Criteri di divisibilità – Parte prima

di Antonino Giambò

1. Tutti gli studenti conoscono (o dovrebbero conoscere) i criteri di divisibilità dei numeri naturali per 10, per 5, per 2, per 3, per 9. Forse qualcuno conosce anche i criteri di divisibilità per 4, per 8, per 11. È assai probabile che pochissimi conoscano qualche criterio di divisibilità per 7 o per 13. Ma quasi certamente nessuno studente è in grado di dimostrare quei criteri, alcuni per lo meno, né che esista un criterio di divisibilità generale del quale i criteri suddetti si possono considerare come casi particolari.

Quanti studenti sono poi consapevoli che tali criteri di divisibilità, valevoli nel sistema di numerazione decimale, non sono più validi se cambia il sistema di numerazione?

Orbene, mi propongo in questo contributo di far conoscere un criterio di divisibilità generale e di mostrare come i criteri elencati prima ne siano effettivamente dei casi particolari.

Ma, per non dare l'impressione che si tratti di forme assolute di criteri di divisibilità, ne mostrerò di alternativi.

Mostrerò pure come tali criteri dipendano dal sistema di numerazione.

Per farlo c'è però bisogno di un discorso propedeutico piuttosto lungo, che riprende argomenti di aritmetica modulare, già affrontati in precedenti articoli e, in particolare, nell'articolo *Dal romanzo "Gli artisti dei numeri" – parte seconda*, sui quali argomenti non intendo però ritornare, rimandando a quell'articolo.

Data la gran mole di cose da trattare, suddividerò questo contributo in due parti: nella prima parte mi occuperò di pervenire alla dimostrazione del criterio generale di divisibilità per un numero $m>1$, nella seconda parte mostrerò alcuni criteri per particolari valori di m, come casi particolari del criterio stesso.

E mostrerò pure alcuni criteri alternativi.

Siccome l'argomento non rientra nel curricolo di studi elementari, mi rendo conto che pochi studenti, o forse nessuno, saranno interessati ad esso, ma voglio sperare che ci sia qualcuno che abbia perlomeno un briciolo di curiosità che lo stimoli a prendere visione dell'argomento.

2. Consideriamo la seguente equazione, nella quale i due membri, anziché essere uguali, devono risultare congrui rispetto ad un determinato modulo:

$$4^x \equiv_7 1 .$$

Una sua soluzione è evidentemente il numero 0. Considerato però che 4 e 7 sono numeri coprìmi, certamente un valore di x che la soddisfa è, in virtù del teorema di Fermat-Eulero, il numero $\varphi(7)=6$.

La domanda, che sorge spontanea, è allora la seguente:

esistono **altri** valori naturali che soddisfano all'equazione?

Per rispondere alla domanda costruiamo la seguente tabella (tabella 1), nella quale "$4^x \bmod 7$" indica il resto della divisione di 4^x per 7.

x	0	1	2	3	4	5	6	7	8	9
4^x	1	4	16	64	256	1.024	4.096	16.384	65.536	262.144
$4^x \bmod 7$	1	4	2	1	4	2	1	4	2	1

tabella 1

Si costata che, per $x\leq 9$, ci sono altri due valori, oltre a $x=0$ e $x=\varphi(7)=6$, che soddisfano all'equazione e sono esattamente $x=3$ e $x=9$. S'intuisce poi che altri valori possano esserci per $x>9$.

In generale, l'equazione:

(1) $$a^x \equiv_m 1 ,$$

con a, m numeri coprìmi ammette sicuramente, come soluzioni nell'insieme $\mathbb{N}$ dei numeri naturali, sia $x=0$ sia $x=\varphi(m)$. Ma ammette anche altre soluzioni.

Ebbene, il più piccolo numero naturale, che soddisfa alla suddetta equazione ma che sia **diverso da 0**, si denomina *gaussiano di* m *rispetto alla base* a.

Si può indicare con la scrittura $g(m, a)$.

Nell'esempio precedente si ha $g(7, 4)=3$, per cui evidentemente $g(7, 4)<\varphi(7)$.

