ARITMETICA MODULARE E ISBN

a cura di Lorenzo Mazza, Andrea Minotti
e Antonio Veredice

INTRODUZIONE

Si discute spesso sul cambiamento del ruolo della matematica da strumento per la gestione di procedure di calcolo a strumento per il controllo e il trattamento di informazioni; si veda, ad esempio, il capitolo «Codici, comunicazioni, computer. La teoria dell'informazione» di [4] in cui viene discussa la definizione matematica di informazione dovuta a Shannon [6]. Si tratta di un tema ampio che unisce aspetti anche molto distanti fra loro, della cultura e della società, a moderne e sofisticate tecniche matematiche. Tuttavia si può avere un'idea, seppur parziale e in scala ridotta, delle applicazioni di uno strumento matematico alla gestione e al controllo di informazioni, guardando all'aritmetica modulare. In quest'articolo mostriamo come l'idea di congruenza, introdotta da Gauss nell'Ottocento, sia quotidianamente sotto i nostri occhi, anche nella gestione di dati come nel caso del codice ISBN. Iniziamo con qualche breve richiamo sulle congruenze partendo da un esempio.

LE CONGRUENZE O L'ARITMETICA DELL'OROLOGIO

A differenza degli orologi digitali, l'orologio analogico è formato da soli 12 numeri naturali (da 1 a 12). Fintanto che è mattina, il valore numerico che leggiamo sull'orologio corrisponde all'ora effettiva. E così ci svegliamo alle 7.00, usciamo da casa alle 8.00, prendiamo un caffè al bar alle 10.00, ecc. Ma cosa accade dopo mezzogiorno? La lancetta delle ore ricomincia «da capo»: questo vuol dire che noi pranziamo alle 13.00 ma l'orologio indica il numero 1, andiamo a fare una corsa alle 18.00 quando però la lancetta delle ore è posizionata sul numero 6, ecc. Dunque il numero 18 e il numero 6, per un orologio con 12 ore, rappresentano lo stesso valore. In termini matematici, questo concetto si esprime dicendo che 18 è congruo a 6 modulo 12, e si scrive con $18 \equiv 6 \bmod 12$.

Quando parliamo delle ore 13.00 o delle 18.00 abbiamo in mente un orologio digitale con 24 ore. Anche in questo caso però c'è una congruenza: infatti negli orologi digitali dopo le ore 23.59 si riparte dalle 00.00. Ad esempio se sono passate 3 ore dopo le 23.00, non sono le 26 ma le 2.00, in quanto $26 \equiv 2 \bmod 24$.

Esistono diversi esempi di questo tipo: gli angoli contati con un goniometro (un angolo di 361° corrisponde ad un angolo di 1°), i giorni della settimana (oggi è lunedì, fra 7 giorni sarà nuovamente lunedì), i mesi dell'anno (anche questi congrui modulo 12 come accade per le ore).

In generale, due numeri interi a e b si dicono congrui modulo un numero naturale n (con $n > 1$) se hanno lo stesso resto nella divisione per n.

Si scriverà $a \equiv b \bmod n$ o, equivalentemente, $a \equiv_n b$ e si dice che a e b fanno parte della stessa *classe resto* modulo n. Ad esempio 13 e 1 appartengono alla stessa classe resto modulo 12.

Esiste anche un'altra definizione di congruenza fra numeri: due numeri interi a e b sono congrui modulo n se la loro differenza $a - b$ è un multiplo di n. Le due definizioni sono equivalenti, come mostrato di seguito:

Se a e b, divisi per n, danno lo stesso resto, allora esistono dei numeri interi h, k e r ($0 \le r < n$) tali che $a = h \cdot n + r$ e $b = k \cdot n + r$.
Quindi $a - b = h \cdot n + r - (k \cdot n + r) = (h - k) \cdot n$, il che equivale a dire che la differenza tra a e b è un multiplo di n.
Viceversa (usando la contronominale), se a e b, divisi per n, danno resti diversi, allora possiamo scrivere $a = h \cdot n + r_1$ e $b = k \cdot n + r_2$ con r_1 e r_2 tali che (senza perdere di generalità) $0 \le r_2 < r_1 < n$.
Pertanto $a - b = h \cdot n + r_1 - (k \cdot n + r_2) = (h - k) \cdot n + (r_1 - r_2)$. Ora, poiché per ipotesi $r_1 \neq r_2$, allora $0 < r_1 - r_2 < n$. Quindi, in particolare, $r_1 - r_2$ non è multiplo di n e ciò significa che nemmeno $a - b$ lo è.

