NOTE DI ALGEBRA E GEOMETRIA (CORSO PAS 2014)

Indice

1. Gli interi

1.1. **Analisi combinatoria.** In questo paragrafo vogliamo *contare* gli elementi di certi insiemi. Rinviamo al corso di *Probabilità e Statistica* per eventuali approfondimenti.

Siano $A = \{x_1, x_2, \ldots, x_k\}$ e $B = \{y_1, y_2, \ldots, y_n\}$ due insiemi finiti.

1. Gli elementi del prodotto cartesiano $A \times B$ sono $n \cdot k$. Infatti ci sono n coppie ordinate del tipo $(x_1, \cdot)$, n del tipo $(x_2, \cdot)$... n del tipo $(x_k, \cdot)$. Tutte queste coppie sono distinte e sono $n \cdot k$.

2. Le applicazioni da A in B sono n^k. Infatti si hanno n scelte per il valore di $f(x_1)$; per ciascuna di queste abbiamo ancora n scelte per $f(x_2)$, sino ad arrivare a n scelte per $f(x_k)$. Si possono quindi fare $n \cdot n \cdot \cdots \cdot n$ (k fattori) scelte, ed ogni scelta dà luogo ad una diversa applicazione.

Esercizio 1. Scrivere tutte le applicazioni nel caso $k = 2$ e $n = 3$ e verificare che sono $3^2 = 9$.

3. Se $k \leq n$, le applicazioni iniettive di A in B sono $n(n-1)(n-2)\cdots(n-k+1)$. Infatti gli elementi $f(x_1), \ldots, f(x_k)$ devono essere distinti e quindi, fatta la prima scelta $f(x_1)$ arbitraria (n possibilità) rimangono $n-1$ scelte possibili per $f(x_2)$, $n-2$ per $f(x_3)$ sino ad arrivare a $n-k+1$ scelte per $f(x_k)$.

Esercizio 2. Individuare nelle applicazioni dell'esercizio precedente quelle iniettive e verificare che sono in numero di $3 \cdot 2 = 6$

4. Le applicazioni iniettive da A in sè ($A = B$, $k = n$) sono anche suriettive e quindi anche bigezioni. Infatti le immagini $f(x_1), \ldots, f(x_n)$ sono tutte distinte e quindi esaurisocno l'insieme B. Usando la formula precedente si ottiene che il numero delle applicazioni iniettive da A in sè (che è anche il numero delle applicazioni suriettive o di quelle bigettive) è uguale a $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$. Indicheremo questo numero con $n!$ e lo chiameremo il *fattoriale* di n. Le bigezioni di A in sè si chiamano anche *permutazioni* di A. Se per esempio A è costituito da tre elementi di trovano 6 permutazioni. Il lettore è invitato a scrivere esplicitamente le 6 permutazioni.

5. Se $k \leq n$, ci proponiamo di contare il numero m di sottoinsiemi di B che contengono precisamente k elementi. Equivalentemente, vogliamo calcolare il numero m degli elementi dell'insieme $\mathcal{C} \subset P(B)$ ($P(B)$ denota l'insieme delle parti di B) costituito da tutti i sottoinsiemi di B che contengono k elementi, cioè $C \in \mathcal{C}$ se e solo se $C \subset B$ e C contiene k elementi. Sia $K = \{1, 2, \ldots, k\}$. Ogni applicazione iniettiva $f : K \to B$ ha per immagine un certo $C \in \mathcal{C}$, cioè $f(K) = C$. D'altra parte, dato $C \in \mathcal{C}$, le applicazioni iniettive da K in C sono $k!$ (per 4.). Quindi il numero delle applicazioni iniettive da K a B è $m \cdot k!$. Quindi per 3. si ottiene

$$m = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

e tale numero si indica con $\binom{n}{k}$.

Esercizio 3. Calcolare $\binom{6}{3}$ e verificare il risultato costruendo tutti i sottoinsiemi di $\{1, 2, 3, 4, 5, 6\}$ costituiti da 3 elementi.

Osservazione 1.1. Si attribuisce un valore anche a $k!$ e a $\binom{n}{k}$ anche quando $k = 0$, ponendo $0! = 1$ e $\binom{n}{0} = 1$. Questo è conforme al fatto che ogni insieme contiene uno ed un solo insieme con 0 elementi cioè $\emptyset$.

Un numero del tipo $\binom{n}{k}$ si dice *coefficiente binomiale* ed i sottoinsiemi di k elementi di un insieme di n elementi $k \leq n$ si dicono *combinazioni semplici* di n oggetti a k a k. Si ha

$\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1}$, $\binom{n}{2} = \binom{n}{n-2}$ e, in generale,

$$\binom{n}{k} = \binom{n}{n-k}$$

perchè nella formula che definisce $\binom{n}{k}$ sostituire k a $n-k$ equivale allo scambio dei due fattori al denominatore.

Vale la seguente formula:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},\ 1 \leq k < n. \tag{1}$$

La si può ottenere meccanicamente usando la formula che definisce $\binom{n}{k}$ (verificare). Oppure usando il significato del coefficiente binomiale. Infatti i sottoinsiemi con k elementi di un insieme con $B = \{x_1, x_2, \dots x_n\}$ con n elementi si possono calcolare come segue. Sia $x_1 \in B$. Allora i sottoinsiemi di B che contengono k elementi si ripartiscono in due classi: (a) quelli che non contengono x_1 il cui numero è pari ai sottoinsiemi di $\{x_2, \dots x_n\}$ che hanno k elementi, cioè a $\binom{n-1}{k}$, (b) quelli che contengono x_1 il cui numero è pari ai sottoinsiemi di $\{x_2, \dots x_n\}$ che hanno $k-1$ elementi, cioè a $\binom{n-1}{k-1}$.

La formula (1) fornisce un modo per costruire i coefficienti binomiali di $\binom{n}{k}$ a partire da $\binom{n-1}{k}$ e $\binom{n-1}{k-1}$ ed è alla base della costruzione del triangolo di Tartaglia (Pascal per i francesi).

6. Mostriamo infine che l'insieme delle parti di $A = \{x_1, \dots, x_k\}$ contiene 2^k elementi. Per fare ciò consideriamo l'insieme $D = \{0, 1\}$. Vogliamo mostrare che tutte le applicazioni da A in D sono in corrispondenza biunivoca con l'insieme delle parti di A. Infatti data un'applicazione $f : A \to D$ la controimmagine $f^{-1}(1)$ è un sottoinsieme di A. Viceversa, ogni sottoinsieme $U \subset A$ è controimmagine del punto 1 tramite *una e una sola* applicazione $f : A \to D$, definita da $f(x) = 1$, se $x \in U$ e $f(x) = 0$ se $x \notin U$. Quindi $P(A)$ contiene tanti elementi quante le applicazioni da A in D che sono 2^k (come segue da 2.).

Quindi per contare i sottoinsiemi di un insieme con n elementi possiamo anche sommare il numero $\binom{n}{k}$ di quelli contengono k elementi per $k = 0, 1, \dots, n-1, n$. Si ottiene quindi la relazione:

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n. \tag{2}$$

1.2. **Induzione.** Dalle scuole inferiori sappiamo cosa sono i numeri interi

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

e sappiamo che si possono sommare e moltiplicare tra loro. Inoltre possiamo dire quando due numeri interi sono uno più piccolo dell'altro. I numeri interi maggiori o uguale a zero sono chiamati i numeri naturali. L'insieme dei numeri naturali verrà indicato con $\mathbb{N}$.

Una proprietà importante dei numeri naturali è il seguente:

Assioma del buon ordinamento. *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *possiede un elemento minimo.*

In altre parole se $S \subset \mathbb{N}$, $S \neq \emptyset$, allora esiste $n_0 \in \mathbb{N}$ tale che $n_0 \leq s$ per ogni $s \in S$.

Come conseguenza dell'assioma del buon ordinamento otteniamo il seguente risultato.

