Capitolo 3

Interi e aritmetica modulare

In questo capitolo lavoreremo con i numeri interi. Nella prima parte richiameremo le proprietà fondamentali dell'aritmetica. Questo ci consentirà, nella seconda parte, di introdurre la cosiddetta aritmetica modulare, fondamentale in molte applicazioni pratiche.

3.1 Somma, prodotto e algoritmo della divisione

Iniziamo con la seguente

Definizione 3.1. Sia A un insieme dotato di due operazioni che denotiamo con $+$ e $\cdot$. Diremo che $(A, +, \cdot)$ è un **anello** se soddisfa le seguenti proprietà.

(1) *La somma è associativa*, ovvero per ogni $a, b, c \in A$ si ha

$$(a + b) + c = a + (b + c).$$

(2) *La somma è commutativa*, ovvero per ogni $a, b \in A$ si ha

$$a + b = b + a.$$

(3) *Esiste un elemento neutro per la somma* (denotato con 0), tale che per ogni $a \in A$ si ha

$$a + 0 = 0 + a = a.$$

(4) *Ogni elemento ammette un inverso rispetto alla somma* (che chiameremo il suo *inverso additivo* o *opposto*), ovvero per ogni $a \in A$ esiste un $b \in A$ tale che

$$a + b = b + a = 0$$

che verrà indicato con $b = -a$.

(5) *Il prodotto è associativo*, ovvero per ogni $a, b, c \in A$ si ha

$$(ab)c = a(bc).$$

(6) *Esiste un elemento neutro per il prodotto* (denotato con 1), tale che per ogni $a \in A$ si ha

$$a1 = 1a = a.$$

(7) *Vale la proprietà distributiva del prodotto rispetto alla somma*, ovvero per ogni $a, b, c \in A$ si ha

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

Se inoltre *Il prodotto è commutativo*, ovvero per ogni $a, b \in A$ si ha $ab = ba$, allora $(A, +, \cdot)$ è detto **anello commutativo**.

Chiaramente l'insieme $\mathbb{Z}$ dei numeri interi soddisfa tutte le proprietà nella Definizione 3.1 ed è quindi un anello commutativo. Si noti che negli interi non vale la proprietà analoga alla (4) per il prodotto. Cioè non è vero che ogni elemento $a \in \mathbb{Z}$ ha inverso rispetto al prodotto (non in $\mathbb{Z}$), che dovrebbe essere un $b \in \mathbb{Z}$ tale che $ab = ba = 1$. Ad esempio, non esiste nessun numero intero b tale che $2b = 1$.
Tale proprietà è invece verificata per tutti gli $a \neq 0$ nell'insieme $\mathbb{Q}$ dei numeri razionali.

Definizione 3.2. Un anello commutativo in cui ogni elemento diverso da 0 ha un inverso rispetto al prodotto si dice **campo**.

L'insieme dei razionali $\mathbb{Q}$ è quindi un esempio di campo (ad esempio, 2 ha come inverso moltiplicativo $\frac{1}{2}$ in $\mathbb{Q}$). Un altro esempio è dato dall'insieme $\mathbb{R}$ dei numeri reali e da quello $\mathbb{C}$ dei numeri complessi.
Nella matematica e nelle sue applicazioni si incontrano vari esempi di anelli diversi dall'insieme degli interi $\mathbb{Z}$ (ne vedremo altri nei prossimi paragrafi e capitoli). Lavorare con questa definizione astratta permette di dimostrare in piena generalità risultati e formule che poi saranno validi in ogni anello, senza doverli dimostrare caso per caso (esattamente come già visto con la nozione di gruppo). Ad esempio il Lemma 2.63, dimostrato per un gruppo qualsiasi, è valido per ogni gruppo che incontreremo.

Osservazione 3.3. Il fatto che l'anello $\mathbb{Z}$ si estenda al campo $\mathbb{Q}$, cioè il fatto che gli interi non zero, come razionali, ammettano (in $\mathbb{Q}$) un inverso moltiplicativo, ha un importante conseguenza. Questa è la cosiddetta *legge di annullamento del prodotto*:

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

cioè se un prodotto è nullo allora almeno uno dei due fattori deve essere nullo[1].
Possiamo dimostrare facilmente questa legge. Sia $ab = 0$ e supponiamo per assurdo che a e b siano entrambi diversi da zero. Considerando gli interi come particolari razionali, e quindi l'uguaglianza $ab = 0$ come un'uguaglianza tra razionali, possiamo moltiplicare entrambi i membri per $\frac{1}{a}$ (che esiste nei razionali sotto l'ipotesi $a \neq 0$). Così troviamo da una parte $\frac{1}{a}(ab) = \frac{1}{a}0 = 0$ e dall'altra

$$\frac{1}{a}(ab) = (\frac{1}{a}a)b = 1b = b\,.$$

Ne deduciamo $b = 0$, che contraddice l'ipotesi che a e b fossero entrambi nulli.

Sottolineiamo che tale proprietà non va data per scontata. Infatti vedremo, nei paragrafi e capitoli successivi, alcuni anelli in cui essa non vale. D'altra parte risulta chiaro dalla discussione precedente che questa proprietà è sempre soddisfatta in un campo.

Un operazione fondamentale definita nell'anello degli interi $\mathbb{Z}$, e che useremo continuamente in questo capitolo, è *la divisione con resto*. Più precisamente, vale il seguente risultato.

Teorema 3.4. *Siano $a, b \in \mathbb{Z}$, con $b \neq 0$. Allora esiste un'unica coppia (q, r) di interi tali che valgono le due seguenti condizioni:*

$$a = bq + r \tag{3.1}$$

$$0 \leqslant r < |b| \tag{3.2}$$

(dove $|b|$ indica il cosiddetto valore assoluto di b, uguale a b se $b \geqslant 0$ e a $-b$ se $b < 0$; in altre parole se necessario si cambia il segno di b per renderlo non negativo). L'intero q si dice **quoziente** *e l'intero r* **resto** *della divisione.*

Esempio 3.5. Siano $a = 7$, $b = 2$. Si ha

$$7 = 2 \cdot 3 + 1$$

quindi quoziente e resto della divisione sono rispettivamente $q = 3$ e $r = 1$. Si noti che ad esempio si ha anche

$$7 = 2 \cdot 2 + 3$$

oppure

$$7 = 2 \cdot 4 + (-1)$$

[1] Proprietà usata spesso quando si risolvono le equazioni. Ad esempio per risolvere $x^2 - x = 0$ osservo che $x^2 - x = x(x-1)$, e quindi la mia equazione si riscrive $x(x-1) = 0$. Per la legge di annullamento del prodotto questa è verificata se $x = 0$ o $x - 1 = 0$.

ma queste due uguaglianze, pur essendo del tipo (3.1), non verificano la (3.2). Questo perché nella prima il resto 3 non è minore di $b = 2$, nella seconda il resto -1, pur essendo minore di $|b| = 2$ non è maggiore o uguale a zero.
Questo esempio mostra che affinché quoziente e resto siano unici e determinati da a e b, la condizione (3.2) è necessaria.

Osservazione 3.6. Come enunciato nel Teorema 3.4, a e b possono essere anche negativi. Ad esempio se $a = -7$ e $b = 2$, si ha

$$-7 = 2 \cdot (-4) + 1 \,.$$

Oppure se $a = 7$ e $b = -2$ si ha

$$7 = (-2) \cdot (-3) + 1 \,.$$

Un'applicazione importante dell'algoritmo della divisione è la possibilità di *scrivere un qualunque numero intero positivo in qualsiasi base* $b \geqslant 2$.
Prima di dare la definizione precisa, osserviamo che quando scriviamo un qualunque numero in notazione decimale, ad esempio $n = 1375$, le cifre $1, 3, 7, 5$ indicano (a partire da destra a sinistra) quante sono le unità, quante le decine, quante le centinaia etc., ovvero

$$1375 = 1 \cdot 1000 + 3 \cdot 100 + 7 \cdot 10 + 5 \,.$$

Usando la notazione usuale per le potenze

$$1375 = 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 5 \,.$$

Quindi qualunque numero non negativo può essere scritto come somma di potenze decrescenti di 10 (l'ultima, a moltiplicare 5, sarebbe $10^0 = 1$ e non la scriviamo) precedute da un coefficiente che può essere un qualunque numero tra 0 e 9 (ovvero un qualunque numero minore di 10 e maggiore o uguale a zero). Vedremo ora che, usando l'algoritmo della divisione, la stessa cosa può essere fatta con un qualunque altro numero naturale maggiore o uguale di 2 al posto di 10.

Teorema 3.7. *Sia $b \geqslant 2$ un intero fissato. Allora ogni intero positivo n può essere scritto in modo unico nella forma seguente*

$$n = r_N b^N + r^{N-1} b^{N-1} + \cdots + r_1 b + r_0 \tag{3.3}$$

con $0 \leqslant r_i < b$ per tutti gli $i = 0, 1, \ldots, N$ (e $r_N \neq 0$). Si scrive allora $n = (r_N\, r_{N-1} \cdots r_1\, r_0)_b$ e si dice che $(r_N\, r_{N-1} \cdots r_1\, r_0)_b$ è la scrittura di n in base b.

Dimostrazione. Come abbiamo anticipato, per dimostrare il teorema si usa l'algoritmo della divisione. Iniziamo col dividere n per b ottenendo

$$n = q_0 b + r_0 \,. \tag{3.4}$$

Se q_0 è minore di b, abbiamo finito: la (3.4) sarebbe già come nel teorema. Cioè una combinazione di potenze di b (in questo caso compaiono solo $b = b^1$ e, sottointesa, $b^0 = 1$ che moltiplica r_0) con coefficienti q_0 e r_0 minori di b (r_0 lo è sicuramente per definizione di resto), come prevede il Teorema 3.7.
Se invece $q_0 \geqslant b$, allora dividiamo q_0 per b:

$$q_0 = q_1 b + r_1 \tag{3.5}$$

e sostituiamo la (3.5) nella (3.4), ottenendo

$$n = (q_1 b + r_1) b + r_0 = q_1 b^2 + r_1 b + r_0 \,. \tag{3.6}$$

Di nuovo, se q_1 è minore di b, abbiamo finito: la (3.6) sarebbe proprio una combinazione di potenze di b (in questo caso compaiono b^2, $b^1 = b$ e il termine di grado zero) con coefficienti q_1, r_1, r_0 minori di b.
Se invece $q_1 \geqslant b$, iteriamo il procedimento. Dividiamo q_1 per b:

$$q_1 = q_2 b + r_2 \tag{3.7}$$

e sostituiamo la (3.7) nella (3.6), ottenendo

$$n = (q_2 b + r_2) b^2 + r_1 b + r_0 = q_2 b^3 + r_2 b^2 + r_1 b + r_0 \tag{3.8}$$

e se q_3 è minore di b, abbiamo finito.
Dal momento che i quozienti successivi sono sempre più piccoli, arriveremo sicuramente a un quoziente minore di b. A questo punto il procedimento si arresta e otteniamo la formula cercata.[2]. □

Osservazione 3.8. La condizione che il primo coefficiente r_N sia diverso da zero serve a evitare addendi inutili nella (3.3) e garantire l'unicità della scrittura in base b. Ad esempio, 1375 è anche uguale a $0 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 5$. Ovvero può esser scritto come 01375, ma chiaramente il primo 0 si può essere omesso.

Esempio 3.9. Scriviamo il numero $n = 19$ in base $b = 2$ con il procedimento descritto sopra: iniziamo dividendo 19 per 2:

$$19 = 9 \cdot 2 + 1 \,.$$

[2]Si noti che se avessimo ammesso come base $b = 1$ questo non sarebbe vero. Dividendo n per 1 si ottiene $n = 1 \cdot n + 0$ ovvero quoziente n, che può essere diviso per 1 rendendo sempre quoziente n, e il procedimento non si arresta mai.

