I CRITERI DI DIVISIBILITÀ: MAGIE DELLA ARITMETICA MODULARE

SILVANA RINAURO

Si vuole risolvere il seguente problema: se oggi è mercoledì, quale giorno della settimana sarà fra 100 giorni? Per rispondere a questa domanda basta notare che il resto della divisione di 100 per 7 è 2, e quindi fra 100 giorni sarà un venerdì (il giorno della settimana che cade 2 giorni dopo il mercoledì). Infatti $100 = 14 \cdot 7 + 2$, quindi fra 100 giorni saranno trascorse 14 settimane intere più 2 giorni. Un problema che può essere affrontato con la stessa tecnica è il seguente: su un circuito lungo 300 metri si deve svolgere una gara ciclistica di 10 km. A quale distanza dal punto di partenza deve essere posto il traguardo? I ciclisti devono percorrere 10.000 metri, e poichè il resto della divisione di 10.000 per 300 è 100, il traguardo deve essere posto 100 metri dopo al partenza. Infatti $10.000 = 33 \cdot 300 + 100$, quindi ciascun ciclista deve percorrere 33 giri più 100 metri.

Per risolvere questo tipo di problemi si può utilizzare l'aritmetica modulare, cioè l'aritmetica nella quale ciascun numero intero può essere sostituito col proprio resto nella divisione per un fissato intero positivo n.

Si consideri l'insieme $\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$ dei numeri interi e si fissi un numero intero positivo n. Si dirà che due numeri interi x e y *sono congrui modulo* n, e si scriverà $x \equiv_n y$ se $x - y$ è divisibile per n. Quindi:

$x \equiv_n y$ se e solo se esiste un numero intero a tale che $x - y = an$.

Esempi.

Se $n = 2$, dire che $x \equiv_2 y$ equivale a dire che $x - y$ è divisibile per 2, cioè è pari, il che accade esattamente quando x e y sono entrambi pari

o entrambi dispari. Dunque $12345 \equiv_2 789$, perché entrambi dispari, ma $234 \not\equiv_2 123$, perché il primo è pari e il secondo è dispari.

Se $n = 10$, dire che $x \equiv_{10} y$ equivale a dire che $x - y$ è divisibile per 10, cioè ha 0 come cifra delle unità. Pertanto $x \equiv_{10} y$ se e solo se x e y hanno la stessa cifra delle unità. Dunque $43267 \equiv_{10} 569307$, ma $763409 \not\equiv_{10} 26473$.

Dimostriamo ora che la relazione $\equiv_n$ è una relazione di equivalenza.

Proposizione 1. *Sia n un numero intero positivo. Allora la relazione $\equiv_n$ è una relazione di equivalenza su $\mathbb{Z}$.*

Dim. Si vuole dimostrare che la relazione $\equiv_n$ è riflessiva, simmetrica e transitiva.
Riflessiva: *Si vuole dimostrare che se x è un numero intero, allora $x \equiv_n x$.*
Per ogni numero intero x, $x - x = 0$ è un multiplo di n e quindi $x \equiv_n x$.
Simmetrica: *Si vuole dimostrare che se x e y sono numeri interi e se $x \equiv_n y$, allora $y \equiv_n x$.*
Si supponga $x \equiv_n y$. Allora esiste un numero intero a tale che $x - y = an$. Dunque $y - x = -(x - y) = (-a)n$ e $y \equiv_n x$.
Transitiva: *Si vuole dimostrare che se x, y e z sono numeri interi e se $x \equiv_n y$ e $y \equiv_n z$, allora $x \equiv_n z$.*
Si supponga $x \equiv_n y$ e $y \equiv_n z$. Dunque esistono due numeri interi a e b tali che $x - y = an$ e $y - z = bn$. Quindi $x - z = (x - y) + (y - z) = an + bn = (a + b)n$. Pertanto $x \equiv_n y$. □

Essendo $\equiv_n$ una relazione di equivalenza su $\mathbb{Z}$, si può considerare l'insieme $\mathbb{Z}_n$ delle classi di equivalenza degli elementi di $\mathbb{Z}$, definite come segue: per ogni numero intero x, la classe di equivalenza di x (modulo n) è denotata

con $[x]_n$, o più semplicemente con $\bar{x}$[1], ed è l'insieme degli interi congrui a x modulo n. Si osservi che $y \equiv_n x$ se e solo se esiste un numero intero a tale che $y - x = an$, o, equivalentemente, $y = x + an$. Quindi l'insieme degli interi congrui a x modulo n è

$$\bar{x} \stackrel{def}{=} [x]_n \stackrel{def}{=} \{\, x + an \,:\, a \in \mathbb{Z} \,\}.$$

Dalla definizione di classe di equivalenza si ha che ogni intero x appartiene ad una ed una sola classe di equivalenza. Inoltre dati due interi x e y,

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv_n y \Leftrightarrow x - y \text{ è un multiplo di } n.$$

Si noti che $\bar{0}$ è l'insieme dei numeri interi divisibili per n.