Teorema 1.2. *(prima forma del principio di induzione) Consideriamo, per ogni numero naturale* n*, un'asserzione* $A(n)$ *ad esso associata, e supponiamo di sapere che:*

(1) $A(0)$ *è vera;*

(2) per ogni $n \in \mathbb{N}$*, supposta vera* $A(n)$*, ne segue che è vera* $A(n+1)$*.*

Allora l'asserzione $A(n)$ *è vera per ogni* $n \in \mathbb{N}$*.*

Dimostrazione. Sia S l'insieme dei numeri naturali per i quali l'asserzione non è vera:

$$S = \{x \in \mathbb{N} \mid A(x) \text{ è falsa}\}.$$

Vogliamo dimostrare che S è vuoto. Supponiamo, per assurdo, che S non sia vuoto e proviamo che ne segue una contraddizione. Sia dunque $S \neq \emptyset$. Allora per l'assioma del buon ordinamento, esiste $n_0 \in \mathbb{N}$ che è un minimo di S. Dunque $A(n_0)$ è falsa perchè $n_0 \in S$. Mentre $A(0)$ è vera per l'ipotesi (1). Allora $n_0 \neq 0$ e quindi $n_0 \geq 1$. Poichè n_0 è il minimo di S, $n_0 - 1 \notin S$ e perciò $A(n_0 - 1)$ è vera. Ma allora, per l'ipotesi (2), $A(n_0)$ è vera in quanto $(n_0 - 1) + 1 = n_0$. Quindi $A(n_0)$ sarebbe contemporaneamente vera e falsa, una contraddizione. Segue che $S = \emptyset$ come volevamo. □

Osservazione 1.3. L'assioma del buon ordinamento vale, ovviamente, anche se al posto di $\mathbb{N}$ si considera un qualunque sottoinsieme di numeri interi che sia limitato inferiormente. Quindi si sostituisce l'ipotesi (1) con l'ipotesi che $A(k)$ sia vera per un certo $k \geq 0$, allora la stessa dimostrazione del Teorema 1.2 mostra che $A(n)$ è vera per ogni $n \geq k$.

Esempio 1.4. *Sia* $A(n)$ *l'asserzione:* la somma dei primi n numeri naturali dispari è uguale ad n^2, cioè: $1 + 3 + \cdots + 2n - 1 = n^2$. *Infatti* $A(1)$ *è vera in quanto* $1 = 1^2$*. Supponiamo* $A(n)$ *sia vera e vogliamo dimostrare che* $A(n+1)$ *è vera. Osserviamo che la somma dei primi* $n+1$ *numeri dispari si ottiene aggiungendo* $2(n+1) - 1 = 2n + 1$ *alla somma dei primi* n *numeri dispari. Allora*

$$1 + 3 + \cdots + 2n - 1 + 2n + 1 = n^2 + 2n + 1 = (n+1)^2.$$

Ma questa è proprio l'asserzione $A(n+1)$*. Segue dal Teorema 1.2 che* $A(n)$ *è vera per ogni* $n \in \mathbb{N}$*.*

Teorema 1.5. *(seconda forma del principio di induzione) Consideriamo, per ogni numero naturale n, un'asserzione $A(n)$ ad esso associata, e supponiamo di sapere che:*

(1) $A(0)$ è vera;

(2) per ogni $n > 0$, se $A(k)$ è vera per ogni k tale che $0 \leq k < n$, allora anche $A(n)$ è vera.

Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Sia S l'insieme dei numeri naturali dove $A(s)$ è falsa. Supponiamo per assurdo che $S \neq \emptyset$ e sia n_0 il suo minimo. Allora $A(n_0)$ è falsa e quindi $n_0 > 0$ perchè per ipotesi $A(0)$ è vera. Mentre $A(k)$ è vera per ogni $k < n_0$ in quanto n_0 è il minimo di S. Ma allora per ipotesi $A(n_0)$ è vera, contraddizione. $\square$

Questa seconda forma del principio di induzione, fornisce un metodo di dimostrazione più potente rispetto al primo. Esistono casi dove si riesce usare la seconda forma ma non la prima come mostra la seguente proposizione.

Proposizione 1.6. *Siano m e n due numeri interi con $m > 0$ e $n \geq 0$. Allora esistono due interi $q, r \geq 0$ con $0 \leq r < m$ tali che $n = mq + r$.*

Dimostrazione. Applichiamo il principio di induzione nella seconda forma (rispetto a n). Se $n = 0$ basta porre $q = r = 0$ e quindi $A(0)$ è vera. Sia $n > 0$. Facciamo vedere che $A(n)$ segue dall'ipotesi che $A(k)$ sia vera per $0 \leq k < n$. Se $m > n$ basta porre $q = 0$, $r = n$. Se invece $m \leq n$ allora $0 \leq n - m < n$. Per l'ipotesi induttiva l'asserto $A(n-m)$ è vero e quindi esistono interi q_1, r_1 tali che $n - m = mq_1 + r_1$, $0 \leq r_1 < m$. Allora $n = m(q_1 + 1) + r_1$ e questa è proprio $A(n)$. Quindi per il Teorema 1.5 $A(n)$ vale per ogni $n \geq 0$. $\square$

Osservazione 1.7. Se cercassimo di dimostrare la proposizione usando il principio di induzione nella prima forma (Teorema 1.2), dovremo provare che $A(n)$ è vera sapendo che sia vera $A(n-1)$. Il problema è che da $n - 1 = mq_1 + r_1$ non è immediato ottenere $n = mq + r$.

Esercizio 4. Dimostrare la formula (2) usando l'induzione.

Esercizio 5. Dimostrare che $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\forall n \geq 1$.

Esercizio 6. Dimostrare che $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\forall n \geq 1$.

Esercizio 7. Dimostrare che $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} = (\sum_{k=1}^{n} k)^2$, $\forall n \geq 1$.

Esercizio 8. Dimostrare che $n! \geq 2^{n-1}$, $\forall n \geq 1$.

Esercizio 9. Dimostrare che $n^2 \geq 2n + 1$, $\forall n \geq 3$.

Esercizio 10. Dimostrare che $2^n \geq n^2$, $\forall n \geq 4$.

Esercizio 11. Dimostrare che $\sum_{k=1}^{n} \frac{1}{4k^2-1} = \frac{n}{2n+1}, \ \forall n \geq 1$.

Esercizio 12. Dimostrare che $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}, \ \forall n \in \mathbb{N}$.

Esercizio 13. Dimostriamo che tutti i numeri naturali sono uguali tra loro come segue. Consideriamo l'affermazione: se il massimo tra due numeri naturali è un numero naturale allora i due numeri sono uguali fra loro. Ossia se $a, b \in \mathbb{N}$ e $\max\{a, b\} = n \in \mathbb{N}$ allora $a = b$. Indichiamo con $A(n)$ la proposizione: *se* $a, b \in \mathbb{N}$ *e* $\max\{a, b\} = n$, *allora* $a = b$. Chiaramente $A(0)$ è vera. Supponiamo $A(n)$ sia vera e proviamo che allora è vera pure $A(n+1)$. Infatti, siano $a, b \in \mathbb{N}$ e $\max\{a, b\} = n+1$, allora $\max\{a-1, b-1\} = n$ e per l'ipotesi induttiva $a-1 = b-1$, da cui $a = b$. Quindi $A(n)$ è vera e per il principio di induzione (nella prima forma, Teorema 1.2) l'affermazione è dimostrata. Dove è l'errore?

1.3. **La divisione euclidea.** Il valore assoluto è quella applicazione da $\mathbb{Z}$ in $\mathbb{Z}$ che ad un numero x associa il numero $|x|$ definito ponendo: $|x| = x$ se $x \geq 0$ e $|x| = -x$ se $x < 0$. Segue che se $|x| = |y|$ allora $x = y$ oppure $x = -y$ e scriveremo anche $x = \pm y$. In particolare $|x| = 0$ se e solo se $x = 0$. Inoltre valgono le seguenti proprietà:

$$|x+y| \leq |x| + |y|, \ \forall x, y \in \mathbb{Z}; \tag{3}$$

$$|x \cdot y| = |x| \cdot |y|, \ \forall x, y \in \mathbb{Z}, \tag{4}$$

che si verificano controllando tutte le possibili scelte per x e y.

Nella Proposizione 1.6 abbiamo fatto vedere cosa significa dividere un numero naturale $n \geq 0$ per un numero naturale $m > 0$, cioè abbiamo trovato $q, r \geq 0$ tali che $n = mq + r$ e $0 \leq r < m$. In altre parole q è il multiplo del divisore m che differisce dal dividendo n il meno possibile.

In effetti possiamo estendere il risultato a tutti i numeri interi.