Poichè il quoziente ottenuto $q_0 = 9$ è maggiore di 2, eseguiamo la seconda divisione:

$$9 = 4 \cdot 2 + 1$$

e sostituiamo

$$19 = (4 \cdot 2 + 1) \cdot 2 + 1 = 4 \cdot 2^2 + 1 \cdot 2 + 1\,. \tag{3.9}$$

Questa non à ancora l'espressione di 19 in base 2 in quanto l'ultimo quoziente ottenuto, $q_1 = 4$, non è ancora minore di 2. Dividendo ulteriormente otteniamo

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

e sostitutendo al posto di 4 nella (3.9) si ottiene

$$19 = (2 \cdot 2 + 0) \cdot 2^2 + 1 \cdot 2 + 1 = 2 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1\,. \tag{3.10}$$

Non abbiamo ancora finito in quanto l'ultimo quoziente ottenuto, $q_2 = 2$, non è minore di 2. Eseguiamo allora un'ulteriore divisione per 2

$$2 = 1 \cdot 2 + 0\,.$$

Ora l'ultimo quoziente ottenuto, $q_3 = 1$, è minore di 2. Sostituendo nella (3.10) si ottiene allora

$$19 = (1 \cdot 2 + 0) \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 \tag{3.11}$$

che è l'uguaglianza cercata, che esprime 19 come combinazione di potenze di 2 con coefficienti minori di 2 (cioè 0 o 1). Possiamo anche scrivere che

$$19 = (1\,0\,0\,1\,1)_2$$

ovvero, più semplicemente, che 19 in base 2 si scrive come

$$10011\,.$$

Osservazione 3.10. Si noti che, viceversa, dato un numero in una certa base, è facile verificare di quale numero si tratti in notazione decimale. Ad esempio, in base 2 il numero 1101 rappresenta, in base alla definizione data nella formula (3.3),

$$1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 = 13\,.$$

La numerazione in base $b = 2$ (o *numerazione binaria*) è di particolare importanza nell'informatica in quanto, esprimendo qualunque numero come successione di 0 e 1, consente a un computer di registrarlo o esprimerlo come successione di stati spento/acceso.

Storicamente, altri casi importanti sono $b = 16$ (numerazione *esadecimale*) o $b = 8$ (numerazione *ottale*). Tuttavia, come afferma il Teorema 3.7, si può usare qualunque $b \geqslant 2$. Ad esempio, se volessimo scrivere 23 in base 7, eseguiremmo la divisione

$$23 = 3 \cdot 7 + 2$$

e poiché il quoziente ottenuto $q_1 = 3$ è già minore della base $b = 7$, il procedimento si ferma qui. Il numero 23, in base 7, si scrive semplicemente come $(3\ 2)_7$.

3.2 Divisori e numeri primi

Se, dividendo un intero a per un intero b capita che il resto sia zero, ovvero che

$$a = b \cdot q$$

allora si dice che a **è un multiplo di** b, o equivalentemente che b **è un divisore di** a (o anche che b **divide** a). In formule, si scrive $b|a$.

Ad esempio, sia $a = 20$. È facile verificare[3] che i divisori di 20 sono

$$\pm 1, \pm 20, \pm 2, \pm 5, \pm 4, \pm 10\,.$$

Si noti che se b è un divisore di a, ovvero se $a = bq$ per qualche q, allora anche $-b$ è divisore di a in quanto vale chiaramente anche $a = (-b)(-q)$.
Si osservi inoltre che tra i divisori di $a \in \mathbb{Z}$ ci sono sicuramente ± 1 (in quanto $a = 1 \cdot a$ e $a = (-1) \cdot (-a)$) e $\pm a$ (in quanto $a = a \cdot 1$ e $a = (-a) \cdot (-1)$). I restanti divisori si chiamano **divisori propri**.
I numeri che non hanno divisori propri sono di fondamentale importanza nella matematica e in tutte le sue applicazioni.

Definizione 3.11. Un numero intero $p \neq \pm 1$ si dice **primo** se i suoi unici divisori sono ± 1 e $\pm p$.

Come vedremo, i numeri primi sono di grandissima importanza per gli scopi di questo corso, quindi è importante conoscerne le proprietà.
Ad esempio, una prima proprietà, che caratterizza i numeri primi, è la seguente:

$$p|ab \Rightarrow p|a \vee p|b,$$

ovvero se un numero primo divide un prodotto, esso divide necessariamente uno dei fattori.

[3] Vedremo dopo un metodo generale.

Per convincersi che tale proprietà non vale per numeri in generale, si noti ad esempio che 10 divide il prodotto $4 \cdot 15 = 60$ ma non è vero né che 10 divide 4 né che 10 divide 15. Il motivo è che essendo $10 = 2 \cdot 5$, esso divide $4 \cdot 15$ in quanto $2|4$ e $5|15$. Per un numero primo p che divida un prodotto ab una cosa del genere non è possibile in quanto non avendo divisori propri non può accadere che si scomponga in un prodotto in cui un fattore divide a e uno divida b.

La proprietà più importante dei numeri primi è però sicuramente quella espressa nel seguente risultato.

Teorema 3.12 (Teorema fondamentale dell'aritmetica)**.** *Dato un qualsiasi numero intero $a > 1$, esiste un unica decomposizione*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

in primi positivi $p_1, p_2, \ldots, p_s$ tali che $p_1 > p_2 > \cdots > p_s$ e $\alpha_1, \alpha_2, \ldots, \alpha_s > 0$.

Il teorema afferma in un certo senso che i primi sono i "mattoni" di cui si compongono tutti i numeri interi.

Esempio 3.13. La decomposizione in primi di $a = 20$ è

$$20 = 5 \cdot 2^2 .$$

In questo caso si ha $s = 2$, $p_1 = 5$ e $p_2 = 2$ cioè 20 si decompone in un prodotto con fattori 2 e 5. Inoltre $\alpha_1 = 1$ e $\alpha_2 = 2$. Non esiste alcun altra decomposizione di 20 che soddisfi le condizioni del Teorema 3.12.

Osservazione 3.14. La decomposizione di un intero in fattori primi ci permette di trovare velocemente tutti i suoi divisori: essi saranno tutti quelli del tipo $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, con gli esponenti $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, $\ldots$, $0 \leqslant \beta_s \leqslant \alpha_s$.
Ad esempio, per $20 = 5^1 \cdot 2^2$, i divisori positivi sono tutti e soli i numeri del tipo $5^{\beta_1} 2^{\beta_2}$ con $0 \leqslant \beta_1 \leqslant 1$ e $0 \leqslant \beta_2 \leqslant 2$, ovvero

$$5^0 2^0 = 1, \;\; 5^0 2^1 = 2, \;\; 5^0 2^2 = 4, \;\; 5^1 2^0 = 5, \;\; 5^1 2^1 = 10, \;\; 5^1 2^2 = 20 .$$

Dati due numeri interi a e b possiamo considerare i loro divisori in comune. Ad esempio, è facile verificare che $a = 30$ e $b = 45$ hanno come divisori comuni

$$\pm 1, \pm 3, \pm 5, \pm 15 .$$

Notiamo che tutti questi divisori comuni dividono 15 o, in altre parole, 15 è multiplo di tutti i divisori comuni. La seguente definizione estende questa osservazione al caso generale.

Definizione 3.15. Siano a e b due interi non entrambi nulli. Un intero positivo d si dice **massimo comune divisore di a e b** se

(1) d è un divisore comune di a e b (in simboli, $d|a \wedge d|b$) e

(2) ogni altro divisore comune di a e b divide d (in simboli, $c|a \wedge c|b \Rightarrow c|d$).

Osservazione 3.16. La condizione che a e b siano non entrambi nulli serve a garantire l'esistenza del massimo comune divisore: 0 ha come divisori tutti i numeri interi, in quanto $0 = n \cdot 0$ per ogni $n \in \mathbb{Z}$, quindi se $a = 0$ e $b = 0$ ogni intero sarebbe un divisore comune di a e b e non ce ne sarebbe uno massimo nel senso della Definizione 3.15[4].
Inoltre, la condizione che b sia positivo serve a garantire l'unicità. Per esempio, nell'esempio di sopra con $a = 30$ e $b = 45$ anche -15 è un divisore comune che è multiplo di ogni altro divisore comune.

Il massimo comune divisore di due interi a e b può essere calcolato semplicemente scrivendo prima tutti i divisori di a, poi tutti quelli di b (usando il metodo descritto nell'Osservazione 3.14) e poi guardando quale tra tutti i divisori comuni è multiplo degli altri.
Tuttavia, tale metodo non è molto efficace in quanto richiede la conoscenza della scomposizione in fattori primi di a e b, che non sempre è facile da trovare. Vedremo quindi un altro metodo, basato sull'algoritmo della divisione, che fornisce informazioni aggiuntive.

Il metodo funziona come segue. Si inizia dividendo a per b:

$$a = bq_1 + r_1\,. \tag{3.12}$$

Si divide poi b per il resto r_1

$$b = r_1 q_2 + r_2 \tag{3.13}$$

ottenendo un secondo resto r_2. A questo punto si divide il primo resto per il secondo resto

$$r_1 = r_2 q_3 + r_3, \tag{3.14}$$

il secondo resto per il terzo resto

$$r_2 = r_3 q_4 + r_4 \tag{3.15}$$

e così via, fino a che non si ottiene resto zero:

$$\vdots$$

[4]Invece uno solo tra a e b può essere nullo, ad esempio se $a = 0$ e $b > 0$, i divisori comuni di a e b sono tutti i divisori di b, e il massimo sarebbe b stesso.

$$r_n = r_{n+1}q_{n+2} + r_{n+2} \tag{3.16}$$

$$r_{n+1} = r_{n+2}q_{n+3}\,. \tag{3.17}$$

Affermiamo che l'ultimo resto r_{n+2} non nullo di queste divisioni successive è esattamente il massimo comune divisore di a e b.
Prima di mostrare perché, vediamo alcuni esempi.

Esempio 3.17. Siano $a = 45$ e $b = 30$, come sopra. Dividendo a per b otteniamo

$$45 = 30 \cdot 1 + 15$$

e dividendo $b = 30$ per il resto $r_1 = 15$ otteniamo

$$30 = 15 \cdot 2$$

Quindi l'ultimo resto prima di ottenere resto zero è 15, che risulta essere come avevamo già detto sopra il massimo comune divisore.

Esempio 3.18. Consideriamo ora $a = 42$ e $b = 30$. Dividendo a per b otteniamo

$$42 = 30 \cdot 1 + 12\,.$$

Dividendo $b = 30$ per il resto $r_1 = 12$ si ha

$$30 = 12 \cdot 2 + 6$$

e dividendo $r_1 = 12$ per il secondo resto $r_2 = 6$ si ottiene

$$12 = 6 \cdot 2$$

cioè resto zero: l'ultimo resto non nullo, 6, è quindi il massimo comune divisore.

Esempio 3.19. Infine, siano $a = 120$ e $b = 23$. Procedendo come sopra, si ha

$$120 = 23 \cdot 5 + 5$$

$$23 = 5 \cdot 4 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

L'ultimo resto non nullo è 1, che risulta essere quindi il massimo comune divisore.

L'ultimo esempio di sopra è un caso della seguente, importante

Definizione 3.20. Due interi a e b si dicono **primi tra loro** o **coprimi** se il loro massimo comune divisore è 1.

In altre parole, due interi sono coprimi se non hanno divisori comuni a parte il caso banale 1.

Vediamo ora perchè il procedimento per divisioni successive descritto e illustrato fornisce effettivamente il massimo comune divisore. Dobbiamo dimostrare che l'ultimo resto non nullo r_{n+2} che compare nella (3.16) è un divisore comune di a e b e che ogni altro divisore comune di a e b divide r_{n+2}.
Per dimostrare la prima affermazione, osserviamo che l'ultima divisione svolta, la (3.17) (quella con resto nullo), mostra che r_{n+2} divide r_{n+1} o, equivalentemente, che r_{n+1} è un multiplo di r_{n+2}. Sostituendola nella (3.16), si trova

$$r_n = r_{n+1}q_{n+2} + r_{n+2} = r_{n+2}q_{n+3}q_{n+2} + r_{n+2} = r_{n+2}(q_{n+3}q_{n+2} + 1) \tag{3.18}$$

che ci dice che r_{n+2} divide anche r_n o, equivalentemente, che r_n è un multiplo di r_{n+2}. Ora per brevità, riscriviamo la (3.18) come $r_n = r_{n+2}k$.
La divisione immediatamente precedente alla (3.16) sarà

$$r_{n-1} = r_n q_{n+1} + r_{n+1}\,. \tag{3.19}$$

Sostituendo sia $r_{n+1} = r_{n+2}q_{n+3}$ che $r_n = r_{n+2}k$ nella (3.19) otteniamo

$$r_{n-1} = r_n q_{n+1} + r_{n+1} = r_{n+2}kq_{n+1} + r_{n+2}q_{n+3} = r_{n+2}(kq_{n+1} + q_{n+3}) \tag{3.20}$$

che dimostra che r_{n+2} divide anche r_{n-1}. In altre parole, stiamo mostrando che r_{n+2} divide tutti resti r_{n+1}, r_n, r_{n-1}... delle divisioni effettuate, dall'ultima alla prima. Quando saremo arrivati alla (3.15) otterremo che r_{n+2} divide r_2, la (3.14) ci dirà che r_{n+2} divide r_1. Infine la (3.13) ci dirà che r_{n+2} divide b e la (3.12) ci dirà che r_{n+2} divide a. Quindi r_{n+2} è un divisore comune di a e b.
Per dimostrare che si tratta effettivamente del massimo comune divisore, basta mostrare che r_{n+2} è multiplo di qualunque divisore comune di a e b. Sia allora c un tale divisore comune: possiamo scrivere $a = ca'$ e $b = cb'$. Sostituendo queste due uguaglianze nella (3.12), otteniamo

$$ca' = cb'q_1 + r_1\,.$$

Portando il primo addendo al primo membro e mettendo in evidenza c scriviamo

$$c(a' - b'q_1) = r_1\,. \tag{3.21}$$

Questa uguaglianza ci dice che anche il primo resto r_1 è un multiplo di c. Per brevità, riscriviamo la (3.21) come $r_1 = cr_1'$. Sostituendo questa uguaglianza e la $b = cb'$ nella

(3.13), si ottiene

$$cb' = cr'_1 q_2 + r_2 \,.$$

Ancora una volta, portando il primo addendo a primo membro e mettendo in evidenza c, troviamo

$$c(b' - r'_1 q_2) = r_2 \,. \tag{3.22}$$

Questa uguaglianza ci dice che anche il secondo resto r_2 è un multiplo di c. Continuando in questo modo per sostituzioni successive nelle divisioni, dalla prima all'ultima, vediamo che tutti i resti sono un multiplo di c, compreso r_{n+2}. Quindi r_{n+2} è proprio il massimo comune divisore, come volevamo.