Ad esempio 29 e 5 sono congrui modulo 12 in quanto hanno lo stesso resto nella divisione per 12 (e tale resto vale 5) o, equivalentemente, la loro differenza è un multiplo di 12 (in questo caso 24).

Come riportato in [2] la notazione di Gauss $a \equiv b \bmod n$ è particolarmente utile perché ha molte proprietà in comune con l'uguaglianza. Innanzitutto è una relazione di equivalenza (cioè è riflessiva, simmetrica e transitiva); inoltre è *compatibile* con le operazioni di somma e prodotto. Con ciò vogliamo dire che se $a \equiv b \bmod n$ e $a' \equiv b' \bmod n$ allora

$$a + a' \equiv b + b' \bmod n \quad \text{e} \quad a \cdot a' \equiv b \cdot b' \bmod n.$$

Queste proprietà ci consentono di ricavare i ben noti criteri di divisibilità. Ad esempio il criterio di divisibilità per 11 si ottiene considerando che $10^n \equiv 1 \bmod 11$ se n è pari mentre è congruo a $-1 \bmod 11$ se n è dispari. Quindi per vedere se un numero, prendiamo ad esempio 21879, è divisibile per 11, lo riscriviamo, usando la scrittura polinomiale in base 10 e le congruenze, come segue

$$21879 = 2 \times 10^4 + 1 \times 10^3 + 8 \times 10^2 + 7 \times 10^1 + 9 \times 10^0 \equiv 2 - 1 + 8 - 7 + 9 = \\ = 11 \equiv 0 \bmod 11$$

Ancora, grazie alle congruenze, si può rispondere a una domanda del tipo: «qual è l'ultima cifra del numero 2022^{2022}?». Dato che trovare l'ultima cifra è equivalente

a determinare il resto del numero nella divisione per 10, possiamo ragionare con le congruenze modulo 10. Sappiamo che $2022 \equiv 2 \bmod 10$ quindi $2022^{2022} \equiv 2^{2022} \bmod 10$. A questo punto, notando la ciclicità nelle potenze di due ($2, 2^2, 2^3, 2^4, 2^5 \equiv 2 \bmod 10$), si ottiene:

$$2022^{2022} \equiv 2^{2022} = 2^{4 \cdot 505 + 2} = 2^{4 \cdot 505 + 1} \cdot 2^1 \equiv 2 \cdot 2 = 4 \bmod 10$$

quindi 4 è l'ultima cifra cercata.

Per approfondimenti sulla definizione e le proprietà delle congruenze si vedano ad esempio [1], [2] e [3]. Nei prossimi paragrafi vedremo altre applicazioni delle congruenze in diversi contesti prendendo spunto da [1] e [5].

CONGRUENZE E CONTROLLO DEGLI ERRORI: LA PROVA DEL NOVE E LA PROVA DEL SETTE

Molte applicazioni delle congruenze sono legate all'esigenza di controllare gli errori. Se riflettiamo sulle nostre esperienze scolastiche, ricordiamo che spesso ci è capitato, soprattutto in matematica, di mettere in campo delle strategie di controllo dei nostri errori. Ne è un esempio la *prova del nove*, un metodo per verificare la correttezza delle operazioni numeriche; riportiamola brevemente rispolverando qualche ricordo della scuola primaria.

Supponiamo di dover calcolare una moltiplicazione come ad esempio 732×68. Il risultato è $732 \times 68 = 49776$. Per controllare l'esattezza del risultato, utilizzando la prova del nove, procediamo in questo modo:

- Sommiamo le cifre del primo numero: $7 + 3 + 2 = 12$ e facciamo lo stesso con il risultato ottenuto (reiterando le somme fino a ottenere un numero con una sola cifra) $1 + 2 = 3$.
- La stessa cosa viene fatta per 68 ($6 + 8 = 14$; $1 + 4 = 5$) e per 49776 ($4 + 9 + 7 + 7 + 6 = 33$; $3 + 3 = 6$).
- Si verifica quindi che la stessa operazione sia valida anche per i numeri così ottenuti ($3 \times 5 = 15$; $1 + 5 = 6$).