Teorema 1.8. *Siano* $a, b \in \mathbb{Z}$, $b \neq 0$. *Allora esistono due interi* q, r *tali che* $a = bq + r$, $0 \leq r < |b|$. *Gli interi* q *e* r *sono unici, nel senso che sono determinati univocamente dalle condizioni precedenti.*

Dimostrazione. Per dimostrare l'esistenza useremo l'assioma del buon ordinamento. Supponiamo b positivo, quindi $|b| = b$ e $b \geq 1$. Consideriamo l'insieme $S = \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\}$, cioè tutti i numeri naturali della forma $a - bx$ al variare di $x \in \mathbb{Z}$. Mostriamo che $S \neq \emptyset$, facendo vedere che $a - b(-|a|) = a + b|a|$ appartiene a S. Infatti, essendo $b \geq 1$ si ha $b|a| \geq |a|$ e $a + b|a| \geq a + |a| \geq 0$. Quindi S ammette minimo $r \geq 0$. Dal momento che $r \in S$ esisterà $q \in \mathbb{Z}$ tale che $r = a - bq$ e e quindi $a = bq + r$ con $r \geq 0$. Resta da dimostrare che $r < b$. Se, per assurdo $r \geq b$, allora si avrebbe

$$0 \leq r - b = a - bq - b = a - b(q-1) \in S$$

e $r-b<r$ contro l'ipotesi che r sia il minimo di S. Supponiamo ora che b sia negativo. Allora osservando che $a=(-b)(-q)+r$ e $|-b|=|b|$ il problema si riconduce al caso precedente, cioè si divide a per $-b$, si cambia segno al quoziente e si lascia inalterato il resto.

Per dimostrare l'unicità di q e r, supponiamo che esistano $q^{'}, r^{'}$ tali che

$$a=bq+r=bq^{'}+r^{'},\ 0\leq r,r^{'}<|b|. \tag{5}$$

Supponiamo, ad esempio che $r^{'}\geq r$ (il caso $r\geq r^{'}$ si ottiene in modo analogo). Allora $0\leq r^{'}-r=b(q-q^{'})$ e prendendo i valori assoluti si ottiene

$$|b||q-q^{'}|=|b(q-q^{'})|=r^{'}-r\leq r^{'}<|b|.$$

Quindi $|q-q^{'}|<1$ e quindi $q=q^{'}$. Sostituendo in (5) si ottiene $r=r^{'}$. □

Osservazione 1.9. Osserviamo che se si sostituisce il dividendo a con il suo opposto $-a$ non è detto che si ottenga $-q$ come quoziente. Ad esempio se prendiamo $a=13$, $b=6$ allora $13=6\cdot 2+1$ ($q=2$, $r=1$) mentre $-13=6\cdot(-3)+5$ ($q=-3$, $r=5$).

Dati due numeri interi a e b si dice che b *divide* a o anche che b è un *divisore* di a se esiste $c\in\mathbb{Z}$ tale che $a=bc$. In tal caso scriviamo $b|a$.

Proposizione 1.10. *Valgono i seguenti fatti:*

(1) $b|0$ *per ogni* $b\in Z$, *mentre* $0|b$ *solo se* $b=0$;
(2) $\pm 1|a$ *e* $\pm a|a$ *per ogni* $a\in\mathbb{Z}$;
(3) se $b|p$ *e* $b|q$, *allora* $b|hp+kq$ *per ogni scelta di* $h,k\in\mathbb{Z}$;
(4) se $b|p$ *e* $b|q$, *allora* $ab|pq$;
(5) se $b_1|b_2$ *e* $b_2|b_1$, *allora* $b_2=\pm b_1$.

Dimostrazione. dimostriamo solo la (5) (lasciando al lettore il compito di dimostrare le altre affermazioni). Se $b_1|b_2$ e $b_2|b_1$. Cioè $b_1=b_2c_2$ e $b_2=b_1c_1$. Sostituendo la seconda equazione nella prima otteniamo $b_1=b_1c_1c_2$, pertanto $c_1c_2=1$. Quindi $c_1=c_2=\pm 1$. Segue che $b_1=\pm b_2$.

□

Esercizio 14. Si provi, usando l'induzione su n che

$$|x_1+x_2+\cdots+x_n|\leq |x_1|+|x_2|+\cdots+|x_n|.$$

Esercizio 15. Si trovino il quoziente q e il resto r della divisione di $a=532$ per $b=-112$ e $a=-87$ e $b=33$.

Esercizio 16. Come cambiano il quoziente q e il resto r nelle divisione euclidea di a per b se sostituiamo a e b con i loro multipli ma e mb, dove $m\in\mathbb{Z}$?

1.4. **I numeri primi: nozioni di base.** Poichè ogni $n \in \mathbb{Z}$ ha come divisori ± 1 e $\pm n$, questi divisori sono chiamati *divisori impropri* di n. Un divisore m di n si dice *proprio* se non è improprio, cioè $m \neq \pm 1, \pm n$.

Definizione 1.11 (numero primo)**.** Un numero $p \in \mathbb{Z}$ si dice primo se $p \neq \pm 1$ e p non ha divisori propri.

Osservazione 1.12. Un intero $p \geq 2$ è primo se può essere diviso solo per se stesso o per 1. Un numero intero $m \geq 2$ non è primo se e solo se è *composto* cioè $m = ab$ con $1 < a < m$ (e quindi $1 < b < m$).

Esempio 1.13. Il numero $6 = 2 \cdot 3$ non è primo mentre 17 è primo.

Il crivello di Eratostene

Il seguente metodo, detto *Crivello di Eratostene* [1], consente di determinare i numeri primi positivi minori di un numero intero positivo assegnato.

Vediamo un esempio con $n = 100$. Scriviamo in ordine tutti i numeri da 2 a 100.

Si eliminano con un tratto / tutti i multipli di 2 (tranne 2) che è primo.

2 3 $\not{4}$ 5 $\not{6}$ 7 $\not{8}$ 9 $\not{1}0$ 11 $\not{1}2$ 13 $\not{1}4$ 15 $\not{1}6$ 17 $\not{1}8$ 19 $\not{2}0$ 21 $\not{2}2$ 23 $\not{2}4$ 25 $\not{2}6$ 27 $\not{2}8$ 29 $\not{3}0$ 31 $\not{3}2$ 33 $\not{3}4$ 35
$\not{3}6$ 37 $\not{3}8$ 39 $\not{4}0$ 41 $\not{4}2$ 43 $\not{4}4$ 45 $\not{4}6$ 47 $\not{4}8$ 49 $\not{5}0$ 51 $\not{5}2$ 53 $\not{5}4$ 55 $\not{5}6$ 57 $\not{5}8$ 59 $\not{6}0$ 61 $\not{6}2$ 63 $\not{6}4$ 65 $\not{6}6$
67 $\not{6}8$ 69 $\not{7}0$ 71 $\not{7}2$ 73 $\not{7}4$ 75 $\not{7}6$ 77 $\not{7}8$ 79 $\not{8}0$ 81 $\not{8}2$ 83 $\not{8}4$ 85 $\not{8}6$ 87 $\not{8}8$ 89 $\not{9}0$ 91 $\not{9}2$ 93 $\not{9}4$ 95 $\not{9}6$ 97
$\not{9}8$ 99 $\not{1}00$

Il primo intero che rimane dopo 2 è 3 che è primo. Si eliminano con un tratto / tutti i multipli di 3 tranne 3.

2 3 $\not{4}$ 5 $\not{6}$ 7 $\not{8}$ $\not{9}$ $\not{1}0$ 11 $\not{1}2$ 13 $\not{1}4$ $\not{1}5$ $\not{1}6$ 17 $\not{1}8$ 19 $\not{2}0$ $\not{2}1$ $\not{2}2$ 23 $\not{2}4$ 25 $\not{2}6$ $\not{2}7$ $\not{2}8$ 29 $\not{3}0$ 31 $\not{3}2$ $\not{3}3$ $\not{3}4$ 35
$\not{3}6$ 37 $\not{3}8$ $\not{3}9$ $\not{4}0$ 41 $\not{4}2$ 43 $\not{4}4$ $\not{4}5$ $\not{4}6$ 47 $\not{4}8$ 49 $\not{5}0$ $\not{5}1$ $\not{5}2$ 53 $\not{5}4$ 55 $\not{5}6$ $\not{5}7$ $\not{5}8$ 59 $\not{6}0$ 61 $\not{6}2$ $\not{6}3$ $\not{6}4$ 65 $\not{6}6$
67 $\not{6}8$ $\not{6}9$ $\not{7}0$ 71 $\not{7}2$ 73 $\not{7}4$ $\not{7}5$ $\not{7}6$ 77 $\not{7}8$ 79 $\not{8}0$ $\not{8}1$ $\not{8}2$ 83 $\not{8}4$ 85 $\not{8}6$ $\not{8}7$ $\not{8}8$ 89 $\not{9}0$ 91 $\not{9}2$ $\not{9}3$ $\not{9}4$ 95 $\not{9}6$ 97
$\not{9}8$ $\not{9}9$ $\not{1}00$

Il primo intero che rimane dopo 2 e 3 è 5 che è primo. Si eliminano con un tratto / tutti i multipli di 5 tranne 5.

