd}{ab} = \frac{h'(ax+by)}{ab} = \frac{h'}{b}x + \frac{h'}{a}y = \beta' x + \alpha' y \in \mathbb{Z}\,,$$

pertanto $m \mid h'$ (proprietà **(mcm2)**). Da ciò ricaviamo che $\frac{ab}{d} = m = \mathrm{mcm}(a,b)$ e, quindi, che $ab = \mathrm{MCD}(a,b)\mathrm{mcm}(a,b)$. $\square$

Osservazione 2.11. In $\mathbb{Z}$, per ogni $x \in \mathbb{Z}$, denotiamo con $xZ := \{xk \ : \ k \in \mathbb{Z}\}$ l'insieme dei "multipli" di x. Allora, si può facilmente verificare che:

(a) $a\mathbb{Z} \supseteq b\mathbb{Z} \quad \Leftrightarrow \quad a \mid b$;

(b) $\mathrm{MCD}(a,b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$;

(c) $\mathrm{mcm}(a,b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Si noti che $a\mathbb{Z} + b\mathbb{Z} \supseteq a\mathbb{Z} \cup b\mathbb{Z}$ e può accadere che $a\mathbb{Z} + b\mathbb{Z} \supsetneq a\mathbb{Z} \cup b\mathbb{Z}$. Ad esempio, se $a := 2$, $b := 3$ allora $2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z} \supsetneq 2\mathbb{Z} \cup 3\mathbb{Z}$ ($5 \in 2\mathbb{Z} + 3\mathbb{Z}$, ma $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$).

Definizione 2.12. Un intero $p \geqslant 2$ si dice *primo* se dati $a, b \in \mathbb{Z}$ allora:

$$p \mid ab \quad \text{e} \quad p \nmid a \quad \Rightarrow \quad p \mid b\,.$$

Un intero $q \geqslant 2$ si dice *irriducibile* se dati $a, b \in \mathbb{Z}$ allora:

$$q = ab \quad \text{e} \quad q \neq \mid a \mid \quad \Rightarrow \quad q = \pm b\,.$$

Proposizione 2.13. *Per un intero $p \geqslant 2$, le seguenti affermazioni sono tra loro equivalenti:*

(i) *p è primo;*

(ii) *p è irriducibile;*

(iii) *i divisori positivi di p sono soltanto 1 e p.*

Dimostrazione. (i) $\Rightarrow$ (ii). Supponiamo che $p = ab$ e che $p \neq \mid a \mid$. Allora, ovviamente, $p \mid ab$. Inoltre, $p \nmid a$, perché se esistesse un intero $k \in \mathbb{Z}$ in modo tale che $pk = a$, allora avremmo che $p = ab = pkb$, da cui dedurremmo che $1 = kb$ (Legge di cancellazione, Esercizio 1.3 (c)), cioè $\mid b \mid = 1$ ovvero $p = \mid a \mid$, pervenendo così ad una contraddizione. Allora, avendo assunto la validità di (i), otteniamo che $p \mid b$. Pertanto, deve esistere un intero $h \in \mathbb{Z}$ in modo tale che $ph = b$. Quindi $p = ab = ahp$, cioè $1 = ah$ (Legge di cancellazione, Esercizio 1.3 (c)), dunque $\mid a \mid = 1$ ovvero $p = \pm b$.

(ii) $\Rightarrow$ (iii). Se, per assurdo la proprietà (iii) non fosse verificata, allora potremmo trovare due interi positivi $1 < a, b < p$ in modo tale che $p = ab$. Ma questo fatto contraddice (ii).

(iii) $\Rightarrow$ (i). Se p verifica (iii) e $p \nmid a$, allora necessariamente $\mathrm{MCD}(p, a) = 1$. Pertanto la conclusione che $p \mid b$ discende dal Lemma di Euclide (Corollario 2.7). $\square$

Teorema 2.14. ***(Teorema Fondamentale dell'Aritmetica,*** Euclide IV-III Sec. A.C.) *Un qualunque intero $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ ammette una decomposizione unica (a meno dell'ordine dei fattori) del tipo:*

$$a = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

dove $r \geqslant 1$, p_i è un intero primo, $e_i \geqslant 1$, per ogni $1 \leqslant i \leqslant r$, ed inoltre $p_i \neq p_j$, se $1 \leqslant i \neq j \leqslant r$.

Dimostrazione. Non è ovviamente restrittivo limitare la dimostrazione del teorema al caso $a \geqslant 2$.

Dimostramo dapprima *l'esistenza* della decomposizione. Procediamo per induzione su a.

Base dell'induzione: $a = 2$. L'enunciato è banalmente vero, essendo $a = 2$ un numero primo.