Quali informazioni ci dà questo tipo di verifica? Su quale principio si basa il suo funzionamento? Il nocciolo della questione sembra essere il passaggio da un numero (ad esempio 732) alla somma delle sue cifre ($7 + 3 + 2 = 12$), passaggio che può essere iterato ($1 + 2 = 3$).

Per spiegare questo passaggio, ripensiamo a quanto detto nel paragrafo precedente riguardo le congruenze e la scrittura di un numero in forma polinomiale in base 10.

Se scriviamo il numero 732 in forma polinomiale, otteniamo:

$$732 = 7 \times 10^2 + 3 \times 10 + 2$$

Dato che $10 \equiv 1 \bmod 9$, $10^2 = 10 \times 10 \equiv 1 \times 1 = 1 \bmod 9$, e in generale $10^n \equiv 1^n \bmod 9$, abbiamo che:

$$732 = 7 \times 10^2 + 3 \times 10 + 2 \equiv 7 \times 1 + 3 \times 1 + 2 = 7 + 3 + 2 \bmod 9$$

In altri termini ci rendiamo conto che 732 è congruo a $7 + 3 + 2 = 12$, che a sua volta è congruo a 3 modulo 9. Pertanto se $732 \times 68 = 49776$ allora, dato che la congruenza è compatibile con la moltiplicazione, si deve avere anche $3 \times 5 \equiv 6 \bmod 9$; se ciò non accade vuol dire che abbiamo commesso un errore in qualche calcolo.

A questo punto nasce spontanea la domanda: «se la prova conferma il risultato possiamo stare tranquilli? L'operazione è stata sicuramente eseguita in modo corretto?». Riprendiamo la moltiplicazione precedente $732 \times 68 = R$ dove R è il risultato; la domanda precedente corrisponde a chiedere: «dal fatto che R è congruo a $3 \times 5 \bmod 9$ possiamo concludere che R è il risultato giusto?». Basta qualche esempio per convincersi che non è così, il risultato corretto è uno solo, 49776, mentre ogni numero congruo a 6 modulo 9 soddisfa la prova del nove anche se non è il risultato giusto (ad esempio 49767 o 49785 che si ottengono sottraendo o aggiungendo 9 al risultato corretto). C'è da dire che gli errori non individuati dalla prova del nove corrispondono ai numeri congrui a 6 modulo 9 (cioè mediamente 1 su 9) e ciò la rende abbastanza affidabile.

Inoltre, una volta scoperto il principio matematico che sta dietro la prova del nove, possiamo chiederci: perché si usa proprio il 9? Non si potrebbe usare un altro qualsiasi numero n per passare dall'operazione di partenza (nell'esempio precedente $732 \times 68 = 49776$) all'operazione più semplice tra le classi resto modulo n? Ad esempio si potrebbe fare la prova del tre, calcolando le congruenze modulo 3. Nell'esempio precedente abbiamo $732 \equiv 0 \bmod 3$, $68 \equiv 2 \bmod 3$ e $49776 \equiv 0 \bmod 3$ e infatti risulta $0 \times 2 = 0$.

In effetti il meccanismo della prova del nove funziona con ogni altro numero n, però non è detto che calcolare la classe resto modulo n di ciascun numero coinvolto nell'operazione sia semplice: si tratta in generale di una divisione. Nel caso della prova del nove invece il calcolo è particolarmente facile perché, dato che le potenze di 10 sono congrue a 1 modulo 9, invece di svolgere la divisione, sommiamo le cifre di ciascun numero.

Tuttavia l'idea di usare una prova alternativa a quella del nove, che faccia uso di un altro numero per controllare ancora meglio gli errori di calcolo, non è peregrina, anzi ha degli illustri sostenitori. Nel 1494, nella *Summa de arithmetica, geometria, proportioni et proportionalitate*, Luca Pacioli scrisse:

> *La prova del 7 de più ci chiaresci che non quella del 9 sequita per questo la prova del 7 esser men rea di quella del 9 e per conseguente quella del 9 essere più rea. […] questa del 7 non si pò pigliare se non partendo* [dividendo]*: e non si piglia infilzando le figure* [sommando le cifre] *del numero sì como facemo per 9.*