Vediamo ora una importante proprietà del massimo comune divisore, che ci sarà molto utile nel paragrafo successivo.

Proposizione 3.21. *Sia d il massimo comune divisore di due interi a e b. Allora, esistono due interi $x, y \in \mathbb{Z}$ tali che*

$$d = ax + by \,. \tag{3.23}$$

Dimostrazione. Denotiamo il massimo comune divisore di a e b con r_{n+2} come nella (3.16). Iniziamo quindi riscrivendo la (3.16) come

$$r_{n+2} = r_n - r_{n+1} q_{n+2}$$

e cioè come

$$r_{n+2} = x_n r_n + y_{n+1} r_{n+1} \tag{3.24}$$

per due interi x_n, y_{n+1}. Ora notiamo che tutte le divisioni precedenti possono essere scritte nella forma

$$r_i = r_{i-2} - r_{i-1} q_i$$

per $i + 3, 4, \ldots, n + 1$. Quindi sostituendo questa scrittura di r_{n+1} in 3.24 otteniamo

$$\begin{aligned} r_{n+2} &= x_n r_n + y_{n+1} \left(r_{n-1} - r_n q_{n+1} \right) \\ &= \left(x_n - y_{n+1} q_{n+1} \right) r_n + y_{n+1} r_{n-1} \end{aligned}$$

e cioè come

$$r_{n+2} = x_{n-1} r_{n-1} + y_n r_n \tag{3.25}$$

per due interi x_{n-1}, y_n. Continuando con le sostituzioni dei resti precedenti sino a r_3 otteniamo

$$r_{n+2} = x_1 r_1 + y_2 r_2 \,.$$

Sostituendo in quest'ultima la (3.13) nella forma $r_2 = b - r_1 q_2$ si arriva a

$$\begin{aligned} r_{n+2} &= x_1 r_1 + y_2 (b - r_1 q_2) \\ &= y_2 b + (x_1 - y_2 q_2) r_1 . \end{aligned} \tag{3.26}$$

Ora dalla (3.12) otteniamo $r_1 = a - bq_1$ che sostituita nella (3.26) rende

$$\begin{aligned} r_{n+2} &= y_2 b + (x_1 - y_2 q_2)(a - bq_1) \\ &= (x_1 - y_2 q_2) a + (y_2 + y_2 q_2 q_1 - x_1 q_1) b . \end{aligned}$$

Abbiamo quindi scritto il massimo comune divisore d di a e b come $d = ax + by$ dove $x = x_1 - y_2 q_2$ e $y = y_2 + y_2 q_2 q_1 - x_1 q_1$. □

Consideriamo il caso dell'Esempio 3.19 in cui, tramite la successione di divisioni

$$120 = 23 \cdot 5 + 5$$

$$23 = 5 \cdot 4 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

abbiamo mostrato che il massimo comune divisore di 120 e 23 è $d = 1$ (l'ultimo resto non nullo delle divisioni). Allo scopo di trovare i due interi x e y tali che $120x + 23y = 1$, la cui esistenza è prevista nella Proposizione 3.21, iniziamo con l'osservare che se nella penultima divisione $3 = 2 \cdot 1 + 1$ portiamo il primo addendo al primo membro, ovvero

$$1 = 3 - 2 \cdot 1 = 1 \cdot 3 + (-1) \cdot 2 , \tag{3.27}$$

otteniamo una scrittura del massimo comune divisore come combinazione degli ultimi due resti 2 e 3 ottenuti prima del massimo comune divisore stesso. Ora, combinando la (3.27) con la divisione precedente $5 = 3 \cdot 1 + 2$ possiamo scrivere 1 come combinazione dei penultimi due resti 5 e 3. Più precisamente, portando al primo membro nella $5 = 3 \cdot 1 + 2$ otteniamo $2 = 5 - 3 \cdot 1$ che sostituito al posto di 2 nella (3.27) ci dà

$$1 = 1 \cdot 3 + (-1) \cdot (5 - 3 \cdot 1) = 3 - 5 + 3 = 3 \cdot 2 + (-1) \cdot 5. \tag{3.28}$$

Iteriamo questo procedimento: usando la divisione $23 = 5 \cdot 4 + 3$, riscritta come $3 =$

$23 - 5 \cdot 4$, e sostituendo al 3 che compare nella (3.28) si ottiene

$$\begin{aligned} 1 &= 3 \cdot 2 + (-1) \cdot 5 = (23 - 5 \cdot 4) \cdot 2 + (-1) \cdot 5 = \\ &= 23 \cdot 2 - 5 \cdot 4 \cdot 2 + (-1) \cdot 5 = 23 \cdot 2 + (-9) \cdot 5 \end{aligned} \tag{3.29}$$

cioè siamo arrivati a scrivere il massimo comune divisore come combinazione di 23 e 5. A questo punto, possiamo usare la prima divisione $120 = 23 \cdot 5 + 5$, riscritta $5 = 120 - 23 \cdot 5$, per esprimere nella combinazione (3.29) il 5 in funzione di 120 e 23. In formule, sostituendo,

$$\begin{aligned} 1 &= 23 \cdot 2 + (-9) \cdot 5 = 23 \cdot 2 + (-9) \cdot (120 - 23 \cdot 5) = \\ &= 23 \cdot 2 + (-9) \cdot 120 + (-9) \cdot (-5) \cdot 23 = \\ &= 47 \cdot 23 + (-9) \cdot 120 \end{aligned} \tag{3.30}$$

e siamo riusciti ad esprimere 1 nella forma $23x + 120y$, con $x = 47$ e $y = -9$.

Vediamo un ulteriore esempio. Sia $a = 42$ e $b = 30$, per i quali abbiamo già mostrato che il massimo comune divisore è 6 nell'Esempio 3.18 mediante la successione di divisioni

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2\,. \end{aligned}$$

Come sopra, usiamo la penultima divisione $30 = 12 \cdot 2 + 6$ per esprimere il massimo comune divisore $6 = 30 + (-2) \cdot 12$ come combinazione di 30 e 12. In tale uguaglianza sostituiamo $12 = 42 - 30$, ricavata dalla prima divisione, ottenendo

$$6 = 30 + (-2) \cdot (42 - 30).$$

Procedendo come sopra, otteniamo

$$6 = 30 + (-2) \cdot 42 + 2 \cdot 30 = 3 \cdot 30 + (-2) \cdot 42\,,$$

cioè siamo riusciti, come volevamo, ad esprimere 6 nella forma $30x + 42y$, con $x = 3$ e $y = -2$.

Osservazione 3.22. Se a e b sono interi uno multiplo dell'altro, diciamo a è multiplo di b, allora il procedimento descritto sopra non si applica. Ad esempio se $a = 140$ e $b = 14$, la prima divisione $140 = 14 \cdot 10 + 0$ dà già resto zero, e quindi non possiamo usare il fatto che il massimo comune divisore è l'ultimo resto non nullo delle divisioni successive. Tuttavia, in tal caso il massimo comune divisore è semplicemente uguale a

b, che in tale situazione è chiaramente divisore di a e anche di b, ed è chiaramente il massimo. Anche per ottenere la forma $d = ax + by$ non è necessario applicare nessun procedimento di divisioni, in quanto essendo $d = b$ basta scrivere $d = a \cdot 0 + b \cdot 1$. Lo stesso ragionamento si applica al caso in cui $a = 0$ o $b = 0$.

Concludiamo questo paragrafo con la seguente domanda: dato un intero positivo N, quanti sono gli interi positivi $k < N$ coprimi con N (ovvero quelli che hanno come unico divisore in comune con N l'intero 1)?
Il numero di tali interi si denota con $\phi(N)$, e definisce quindi una funzione ϕ detta **funzione di Eulero**, che è di fondamentale importanza nelle applicazioni che vedremo nell'ultima sezione di questo capitolo.
Vediamo allora come calcolare $\phi(N)$ per ogni N. L'idea è sfruttare il fatto che N, in base al teorema fondamentale dell'aritmetica, si può scrivere come $N = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_s^{\alpha_s}$ con $P_1, P_2, \ldots, P_s$ primi.
Innanzitutto, se N è un numero primo P, si ha

$$\phi(P) = P - 1\,. \tag{3.31}$$

Infatti, dal momento che P è primo, per definizione esso non ha altri divisori (positivi) oltre 1 e P stesso. Quindi, un numero k che ammette divisori diversi da 1 in comune con P è necessariamente un multiplo di P. Questo chiaramente non può succedere se $k < P$: tutti gli interi $k < P$, ovvero $k = 1, 2, \ldots, P - 1$ sono coprimi con P, da cui la (3.31).
Generalizziamo ora al caso in cui $N = P^\alpha$ è potenza di un primo:

$$\phi(P^\alpha) = P^\alpha - P^{\alpha-1}\,. \tag{3.32}$$

Infatti, $\phi(P^\alpha)$ è dato dai numeri positivi minori di P^α che sono coprimi con P^α. Possiamo contarli come tutti i numeri da 1 a P^α, che sono proprio P^α, meno quelli che hanno divisori in comune (oltre a 1) con P^α. Se dimostriamo allora che gli interi minori o uguali a P^α che hanno divisori in comune con P^α sono $P^{\alpha-1}$, avremo finito.
Dal momento che P^α è potenza di P, un intero k può avere un divisore in comune con P^α solo se contiene P tra i suoi fattori, ovvero solo se k è un multiplo di P. Tali multipli sono chiaramente

$$P,\ 2P,\ 3P, \ldots, P^{\alpha-1}P$$

(ci siamo fermati a $P^{\alpha-1}P = P^\alpha$ perché dobbiamo considerare solo interi minori o uguali a P^α). Quindi il numero di interi in questo intervallo non coprimi con P^α è $P^{\alpha-1}$, come volevamo.

Infine, per calcolare $\phi(N)$ per ogni N useremo il seguente risultato, che non dimostriamo.

Lemma 3.23. *Se N_1 e N_2 sono due interi primi tra loro, allora*

$$\phi(N_1N_2) = \phi(N_1)\phi(N_2)\,. \tag{3.33}$$

Possiamo combinare questo lemma con la formula (3.32) per calcolare la funzione di Eulero per ogni N.
Supponiamo che sia, in base al teorema fondamentale dell'aritmetica, $N = P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_s^{\alpha_s}$. Chiaramente i fattori $P_1^{\alpha_1}$, $P_2^{\alpha_2},\ldots,P_s^{\alpha_s}$ sono tutti primi tra loro in quanto potenze di primi diversi. Concludiamo che, in base al Lemma 3.23,

$$\phi(N) = \phi(P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_s^{\alpha_s}) = \phi(P_1^{\alpha_1})\phi(P_2^{\alpha_2})\cdots\phi(P_s^{\alpha_s}) =$$

(per la (3.32))

$$= (P_1^{\alpha_1} - P_1^{\alpha_1-1})(P_2^{\alpha_2} - P_2^{\alpha_2-1})\cdots(P_s^{\alpha_s} - P_s^{\alpha_s-1})\,. \tag{3.34}$$

Se nelle parentesi tonde che compaiono nella (3.34) mettiamo in evidenza rispettivamente $P_1^{\alpha_1}, P_2^{\alpha_2},\ldots,P_s^{\alpha_s}$, notiamo che

$$\phi(N) = \left[P_1^{\alpha_1}\left(1-\frac{1}{P_1}\right)\right]\left[P_2^{\alpha_2}\left(1-\frac{1}{P_2}\right)\right]\cdots\left[P_s^{\alpha_s}\left(1-\frac{1}{P_s}\right)\right]\,. \tag{3.35}$$

Ovvero, permutando i fattori,

$$\phi(N) = P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_s^{\alpha_s}\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\cdots\left(1-\frac{1}{P_s}\right) \tag{3.36}$$

che, ricordando che $P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_s^{\alpha_s}$ è proprio N, significa

$$\phi(N) = N\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\cdots\left(1-\frac{1}{P_s}\right)\,. \tag{3.37}$$

Questa è la formula che si trova solitamente nei libri per la funzione di Eulero ϕ.
Ad esempio, se $N = 100$, abbiamo $N = 5^2\cdot 2^2$, quindi

$$\phi(100) = 100\left(1-\frac{1}{5}\right)\left(1-\frac{1}{2}\right) = 100\cdot\frac{4}{5}\cdot\frac{1}{2} = 40.$$

Osserviamo che il calcolo di ϕ mediante la formula (3.37) richiede di conoscere la decomposizione di N in fattori primi, che non è sempre facile da trovare.