Passo Induttivo: Supponiamo, per ipotesi induttiva, che l'enunciato sia vero per ogni intero $2 \leqslant b < a$. Se a è un numero primo, non c'è nulla da dimostrare. Se a non è primo, allora $a = xy$, con $2 \leqslant x, y < a$. Per l'ipotesi induttiva (applicata ad x ed y), possiamo scrivere:

$$x = p'^{f_1}_1 p'^{f_2}_2 \dots p'^{f_n}_n \quad \text{e} \quad y = p''^{g_1}_1 p''^{g_2}_2 \dots p''^{g_m}_m$$

dunque:

$$a = p'^{f_1}_1 p'^{f_2}_2 \dots p'^{f_n}_n p''^{g_1}_1 p''^{g_2}_2 \dots p''^{g_m}_m .$$

Dopo aver raccolto gli eventuali fattori aventi la stessa "base" (cioè, multipli dello stesso fattore primo), otteniamo proprio una decomposizione del tipo enunciato.

Dimostriamo ora *l'unicità* della decomposizione. Supponiamo di avere due decomposizioni di a con le proprietà enunciate:

$$p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} = a = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s} .$$

Poiché p_1 è un numero primo e $p_1 \mid q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$, allora $p_1 \mid q_j$, per un qualche $1 \leqslant j \leqslant s$. Essendo anche q_j un numero primo (ovvero irriducibile), allora necessariamente $p_1 = q_j$. Dividendo le due decomposizioni di a per p_1 (quella di destra) e per q_j (quella di sinistra) (o, più precisamente, applicando la Legge di cancellazione, Esercizio 1.3 (c)) ed iterando il procedimento precedente, otteniamo necessariamente che $r = s$, $p_i = q_i$ (a meno di un cambiamento degli indici dei fattori ovvero del loro ordine) e $e_i = f_i$, per ogni $1 \leqslant i \leqslant r$. $\square$

2. Esercizi e Complementi

2.1. Siano $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, con $n \geqslant 2$, interi non tutti nulli. *Un Massimo Comun Divisore di* $a_1, a_2, \ldots, a_n$ (in breve, $\mathrm{MCD}(a_1, a_2, \ldots, a_n)$) è un intero $d \in \mathbb{Z}$ tale che:

(MCD1) $d \mid a_i$, per ogni $1 \leqslant i \leqslant n$;

(MCD2) $d' \in \mathbb{Z}$, $d' \mid a_i$, per ogni $1 \leqslant i \leqslant n \;\Rightarrow\; d' \mid d$.

Mostrare che *esiste un unico Massimo Comun Divisore* $d \in \mathbb{N}$ *di* $a_1, a_2, \ldots, a_n$, il quale coincide con in minimo intero nell'insieme non vuoto:

$$S_{a_1,a_2,\ldots,a_n} := \{a_1y_1 + a_2y_2 + \ldots + a_ny_n \;:\; y_i \in \mathbb{Z},\ 1 \leqslant i \leqslant n,\ a_1y_1 + a_2y_2 + \ldots + a_ny_n > 0\}.$$

In particolare, esistono $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ in modo tale che il Massimo Comun Divisore (univocamente determinato in $\mathbb{N}$) si può esprimere nella forma seguente:

$$\mathrm{MCD}(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n \qquad \text{(Identità di Bézout)}.$$

[Suggerimento. Basta seguire, con le appropriate modifiche, la dimostrazione del Teorema 2.3.]

2.2. Siano a, b, c degli interi non nulli di $\mathbb{Z}$. Mostrare che valgono le seguenti proprietà (a meno del segno, qualora non si scelga *il* MCD in $\mathbb{N}$):

(a) $\mathrm{MCD}(a, \mathrm{MCD}(b, c)) = \mathrm{MCD}(a, b, c) = \mathrm{MCD}(\mathrm{MCD}(a, b), c)$.

(b) $\mathrm{MCD}(a, 1) = 1$.

(c) $\mathrm{MCD}(ab, ac) = a\mathrm{MCD}(b, c)$.

(d) $d = \mathrm{MCD}(a, b) \quad\Rightarrow\quad \mathrm{MCD}(\frac{a}{d}, \frac{b}{d}) = 1$.

(e) $\mathrm{MCD}(a, b) = 1 = \mathrm{MCD}(a, c) \quad\Rightarrow\quad \mathrm{MCD}(a, bc) = 1$.

(f) $a \mid c$, $b \mid c$, e $\mathrm{MCD}(a, b) = 1 \quad\Rightarrow\quad ab \mid c$.