In che senso la prova del sette risulta *men rea* di quella del nove? Probabilmente Pacioli intende dire che la prova del sette ci dà la possibilità di individuare più errori di calcolo notando però, al contempo, che per lavorare con le congruenze modulo 7 bisogna necessariamente calcolare le divisioni («partire») mentre per calcolare le congruenze modulo 9 basta sommare («infilzare») le cifre. Torniamo all'esempio precedente: il prodotto tra 732 e 68. Calcoliamolo in colonna come si fa alla scuola primaria

$$\begin{array}{r} 732\ \times \\ 68\ = \\ \hline \end{array}$$

simuliamo ora un tipico errore di incolonnamento

$$\begin{array}{r} 732\ \times \\ 68\ = \\ \hline 5856\ + \\ 4392\ = \\ \hline 10248 \end{array}$$

nell'operazione precedente abbiamo commesso l'errore di incolonnare il numero 4392 senza lasciare lo spazio a destra, la prova del nove individuerà questo errore? Vediamo:

$$732 \equiv 3 \bmod 9 \qquad 68 \equiv 5 \bmod 9 \qquad 10248 \equiv 6 \bmod 9;$$
$$3 \times 5 = 15 \equiv 6 \bmod 9$$

La prova è riuscita ma il risultato è sbagliato, quindi la prova del nove non ha individuato l'errore di incolonnamento. Del resto potevamo prevederlo dato che:

$$732 \times 68 = 732 \times (60 + 8) = 732 \times 60 + 732 \times 8$$

a questo punto, dato che $60 \equiv 6 \bmod 9$, nell'espressione precedente possiamo sostituire a 60 il numero 6 e avremo lo stesso risultato modulo 9; tale sostituzione corrisponde all'errore di incolonnamento:

$$732 \times 60 + 732 \times 8 \equiv 732 \times 6 + 732 \times 8 = 5856 + 4392 = 10248$$

E con la prova del sette cosa sarebbe accaduto? Prima di esaminare il funzionamento della prova del sette ragioniamo sul valore delle potenze di 10 modulo 7. Abbiamo $10^0 \equiv 1 \bmod 7$, $10^1 \equiv 3 \bmod 7$, $10^2 = 10 \times 10 \equiv 3 \times 3 = 9 \equiv 2 \bmod 7$, $10^3 = 10^2 \times 10 \equiv 2 \times 3 = 6 \equiv -1 \bmod 7$, $10^4 \equiv -3 \bmod 7$, $10^5 \equiv -2 \bmod 7$, $10^6 \equiv 1 \bmod 7$, e così via. Una volta note le potenze di 10 modulo 7 possiamo riscrivere i nume-

ri coinvolti nelle operazioni in forma polinomiale e poi passare alle congruenze modulo 7:

$$732 = 7 \times 10^2 + 3 \times 10^1 + 2 \times 10^0 \equiv 0 + 3 \times 3 + 2 = 11 \equiv 4 \bmod 7$$
$$68 \equiv 5 \bmod 7$$
$$10248 = 1 \times 10^4 + 0 \times 10^3 + 2 \times 10^2 + 4 \times 10^1 + 8 \times 10^0 \equiv$$
$$\equiv -3 + 0 + 2 \times 2 + 4 \times 3 + 8 = 21 \equiv 0 \bmod 7$$

Notiamo che in questo caso la prova dà:

$4 \times 5 = 20 \not\equiv 0 \bmod 7$ quindi l'errore è stato individuato. Per ulteriori approfondimenti sulla prova del sette si veda [9].

In ogni caso anche la prova del sette non individua alcuni errori, ad esempio tutti i numeri congrui modulo 7 al risultato giusto saranno comunque considerati corretti secondo tale prova. Ciò si esprime dicendo che la prova del nove e la prova del sette rappresentano condizioni necessarie ma non sufficienti per la correttezza delle operazioni. Come vedremo nel prossimo paragrafo, anche i criteri di controllo dei codici associati ad alcuni tipi di informazioni si basano su condizioni necessarie ma non sufficienti che sfruttano le congruenze.

IL CODICE ISBN

Spesso le informazioni vengono associate a codici (numerici o alfanumerici) e, ogni volta che questi codici vengono comunicati, emerge naturalmente l'esigenza di verificare che la stringa ricevuta sia corretta. Prendiamo in considerazione ora un codice che abbiamo quotidianamente sotto gli occhi.