Può capitare però che sia $\varphi(m)=g(m, a)$, come nel caso in cui sia $a=3$ ed $m=5$ e come mostra la tabella sottostante (tabella 2), dalla quale si desume che $x=4=\varphi(5)$ è il più piccolo numero naturale non nullo che risolve l'equazione $3^x \equiv_5 1$.

x	0	1	2	3	4
3^x	1	3	9	27	81
$3^x \bmod 5$	1	3	4	2	1

tabella 2

3. Ci soffermiamo adesso su alcune proprietà del gaussiano di un determinato numero rispetto ad una data base, precisamene su quelle proprietà che sono funzionali al caso nostro, puntualizzando una volta per tutte che, se non ci sono motivi di ambiguità, porremo per comodità $g(m,a)=g$.

- PROPRIETÀ 1.

Ogni soluzione dell'equazione (1) nell'insieme $\mathbb{N}_0$ dei numeri naturali non nulli è un multiplo di g.

DIMOSTRAZIONE.

Ammettiamo che $k>0$ sia una qualsiasi soluzione dell'equazione (1). Per definizione di gaussiano, deve essere $k \geq g$. Se allora q ed r sono il quoziente e il resto della divisione di k per g (ovviamente $r<g$), si ha: $k = g\,q + r$. Pertanto si ha in sequenza:

$$a^k \equiv_m 1 \quad \Longrightarrow \quad a^{g\,q\,+\,r} \equiv_m 1 \quad \Longrightarrow \quad (a^g)^q \cdot a^r \equiv_m 1 .$$

D'altro canto, essendo g soluzione dell'equazione (1), si ha $a^g \equiv_m 1$, e, inoltre, per una nota proprietà delle congruenze: $(a^g)^q \equiv_m 1^q$, vale a dire: $(a^g)^q \equiv_m 1$.

Cosicché, tenendo presente la proprietà delle congruenze in base alla quale possiamo cancellare due valori congrui rispetto al modulo nei due membri della congruenza (i valori congrui rispetto al modulo m sono $(a^g)^q$ nel primo membro e 1 nel secondo membro), risulta che:

$$(a^g)^q \cdot a^r \equiv_m 1 \quad \Longrightarrow \quad a^r \equiv_m 1 .$$

Il numero r sarebbe dunque una soluzione dell'equazione (1).

Ricordando però che $r<g$ e che g è il più piccolo valore non nullo che soddisfa all'equazione, l'unica possibilità è che sia $r=0$. Per cui risulta $k = g\,q$. Come dire che k è multiplo di g. [c.v.d.]

- PROPRIETÀ 2.

Il numero $\varphi(m)$, cioè il numero dei numeri naturali non nulli minori di m e primi con esso, è un multiplo del gaussiano g di m rispetto ad una data base a.

DIMOSTRAZIONE.

In virtù delle proprietà 1, ogni soluzione dell'equazione (1) è un multiplo di g. Quindi anche $\varphi(m)$ è multiplo di g. Il che ovviamente non esclude che $\varphi(m)$ sia proprio g, dal momento che ogni numero è multiplo di se stesso.

- PROPRIETÀ 3.

Se sussiste la congruenza $a^b \equiv_m a^c$ allora sussiste anche la congruenza $b \equiv_g c$.

DIMOSTRAZIONE.

Se fosse $b=c$, la proprietà sarebbe evidente. Supponiamo allora $b \neq c$ e ammettiamo che sia $b>c$ (cambia poco nel ragionamento se si suppone $c>b$). Allora si ha in sequenza:

$$a^b \equiv_m a^c \quad \Longrightarrow \quad a^b : a^c \equiv_m a^c : a^c \quad \Longrightarrow \quad a^{b-c} \equiv_m 1 .$$

Questo significa che b−c è una soluzione dell'equazione $a^x \equiv_m 1$. Per cui, in base alla proprietà 1, b−c deve essere multiplo del gaussiano g di m rispetto ad a. Ragion per cui, esiste un numero naturale h tale per cui risulta b−c = h g. Vale a dire che $b \equiv_g c$. [c.v.d.]

- PROPRIETÀ 4.