$\mathbb{Z}_n$ è detto l'insieme degli interi modulo n. In virtù del Lemma di divisione euclideo, che qui enunciamo senza dimostrazione, si vedrà con la Proposizione 2 che nella classe di x c'è il resto della divisione di x per n e che le classi modulo n, ovvero gli elementi di $\mathbb{Z}_n$ sono esattamente le classi degli n possibili resti della divisione per n, cioè le classi $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$, che sono a due a due distinte.

Lemma 1 (Lemma di divisione euclidea). *Dati un intero x e un intero positivo n, esistono e sono unici due interi q ed r tali che $x = qn + r$ e $0 \leq r < n$.*

Gli interi q ed r dell'enunciato sono detti rispettivamente il *quoziente* ed il *resto* della divisione di x per n. Diremo anche che *r è il resto di x modulo n*.

[1] Bisogna fare attenzione all'uso della notazione $\bar{x}$, che è qui preferita alla meno semplice $[x]_n$, in quanto $\bar{x}$ denota insiemi diversi a seconda di quale sia il modulo n. Ad esempio, come si vedrà più avanti, $\bar{0}$ modulo 2 è l'insieme dei multipli di 2, mentre $\bar{0}$ modulo 3 è l'insieme dei multipli di 3.

Proposizione 2. *Sia n un numero intero positivo e sia x un intero.*

Allora nella classe di x modulo n c'è uno e un solo intero r tale che $0 \leq r < n$: r è il resto di x modulo n. Pertanto $\mathbb{Z}_n$ ha esattamente n elementi: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$.

Dim. Per il Lemma di divisione euclidea, esistono q ed r interi tali che $x = qn + r$ e $0 \leq r < n$. Quindi $x - r = qn$ è un multiplo di n e dunque r appartiene alla classe di x modulo n. Per dimostrare l'unicità di r, sia r' un altro intero tale che r' appartiene alla classe di x modulo n e $0 \leq r' < n$. Allora $x \equiv_n r'$ e quindi esiste un intero a tale che $x = an + r'$. Per l'unicità del quoziente e del resto nella divisione euclidea si ottiene $r' = r$. □

Esempi. Le classi di equivalenza modulo 2, cioé gli elementi di $\mathbb{Z}_2$, sono $\bar{0}$ e $\bar{1}$. La classe $\bar{0}$ è l'insieme dei multipli di 2, quindi l'insieme dei numeri pari, mentre $\bar{1} = \{\, 1 + 2a \,:\, a \in \mathbb{Z} \,\}$ è l'insieme dei numeri dispari.

Le classi di equivalenza modulo 3, cioé gli elementi di $\mathbb{Z}_3$, sono $\bar{0}$, $\bar{1}$ e $\bar{2}$. La classe $\bar{0}$ è l'insieme dei multipli di 3, la classe $\bar{1}$ è l'insieme degli interi che hanno resto uguale ad 1 modulo 3 e la classe $\bar{2}$ è l'insieme degli interi che hanno resto uguale a 2 modulo 3. Quindi 51 appartiene a $\bar{0}$, perché è un multiplo di 3, mentre 65 appartiene a $\bar{2}$, perché il suo resto modulo 3 è 2.

La relazione $\equiv_n$, come è già anticipato dal suo nome, è una *congruenza*, cioè è compatibile con le operazioni di somma e prodotto, nel senso seguente:

Proposizione 3. *Sia n un intero positivo e siano x, x', y, y' interi.*
(1) Se $x \equiv_n x'$ e $y \equiv_n y'$, allora $x + y \equiv_n x' + y'$.
(2) Se $x \equiv_n x'$ e $y \equiv_n y'$, allora $x \cdot y \equiv_n x' \cdot y'$.