Molti lettori avranno notato che nel retro della copertina di ogni pubblicazione (anche nella rivista che avete fra le mani in questo momento) c'è un codice a barre e, sotto di esso, una sequenza di 13 cifre. Quest'ultima si chiama codice ISBN. Di cosa si tratta? Viene abbastanza spontaneo pensare che si tratti di un numero che, in qualche modo, *identifica* il libro in questione. In effetti è proprio così: l'acronimo sta per International Standard Book Number, si tratta di un «numero che identifica, a livello internazionale in modo univoco e duraturo, un titolo o una edizione di un titolo di un determinato editore» ([7]) ([1]).

([1]) Il codice ISBN, approvato (nella sua versione a 10 cifre) nel 1970 dall'ISO (International Organization for Standardization) e portato a 13 cifre nel 2007, presenta diversi vantaggi, *in primis* per il venditore, il quale può evadere in maniera più efficace gli ordini e gestire meglio le rese librarie, oltre al fatto che una piccola serie di numeri racchiude un gran numero di informazioni. Il codice ISBN è collegato anche ad un codice a barre per la lettura ottica, in modo da velocizzare tutte le fasi legate alla commercializzazione del prodotto [8].

Come si evince dalla figura precedente, le prime 12 cifre dell'ISBN contengono informazioni sul prodotto ([2]).

Perché usare un codice numerico per identificare un libro? Non bastano il titolo, l'autore ed eventualmente la casa editrice? Se ci pensiamo bene, l'uso di una sequenza numerica crea meno ambiguità e fraintendimenti, non c'è il rischio di confondere due titoli o due edizioni diverse dello stesso testo.

Ma guardando la figura precedente c'è un altro aspetto che non abbiamo ancora considerato: l'ultima cifra a cosa serve? In effetti essa non contiene alcuna informazione sul prodotto; dalla figura si evince che tale cifra rappresenta un *numero di controllo*. Cosa significa? Cosa c'è da controllare?

Pensiamo a come viene utilizzato tale codice quotidianamente, probabilmente ci sarà anche capitato di dover comunicare un codice ISBN, magari di un libro di testo che dobbiamo ordinare in libreria. In quei casi il codice viene dettato, eventualmente al telefono, poi riscritto e, in questi passaggi, è possibile commettere degli errori.

Così emerge la necessità di attuare dei meccanismi di controllo analoghi alle *prove* del paragrafo precedente. La cifra di controllo serve a verificare la validità del codice. Facendo una breve ricerca sul funzionamento del codice ISBN, si scopre che la cifra di controllo viene determinata nel modo seguente: si sommano le prime 12 cifre del codice, moltiplicando le cifre di posto pari per 3, e si ottiene un numero N; la cifra di controllo è il numero che manca ad N per arrivare al successivo multiplo di 10 che chiameremo N'. In altri termini, siano $d_1, d_2, \ldots, d_{13}$ le 13 cifre del codice ISBN, se il codice è corretto allora il numero:

$$N' = N + d_{13} = d_1 + 3 \times d_2 + d_3 + 3 \times d_4 + d_5 + 3 \times d_6 + d_7 + 3 \times d_8 + d_9 + 3 \times d_{10} + d_{11} + 3 \times d_{12} + d_{13}$$

([2]) Le prime tre cifre (978 o 979) indicano che si è in presenza di un libro. Si tratta di cifre standard, presenti in tutti i codici ISBN di tutti i testi del mondo. Le cifre successive (da un minimo di 1 a un massimo di 5) rappresentano il prefisso dell'area linguistica. Per i testi in italiano, tale valore è generalmente pari a 88 (nel caso in cui le tre cifre iniziali siano 978; diversamente se le prime tre cifre sono 979, il prefisso linguistico sarà 12). Il valore più basso è per la lingua inglese, il cui codice linguistico è 0 oppure 1. Il più alto è per i testi del Benin, il cui codice linguistico è 99982. Le cifre successive indicano la casa editrice o il marchio editoriale, e possono andare da un minimo di 2 a un massimo di 7 cifre. In particolare ad un editore con un'ampia produzione di testi viene associato un valore basso (in modo da avere a disposizione più cifre nel gruppo successivo); viceversa ad editori con una minor produzione viene associato un prefisso più lungo. Il gruppo di cifre successive è l'identificativo del titolo, e può andare da una a sei cifre, rispettando il criterio che il numero di cifre totali fin qui considerato sia pari a 12 (ad esse si aggiungerà l'ultima cifra, il cosiddetto codice di controllo).