Premesso che due numeri a, b che non siano congrui rispetto ad un modulo m si dicono *incongrui* rispetto a quel modulo e si scrive $a \not\equiv_m b$, la nuova proprietà è la seguente:

Sia g il gaussiano di m rispetto ad una data base a e siano le seguenti g potenze di a:

$$a^0,\ a^1,\ a^2,\ \dots,\ a^{g-2},\ a^{g-1}.$$

Queste potenze, prese a due a due, sono incongrue rispetto al modulo m.

Inoltre, i resti delle divisioni di queste potenze per il modulo m, rispettivamente:

$$r_0,\ r_1,\ r_2,\ \dots\ ,\ r_{g-2},\ r_{g-1},$$

si ripetono quando si considerano le potenze di a con esponenti maggiori o uguali a g, vale a dire che la successione dei resti delle divisioni delle successive potenze di a per m è periodica con periodo g.

DIMOSTRAZIONE.

Teniamo sempre presente che a ed m sono numeri coprìmi e che pure sono coprìmi a^b e a^c, dove b, c sono numeri minori di g.

- Dimostriamo la prima parte della proprietà, cioè che le potenze, prese a due a due, sono incongrue rispetto al modulo m

Supponiamo allora che, fra le potenze di a elencate nell'enunciato ce ne siano due congrue fra loro rispetto al modulo m, e siano a^b e a^c, dove chiaramente sia b sia c sono numeri minori di g. Essendo dunque $a^b \equiv_m a^c$, ragionando come nella dimostrazione della precedente proprietà 3, si desume che $b - c$ è una soluzione dell'equazione $a^x \equiv_m 1$. Il che, essendo chiaramente b−c <g, è possibile solo se b=c, cioè se le due potenze coincidono. In caso contrario, cioè se le due potenze sono distinte, allora sono incongrue rispetto al modulo m.

- Passiamo alla seconda parte, cioè che la successione dei resti delle divisioni delle successive potenze di a per m è periodica con periodo g

Intanto è evidente che i resti $r_0, r_1, r_2, \dots, r_{g-2}, r_{g-1}$ sono diversi l'uno dagli altri, dal momento che se ce fe fossero due uguali, le relative potenze sarebbero congrue rispetto al modulo m, mentre sappiamo che tali potenze sono incongrue (mod m).

Osserviamo ora che, essendo $a^g \equiv_m 1$, in virtù di note proprietà delle congruenze, possiamo scrivere in sequenza:

$a^{g+0} \equiv_m a^0$,

$a^g \cdot a \equiv_m 1 \cdot a$, vale a dire: $a^{g+1} \equiv_m a^1$,

$a^g \cdot a^2 \equiv_m 1 \cdot a^2$, vale a dire: $a^{g+2} \equiv_m a^2$,

… … … … … … … ,

$a^g \cdot a^{g-2} \equiv_m 1 \cdot a^{g-3}$, vale a dire: $a^{g+(g-2)} \equiv_m a^{g-2}$,

$a^g \cdot a^{g-1} \equiv_m 1 \cdot a^{g-1}$, vale a dire: $a^{g+(g-1)} \equiv_m a^{g-1}$.

In generale: $a^{k+g} \equiv_m a^k$.

In virtù di ciò, i resti delle divisioni di tali potenze per m si ripetono per gruppi di g elementi.

Insomma, come volevamo dimostrare, la successione dei resti delle divisioni delle successive potenze di a per m è periodica con periodo g.

Cosicché, posto che sia p il numero delle cifre del periodo, ossia posto p=g(m,a), uno schema che indichi le successive potenze di a e i corrispondenti resti delle loro divisioni per m, potrebbe essere il seguente:

a^0	a^1	a^2	…	a^{p-1}	a^p	a^{p+1}	a^{p+2}	…	a^{p+p-1}	a^{2p}	a^{2p+1}	a^{2p+2}	…	a^{2p+p-1}	… .
r_0	r_1	r_2	…	r_{p-1}	r_0	r_1	r_2	…	r_{p-1}	r_0	r_1	r_2	…	r_{p-1}	…. .

