# Una introduzione all'aritmetica modulare

GIOVANNI CUTOLO

Questo articolo è pensato per studenti non universitari che abbiano qualche curiosità nei confronti di un argomento non abitualmente incontrato nei corsi scolastici. La trattazione è elementare e di tono informale quanto possibile, anche se non rinucia del tutto a dare qualche indicazione di cosa si possa incontrare oltre questo primo approcio, e non ha alcuna pretesa di completezza. Sono presentate, nella seconda nella terza sezione dell'articolo, due applicazioni elementari dell'aritmetica modulare.

## 1. Introduzione informale

Siamo abituati a suddividere i numeri interi in due categorie: quella dei numeri pari e quella dei numeri dispari. Sappiamo anche, magari senza esserne del tutto consapevoli, che questa suddivisione ha una semplice ma importante proprietà di "buon comportamento" (*compatibilità* è la parola che si usa in matematica) nei confronti delle operazioni di addizione e moltiplicazione tra numeri interi. La proprietà è questa: dati due arbitrari numeri interi $a$ e $b$, basta conoscere la parità di $a$ e quella di $b$ (cioè se $a$ e $b$ siano pari o dispari) per conoscere la parità di $a+b$ e $ab$: se $a$ e $b$ sono entrambi pari o entrambi dispari allora $a+b$ è pari, altrimenti $a+b$ è dispari; se $a$ e $b$ sono entrambi dispari allora $ab$ è dispari, altrimenti $ab$ è pari. Questo fa sì che abbiano senso affermazioni come 'pari più dispari fa dispari', o 'pari per dispari fa pari', che tavolta si utilizzano.

Vale qualcosa del genere per altre "suddivisioni" (anche qui c'è un termine tecnico: nel linguaggio della teoria degli insiemi queste suddivisioni si chiamano *partizioni*) dell'insieme dei numeri interi? Vediamo:possiamo ripartire l'insieme degli interi in tre sottoinsiemi: quello dei numeri interi positivi, quello dei numeri interi negativi, quello che consiste del solo zero. Questa partizione è compatibile con la moltiplicazione: dati due numeri interi $a$ e $b$ per stabilire se $ab$ è positivo, negativo o zero basta sapere se sono positivi, negativi o zero $a$ e $b$ (positivo per positivo dà positivo, negativo per zero dà zero etc.). Lo stesso non vale però per l'addizione: se, ad esempio, $a$ è positivo e $b$ è negativo, la loro somma $a+b$ può essere negativa, zero o positiva ($1+(-2)<0$; $1+(-1)=0$; $2+(-1)>0$). Diciamo quindi che la suddivisione degli interi tra positivi, negativi e zero non è compatibile con l'operazione di addizione tra interi.

Vediamo un altro esempio; questa volta, per semplicità, ci limiteremo agli interi positivi. Ripartiamo gli interi positivi per ultima cifra (quella delle unità; stiamo facendo riferimento alla consueta rappresentazione degli interi in base 10 che siamo abituati ad usare sin da piccoli). Supponiamo cioè di disporre gli interi positivi in dieci contenitori, ad esempio, dieci cassetti, ciascuno etichettato da una cifra $(0,1,2,\dots,9)$, infilando nel cassetto etichettato da 0 tutti gli interi positivi con ultima cifra 0, in quello etichettato da 1 tutti gli interi positivi con ultima cifra 1 e così via: il cassetto con etichetta $i$, che possiamo chiamare $C_i$, conterrà tutti (e soli) i numeri interi positivi con cifra delle unità $i$. Ci vuol poco a convincersi che anche questa suddivisione degli interi positivi è compatibile con l'addizione e la moltiplicazione: scelti comunque due cassetti $C_i$ e $C_j$ e due numeri, $a$ in $C_i$ e $b$ in $C_j$, quale sia il cassetto che contiene la somma $a+b$ e quale sia il cassetto che contiene il prodotto $ab$ dipende solo da $i$ e da $j$ e non cambia se sostituiamo $a$ con un qualsiasi altro numero $a'$ in $C_i$ e $b$ con un qualsiasi altro $b'$ in $C_j$. Ad esempio, comunque scegliamo un $a$ nel cassetto $C_3$ ed un $b$ nel cassetto $C_4$, $a+b$ sarà nel cassetto $C_7$ e $ab$ nel cassetto $C_2$ (provare per credere).

È possibile generalizzare questa idea; vediamo come. Il cassetto $C_0$ è costituito, abbiamo detto, dai numeri interi positivi con cifra delle unità zero. Ma questi sono precisamente i multipli di 10. I numeri nel cassetto $C_1$, quelli con ultima cifra 1, sono precisamente (tra gli interi positivi) quelli che nella divisione per 10 hanno resto 1. In generale, possiamo facilmente constatare che, se $i$ è una qualsiasi delle cifre $0,1,2,\dots,9$ (che sono, guarda caso, i possibili resti nella divisione di un intero per 10) il cassetto $C_i$

Università degli Studi di Napoli "Federico II", Dipartimento di Matematica e Applicazioni "R. Caccioppoli", Via Cintia — Monte S. Angelo, I-80126 Napoli, Italy,
e-mail: cutolo@unina.it
http://www.dma.unina.it/~cutolo/, http://www.dma.unina.it/~cutolo/didattica/

conterrà tutti e soli gli interi positivi che, divisi per 10, dànno resto $i$. Ci accorgiamo poi che anche la suddivisione degli interi tra pari e dispari risponde alla stessa logica: i numeri pari sono quelli che, divisi per 2, dànno resto zero, quelli dispari sono quelli che, divisi per due dànno resto uno. Una differenza è che per la suddivisione tra pari e dispari abbiamo preso in esame tutti gli interi, mentre la suddivisione "per cifra delle unità" l'abbiamo ristretta ai soli insiemi positivi. Questa differenza, vedremo, è inessenziale. L'unica altra differenza è che la prima suddivisione può essere descritta con riferimento alla divisione per 2, nel secondo alla divisione per 10. Ma se qualcosa funziona allo stesso modo per 2 e per 10, magari si può pensare che funzioni allo stesso modo anche per altri numeri. Difatti è così. Fissiamo un arbitario intero positivo $m$ e disponiamo tutti gli interi (non solo quelli positivi) in una cassettiera con $m$ cassetti, etichettati con i numeri $0, 1, 2, \ldots, m-1$, mettendo nel cassetto con etichetta $i$ tutti e soli gli interi che, divisi per $m$, dànno resto $i$. In questo modo otteniamo che ciascun numero intero è finito in un cassetto (ed uno solo), perché i numeri con cui abbiamo etichettato i cassetti sono precisamente i possibili resti nella divisione di un intero per $m$.

Queste cassettiere con $m$ cassetti sono dunque una versione più generale dei due esempi precedenti, ed hanno anche esse, per qualsiasi valore dell'intero positivo $m$, la stessa proprietà di compatibilità rispetto sia all'addizione che alla moltiplicazione tra numeri interi. Questo lo verificheremo nella prossima sezione, ma discutiamo da subito di cosa ciò significhi: nella sostanza, che possiamo definire un'operazione di addizione ed una di moltiplicazione tra i "cassetti". Consideriamo infatti fissato l'intero positivo $m$. Se $A$ e $B$ sono due dei cassetti (uguali o diversi tra loro, non importa) della nostra cassettiera con $m$ cassetti, $a$ è un numero in $A$ e $b$ un numero in $B$, chiamiamo $A+B$ il cassetto a cui appartiene $a+b$. La definizione ha senso proprio per via della compatibilità: $A+B$ non dipende dalla scelta di $a$ in $A$ e di $b$ in $B$; anche se sostituiamo $a$ con un altro elemento $a'$ di $A$ e $b$ con un altro elemento $b'$ di $B$ non cambia il "cassetto somma" $A+B$, perché $a'+b'$ è nello stesso cassetto di $a+b$. Simile discorso vale per la moltiplicazione: la compatibilità garantisce che sia univocamente definito il "cassetto prodotto" $AB$ come quel cassetto a cui appartiene $ab$. Abbiamo così un "ambiente di calcolo" (i matematici parlano di *struttura algebrica*): un insieme in cui siano definite delle operazioni, che benché sia definito a partire dai numeri interi non è più quello dei numeri interi: continuando nella metafora, questo ambiente è la nostra cassettiera. Anzi, abbiamo infiniti ambienti di calcolo, uno per ogni scelta dell'intero positivo $m$, tutti diversi tra loro e diversi dall'ambiente originale (quello dei numeri interi). L'aritmetica modulare si può descrivere come l'algebra di questi nuovi ambienti di calcolo o, per dirla in modo più educato, di queste strutture e delle loro proprietà.

## 2. In modo un po' più preciso ...

Indichiamo, come si fa di consueto, con $\mathbb{Z}$ l'insieme dei numeri interi. Come sappiamo, se $u, v \in \mathbb{Z}$ (cioè: se $u$ e $v$ sono numeri interi), dire che $u$ divide $v$ (o, equivalentemente, che $v$ è divisibile per $u$, o ancora che $v$ è multiplo di $u$) significa dire che esiste $k \in \mathbb{Z}$ tale che $v = uk$. Aggiungiamo una nuova definizione: se $m$ è un intero positivo e $a, b \in \mathbb{Z}$, diciamo che $a$ e $b$ sono *congrui modulo* $m$, e scriviamo in questo caso $a \equiv_m b$, se e solo se $m$ divide la differenza $a-b$. Ad esempio, $8 \equiv_3 2$ (perché 3 divide $8-2=6$) e $7 \equiv_{10} -3$ (perché 10 divide $7-(-3)=10$). Vediamo alcune proprietà essenziali di questa relazione di congruenza modulo $m$, senza entrare troppo in dettagli (né in dimostrazioni), che possono comunque essere trovati facilmente altrove da chi lo desidera.

Innanzitutto, la congruenza modulo $m$ è una *relazione di equivalenza* in $\mathbb{Z}$, nel senso che verifica le proprietà riflessiva (si ha $a \equiv_m a$ per ogni $a \in \mathbb{Z}$, dal momento che $m$ certamente divide $0 = a-a$), simmetrica (se $a$ e $b$ sono interi tali che $a \equiv_m b$, allora $b \equiv_m a$: infatti se $a-b$ è un multiplo di $m$ allora anche $b-a$, che è l'opposto di $a-b$, è un multiplo di $m$) e transitiva (se $a, b, c \in \mathbb{Z}$ e si ha $a \equiv_m b$ e $b \equiv_m c$, allora $a \equiv_m c$, infatti se $a-b$ e $b-c$ sono entrambi multipli di $m$, allora anche la loro somma $(a-b)+(b-c) = a-c$ è un multiplo di $m$)[1]. Per ogni $a \in \mathbb{Z}$, l'insieme di tutti i numeri interi che siano congrui ad $a$ modulo $m$ si chiama *classe di resto* di $a$ modulo $m$ e si indica con $[a]_m$.[2] Da quali interi è costituito questo insieme? Si ha:

$$[a]_m = \{a + mk \mid k \in \mathbb{Z}\}$$

[1] useremo spesso questa osservazione, che è tanto importante quanto ovvia: se $u$ e $v$ sono due multipli dello stesso intero $m$, allora anche la loro somma è un multiplo di $m$; infatti se $u = mh$ e $v = mk$, per opportuni interi $h$ e $k$, allora $u + v = m(h+k)$.

[2] chi ha familiarità con il linguaggio e la teoria delle relazioni di equivalenza si accorgerà che $[a]_m$ non è altro che la classe di equivalenza di $a$ rispetto alla relazione (di equivalenza) di congruenza modulo $m$.