deve essere multiplo di 10. Questa affermazione può essere riformulata in termini di congruenze, dicendo che la precedente somma deve essere congrua a zero modulo 10. A titolo di esempio verifichiamo il codice ISBN riportato nella figura precedente utilizzando le proprietà delle congruenze per semplificare il calcolo:

$$9 + 3 \times 7 + 8 + 3 \times 8 + 8 + 3 \times 8 + 9 + 3 \times 6 + 3 + 3 \times 7 + 1 + 3 \times 5 + 9 \equiv$$
$$\equiv 9 + 1 + 8 + 4 + 8 + 4 + 9 + 8 + 3 + 1 + 1 + 5 + 9 \equiv 0 \bmod 10$$

Quindi se qualcuno ci detta un codice ISBN possiamo verificare che la somma N' è un multiplo di 10; se così non fosse allora il codice ISBN che abbiamo sarebbe sbagliato.

A questo punto, una volta capito il funzionamento e dopo averlo verificato su qualche libro che abbiamo sottomano, nasce la curiosità di capire perché la cifra di controllo funziona proprio così, di sperimentare con i codici, chiedersi se potrebbe funzionare diversamente, ipotizzare, inventare nuovi meccanismi di controllo.

Ad esempio potremmo chiederci perché si usa proprio la congruenza modulo 10. Si può intuire che il motivo sia legato al fatto che la scrittura dei numeri che usiamo solitamente è in base 10. Infatti, qualunque sia il numero N precedentemente calcolato, che dipende come abbiamo visto dalle prime 12 cifre dell'ISBN, esisterà sempre una cifra, cioè un numero tra 0 e 9, che sommato a N darà come risultato un multiplo di 10; tale numero sarà la cifra di controllo.

Un'altra possibile domanda riguarda proprio il calcolo del numero N a partire dalle prime 12 cifre dell'ISBN. Perché N si calcola proprio in quel modo, moltiplicando le cifre di posto pari per 3? In questo caso possono aiutarci le considerazioni precedenti sull'esigenza di un controllo per il codice ISBN. Un possibile errore nella trascrizione di un codice numerico potrebbe essere lo scambio di due numeri consecutivi. Come abbiamo visto nel caso della prova del nove, se sommassimo semplicemente le cifre, non riusciremmo a distinguere le prime 12 cifre del seguente codice ISBN (in cui l'ultima cifra X è ignota):

$$979128006800X$$

dalle prime 12 cifre del codice:

$$979128008600X$$

in quanto la somma delle prime 12 cifre sarebbe comunque:

$$9 + 7 + 9 + 1 + 2 + 8 + 0 + 0 + 6 + 8 + 0 + 0 =$$
$$= 9 + 7 + 9 + 1 + 2 + 8 + 0 + 0 + 8 + 6 + 0 + 0 = 50$$

e quindi dovremmo concludere in entrambi i codici che la cifra di controllo è $X = 0$ (infatti 50 è già multiplo di 10) ma tale cifra non ci permette di individuare il codice corretto.

Invece, moltiplicando le cifre di posto pari per 3 otteniamo nel primo caso:

$$9 + 7 \times 3 + 9 + 1 \times 3 + 2 + 8 \times 3 + 0 + 0 \times 3 + 6 + 8 \times 3 + 0 + 0 \times 3 = 98$$

e nel secondo:

$$9 + 7 \times 3 + 9 + 1 \times 3 + 2 + 8 \times 3 + 0 + 0 \times 3 + 8 + 6 \times 3 + 0 + 0 \times 3 = 94$$

Questa volta le cifre di controllo sono diverse ($X = 2$ nel primo caso e $X = 6$ nel secondo) quindi conoscendo la cifra di controllo possiamo individuare il codice errato.

Ciò significa che questo modo di calcolare il numero N ci permette di individuare ogni tipo di errore? Purtroppo la risposta è negativa: se invece di scambiare due cifre consecutive scambiamo due cifre che sono separate da un'altra cifra, ci rendiamo conto che l'errore non viene riscontrato. Se ad esempio prendiamo il codice ISBN 9788809041165 e scambiamo la settima cifra con la nona otteniamo il codice 9788804091165. Proviamo ora a verificare la correttezza dei due codici con la regola del codice ISBN. Otteniamo in entrambi i casi:

$$9 + 7 \times 3 + 8 + 8 \times 3 + 8 + 0 \times 3 + 9 + 0 \times 3 + 4 + 1 \times 3 + 1 + 6 \times 3 + 5 = 110$$

$$9 + 7 \times 3 + 8 + 8 \times 3 + 8 + 0 \times 3 + 4 + 0 \times 3 + 9 + 1 \times 3 + 1 + 6 \times 3 + 5 = 110$$

quindi entrambi i codici ci sembrano corretti mentre noi sappiamo che il secondo è stato ottenuto commettendo un errore sul primo. Ciò è un esempio del fatto che il criterio utilizzato per il calcolo dell'ISBN distingue le cifre di posto pari da quelle di posto dispari, ma non distingue le cifre di posto dispari fra loro né quelle di posto pari fra loro.