4. Finora, in tutti i ragionamenti fatti, abbiamo supposto che i numeri a ed m fossero primi fra loro. Ci interessa osservare che, anche quando a ed m non sono numeri coprìmi, i resti delle divisioni delle successive potenze di a per il modulo m, vale a dire:

$$a^0 \bmod m,\ \ a^1 \bmod m,\ \ a^2 \bmod m,\ \ \dots\ ,\ \ a^n \bmod m,\ \ \dots\ ,$$

sono comunque minori del divisore m. Questo significa che i resti diversi fra loro possono essere al più m, dopo di che, da un certo punto in poi devono ripetersi, esattamente come quando a ed m sono primi fra loro.

L'unica differenza è che adesso, la successione dei resti presenta, prima del gruppo che si ripete (periodo), un gruppo di resti che poi non si ripeterà (antiperiodo). Cosicché, posto che sia p il numero delle cifre del periodo e sia q il numero delle cifre dell'antiperiodo, uno schema che indichi le successive potenze di a e i corrispondenti resti delle loro divisioni per m, potrebbe essere il seguente:

$$\begin{array}{cccccc|cccccc|ccccc|c} a^0 & a^1 & a^2 & \dots & a^{q-1} & | & a^q & a^{q+1} & a^{q+2} & \dots & a^{q+p-1} & | & a^{q+p} & a^{q+p+1} & a^{q+p+2} & \dots & a^{q+2p-1} & | \ \dots . \\ r_0 & r_1 & r_2 & \dots & r_{q-1} & | & r_q & r_{q+1} & r_{q+2} & \dots & r_{q+p-1} & | & r_q & r_{q+1} & r_{q+2} & \dots & r_{q+p-1} & | \ \dots . \end{array}$$

A titolo di esempio si possono prendere in considerazione le potenze di a=6, assumendo per modulo m=4. Una tabella (tabella 3) riassume i risultati. Vi si può notare che l'antiperiodo è formato dalle cifre 1, 2, mentre il periodo è costituito dalla sola cifra 0.

x	0	1	2	3
6^x	1	6	36	216
$6^x \bmod 4$	1	2	0	0

tabella 3

5. Abbiamo adesso tutti gli elementi per ottenere un criterio generale di divisibilità nel sistema di numerazione decimale.

Sia allora N un qualsiasi numero naturale e, nel sistema di numerazione decimale, siano $a_0, a_1, a_2, \dots, a_{n-1}, a_n$ le sue cifre a partire da destra, cioè le cifre di ordine rispettivamente 0, 1, 2 , … , n–1, n, tutte ovviamente minori di 10. Per cui il numero può essere messo nella nota forma polinomiale:

(2) $$N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10^1 + a_0 10^0 .$$

Ci proponiamo di trovare un criterio di divisibilità di N per un determinato numero naturale m>1.

Indichiamo con r_k (k = 0, 1, 2, ..., n – 1, n) il resto della divisione di 10^k per m, per cui si ha:

$$10^k \equiv_m r_k .$$

In base a questa posizione, il numero N risulta congruo (mod. m) del polinomio che si ottiene ponendo r_k al posto di 10^k nel polinomio (2), vale a dire:

(3) $$N \equiv_m a_n r_n + a_{n-1} r_{n-1} + \dots + a_2 r_2 + a_1 r_1 + a_0 r_0 .$$

I resti delle divisioni delle potenze di 10^k per m, cioè:

$$r_0\ ,\ r_1\ ,\ r_2\ ,\ \dots\ ,\ r_{n-1}\ ,\ r_n$$

si denominano *coefficienti di divisibilità per m (nel sistema di numerazione decimale) di ordine rispettivamente* 0, 1, 2, ... , n–1, n, che sono esattamente gli stessi ordini delle cifre di N.

La relazione (3), alla luce di quanto detto, fornisce la seguente proprietà.

PROPRIETÀ.

Il numero $N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10^1 + a_0 10^0$ – scritto nel sistema di numerazione decimale, e del quale siano $r_0\ ,\ r_1\ ,\ r_2\ ,\ \dots\ ,\ r_{n-1}\ ,\ r_n$ i coefficienti di divisibilità per m, di ordine rispettivamente 0, 1, 2, ... , n–1, n – quand'è diviso per un numero m>1, dà lo stesso resto dell'espressione

(4) $$a_n r_n + a_{n-1} r_{n-1} + \dots + a_2 r_2 + a_1 r_1 + a_0 r_0,$$

ossia della somma dei prodotti che si ottengono moltiplicando ciascuna cifra di N per il corrispondente coefficiente di divisibilità per m.