Dim. Si supponga $x \equiv_n x'$ e $y \equiv_n y'$. Allora esistono due interi a e b tali che $x' = x + an$ e $y' = y + bn$.
(1) Si ha $x' + y' = (x + an) + (y + bn) = (x + y) + (a + b)n$ e quindi $x + y \equiv_n x' + y'$.
(2) Si ha $x' \cdot y' = (x + an) \cdot (y + bn) = (x \cdot y) + (xb + ay + abn)n$ e quindi $x \cdot y \equiv_n x' \cdot y'$. □

La Proposizione 3 permette di definire, senza ambiguità, la somma e il prodotto fra classi nel modo seguente. Dati due interi x ed y, si definiscono:

$$\bar{x} + \bar{y} \stackrel{def}{=} \overline{x + y}, \quad \bar{x} \cdot \bar{y} \stackrel{def}{=} \overline{x \cdot y}.$$

La Proposizione 3 assicura che se $\overline{x'} = \overline{x}$ e $\overline{y'} = \overline{y}$, allora $\overline{x + y} = \overline{x' + y'}$ e $\overline{x \cdot y} = \overline{x' \cdot y'}$, quindi per sommare, o per moltiplicare, due classi basta scegliere un elemento in ciascuna classe e sommarli, o moltiplicarli. Ecco che se si vogliono eseguire operazioni su numeri ma quello che interessa non è il risultato, ma il suo resto modulo n, si riesce a semplificare molto i calcoli. Perché dalla Proposizione 3 segue che in ogni passaggio possiamo sostituire a ciascun numero x il suo resto modulo n, o un qualunque altro numero x' congruo ad x modulo n.

Torniamo al primo problema enunciato all'inizio di questo articolo: se oggi è mercoledì, fra 100 giorni quale giorno della settimana sarà? Si può affrontare questo problema direttamente con l'aritmetica modulare: I giorni della settimana sono 7 quindi si considera n=7. L'insieme dei giorni della settimana può essere rappresentato dall'insieme $\mathbb{Z}_7$, dove $\bar{1}$ = lunedì, $\bar{2}$ = martedì, $\ldots, \bar{6}$ = sabato e $\bar{7} = \bar{0}$ = domenica. Il problema si risolve calcolando semplicemente $\bar{3} + \overline{100} = \overline{103} = \bar{5}$ =venerdì. Oppure si possono fare i calcoli sostituendo prima a 100 il suo resto modulo 7, e poi facendo

la somma. Quindi: $\bar{3} + \overline{100} = \bar{3} + \bar{2} = \bar{5}$ =venerdì. E' un esempio semplice, ma si capisce che con lo stesso metodo si riescono a risolvere problemi molto più complicati con calcoli semplici.

Criteri di divisibilità

L'aritmetica modulare è alla base dei criteri di divisibilità che si studiano sin dalle elementari. Per spiegare tali criteri, ricordiamo che se a è un numero intero positivo, scrivere $a = a_m a_{m-1} a_{m-2} \dots a_2 a_1 a_0$, dove ciascun a_i è un numero intero compreso fra 0 e 9 e a_0 è la cifra delle unità di a, a_1 è la cifra delle decine di a, a_2 è la cifra delle centinaia di a, e così via, significa che

$$(*) \quad a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_{m-2} \cdot 10^{m-2} + a_{m-1} \cdot 10^{m-1} + a_m \cdot 10^m.$$

Inoltre se b è il numero ottenuto cancellando la cifra delle unità di a e c è la cifra delle unità di a (cioè $c = a_0$), si può scrivere

$$(**) \quad a = b \cdot 10 + c.$$

L'idea che è alla base dei criteri di divisibilità è quella di calcolare il resto di a modulo n usando il secondo membro della $(*)$, o della $(**)$, e ciò funziona quando, modulo n, $\overline{10}$ è uno fra $\bar{0}$, o $\bar{1}$, o $\overline{-1}$, cosicché anche le potenze di $\overline{10}$ sono rispettivamente $\bar{0}$, o $\bar{1}$, o $\overline{\pm 1}$.

Un numero intero positivo a è divisibile per 2 se e solo se la sua cifra delle unità è uno dei numeri $0, 2, 4, 6, 8$. In altri termini a è pari se e solo se la sua cifra delle unità è pari.

Infatti, usando la $(**)$, si ha che $a = b \cdot 10 + c \equiv_2 c$. Quindi a è pari se e solo se c (la cifra delle unità di a) è pari.

Un numero intero positivo a è divisibile per 5 se e solo se la sua cifra delle unità è 0 o 5. Infatti, come nel caso precedente $a = b \cdot 10 + c \equiv_5 c$. Quindi a è divisibile per 5 se e solo se c (la cifra delle unità di a) è divisibile per 5, cioè se e solo se c è 0 o 5. Inoltre il resto di a modulo 5 è uguale al resto di c modulo 5.

Ad esempio il resto di 6729305128 modulo 5 è uguale al resto di 8 modulo 5, quindi è 3.