vale a dire: gli interi congrui ad $a$ modulo $m$ sono quelli della forma $a + mk$ per un opportuno $k \in \mathbb{Z}$. Infatti, se $b \equiv_m a$ allora $b - a$ è un multiplo di $m$, quindi $b - a = mk$ per un opportuno $k \in \mathbb{Z}$, vale a dire: $b = a + mk$. Viceversa, se $b$ è un numero della forma $b = a + mk$, per un $k \in \mathbb{Z}$, allora $b - a = mk$ è multiplo di $m$ e quindi $b \equiv_m a$. Questo prova l'uguaglanza $[a]_m = \{a + mk \mid k \in \mathbb{Z}\}$. Ad esempio, la classe di resto di 2 modulo 6, cioè $[2]_6$ è costituita da tutti gli interi della forma $2 + 6k$ al variare di $k \in \mathbb{Z}$; per $k$ uguale a 0, 1, 2, 3, etc. otteniamo così $2 = 2 + 6 \cdot 0$, $8 = 2 + 6 \cdot 1$, $14 = 2 + 6 \cdot 2$, $20 = 2 + 6 \cdot 3$, e così via, scegliendo per $k$ valori negativi otteniamo invece $-4 = 2 + 6 \cdot (-1)$, $-10 = 2 + 6 \cdot (-2)$, $-16 = 2 + 6 \cdot (-3)$, e così via. Abbiamo così:

$$[2]_6 = \{\dots, -22, -16, -10, -4, 2, 8, 14, 20, 26, \dots\};$$

possiamo visualizzare la classe di resto di 2 modulo 6 come l'insieme costituito dai numeri che incontriamo partendo da 2 ed percorrendo l'intera lista dei numeri interi facendo passi di lunghezza 6, sia nel verso positivo che in quello negativo. Scegliamo un qualsiasi altro numero in $[2]_6$, ad esempio 14. Qual è la classe di resto di 14 modulo 6? Se ci pensiamo un attimo, ci accorgiamo che è la stessa classe trovata per 2. Infatti ci possiamo spostare da 14 a 2 (con due passi "all'indietro" di lunghezza 6) e da qui, sempre con passi di lunghezza 6, raggiungere tutti i numeri in $[2]_6$ (per esempio, siccome con cinque passi all'indietro, da 2 si raggiunge $-28 = 2 + 6(-5)$, si potrà raggiungere $-28$ da 14 effettuando sette passi all'indietro; i primi due passi portano a 2, con i rimanenti cinque si arriva a $-28$). Vediamo così che ogni numero in $[2]_6$ è anche in $[14]_6$. Viceversa, ragionando in modo analogo ma invertendo i ruoli di 14 e 2, scopriamo che, partendo da 2 ed muovendoci solo con passi di lunghezza 6, siccome possiamo raggiungere 14 possiamo anche raggiungere ogni numero in $[14]_6$, quindi ogni numero in $[14]_6$ è anche in $[2]_6$. Mettendo insieme questa informazione con la precedente, concludiamo che $[14]_6 = [2]_6$. Questa è una regola generale, si ha infatti, per ogni coppia di interi $a$ e $b$ e per ogni intero positivo $m$:

$$a \equiv_m b \iff [a]_m = [b]_m.$$

Questa è una proprietà generale delle relazioni di equivalenza, e può darsi che chi legge la abbia già incontrata. La si può verificare utilizzando la proprietà transitiva (e la proprietà simmetrica). Supponiamo infatti $a \equiv_m b$. Se $c$ è un elemento di $[b]_m$, allora $b \equiv_m c$ (per definizione di $[b]_m$), dunque $a \equiv_m c$ per la proprietà transitiva, vale a dire: $c \in [a]_m$. Questo prova l'inclusione $[b]_m \subseteq [a]_m$; in modo analogo si prova l'inclusione opposta: $[a]_m \subseteq [b]_m$. Dunque è vero che $[a]_m = [b]_m$ se $a \equiv_m b$. A guardar bene, questa dimostrazione non è altro che una versione un po' più astratta del ragionamento che abbiamo svolto sopra per arrivare all'uguaglianza $[14]_6 = [2]_6$. Ci resta ancora da fare una cosa: verificare l'implicazione opposta, cioè che $a \equiv_m b$ se $[a]_m = [b]_m$. Ma questo è chiaro: si ha $a \in [a]_m$, perché $a \equiv_m a$ (proprietà riflessiva!); dunque, se $[a]_m = [b]_m$ allora $a \in [b]_m$ e quindi $a \equiv_m b$.

Un'altra utile espressione della stessa proprietà è:

*scelta comunque una classe di resto $A$ ed un $a \in A$, allora $A = [a]_m$.*

Le classi di resto si chiamano così perché sono strettamente legate alla nozione di resto che appare nella divisione tra numeri interi. Ricordiamo di cosa stiamo parlano:

**Teorema.** *Scelti comunque due numeri interi $a$ ed $m$, se $m > 0$ esiste una ed una sola coppia ordinata $(q, r)$ di numeri interi tali che $a = mq + r$ e $0 \leq r < m$.*

Come sappiamo, questi numeri $q$ ed $r$ si chiamano, nell'ordine, quoziente e resto nella divisione di $a$ per $m$. Siccome $a - r = mq$ è un multiplo di $m$, osserviamo che $r$ è congruo ad $a$ modulo $m$. Meglio ancora, $r$ è l'*unico* numero congruo ad $a$ modulo $m$ che sia compreso tra 0 e $m - 1$, infatti tra gli elementi della classe $[a]_m$ (che coincide, ricordiamo, con $[r]_m = \{r + mk \mid k \in \mathbb{Z}\}$, dal momento che $r \equiv_m a$) quello che immediatamente segue $r$ è $r + m$, che è più grande di $m - 1$, quello che immediatamente precede $r$ è $r - m$, che è negativo. Se $b$ è un arbitrario numero congruo ad $a$ modulo $m$ e $s$ è il resto di $b$ nella divisione per $m$, allora $s \equiv_m b \equiv_m a$ e $0 \leq s < m$, quindi anche $s$, come $r$, è congruo ad $a$ modulo $m$ (proprietà transitiva!) ed è compreso tra 0 e $m - 1$. Ma $r$ è l'unico numero con queste proprietà, quindi $s = r$. Cosa concludiamo? Che *tutti* i numeri in $[a]_m$, se divisi per $m$, hanno come resto $r$. Vale anche il viceversa, infatti se un numero intero $b$, diviso per $m$, ha resto $r$, allora $b \equiv_m r$; ma $r \equiv_m a$ e quindi $b \equiv_m a$, ovvero $b \in [a]_m$. Possiamo a questo punto dire che $[a]_m$ è costituita da tutti e soli gli interi che, divisi per $m$, dànno resto $r$. Questo spiega il nome 'classe di resto' dato a questi insiemi. Possiamo anche dire:

*due numeri sono congrui modulo $m$ se e solo se hanno lo stesso resto nella divisione per $m$.*

Beh, allora queste classi di resto sono niente di più e niente di meno che i 'cassetti' che avevamo informalmente introdotto nella sezione precedente: fissato l'intero positivo $m$, esistono esattamente $m$ classi di resto (di numeri interi) modulo $m$, una per ogni possibile resto nella divisione per $m$. L'insieme di queste classi di resto si indica con $\mathbb{Z}_m$ (e si chiama l'insieme degli *interi modulo* $m$):

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$$

dove, per ciascun $i$, $[i]_m$ è l'insieme degli interi che, divisi per $m$, dànno resto $i$. Come abbiamo visto, $[i]_m = \{i + mk \mid k \in \mathbb{Z}\}$. Notiamo, in particolare, che $[0]_m$ è l'insieme degli interi multipli di $m$ (che si indica talvolta con $m\mathbb{Z}$). Notiamo anche che ciascuna delle classi di resto si può rappresentare in tanti (addirittura infiniti) modi diversi, ad esempio $[2]_6 = [14]_6 = [6000002]_6$, quindi anche $\mathbb{Z}_m$ si potrà descrivere in molti modi. Ad esempio,

$$\mathbb{Z}_m = \{[1]_m, [2]_m, \dots, [m-1]_m, [m]_m\},$$

dal momento che $[0]_m = [m]_m$, ma abbiamo anche

$$\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}.$$

Giusto per chiarire un punto lasciato in sospeso nella sezione precedente, esaminiamo il caso $m = 10$. $\mathbb{Z}_{10}$ consiste delle dieci classi $[i]_{10} = \{i + 10k \mid k \in \mathbb{Z}\}$ al variare dell'intero $i$ tra 0 e 9. Come sono fatte queste classi di resto? Lo capiamo da un esempio: i numero positivi in $[7]_{10}$ sono tuti e soli quelli che hanno 7 come cifra delle unità. E quelli negativi? Si capisce che $-7$ non è in questa classe, perché la differenza $7 - (-7)$ è 14, che non è multiplo di 10. Invece in questa classe troviamo $-3 = 7 - 10$. Difatti si riconosce facilmente che $[7]_{10}$ è costituita dagli interi positivi con ultima cifra 7 e dagli interi negativi con ultima cifra 3. È per evitare questa complicazione che, nella sezione precedente, abbiamo descritto la cassettiera a dieci cassetti limitandoci ai numeri interi positivi.

2.1. **Compatibilità.** Abbiamo detto, nella sezione precedente, che è la proprietà di compatibilità a rendere interessanti le 'cassettiere', perché rende possibile definire operazioni 'tra cassetti' in aggiunta a quelle tra numeri. Vediamo in che modo questa proprietà si può riformulare e giustificare.

**Teorema** (Compatibilità delle congruenze)**.** *Siano dati un intero positivo $m$ e $a, a', b, b' \in \mathbb{Z}$. Allora:*

$$\left.\begin{array}{c} a \equiv_m a' \\ e \\ b \equiv_m b' \end{array}\right\} \implies \left\{\begin{array}{c} a+b \equiv_m a'+b' \\ e \\ ab \equiv_m a'b' \end{array}\right.$$

*Dimostrazione.* Supponiamo che valgano $a \equiv_m a'$ e $b \equiv_m b'$. Questa ipotesi significa che $a-a'$ e $b-b'$ sono entrambi multipli di $m$. Per provare $a + b \equiv_m a' + b'$ ci serve verificare che la differenza $(a + b) - (a' + b')$ è un multiplo di $m$. Ma questo non è difficile: $(a + b) - (a' + b') = (a - a') + (b - b')$ è la somma tra due multipli di $m$, quindi è essa stessa un multiplo di $m$. Dunque è vero che $a + b \equiv_m a' + b'$.

Proviamo ora che $ab \equiv_m a'b'$. Aggiungendo e sottraendo $ab'$ a $ab - a'b'$ si ha

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

Ora, sia $a(b - b')$ che $(a - a')b'$ sono multipli di $m$, quindi $ab - a'b'$ è multiplo di $m$, sicché $ab \equiv_m a'b'$. A questo punto l'asserto è provato. □

Come già detto, questo risultato è il punto essenziale dell'aritmetica modulare. Lo possiamo vedere da due punti di vista.

In primo luogo, supponiamo di voler conoscere non il risultato di alcune operazioni tra interi, ma solo il resto che questo risultato ha nella divisione per un certo intero positivo $m$. Ad esempio, per assegnati numeri interi $a, b, c, d, e, f$ abbiamo bisogno di calcolare il resto modulo $m$ di $k := (a^2b - c)(d + e^5) + f$. Possiamo sostituire $a, b, c, d, e, f$ con numeri interi $a', b', c', d', e', f'$, ciascuno congruo modulo $m$ a quello che sostituisce ($a \equiv_m a'$, $b \equiv_m b'$ e così via) e calcolare $k' = ((a')^2b' - c')(d' + (e')^5) + f'$, avendo scelto naturalmente i numeri che sostituiamo in modo che questo secondo calcolo sia più semplice dell'originale. Siccome $k' \equiv_m k$, per la proprietà di compatibilità, $k'$ ha lo stesso resto di $k$ nella divisione per $m$. Notiamo in particolare come questo vale anche per le potenze: ad esempio, $a^2 = a \cdot a \equiv_m a' \cdot a' = (a')^2$. Ci si trova in questa situazione molto più frequentemente di quanto possa sembrare a prima vista, sia in contesti puramente matematici che in situazioni di applicazione della matematica a problemi del mondo reale, ad esempio, quando dobbiamo far conti che abbiano a che fare con lo scorrere del tempo, che calcoliamo ciclicamente (l'orario si azzera ogni ventiquatt'ore, il giorno delle settimana ogni sette giorni,

etc.). Vediamo subito qualche esempio di questo secondo tipo (dove l'espressione 'mondo reale' è usata in un senso piuttosto generoso).

**Esempio 1.** È domenica, e mio cugino Asdrubale vuole sapere da me che giorno (della settimana) sarà tra $8500 \cdot 33 + 4^{200}$ giorni. Asdrubale non è particolarmente sensibile a quell'utile qualità chiamata buonsenso, e non accetta come valida la mia risposta che l'espressione "tra $4^{200}$ giorni" non ha alcun significato reale: ben prima che possa essere trascorso una tale lasso di tempo non esisterà più nessuno, o almeno nessuno che misuri il tempo in giorni e in settimane come facciamo noi. Lui vuole la risposta comunque! E allora diamogliela. Si tratta innanzitutto di calcolare il resto modulo 7 di $8500 \cdot 33 + 4^{200}$. Procediamo con ordine: $8500 = 8000 + 500 \equiv_7 1000 + 500$, dal momento che $8000 - 1000$ è chiaramente multipo di 7. Dunque, $8500 \equiv_7 1500$. Ma $1500 = 1400 + 100 \equiv_7 100$ e $100 = 70 + 30 \equiv_7 30 = 28 + 2 \equiv_7 2$. Dunque, $8500 \equiv_7 2$. Inoltre $33 \equiv_7 -2$. Quindi $8500 \cdot 33 \equiv_7 2 \cdot (-2) = -4 \equiv_7 3$. Esaminiamo ora $4^{200}$. Abbiamo $4^2 = 16 \equiv_7 2$, quindi $4^3 = 4^2 \cdot 4 \equiv_7 2 \cdot 4 \equiv_7 8 \equiv_7 1$. Ma allora abbiamo anche $4^4 \equiv_7 4^3 \cdot 4 \equiv_7 4$, $4^5 \equiv_7 4^3 \cdot 4^2 \equiv_7 4^2$, $4^6 \equiv_7 4^3 \cdot 4^3 \equiv_7 1$: le "potenze di 4 modulo 7" si ripetono di tre in tre, il che rende facile calcolarle. Precisiamo questa idea. Da $4^3 \equiv_7 1$ segue $4^{3k} = (4^3)^k \equiv_7 1^k = 1$ per ogni intero positivo $k$. Immaginiamo di aver diviso 200 per 3, ottenendo un quoziente $k$ ed un resto $r$, dunque $200 = 3k + r$. Allora $4^{200} = 4^{3k+r} = 4^{3k} \cdot 4^r \equiv_7 1 \cdot 4^r$. Quindi per calcolare $4^{200}$ modulo 7 l'unica cosa che serve conoscere è il resto di 200 nella divisione per 3. Esiste un metodo rapidissimo per calcolarlo, lo vedremo più avanti, ma procediamo in modo ingenuo: $200 = 2 \cdot 100$ e $100 \equiv_3 1$ (perché 99 è multiplo di 3); allora $200 \equiv_3 2 \cdot 1 = 2$ e da ciò segue che 2 è il resto $r$ cercato. Allora, per le osservazioni fatte sopra, $4^{200} \equiv_7 4^2 \equiv_7 2$ (notare che non abbiamo avuto bisogno di calcolare il quoziente $k$; che $4^2 \equiv_7 2$ lo avevamo già osservato). In definitiva,

$$8500 \cdot 33 + 4^{200} \equiv_7 3 + 2 = 5.$$

Sappiamo allora che questo gran numero (di giorni) è un multiplo di 7 più 5. Aggiungere alla data un numero di giorni multiplo di 7 (cioè un numero intero di settimane) non cambia il giorno della settimana, quindi per rispondere alla domanda di Asdrubale basta aggiungere cinque giorni al giorno attuale (che, abbiamo detto, è domenica), ottenendo un venerdì. Possiamo dire allora ad Asdrubale che il giorno che tanto gli sta a cuore sarà un venerdì. Contento lui ... □