Questa proprietà permette dunque di calcolare il resto della divisione di N per m>1.

Basta calcolare il resto della divisione per m dell'espressione (4).

In particolare, permette di stabilire se questo resto è 0. Il che accade quando il resto della divisione per m dell'espressione (4) è appunto 0.

Insomma N è divisibile per m se e solo se lo è l'espressione (4).

Ecco dunque il criterio che andiamo cercando.

CRITERIO DI DIVISIBILITÀ NEL SISTEMA DI NUMERAZIONE DECIMALE.

Condizione necessaria e sufficiente affinché un numero, scritto nel sistema di numerazione decimale, sia divisibile per il numero m>1, è che sia divisibile per m la somma dei prodotti che si ottengono moltiplicando ciascuna cifra di N per il corrispondente coefficiente di divisibilità per m.

6. Un esempio può essere utile per comprendere il procedimento suggerito dal criterio.

Sia dunque il numero N=3.388.117.799. Ci proponiamo di stabilire se è divisibile per 17, utilizzando il criterio sopraddetto.

Intendiamoci, potremmo stabilire se il numero è divisibile per 17 semplicemente con una calcolatrice, ma qui ci interessa spiegare come funziona il criterio.

Anche se, bisogna dirlo con franchezza, per questo fa comodo comunque una calcolatrice.

Allora, siccome 10 è primo con 17, la successione dei resti delle divisioni delle successive potenze di 10 per 17 è periodica semplice. Possiamo stabilire a priori di quanti termini consta il periodo della successione.

Di fatto, essendo questo numero il gaussiano g di 17 rispetto alla base 10, esso è il più piccolo numero naturale non nullo che soddisfa all'equazione $10^x \equiv_{17} 1$.

Con un po' di pazienza (e una calcolatrice di supporto) si trova anzitutto g=16 e, in secondo luogo, che la successione dei 16 resti è la seguente:

$$10^0 \bmod 17 = 1,\ \ 10^1 \bmod 17 = 10,\ \ 10^2 \bmod 17 = 15,\ \ 10^3 \bmod 17 = 14,$$
$$10^4 \bmod 17 = 4,\ \ 10^5 \bmod 17 = 6,\ \ 10^6 \bmod 17 = 9,\ \ 10^7 \bmod 17 = 5,$$
$$10^8 \bmod 17 = 16,\ \ 10^9 \bmod 17 = 7,\ \ 10^{10} \bmod 17 = 2,\ \ 10^{11} \bmod 17 = 3,$$
$$10^{12} \bmod 17 = 13,\ \ 10^{13} \bmod 17 = 11,\ \ 10^{14} \bmod 17 = 8,\ \ 10^{15} \bmod 17 = 12,$$

Pertanto, la successione dei coefficienti di divisibilità per 17, ha il seguente periodo:

$$1\ \ 10\ \ 15\ \ 14\ \ 4\ \ 6\ \ 9\ \ 5\ \ 16\ \ 7\ \ 2\ \ 3\ \ 13\ \ 11\ \ 8\ \ 12\,.$$

Possiamo calcolare adesso la somma S dei prodotti che si ottengono moltiplicando ciascuna cifra di N per il corrispondente coefficiente di divisibilità per 17. Essa è la seguente:

$$S = 9 \cdot 1 + 9 \cdot 10 + 7 \cdot 15 + 7 \cdot 14 + 1 \cdot 4 + 1 \cdot 6 + 8 \cdot 9 + 8 \cdot 5 + 3 \cdot 16 + 3 \cdot 7 + 0 = 493\,.$$

Siccome $N \equiv S \pmod{17}$, allora $N \equiv 493 \pmod{17}$. Cosicché, considerato che 493 è divisibile per 17, anche N lo è.

A volte può far comodo procedere diversamente dopo aver determinato i coefficienti di divisibilità per 17.