Osservazione 3.24. Lo studio dei numeri primi, e in particolare della loro distribuzione nell'insieme dei numeri interi, costituisce un capitolo fondamentale nella matematica. Intanto, sappiamo che i numeri primi sono infiniti. La dimostrazione di questo fatto è dovuta ad Euclide ed è apprezzata ancora oggi per la sua semplicità ed eleganza. Se per assurdo i primi fossero in numero finito, diciamo $p_1, p_2,\ldots,p_k$, il numero

$N = p_1 p_2 \cdots p_k + 1$ sarebbe un numero non divisibile per nessun primo. Infatti il resto della divisione di N per uno qualunque dei p_i sarebbe sempre 1, ma questo per il teorema fondamentale dell'aritmetica non è possibile a meno che non sia primo con $p_1, p_2, \ldots, p_k$. Quindi deve esistere un altro primo che divide N (possibilmente anche N stesso), contraddicendo l'ipotesi che i primi fossero solo $p_1, p_2, \ldots, p_k$.
Come è distribuito tale insieme infinito all'interno degli interi? Quanto è raro trovare primi quando si considerano numeri sempre più grandi?
Da una parte, si congettura che esistano infinite coppie di numeri primi a distanza 2 l'uno dall'altro (ad esempio 3 e 5, oppure 17 e 19), detti *numeri primi gemelli*. Dall'altra esistono sequenze lunghe quanto vogliamo di numeri che non contengono nessun primo. Dato n, la sequenza

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

è una sequenza di $n - 1$ numeri consecutivi (quindi possiamo renderla lunga a piacere scegliendo n) in cui nessuno è primo. Infatti, $n! + 2$ è divisibile per 2 in quanto sia $n!$ che 2 lo sono (ricordiamo che $n!$ è il prodotto di tutti i numeri naturali da 1 a n), $n! + 3$ è divisibile per 3 in quanto sia $n!$ che 3 lo sono, e così via.
Un importante teorema afferma che se $\pi(n)$ indica il numero dei primi minori di n, allora la quantità $\frac{\pi(n)}{n}$ (che descrive la percentuale di primi minori di n rispetto al totale dei numeri da 1 a n) si avvicina sempre di più a $\frac{1}{\log n}$ (ovvero il rapporto tra $\frac{\pi(n)}{n}$ e $\frac{1}{\log n}$ tende a 1 al crescere di n).

3.3 Congruenze e aritmetica modulare

Basandoci sui risultati esposti nella prima parte di questo capitolo, introdurremo e studieremo ora un'importante relazione di equivalenza sull'insieme dei numeri interi, la cosiddetta *congruenza modulo n*.

Definizione 3.25. Sia n un intero positivo fissato. Dati $a, b \in \mathbb{Z}$, diremo che a è **congruo a** b **modulo** n se a e b divisi per n danno lo stesso resto. Equivalentemente, a è congruo a b modulo n se la differenza $a - b$ è un multiplo di n.

Che le due formulazioni della definizione appena data siano equivalenti si vede facilmente. Infatti, da una parte, se a e b divisi per n danno lo stesso resto, ovvero $a = nq_1 + r$ e $b = nq_2 + r$, allora

$$a - b = (nq_1 + r) - (nq_2 + r) = nq_1 + r - nq_2 - r = nq_1 - nq_2 = n(q_1 - q_2)\,,$$

ovvero la differenza $a - b$ è un multiplo di n.
Viceversa, supponiamo che $a - b = kn$ per qualche k, ovvero $a = b + kn$. Se il resto della divisione di b per n è r, ovvero $b = nq + r$, allora sostituendo in $a = b + kn$ si

trova

$$a = b + kn = nq + r + kn = n(q + k) + r$$

da cui si vede che anche a, divisa per n, ha resto r (con quoziente $q + k$).

Per indicare che a è congruo a b modulo n, scriveremo

$$a \equiv b \pmod{n}$$

o anche

$$a \equiv_n b\,.$$

Mostriamo ora che la congruenza è una relazione di equivalenza, ovvero che gode delle proprietà riflessiva, simmetrica e transitiva (Definizione 2.6). Innanzitutto, si ha

$$a - a = 0 = 0 \cdot n$$

ovvero la differenza tra a e se stesso è un multiplo di n. Per la definizione data, questo significa che $a \equiv_n a$, cioè la congruenza è riflessiva.
Inoltre, se $a \equiv_n b$, ovvero $a - b = kn$ per qualche $k \in \mathbb{Z}$, si ha, semplicemente cambiando di segno,

$$b - a = -kn = (-k)n\,.$$

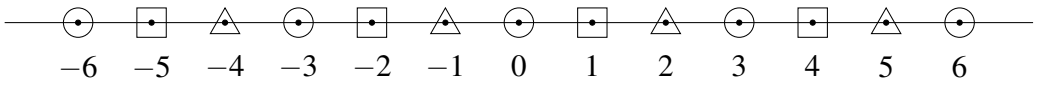
Perciò anche $b - a$ è un multiplo di n, cioè $b \equiv_n a$: la relazione di congruenza è simmetrica.
Infine, se $a \equiv_n b$ (ovvero $a - b = kn$ per qualche $k \in \mathbb{Z}$) e $b \equiv_n c$ (ovvero $b - c = ln$ per qualche $l \in \mathbb{Z}$) allora si ha

$$a - c = a - b + b - c = kn + ln = (k + l)n\,.$$

Quindi anche $a - c$ è un multiplo di n, cioè $a \equiv_n c$: la relazione di congruenza è transitiva.

In base alla teoria vista nel capitolo precedente, tale relazione ripartisce allora $\mathbb{Z}$ in classi di equivalenza non vuote e disgiunte. Una classe contiene tutti i numeri interi che hanno lo stesso resto quando li si divide per n.
Dal momento che il resto r della divisione per n deve soddisfare $0 \leqslant r < n$, i possibili resti sono $0, 1, 2, \ldots, n - 1$, quindi avremo esattamente n classi di equivalenza: $[0], [1], \ldots, [n - 1]$. L'insieme $\{[0], [1], \ldots, [n - 1]\}$ delle classi di equivalenza su $\mathbb{Z}$ della congruenza modulo n si denota con $\mathbb{Z}_n$.
Ad esempio, per $n = 3$ i possibili resti della divisione sono $0, 1, 2$. La classe $[0]$ di equivalenza di 0 contiene tutti i numeri a tali che $a = a - 0 = 3k$, ovvero i multipli di 3. La classe $[1]$ di equivalenza di 1 contiene tutti gli interi a tali che $a - 1 = 3k$, ovvero

$a = 3k+1$ (ad esempio 4, 7, 10, -2, -5 etc.). La classe $[2]$ di equivalenza di 2 contiene tutti gli interi a tali che $a - 2 = 3k$, ovvero $a = 3k + 2$ (ad esempio 5, 8, 11, -1, -4 etc.).



Nel disegno stiamo etichettando con lo stesso simbolo interi che appartengono alla stessa classe.

Se $n = 2$, abbiamo solo due resti possibili, 0 e 1 e quindi due classi, $[0]$ e $[1]$. La prima contiene tutti gli interi a del tipo $2k$ e la seconda tutti gli interi del tipo $2k + 1$. In altre parole, la partizione indotta su $\mathbb{Z}$ è quella in numeri pari e numeri dispari.

Come tutte le relazioni di equivalenza, la relazione di congruenza è una sorta di "uguaglianza in senso largo": consideriamo due numeri "uguali" se lo sono "a meno di mutipli di n".
La relazione di equivalenza per eccellenza, l'uguaglianza, verifica l'ovvia proprietà che se $a = b$ e $a' = b'$ allora $a + a' = b + b'$ e $aa' = bb'$. Lo stesso vale per la congruenza modulo n.

Lemma 3.26. *La congruenza modulo n verifica le due seguenti proprietà.*

(1) Se $a \equiv_n a'$ e $b \equiv_n b'$, allora $a + b \equiv_n a' + b'$.

(2) Se $a \equiv_n a'$ e $b \equiv_n b'$, allora $ab \equiv_n a'b'$.

Dimostrazione. (1): se $a \equiv_n a'$ e $b \equiv_n b'$ allora $a - a' = kn$ e $b - b' = ln$ per qualche $k, l \in \mathbb{Z}$. Dobbiamo dimostrare che anche la differenza tra $a + b$ e $a' + b'$ è un multiplo di n. Infatti

$$a + b - (a' + b') = a - a' + b - b' = kn + ln = (k + l)n$$

come volevamo.
(2): sotto la stessa ipotesi dobbiamo dimostrare che la differenza tra ab e $a'b'$ è un multiplo di n o, equivalentemente, che $ab = a'b' + qn$ per qualche $q \in \mathbb{Z}$. Usando $a - a' = kn$ e $b - b' = ln$ (riscrivibili come $a = a' + kn$ e $b = b' + ln$) abbiamo

$$ab = (a' + kn)(b' + ln) = a'b' + a'ln + knb' + kln^2 = a'b' + n(a'l + kb' + kln)\,,$$

il che dimostra l'asserto (con $q = a'l + kb' + kln$). □

Le due proprietà appena dimostrate, come vedremo, hanno molte applicazioni.
La prima è la data da alcuni criteri di divisibilità. È noto che un numero n è divisibile per 3 se e solo se la somma delle sue cifre è divisibile per 3 (lo stesso enunciato vale per 9).
Ad esempio, il numero $n = 1917$ è divisibile per 3 in quanto lo è la somma $1+9+1+7 = 18$ delle sue cifre; il numero 313 non lo è perché $3 + 1 + 3 = 10$ non lo è.
La spiegazione di tale criterio si basa proprio sul Lemma 3.26. Infatti, dire che le cifre di n (nella notazione decimale) sono $a_k, a_{k-1}, \ldots, a_1, a_0$ significa dire che

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \,. \tag{3.38}$$

Ora, poiché $10 = 3 \cdot 3 + 1$, si ha $10 \equiv_3 1$; applicando la (2) del Lemma 3.26 al particolare caso $a = a' = 10$, $b = b' = 1$, si ha che $10 \cdot 10 \equiv_3 1 \cdot 1$, ovvero $10^2 \equiv_3 1$; sempre applicando la stessa proprietà, si ha $10^2 \cdot 10 \equiv_3 1 \cdot 1$, ovvero $10^3 \equiv_3 1$ e così via. Si vede quindi che tutte le potenze positive 10^i di 10 sono congrue a 1 modulo 3.
Ora, questo implica che per ogni addendo della rappresentazione (3.38), che è del tipo $a_i 10^i$, valga $a_i 10^i \equiv_3 a_i$. Infatti, applicando di nuovo la (2) del Lemma 3.26, si ha che $a_i \equiv_3 a_i$ (la congruenza gode della proprietà riflessiva) e $10^i \equiv_3 1$ implicano proprio $a_i \cdot 10^i \equiv_3 a_i \cdot 1$.
A questo punto, poichè $a_k 10^k \equiv_3 a_k$, $a_{k-1} 10^{k-1} \equiv_3 a_{k-1}$ e così via fino a $a_1 10 \equiv_3 a_1$ (l'ultima, $a_0 \equiv_3 a_0$ è chiara per la riflessività della relazione di congruenza), possiamo sommare membro a membro usando la (1) del Lemma 3.26 e ottenere

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv_3 a_k + a_{k-1} + \cdots + a_1 + a_0 \,. \tag{3.39}$$

In altre parole, un qualunque n è congruente modulo 3 alla somma delle sue cifre.
Ma allora, poiché n divisibile per 3 significa che n è congruente a 0 modulo 3, si ha che n è divisibile per 3 se e solamente se la somma delle sue cifre è congruente a zero modulo 3, ovvero anche lei divisibile per 3. Il criterio è dimostrato.