2 3 $\not{4}$ 5 $\not{6}$ 7 $\not{8}$ $\not{9}$ $\not{1}0$ 11 $\not{1}2$ 13 $\not{1}4$ $\not{1}5$ $\not{1}6$ 17 $\not{1}8$ 19 $\not{2}0$ $\not{2}1$ $\not{2}2$ 23 $\not{2}4$ $\not{2}5$ $\not{2}6$ $\not{2}7$ $\not{2}8$ 29 $\not{3}0$ 31 $\not{3}2$ $\not{3}3$ $\not{3}4$ $\not{3}5$
$\not{3}6$ 37 $\not{3}8$ $\not{3}9$ $\not{4}0$ 41 $\not{4}2$ 43 $\not{4}4$ $\not{4}5$ $\not{4}6$ 47 $\not{4}8$ 49 $\not{5}0$ $\not{5}1$ $\not{5}2$ 53 $\not{5}4$ $\not{5}5$ $\not{5}6$ $\not{5}7$ $\not{5}8$ 59 $\not{6}0$ 61 $\not{6}2$ $\not{6}3$ $\not{6}4$ $\not{6}5$ $\not{6}6$
67 $\not{6}8$ $\not{6}9$ $\not{7}0$ 71 $\not{7}2$ 73 $\not{7}4$ $\not{7}5$ $\not{7}6$ 77 $\not{7}8$ 79 $\not{8}0$ $\not{8}1$ $\not{8}2$ 83 $\not{8}4$ $\not{8}5$ $\not{8}6$ $\not{8}7$ $\not{8}8$ 89 $\not{9}0$ 91 $\not{9}2$ $\not{9}3$ $\not{9}4$ $\not{9}5$ $\not{9}6$ 97
$\not{9}8$ $\not{9}9$ $\not{1}00$

[1] Eratostene di Cirene, visse nel 276 a.C. Egli è ricordato soprattutto per aver misurato con ottima approssimazione il raggio della terra (in quel tempo la gente comune non sapeva che la terra fosse sferica!)

Il primo intero che rimane dopo 2, 3 e 5 è 7 che è primo. Si eliminano con un tratto / tutti i multipli di 7 tranne 7.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~ 61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ ~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

I numeri restanti sono i seguenti:
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97.

Con lo stessa tecnica si possono ottenere tutti i numeri primi minori di 1000. Eccone la lista:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997

Osserviamo che per trovare tutti i numeri primi minori di un numero naturale N ci si può limitare ad applicare il crivello di Eratostene a tutti i numeri primi minori o uguali a $\sqrt{N}$. Infatti supponiamo di aver eliminato tutti i multipli dei numeri primi minori o uguali a $\sqrt{N}$ e che esista, per assurdo, un numero a non primo tale che $\sqrt{N} \leq a < N$. Sia p il più piccolo primo che divide a quindi $a = pq$ e $q \geq p$. Osserviamo ora che $p \leq \sqrt{N}$ altrimenti $q \geq p > \sqrt{N}$ e quindi $pq > N$. Ma allora un tale a non può esistere (sarebbe stato cancellato come mulitplo di p). Questo conclude il ragionamento.

Un tentativo di capire quanti e quali siano i numeri primi potrebbe essere quello di osservare attentamente le tabelle costituite dai numeri primi minori di un numero assegnato.

Per esempio se una controlla la tabella dei numeri primi da 2 a 100, e cioè:

2 **3** 4 **5** 6 **7** 8 9 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20 21 22 **23** 24 25 26 27 28 **29** 30 **31** 32 33 34 35 36 **37** 38 39 40 **41** 42 **43** 44 45 46 **47** 48 49 50 51 52 **53** 54 55 56 57 58 **59** 60 **61** 62 63 64 65 66 **67** 68 69 70 **71** 72 **73** 74 75 76 77 78 **79** 80 81 82 **83** 84 85 86 87 88 **89** 90 91 92 93 94 95 96 **97** 98 99 100

constata che da 2 a 11 ci sono 5 numeri primi, $2, 3, 5, 7, 11$, esattamente la metà dei numeri da 2 a 11; tra i successivi dieci da 12 a 21, ci sono 3 numeri primi, 13, 17, 19, cioè il 30% ;

tra 22 e 31, ci sono ancora 3 numeri primi, 23, 29, 31, cioè ancora il 30% ; mentre tra 32 e 41, ci sono 2 numeri primi, 37, 41, cioè il 20%; e così tra 42 e 51.

Sembra che il calcolo si stabilizzi a circa il 20% . Ma non è così. Si considerino per esempio i cento numeri che vanno da 9.999.901 a 10.000.000 allora:

9.999.901 9.999.902 9.999.903 9.999.904 9.999.905 9.999.906 9.999.907 9.999.908 9.999.909
9.999.910 9.999.911 9.999.912 9.999.913 9.999.914 9.999.915 9.999.916 9.999.917 9.999.918 9.999.919
9.999.920 9.999.921 9.999.922 9.999.923 9.999.924 9.999.925 9.999.926 9.999.927 9.999.928 9.999.929
9.999.930 9.999.931 9.999.930 9.999.931 9.999.932 9.999.933 9.999.934 9.999.935 9.999.936 9.999.937
9.999.938 9.999.939 9.999.940 9.999.941 9.999.942 9.999.943 9.999.944 9.999.945 9.999.946 9.999.947
9.999.948 9.999.949 9.999.950 9.999.951 9.999.952 9.999.953 9.999.954 9.999.955 9.999.956 9.999.957
9.999.958 9.999.959 9.999.960 9.999.961 9.999.962 9.999.963 9.999.964 9.999.965 9.999.966 9.999.967
9.999.968 9.999.969 9.999.970 9.999.971 9.999.972 9.999.973 9.999.974 9.999.975 9.999.976 9.999.977
9.999.970 9.999.971 9.999.972 9.999.973 9.999.974 9.999.975 9.999.976 9.999.977 9.999.978 9.999.979
9.999.980 9.999.981 9.999.982 9.999.983 9.999.984 9.999.985 9.999.986 9.999.987 9.999.988 9.999.989
9.999.990 9.999.991 9.999.992 9.999.993 9.999.994 9.999.995 9.999.996 9.999.997 9.999.998 9.999.999
10.000.000

Mentre i numeri primi che si trovano tra 10.000.000 a 10.000.100 sono solo 2.

10.000.000 10.000.001 10.000.002 10.000.003 10.000.004 10.000.005 10.000.006 10.000.007 10.000.008
10.000.009 10.000.010 10.000.011 10.000.012 10.000.013 10.000.014 10.000.015 10.000.016 10.000.017
10.000.018 10.000.019 10.000.020 10.000.021 10.000.022 10.000.023 10.000.024 10.000.025 10.000.026
10.000.027 10.000.028 10.000.029 10.000.030 10.000.031 10.000.032 10.000.033 10.000.034 10.000.035
10.000.036 10.000.037 10.000.038 10.000.039 10.000.040 10.000.041 10.000.042 10.000.043 10.000.044
10.000.045 10.000.046 10.000.047 10.000.048 10.000.049 10.000.050 10.000.051 10.000.052 10.000.053
10.000.054 10.000.055 10.000.056 10.000.057 10.000.058 10.000.059 10.000.060 10.000.061 10.000.062
10.000.063 10.000.064 10.000.065 10.000.066 10.000.067 10.000.068 10.000.069 10.000.070 10.000.071
10.000.072 10.000.073 10.000.074 10.000.075 10.000.076 10.000.077 10.000.078 10.000.079 10.000.080
10.000.081 10.000.082 10.000.083 10.000.084 10.000.085 10.000.086 10.000.087 10.000.088 10.000.089
10.000.090 10.000.091 10.000.092 10.000.093 10.000.094 10.000.095 10.000.096 10.000.097 10.000.098
10.000.099 10.000.100

La situazione è ancora più complicata per il fatto che esistono intervalli di numeri naturali, di ampiezza arbitraria, all'interno dei quali non si incontra alcun numero primo!!!!