[Suggerimento. **(a)** Ci limitiamo a dimostrare la prima uguaglianza. Sia $d := \mathrm{MCD}(a, b, c)$ e $\tilde{d} := \mathrm{MCD}(a, \mathrm{MCD}(b, c))$. Poiché $d \mid b$ e $d \mid c$, allora, $d \mid \mathrm{MCD}(b, c)$ e, quindi $d \mid \tilde{d} = \mathrm{MCD}(a, \mathrm{MCD}(b, c))$. Viceversa, poché $\tilde{d}$ divide a, b, c, allora $\tilde{d} \mid d = \mathrm{MCD}(a, b, c)$. Dunque, $d = \pm\tilde{d}$.
(b) Segue dal fatto che $1 \mid a$ e se $x \mid 1$, allora $x = \pm 1$.
(c) Sia $t := \mathrm{MCD}(b, c)$ e $\tilde{t} := \mathrm{MCD}(ab, ac)$. E' ovvio che $at \mid ab$ e $at \mid ac$, quindi $at \mid \mathrm{MCD}(ab, ac) = \tilde{t}$. Poiché $a \mid \mathrm{MCD}(ab, ac) = \tilde{t}$ allora $\tilde{t} = ax$, per un qualche intero x. D'altra parte sappiamo che $at \mid \tilde{t} = ax$, quindi $t \mid x$. Inoltre $ax = \tilde{t} \mid ab$ e $ax = \tilde{t} \mid ac$, quindi $x \mid b$ e $x \mid c$, dunque $x \mid \mathrm{MCD}(b, c) = t$. Pertanto $x = \pm t$, ovvero $\tilde{t} = \pm at$.
(d) Da **(c)** ricaviamo che $d = \mathrm{MCD}(a, b) = \mathrm{MCD}(d\frac{a}{d}, d\frac{b}{d}) = d\mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$, quindi $1 = \mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$.
(e) Per l'identità di Bézout, esistono $x, y, u, v \in \mathbb{Z}$ in modo tale che $ax + by = 1 = au + cv$. Quindi $1 = (ax + by)(au + cv) = a(axu + byu + cvx) + bc(yv) = a(u + cvx) + bc(yv)$, da cui si ricava che $1 = \mathrm{MCD}(a, bc)$ (Teorema 2.3).
(f) Poiché $a \mid c$, allora $ab \mid cb$. Analogamente si prova che $ab \mid ac$. Dunque $ab \mid \mathrm{MCD}(cb, ca) = c\mathrm{MCD}(b, a) = c$.]

2.3. Algoritmo euclideo delle divisioni successive (metodo algoritmico per il calcolo del MCD di due elementi in $\mathbb{Z}$). Siano a e b due interi non nulli di $\mathbb{Z}$ dei quali si vuole calcolare il MCD. Dal momento che $\mathrm{MCD}(a,b) = \mathrm{MCD}(|\,a\,|, |\,b\,|)$, allora possiamo supporre, senza perdere in generalità che $a \geqslant b > 0$. Applicando ricorsivamente l'Algoritmo di divisione abbiamo:

$$\begin{array}{ll}
a = bq_1 + r_1\,, & 0 < r_1 < b =: r_0 \\
b = r_1 q_2 + r_2\,, & 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3\,, & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_k = r_{k+1} q_{k+2} + r_{k+2}\,, & 0 < r_{k+2} < r_{k+1} \\
\vdots & \vdots \\
r_{n-2} = r_{n-1} q_n + r_n\,, & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} + 0\,, & 0 = r_{n+1} < r_n
\end{array}$$

dove $n \geqslant 0$.
Mostrare che:

(a) $\mathrm{MCD}(a,b) = r_n$.

(b) $r_n = ax_n + by_n$ (Identità di Bézout)
dove x_n e y_n in $\mathbb{Z}$ sono calcolabili ricorsivamente tramite le seguenti formule:

$$\begin{array}{ll}
x_0 := 0 & y_0 := 1 \\
x_1 := 1 & y_1 := -q_1 \\
\vdots & \vdots \\
x_k := x_{k-2} - q_k x_{k-1} & y_k := y_{k-2} - q_k y_{k-1}\,, \quad \text{per ogni } k \geqslant 2.
\end{array}$$

[Suggerimento. **(a)** Osserviamo che se $a = bq + r$, con $0 \leqslant r < b$, allora $\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r)$. Infatti l'insieme dei divisori comuni di a e b coincide con l'insieme dei divisori comuni di b ed $r = a - bq$ e quindi, ovviamente, il "massimo" elemento del primo insieme coincide con il "massimo" elemento del secondo insieme. Applicando ricorsivamente questa proprietà alla successione di divisioni euclidee, abbiamo $\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r_1) = \mathrm{MCD}(r_1,r_2) = \ldots = \mathrm{MCD}(r_{n-1},r_n) = r_n$.