**Esempio 2.** La riproduzione del batterio *Duplicator Freneticus Suicidalis*, o *DFS*, (fortunatamante non particolarmente dannoso se non per se stesso) ha questo curioso andamento. In ambiente favorevole, ogni esemplare si duplica dopo esattamente tre minuti di vita, dando luogo a due individui identici, che a loro volta si duplicheranno (istantaneamente) dopo esattamente tre minuti, e così via. C'è però una restrizione: ogni ambiente chiuso (ad esempio una provetta) ha un suo limite di popolazione, diciamo di $n$ batteri. Se dopo una duplicazione della popolazione della provetta il numero di batteri raggiunge o supera $n$, istantaneamente $n$ batteri muoiono abbassando la popolazione al di sotto di $n$ (perché? la natura è misteriosa e a volte un poco stupida); passati tre minuti la popolazione superstite si duplicherà, come al solito. Ad esempio, se per una certa provetta questo limite è di 90 batteri, e in un certo istante la provetta contiene precisamente 50 batteri vivi, appena "nati", dopo tre minuti questi 50 batteri si duplicheranno, ma allora diventerebbero 100, il che non è consentito dalla natura del batterio e della provetta, quindi 90 batteri muoiono e ne restano in vita 10, che dopo tre minuti diventano 20, dopo sei minuti 40, poi 80, e dopo altri tre minuti diventano 70 (dovrebbero essere 160, ma 90 di essi devono morire), e così si ripetono questi (molto) strani cicli biologici.

In un certo laboratorio è stata preparata una provetta per la quale il limite di popolazione di batteri *DFS* che non può essere raggiunto è di 85 batteri. Nell'istante $t_0$ in cui si forma, un (solo) batterio viene lasciato cadere nella provetta (che prima non ne conteva), in modo che dopo tre minuti si possa duplicare e dare avvio al popolamento della provetta. La questione è: quanti batteri saranno nella provetta esattamente cinque ore e dieci secondi dopo $t_0$? In ogni ora avvengono $20 (= 60/3)$ cicli di duplicazione dei batteri, quindi allo scoccare della quinta ora ne saranno avvenuti cento. Ogni duplicazione è un "raddoppio modulo 85", vale a dire: se subito prima della duplicazione la provetta $X$ conteneva $n$ batteri, subito dopo ne conterrà $2n$ (se $2n < 85$) o $2n - 85$ (se $2n > 85$; ovviamente in nessun caso possiamo avere $2n = 85$, che causerebbe l'estinzione della popolazione dei batteri in $X$); in ogni caso il numero dei batteri è il resto nella divisione di $2n$ per 85. Dopo cento duplicazioni dei batteri il numero sarà allora il resto di $2^{100}$ nella divisione per 85 (dobbiamo moltiplicare cento volte per due il batterio iniziale, ma la moltiplicazione è fatta "modulo 85"). Calcoliamolo. La prima potenza di 2 che si avvicini al modulo 85 è $2^6 = 64 = 85 - 21 \equiv_{85} -21$. Allora $2^7 \equiv_{85} 2(-21) = -42$ e $2^8 \equiv_{85} 2(-42) = -84 \equiv_{85} 1$. Ragionando come

fatto nell'esempio precedente, allora ci basta calcolare il resto modulo 8 dell'esponente 100 per calcolare $2^{100}$ modulo 85. Abbiamo $100 \equiv_8 20 \equiv_8 4$, quindi questo resto è 4. Il numero dei batteri cercato sarà allora congruo, modulo 85, a $2^4 = 16$ (posto $100 = 8k+4$, abbiamo infatti $2^{100} = (2^8)^k \cdot 2^4 \equiv_{85} 1^k 2^4 = 2^4$), dunque proprio 16. □

**Esempio 3.** Ci troviamo nella stessa situazione dell'esempio precedente, ma stiamo conducendo un esperimento parallelo in una seconda provetta $Y$, più piccola di $X$, per la quale il limite di popolazione di batteri *DFS* che non può essere raggiunto è di 30 batteri. Come nel caso di $X$, al tempo $t_0$ la provetta $Y$ contiene esattamente un batterio, neonato, e vogliamo conoscere il numero di batteri in $Y$ cinque ore e pochi secondi dopo $t_0$, vale a dire: dopo cento duplicazioni. Dobbiamo allora calcolare il resto di $2^{100}$ nella divisione per 30. Possiamo provare a ragionare come fatto nei due esempi precedenti. Una potenza di 2 che si avvicina molto a 30 è $2^5 = 32$. Abbiamo $2^5 \equiv_{30} 2$, quindi $2^6 \equiv_{30} 2^2$, $2^7 \equiv_{30} 2^3$, $2^8 \equiv_{30} 2^4$, $2^9 \equiv_{30} 2^5 \equiv_{30} 2$, $2^{10} \equiv_{30} 2^2$ e così via: le potenze di 2 modulo 30 si ripetono di quattro in quatto a partire da $2^1 = 2$. Precisiamo questa frase: supponiamo che $s$ sia un intero *positivo*. Allora: $2^s = 2 \cdot 2^{s-1} \equiv_{30} 2^5 \cdot 2^{s-1} = 2^{s+4}$. Ora, per ogni intero positivo $n$, se $q$ ed $r$ sono rispettivamente il quoziente ed il resto nella divisione di $n-1$ per 4, abbiamo $n-1 = 4q+r$, quindi $n = 4q+(r+1)$. Dunque $n$ si ottiene aggiungendo un certo numero ($q$, ma non importa) di volte 4 all'intero *positivo* $r+1$. Per quanto visto sopra, questo garantisce che $2^{r+1} \equiv_{30} 2^{r+1+4} \equiv_{30} 2^{r+1+4\cdot 2} \equiv_{30} 2^{r+1+4\cdot 3} \equiv_{30} \cdots \equiv_{30} 2^{r+1+4q} = 2^n$.

Ora sappiamo come calcolare la nostra potenza $2^{100}$ modulo 30. Il resto di $99 = 100 - 1$ modulo 4 è 3, perché 100 è multiplo di 4, quindi $99 \equiv_4 -1 \equiv_4 3$ (con riferimento alle notazioni appena usate, 100 è $n$, dunque $r$ è 3). Allora $2^{100} \equiv 2^{3+1} = 16$; la provetta, al tempo indicato (cinque ore dopo $t_0$) conterrà 16 batteri.

Osserviamo come, in questo caso, il calcolo delle potenze è un po' più complicato che nel caso dei due esempi precedenti. La differenza è che mentre le potenze di 4 modulo 7 e quelle di 2 modulo 85 si ripetono a partire da quella di esponente zero ($1 = 4^0 \equiv_7 4^3$ e $1 = 2^0 \equiv_{85} 2^8$), quelle di 2 modulo 30 si ripetono anch'esse, ma non da quella di esponente 0. Infatti, per ogni intero positivo $t$ si ha $1 = 2^0 \not\equiv_{30} 2^t$, perché per ogni numero congruo a 1 modulo 30 è dispari (dal momento che è $30k+1$ per qualche $k \in \mathbb{Z}$), mentre tutte le potenze di 2 con esponente intero positivo sono, ovviamente, pari. Come abbiamo visto, si ha una ripetizione periodica delle potenze di 2 modulo 30 solo a partire dalla potenza di esponente uno, cioè da $2 = 2^1 = 2^5 = 2^9 \ldots$. □

Fissiamo in forma generale una osservazione sul calcolo di potenze in aritmetica modulare. Siano $m$ (come al solito) un intero positivo e $a$ un intero arbitrario. Come abbiamo visto negli esempi, può capitare che esista un intero positivo $t$ tale che $a^t \equiv_m 1$. Limitandoci al caso più semplice, supponiamo che questo accada (a titolo di notizia: si verifica questo caso se e solo se $a$ ed $m$ sono *coprimi*[3]) In questo caso il minimo tale $t$ si chiama *periodo* (o anche periodo moltiplicativo) di $a$ modulo $m$, o anche, in modo più appropriato, periodo (moltiplicativo) di $[a]_m$. Estendendo al caso generale i ragionamenti svolti negli esempi, si ha che per ogni intero $n \geq 0$ vale $a^n \equiv_m a^r$, dove $r$ è il resto nella divisione di $n$ per $t$.

2.2. **Le operazioni in $\mathbb{Z}_m$.** Veniamo al secondo punto di vista. Come visto già parlando di "cassettiere" la proprietà di compatibilità rende possibile definire operazioni di addizione e moltiplicazione tra "cassetti". La versione "precisata" di questa idea è che la proprietà di compatibilità garantisce la possibilità di definire, per ogni fissato intero positivo $m$, operazioni di addizione e moltiplicazione tra classi di resto modulo $m$, cioè tra elementi di $\mathbb{Z}_m$. Si usano per queste operazioni gli stessi simboli $+$ e $\cdot$ che usiamo per le corrispondenti operazioni tra numeri; le nuove operazioni sono definite da:

$$[a]_m + [b]_m = [a+b]_m \qquad \text{e} \qquad [a]_m \cdot [b]_m = [ab]_m$$

per ogni $a, b \in \mathbb{Z}$. Cosa significa? Niente di diverso di quanto abbiamo detto parlando di cassetti nella sezione introduttiva: la somma tra due classi di resto $A$ e $B$ (modulo $m$) si ottiene prendendo un numero $a$ in $A$ ed uno $b$ in $B$, sommando questi due numeri e considerando come risultato la classe a cui appartiene $a+b$. Infatti, come abbiamo visto sopra, se $a \in A$ e $b \in B$ allora $A = [a]_m$ e $B = [b]_m$, e la classe a cui appartiene $a+b$ è $[a+b]_m$. Ripetiamolo ancora una volta: questa "classe somma" non dipende dalla scelta di quale particolare elemento $a$ abbiamo selezionato in $A$ e quale $b$ in $B$: se $a' \in [a]_m$ e $b' \in [b]_m$ allora $a \equiv_m a'$ e $b \equiv_m b'$, quindi, per il teorema sulla compatibilità, $a+b \equiv_m a'+b'$, cioè $[a'+b']_m = [a+b]_m$. Analogo discorso vale per la moltiplicazione.

[3]due numeri interi sono coprimi, o *primi tra loro*, o *relativamente primi*, se e solo se hanno 1 come massimo comun divisore. In modo equivalente, due interi sono coprimi se e solo se non esiste alcun numero primo che li divida entrambi.

Abbiamo ora, per ogni fissato $m$, un insieme, $\mathbb{Z}_m$, e due operazioni definite tra elementi di $m$; abbiamo dunque quella che in matematica si chiama una struttura algebrica. Queste operazioni verificano le consuete proprietà (commutativa, associativa, distributiva) che ci sono familiari dall'aritmetica elementare, cioè le stesse proprietà delle operazioni tra numeri interi. Senza entrare in dettagli diciamo che queste strutture algebriche sono dello stesso tipo di quelle nelle quali siamo abituati a fare i conti, in $\mathbb{Z}$, nell'insieme dei numeri razionali, nell'insieme dei numeri reali. In algebra queste strutture si chiamano anelli, più precisamente, nel nostro caso, anelli commutativi unitari.

È utile visualizzare queste operazioni nelle cosiddette tavole di Cayley, di cui qui vediamo alcuni esempi, nei casi $m = 5$ e $m = 6$. Iniziamo con $\mathbb{Z}_5$:

$\mathbb{Z}_5$ :

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| · | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

La prima tabella descrive l'addizione, la seconda la moltiplicazione in $\mathbb{Z}_5$. In entrambe, per motivi di leggibilità, abbiamo scritto 0, 1, 2, 3, 4 piuttosto che $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$. Come sono composte e come vanno lette queste tabelle? Molto semplice: nella prima tabella, incrociando una riga, intestata da $i$, con una colonna, intestata da $j$, otteniamo un numero che rappresenta la classe $[i + j]_5$. Ad esempio, la terza riga (quella intestata da 2) ha uno zero nella quarta posizione (colonna intestata da 3). Questo esprime il fatto che $[2]_5 + [3]_5 = [0]_5$. La seconda tabella è costruita allo stesso modo ma con riferimento alla moltiplicazione: nella stessa posizione in cui prima abbiamo trovato uno zero abbiamo ora 1, perché $[2]_5 \cdot [3]_5 = [1]_5$. La prima riga (intestata da 0) della tabella per l'addizione riproduce la riga delle intestazioni, perché descrive le somme tra $[0]_5$ e gli elementi di $\mathbb{Z}_5$, che coincidono con gli elementi stessi: $[0]_5 + [j]_5 = [j]_5$ per ogni scelta di j; questa proprietà si esprime dicendo che $[0]_5$ è *elemento neutro* per l'operazione +. Lo stesso vale per la seconda riga (quella intestata da 1) della tabella per la moltiplicazione: $[1]_5$ è elemento neutro per l'operazione $\cdot$ in $\mathbb{Z}_5$.