Per vedere questo, consideriamo il fattoriale $n!$ di un numero naturale definito in precedenza, cioè $n! = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot .... \cdot 3 \cdot 2 \cdot 1$.

Osserviamo che $n!$ è divisibile per ciascuno dei numeri tra 1 e n; $n!+2$ è divisibile per 2, $n!+3$ è divisibile per 3, e quindi $n!+n$ è divisibile per n. Abbiamo così trovato un intervallo di $n-1$ numeri naturali consecutivi

$$n!+2,\ n!+3,\ \cdots,\ n!+n$$

e nessuno di essi primo.

Nasce spontanea una domanda: *I numeri primi sono infiniti?*

Risponderemo affermativamente a questa domanda nel Teorema 1.20.

Concludiamo comunque osservando che molte domande *naturali* sui numeri primi sono ancora problemi aperti. Ecco una lista di alcuni di questi problemi.

1. NON SI SA se ogni numero pari maggiore di 2 possa essere scritto come somma di due numeri primi (*congettura binaria di Goldbach (1690-1764)*).

2. NON SI SA se ogni numero dispari maggiore di 5 possa essere scritto come somma di tre numeri primi (*congettura ternaria di Goldbach*).

3. NON SI SA se esistono infiniti numeri primi della forma $n! \pm 1$.

4. NON SI SA se esistono infiniti numeri primi della forma n^2+1.

5. NON SI SA se esiste sempre un numero primo tra n^2 e $(n+1)^2$ (il fatto che esista un numero primo tra n e $2n$ è stato dimostrato da Chebyshev).

6. NON SI SA se la successione di Fibonacci

$$F_0 = F_1 = 1, F_n = F_{n-1} + F_{n-2},\ n > 1$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55 \ldots$$

contenga un numero infinito di numeri primi. Osserviamo che $F_{19} = 4.181 = 113 \times 37$ non è primo nonostante 19 lo sia.

7. NON SI SA se esistano infiniti numeri primi gemelli. Due numeri primi sono detti *gemelli* se la loro distanza è due (es. 17 e 19 sono primi gemelli). [2].

Esercizio 17. Esibire un intervallo di 100 numeri consecutivi che non contiene nessun numero primo.

1.5. **Il massimo comun divisore e il minimo comune multiplo.**

Definizione 1.14 (massimo comun divisore)**.** Dati due interi a e b non entrambi nulli, un massimo comun divisore di a e b (brevemente MCD) è definito come un numero intero d tale che

(*i*) $d|a$ e $d|b$,

(*ii*) se $c|a$ e $c|b$ allora $c|d$,

Se d è un massimo comun divisore di a e b, lo è anche $-d$. Quindi il massimo comun divisore è determinato solo a meno del segno. Infatti, siano d_1 e d_2 due MCD di a e b. Allora

[2] I numeri primi gemelli più grandi che si conoscono sono: $(2003663613)2^{2195000}-1$ e $(2003663613)2^{2195000}+1$

la condizione (i) per d_1 e la (ii) per d_2 comportano $d_1|d_2$ e scambiando i ruoli otteniamo $d_2|d_1$. Ma allora dalla (5) della Proposizione 1.10 $d_1 = \pm d_2$. Spesso prenderemo in considerazione *il* MCD *positivo*, denotato con (a, b) di a e b. Quindi (a, b) è il più grande di tutti i divisori comuni di a e b ed è univocamente determinato.

Osservazione 1.15. Si osservi che

$$(a, b) = (-a, b) = (a, -b) = (-a, -b), \ (0, b) = b. \tag{6}$$

Per dimostrare l'esistenza di (a, b) consideriamo l'insieme

$$S = \{s \mid s = ax + by; x \in \mathbb{Z}, y \in \mathbb{Z}, s > 0\},$$

cioè la totalità dei numeri interi positivi della forma $ax + by$. Poichè a, b non sono entrambi nulli, S non è vuoto, e perciò contiene un elemento minimo $d = at + bs$. Proviamo che risulta $d = (a, b)$. Dividiamo a per d e otteniamo $a = dq + r, \ 0 \leq r < d$. Allora

$$r = a - dq = a - (at + bs)q = a(1 - tbq) + b(-sq).$$

Dunque r è del tipo $ax + by$. Se fosse $r > 0$ allora $r \in S$ e $r < d$, in contrasto con la minimilità di d. Ne segue che $r = 0$ e quindi $d|a$. Analogamente $d|b$, e la condizione (i) per il MCD è soddisfatta. Quanto alla (ii) se $c|a$ e $c|b$ allora $a = ca_1$ e $b = cb_1$ e quindi

$$d = at + bs = ca_1t + cb_1s = c(a_1t + b_1s)$$

ossia $c|d$.

Algoritmo di Euclide. Diamo ora un procedimento per la determinazione di (a, b). Illustreremo il procedimento con un esempio.

Per esempio calcoliamo $(756, 210)$. Dividiamo successivamente 756 per 210, poi 210 per il resto, il primo resto per il secondo resto e così via, fino ad ottenere resto 0.

$$\begin{aligned} 756 &= 210 \cdot 3 + 126 \\ 210 &= 126 \cdot 1 + 84 \\ 126 &= 84 \cdot 1 + 42 \\ 84 &= 42 \cdot 2 + 0 \end{aligned}$$

Affermiamo che l'ultimo resto positivo è il MCD: $(756, 210) = 42$; infatti leggendo le divisioni precedenti dall'ultima alla prima e tendendo conto della (3) nella Proposizione 1.10, si ottiene che $42|84$, $42|126$ perchè $42|42$ e $42|84$; $42|210$ perchè $42|84$ e $42|126$; $42|756$ perchè $42|126$ e $42|210$. Allora il numero 42 soddisfa la condizione (i) del MCD. Inoltre se $c|756$ e $c|210$, allora, leggendo le divisioni dalla prima all'ultima, si ottiene $c|126$ perchè $126 = 756 - 210 \cdot 3$; $c|84$ perchè $84 = 210 - 126 \cdot 1$; $c|42$ perchè $42 = 126 - 84 \cdot 1$. Quindi anche la condizione (ii) è provata.

Osserviamo che l'algoritmo di Euclide permette di risolvere il problema di determinare gli interi t e s tali che $d = at + bs$ e che appaiono nella dimostrazione dell'unicità del MCD. Nell'esempio precedente, utilizzando le divisioni precedenti dall'ultima alla prima, otteniamo:

$$42 = 126-84\cdot 1 = 126-(210-126) = 126\cdot 2-210 = (756-210\cdot 3)\cdot 2-210 = 756\cdot 2+210(-7),$$

quindi $t = 2$ e $s = -7$ in questo caso.

Definizione 1.16. *Due interi a e b di dicono* coprimi *oppure* primi tra loro *se $(a, b) = 1$.*

Nel lemma che segue riassumiamo due proprietà del MCD.

Lemma 1.17. *Siano a, b interi non entrambi nulli. Allora:*

(i) *se $d|a$ e $d|b$ e $d = ax + by$ con $x, y \in \mathbb{Z}$ allora d è un massimo comun divisore di a e b, cioè $d = \pm(a, b)$;*

(ii) *due interi a, b sono coprimi se e solo se esistono $x, y \in \mathbb{Z}$ tali che $ax + by = 1$; in particolare due interi consecutivi sono coprimi;*

(iii) *se $d = (a, b)$, allora $a = da_1$ e $b = db_1$, con $(a_1, b_1) = 1$;*

(iv) *se $c|ab$ e $(a, c) = 1$, allora $c|b$;*

(v) *se p è primo e $p|ab$ allora $p|a$ oppure $p|b$;*

(vi) *se $a|m$ e $b|m$ e $(a, b) = 1$, allora $ab|m$.*

Dimostrazione. (i) sia c un divisore comune di a e b, cioè $c|a$ e $c|b$, allora $c|d = ax + by$; quindi d è un massimo comun divisore di a e b e la (i) è dimostrata.