Un numero intero positivo a è divisibile per 3 se e solo se la somma delle sue cifre è divisibile per 3. Poiché $10 \equiv_3 1$, si ha che $10^k \equiv_3 1^k = 1$, per ogni numero intero positivo k. Quindi il criterio è vero in quanto $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_{m-2} \cdot 10^{m-2} + a_{m-1} \cdot 10^{m-1} + a_m \cdot 10^m \equiv_3 a_0 + a_1 + a_2 + \cdots + a_{m-2} + a_{m-1} + a_m$.

Inoltre per calcolare il resto di a modulo 3 si sommano le cifre di a (e ad ognuna di queste si può sostituire il suo resto modulo 3) e si calcola il resto del numero a' così ottenuto. Ovviamente si può ripetere il procedimento sommando le cifre di a', e continuare così fino ad ottenere un numero di 1 cifra, per il quale calcolare il resto è facile.

Ad esempio, si vede subito che 425334 è un numero divisibile per 3 in quanto la somma delle cifre può essere calcolata come

$$a' = (4 + 2) + (5 + 4) + 3 + 3 = 6 + 9 + 3 + 3,$$

che è un multiplo di 3. Per calcolare il resto di 5637298 modulo 3 basta osservare che

$$5637298 \equiv_3 5+6+3+7+2+9+8 \equiv_3 2+0+0+(1+2)+0+2 \equiv_3 4 \equiv_3 1.$$

Quindi il resto di 5637298 modulo 3 è 2.

Un numero intero positivo a è divisibile per 9 se e solo se la somma delle sue cifre è divisibile per 9. Si ragiona in modo del tutto simile al precedente, poiché anche in questo caso $10 \equiv_9 1$, e dunque $10^k \equiv_9 1^k = 1$, per ogni numero intero positivo k. Quindi di nuovo:

$$a \equiv_9 a_0 + a_1 + a_2 + \cdots + a_{m-2} + a_{m-1} + a_m.$$

Inoltre di nuovo per calcolare il resto di a modulo 9 si sommano le cifre di a (omettendo le cifre uguali a 9), iterando questo procedimento fino ad arrivare al resto.

Ad esempio, per calcolare il resto di 8956328716 modulo 9 basta osservare che $8956328716 \equiv_9 8 + 5 + (6 + 3) + (2 + 7) + (8 + 1) + 6 \equiv_9 13 + 0 + 0 + 0 + 6 \equiv_9 19 \equiv_9 1$. Quindi il resto di 8956328716 modulo 9 è 1.

Sulla compatibilità delle congruenze con le operazioni di somma e prodotto e sul criterio di divisibilità per 9 è basata la prova del 9 che si impara alle scuole elementari.

Un numero intero positivo a è divisibile per 11 se e solo se la differenza fra la somma delle sue cifre di posto pari e la somma delle sue cifre di posto dispari è divisibile per 11. Poiché $10 \equiv_{11} -1$, si ha che $10^k \equiv_{11} (-1)^k = 1$, se k è pari, e $10^k \equiv_{11} (-1)^k = -1$, se k è dispari, per ogni numero intero positivo k. Quindi:
$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + a_5 \cdot 10^5 \cdots \equiv_{11} a_0 - a_1 + a_2 - a_3 + a_4 - a_5 \cdots = (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$.
Iterando, come nei casi precedenti, questa formula, si può trovare il resto di a modulo 11.

Ad esempio $562739278 \equiv_{11} (8 + 2 + 3 + 2 + 5) - (7 + 9 + 7 + 6) = -9 \equiv_{11} 2$, quindi il resto di 562739278 modulo 11 è 2.

Un'altra situazione nella quale la $(*)$ permette di enunciare un criterio di divisibilità è quando $\overline{100} = \bar{0}$.

Un numero intero positivo a è divisibile per 4 se e solo se il numero formato dalla sua cifra delle decine e da quella dell'unità è divisibile per 4. Infatti raggruppando a due a due le cifre di a, si può scrivere $a = d \cdot 100 + e$, dove d è il numero ottenuto cancellando le ultime due cifre di a, mentre $e \overset{def}{=} a_0 + a_1 \cdot 10$ è il numero formato dalla cifra delle unità e quella delle decine di a. Poiché $d \cdot 100$ è divisibile per 4, si ha che $a = d \cdot 100 + e \equiv_4 e$, dunque il resto di a modulo 4 è uguale al resto di e modulo 4.

Ad esempio il resto di 65934713 modulo 4 è uguale al resto di 13 modulo 4 e quindi è 1.

Osservando che gli unici multipli di 25 minori di 100 sono $0, 25, 50, 75$, con lo stesso procedimento dimostrativo, lasciato al lettore, si può dimostrare che:

Un numero intero positivo a è divisibile per 25 se e solo se le sue ultime due cifre sono 00, 25, 50 o 75.