Lo stesso criterio vale per la divisibilità per 9. Il motivo è che si ha anche $10 \equiv_9 1$, quindi si la stessa dimostrazione che abbiamo usato per 3 è valida in questo caso.

Il Lemma 3.26 ci consente quindi di definire una somma e una moltiplicazione sull'insieme $\mathbb{Z}_n$ delle classi di congruenza modulo n. Questo ci permetterà di fare calcoli su questo insieme, e sviluppare quella che si chiama **aritmetica modulare**.
Piú precisamente, date due classi $[i]$ e $[j]$ della congruenza modulo n, definiamo la loro somma come

$$[i] + [j] := [i + j] \tag{3.40}$$

e il loro prodotto come

$$[i] \cdot [j] := [ij]. \tag{3.41}$$

Il problema di tali definizioni è che definire la somma o il prodotto tra due classi mediante la somma o il prodotto dei rappresentanti i e j potrebbe essere ambiguo. Infatti, una stessa classe può essere rappresentata da interi diversi (ad esempio, modulo 3 si ha $[1] = [4]$). Quindi dobbiamo assicurarci che anche scegliendo rappresentanti diversi i' e j' per le classi $[i]$ e $[j]$ rispettivamente, la somma e il prodotto definiti da (3.40) e (3.41) diano sempre lo stesso risultato (ovvero la stessa classe).
Ma questo è garantito proprio dal Lemma 3.26. Infatti, supponiamo che sia $[i'] = [i]$ e $[j'] = [j]$: questo significa che $i \equiv_n i'$ e $j \equiv_n j'$. Ma allora, applicando la (1) del Lemma 3.26 si ha $i + j \equiv_n i' + j'$, ovvero $[i + j] = [i' + j']$. Quindi la somma che abbiamo definito non dipende dai rappresentanti scelti per le classi e non c'è ambiguità. Analogamente, sempre supponendo che sia $[i'] = [i]$ e $[j'] = [j]$, ovvero $i \equiv_n i'$ e $j \equiv_n j'$, applicando la (2) del Lemma 3.26 si ha $ij \equiv_n i'j'$, ovvero $[ij] = [i'j']$. Anche il prodotto per come lo abbiamo definito non dipende dai rappresentanti scelti per le classi e non c'è ambiguità.

A questo punto, come abbiamo fatto ogni volta che ci siamo trovati in presenza di un insieme con una o più operazioni, verifichiamo quali proprietà sono soddisfatte da queste operazioni.

(1) La somma è associativa:

$$([i] + [j]) + [k] = [i + j] + [k] = [(i + j) + k] =$$

(sfruttando l'associatività della somma usuale tra gli interi i, j, k)

$$[i + (j + k)] = [i] + [j + k] = [i] + ([j] + [k]).$$

(2) La somma è commutativa:

$$[i] + [j] = [i + j] = [j + i] = [j] + [i]$$

dove nell'uguaglianza centrale abbiamo sfruttato il fatto che la somma usuale tra interi è commutativa.

(3) Esiste un elemento neutro per la somma: la classe $[0]$ di 0. Infatti si ha

$$[i] + [0] = [i + 0] = [i] = [0 + i] = [0] + [i].$$

Si noti che, dal momento che $[0] = [kn]$ per ogni multiplo kn di n, possiamo anche scrivere $[i] + [kn] = [i]$ o, equivalentemente, $i + kn \equiv_n i$.

(4) Per ogni classe $[i]$ esiste un elemento inverso per la somma (ovvero un opposto), dato dalla classe $[-i]$:

$$[i] + [-i] = [i + (-i)] = [0]\,.$$

A volte si preferisce vedere ogni classe rappresentata da un numero compreso tra 0 e $n-1$. In questo caso si può anche rappresentare l'opposto di $[i]$ come $[n-i]$ in quanto chiaramente $-i \equiv_n n - i$. Ad esempio, in $\mathbb{Z}_5$ l'opposta della classe $[2]$ è certamente $[-2]$, che può essere anche espressa come $[5-2] = [3]$ (e infatti $[2] + [3] = [5] = [0]$).

(5) Il prodotto è associativo:

$$([i][j])[k] = [ij][k] = [(ij)k] =$$

(sfruttando l'associatività del prodotto usuale tra gli interi i, j, k)

$$[i(jk)] = [i][jk] = [i]([j][k])\,.$$

(6) Il prodotto è commutativo:

$$[i][j] = [ij] = [ji] = [j][i]$$

dove nell'uguaglianza centrale abbiamo sfruttato il fatto che il prodotto usuale tra interi è commutativo.

(7) Esiste un elemento neutro per il prodotto, che è la classe $[1]$ di 1. Infatti si ha

$$[i][1] = [i \cdot 1] = [i] = [1 \cdot i] = [1][i]\,.$$

(8) Il prodotto è distributivo rispetto alla somma:

$$[i]([j] + [k]) = [i][j + k] = [i(j + k)] = [ij + ik] = [ij] + [ik] = [i][j] + [i][k]\,.$$

Analogamente si mostra che $([i] + [j])[k] = [i][j] + [i][k]$.

Le proprietà appena elencate di dicono che $\mathbb{Z}_n$, dotato delle operazioni di somma e prodotto definite dalle (3.40) e (3.41), è un anello commutativo (Definizione 3.1).
Tuttavia, rispetto all'anello $\mathbb{Z}$ degli interi, $\mathbb{Z}_n$ presenta alcune importanti differenze. La prima, più evidente, è che si tratta di un anello finito, diversamente da $\mathbb{Z}$ che è infinito. La seconda importante differenza tra $\mathbb{Z}$ e $\mathbb{Z}_n$ è che in quest'ultimo non vale la legge di annullamento del prodotto (che afferma che un prodotto è zero solo se almeno uno dei due fattori è nullo). Ad esempio, in $\mathbb{Z}_6$ consideriamo le classi $[2]$ e $[3]$: nessuna di

queste due è la classe nulla (ovvero $[2] \neq [0]$ e $[3] \neq [0]$) in quanto né 2 né 3 sono congruenti a zero modulo 6. Tuttavia il loro prodotto è dato da

$$[2][3] = [2 \cdot 3] = [6] = [0] .$$

Un'altra domanda fondamentale nell'aritmetica di $\mathbb{Z}_n$ riguarda l'esistenza dell'inverso moltiplicativo di una classe $[a]$ data. Nell'anello degli interi $\mathbb{Z}$ sappiamo che gli unici interi x ad avere un inverso moltiplicativo (ovvero un elemento y per cui $xy = yx = 1$) sono $+1$ e -1. Vediamo ora che in $\mathbb{Z}_n$ la questione è più complessa.
Sia $[a]$ una classe in $\mathbb{Z}_n$. l'esistenza di un inverso moltiplicativo di $[a]$ equivale all'esistenza di una classe $[x]$ tale che $[a][x] = [1]$. Ma quest'ultima uguaglianza , per definizione di prodotto tra classi, significa $[ax] = [1]$ ovvero che ax e 1 sono congrui modulo n. In altre parole la loro differenza è un multiplo di n:

$$ax - 1 = yn$$

per un certo intero $y \in \mathbb{Z}$.
Portando yn a primo membro e -1 a secondo, concludiamo che la classe di a ha inverso modulo n se e solo esistono due interi x, y tali che

$$ax - yn = 1 \tag{3.42}$$

e in tal caso l'inverso di $[a]$ è dato proprio dalla classe $[x]$.
Ora, la relazione (3.42), come sappiamo dalla Proposizione 3.21, è verificata sicuramente se il massimo comune divisore di a e n è 1. Viceversa, se vale tale relazione allora necessariamente il massimo comune divisore di a e n è 1. Questo perché se d è un divisore comune di a e n (ovvero $a = da'$ e $n = dn'$) allora sostituendo nella (3.42) otteniamo

$$ax - yn = da'x - ydn' = d(a'x - yn') = 1 .$$

Quindi necessariamente $d = \pm 1$ (perché non esiste nessun intero che moltiplicato per d dà 1).

In altre parole, abbiamo appena dimostrato che *una classe $[a]$ in $\mathbb{Z}_n$ è invertibile se e solo se il massimo comune divisore di a e n è 1, ovvero se e solo se a e n sono primi tra loro.*

Quanto detto sopra per ottenere questo risultato ci fornisce anche un modo pratico per il calcolo dell'inverso, quando questo esiste. Ad esempio, determiniamo l'inverso di $[5]$ in $\mathbb{Z}_{14}$ (o, detto in altre parole, l'inverso di 5 modulo 14).
Innanzitutto, tale inverso esiste perché 5 e 14 sono primi tra loro. Per trovare tale inverso, ovvero l'intero x per cui è soddisfatta la (3.42), eseguiamo il procedimento di divisioni successive visto nella sezione precedente:

$$14 = 5 \cdot 2 + 4$$
$$5 = 4 \cdot 1 + 1$$
$$4 = 1 \cdot 4\,.$$

Dalla seconda divisione troviamo $1 = 5 - 4$, e sostituendo 4 tramite $4 = 14 - 5 \cdot 2$ (ricavata dalla prima divisione) otteniamo

$$1 = 5 - 4 = 5 - (14 - 5 \cdot 2) = 5 - 14 + 5 \cdot 2 = 5 \cdot 3 + (-1) \cdot 14\,.$$

Quindi, in base a quanto visto sopra, 3 è l'inverso di 5 modulo 14, ovvero $[3]$ è l'inverso di $[5]$ in $\mathbb{Z}_{14}$ (infatti, $[5][3] = [15] = [1]$ in $\mathbb{Z}_{14}$).

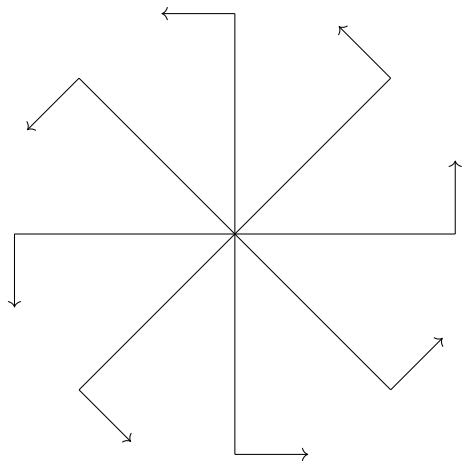
Come corollario di quanto appena detto, notiamo che se n è un numero primo, allora per ogni $i = 1, 2, \ldots, n-1$ si ha che i è primo con n. Quindi in $\mathbb{Z}_n$ le classi $[1], [2], \ldots, [n-1]$ (cioè tutte le classi tranne la classe nulla $[0]$) ammettono un inverso. Questo, in base alla Definizione 3.2, significa che *se n è primo allora* $\mathbb{Z}_n$ *è un campo* (esattamente come $\mathbb{Q}$ e $\mathbb{R}$).

In particolare, in base all'Osservazione 3.3, la legge dell'annullamento del prodotto è soddisfatta in $\mathbb{Z}_n$ con n primo, come in tutti i campi.

Osservazione 3.27. Le proprietà (1), (2), (3) e (4) dell'operazione di somma tra classi che abbiamo visto nella Definizione 3.1 ci dicono che $\mathbb{Z}_n$, rispetto a tale operazione, è un gruppo commutativo (Definizione 2.56).

Una interessante "realizzazione geometrica" di questo gruppo può essere data come segue. Consideriamo il gruppo delle simmetrie della seguente figura del piano[5], una sorta di girandola con tutti i bracci della stessa lunghezza, ottenuta dividendo l'angolo giro di $360^\circ = 2\pi$ in 8 parti uguali.

[5]Ricordiamo che le simmetrie di una figura sono i movimenti rigidi (traslazioni, rotazioni, riflessioni) che la lasciano invariata, rispetto all'operazione di composizione.