(ii) segue immediatamente dalla (i);

Per dimostrare la (iii) sia $d' = (a_1, b_1)$. Allora $d'|a_1$ e $d'|b_1$, quindi $dd'|da_1 = a$ e $dd'|db_1 = b$. Quindi dd' è un divisore comune di a e b. Dunque $dd'|d$. Poichè anche $d|dd'$ si conclude che $dd' = \pm d$, cioè $d' = 1$.

(iv) per (ii) sappiamo che $cx + ay = 1$ per opportuni $x, y \in \mathbb{Z}$. Moltiplicando per b otteniamo $b = bcx + aby$. Ma, per ipotesi, $ab = ce$ per qualche $e \in \mathbb{Z}$, quindi $b = bcx + cey = c(bx + ey)$ e quindi $c|b$.

(v) per definizione i divisori di p sono solo ± 1 e $\pm p$. Se allora p non divide a, i divisori comuni di p e a sono ± 1. Allora $(p, a) = 1$ e applicando (iv) otteniamo che $p|b$.

(vi) per ipotesi $m = ac$ per qualche c; per ipotesi $b|ac$ e quindi per (iv) $b|c$ ossia $c = be$, Segue che $m = ac = abe$ e quindi $ab|m$. □

Definizione 1.18 (minimo comune multiplo)**.** Dati due interi a e b non entrambi nulli, un minimo comune multiplo di a e b (brevemente mcm) è definito come un numero intero m tale che

(i) $a|m$ e $b|m$ (m è multiplo di entrambi) (*ii*) se $a|c$ e $b|c$ allora $m|c$ (m è un divisore di ogni intero che sia multiplo di entrambi).

Osserviamo innanizitutto che anche il mcm (come il MCD) è individuato a meno del segno. Infatti, siano m_1 e m_2 due mcm di a e b. Allora la condizione (i) per m_1 e la (ii) per m_2 comportano $m_2|m_1$ e scambiando i ruoli otteniamo $m_1|m_1$. Ma allora, dalla (5) della Proposizione 1.10, $m_2 = \pm m_1$. Si indicherà con il simbolo $[a, b]$ il mcm non negativo dei numeri a, b.

Il seguente teorema riconduce il calcolo del minimo comune multiplo al calcolo del massimo comun divisore.

Teorema 1.19. *Siano a, b due interi entrambi non nulli. Allora*

$$(a, b)[a, b] = |ab|.$$

Dimostrazione. Dividendo ab per (a, b) si ottiene resto zero e quindi $(a, b)q = ab$. Si tratta di provare che q soddisfa le condizioni (i) e (ii) della Definizione 1.18. Per (iii) del Lemma 1.17 possiamo scrivere $a = (a, b)a_1$ e $b = (a, b)b_1$ con $(a_1, b_1) = 1$. Si ottiene quindi $(a, b)q = ab = (a, b)a_1b = (a, b)ab_1$. Segue che $q = a_1b = ab_1$ che mostra che $a|q$ e $b|q$ e quindi q soddisfa la (i). Per dimostrare che q soddisfa la (ii) supponiamo $a|c$ e $b|c$ quindi $c = ae$, $c = bf$, $(a, b)|c$ e possiamo scrivere $c = (a, b)c_1$. Moltiplicando per a_1 si ottiene $a_1ae = a_1c = (a, b)a_1c_1 = ac_1$. Siccome $a \neq 0$ deduciamo che $a_1e = c_1$ e quindi $a_1|c_1$. Analogamente si ottiene $b_1|c_1$. Essendo $(a_1, b_1) = 1$ per la (vi) del Lemma 1.17 si deduce $a_1b_1|c_1$. Quindi $q = a_1b = a_1b_1(a, b)|c_1(a, b) = c$ e anche la (ii) è verificata. □

1.6. **Il teorema fondamentale dell'aritmetica.**

Teorema 1.20. *(teorema fondamentale dell'aritmetica) Ogni intero maggiore di* 1 *si può esprimere come prodotto di numeri primi positivi. Questa espressione è unica, a meno dell'ordine in cui compaiono i fattori.*

Dimostrazione. Dimostriamo prima l'esistenza di una tale fattorizzazione. Supponiamo, per assurdo, che esistano interi maggiori di uno che non si possano esprimere come prodotto di primi e sia m il minore di essi. Allora m non è primo e quindi ammette divisori diversi da ± 1 e $\pm m$, e quindi, per la minimalità di m, essi si esprimono come prodotti di primi $n = p_1p_2 \cdots p_r$, $q = q_1q_2 \cdots q_s$. Si ottiene quindi $m = p_1p_2 \cdots p_r q q_1 q_2 \cdots q_s$ una contraddizione. Quindi per ogni $n > 1$ esistono numeri primi positivi p_1, p_2, p_r tali che $n = p_1p_2 \cdots p_r$.

Dimostriamo l'unicità. Supponiamo $n = q_1q_2 \cdots q_s$ sia un'altra fattorizzazione di n in primi positivi. Allora, per il punto (v) del Lemma 1.17, $p_1|q_1$ oppure $p_1|q_2 \cdots q_s$. Nel primo caso $p_1 = q_1$ (in quanto si tratta di primi positivi). Nel secondo caso, sempre per il (v) del Lemma 1.17, $p_1|q_2$ oppure $p_1|q_3 \cdots q_s$. Procedendo in questo modo si trova $j \leq u$ tale che $p_1 = q_j$. Allora i fattori primi si posso riordinare in modo tale che q_j sia al primo posto (cioè per $j = 1$). Quindi $n = p_1 p_2 \cdots p_t = p_1 q_2 \cdots q_r$ da cui $p_2 \cdots p_t = q_2 \cdots q_r$. Si continua sin quando non si esauriscono tutti i p_i. Allo stesso tempo si devono esaurire anche i q_j. Si conclude che nelle due fattorizzazioni compare lo stesso numero di fattori ($r = s$) e compaiono i medesimi fattori primi a meno dell'ordine. $\square$

Nella fattorizzazione di un numero n ovviamente il medesimo primo può comparire più volte. Si possono riordinare i fattori in modo da riavvicinare i primi uguali. Quindi se $p_1, p_2, \ldots, p_t$ sono i fattori primi distinti nella fattorizzazione di n, allora $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ e gli interi positivi $\alpha_1, \alpha_2, \ldots, \alpha_t$ sono univocamente individuati da n.

Per trattare alcuni problemi di divisibilità è conveniente scrivere i numeri positivi coinvolti come prodotti di potenze dei medesimi primi (distinti). Se $a, b > 0$ allora $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$. Ciò è sempre possibile purchè si ammettano valori nulli degli esponenti. L'unicità delle fattorizzazione ci garantisce che se $a|b$ allora $\alpha_i \leq \beta_i$ per ogni $i = 1, 2, \ldots, t$. Inoltre possiamo descrivere il metodo tradizionale per il calcolo del MCD e del mcm. Infatti si deduce che $(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t}$, dove γ_i è il minimo tra α_i e β_i e che $[a, b] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_t^{\delta_t}$, dove δ_i è il massimo tra α_i e β_i.

Dimostriamo ora che i numeri primi sono infiniti.

Teorema 1.21. *(Elementi di Euclide, Libro IX, Proposizione 20) Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo che i primi siano in numero finito: $p_1, p_2, \ldots, p_t$. Allora il numero $m = p_1 p_2 \cdots p_t + 1$ sarebbe coprimo con $p_1 p_2 \cdots p_t$ (cfr. (ii) Lemma 1.17) e dunque con ogni p_i. Allora m non potrebbe essere un prodotto di numeri primi in contrasto con il teorema fondamentale dell'aritmetica. $\square$

Osservazione 1.22. Non si sa se i numeri della forma $Q_N = p_1 p_2 p_3 \ldots p_N + 1$ siano infiniti. Per esempio $Q_1 = 2 + 1 = 3, Q_2 = 2 \cdot 3 + 1 = 7, Q_3 = 2 \cdot 3 \cdot 5 + 1 = 31, Q_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211, Q_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ sono primi. Mentre $Q_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ e $Q_7 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511 = 19 \cdot 97 \cdot 277$ sono composti.

1.7. **Congruenze e criteri di divisibilità.** Dato un numero naturale $m \geq 0$, diremo che due interi a e b sono *congrui modulo* m e scriveremo $a \equiv b \mod m$ se essi differiscono per un multiplo di m, cioè $m|a - b$. Per esempio $5 \equiv 1 \mod 4$, Osserviamo che $a \equiv b \mod 0$ se e solo se $a = b$. Se a e b non sono congui modulo m scriveremo $a \not\equiv b \mod m$. Per esempio $-5 \not\equiv 12 \mod 4$.