Notiamo la simmetria delle tabelle rispetto alla diagonale dall'angolo in alto a sinistra a quello opposto. Sia ha questa simmetria precisamente perché le operazioni considerate verificano la proprità commutativa; chi legge sa riconoscere il perché?

Confrontiamo le tavole di Cayley per $\mathbb{Z}_5$ con quelle per $\mathbb{Z}_6$:

$\mathbb{Z}_6$ :

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| · | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Vediamo che mentre la tavola per l'addizione è molto simile a quella che abbiamo costruito per $\mathbb{Z}_5$, quella relativa alla moltiplicazione è molto diversa. Nel caso di $\mathbb{Z}_5$, esclusa la riga intestata da zero, che contiene solo zeri, in ogni riga sono rappresentati (una ed una sola volta) tutti gli elementi di $\mathbb{Z}_5$. Nel caso di $\mathbb{Z}_6$, invece, questo accade solo per la seconda e l'ultima riga, quelle intestate da 1 e 5, non per le altre. Questa differenza è molto significativa: ci dice che $\mathbb{Z}_5$ e $\mathbb{Z}_6$ sono strutture algebriche molto diverse tra loro. In $\mathbb{Z}_5$ ogni elemento diverso dallo zero è, come si dice, *invertibile*, cioè moltiplicato per un opportuno elemento dà $[1]_5$, che è, come accennato sopra, elemento neutro rispetto alla moltiplicazione in $\mathbb{Z}_5$. Questo si vede dalla tavola di Cayley per la moltiplicazione di $\mathbb{Z}_5$: in ogni riga, esclusa quella intestata da 0, appare 1. Ad esempio, nella riga intestata da 2 abbiamo trovato 1 in corrispondenza della colonna intestata da 3, perché $[2]_5 \cdot [3]_5 = [1]_5$; possiamo esprimere questo fatto dicendo, appunto, che $[2]_5$ è invertibile in $\mathbb{Z}_5$ e che $[3]_5$ è inverso di $[2]_3$. In questo $\mathbb{Z}_5$ si comporta come l'anello $\mathbb{Q}$ dei numeri razionali o quello $\mathbb{R}$ dei numeri reali (anelli di questo tipo si chiamano *campi*), in cui tutti gli elementi diversi da zero hanno inverso (il reciproco) o, equivalentemente, in cui è sempre possibile dividere un elemento per un elemento diverso da zero, e non come $\mathbb{Z}$, in cui queste proprietà non valgono. Al contrario, $\mathbb{Z}_6$ ha proprietà più deboli di quelle che valgono in $\mathbb{Z}$. Ad esempio, in $\mathbb{Z}$ (come in $\mathbb{Q}$ ed in $\mathbb{R}$, ed anche in $\mathbb{Z}_5$) vale la legge di annullamento

del prodotto: se il prodotto tra due numeri è zero, uno dei due numeri deve essere zero. Questo non vale in $\mathbb{Z}_6$, come si vede anche dalla tabella; ad esempio $[2]_6 \cdot [3]_6 = [0]_6$, benché $[2]_6 \neq [0]_6 \neq [3]_6$.

Vediamo quindi che $\mathbb{Z}$, $\mathbb{Z}_5$ e $\mathbb{Z}_6$ sono strutture algebriche di natura molto diversa tra loro. Senza entrare in dettagli che qui sarabbero fuori luogo, diciamo che la natura dei singoli anelli $\mathbb{Z}_m$ è determinata dalle proprietà aritmetiche dei numeri $m$ che li definiscono. Ad esempio, si dimostra che $\mathbb{Z}_m$ è un campo se e solo se $m$ è un numero primo, su questo torneremo più avanti.

2.3. **Approfondimenti.** In queste prime due sezioni abbiamo menzionato due nozioni, quella di *partizione* e quella di *relazione di equivalenza*, che sono tra le più fondamentali dell'intera matematica. La seconda rientra dei programmi scolastici standard ed è generalmente nota, la prima forse no. Definiamola: se $A$ è un insieme, una partizione di $A$ è un insieme $F$ di sottoinsiemi non vuoti di $A$ con la proprietà che ogni elemento di $A$ appartenga ad uno ed un solo elemento di $F$. Esempi ne abbiamo già visti nella sezione iniziale: se $P$ e $D$ sono l'insieme dei numeri interi pari e l'insieme dei numeri interi dispari, allora l'insieme $\{P, D\}$ è una partizione di $\mathbb{Z}$; se $\mathbb{Z}^+$ e $\mathbb{Z}^-$ sono l'insieme dei numeri interi positivi e l'insieme dei numeri interi negativi, allora anche $\{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$ è una partizione di $\mathbb{Z}$.

Se $\sim$ è una relazione di equivalenza in $A$ e $a \in A$, si chiama classe di equivalenza di $a$ rispetto a $\sim$ l'insieme di tutti gli elementi di $A$ che sono equivalenti (rispetto alla relazione $\sim$) ad $a$. Ad esempio, come già detto, le classi di resto sono classi di equivalenza. L'insieme delle classi di equivalenza degli elementi di $A$ rispetto a $\sim$, che si chiama *insieme quoziente* e si indica con $A/\sim$ è (lo si dimostra) una partizione di $A$. Viceversa, per ogni partizione $F$ di $A$ esiste una ed una sola relazione di equivalenza $\sim$ tale che $S/\sim$ sia proprio $F$. Si ha così una corrispondenza biettiva tra l'insieme di tutte le relazioni di equivalenza in $A$ e quello di tutte le partizioni di $A$. Questa perfetta corrispondenza fa sì che studiare le relazioni di equivalenza in $A$ sia essenzialmente lo stesso che studiare le partizioni in $A$ e tutto quello che diciamo a proposito di partizioni si può riformulare in termini di relazioni di equivalenza, e viceversa. È per questo motivo che abbiamo potuto presentare la nozione di compatibilità prima riferendoci (anche se informalmente) a partizioni di $\mathbb{Z}$, poi a relazioni di equivalenza. A questo punto a chi legge non sfuggirà che, per ogni $m$, l'insieme $\mathbb{Z}_m$ che abbiamo definito in questa sezione non è niente altro che l'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza modulo $m$.

Tornando alla questione della compatibilità, si può dimostrare che le nostre relazioni di congruenza modulo $m$ e la relazione di uguaglianza (che, come stiamo per vedere, si può fare rientrare nello stesso discorso) sono le sole relazioni di equivalenza compatibili con l'addizione in $\mathbb{Z}$: non ce ne sono altre. Ce ne sono invece di altre che siano compatibili con la moltiplicazione—un esempio l'abbiamo già fatto all'inizio di questo testo. Chi legge si può divertire a cercare altre partizioni di $\mathbb{Z}$ che siano compatibili con la moltiplicazione o che non lo siano. Una del primo tipo è la partizione che consiste di $\{0\}$, $\{1, -1\}$, l'insieme dei numeri primi e dei loro opposti, l'insieme di tutti gli altri numeri interi (i numeri composti); una del secondo è la partizione in numeri che siano quadrati di interi $\{0, 1, 4, 9, \dots\}$ e numeri che non siano.

Infine, giusto per non lasciarlo non detto, è il caso di avvertire che (quasi) tutto ciò che abbiamo detto facendo riferimento ad un intero positivo $m$ ha senso e continua a valere per *tutti* gli interi: la restrizione ai positivi serve solo a semplificare l'esposizione. Ad esempio, si definisce la relazione di congruenza modulo un intero arbitrario $m$ esattamente come fatto per gli interi positivi. Però non c'è nessun reale vantaggio nel farlo: si vede molto rapidamente che due interi sono congrui modulo 0 se e solo se coincidono (quindi la relazione di congruenza modulo 0 è la relazione di uguaglianza), e sono congrui modulo un intero negativo $m$ se e solo se lo sono modulo l'intero positivo $-m$ (quindi le relazioni di congruenza modulo i numeri negativi coincidono con quelle modulo i numeri positivi; non ricaviamo niente di nuovo se li aggiungiamo al discorso). Anche la divisione con resto, quella richiamata nel precedente teorema, si può effettuare anche con divisori $m$ negativi, ma (ed a questo si riferisce il "quasi" di qualche rigo fa) non per zero: una versione più generale del teorema si ottiene sostituendo l'ipotesi '$m > 0$' con '$m \neq 0$' e la restrizione '$0 \leq r < m$' con '$0 \leq r < |m|$'.

## 3. Criteri di divisibilità

Ci occuperemo qui di uno dei grandi misteri dell'istruzione matematica nella scuola. A tutti noi sono stati insegnati, già nella scuola elementare, i cosiddetti 'criteri di divisibilità' per alcuni numeri: 2, 3, 5, 11. Sono dei semplicissimi metodi che permettono di stabilire rapidamente se un assegnato numero intero positivo è o meno divisibile per, appunto, 2, 3, 5, 11. Ma cosa ci assicura che questi criteri forniscano sempre risposte corrette? La risposta si trova nell'aritmetica modulare.

Questi criteri sono riferiti alla scrittura di un numero intero in base 10 (che è quella che abitualmente usiamo). Ricordiamo di cosa si tratta, partendo da un esempio. Se scriviamo $n = 2375$ stiamo dicendo che $n$ è la somma $5+7\cdot 10+3\cdot 10^2+2\cdot 10^3$ (e chiamiamo 5, 7, 3, 2, nell'ordine, cifra delle unità, delle decine, delle centinaia, delle migliaia). In generale, utilizziamo una stringa di cifre $\langle a_t a_{t-1} a_{t-2} \dots a_2 a_1 a_0\rangle$ (dove $t$ è un numero intero non negativo, per cifra intendiamo un numero intero compreso tra 0 e 9, ed usiamo il simbolo $\langle \dots \rangle$ all'unico scopo di non confondere, come sarebbe altrimenti possibile, questa scrittura con quella del prodotto tra le cifre[4]) per indicare il numero $a_0 + 10a_1 + 10^2 a_2 + \dots + 10^t a_t$. In forma più compatta:

$$\langle a_t a_{t-1} a_{t-2} \dots a_2 a_1 a_0\rangle = \sum_{i=0}^{t} a_i 10^i.$$

Poniamo $n = \langle a_t a_{t-1} a_{t-2} \dots a_2 a_1 a_0\rangle$ e cerchiamo di calcolare $n$ modulo $m$, per alcuni valori dell'intero $m$. È abbastanza ovvio che

$$n \equiv_{10} a_0,$$

dunque $a_0$ (la cifra delle unità) è proprio il resto di $n$ nella divisione per 10. Fermiamoci un attimo per una semplice osservazione:

**Lemma.** *Siano $u, v \in \mathbb{Z}$ e sia $m$ un intero positivo. Se $u \equiv_m v$, allora $u \equiv_d v$ per ogni divisore positivo $d$ di $m$,*

*Dimostrazione.* Se $u \equiv_m v$, allora $u - v$ è un multiplo di $m$. Se $d$ è un divisore di $m$, tutti i multipli di $m$ sono anche multipli di $d$, quindi $u - v$ è un multiplo di $d$, vale a dire: $u \equiv_d v$. □

Ne deduciamo che, con le notazioni usate sopra, in conseguenza di $n \equiv_{10} a_0$ abbiamo anche $n \equiv_5 a_0$ e $n \equiv_2 a_0$. Da ciò i ben noti criteri di divisibilità per 2, per 5 e per 10: un intero positivo $n$ è divisibile per 2 (risp. 5, 10) se e solo se lo è la sua cifra delle unità. Detto diversamente: un intero positivo è pari se e solo se la sua cifra delle unità è pari, è divisibile per 5 se e solo se la sua cifra delle unità è una tra 5 e 0 (questo perché tra le cifre solo queste due sono numeri divisibili per 5), è divisibile per 10 se e solo se la sua cifra delle unità è 0.

Cosa succede per altre potenze di 10? Abbiamo sicuramente $n \equiv_{100} 10a_1 + a_0 = \langle a_1 a_0\rangle$, dal momento che nella somma $\sum_{i=0}^{t} a_i 10^i$ ogni addendo $10^i a_i$ per $i > 1$ è multiplo di 100. Dunque, modulo 100, il nostro intero positivo $n$ è congruo al numero formato dalle sue ultime due cifre. Usando il lemma precedente, otteniamo anche che vale l'analoga congruenza modulo un qualsiasi divisore di 100, quindi $n \equiv_d \langle a_1 a_0\rangle$ se $d$ è uno tra 4, 20, 25, 50, 100. Per ciascuno di questi numeri abbiamo dunque il criterio di divisibilità: $n$ è divisibile per $d$ se e solo se lo è il numero costituito dalle ultime sue due cifre. Si potrebbe continuare all'infinito considerando tutte le potenze di 10 ed i loro divisori ed ottenendo per essi criteri di divisibilità: per ogni intero positivo $\ell$, infatti, $n$ è congruo modulo $10^\ell$ al numero formato dalle sue ultime $\ell$ cifre (questo numero è il resto di $n$ nella divisione per $10^\ell$).