Sicuramente la rotazione di angolo $\frac{2\pi}{8} = 45^\circ$ in senso antiorario lascia invariata la figura (comprese le freccette che spuntano da ogni braccio), così come la rotazione di $\frac{2\pi}{8} \cdot 2 = 90^\circ$ (ottenuta componendo la rotazione di 45° con se stessa), la rotazione di $\frac{2\pi}{8} \cdot 3 = 135^\circ$ (ottenuta componendo la rotazione di 45° con se stessa 3 volte) e così via tutte le rotazioni di angolo $\frac{2\pi}{8} \cdot k$, ottenute componendo k volte la rotazione di 45°.
Tuttavia, è chiaro che se considero la rotazione di angolo $\frac{2\pi}{8} \cdot 8$, ottengo esattamente la funzione identica che manda ogni punto in se stesso (8 rotazioni di 45° una dietro l'altra danno un giro completo). La stessa cosa sarà vera se ruoto di $\frac{2\pi}{8} \cdot 16$, $\frac{2\pi}{8} \cdot 24$ e in generale per qualunque multiplo di 8. Analogamente, una rotazione di $\frac{2\pi}{8} = 45^\circ$ muove i punti nello stesso modo di una rotazione di $\frac{2\pi}{8} \cdot 9$ (un giro completo più altri 45°), o di $\frac{2\pi}{8} \cdot 17$ (due giri completi più altri 45°) e così via per tutte le rotazioni di $\frac{2\pi}{8} \cdot k$ con k che differisce da 1 per un multiplo di 8.
In generale, avremo che un angolo di $\frac{2\pi}{8} \cdot k$ e un angolo di $\frac{2\pi}{8} \cdot l$ rappresentano la stessa rotazione se e solo se k e l differiscono per un multiplo di 8. Questa è esattamente la relazione di congruenza modulo 8 che definisce le classi di $\mathbb{Z}_8$.
Quindi c'è una corrispondenza biunivoca tra le classi $\{[0],[1],[2],[3],[4],[5],[6],[7]\}$ e le rotazioni che lasciano invariata la figura: alla classe $[k]$ corrisponde la rotazione di angolo $\frac{2\pi}{8} \cdot k$. Chiaramente $[k] = [k']$ se e solo se la rotazione di $\frac{2\pi}{8} \cdot k$ coincide con la rotazione di $\frac{2\pi}{8} \cdot k'$ (visto che k e k' differiscono per un multiplo di 8).
Questa corrispondenza identifica il gruppo $\mathbb{Z}_n$ con il gruppo delle simmetrie della figura non solo come insiemi, ma come gruppi, cioè anche rispetto alle operazioni in ciascuno dei due. Infatti se compongo due rotazioni di angoli $\frac{2\pi}{8} \cdot k$ e $\frac{2\pi}{8} \cdot l$ (che corrispondono alle classi $[k]$ e $[l]$ in $\mathbb{Z}_n$), il risultato sarà la rotazione di $\frac{2\pi}{8} \cdot k + \frac{2\pi}{8} \cdot l = \frac{2\pi}{8} \cdot (k+l)$, che corrisponde alla classe $[k+l]$. Quindi la composizione in un gruppo corrisponde esattamente alla somma nell'altro, e così vengono preservate anche tutte le altre relazioni. Ad esempio, il fatto che in $\mathbb{Z}_8$ si abbia $[5] + [3] = [0]$ corrisponde nel gruppo delle simmetrie della figura al fatto che se compongo una rotazione di $\frac{2\pi}{8} \cdot 5$ con una di $\frac{2\pi}{8} \cdot 3$

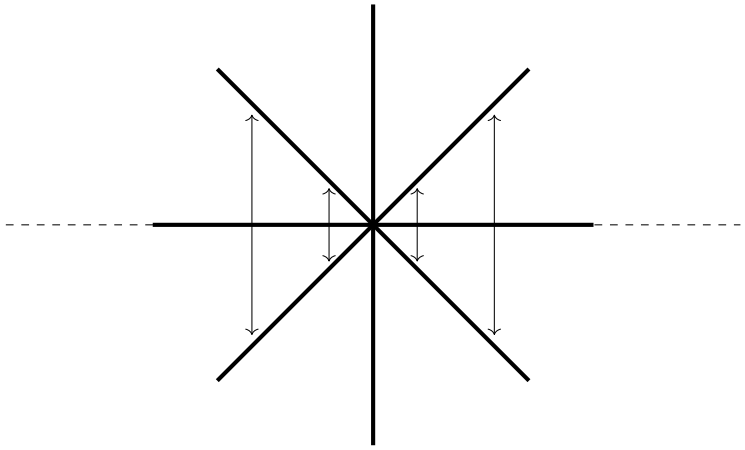
ottengo l'identità (l'elemento neutro per la composizione), in quanto avrò fatto un giro completo.

Definizione 3.28. Un **isomorfismo** f tra due gruppi $(G, \cdot)$ e $(H, \cdot')$ è una funzione biiettiva $f\colon G \longrightarrow H$ tale che

$$f(g_1 \cdot g_2) = f(g_1) \cdot' f(g_2)$$

per qualsiasi coppia di elementi $g_1, g_2 \in G$. Se esiste un isomorfismo tra due gruppi, questi si dicono **isomorfi**.

In pratica, se due gruppi sono isomorfi possiamo considerarli come se fossero lo stesso gruppo, anche se sono di natura molto diversa tra loro come nel nostro esempio (il primo è costituito di classi di numeri interi e l'operazione è una somma, il secondo da trasformazioni geometriche e l'operazione è la composizione).
Per concludere, si noti che le freccette nella figura servono a far sì che le rotazioni siano le sue *uniche* simmetrie, così da poterle identificare con gli elementi di $\mathbb{Z}_8$. Se non avessimo messo le freccette, ci sarebbero state altre simmetrie (ad esempio le riflessioni rispetto alle rette che contengono i bracci) e tale identificazione non sarebbe stata possibile:



Abbiamo visto che trovare l'inverso di un intero a modulo n (cioè un x tale che $[a][x] = [1]$, ovvero $[ax] = [1]$) equivale a risolvere l'equazione

$$ax \equiv_n 1.$$

Affrontiamo ora il problema più generale di determinare le soluzioni dell'equazione

$$ax \equiv_n b \tag{3.43}$$

dove b è un qualunque numero intero. Le domande a cui vogliamo rispondere sono: questa equazione è risolubile? se sì, quali e quante sono le sue soluzioni?
La risposta alla prima domanda ci è fornita dal seguente

Teorema 3.29. *L'equazione $ax \equiv_n b$ ammette soluzioni se e solo se il massimo comune divisore d di a e n divide b.*

Dimostrazione. Mostriamo prima che se il massimo comune divisore $d = (a,n)$ divide b, allora l'equazione ha soluzioni. Come sappiamo dalla Proposizione 3.21, se d è il massimo comune divisore di a e n, esistono due interi t e s tali che

$$d = at + ns\,. \tag{3.44}$$

Ora, l'ipotesi che d divida b significa che $b = db'$ per qualche intero b'. Moltiplicando allora la (3.44) per b' si ottiene

$$b = db' = atb' + nsb'\,. \tag{3.45}$$

Ma quest'ultima uguaglianza ci dice che atb' è congruo a b modulo n (perché differisce da b per nsb', che è un multiplo di n), ovvero $atb' \equiv_n b$: allora $x = tb'$ è una soluzione di $ax \equiv_n b$. Quindi, come volevamo, abbiamo mostrato che l'equazione ammette soluzioni sotto l'ipotesi che il massimo comune divisore di a e n divida b.
Viceversa, supponiamo che l'equazione $ax \equiv_n b$ ammetta soluzioni. Questo significa che esiste un intero x_0 tale che b e ax_0 differiscono solo per un multiplo di n, ovvero

$$b = ax_0 + ny \tag{3.46}$$

per qualche $y \in \mathbb{Z}$. Ma da questa uguaglianza è facile mostrare che il massimo comune divisore d di a e n divide b. Infatti, essendo d un divisore comune di a e n si ha che $a = da'$ e $n = dn'$ per certi interi a', n'. Ora sostituendo queste due uguaglianze nella (3.46) si trova

$$b = da'x_0 + dn'y = d(a'x_0 + n + y)$$

che ci dice proprio che d divide b. □

La dimostrazione precedente, oltre a darci il criterio necessario e sufficiente perché l'equazione $ax \equiv_n b$ sia risolubile, ci suggerisce anche come trovarne almeno una soluzione.
Esempio 3.30. Supponiamo di voler risolvere l'equazione

$$12x \equiv_{39} 15.$$

Poiché il massimo comune divisore tra $a = 12$ e $n = 39$ è $d = 3$, e 3 divide $b = 15$, l'esistenza di una soluzione è garantita dal Teorema 3.29. Per trovarla, seguiamo passo passo la dimostrazione. Esprimiamo prima $d = 3$ come combinazione di $n = 39$ e $a = 12$ come fatto nella (3.44), tramite il metodo delle divisioni successive.

$$39 = 12 \cdot 3 + 3$$

$$12 = 3 \cdot 4$$

Le divisioni confermano che il massimo comune divisore di 12 e 39 è 3, in quanto è l'ultimo resto non nullo. Dalla prima divisione otteniamo $3 = 39 - 12 \cdot 3$, ovvero

$$3 = 12 \cdot (-3) + 39 \cdot 1 \tag{3.47}$$

che sarebbe la (3.44) con $t = -3$ e $s = 1$. Ora, esattamente come fatto nella dimostrazione, osserviamo che $b = 15 = 3 \cdot 5$ (cioè, sempre in riferimento alla dimostrazione, sarebbe $b' = 5$) e moltiplichiamo la (3.47) proprio per 5, ottenendo

$$15 = 3 \cdot 5 = 12 \cdot (-3) \cdot 5 + 39 \cdot 5 = 12 \cdot (-15) + 39 \cdot 5\,. \tag{3.48}$$

Ma allora $x_0 = -15$ è una soluzione dell'equazione. Infatti, la (3.48) ci dice proprio che $12 \cdot (-15)$ è uguale a 15 modulo 39 (essi differiscono per $39 \cdot 5$).

Quella che abbiamo trovato è solo una soluzione dell'equazione: ce ne sono altre? La risposta è data dal seguente risultato, di cui omettiamo la dimostrazione.

Teorema 3.31. *Se l'equazione $ax \equiv_n b$ ha soluzioni, esse si ottengono tutte sommando a una qualunque di esse x_0 i multipli di $\frac{n}{d}$ (ovvero $x = x_0 + \frac{n}{d}k$, per ogni $k \in \mathbb{Z}$), dove d è il massimo comune divisore di a e n.*

Per illustrare il teorema, applichiamolo all'equazione $12x \equiv_{39} 15$, di cui sopra abbiamo trovato una soluzione $x_0 = -15$.
Poiché in quel caso $n = 39$ e $d = 3$, abbiamo che le soluzioni sono tutti e soli gli interi del tipo

$$x = x_0 + k\frac{n}{d} = -15 + \frac{39}{3}k = -15 + 13k$$

Queste, al variare di $k \in \mathbb{Z}$, sono tutte le soluzioni dell'equazione $12x \equiv_{39} 15$, che quindi risulta avere infinite soluzioni in $\mathbb{Z}$.
Per comprendere meglio la struttura dell'insieme delle soluzioni, distinguiamo però nell'espressione generale della soluzione $x = -15 + 13k$ tre casi:

(1) k è un multiplo di 3, ovvero $k = 3k'$ per qualche $k' \in \mathbb{Z}$ (ovvero $[k] = [0] \in \mathbb{Z}_3$).

In tal caso le soluzioni sono date da

$$x = -15 + 13k = -15 + 13 \cdot 3k' = -15 + 39k'$$

Questo ci dice che le soluzioni ottenute quando k è multiplo di 3, pur essendo interi diversi, sono tutte equivalenti modulo 39, ovvero appartengono tutte alla classe $[-15]$ di -15.

(2) k è un intero del tipo $k = 3k' + 1$ per qualche $k' \in \mathbb{Z}$ (ovvero $[k] = [1] \in \mathbb{Z}_3$).

In tal caso le soluzioni sono date da

$$x = -15 + 13k = -15 + 13 \cdot (3k' + 1) = -15 + 39k' + 13 = -2 + 39k'$$

Di nuovo otteniamo una famiglia di soluzioni tutte equivalenti modulo 39, e più precisamente tutte congruenti a -2. Esse formano la classe $[-2]$ di -2 modulo 39. Si noti che questa classe è diversa in $\mathbb{Z}_{39}$ dalla classe ottenuta nel primo caso (infatti, $[-15] \neq [-2]$ in quanto la differenza $-15 - (-2) = -13$ non è un multiplo di 39).

(3) k è un intero del tipo $k = 3k' + 2$ per qualche $k' \in \mathbb{Z}$ (ovvero $[k] = [2] \in \mathbb{Z}_3$).