Quindi, come nel caso delle prove del sette e del nove abbiamo solo una condizione necessaria per la correttezza del codice ma non sufficiente. In ogni caso, l'idea di moltiplicare le cifre di posto pari per 3 risulta efficace per prevenire un certo tipo di errori.

A questo punto è naturale chiedersi perché come fattore per cui moltiplicare sia stato scelto proprio il 3. Non potremmo scegliere ad esempio 4, 5 o 6? Cerchiamo di capire che differenza c'è tra la scelta di 3 e, ad esempio, di 6 come numero per cui moltiplicare le cifre di posto pari nel codice ISBN. Per farlo proviamo a moltiplicare tutte le cifre per 3 e poi anche per 6 e confrontiamo i risultati modulo 10 (le congruenze seguenti sono tutte modulo 10 anche se non è scritto esplicitamente):

$0 \times 3 \equiv 0; 1 \times 3 \equiv 3; 2 \times 3 \equiv 6; 3 \times 3 \equiv 9; 4 \times 3 \equiv 2; 5 \times 3 \equiv 5; 6 \times 3 \equiv 8; 7 \times 3 \equiv 1;$
$8 \times 3 \equiv 4; 9 \times 3 \equiv 7$

$0 \times 6 \equiv 0; 1 \times 6 \equiv 6; 2 \times 6 \equiv 2; 3 \times 6 \equiv 8; 4 \times 6 \equiv 4; 5 \times 6 \equiv 0; 6 \times 6 \equiv 6; 7 \times 6 \equiv 2;$
$8 \times 6 \equiv 8; 9 \times 6 \equiv 4$

Se confrontiamo le due sequenze precedenti ci rendiamo conto che, moltiplicando le cifre per 3, otteniamo tutte le cifre modulo 10, mentre moltiplicando ogni cifra per 6 otteniamo solo le cifre 0, 6, 2, 8, 4 cioè le cifre pari.

Quindi moltiplicando per 6 abbiamo ottenuto, a partire da cifre qualsiasi, solo cifre pari. Di conseguenza due cifre diverse, se moltiplicate per 6, possono coincidere modulo 10 e ciò riduce la capacità di individuare errori (ad esempio la confusione tra la cifra 2 e la cifra 7 in un posto pari di un codice siffatto non verrebbe rilevata).

Ancora più eclatante è il caso in cui le cifre di posto pari siano moltiplicate per 5. In questo caso i risultati della moltiplicazione sarebbero solo 0 e 5 modulo 10.

Perché accade ciò con 6 e con 5 e non accade con 3? Indaghiamo meglio la questione ponendoci le seguenti domande:

1. da $a \times 3 \equiv b \times 3 \bmod 10$ possiamo concludere $a \equiv b \bmod 10$?
2. da $a \times 6 \equiv b \times 6 \bmod 10$ possiamo concludere $a \equiv b \bmod 10$?

Nella prima domanda, in base alla definizione di congruenza che abbiamo dato, $a \times 3 \equiv b \times 3 \bmod 10$ equivale a dire che $3(a - b) = 10 \cdot n$ per qualche numero intero n. Perché $3(a - b)$ sia un multiplo di 10, deve avere come fattori 2 e 5; dato che 3 non ha come fattori né 2 né 5, ciò significa che $(a - b)$ deve avere come fattori 2 e 5 ovvero che $(a - b)$ è un multiplo di 10 che equivale a dire $a \equiv b \bmod 10$. Quindi la risposta alla prima domanda è affermativa; per questo motivo, moltiplicando per 3 le cifre da 0 a 9 si ottengono tutte cifre distinte modulo 10.