Veniamo ad un caso più interessante: ragioniamo modulo 9. Abbiamo $10 \equiv_9 1$ e quindi $10^i \equiv_9 1^i \equiv_9 1$ per ogni intero non negativo $i$. Allora

$$n = \langle a_t a_{t-1} a_{t-2} \dots a_2 a_1 a_0\rangle = \sum_{i=0}^{t} a_i 10^i \equiv_9 \sum_{i=0}^{t} a_i.$$

Abbiamo provato che ogni numero intero positivo è congruo, modulo 9, alla somma delle sue cifre. Ne ricaviamo un metodo per calcolare il resto modulo 9 di un arbitrario intero positivo: sostituire ripetutamente al numero la somma delle sue cifre sino ad ottenere un numero di una sola cifra; questo numero è il resto cercato se è diverso da 9, se invece questo numero è 9 allora il resto è 0. Vediamo un esempio: sia $n = 672455978913$. Allora $n \equiv_9 6 + 7 + 2 + 4 + 5 + 5 + 9 + 7 + 8 + 9 + 1 + 3$. Notiamo che non è necessario effettuare realmente la somma, dato che siamo interessati solo al calcolo modulo 9. Possiamo dunque cancellare i 9, 2 con uno dei 7, 6 con 3, 4 con uno dei 5 e 8 con 1, ottenendo $n \equiv_9 5 + 7 = 12 \equiv_9 1 + 2 = 3$. Il resto, dunque è 3. Partendo da 1008 otteniamo invece $1008 \equiv_9 1 + 0 + 0 + 8 = 9 \equiv_9 0$; ovviamente il resto non è 9 ma 0.

Ricaviamo poi, per il solito lemma, che ogni intero positivo è congruo alla somma delle sue cifre anche modulo 3. Da queste considerazioni seguono (come caso particolare, il nostro risultato dice qualcosa in più) i criteri di divisibilità per 9 e per 3: *un numero intero è divisibile per* 9, *ovvero per* 3 *se e solo*

[4]per intenderci meglio, anche alla luce di quanto stiamo per dire: se $t = 1$, $a_0 = 2$ e $a_1 = 7$, se scriviamo $\langle a_1 a_0\rangle$ intendiamo il numero 72, non il numero $14 = 7 \cdot 2$, come invece siamo portati a fare quando scriviamo $a_1 a_0$.

*se lo è la somma delle sue cifre* ed anche un altro classico ed un po' misterioso strumento che viene spesso introdotto nelle scuole elementari: la cosiddetta *prova del nove*. Si tratta di un metodo di verifica della correttezza del risultato di un calcolo tra numeri interi e consiste, in sostanza, nel calcolare i resti modulo 9 di due numeri, differentemente rappresentati, che si ritiene coincidano. Se questi resti non coincidono, allora sicuramente non coincidono i due numeri. Ad esempio, supponiamo di aver calcolato il prodotto tra due numeri $a$ e $b$, ottenendo $c$ (discorso analogo varrebbe per una somma anziché un prodotto). Con il metodo della somma delle cifre possiamo calcolare i resti $a'$ di $a$, $b'$ di $b$ e $c'$ di $c$ modulo 9. Moltiplichiamo poi tra loro $a'$ e $b'$, e calcoliamo il resto (sempre modulo 9) di $a'b'$. Se i nostri calcoli, a partire da $ab = c$, sono corretti, allora l'ultimo resto trovato deve essere proprio $c'$, altrimenti c'è un errore da qualche parte. Infatti, se $ab = c$ allora deve essere $a'b' \equiv_9 ab = c \equiv_9 c'$. È bene tenere a mente che, viceversa, il fatto che il test "prova del nove" sia passato non garantisce affatto che il calcolo originario sia corretto. Ad esempio, calcoli come $7 + 2 = 702$ oppure $33 \cdot 21 = 0$ passano senza problemi la prova del nove.

Veniamo ad un altro criterio di divisibilità molto noto, quello per 11. Ragionando come abbiamo fatto per 9, iniziamo a notare che $10 \equiv_{11} -1$ e da ciò segue $10^i \equiv_{11} (-1)^i$, per ogni intero non negativo $i$; si ha dunque $10^i \equiv_{11} 1$ se $i$ è pari e $10^i \equiv_{11} -1$ se $i$ è dispari. Allora, per il nostro solito intero positivo $n = \langle a_t a_{t-1} a_{t-2} \dots a_2 a_1 a_0 \rangle$ abbiamo:

$$n = \sum_{i=0}^{t} a_i 10^i \equiv_{11} \sum_{i=0}^{t} (-1)^i a_i = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^t a_t,$$

vale a dire: modulo 11, $n$ è congruo alla somma delle sue cifre prese a segni alterni, ad iniziare da quella delle unità con segno positivo. Otteniamo così il criterio di divisibilità per 11: *un intero $n$ è divisibile per 11 se e solo se la differenza tra la somma delle sue cifre di posto pari e quelle di posto dispari è un multiplo di* 11. Meglio, quello che abbiamo dimostrato è che si può calcolare il resto della divisione per 11 di un numero intero positivo calcolando ripetutamente la somma alterna delle cifre menzionata sopra sino a ridursi ad un numero minore di 11; questo numero sarà il resto cercato. Come fatto per i calcoli modulo 9, anche in questo caso, piuttosto che eseguire tutte le somme possiamo usare liberamente le scorciatoie fornite dall'aritmetica modulare per arrivare più rapidamente al risultato. Ad esempio, per lo stesso $n = 672455978913$ esaminato sopra con riferimento a 9, abbiamo $n \equiv_{11} 3-1+9-8+7-9+5-5+4-2+7-6$, che semplificando in modo ovvio diventa $n \equiv_{11} 3-1-8+7+4-2+7-6 = -1+4+7-6 \equiv_{11} -1-6 = -7 \equiv_{11} 4$. Il resto di $n$ nella divisione per 11 è dunque 4.

3.1. **Altri criteri.** Serve a qualcosa un criterio di divisibilità per 6? Si potrebbe rispondere di no: un numero intero è divisibile per 6 se e solo se è divisibile sia per 2 che per 3, quindi per sapere se un numero è o meno divisibile per 6 basta applicare i due criteri, già noti, per 2 e per 3. E ci serve davvero un criterio di divisibilità per $121 = 11^2$? Anche in questo caso si potrebbe farne a meno: per stabilire se un certo intero $n$ è o meno divisibile per 121 si potrebbe applicare ad esso il criterio di divisibilità per 11; se il criterio fallisce allora $n$ non è divisibile per 121 (per esserlo dovrebbe essere divisibile per 11), se invece $n$ risulta divisibile per 11 allora si può calcolare $n' = n/11$ ed applicare lo stesso criterio ad $n'$; infatti $n$ è divisibile per 121 se e solo se $n'$ è divisibile per 11. Questo metodo si può estendere a potenze arbitrarie di 11 (o di altri numeri per i quali un criterio di divisibilità sia disponibile); ovviamente non è altrettanto veloce quanto criteri più diretti, come quello per 9.

Queste argomentazioni si possono ulteriormente estendere per raggiungere la conclusione che basti avere criteri di divisibilità per numeri primi per avere criteri di divisibilità per interi arbitrari. Se guardiamo ai numeri interi positivi primi più piccoli, ci accorgiamo di avere a disposizione criteri per 2, 3, 5, 11, ma non per 7, 13, 17 etc.

Esaminiamo il caso di 7. Da un intero positivo $n$, isoliamo la cifra $a$ dell'unità e scriviamo $n$ come $10b + a$; dunque $b$ è il numero ottenuto da $n$ cancellando l'ultima cifra (naturalmente $b$ ed $a$ sono il quoziente ed il resto nella divisione di $n$ per 10). Poiché 21 è multiplo di 7, abbiamo $20 \equiv_7 -1$, dunque $2n = 20b + 2a \equiv_7 -b + 2a$. Ora, non è difficile riconoscere che $n$ è divisibile per 7 se e solo se lo è il suo doppio $2n$[5], o, equivalentemente, $-2n = b - 2a$. Dunque, per verificare se $n$ è o meno divisibile

[5]che $2n$ sia multiplo di 7 se lo è $n$ è del tutto ovvio. Viceversa, assumiamo che 7 divida $2n$. Assumendo nota l'unicità della fattorizzazione degli interi in prodotti di primi, sappiamo che la fattorizzazione di $2n$ (nella quale deve apparire 7) si ottiene aggiungendo un 2 alla fattorizzazione di $n$, quindi 7 deve apparire in questa fattorizzazione, cioè: 7 divide $n$.

Più in generale, vale un importantissimo risultato, noto come *lemma di Euclide: siano $a, b$ e $c$ numeri interi. Se $a$ divide $bc$ ed $e$ coprimo con $b$, allora $a$ divide $c$.*

Nell'argomentazione appena svolta abbiamo un po' barato: nella maggior parte delle trattazioni dell'aritmetica il lemma

per 7 possiamo sostituire $n$ con $n_1 = b - 2a$; queso numero sarà quasi sempre più piccolo di $n$: quasi sempre avrà una cifra in meno. Se sappiamo se $n_1$ è o meno divisibile per 7, a questo punto ci possiamo fermare: $n$ è divisibile per 7 se e solo se lo è $n_1$. Altrimenti, ripetiamo il procedimento partendo da $n_1$ piuttosto che da $n$, e andiamo avanti con la procedura finché non otteniamo la risposta. Un esempio: partiamo da $n = 314932$. Dunque, con la notazioni di sopra, $a = 2$ e $b = 31493$; allora da $n$ passiamo a $n_1 = b - 2a = 31489$. Allo stesso modo, da $n_1$ passiamo a $3148 - 2 \cdot 9 = 3130$, da qui a $313 - 2 \cdot 0 = 313$, poi a $31 - 2 \cdot 3 = 25$, che sappiamo non essere multiplo di 7. La conclusione è che 7 non divide $n$. Si potrebbe velocizzare la procedura e semplificare i conti? Certamente: ragionando come nell'Esempio 1, vediamo che da $n = 314932$ possiamo "azzerare" il 14; più precisamente $n \equiv_7 n' := n - 14000 = 300932$; inoltre possiamo "ridurre la cifra 9 a 2: $n' \equiv_7 n'' := n' - 700 = 300232$. Proseguendo, ed applicando qua e là gli stessi trucchi, da $n''$ passiamo a $30023 - 2 \cdot 2 = 30019 \equiv_7 30012$, da questo a $3001 - 2 \cdot 2 = 2997 \equiv_7 2220$, poi a $222 - 2 \cdot 0 = 222$, infine a $22 - 2 \cdot 4 = 18$, non multiplo di 7.

Osserviamo che, a differenza di quanto accadeva con i criteri di divisibilità esaminati prima, questo criterio di divisibilità per 7, così descritto, non fornisce il resto della divisione del numero per 7, ma si limita solo a stabilire se 7 divide o meno il numero, cioè se questo resto è o non è 0 (in realtà si potrebbe modificare il metodo in modo che si tenga traccia anche del resto, ma al costo di complicarlo).

Possiamo trovare analoghi criteri di divisibilità anche per altri primi. Ad esempio, facciamolo per 13: come nel caso di 7 ci serve un multiplo di 13 che differisca di 1 da un multiplo di 10; andrà bene 39. Definiti $n$, $a$ e $b$ come sopra, quindi $n = 10b + a$, abbiamo che 13 divide $n$ se e solo se divide $4n = 40b + 4a \equiv_{13} b + 4a$. Quindi si può decidere se un numero intero è o meno divisibile per 13 con lo stesso metodo usato per 7: l'unica differenza è che, ad ogni passaggio, si sommerà il quadruplo della cifra delle unità anziché sottrarre il doppio. Vediamo direttamente un esempio. Partendo dallo stesso $n = 314932$ di prima, passiamo a $31493 + 4 \cdot 2 = 31501$, poi a $3150 + 4 \cdot 1 = 3154$, poi a $315 + 4 \cdot 4 = 331$, a $33 + 4 \cdot 1 = 37$, che non è multiplo di 13, quindi non lo è $n$ (volendo avremmo potuto proseguire anche oltre 37, ottenendo $3 + 4 \cdot 7 = 31$ e quindi $3 + 4 \cdot 1 = 7$). Nulla vieta, anche in questo caso di usare semplificazioni: ad esempio, poiché $14 \equiv_{13} 1$, si ha $n \equiv_{13} 301932$, quindi saremmo potuti partire da questo numero, o anche da 301802, sfruttando $93 \equiv_{13} 80$.

Lo stesso metodo si può applicare, ad esempio, a 17, a 19 ed a primi maggiori. Nel caso di 17 dovremmo usare, con le solite notazioni, la trasformazione $n \mapsto b - 5a$ (quindi $-5$ svolge il ruolo he avevano $-2$ nel caso di 7 e 4 nel caso di 13; questo perché $50 \equiv_{17} -1$); per 19 useremo invece $n \mapsto b + 2a$, per 23 useremo $n \mapsto b + 7a$, per 29 useremo $n \mapsto b + 3a$. Chi legge si può divertire a verificare la correttezza di queste affermazioni, a costruirsi esempi, a trovare criteri di divisibilità per altri primi.

## 4. Calendario di un girone all'italiana

Supponiamo di volere organizzare un torneo tra un certo numero $n$ (ovviamente intero e positivo!) di squadre. Il formato prescelto è quello, piuttosto familiare, del *girone all'italiana*: il torneo è articolato in più giornate, in ciascuna delle quali si svolgeranno gli incontri (le partite) tra le squadre; alla fine del torneo ogni squadra dovrà avere incontrato esattamente una volta ciascuna delle altre—il girone di andata (o quello di ritorno) del campionato di calcio di serie A è un esempio di girone all'italiana.