Consideriamo infatti che stiamo prendendo in esame numeri congrui rispetto al modulo 17, per cui, rispetto appunto a questo modulo, valgono le seguenti congruenze:

$$10 \equiv -7,\ \ 15 \equiv -2,\ \ 14 \equiv -3,\ \ 9 \equiv -8,\ \ 16 \equiv -1,\ \ 13 \equiv -4,\ \ 11 \equiv -6,\ \ 12 \equiv -5.$$

Questo significa che possiamo assumere come periodo della successione dei coefficienti di divisibilità per 17, il periodo seguente, ottenuto dal precedente, sostituendo al posto di 9, 10, 11, 12, 13, 14 15, i valori cui essi sono congrui:

$$1\ \ -7\ \ -2\ \ -3\ \ \ 4\ \ \ 6\ \ -8\ \ \ 5\ \ -1\ \ \ 7\ \ \ 2\ \ \ 3\ \ -4\ \ -6\ \ \ 8\ \ -5\,.$$

Possiamo calcolare adesso la somma S' dei prodotti che si ottengono moltiplicando ciascuna cifra di N per il corrispondente coefficiente di divisibilità per 17. Essa è la seguente:

$$S' = 9 \cdot 1 + 9 \cdot (-7) + 7 \cdot (-2) + 7 \cdot (-3) + 1 \cdot 4 + 1 \cdot 6 + 8 \cdot (-8) + 8 \cdot 5 + 3 \cdot (-1) + 3 \cdot 7 + 0 = -85\,.$$

Siccome $N \equiv S' \pmod{17}$, allora $N \equiv -85 \pmod{17}$. Cosicché, considerato che 85 è divisibile per 17, anche N lo è.

Un contro-esempio. Sia $M=417.608$. Di nuovo, ci proponiamo di stabilire se è divisibile per 17.

Conosciamo già i coefficienti di divisibilità per 17, in particolare nella seconda delle due forme precedenti.

Calcoliamo allora la somma Σ dei prodotti che si ottengono moltiplicando ciascuna cifra di M per il corrispondente coefficiente di divisibilità. Otteniamo:

$$\Sigma = 8 \cdot 1 + 0 \cdot (-7) + 6 \cdot (-2) + 7 \cdot (-3) + 1 \cdot 4 + 4 \cdot 6 + 0 = 3 \,.$$

Siccome $M \equiv \Sigma \pmod{17}$ allora $M \equiv 3 \pmod{17}$. Si desume che, non essendo 3 divisibile per 17, nemmeno M lo è.

7. Con questi esempi non abbiamo, in realtà, fornito un criterio di divisibilità per 17, ma solamente come sia possibile stabilire se un particolare numero sia o non sia divisibile per 17.

È comunque solo un assaggio.

In un prossimo articolo ci occuperemo di mostrare come, applicando il criterio qui dimostrato, si possano giustificare i noti criteri di divisibilità per particolari valori di m e ottenerne altri che forse noti non sono.

Ribadisco che al giorno d'oggi basta una calcolatrice per stabilire rapidamente se un determinato numero è o non è divisibile per un altro numero, almeno nei limiti di calcolo consentiti dalla calcolatrice. Questo non ci interessa. Ci interessa invece chiarire quali siano i criteri di divisibilità e come si dimostrino.

Occorre dire che i criteri di divisibilità per 3, 9 e 11, dei quali comunque ci occuperemo nella seconda parte dell'articolo, figurano nella sezione I, di sole 5 pagine, dell'opera *Disquisitiones Arithmeticae* (1801) di Carl Friedrich Gauss (1777-1855), al quale si deve pure la creazione dell'aritmetica delle congruenze, oggigiorno denominata *aritmetica modulare*. Aritmetica introdotta da Gauss nella stessa sezione I, ma sviluppata nella sezione II dell'opera succitata.

BIBLIOGRAFIA.

[1] Armando Chiellini – Roberto Giannarelli, *L'esame orale di matematica nei concorsi a cattedre di scuole secondarie*, Roma, Libreria Eredi Virgilio Veschi, 1962, pagg. 96-102.

[2] Antonio Rufián Lizana, *Gauss*, collana Geni della Matematica, Milano, RBA Italia, 2017.

[3] Wikipedia, libera enciclopedia on-line.