Non si sono esauriti tutti i possibili criteri di divisibilità. In realtà quelli che servono sono solo quelli per n numero primo. Applichiamo infatti il Teorema fondamentale dell'aritmetica, secondo il quale ogni numero intero > 1 è, in unico modo, prodotto di potenze di primi. Dunque per verificare se a è divisibile per $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ basta verificare che a sia divisibile per $p_1^{m_1}$, $p_2^{m_2}, \ldots, p_s^{m_s}$. Ad esempio per capire se 3792888 sia divisibile per 396, basta osservare che $396 = 2^2 \cdot 3^2 \cdot 11$ e quindi verificare se 3792888 sia divisibile sia per 4 che per 9 che per 11, esercizio che si lascia al lettore. Inoltre per scoprire se a sia divisibile per p^m, una potenza di un primo p, con $m > 1$, si può prima controllare se il numero a è divisibile per p. Se la risposta è no, a non è divisibile neanche per p^m. Altrimenti si considera

$b = \frac{a}{p}$, e si può notare che a è divisibile per p^m se e solo se b è divisibile per p^{m-1}. Basta reiterare il ragionamento e dopo al più $m-1$ passi si troverà la risposta.

Ad esempio, si vuole sapere se 127776 è divisibile per 1331. Poiché $1331 = 11^3$, si può iniziare con lo stabilire se 127776 è divisibile per 11. La risposta è sì, in quanto la differenza fra la somma delle cifre di posto pari e la somma delle cifre di posto dispari di 127776 è $(6+7+2)-(7+7+1) = 0$. Per vedere se $\frac{127776}{11} = 11616$ è divisibile per 11^2, stabiliamo se 11616 è divisibile per 11. La risposta è ancora sì, in quanto $(6+6+1)-(1+1) = 11$. Infine vediamo se $\frac{11616}{11} = 1056$ è divisibile per 11. La risposta è di nuovo sì, come il lettore può facilmente verificare. Quindi si è ottenuto che 127776 è divisibile per $11^3 = 1331$. Si sarà notato che questo metodo necessita di un bel po' di conti e passaggi, anche se elementari, quindi i criteri di divisibilità diretti che abbiamo fornito per 4 o per 9 sono utili per risparmiare fatica.

Dunque ci piacerebbe avere criteri di divisibilità per ogni primo p. Si sono forniti criteri per i primi 2, 3, 5, 11, ma non per 7, 13, 17 (e così via). Anche per questi altri primi si possono scrivere dei criteri, ma sono un po' più complicati. Per esempio vediamo quale può essere un criterio per la divisibilità modulo 7.

Un numero intero positivo a è divisibile per 7 se e solo se detto b il numero ottenuto da a eliminando la cifra delle unità e detta c la cifra delle unità, $b - 2c$ è divisibile per 7. Per dimostrare questo criterio si sfrutterà il fatto che, essendo 21 un multiplo di 7, $-20 \equiv_7 1$. Moltiplicando per -2 la $(**)$, si ha $-2a = -20 \cdot b - 2c \equiv_7 b - 2c$. Dal momento che $-6 \equiv_7 1$, si ottiene $a \equiv_7 -6a \equiv_7 3(-2a) \equiv_7 3(b-2c)$. Poiché 7 è coprimo con 3, $3(b-2c)$ è divisibile per 7 se e solo se $b-2c$ lo è[2].

[2]Utilizzando il Lemma di Euclide: Se n divide un prodotto $x \cdot y$ ed è coprimo con x, allora n divide y.

Applichiamo questo criterio più volte per vedere se 669774 è divisibile per 7. Basta calcolare $66977 - 2 \cdot 4 = 66969$, e quindi $6696 - 2 \cdot 9 = 6678$, e ancora $667 - 2 \cdot 8 = 651$, e infine $65 - 2 \cdot 1 = 63$. Poiché quest'ultimo è divisibile per 7, lo è anche 669774.

Si noti che questo metodo non può essere utilizzato per trovare il resto di a, modulo 7, in quanto nei passaggi fatti nella dimostrazione si vede che $a \equiv_7 3(b - 2c)$ e dunque non è detto che a e $b - 2c$ abbiano lo stesso resto modulo 7 (ciò accade se e solo se tale resto è 0).

Il lettore potrebbe trovare un criterio simile per 13, sfruttando il fatto che $40 \equiv_{13} 1$, e utilizzarlo per verificare che 6792786 è divisibile per 13. E per 17, sfruttando il fatto che $-50 \equiv_{17} 1$, e utilizzarlo per verificare che 16385484 è divisibile per 17.