Il ragionamento precedente non può essere ripetuto in maniera identica per la seconda domanda. Infatti $a \times 6 \equiv b \times 6 \bmod 10$ equivale a dire che $6(a - b) = 10 \cdot n$ per qualche numero intero n. Perché $6(a - b)$ sia un multiplo di 10, deve avere come fattori 2 e 5; però, in questo caso, 6 ha come fattore 2, quindi basta che $(a - b)$ abbia come fattore 5 ovvero che $(a - b)$ sia un multiplo di 5, che equivale a dire $a \equiv b \bmod 5$. Quindi la risposta alla seconda domanda è negativa; infatti, moltiplicando per 6 le cifre da 0 a 9, si ottengono valori congrui modulo 10 quando le cifre di partenza sono congrue modulo 5: per esempio da 2 e da 7 (che sono congrui modulo 5) si ottiene $2 \times 6 \equiv 2 \equiv 7 \times 6 \bmod 10$ anche se 2 e 7 non sono congrui modulo 10. Pertanto la scelta del 3 è riconducibile al fatto che 10 e 3 sono primi fra loro mentre 10 e 6 e 10 e 5 hanno dei fattori comuni, rispettivamente 2 e 5.

Questa esplorazione delle relazioni tra congruenze e rapporto di primalità fra numeri ci ha aiutato ad approfondire il ruolo del 3 nel moltiplicare le cifre di posto pari del codice ISBN. Possiamo chiederci se la scelta del numero 3 per assolvere a tale ruolo sia l'unica possibile. I ragionamenti appena fatti dovrebbero guidarci nel rispondere che ogni altro numero primo con 10 può svolgere il ruolo del 3 in modo analogo. Probabilmente la scelta del 3 è dovuta al fatto che si tratta del più piccolo numero primo con 10.

Per concludere, dopo aver riflettuto sui perché legati all'ISBN e alla cifra di controllo, possiamo lavorare concretamente (giocare?) con i codici ISBN in modo da far nascere in maniera spontanea altre riflessioni. Presentiamo alcune attività che possono essere svolte in quest'ottica:

Attività 1. Si considerano alcuni codici ISBN, se ne cancella una cifra come negli esempi seguenti:
978880816204... 97888477...2810 97888045989...7
E si chiede di ricostruire la cifra mancante utilizzando l'aritmetica modulare.

Attività 2. Supponiamo di avere un codice ISBN scritto frettolosamente da qualcuno su un foglietto, nel foglietto i 7 si confondono con gli 1, il codice che riusciamo a leggere è 3908730681238. È possibile risolvere l'ambiguità di scrittura?

Attività 3. Discutere in gruppo su come «progettare» un altro tipo di codice che riesca ad individuare anche altri errori di trascrizione che il codice ISBN non individua.

Mentre nelle attività 1 e 2, in cui si richiede di individuare delle cifre o risolvere una ambiguità di scrittura, esiste la «soluzione giusta», ciò non è vero per l'attività 3. Quest'ultima si configura come un'attività aperta di riflessione e confronto in gruppo, che possa condurre a ipotesi di codici migliorativi rispetto all'ISBN con la consapevolezza che non si potrà mai pervenire alla progettazione di un codice «perfetto» che prevenga ogni tipo di errore.

Lorenzo Mazza
lorenzo.mazza@uniroma1.it

Andrea Minotti
andrea.minotti@liceoplinio.edu.it

Antonio Veredice
antonio.veredice@uniroma1.it

Bibliografia

[1] Salvatore Damantino, Emanuele Campeotto, *Aritmetica modulare – Teorie e applicazioni* (UMath), Scienza express, 2020.
[2] Richard Courant, Herbert Robbins, *Che cos'è la matematica?*, Bollati Boringhieri, 1971.
[3] Giulia M. Piacentini Cattaneo, *Algebra. Un approccio algoritmico*, Zanichelli, 1996.
[4] Ian Stewart, *Le 17 equazioni che hanno cambiato il mondo,* Einaudi, 2017.
[5] Edward B. Burger, Michael Starbird, *The Heart of Mathematics: An Invitation to Effective Thinking,* John Wiley & Sons Inc, 2012.
[6] C.E. Shannon, *A mathematical theory of communication*, in «The Bell System Technical Journal», vol. 27, no. 3, pp. 379-423, July 1948.

Sitografia

[7] https://www.isbn.it.
[8] https://it.wikipedia.org/wiki/ISBN.
[9] http://www.vdepetris.it/t06/Text06.htm.