(b) Per induzione. Base dell'induzione:

$$\begin{array}{ll}
n = 0\,: & r_0 := b = a \cdot 0 + b \cdot 1 \;\Rightarrow\; x_0 = 0\,,\; y_0 = 1\,. \\
n = 1\,: & r_1 = a \cdot 1 - bq_1 \;\Rightarrow\; x_1 = 1\,,\; y_1 = -q_1\,.
\end{array}$$

Passo induttivo. Supponiamo che, per ogni h, con $0 \leqslant h \leqslant k$, con $k \geqslant 1$, si abbia $r_h = ax_h + by_h$. Poiché:

$$r_{k-1} = r_k q_{k+1} + r_{k+1}\,, \quad \text{cioè } r_{k+1} = r_{k-1} - r_k q_{k+1}\,,$$

allora l'espressione di r_{k+1}, come combinazione lineare di a e b, può essere calcolata ricorsivamente:

$$\begin{array}{rl}
r_{k+1} = & r_{k-1} - r_k q_{k+1} = ax_{k-1} + by_{k-1} - (ax_k + by_k)q_{k+1} = \\
= & a(x_{k-1} - q_{k+1}x_k) + b(y_{k-1} - q_{k+1}y_k)\,.\,]
\end{array}$$

2.4. Siano a e b due interi non nulli di $\mathbb{Z}$. Utilizziamo le notazioni dell'Esercizio 2.3. Per il calcolo del MCD(a,b), abbiamo già osservato che non è restrittivo supporre che $a > b > 0$. Definiamo *lunghezza* $\lambda(a,b)$ *dell'algoritmo euclideo della coppia* (a,b) il numero $n+1$ di divisioni necessarie per ottenere un resto $r_{n+1} = 0$. Definiamo *lunghezza euclidea di* a, $\boldsymbol{\lambda}(a)$, il massimo valore raggiunto da $\lambda(a,b)$, al variare di b, con $a > b > 0$, i.e.

$$\boldsymbol{\lambda}(a) := \mathrm{Max}\{\lambda(a,b) \ : \ \ b \in \mathbb{N}\,, \ \ a > b > 0\}\,.$$

(a) Mostrare che: $\boldsymbol{\lambda}(a) = 1 \ \Leftrightarrow \ \ a = 2\,.$

(b) Calcolare $\boldsymbol{\lambda}(a)$ per tutti gli interi a, con $2 \le a \le 8\,.$

La successione di Fibonacci è la successione di numeri naturali definita induttivamente nella maniera seguente:

$$u_0 := 1\,, \ \ u_1 := 1\,, \quad u_n := u_{n-1} + u_{n-2}\,, \quad \text{per ogni } n \ge 2\,.$$

Dunque, $u_2 := 2\,, u_3 := 3\,, u_4 := 5\,, u_6 := 8\,, u_7 := 13\,, \ldots$.

(c) Mostrare che MCD$(u_{n+1}, u_n) = 1$ e che $\lambda(u_{n+1}, u_n) = n$, per ogni $n \ge 1$.

Date due coppie di interi positivi $(a,b)\,, \ (a',b')$ con $a > b$ e $a' > b'$, diremo che (a,b) *precede* (a',b') se $\lambda(a,b) \le \lambda(a',b')$.

(d) Fissato $n \ge 1$, mostrare che (u_{n+1}, u_n) precede tutte le coppie $(a,b)\,,$ con $a > b\,,$ tali che $\lambda(a,b) = n\,.$

(e) (**Teorema di Lamé,** 1845) Mostrare che: $\boldsymbol{\lambda}(u_{n+1}) = n$ *e, se* $\boldsymbol{\lambda}(a) = n$, *allora* $a \ge u_{n+1}\,.$

(f) Mostrare che $\lambda(a,b) \le 2\log_2(b) + 1$.

Osservare che la stima della lunghezza dell'algoritmo euclideo, data in **(f)**, è collegata al numero delle cifre, $\boldsymbol{cf}_2(b)$, del numero b nella sua scrittura in base 2 (ad esempio, se $b = 8 = (1000)_2$, $\boldsymbol{cf}_2(8) = 4$, $\log_2(8) = 3$). Infatti, per ogni $b \ge 1$, $\log_2(b) < \boldsymbol{cf}_2(b)$.

(g) Mostrare che $\boldsymbol{\lambda}(a) < 2\boldsymbol{cf}_2(a) + 1$.

(h) Mostrare per induzione su $n \ge 1$ che:

$$u_n \le \left(\frac{7}{4}\right)^{n+1}\,.$$

Per ottenere una migliore approssimazione del valore di u_n, abbiamo bisogno di richiamare la nozione di numero aureo. Ricordiamo che il *rapporto aureo tra due lunghezze* era quella proporzione giudicata la più armoniosa secondo i canoni estetici classici tra le lunghezze a e b dei lati di un rettangolo e si ha quando $a > b$ e

$$\frac{a}{b} = \frac{a+b}{a} \quad \text{ovvero} \quad \frac{a}{b} = \frac{1+\sqrt{5}}{2} =: \omega\,,$$

(si noti che il numero reale ω (≈ 1.61803), detto *numero aureo,* è una delle due radici reali dell'equazione $X^2 - X - 1 = 0\,,$ equazione determinata dalla relazione di rapporto aureo; l'altra soluzione è $\overline{\omega} := \frac{1-\sqrt{5}}{2}$ (≈ -0.618034)).