Cerchiamo di essere più precisi. Richiediamo che ogni partita coinvolga esattamente due squadre tra le $n$ partecipanti al torneo (non è un'osservazione inutile: in un torneo di calcio, basket, rugby, pallavolo lo diamo per scontato, ma in un torneo di bocce o di poker?). Stiamo così anche dicendo che una partita non può essere giocata da una squadra contro se stessa. Altre richieste sono: (1) che ogni giornata coinvolga quante più squadre possibile, ma (2) nessuna squadra abbia due impegni (cioè appaia in due partite) nella stessa giornata. Quante sono, allora, in ciascuna giornata, le partite? Questo è facile: se il numero $n$ delle squadre è pari, allora ogni giornata consisterà di $n/2$ partite e vedrà impegnate tutte le squadre; se invece $n$ è dispari, allora, in ogni giornata, una delle squadre dovrà restare ferma (avrà un *turno di riposo*, come si dice) e le rimanenti $n - 1$ si affronteranno in $(n - 1)/2$ partite. E quante sono le giornate in cui si articola il torneo? Beh, qui bisogna esaminare separatamente i casi in cui $n$ è pari e quello in cui $n$ è dispari. Siccome ogni squadra deve incontrare (in giornate diverse) una ed una sola volta ciascuna delle altre, ogni squadra dovrà disputare $n - 1$ partite, e questo è vero in entrambi i casi, ma:

di Euclide viene usato per dimostrare il teorema di fattorizzazione unica; quindi la nostra argomentazione assume per noto un teorema più forte di quello che intende provare. Aggiungiamo anche in matematica si preferisce dare un definizione generale di 'primo' diversa da quella scolastica, come elemento (ad esempio, numero) per il quale valga una particolare forma del lemma di Euclide.

- se $n$ è pari ogni squadra gioca precisamente una partita per giornata, quindi il numero delle giornate coincide con quello della partite giocate da una squadra, vale a dire $n-1$;
- se $n$ è dispari il calcolo è meno diretto: ciascuna squadra giocherà $n-1$ partite (in $n-1$ giornate), come per il caso precedente, ma avrà anche dei turni di riposo. Se il numero dei turni di riposo della squadra considerata è $r$, il numero delle giornate sarà quindi $n-1+r$; questo numero non lo non conosciamo perché non conosciamo ancora $r$. Possiamo seguire una strada diversa: contare il numero complessivo di partite: ci sono $n$ squadre, ciascuna di esse gioca $n-1$ partite, abbiamo quindi un totale di $n(n-1)$ coppie ordinate $(S,P)$ costituite da una squadra $S$ ed una partita $P$ giocata da $S$; ma ogni partita è giocata da due squadre, quindi per ottenere il numero delle partite dobbiamo dividere il numero di tali coppie per 2. In definitiva, nel torneo verranno giocate in tutto $n(n-1)/2$ partite.[6] Poiché ogni giornata consiste di $(n-1)/2$ partite, la conclusione è che di giornate ce ne sono $n$ (il numero $n(n-1)/2$ delle partite nel torneo diviso per il numero $(n-1)/2$ di partite per giornata). Una conclusione accessoria è anche che ogni squadra osserverà esattamente un turno di riposo, infatti il numero delle giornate del torneo lo avevamo anche calcolato come $n-1+r$.

Ad esempio, il torneo di rugby delle sei nazioni che, non sorprendentemente, si disputa tra sei squadre (Irlanda, Galles, Scozia, Inghilterra, Francia, Italia) si svolge con un girone all'italiana (di sola andata); il torneo prevede dunque cinque giornate di tre partite ciascuna ($n=6$ è il numero delle squadre, che è dunque pari; $n-1=5$ le giornate; $n/2$ le partite per giornata). Prima dell'anno 2000 l'Italia non partecipava al torneo, che era ristretto alle altre squadre e si chiamava allora torneo delle cinque nazioni. All'epoca, dunque, il numero delle squadre partecipanti, $n=5$, era dispari, il torneo si svolgeva comunque in cinque giornate, ciascuna delle quali prevedeva due partite ($2=(5-1)/2$) ed una squadra ferma in turno di riposo.

Preparare un calendario per il torneo delle sei nazioni è semplicissimo: quando il numero delle squadre partecipanti è così piccolo, è piuttosto facile stendere un calendario per un girone all'italiana, procedendo per tentativi (si abbinano in qualche modo le squadre per mettere assieme la prima giornata e poi si procede, evitando di ripetere partite già disputate, con le giornate successive), ma quando il numero dei partecipanti sale diventa molto più complicato farlo (procedendo alla cieca si rischia, dopo un certo numero di giornate, di non potere evitare ripetizioni di partite; a quel punto bisogna fare un passo indietro e riprovare), a meno di non disporre di un metodo sistematico da utilizzare allo scopo. Ne discuteremo qui uno molto semplice.

Abbiamo fatto sopra una distinzione tra il caso in cui il numero $n$ delle squadre partecipanti è pari da quello in cui $n$ è dispari; effettivamente, nei due casi, i calendari dei tornei hanno aspetto diverso (solo nel secondo caso sono previsti turni di riposo). Potrebbe sembrare necessario cercare due metodi diversi per costruire il nostro calendario; uno da usare nel caso $n$ sia pari, l'altro nel caso dispari. Fortunatamente non è così: se sappiamo risolvere il nostro problema in uno dei due casi è molto facile risolverlo anche nell'altro.

Supponiamo infatti di saper comporre un calendario per tornei con un arbitrario numero dispari di squadre e trovarci, invece, a doverne comporre uno con un numero pari $n$ di squadre. Per farlo sarà sufficiente mettere momentaneamente da parte una delle squadre, chiamiamola $A$, compilare un calendario per un torneo tra le $n-1$ squadre rimanenti (che sono dunque in numero dispari) e poi modificarlo inserendo, ad ogni giornata, una partita tra $A$ e la squadra che nel primo calendario aveva, in quella giornata, il turno di riposo. Ad esempio, per compilare un calendario per il torneo delle sei nazioni dell'anno 2000 (a sei squadre) sarebbe stato sufficiente prendere il calendario dell'anno precedente (a cinque squadre: mancava l'Italia), che come abbiamo visto prima si svolgeva in cinque giornate di due partite l'una ed aggiungere, in ciascuna giornata, una partita tra l'Italia e la squadra col turno di riposo.

Viceversa, se sappiamo comporre un calendario per tornei con un numero pari di squadre ma abbiamo il compito di organizzare un girone all'italiana per un numero dispari $n$ di squadre non dovremo fare altro che inventarci una squadra fittizia aggiuntiva, chiamiamola $F$, e preparare il calendario per il girone tra le $n+1$ squadre (quelle originali più $F$; sono in numero pari quindi siamo capaci di farlo). Per ottenere il calendario desiderato basterà cancellare, ad ogni giornata, la partita che vedeva coinvolta $F$; la squadra avversaria avrà, giocoforza, turno di riposo. Ad esempio, un calendario per un'edizione del torneo delle cinque nazioni si può ottenere da un calendario per il torneo delle sei nazioni cancellando

[6] Abbiamo fatto del semplice calcolo combinatorio, chi ne ricorda un po' riconosce qui il coefficiente binomiale $\binom{n}{2} = n(n-1)/2$, che è il numero dei sottoinsiemi costituiti da due elementi in un insieme costituito da $n$ elementi: osservare che una partita si può anche riguardare come la selezione di un sottoinsieme di due elementi nell'insieme di tutte le squadre.

sistematicamente le partite dell'Italia e lasciando a riposo, giornata per giornata, l'avversario di turno dell'Italia.

Non è difficile verificare (e chi legge è invitato a farlo) che i calendari ottenuti da questi due procedimenti verificano le richieste fatte (che ogni squadra incontri ciascuna altra squadra esattamente una volta nel torneo, eccetera).

A questo punto sappiamo che per descrivere un metodo generale per la stesura di un calendario per un girone all'italiana basta limitarsi a farlo nel caso in cui il numero delle squadre è pari, o, in alternativa, nel caso in cui questo numero è dispari. Anche se la prima opzione è quella che corrisponde al caso più consueto (in genere i tornei sono organizzati tra un numero pari di squadre) ci pare più semplice, dal punto di vista matematico, la descrizione della procedura nel secondo caso, quindi supporremo che il numero $n$ delle squadre partecipanti al torneo sia dispari.

I dati di partenza sono dunque questi: un intero positivo dispari $n$ e $n$ squadre (distinte tra loro), che indichiamo come $S_1$, $S_2, \dots, S_n$. In accordo con i calcoli svolti sopra, dobbiamo definire $n$ giornate del nostro torneo, che possiamo ovviamente chiamare prima giornata, seconda giornata, e così via, sino alla $n$-esima giornata. Ciascuna delle giornate è specificata dalle $(n-1)/2$ partite che vi si svolgono (tra $n-1$ delle squadre; la rimanente ha il turno di riposo). La definizione che proponiamo è questa:

> *scelti comunque gli interi $i, j, k$ nell'insieme $\{1, 2, 3, \dots, n\}$, nella $k$-giornata si svolge la partita tra le squadre $S_i$ e $S_j$ se e solo se*
> $$i \neq j \quad e \quad i + j \equiv_n k.$$

Ad esempio, se $n = 15$, nella prima giornata giocheranno tra loro $S_4$ ed $S_{12}$, perché $4 + 12 \equiv_{15} 1$; nella tredicesima, invece, $S_4$ giocherà contro $S_9$, perché $4 + 9 \equiv_{15} 13$.

Verifichiamo che la definizione che abbiamo proposto fornisce un calendario "corretto". Si tratta di controllare che il calendario che stiamo definendo soddisfa tutti i vincoli che avevamo richiesto. Innanzitutto, nessuna squadra gioca mai con se stessa: la nostra definizione impone che affinché si possa svolgere una partita tra le squadre $S_i$ e $S_j$ si debba avere $i \neq j$. Dunque, ogni partita coinvolge precisamente due squadre (distinte). È vero che ogni squadra incontra ciascuna altra squadra esattamente una volta nel torneo? Sì, perché se $S_i$ e $S_j$ sono due tra le nostre squadre, e $i \neq j$, sappiamo che esiste uno ed un solo $k_{ij} \in \{1, 2, 3, \dots, n\}$ tale che $i + j \equiv_n k_{ij}$ (detto $r$ il resto nella divisione di $i + j$ per $n$, se $r \neq 0$, allora questo $k_{ij}$ è proprio $r$, altrimenti $k_{ij}$ è $n$). Questo significa che $S_i$ e $S_j$ si incontreranno esattamente una volta: nella $k_{ij}$-esima giornata. Notiamo anche che quando $S_i$ gioca con $S_j$, si ha anche che $S_j$ gioca con $S_i$ (meno male! Se così non fosse le "partite" non sarebbero ben definite), questo è conseguenza della proprietà commutativa dell'addizione. Quante sono le partite che si svolgono in una fissata ora una giornata, diciamo la $k$-esima? Fissato $i \in \{1, 2, \dots, n\}$, esiste uno ed un solo $j \in \{1, 2, \dots, n\}$ tale che $i + j \equiv_n k$: è quel'unico $j$ nell'insieme dato tale che $j \equiv_n k - i$. La nostra definizione assicura che nella $k$-esima giornata $S_i$ non potrà giocare con alcuna squadra diversa da $S_j$; quindi $S_i$ gioca al massimo una partita in questa giornata. Ora si dànno due possibilità: o $i \neq j$, ed allora $S_i$ gioca con $S_j$, oppure $i = j$ e quindi $S_i$ non gioca con $S_j$; ma in questo secondo caso $S_i$, nella $k$-esima giornata non gioca proprio ed osserva un turno di riposo. Benissimo, quante sono le squadre che riposano nella $k$-esima giornata? Da quanto abbiamo appena visto segue subito che una squadra $S_i$ riposa nella $k$-esima giornata se e solo se si ha $2i \equiv_n k$, quindi bisogna stabilire quanti sono gli $i \in \{1, 2, \dots, n\}$ tali che $2i \equiv_n k$. Lo si potrebbe fare immediatamente utilizzando la teoria delle equazioni congruenziali (vedi oltre per qualche cenno a riguardo), ma possiamo anche arrivarci per via diretta. Se $k$ è pari, un tale $i$ è certamente $i/2$. Se $k$ è dispari, invece, $n + k$ è pari (perché $n$, ricordiamo, è dispari), dunque $(n + k)/2$ è un intero; ponendo appunto $i = (n + k)/2$ abbiamo di nuovo $2i = n + k \equiv_n k$. Dunque, in ciascun caso almeno un $i \in \{1, 2, \dots, n\}$ verifica la condizione.[7] È possibile che più di una squadra riposi nella $k$-esima giornata? Vediamo: supponiamo che riposino sia $S_i$ che $S_{i'}$, dove, naturalmente, $i, i' \in \{1, 2, \dots, n\}$. Allora sia $2i$ che $2i'$ sono congrui a $k$ modulo $n$; in particolare $2i \equiv_k 2i'$, vale a dire: $k$ divide $2(i - i')$. Poiché $k$ è dispari, se ne ricava che $k$ divide $i - i'$, ovvero $i' \equiv_n i$.[8] Ricordando che gli elementi di $\{1, 2, \dots, n\}$ sono a due a due non congrui modulo $n$, otteniamo $i' = i$, cioè $S_i = S_{i'}$. In questo modo abbiamo provato che

[7] in altri termini: almeno una squadra riposa nella $k$-esima giornata. Del resto questo segue anche dal fatto che le partite che si svolgono nella giornata coinvolgono un numero totale pari di squadre (due per partita, tutte diverse tra loro); essendo il numero delle squadre partecipanti dispari, è chiaro che almeno una di esse non gioca.