In tal caso le soluzioni sono date da

$$x = -15 + 13k = -15 + 13 \cdot (3k' + 2) = -15 + 39k' + 26 = 11 + 39k' .$$

Ancora una volta, otteniamo una famiglia di soluzioni tutte equivalenti modulo 39, e più precisamente tutte congruenti a 11. Esse formano la classe $[11]$ di 11 modulo 39. Si noti che questa classe è diversa in $\mathbb{Z}_{39}$ da entrambe le classi ottenute nei casi precedenti. Infatti, $[11] \neq [-2]$ e $[11] \neq [-15]$ in quanto nessuna delle due differenze $11 - (-2) = 13$ e $11 - (-15) = 26$ è un multiplo di 39.

Si noti che non abbiamo altri casi: le uniche possibilità quando dividiamo k per 3 è che il resto sia $0, 1$ o 2, che corrispondono rispettivamente ai tre casi considerati $k = 3k'$, $k = 3k' + 1$ o $k = 3k' + 2$.

Possiamo riassumere quanto appena visto come segue. L'equazione $12x \equiv_{39} 15$ ha infinite soluzioni se la consideriamo come un'equazione da risolvere in $\mathbb{Z}$. Ma possiamo pensarla come l'equazione $[12][x] = [15]$ in $\mathbb{Z}_{39}$. Infatti, l'equazione $12x \equiv_{39} 15$ significa $[12x] = [15]$, ovvero, per definizione di prodotto tra classi, proprio $[12][x] = [15]$. In questo caso essa ha esattamente tre soluzioni distinte: $[-15], [-2], [11] \in \mathbb{Z}_{39}$.

Aiutati da questo esempio, possiamo allora dire che, in generale, *se l'equazione* $ax \equiv_n b$ *ha soluzioni se e solo se il massimo comune divisore d di a e n divide b, e in tal caso l'equazione ha esattamente d soluzioni modulo n*. In particolare, *se a e n sono primi tra loro, ovvero il loro massimo comune divisore d è* 1*, allora la soluzione esiste per ogni b ed è unica (modulo n)*. Questo è in accordo con il fatto che se a e n sono primi tra loro, allora a ammette un inverso moltiplicativo modulo n, che possiamo denotare a^{-1}. Quindi l'equazione $ax \equiv_n b$ può essere risolta (cioè, x può essere determinato in modo unico modulo n) semplicemente moltiplicando entrambi i membri per a^{-1}:

$$ax \equiv_n b \Rightarrow a^{-1}(ax) \equiv_n a^{-1}b \Rightarrow (a^{-1}a)x \equiv_n a^{-1}b \Rightarrow 1x \equiv_n a^{-1}b \Rightarrow x \equiv_n a^{-1}b\,.$$

In altre parole, se esiste l'inverso di a la soluzione può essere trovata esattamente come si risolve normalmente l'equazione $ax = b$ nei reali o nei razionali.

3.4 Applicazioni: cenni alla crittografia e ai numeri casuali

Vedremo adesso alcune importanti applicazioni pratiche dell'aritmetica modulare e dei teoremi visti nel capitolo precedente.
La prima di tali applicazioni riguarda la crittografia, ovvero lo studio delle tecniche con le quali un mittente può spedire un messaggio rendendolo illeggibile a tutti tranne al destinatari, l'unico a conoscere il modo di decriptarlo.

Per capire in che modo l'aritmetica modulare possa entrare in questo discorso, supponiamo di voler criptare un messaggio scritto con le 21 lettere dell'alfabeto italiano

$$A, B, C, D, \ldots, T, U, V, Z.$$

Per farlo potremmo far corrispondere a ogni lettera dell'alfabeto un'altra lettera e poi sostituire le lettere che compaiono nel messaggio dato in base alla corrispondenza scelta. Se, per esempio, la corrispondenza che scegliamo manda A in P, D in V, T in L , la parola $DATA$ verrà trasformata nella parola $VPLP$.
Il destinatario, per decriptare tale messaggio, deve essere a conoscenza della corrispondenza scelta e deve applicarla a ritroso per ottenere il messaggio originale.
Chiaramente, quella che stiamo chiamando corrispondenza tra le lettere dell'alfabeto deve essere più precisamente una corrispondenza biunivoca di tali lettere, ovvero una funzione biiettiva tra l'alfabeto e se stesso (in altre parole, una permutazione delle lettere dell'alfabeto). Infatti se la corrispondenza non fosse iniettiva, cioè se per esempio mandassimo A in P e anche O in P, il destinatario leggendo $VPLP$ non saprebbe se

sostituire una A o una O al posto della P. In questo modo non saprebbe se il messaggio originale era per esempio $DATA$, $DATO$, $DOTO$ o $DOTA$.
Quindi, una qualunque permutazione realizza una cifratura del messaggio, e la decifratura si realizza applicando la permutazione inversa (che esiste ben definita perché una permutazione è una funzione biiettiva, ovvero invertibile).

Ora, tra tutte le permutazioni del nostro insieme di 21 elementi può essere conveniente (per comodità di comunicazione con il destinatario) scegliere quelle che possono essere descritte tramite una regola generale, senza dover per forza dare il corrispondente di ogni lettera.
Ad esempio, è noto che Cesare per cifrare i suoi messaggi usava la permutazione che si ottiene associando ad ogni lettera quella che si trova 3 posizioni più avanti nell'alfabeto. Più precisamente, alla A associa la D, alla B la E, e così via, fino alla T, a cui verrà associata la Z, che è l'ultima lettera dell'alfabeto. A quel punto per le ultime tre lettere si riparte da capo: alla U si associa la A, alla V la B e alla Z la C.
Nel linguaggio del gruppo delle permutazioni imparato nel capitolo precedente, la permutazione usata da Cesare non è nient'altro che il prodotto di tre cicli disgiunti, ciascuno di lunghezza 7.

$$(A\ \ D\ \ G\ \ L\ \ O\ \ R\ \ U)(B\ \ E\ \ H\ \ M\ \ P\ \ S\ \ V)(C\ \ F\ \ I\ \ N\ \ Q\ \ T\ \ Z)$$

Benché fino a questo punto l'oggetto matematico che più si presta allo studio dei cifrari sembrino essere le permutazioni, vediamo ora che il modo più semplice di scrivere la corrispondenza di Cesare si ottiene usando il linguaggio delle congruenze.
A questo scopo, iniziamo con il tradurre numericamente l'alfabeto, assegnando a ogni lettera il numero della sua posizione nell'alfabeto: la A sarà quindi rappresentata dal numero 1, la B dal numero 2 e così via fino alla Z che sarà rappresentata dal numero 21.
Allora, la regola stabilita da Cesare per il suo cifrario dovrebbe essere semplicemente

$$x \mapsto x + 3\,,$$

cioè alla lettera corrispondente al numero x associamo la lettera che corrisponde alla posizione $x + 3$. Per esempio ad 1, cioè A, corrisponde $1 + 3 = 4$, cioè D, e così via.
Tuttavia, la formula sembra funzionare solo fino a $x = 18$ (ovvero T) a cui viene associata come abbiamo detto sopra $x + 3 = 21$ (ovvero la Z), dal momento che per $x = 19$ (cioè la U) abbiamo $x + 3 = 22$, che non corrisponde a nessuna lettera dell'alfabeto.
In realtà il problema si risolve se lavoriamo nell'aritmetica modulo 21 invece che nell'aritmetica usuale degli interi. Infatti, in $\mathbb{Z}_{21}$, 22 corrisponde a 1 (ovvero alla A) ed il cifrario di Cesare prevede di associare alla U la A. Analogamente, a $x = 20$ (cioè la V) corrisponde $x + 3 = 23$ che è congruo a 2 (ovvero la B) modulo 21 e a $x = 21$ (cioè la Z) corrisponde $x + 3 = 24$ che è congruo a 3 (ovvero la C) modulo 21.
Quindi la formula che descrive correttamente il cifrario di Cesare è

$$x \mapsto x + 3 \pmod{21}. \tag{3.49}$$

Il fatto che il cifrario di Cesare sia un procedimento crittografico corretto, cioè una funzione biiettiva sull'insieme delle lettere dell'alfabeto, equivale al fatto che la (3.49) sia una funzione biiettiva sull'insieme $\mathbb{Z}_{21} = \{1, 2, \ldots, 21\}$ (per comodità di notazione stiamo omettendo le parentesi quadre nell'indicare le classi).
Infatti, la biiettività della (3.49) discende dal fatto che se $x + 3 \equiv y \pmod{21}$, allora x è determinata da y semplicemente risolvendo l'equazione. In questo caso si fa semplicemente portando il 3 a secondo membro: $x \equiv y - 3 \pmod{21}$. Equivalentemente, essendo -3 congruo a $21-3 = 18$ modulo 21, potremmo scrivere $x = y+18 \pmod{21}$: ad esempio, se $y = 4$, che corrisponde alla D, decriptando abbiamo $x = y + 18 = 22$ che è congruo a 1 modulo 21, ovvero la A.

Ispirati da questo, possiamo pensare di realizzare nuovi cifrari semplicemente sostituendo una qualunque funzione $f(x)$ al posto di $x + 3$ purché questa sia invertibile in $\mathbb{Z}_{21}$. Come primo esempio, possiamo considerare, per ogni b, la generalizzazione del cifrario di Cesare

$$x \mapsto x + b \pmod{21} \tag{3.50}$$

che corrisponde ad associare a ogni lettera che si trova nella posizione x dell'alfabeto la lettera che si trova b posizioni più avanti (se $b > 0$) o più indietro (se $b < 0$).
L'invertibilità di tale funzione si mostra esattamente come fatto per il cifrario di Cesare, ovvero basta osservare che, per ogni y, l'equazione $x + b \equiv y \pmod{21}$ ha unica soluzione data da $x \equiv y - b \pmod{21}$.
Un ulteriore passo avanti nella generalizzazione del cifrario di Cesare si ottiene come segue:

$$x \mapsto ax + b \pmod{21}. \tag{3.51}$$

Ad esempio, se $a = 5$ e $b = 3$, allora la lettera D, che corrisponde a $x = 4$, viene mandata in $5 \cdot 4 + 3 = 23 \pmod{21}$ ovvero $2 \pmod{21}$, che corrisponde alla lettera B.
Stavolta, però, dobbiamo fare più attenzione, in quanto non ogni scelta di a dà un procedimento crittografico corretto. Infatti, come abbiamo detto sopra, la funzione (3.51) deve essere biiettiva, e questo corrisponde a dire che per ogni y l'equazione $ax + b \equiv y \pmod{21}$ deve avere soluzione e questa deve essere unica.
Ora, portando b a secondo membro questo equivale a dire che deve essere unica la soluzione di $ax \equiv y - b \pmod{21}$.
Ma alla fine della sezione precedente abbiamo visto qual è la condizione per l'unicità di tale soluzione: a deve essere primo con 21. Questo infatti garantisce che a abbia un inverso a^{-1} modulo 21. Come abbiamo visto nel paragrafo precedente, la soluzione si ottiene moltiplicando entrambi i membri per a^{-1}:

$$x \equiv a^{-1}(y-b) \pmod{21}$$

che è la formula per decriptare il messaggio.
Un cifrario dato dalla (3.51) è detto *cifrario affine*.

Esempio 3.32. Supponiamo, sbagliando, di voler criptare un messaggio con la regola $x \mapsto 6x \pmod{21}$ (l'errore consiste nel fatto che si tratta di una formula del tipo (3.51) con $b = 0$ e $a = 6$ non primo con $n = 21$).
Allora, vediamo ad esempio che 1 (cioè la A) viene mandato in 6 (cioè F); ma anche H, che corrisponde a 8, viene mandato in $6x = 48 \equiv 6 \pmod{21}$, ovvero nuovamente la F.
Tale metodo di cifratura non è quindi corretto in quanto si hanno lettere diverse mandate nella stessa lettera, e il messaggio criptato sarebbe ambiguo.