Un criterio per stabilire se due numeri sono congrui modulo m è epresso dalla seguente:

Proposizione 1.23. *Due interi a e b sono interi congrui modulo m ($m \neq 0$) se solo se divisi per m danno lo stesso resto.*

Dimostrazione. Sia infatti $a = mq_1 + r_1$, $b = mq_2 + r_2$, $0 \leq r_1, r_2 < m$. Se $r_1 = r_2$ allora $a - b = m(q_1 - q_2)$, e quindi $a \equiv b \mod m$. Viceversa se $a \equiv b \mod m$ esiste $c \in \mathbb{Z}$ tale che $b = a + mc$ e quindi $b = mq_1 + r_1 + mc = m(q_1 + c) + r_1$. Per l'unicità del quoziente e del resto della divisione euclidea, si conclude $q_1 + c = q_2$ e $r_1 = r_2$. □

Il seguente lemma riassume le proprietà principali della congruenza che sono lasciate al lettore come un semplice esercizio.

Lemma 1.24. *Siano $a, b, c \in \mathbb{Z}$ e m un numero naturale. Allora:*

(1) $a \equiv a \mod m$ (riflessività);
(2) $a \equiv b \mod m$ allora $b \equiv a \mod m$ (simmetria);
(3) se $a \equiv b \mod m$ e $b \equiv c \mod m$ allora $a \equiv c \mod m$ (transitività);
(4) se $a \equiv b \mod m$ e $c \equiv d \mod m$ allora $a + c \equiv b + d \mod m$;
(5) se $a \equiv b \mod m$ e $c \equiv d \mod m$ allora $ac \equiv bd \mod m$.

Osservazione 1.25. La proprietà (5) non si inverte. Per esempio $5 \cdot 2 \equiv 2 \cdot 1 \mod 8$ non implica $5 \equiv 1 \mod 8$. Questo accade perchè il numero 2 che si vorrebbe *cancellare* è un divisore del modulo. Vale però la seguente regola: se c è primo con m allora da $ac \equiv bc \mod m$ si deduce $a \equiv b \mod m$. Infatti, per ipotesi, $m|ac - bc = (a - b)c$ e $(c, m) = 1$. Segue allora da (iv) del Lemma 1.17 che $m|(a - b)$ e quindi $a \equiv b \mod m$.

La relazione di congruenza ha diverse interessanti applicazioni. Qui analizzeremo il suo utilizzo per dedurre alcuni criteri di divisibilità.

Osserviamo che la *notazione* che adoperiamo per gli interi è quella *decimale* o in *base* 10. Con ciò intendiamo ad esempi che il simbolo 7209 si associa il numero $7 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10 + 2$; la notazione è cioè la seguente: se un numero si ottiene dalla somma

$$a = a_h 10^h + a_{h-1} 10^{h-1} + \cdots + a_3 10^3 + a_2 10^2 + a_1 10^1 + a_0 \tag{7}$$

con $0 \leq a_i < 10$ allora tale numero si ottiene giustapponendo (non moltiplicando!) gli a_i nell'ordine $a_h a_{h-1} \cdots a_1 a_0$.. Chiameriamo gli a_i le cifre del numero a.

Teorema 1.26. *Sia $a = a_h a_{h-1} \cdots a_1 a_0$ un numero naturale. Allora valgono i seguenti criteri di divisibilità.*

- *a è divisibile per 2 se e solo se $2|a_0$, ovvero se e solo se a_0 è pari;*
- *a è divisibile per 3 se e solo se e solo se la somma delle sue cifre è divisibile per 3 $(3|(a_h + a_{h-1} + \cdots + a_1 + a_0))$;*
- *a è divisibile per 4 se le ultime due cifre sono 00 oppure formano un numero multiplo di 4;*
- *a è divisibile per 5 se e solo se $a_0 = 0$ oppure $a_0 = 5$;*
- *a è divisibile per 6 se è divisibile sia per 2 che per 3;*

- *a è divisibile per 7 se e solo se la differenza del numero ottenuto escludendo la cifra delle unità e il doppio della cifra delle unità è un multiplo di 7;*
- *a è divisibile per 8 se e solo se a termina con tre zeri o se è divisibile per 8 il numero formato dalle sue ultime 3 cifre ;*
- *a è divisibile per 9 se e solo se la somma delle sue cifre è divisibile per 9 ($9|(a_h + a_{h-1} + \cdots + a_1 + a_0)$);*
- *a è divisibile per 10 se e solo se $a_0 = 0$;*
- *a è divisibile per 11 se e solo se la differenza tra la somma delle cifre di posto pari e la somma delle cifre di posto dispari è divisibile per 11;*
- *a è divisibile per 12 se e solo se è divisibile sia per 3 che per 4 ;*
- *a è divisibile per 13 se e solo se la somma del numero ottenuto escludendo la cifra delle unità più il quadruplo della cifra delle unità è un multiplo di 13;*
- *a è divisibile per 17 se e solo se la differenza del numero ottenuto escludendo la cifra delle unità e il quintuplo della cifra delle unità è un multiplo di 17;*
- *a è divisibile per 25 se e solo se le sue ultime due cifre (a_1a_0) sono 00, 25, 50, 75;*
- *a è divisibile per 100 se e solo se le sue ultime due cifre sono 00.*

Dimostrazione. vedi appunti presi in classe. □

1.8. **La funzione di Eulero e il teorema di Eulero.**

Definizione 1.27. Per ogni numero intero $n > 0$, indichiamo con $\Phi(n)$ il numero degli interi compresi tra 0 e n che siano primi con n.

Denotiamo con $\mathbb{N}^*$ l'insieme dei numeri interi positivi. La funzione $\Phi : N^* \to N$ che a n associa $\Phi(n)$ si chiama la *funzione di Eulero*. Ad esempio $\Phi(1) = 1$, $\Phi(2) = 1$, $\Phi(3) = 2$, $\Phi(4) = 2$, $\Phi(5) = 4$, $\Phi(6) = 2$, ecc.

Come si riesce a calcolare il $\Phi(n)$ quando n è grande? Il seguente risultato ci viene in aiuto.

Proposizione 1.28. *Valgono i seguenti fatti:*

(1) se p è primo, $\Phi(p) = p - 1$;
(2) se p è primo e a è un intero positivo, allora $\Phi(p^a) = p^a - p^{a-1}$;
(3) se m e n sono coprimi, allora $\Phi(mn) = \Phi(m)\Phi(n)$;
(4) se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ è la decomposizione di n in prodotto di potenze di numeri primi diversi tra loro, allora

$$\Phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_t^{\alpha_t} - p_t^{\alpha_t - 1}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_t})$$

Dimostrazione. la (1) segue dal fatto che tutti i numeri $1, 2, \ldots, p-1$ sono coprimi con p.

La (2) si ottiene sottraendo a p^a i numeri $h \leq p^a$ che non sono primi con p^a. Questi sono $p, 2p, \ldots, p^{a-1}, p^a$ e il loro numero è p^{a-1}. Quindi i numeri minori di p^a e primi con p sono $p^a - p^{a-1}$.

La (3) non verrà dimostrata.

La (4) segue immediatamente dalla (2) e dalla (3).

□

Le proprietà elencate nella proposizione ci permettono di calcolare facilmente il valore di Φ di un qualunque intero positivo (una volta che si è scritta la sua scomposizione in fattori primi). Vediamo qualche esempio.

Esempio 1.29. $\Phi(30) = \Phi(6 \cdot 5) = \Phi(6)\Phi(5) = 2 \cdot 4 = 8$.

Esempio 1.30. $\Phi(98) = \Phi(2 \cdot 49) = \Phi(2)\Phi(7^2) = 1 \cdot (7^2 - 7) = 42$.

Teorema 1.31 (teorema di Eulero–Fermat)**.** *Sia n un intero postivo e a un intero coprimo con n. Allora*

$$a^{\Phi(n)} \equiv 1 \bmod n.$$

Osservazione 1.32. L'ipotesi che a e n siano coprimi è necessaria. Se prendiamo, ad esempio, $n = 12$ e $a = 2$ abbiamo $\Phi(12) = \Phi(6)\Phi(2) = 2$, da cui $2^2 \not\equiv 1 \bmod 12$.