[8] la cosa è abbastanza intuitiva, ma dipende in ultima analisi dal lemma di Euclide; vedi la nota 5.

solo una squadra riposa nella $k$-esima giornata. A questo punto siamo certi del fatto che il nostro metodo fornisce un calendario corretto per un girone all'italiana.

Possiamo descrivere questo metodo in modo ancora più sintetico facendo riferimento alle tavole di Cayley, che abbiamo discusso in precedenza: il calendario che abbiamo descritto è codificato nella tavola di Cayley per l'addizione in $\mathbb{Z}_n$. Lo possiamo comprendere bene con un esempio concreto. Poniamo $n = 7$ e scriviamo la tavola di Cayley per l'addizione in $\mathbb{Z}_7$. Per poter mantenere le stesse notazioni che stiamo usando in questa sezione, utilizziamo però 7 anziché 0 per rappresentare la classe $[0]_7$:

| $+$ | 7 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 7 | 7 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 1 | 2 | 3 | 4 | 5 |

Leggiamo in questa tabella il calendario: assumendo $i \neq j$, la squadra $S_i$ incontra la squadra $S_j$ nella giornata indicata dal numero nella riga intestata da $i$ e colonna intestata da $j$, dal momento che questo numero è congruo a $i + j$. Ad esempio, $S_2$ incontra $S_6$ nella prima giornata, ed incontra $S_3$ nella quinta. Quindi i numeri che leggiamo nella tabella, al di fuori della diagonale da "alto-sinistra" a "basso-destra" ci dicono in quale giornata si incontreranno le squadre che descrivono la posizione del numero. E cosa ci dicono invece i numeri sulla diagonale? Beh, un numero che appare sulla diagonale, alla riga intestata da un certo $i$, è anche nella colonna intestata da $i$, quindi rappresenta la classe $[i]_7 + [i]_7 = [2i]_7$; in altre parole è congruo a $2i$. Di conseguenza quel numero indica la giornata in cui la squadra $S_i$ ha il suo turno di riposo; ad esempio, $S_5$ riposa nella terza giornata, $S_6$ nella quinta.

Abbiamo mostrato come, per un qualsiasi intero positivo dispari $n$ si possa usare l'addizione in $\mathbb{Z}_n$ per organizzare un girone all'italiana per un torneo con $n$ squadre. Lo stesso procedimento si può adottare per ottenere altri calendari, utilizzando altri tipi di strutture al posto di $\mathbb{Z}_n$. Forse chi legge sa cosa sia un gruppo abeliano (è un tipo di struttura algebrica di cui $\mathbb{Z}_n$, con l'operazione di addizione, è un esempio; 'abeliano' è solo un modo complicato per dire che vale la proprietà commutativa); se lo sa potrà facilmente riconoscere si può usare la tavola di Cayley di un qualsiasi gruppo abeliano con $n$ elementi per costruire, con lo stesso metodo che abbiamo usato qui, un calendario per un girone all'italiana tra $n$ squadre. Questo dipende dal fatto che le tavole di Cayley dei gruppi abeliani hanno le due proprietà che abbiamo sfruttato per costruire i nostri calendari a partire dall'addizione in $\mathbb{Z}_n$: sono simmetriche rispetto alla diagonale (perché l'operazione è commutativa) e, come nel Sudoku, non presentano mai ripetizioni dello stesso simbolo in alcuna riga. Questa seconda proprietà (che si chiama cancellabilità) avrà un ruolo importante nella prossima sezione.

## 5. Invertibili, Fermat ed Eulero

Torniamo ora a qualcosa di carattere più teorico (e quindi, a giudizio di chi scrive, probabilmente più interessante). Nello studio degli anelli $\mathbb{Z}_m$ ha grande importanza la descrizione degli elementi invertibili. Abbiamo già incontrato questa nozione: un elemento $[a]_m$ di $\mathbb{Z}_m$ (consideriamo fissato l'intero positivo $m$) è invertibile se e solo se esiste un $[b]_m \in \mathbb{Z}_m$ tale che $[a]_m[b]_m = [1]_m$. Si dimostra (lo si potrebbe far seguire dalla proprietà di cancellabilità che vedremo tra poco) che se $[a]_m$ è invertibile allora esiste esattamente un $[b]_m$ con la proprietà richiesta; questo $[b]_m$ si chiama l'*inverso* di $[a]_m$.[9]

Notiamo che $[a]_m[b]_m$ è di per sé $[ab]_m$; la condizione di invertibilità si può dunque riformulare così: $[a]_m$ è invertibile se e solo se esiste $b \in \mathbb{Z}$ tale che $[ab]_m = [1]_m$, ovvero $ab \equiv_m 1$. Ad esempio, abbiamo già visto che in $\mathbb{Z}_5$ sono invertibili tutti gli elementi tranne $[0]_5$, mentre in $\mathbb{Z}_6$ sono invertibili solo $[1]_6$

[9] la definizione di elemento invertibile e di inverso si dà in contesti molto più generali, quella che abbiamo formulato qui ne è giusto un caso particolare. Quando la si dà in altre strutture, il ruolo che qui svolge $[1]_m$ è riservato all'elemento neutro della struttura (anche dell'elemento neutro si può dimostrare l'unicità). Aggiungiamo anche, giusto per scrupolo di precisione, che la definizione va modificata (è un po' più elaborata) nel caso in cui la struttura considerata non sia commutativa, come invece è quella che stiamo considerando in $\mathbb{Z}_m$.

e $[-1]_6 = [5]_6$ (ciascuno dei quali coincide col suo inverso); in $\mathbb{Z}_{10}$ è, tra gli altri, invertibile $[3]_{10}$, il cui inverso è $[7]_{10}$ (verificare!).

Esiste un semplice modo per stabilire se un elemento di $\mathbb{Z}_m$ è o meno invertibile. Per descriverlo possiamo fare riferimento alle cosiddette *equazioni congruenziali* (di primo grado). Cosa sono? Essenzialmente ordinarie equazioni considerate in $\mathbb{Z}_m$ anziché in uno degli abituali insiemi di numeri. Una equazione di primo grado in $\mathbb{Z}_m$, in una incognita $X$, è una equazione della forma

$$AX = B \tag{$*$}$$

dove $A$ e $B$ sono due elementi di $\mathbb{Z}_m$, cioè due classi di resto modulo $m$. Ad esempio, $[2]_7X = [3]_7$ è un'equazione del genere, per $m = 7$. Naturalmente risolvere l'equazione $(*)$ significa trovare una classe (o le classi) che sostituite ad $X$ rendano vera l'uguaglianza. Siano $a$ un numero in $A$ e $b$ un numero in $B$, quindi $A = [a]_m$ e $B = [b]_m$. Siccome $X$ rappresenta una classe di resto, possiamo anche scrivere $X = [x]_m$, dove $x$ è una incognita che rappresenta un numero intero. Allora l'equazione $(*)$ si può anche scrivere come $[a]_m[x]_m = [b]_m$, ovvero:

$$ax \equiv_m b. \tag{$**$}$$

Questa si chiama una equazione congruenziale; è, meglio ripeterlo, una forma equivalente di $(*)$. Ad esempio, $[2]_7X = [3]_7$ diventa l'equazione congruenziale $2x \equiv_7 3$, della quale 5 è una soluzione. Non sempre un'equazione congruenziale come $(**)$ ha soluzione; esiste un importante teorema che fornisce un criterio affinché ne abbia. Lo enunciamo ma non lo dimostriamo:

**Teorema** (Criterio di esistenza di soluzioni per equazioni congruenziali)**.** *Scelti comunque $a, b \in \mathbb{Z}$ e l'intero positivo $m$, detto $d$ un massimo comun divisore tra $a$ e $m$, l'equazione congruenziale $(**)$ ha soluzione se e solo se $d$ divide $b$.*

Ad esempio, $12x \equiv_{58} 73$ non ha soluzioni, mentre $12x \equiv_{58} 74$ ne ha, perché il massimo comun divisore positivo tra 12 e 58 è 2, che divide 74 ma non 73. Esiste un metodo esplicito per trovare tutte le (eventuali) soluzioni di una equazione congruenziale di primo grado, ma non ci addentriamo nella sua descrizione. Dimostriamo invece la conseguenza che ci interessa del teorema appena enunciato:

**Corollario.** *Siano $a$ un intero e $m$ un intero positivo. Allora $[a]_m$ è un elemento invertibile di $\mathbb{Z}_m$ se e solo se $a$ ed $m$ sono coprimi.*

*Dimostrazione.* Dire che $[a]_m$ è invertibile significa dire che esiste $b \in \mathbb{Z}$ tale che $ab \equiv_m 1$, ovvero: che l'equazione congruenziale $ax \equiv_m 1$ ha soluzione. Se $d$ è il massimo comun divisore positivo tra $a$ e $m$, allora, per il criterio di esistenza di soluzioni per equazioni congruenziali, appena enunciato, $ax \equiv_m 1$ ha soluzione se e solo se $d$ divide 1. Ma l'unico divisore positivo di 1 è 1 stesso, quindi questa condizione equivale a richiedere che $d$ sia 1, cioè che $a$ ed $m$ siano coprimi. Dunque, $[a]_m$ è invertibile se e solo se $a$ ed $m$ sono coprimi. □

Questo risultato spiega la differenza che avevamo osservato tra $\mathbb{Z}_5$ e $\mathbb{Z}_6$ quando avevamo costruito le tavole di Cayley delle rispettive operazioni di moltiplicazione. Il numero 5 è primo, da questo si deduce che ogni numero intero compreso tra 1 e 4 è coprimo con 5; quindi tutti gli elementi di $\mathbb{Z}_5$ escluso $[0]_5$ sono invertibili (che $[0]_m$ non possa mai essere invertibile, per alcun $m > 1$, è molto facile da riconoscere, anche senza far ricorso al corollario appena provato). Invece la situazione è diversa per $\mathbb{Z}_6$: nessuno tra 2, 3 e 4 è coprimo con 6, quindi $[2]_6$, $[3]_6$ e $[4]_6$ non sono invertibili. Possiamo generalizzare il discorso fatto per 5: se $m$ è un numero primo e $a$ è un intero tale che $1 \leq a < m$, allora $a$ ed $m$ sono certamente coprimi, quindi $[a]_m$ è invertibile (se $a$ non fosse coprimo con $m$ dovrebbe essere divisibile per un primo divisore anche di $m$. Ma l'unico primo che divida $m$ è $m$ stesso, quindi $a$, per non essere coprimo con $m$, dovrebbe essere un multiplo di $m$, cosa impossibile dal momento che $0 < a < m$). Dunque, se $m$ è primo ogni elemento di $\mathbb{Z}_m$ diverso da $[0]_m$ è invertibile; come detto in precedenza, si esprime questo fatto dicendo che $\mathbb{Z}_m$ è, in questo caso, un campo. Si potrebbe anche dimostrare (e non è difficile, chi legge è invitato a provarci) che vale anche il viceversa: se $\mathbb{Z}_m$ è un campo allora $m$ è primo.

5.1. **La funzione di Eulero.** Il numero degli elementi invertibili in $\mathbb{Z}_m$ è espresso da una funzione (dall'insieme dei numeri interi positivi in sé), tradizionalmente indicata con $\varphi$ e nota come *funzione di Eulero.*[10] Dunque, per ogni intero positivo $m$, con $\varphi(m)$ si intende il numero degli elementi invertibili in $\mathbb{Z}_m$. Dalla descrizione degli elementi di $\mathbb{Z}_m$ e dal corollario che abbiamo dimostrato poco fa segue che $\varphi(m)$ è anche il numero degli interi $a$ coprimi con $m$ e tali che $0 \leq a < m$. Ad esempio, se $m = 2$, l'unico

[10] vengono usati anche altri nomi: funzione (o indicatore) di Eulero-Gauss, funzione totiente.

intero con la proprietà richiesta per $a$ è 1, quindi $\varphi(2) = 1$, se $m = 3$ abbiamo invece due tali interi (1 e 2) e lo stesso vale se $m = 4$ (in questo caso gli interi sono 1 e 3). In un certo modo abbiamo già visto che $\varphi(5) = 4$ e $\varphi(6) = 2$.