(i) Mostrare per induzione su $n \ge 0$ che:

$$u_n = \frac{\omega^{n+1} - \overline{\omega}^{n+1}}{\sqrt{5}}\,.$$

(j) Dedurre dal punto precedente che, per ogni $n \geq 1$,

$$\left| u_n - \frac{\omega^{n+1}}{\sqrt{5}} \right| \; < \; \frac{1}{2} \, ,$$

dunque u_n è l'intero più prossimo al numero reale $\frac{\omega^{n+1}}{\sqrt{5}}$ e quindi:

$$u_n \gtrapprox \frac{\omega^{n+1}}{\sqrt{5}} \, .$$

(k) Sia a un intero positivo, denotiamo con $\boldsymbol{cf}_{10}(a)$ il numero delle cifre di a nella sua scrittura decimale (ad esempio, se $a = 9705$ allora $\boldsymbol{cf}_{10}(a) = 4$). Mostrare che:

$$\begin{aligned} \boldsymbol{\lambda}(a) \lessapprox \log_\omega(a) + \tfrac{1}{2}\log_\omega(5) - 2 &\approx \log_\omega(a) - 0.327724 \; \approx \\ &\approx 4.78497 \cdot \mathrm{Log}(a) - 0.327724 \; < \; 5\boldsymbol{cf}_{10}(a) \, . \end{aligned}$$

[Suggerimento. **(a, $\Leftarrow$)** Se $a = 2$, allora $b = 1$, quindi $a = 2b + 0$, cioè, in questo caso, $r_1 = 0$, dunque $\boldsymbol{\lambda}(a) = 1$.
(a, $\Rightarrow$) Se, per assurdo, $a > 2$, prendiamo $b := a - 1$, allora:

$$a = b \cdot 1 + 1 \, , \qquad b = 1 \cdot b + 0 \, ,$$

dunque $\boldsymbol{\lambda}(a) \geq \lambda(a, a-1) = 2$.
(b) $\boldsymbol{\lambda}(3) = \boldsymbol{\lambda}(4) = \boldsymbol{\lambda}(6) = 2 \, ; \quad \boldsymbol{\lambda}(5) = \boldsymbol{\lambda}(7) = 3 \, ; \quad \boldsymbol{\lambda}(8) = 4 \; (= \lambda(8,5)) \, .$
(c) Dalla definizione stessa dei numeri di Fibonacci abbiamo che:

$$\begin{array}{ll} u_{n+1} = u_n \cdot 1 + u_{n-1} \, , & 0 < u_{n-1} < u_n \\ u_n = u_{n-1} \cdot 1 + u_{n-2} \, , & 0 < u_{n-2} < u_{n-1} \\ \vdots & \vdots \\ u_3 = u_2 \cdot 1 + u_1 \, , & 0 < 1 = u_1 < u_2 \\ u_2 = u_1 \cdot 2 + 0 \, . & \end{array}$$

(d) Per minimalizzare il valore di a, in un algoritmo euclideo che conta n divisioni con il resto, dobbiamo prendere gli interi $q_1, \; q_2, \; \ldots, q_n$ ed r_{n-1} il più piccoli possibile e, poi, ricavare attraverso le equazioni dell'algoritmo i valori di $r_{n-2}, \; r_{n-1}, \; \ldots, r_1, \; b, \; a$. Poiché $q_1, \; q_2, \; \ldots, q_{n-1} \geq 1$ e $q_n \geq 2$ (dal momento che $q_n r_{n-1} = r_{n-2} > r_{n-1}$) ed, inoltre, $r_{n-1} \geq 1$ (dal momento che $r_{n-1} > r_n = 0$), allora prendendo esattamente $q_1 = q_2 = \ldots = q_{n-1} = 1 \, , \;\; q_n = 2 \;\; \text{e} \;\; r_{n-1} = 1 \, ,$ otteniamo proprio che a deve coincidere con u_{n+1} (in tal caso, poi, $b = u_n$).
(e) Se $u_{n+1} \geq a > b > 0$ e se $\lambda(a,b) = m$ allora, per il punto (d), $a \geq u_{m+1}$ e quindi $u_{n+1} \geq u_{m+1}$. Pertanto $m \leq n$, dunque $\boldsymbol{\lambda}(a) \leq n$. In particolare, per $a = u_{n+1}$, ricaviamo $\boldsymbol{\lambda}(u_{n+1}) \leq n$. Quindi, utilizzando (c), concludiamo che $\boldsymbol{\lambda}(u_{n+1}) = n$.
(f) Supponiamo che $\lambda(a,b) = n + 1$. E' subito visto che $r_{-1} := a > 2r_1$ e $r_0 := b > 2r_2$. In generale, $r_{k-2} > 2r_k$, per ogni k, con $1 \leq k \leq n$. Pertanto, se n è pari, allora $b > 2^{\frac{n}{2}}$; se n è dispari, allora $b > 2^{\frac{n-1}{2}}$. In ogni caso, $b > 2^{\frac{n-1}{2}}$, dunque $\log_2(b) > \frac{n-1}{2}$. Pertanto, $2\log_2(b) + 1 > n$, quindi $2\log_2(b) + 1 \geq n + 1 = \lambda(a,b)$.
(g) è una conseguenza immediata di (f), dal momento che $a > b$ e, quindi, $\log_2(a) > \log_2(b)$.