Quando p è primo $\Phi(p) = p - 1$ e come corollario del precedente teorema si ottiene:

Teorema 1.33 (piccolo Teorema di Fermat)**.** *Sia p un numero primo e sia a un intero non divisibile per p. Allora:*

$$a^p \equiv a \bmod p.$$

Osservazione 1.34. Nel teorema precedente è necessario che p sia primo, infatti per esempio se $p = 4$ e $a = 3$ abbiamo $3^3 \not\equiv 3 \bmod 4$.

1.9. **Qualche domanda e problema sui numeri interi.**

Esercizio 18. Rispondere alle seguenti domande:

(1) Quale è l'ultima cifra di 725843^{594}?
(2) Quali sono le ultime due cifre dei numeri 3^{1492}, 523^{321}, 48353^{483}?
(3) Quali sono le ultime tre cifre di 3020173^{31}?
(4) Quale è il resto della divisione 89741^{527} per 3?
(5) Quale è il resto della divisione di 362971^{29345} e di 29345^{362971} per 6?
(6) Quale è il resto della divisione di 4526^{236} e di $7574632^{2845301}$ per 7?
(7) Quale è il resto della divisione di 57432^{1142} e di 725843^{594} per 9?
(8) Quale è il resto della divisione 43816^{20321} per 10?

(9) Quale è il resto della divisione $7574632^{2845301}$ per 11?

(10) Quale è il resto della divisione 109^{597} per 17?

I problemi che seguono non sono di facile soluzione quindi non demoralizzatevi!

Problema 1. Dimostrare che qualunque siano i numeri naturali k, m, n, il numero

$$5^{5k+1} + 4^{5m+2} + 3^{5n}$$

è divisibile per 11.

Problema 2. Dimostrare che il numero $3^{105} + 4^{105}$ è divisibile per $7, 13, 49, 181, 379$, ma non è divisibile per 5 e per 11.

Problema 3. Scriviamo un numero naturale qualsiasi (per esempio 2583) e quindi sommiamo i quadrati delle sue cifre ($2^2 + 4^2 + 8^2 + 3^2 = 102$). Ora facciamo lo stesso con il numero così ottenuto ($1^2 + 0^2 + 2^2 = 5$) e continuiamo nello stesso modo ($5^2 = 25$, $2^2 + 5^2 = 29$, $2^2 + 9^2 = 85...$). Dimostrare che il procedimento giungerà ad una delle seguenti situazioni:

(1) si ottiene il valore 1, che quindi si ripeterà indefinitamente;

(2) si ottiene il valore che appartiene al ciclo $145, 42, 20, 4, 20, 16, 37, 58, 89$.

Problema 4. (forma semplificata del teorema di Fermat) Dimostrare che la relazione

$$x^n + y^n = z^n$$

non è verificata per nessuna scelta degli interi positivi x, y, z, n con $n \geq z$.

2. Solidi convessi

Concludiamo queste note con la dimostrazione che esistono esattamente cinque solidi convessi e regolari nello spazio i cosiddetti *solidi platonici*. Un *solido convesso* S è un sottoinsieme limitato dello spazio $\mathbb{R}^3$ definito dalle due condizioni seguenti:

- S non è contenuto in un sottospazio affine proprio di $\mathbb{R}^3$;
- S è l'intersezione di un numero finito di semispazi di $\mathbb{R}^3$.

Un solido convesso S è effettivamente un sottoinsieme convesso di $\mathbb{R}^3$ in quanto intersezione di semispazi di $\mathbb{R}^3$ che sono convessi.

Sia S un solido convesso di $\mathbb{R}^3$ e α un piano di $\mathbb{R}^3$ tale che S sia contenuto in uno dei due semispazi definiti da α. Si hanno le seguenti possibilità:

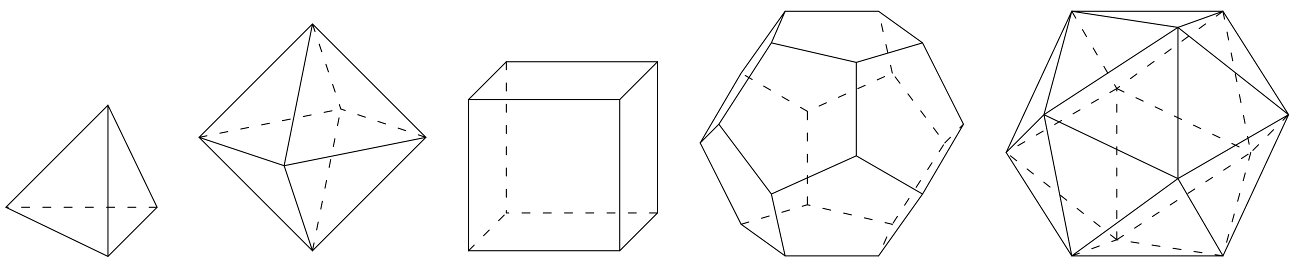
- $S \cap \alpha = \emptyset$;
- $S \cap \alpha$ è un punto che si chiama *vertice* di S;
- $S \cap \alpha$ è un segmento che si chiama *spigolo* o *lato* di S;
- $S \cap \alpha$ è un poligono, che si chiama *faccia* di S.

Dal momento che S è intersezione di un numero finito di semispazi segue che esso possiede un numero finito di vertici V, di lati L e di facce F. Inoltre ogni spigolo è un lato di due facce e ogni vertice è vertice e di almeno tre facce e di altrettanti spigoli. Vale il seguente risultato che era già noto a Cartesio 1640 ma che fu poi dimostrato da Eulero nel 1752.

Teorema 2.1. *Sia S un solido convesso di $\mathbb{R}^3$ e siano V, L e F come sopra. Allora*

$$V - L + F = 2.$$

Un *solido regolare* è un solido convesso di $\mathbb{R}^3$ avente per facce poligoni regolari tutti uguali tra loro e con lo stesso numero di lati uscenti da ogni vertice (quindi lo stesso numero di facce che si incontrano in un vertice). Esempi di solidi regolari sono: il *tetraedro*, l'*ottaedro*, il *cubo*, il *dodecaedro* e l'*icosaedro*.



Tetraedro Ottaedro Cubo Dodecaedro Icosaedro

Questi sono chiamati anche *solidi platonici* in quanto Platone ne parla nel Timeo. Di essi tratta il XIII libro (l'ultimo) degli *Elementi* di Euclide dove si fornisce una dimostrazione della loro esistenza. Il fatto notevole, che a differenza dei poligoni regolari, i solidi platonici sono precisamente i 5 appena descritti. La dimostrazione di questo fatto si ottiene tramite l'uso del Teorema 2.1. Sia infatti S un solido platonico. Denotiamo con n, $n \geq 3$, il numero di lati di ogni faccia (e quindi il numero di vertici in ogni faccia) e con m, $m \geq 3$, il numero di lati uscenti da un vertice (e quindi il numero di facce che si incontrano in un vertice). Si osservi che n e m non dipendono dalla faccia o dal vertice scelto perché il solido è, per ipotesi, regolare. Dal momento che ogni lato ha in comune due facce si ottiene allora che il numero di lati L e il numero di vertici V si possono scrivere in funzione del numero di facce F del poligono come segue:

$$L = \frac{nF}{2}, \ V = \frac{nF}{m}.$$

Per il Teorema 2.1 si ottiene allora:

$$F - L + V = F\left(\frac{n}{m} - \frac{n}{2} + 1\right) = 2.$$

e quindi $F = \frac{4m}{2n-mn+2m}$ dalla quale segue (essendo $F > 0$) che

$$\frac{2n}{n-2} > m. \tag{8}$$

Usando questa disuguaglianza e il fatto che $m \geq 3$ si ottiene che $n < 6$ e $m < 6$. Dalla (8) le uniche possibilità per le coppie (n, m) con $3 \leq n < 6$ e $3 \leq m < 6$ sono cinque e cioè:

$$(3,3), (3,4), (3,5), (4,3), (5,3)$$

che corrispondono rispettivamente al tetraedro, all'ottaedro, all'icosaedro, al cubo e al dodecaedro.

Esercizio 19. Una palla da calcio è formata da pentagoni e esagoni tali che tre facce si incontrano in un vertice e due facce distinte si incontrano al più in un vertice o in un lato. Mostrare che il numero di pentagoni è 12.