Quando si trasmette un messaggio criptato si vuole che questo sia il più difficile possibile da decriptare per chi, non essendo il destinatario, lo intercettasse.
Ora, per decriptare un messaggio bisogna innanzittutto conoscere la funzione $x \mapsto f(x)$ con cui si cripta il messaggio, e poi saper calcolare l'inversa di tale funzione.
Per quello che riguarda la conoscenza della funzione f, supponendo che chi intercetta il messaggio sappia di che tipo di cifrario si tratta, ad esempio un cifrario affine (3.51), questi dovrebbe conoscere la coppia (a,b) per avere esplicitamente la funzione e invertirla. Tale coppia, e più in generale i parametri che servono per costruire la funzione con cui criptiamo il messaggio, si chiama la *chiave del cifrario*.
Chiaramente, più sono le chiavi possibili di un tipo di cifrario, più sarà difficile per chi lo intercetta di determinarle. Ad esempio, il cifrario di Cesare generalizzato $x \mapsto x + b \pmod{21}$ ha come chiave la b e questa può essere scelta esattamente in 21 modi ($b = 1, 2, \ldots, 21$). Escludendo $b = 21$ con il quale assoceremmo a ogni lettera se stessa, otteniamo 20 cifrari diversi.
Nel caso del cifrario affine (3.51), b può variare tra 1 e 21 mentre a può essere un qualunque intero positivo minore di 21 e primo con esso. Il numero di interi positivi minori di 21 e primi con esso è dato, come abbiamo visto a pagina 105, da $\phi(21)$, dove ϕ è la funzione di Eulero. Essendo $21 = 3 \cdot 7$, in base alla formula (3.37) abbiamo $\phi(21) = 21(1-1/3)(1-1/7) = 12$.
Quindi per un cifrario affine, tenendo conto che per ognuna delle 12 scelte di a abbiamo 20 scelte possibili di b, abbiamo $12 \cdot 21 = 252$ possibili chiavi. Da queste escludiamo però il caso $a = 1, b = 21$, che, essendo 21 congruente a 0 modulo 21, manda ogni numero in stesso. Quindi, chiunque sia interessato a decriptare il messaggio, sospettando che si tratti di un cifrario affine, potrebbe doverle provare tutte (il che chiaramente non è troppo complicato con i computer a disposizione oggi).

Il secondo aspetto della sicurezza di un codice, come abbiamo detto, riguarda la difficoltà di calcolare la funzione inversa di quella usata per la cifratura. A prima vista,

sembrerebbe che una volta nota la chiave, ovvero la funzione f, calcolare l'inversa di f sia una cosa relativamente semplice. In realtà stiamo per mostrare un codice, detto RSA[6], nel quale il calcolo della funzione inversa si rivela talmente complesso che, conoscendo solo in che modo il messaggio è stato criptato e la chiave, la decifratura risulta praticamente impossibile.
Vediamo i dettagli: supponiamo che il messaggio che vogliamo trasmettere sia un numero intero x (che può rappresentare una lettera dell'alfabeto ma anche una qualunque altra informazione). Il destinatario del messaggio comunica (pubblicamente) al mittente in che modo deve criptare il messaggio, che poi solo lui saprà decriptare invertendo la funzione usata. Più precisamente, il destinatario procede come segue.

(1) Sceglie due numeri primi p_1 e p_2 il più grandi possibile e li moltiplica ottenendo $N = p_1 p_2$.

(2) Calcola la funzione di Eulero $\phi(N)$ (in questo caso si ha $\phi(N) = (p_1-1)(p_2-1)$).

(3) Sceglie un intero positivo $e < \phi(N)$ e che sia primo con $\phi(N)$.

(4) Comunica al mittente, che vuole spedire l'intero x, di calcolare il valore di $x^e \pmod N$ e spedirglielo.

In altre parole, la funzione di cifratura è $x \mapsto y \equiv x^e \pmod N$.
In realtà, per la correttezza della cifratura, x deve essere minore di N, ma tale condizione non è difficile da realizzare visto che il destinatario ha ottenuto N moltiplicando due primi molto grandi.
Ora vediamo che, sotto le condizioni date, tale funzione è invertibile ma il calcolo della sua inversa richiede un'informazione aggiuntiva, oltre alla chiave (N, e) comunicata pubblicamente, che solo il destinatario possiede e che risulta estremamente difficile ricavare dalla chiave, anche con l'ausilio di un computer.
Più precisamente, il destinatario che ha ricevuto $y \equiv x^e \pmod N$ e lo decripta come segue. Dal momento che e è primo con $\phi(N)$, esso è invertibile modulo $\phi(N)$ e ne calcola il suo inverso, che chiamiamo d. A questo punto, affermiamo che la x può essere ricostruita dalla y tramite la formula

$$x = y^d \pmod N . \tag{3.52}$$

Prima di spiegare il perché, osserviamo che il calcolo di d, che è l'inverso di e modulo $\phi(N)$, richiede la conoscenza del valore $\phi(N)$, e qui sta esattamente la difficoltà di violare il codice. Infatti, tutti conoscono N, che fa parte della chiave pubblica, ma il calcolo di $\phi(N) = (p_1 - 1)(p_2 - 1)$ richiede la conoscenza della decomposizione $N = p_1 p_2$

[6] Si tratta di un esempio di cosiddetta *crittografia a chiave pubblica* che deve il nome RSA alle iniziali dei nomi Rivest, Shamir e Adleman degli studiosi che l'hanno introdotta nel 1977.

di N come prodotto di primi, e questo è un calcolo estremamente difficile, per numeri grandi, anche per computer molto potenti.

Ora spieghiamo perché la (3.52) fornisca l'inversa che serve per decifrare il messaggio cifrato. Dal momento che $y \equiv x^e \pmod N$, elevando entrambi i membri della congruenza alla potenza d si ha

$$y^d \equiv (x^e)^d \equiv x^{ed} \pmod N. \tag{3.53}$$

Quindi, per concludere che $y^d \equiv x \pmod N$ ci basta mostrare che

$$x^{ed} \equiv x \pmod N. \tag{3.54}$$

Per dimostrare la (3.54) bisogna distinguere due casi: quello in cui x è primo con N e quello in cui x non è primo con N. Per semplicità, mostreremo la (3.54) solo nel primo caso.
In tal caso, si sfrutta il seguente cosiddetto *teorema di Eulero*, che non dimostriamo:

Teorema 3.33 (Teorema di Eulero)**.** *Se x e N sono interi primi tra loro, allora*

$$x^{\phi(N)} \equiv 1 \pmod N \tag{3.55}$$

In che modo il teorema di Eulero ci serve per dimostrare la (3.54)?
Per definizione, d è l'inverso di e modulo $\phi(N)$, ovvero $ed \equiv_{\phi(N)} 1$. In altre parole questo significa che esiste un intero k per cui $ed = 1 + k\phi(N)$. Ma allora si ha

$$x^{ed} \equiv x^{1+k\phi(N)} \pmod N. \tag{3.56}$$

Ora, in base al teorema di Eulero, $x^{\phi(N)} \equiv 1 \pmod N$, ovvero, elevando entrambi i membri di tale congruenza alla potenza k si ha

$$x^{k\phi(N)} \equiv (x^{\phi(N)})^k \equiv 1^k \equiv 1 \pmod N \tag{3.57}$$

ovvero anche $x^{k\phi(N)} \equiv 1 \pmod N$. Ma allora, moltiplicando entrambi i membri di questa uguaglianza per x si ottiene

$$x \cdot x^{k\phi(N)} \equiv x \cdot 1 \pmod N$$

ovvero

$$x^{1+k\phi(N)} \equiv x \pmod N. \tag{3.58}$$

Combinando la (3.56) e la (3.58) si ha proprio la (3.54), e abbiamo concluso.

Esempio 3.34. Supponiamo di prendere $p_1 = 7$, $p_2 = 5$: allora $N = 35$ e $\phi(N) = (p_1 - 1)(p_2 - 1) = 6 \cdot 4 = 24$. Scegliamo allora $e = 5$ che come previsto è primo con $\phi(N) = 24$.
Supponiamo che il mittente voglia mandare al destinatario il messaggio $x = 3$. Allora, il destinatario gli chiede prima di criptarlo secondo la formula $x \mapsto x^e \pmod N$, dopo avergli comunicato pubblicamente la chiave $(N, e) = (35, 5)$. Si ha

$$x^e = 3^5 = 243 \equiv 33 \pmod{35}$$

Il mittente comunica quindi al destinatario il messaggio criptato $y = 33$.
A questo punto, per decriptarlo, il destinatario calcola prima l'inverso di $e = 5$ modulo $\phi(N) = 24$. Essendo

$$24 = 5 \cdot 4 + 4$$
$$5 = 4 \cdot 1 + 1$$
$$4 = 4 \cdot 1$$

dalla seconda divisione troviamo $1 = 5 - 4$, e sostituendo $4 = 24 - 5 \cdot 4$ (ricavato dalla prima) si trova

$$1 = 5 - (24 - 5 \cdot 4) = 5 - 24 + 5 \cdot 4 = -24 + 5 \cdot 5$$

che ci dice che 5 è l'inverso di 5 modulo 24, ovvero $d = 5$.
Allora, il destinatario decripta il messaggio calcolando

$$33^5 = 39.135.393 \equiv 3 \pmod{35}$$

(in quanto $39.135.393 = 35 \cdot 1.118.154 + 3$) e ritrova quindi il messaggio originale $x = 3$.

Osservazione 3.35. Se N è un numero primo P, allora sapendo che $\phi(P) = P - 1$ si trova che il teorema di Eulero in questo caso si scrive

$$x^{P-1} \equiv 1 \pmod P \tag{3.59}$$

(sempre valida sotto l'ipotesi che x sia primo con P).
Questo risultato è noto sotto il nome di *piccolo teorema di Fermat*.
Moltiplicando entrambi i membri della (3.59) per x si ottiene

$$x^P \equiv x \pmod P \tag{3.60}$$

che ha il vantaggio di essere vera anche senza ipotesi su x. Infatti, se x non è primo con P, essendo P primo, deve essere un multiplo di P. Questo implica che sia x^P che x sono

congruenti a zero modulo P, e quindi congruenti tra loro. A volte quando si parla di piccolo teorema di Fermat si intende la (3.60).

Concludiamo il capitolo accennando ad un'altra importante applicazione delle congruenze. Spesso, nella pratica, serve avere a disposizione sequenze di numeri casuali o meglio *pseudocasuali*. Per capire di cosa si tratta, facciamo un esempio. I sistemi di identificazione online di certe banche sono basati sull'uso di una chiavetta che premendo un tasto fornisce una sequenza di numeri che l'utente deve inserire nella pagina di accesso, assieme ad altre credenziali. Succede è che dall'altra parte un meccanismo genera, in base allo stesso algoritmo usato nella chiavetta, la stessa sequenza di numeri, riconoscendo così l'utente.
Affinché il sistema sia sicuro, la sequenza di numeri generata deve essere "apparentemente casuale". Chiaramente non lo è davvero visto che sia l'utente che il sito della banca usano un algoritmo per generare la stessa sequenza e riconoscersi, ma deve essere tale da avere caratteristiche simili a quelle di una sequenza di numeri casuali (si parla allora appunto di numeri pseudocasuali), in modo che individuare l'algoritmo usato e entrare anche senza la chiavetta sia il più difficile possibile per chi volesse violare il sistema. La definizione precisa di cosa significhi "caratteristiche simili a quelle di una sequenza casuale" spetta alla statistica, ma non approfondiamo questo aspetto: basti sapere che esiste una definizione precisa e un modo di testare se una sequenza ha queste caratteristiche.
Solitamente un algoritmo che generi una sequenza funziona nel seguente modo: parte da un numero iniziale x_0 (detto il *seme*) e genera la sequenza applicando ripetutamente una funzione f scelta. In altre parole la sequenza è data da

$$x_0, x_1 = f(x_0), x_2 = f(x_1), x_3 = f(x_2) \dots$$

ovvero è data dalla regola[7] che $x_{i+1} = f(x_i)$.
Ad esempio, se f fosse la funzione $f(x) = x + 1$, partendo da $x = 2$ avremmo

$$x_0 = 2, x_1 = f(2) = 3, x_2 = f(3) = 4, x_3 = f(x_2) = 5 \dots$$

Chiaramente se si usasse questa funzione come generatrice dei numeri sulla chiavetta si otterrebbero sempre sequenze di numeri consecutivi, e chi riuscisse a vedere i numeri usati capirebbe subito il meccanismo e non avrebbe difficoltà a violare il sistema.
Nuovamente l'aritmetica modulare ci viene in aiuto: è tramite le congruenze che si riescono a generare sequenze di numeri pseudocasuali soddisfacenti. Ad esempio, si fissa un certo n e si lavora modulo n, definendo una sequenza di numeri tramite la formula

[7] Si dice che abbiamo definito la sequenza *induttivamente*: infatti, la stiamo definendo per $i = 0$ dando il seme x_0 e poi tramite la $x_{i+1} = f(x_i)$ stiamo dicendo che, una volta che è definita per i, risulta definita anche per $i + 1$. In base al principio di induzione, la sequenza è allora definita per ogni numero naturale i.

$$x_{i+1} = ax_i + b \pmod{n}. \tag{3.61}$$

Sotto opportune ipotesi su a e b (omettiamo i dettagli per semplicità) si dimostra che la (3.61) genera, a partire da un seme x_0, una sequenza di numeri pseudocasuali. La (3.61) si chiama *generatore lineare* di numeri pseudocasuali

La combinazione dell'uso di generatori di numeri casuali e di crittografia RSA è alla base di molte importanti procedure di identificazione on line (ad esempio, la firma digitale).