(h) Per $n = 0,\ 1,\ 2$ la disuguaglianza è banalmente verificata:

$$\begin{array}{rl} u_0 = & 1 = (\frac{7}{4})^0 \\ u_1 = & 1 < (\frac{7}{4})^1 = 1.75 \\ u_2 = & 2 < (\frac{7}{4})^2 \approx 3.0625\,. \end{array}$$

Sia $n \geq 3$, applicando l'ipotesi induttiva ai casi $n-1$ ed $n-2$, allora possiamo concludere:

$$u_n = u_{n-1} + u_{n-2} < \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2} = \left(\frac{7}{4}\right)^{n-2}\left(\frac{7}{4}+1\right) < \left(\frac{7}{4}\right)^{n-2}\left(\frac{7}{4}\right)^{2}\,.$$

(i) Per $n = 0$ e per $n = 1$ l'uguaglianza è banalmente verificata:

$$\begin{array}{rl} u_0 = & \frac{\omega - \overline{\omega}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 \\ u_1 = & \frac{\omega^2 - \overline{\omega}^2}{\sqrt{5}} = \\ = & \frac{\omega+1-(\overline{\omega}+1)}{\sqrt{5}} = 1 \end{array}$$

(si ricordi che $\omega^2 - \omega - 1 = 0 = \overline{\omega}^2 - \overline{\omega} - 1$). Supponiamo, per ipotesi induttiva che, per $n \geq 2$, $u_{n-1} = \frac{\omega^n - \overline{\omega}^n}{\sqrt{5}}$ e $u_{n-2} = \frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\sqrt{5}}$. Allora:

$$\begin{array}{rl} u_n = u_{n-1} + u_{n-2} = & \frac{\omega^n - \overline{\omega}^n}{\sqrt{5}} + \frac{\omega^{n-1} - \overline{\omega}^{n-1}}{\sqrt{5}} = \\ = & \frac{\omega^{n-1}(\omega+1) - \overline{\omega}^{n-1}(\overline{\omega}+1)}{\sqrt{5}} = \frac{\omega^{n+1} - \overline{\omega}^{n+1}}{\sqrt{5}}\,. \end{array}$$

(j) Basta osservare che, per ogni $n \geq 1$,

$$\left|\frac{\overline{\omega}^n}{\sqrt{5}}\right| \ < \ \left|\frac{\overline{\omega}}{\sqrt{5}}\right| \ \approx 0.276393 \ < \ \frac{1}{2}\,.$$

(k) Se $n = \boldsymbol{\lambda}(a)$ allora $a \geq u_{n+1} \gtrapprox \frac{\omega^{n+2}}{\sqrt{5}}$, dunque:

$$\log_\omega(a) \gtrapprox n + 2 - \log_\omega(\sqrt{5}) \quad \Rightarrow \quad n \ \lessapprox \ \log_\omega(a) + \frac{1}{2}\log_\omega(5) - 2\,.$$

La conclusione discende dal momento che $\log_\omega(5) \approx 3.34455$, $\frac{1}{2}\log_\omega(5) - 2 \approx -0.327724$, $\log_\omega(a) = \mathrm{Log}(a)/\mathrm{Log}(\omega) \approx 4.78497 \cdot \mathrm{Log}(a)$, $\mathrm{Log}(a) \ < \ \boldsymbol{cf}_{10}(a)$.]

2.5. Siano a e b due interi non nulli di $\mathbb{Z}$ e sia $d := \mathrm{MCD}(a,b)$.

(a) Mostrare che, nell'espressione $d = ax + by$, nota come Identità di Bézout, la coppia di interi $x, y \in \mathbb{Z}$ non è univocamente determinata (mostrare con un esempio esplicito, ad esempio $a = 4,\ b = 6,\ d = 2$, che possono esistere due coppie distinte di interi (x,y) e (x',y') in modo tale che $d = ax + by = ax' + by'$).

(b) Siano $x_0, y_0 \in \mathbb{Z}$ tali che $ax_0 + by_0 = 1$. Preso comunque $n \in \mathbb{Z}$, poniamo $x_n := x_0 + nb$ e $y_n := y_0 - na$. Verificare che, per ogni $n \in \mathbb{Z}$, risulta $ax_n + by_n = 1$.