In alcuni casi il calcolo di $\varphi(m)$ è molto semplice. Se $m$ è primo, infatti, sappiamo che tutti gli elementi di $\mathbb{Z}_m$ tranne uno di essi ($[0]_m$) sono invertibili; ma allora, siccome $\mathbb{Z}_m$ ha precisamente $m$ elementi, $\varphi(m) = m - 1$. Più in generale, cosa succede se $m$ è una potenza di primo, poniamo $m = p^n$, dove $p$ è primo e $n$ è un intero positivo? Duplicando un ragionamento svolto sopra, vediamo che un numero intero $a$, per non essere coprimo con $p^n$, deve essere divisibile per un qualche primo che divida anche $p^n$, ma l'unico primo che divida $p^n$ è $p$. Allora, per un arbitrario $a \in \mathbb{Z}$, i casi possibili sono due: o $p$ divide $a$ (ed allora $a$ non è coprimo con $p^n$), oppure $p$ non divide $a$ (ed allora $a$ è coprimo con $p^n$). Di conseguenza, $\varphi(p^n)$ è uguale al numero degli interi compresi tra 0 e $p^n - 1$ che non siano multipli di $p$. Siccome i numeri compresi tra 0 e $p^n - 1$ sono in tutto $p^n$ e, tra essi i multipli di $p$ sono quelli della forma $kp$, al variare di $k$ tra 0 e $p^{n-1} - 1$, che sono $p^{n-1}$, concludiamo che

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}.$$

Una proprietà estremamente significativa della funzione di Eulero, che si chiama moltiplicatività, è:

*se $a$ e $b$ sono due numeri interi positivi tra loro coprimi, allora $\varphi(ab) = \varphi(a)\varphi(b)$.*

Non dimostriamo questa proprietà, diciamo però (così abbiamo la scusa per imparare qualcosa in più) che dipende da un teorema noto come *teorema cinese dei resti*: *se $a$ e $b$ sono due numeri interi tra loro coprimi e $r, s \in \mathbb{Z}$, allora esiste un intero $n$ tale che $n \equiv_a r$ e $n \equiv_b s$; l'insieme di tali interi $n$ costituisce una classe di resto modulo $ab$.*

La moltiplicatività, assieme alle osservazioni svolte prima, permette di calcolare i valori della funzione di Eulero per ogni intero positivo $n$ *di cui conosciamo la decomposizione in prodotto di primi.* Supponiamo infatti $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_t^{\lambda_t}$, dove $t$ è un intero non negativo, i $p_i$ sono numeri primi (positivi) a due a due distinti e ciascuno degli esponenti $\lambda_i$ è un intero positivo. Poiché ciascuno dei fattori $p_i^{\lambda_i}$ è coprimo col prodotto degli altri fattori di $n$, possiamo usare ripetutamente la moltiplicatività della funzione di Eulero per ottenere:

$$\varphi(n) = \varphi(p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_t^{\lambda_t}) = \varphi(p_1^{\lambda_1})\varphi(p_2^{\lambda_2}) \cdots \varphi(p_t^{\lambda_t}) = (p_1^{\lambda_1} - p_1^{\lambda_1 - 1})(p_2^{\lambda_2} - p_2^{\lambda_2 - 1}) \cdots (p_t^{\lambda_t} - p_t^{\lambda_t - 1}).$$

Ad esempio, $\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4$, infatti si verifica direttamente che le classi di resto invertibili in $\mathbb{Z}_{10}$ sono quattro: $[1]_{10}$, $[3]_{10}$, $[-3]_{10} = [7]_{10}$ e $[-1]_{10} = [9]_{10}$. Un altro esempio: poiché $6000 = 2^4 \cdot 3 \cdot 5^3$, si ha $\varphi(6000) = (2^4 - 2^3) \cdot (3-1) \cdot (5^3 - 5^2) = 8 \cdot 2 \cdot 100 = 1600$. Osserviamo anche che $\varphi(6000)$ non è uguale a $\varphi(6)\varphi(1000) = 800$ (verificarlo!), benché $6000 = 6 \cdot 1000$: per poter utilizzare la proprietà di moltiplicatività della funzione di Eulero bisogna che i fattori del prodotto che si considera siano coprimi, ma 6 e 1000 non lo sono.

5.2. **Il teorema di Fermat-Eulero.** Il teorema è questo:

**Teorema** (Fermat-Eulero)**.** *Siano $m$ un intero positivo e $a$ un intero coprimo con $m$. Allora $a^{\varphi(m)} \equiv_m 1$.*

Questo teorema fu dimostrato da Leonhard Euler (svizzero, uno dei grandissimi nella storia della matematica) nel 1763, estendendo un precedente teorema, annunciato da Pierre de Fermat (un altro grande matematico, questa volta francese, che non aveva l'abitudine di rendere pubbliche le dimostrazioni dei suoi teoremi) in una lettera ad un amico nel 1640.

**Teorema** (Piccolo Teorema di Fermat)**.** *Siano $p$ un numero primo ed $a$ un intero. Allora $a^p \equiv_p a$.*

Questo secondo teorema si può dimostrare molto facilmente come conseguenza del precedente (che però è storicamente successivo). Infatti, come ormai abbiamo visto in un paio di occasioni, dal momento che $p$ è primo solo due casi sono possibili: o $p$ divide $a$ oppure $a$ e $p$ sono coprimi. Nel primo caso $p$ divide anche $a^p$, ovviamente, quindi $a^p \equiv_p 0 \equiv_p a$, nel secondo, applicando il teorema di Fermat-Eulero, siccome

$\varphi(p) = p - 1$ abbiamo $a^{p-1} = a^{\varphi(p)} \equiv_p 1$, e quindi (moltiplicando per $a$) $a^p = a \cdot a^{p-1} \equiv_p a \cdot 1 = a$. In entrambi i casi, dunque, $a^p \equiv_p a$, come richiesto dall'enunciato.[11]

Vediamo qualche esempio: abbiamo fatto dei calcoli per la determinazione di giorni della settimana, quindi in aritmetica modulo 7. Bene, ora sappiamo che, ogni numero $a$ che non sia multiplo di 7 verifica $a^6 \equiv_7 1$, per il teorema di Fermat-Eulero; saperlo da prima ci avrebbe risparmiato qualche calcolo. Ma anche, ad esempio, scopriamo, senza dover fare conti, che $379^{1600} - 1$ è un multplo di 6000; infatti abbiamo visto che $\varphi(6000) = 1600$ e, inoltre, 379, non essendo divisibile né per 2, né per 3 né per 5, è coprimo con 6000 e quindi $379^{1600} \equiv_{6000} 1$. Esempi del genere dovrebbero convincere chi legge del gran significato e della grande utilità del teorema di Fermat-Eulero.

Veniamo ad una sua dimostrazione. Ne possiamo fornire una del tutto elementare, che parte da due semplici considerazioni sugli elementi invertibili degli anelli $\mathbb{Z}_m$ (e restano valide anche in contesti molto più generali).

La prima: il prodotto tra due elementi invertibili è ancora invertibile. Infatti, se $A$ e $B$ sono due classi di resto invertibili in $\mathbb{Z}_m$, con inversi, rispettivamente, $A'$ e $B'$, allora si ha $(AB)(A'B') = A(BB')A' = A[1]_m A' = AA' = [1]_m$. Questo, (riguardarsi le definizioni all'inizio di questa sezione) significa che $AB$ è invertibile, come volevamo provare, ed anche che $B'A'$ è il suo inverso.

La seconda: ogni elemento invertibile $A$ verifica questa proprietà, detta *cancellabilità*:

$$\textit{per ogni } X, Y \in \mathbb{Z}_m \textit{ se } AX = AY \textit{ allora } X = Y.$$

Infatti, se $AX = AY$, moltiplicando per l'inverso $A'$ di $A$ otteniamo $A'AX = A'AY$, quindi $X = A'AX = A'AY = Y$.[12]

Una parentesi: avevamo già accennato alla cancellabilità nella sezione precedente, in relazione ai calendari dei gironi all'italiana ed alla tavole di Cayley. Ribadiamo questo punto: la cancellabilità di un elemento $A$ di $\mathbb{Z}_m$ significa precisamente che, nella tavola di Cayley di $\mathbb{Z}_m$ rispetto alla moltiplicazione, la riga di $A$ non presenta ripetizioni. Infatti, dire che ci sono ripetizioni significa dire che, in due posizioni distinte della riga, quindi in corrispondenza di due colonne distinte, quella di un elemento $X$ e quella di un elemento $Y$, con $X \neq Y$, dobbiamo avere lo stesso elemento $Z$, quindi $Z = AX = AY$. Questo è precisamente ciò che la proprietà di cancellabilità per $A$ esclude.

Torniamo alla dimostrazione. Elenchiamo gli elementi invertibili di $\mathbb{Z}_m$:

$$X_1, X_2, X_3, \ldots, X_{\varphi(m)}$$

(ricordiamo che gli invertibili di $\mathbb{Z}_m$ sono in tutto $\varphi(m)$, di conseguenza questa è una lista priva di ripetizioni: le classi di resto elencate sono a due a due distinte). Sia $A$ uno di essi. Se moltiplichiamo ciascun elemento della lista precedente per $A$ otteniamo ancora una lista:

$$AX_1, AX_2, AX_3, \ldots, AX_{\varphi(m)}$$

di elementi invertibili di $\mathbb{Z}_m$ (perché il prodotto di due elementi invertibili è sempre invertibile). Inoltre questi elementi sono a due a due distinti: se così non fosse ci sarebbero un $i$ ed un $j$ in $\{1, 2, 3, \ldots, \varphi(m)\}$ tali che $i \neq j$ e $AX_i = AX_j$, ma allora $X_i = X_j$ per la cancellabilità di $A$; questo è impossibile perché la nostra prima lista non presenta ripetizioni. Dunque, anche la seconda lista consiste di $\varphi(m)$ elementi invertibili di $\mathbb{Z}_m$. Siccome $\mathbb{Z}_m$ ha esattamente $\varphi(m)$ elementi, anche questa seconda lista comprende tutti (e soli) gli elementi invertibili di $\mathbb{Z}_m$, senza ripetizioni. In conclusione: le due liste elencano esattamente gli stessi elementi; esse possono differire solo per l'ordine in cui questi appaiono. Moltiplichiamo tra loro le classi nella prima lista da una parte, e quelle nella seconda lista dall'altra. Siccome vale la proprietà commutativa, quindi l'ordine dei fattori è irrilevante ai fini del calcolo del prodotto, otteniamo nei due

[11] Molto spesso la presentazione dei risultati della matematica riflette la loro storia in modo poco fedele. Anche questo è il caso: andando a rileggere la lettera originale di Fermat si scopre che Fermat non enunciò il teorema nella forma che gli abbiamo dato, che è quella diventata canonica ed usata dai matematici moderni: un enunciato valido per ogni intero $a$. Fermat, invece, si limitò ad enunciare il teorema solo nel caso in cui $p$ non divida $a$ (che è comunque l'unico caso non banale del teorema). Quindi quello che Fermat enunciò è proprio il teorema che abbiamo chiamato di Fermat-Eulero ristretto, nelle ipotesi, al caso in cui $m$ sia primo.

Questo non è un caso isolato: quasi mai succede, in matematica, che il 'Teorema di Tizio' sia davvero ciò che Tizio aveva detto. Ciò dipende, probabilmente, non da da incuria o sciatteria, ma proprio dalla natura della matematica: una disciplina in cui ciò che è stato scoperto una volta varrà per sempre, ma verrà anche rielaborato e riformulato senza sosta da chi lo guarda da prospettive sempre diverse.

[12] un'osservazione di carattere algebrico: qui è essenziale la proprietà associativa.

casi lo stesso risultato, chiamiamolo $Y$:

$$\prod_{i=1}^{\varphi(m)} X_i = Y = \prod_{i=1}^{\varphi(m)} (AX_i).$$

Raggruppando i fattori indicati come $A$ nel secondo prodotto otteniamo anche

$$Y = \prod_{i=1}^{\varphi(m)} (AX_i) = \left(\prod_{i=1}^{\varphi(m)} A\right) \cdot \left(\prod_{i=1}^{\varphi(m)} X_i\right) = A^{\varphi(m)} Y.$$

Dunque $[1]_m Y = Y = A^{\varphi(m)} Y$. Ricordando che $Y$ è invertibile (in quanto prodotto di invertibili) e quindi cancellabile, ne deduciamo $[1]_m = A^{\varphi(m)}$.

Abbiamo così verificato che la potenza $\varphi(m)$-esima di un qualsiasi elemento invertibile di $\mathbb{Z}_m$ è la classe $[1]_m$. Con questo siamo quasi alla conclusione. Sia infatti $a$ un intero coprimo con $m$ e poniamo $A = [a]_m$. Sappiamo che $A$ è invertibile (lo avevamo visto con il corollario nella prima parte di questa sezione), quindi $A^{\varphi(m)} = [1]_m$. Ma $A^{\varphi(m)} = ([a]_m)^{\varphi(m)} = [a^{\varphi(m)}]_m$, dunque $[a^{\varphi(m)}]_m = [1]_m$, ovvero

$$a^{\varphi(m)} \equiv_m 1,$$

che è precisamente ciò che volevamo provare. La dimostrazione del teorema di Fermat-Eulero è così completa.

## 6. Per approfondire...

La lettura di questo articolo può essere utilmente complementata da quella di un articolo di natura analoga: M.R. Celentani, *Aritmetica modulare: una proposta didattica*, Periodico di Matematiche, vol. 6 serie XI, anno CXXIV, pag. 19.

Chi ha trovato interessante la matematica discussa in questi articoli, può approfondire l'argomento consultando una fonte che ne fornisca una trattazione più sistematica, come ad esempio un testo universitario di algebra.

Uno dei motivi dell'inclusione del teorema di Fermat-Eulero in queste note è che questo teorema trova applicazione in crittografia: esso è infatti alla base del primo protocollo crittografico moderno (a chiave pubblica), il protocollo RSA. Si è preferito però evitare di trattare qui questo genere di applicazioni; presentazioni della crittografia, a qualsiasi livello, ce ne sono a bizzeffe. Una che, come questo articolo, è rivolta a studenti delle scuole superiori è in un mio articolo divulgativo (*Matematica e crittografia*) reperibile all'indirizzo http://www.dma.unina.it/~cutolo/didattica/varia/coinor-cutolo.pdf.