(c) Mostrare che, se $ax_0 + by_0 = 1 = ax + by$, con $x_0, y_0, x, y \in \mathbb{Z}$, allora esiste un intero $n \in \mathbb{Z}$ in modo tale che $x = x_0 + nb$ e $y = y_0 - na$.

(d) Mostrare che, se $ax_0 + by_0 = d = ax + by$ con $x_0, y_0, x, y \in \mathbb{Z}$, allora esiste un intero $n \in \mathbb{Z}$ in modo tale che $x = x_0 + n\frac{\mathrm{mcm}(a,b)}{a}$ e $y = y_0 - n\frac{\mathrm{mcm}(a,b)}{b}$.

[Suggerimento. **(a)** Basta prendere, ad esempio, $(x, y) = (-1, 1)$ e $(x', y') = (2, -1)$.
(b) $ax_n + by_n = a(x_0 + nb) + b(y_0 - na) = ax_0 + by_0 = 1$.
(c) Se $ax_0 + by_0 = 1$, allora $\mathrm{MCD}(a, b) = 1$ (Teorema 2.3). Da $ax_0 + by_0 = 1 = ax + by$, ricaviamo che $a(x - x_0) = b(y_0 - y)$, cioè $a \mid b(y_0 - y)$, quindi $a \mid y_0 - y$. Se poniamo $n := \frac{(y_0 - y)}{a}$ allora abbiamo $x = x_0 + nb$ e $y = y_0 - na$.
(d) Poiché

$$a\frac{x_0}{d} + b\frac{y_0}{d} = 1 = a\frac{x}{d} + b\frac{y}{d}\,,$$

allora, per **(c)**, $x = x_0 + n\frac{b}{d}$ e $y = y_0 - n\frac{a}{d}$. Per concludere basta ricordare che:

$$\mathrm{mcm}(a, b) = \mathrm{mcm}(a, b)\frac{\mathrm{MCD}(a, b)}{d} = \frac{ab}{d}\,.\ ]$$

2.6. Mostrare la validità della seguente variante dell'algoritmo euclideo di divisione (Teorema 2.1):
Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora, esistono e sono univocamente determinati due interi $q, r \in \mathbb{Z}$ in modo tale che:

$$a = bq + r\,, \qquad -\frac{1}{2} \mid b \mid \leqslant r < \frac{1}{2} \mid b \mid\,.$$

[Suggerimento. Sappiamo (Teorema 2.1) che esistono e sono univocamente determinati due interi $q, r \in \mathbb{Z}$ in modo tale che $a = bq + r$, con $0 \leqslant r <\mid b \mid$. Se $(0 \leqslant)\ r < \frac{1}{2} \mid b \mid$, allora non c'è null'altro da dimostrare. Supponiamo, dunque, che $\frac{1}{2} \mid b \mid \leqslant r\ (<\mid b \mid)$. In tal caso, $0 <\mid b \mid - r \leqslant \mid b \mid - \frac{1}{2} \mid b \mid = \frac{1}{2} \mid b \mid \leqslant r <\mid b \mid$. Scriviamo $r = (\mid b \mid - r) + r'$, con $r' := 2r - \mid b \mid$. Dunque, per un'opportuna scelta del segno (dipendente dal segno di $\mid b \mid$), abbiamo $a = qb + r = (q \pm 1)b + (r' - r)$. Se poniamo $q'' := q \pm 1$ e $r'' := r' - r = r - \mid b \mid$, allora abbiamo $a = q''b + r''$, con $q'', r'' \in \mathbb{Z}$ ed, inoltre, $-\frac{1}{2} \mid b \mid \leqslant r'' < 0$. Si vede facilmente che q'' e r'' sono univocamente determinati perché q ed r (da cui sono dedotti) sono univocamente determinati.
Si noti che, utilizzando tale versione dell'algoritmo di divisione, si ottiene una versione modificata dell'algoritmo euclideo delle divisioni successive (Esercizio 2.3; nel caso attuale $\frac{-|r_k|}{2} \leq r_{k+1} < \frac{|r_k|}{2}$) che tende ad arrestarsi più rapidamente del tradizionale algoritmo euclideo, dal momento che i resti si avvicinano più rapidamente allo zero.]

2.7. Siano $a, b \in \mathbb{Z} \setminus \{0, 1, -1\}$ due interi dei quali sia nota la fattorizzazione in numeri primi:

$$a = \pm p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r} \quad \text{e} \quad b \pm p_1^{f_1} p_2^{f_2} \ldots p_r^{f_r}$$

con $e_i \geqslant 0$ e $f_i \geqslant 0$, per ogni $1 \leqslant i \leqslant r$ (ammettendo, come abbiamo fatto ora, che alcuni esponenti possano essere uguali a 0, possiamo assumere che i fattori primi che appaiono nella decomposizione di a e di b siano gli stessi (!), senza per questo perdere di generalità). Mostrare che:

(a) $\mathrm{MCD}(a, b) = p_1^{u_1} p_2^{u_2} \ldots p_r^{u_r}$, dove $u_i := \mathrm{Min}(e_i, f_i)$, per ogni $1 \leqslant i \leqslant r$.

(b) $\mathrm{mcm}(a, b) = p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r}$, dove $v_i := \mathrm{Max}(e_i, f_i)$, per ogni $1 \leqslant i \leqslant r$.

[Suggerimento. **(a)** Se p è un divisore primo di a e di b allora, necessariamente, $p = p_i$, per un qualche i, con $1 \leqslant i \leqslant r$. Pertanto un divisore comune t di a e b ha una decomposizione in numeri primi del tipo $t = p_1^{\tau_1} p_2^{\tau_2} \dots p_r^{\tau_r}$, con $\tau_i \leq u_i$, per ogni i. Pertanto il massimo di questi divisori comuni di a e b è dato da $d = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$.

(b) Se m è un multiplo comune di a e b, allora $p_i^{v_i} \mid m$, per ogni i, con $1 \leqslant i \leqslant r$. Quindi $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r} \mid m$. Pertanto il minimo tra questi multipli comuni di a e b è proprio $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$.]

2.8. **(a)** **(Euclide,** IV–III Sec. A.C.**)**. Mostare che esistono infiniti interi primi.

(b) Dimostare che, preso comunque un intero $N > 0$ (grande come si vuole), è possibile trovare N interi consecutivi, nessuno dei quali è primo.

(c) Mostrare che, per ogni intero $n > 0$, esiste sempre un primo p in modo tale che $n < p \leqslant n! + 1$.

[Suggerimento. **(a)** Per assurdo sia $\{p_1, p_2, \dots, p_N\}$ l'insieme (finito) di tutti i numeri primi. L'intero positivo $n := p_1 p_2 \dots p_N + 1$ ($> p_i$, per ogni $1 \leqslant i \leqslant N$), come ogni intero non primo, deve possedere un fattore primo. Dunque, deve esistere j, con $1 \leqslant j \leqslant N$, in modo tale che $p_j \mid n = p_1 p_2 \dots p_N + 1$. Poiché, ovviamente, $p_j \mid p_1 p_2 \dots p_N$, allora $p_j \mid 1 = n - p_1 p_2 \dots p_N$. Si perviene così ad un assurdo.
(b) Basta considerare i seguenti N interi consecutivi:

$$(N+1)! + 2\,,\ (N+1)! + 3\,,\ (N+1)! + 4\,,\ \dots\dots\,, (N+1)! + N + 1\,,$$

e notare che $k \mid (N+1)! + k$, per ogni $2 \leqslant k \leqslant N + 1$.
(c) Se p è un numero primo e se $p \leqslant n$ allora ovviamente $p \mid n!$ (dunque, $p \nmid n! + 1$). Pertanto, se q è un fattore primo di $n! + 1$, allora $n < q \leqslant n! + 1$.]

2.9. Utilizzare le proprietà dei numeri primi ed il Teorema Fondamentale della Aritmetica per dimostrare:

(a) **(Pitagora,** VI Sec. A.C.**)** $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. (Con un argomento simile si dimostri che, più generalmente, $\sqrt{p} \in \mathbb{R} \setminus \mathbb{Q}$, per ogni numero primo p.)

(b) Presi $n, r \in \mathbb{N}$, con $\sqrt[r]{n}$ non intero, allora $\sqrt[r]{n} \in \mathbb{R} \setminus \mathbb{Q}$.

(c) $\mathrm{Log}_{10}(2) \in \mathbb{R} \setminus \mathbb{Q}$.

[Suggerimento. **(a)** Per assurdo, se $\sqrt{p} \in \mathbb{Q}$, allora $b^2 p = a^2$ per una qualche coppia di interi $a, b \in \mathbb{Z}$, con $b \neq 0$ e $\mathrm{MCD}(a, b) = 1$. Da cui ricaviamo che $p \mid a^2$, dunque $p \mid a$. Pertanto $pk = a$, per un qualche $k \in \mathbb{Z}$. Quindi $b^2 p = a^2 = p^2 k^2$, cioè $b^2 = pk^2$, dunque $p \mid b$. Questo contraddice il fatto che $\mathrm{MCD}(a, b) = 1$.
La dimostrazione di **(b)** è del tutto simile a quella di **(a)**.
(c) Per assurdo, se $\mathrm{Log}_{10}(2) \in \mathbb{Q}$, allora $b\mathrm{Log}_{10}(2) = a$, per una qualche coppia di interi $a, b \in \mathbb{N}$, con $b \neq 0$ e $\mathrm{MCD}(a, b) = 1$. Dunque, $2^b = 10^a = 2^a 5^a$. Per il Teorema Fondamentale dell'Aritmetica deve essere $b = a$ ed $a = 0$, perveniamo così ad una contraddizione.]