

NUOVI CRITERI DI DIVISIBILITÀ

BRUNO BIZZARRI, FRANCO EUGENI, DANIELA TONDINI¹

1. – Su tutti i testi scolastici di Scuola Media, nonostante siano riportati i criteri di divisibilità per i numeri 2, 3, 4, 5, 6, 8, 9, 10, 11, viene omissso, com'è immediato constatare, il criterio di divisibilità sia per 7 che per i successivi valori 12, 13, etc.

Ma allora esiste un criterio di divisibilità per 7? La risposta a tale domanda risulta essere affermativa anche se i vari criteri noti, sia per il 7 che per altri numeri, quali il 12 ed il 13, sono in generale difficili, non solo da applicare ma anche e soprattutto da ricordare.

a) Il più noto ed antico criterio consiste nel prendere un numero in rappresentazione decimale, scriverlo in ordine inverso come vettore–cifre e moltiplicarlo scalarmente, ovvero effettuando la somma dei prodotti cifra per cifra, per i numeri della sequenza 1, 3, 2, 6, 4, 5 accorciata o ripetuta a seconda della lunghezza del vettore dato.

Esempio 1.

Il numero 219135 è divisibile per 7?

Se consideriamo il numero, cifra per cifra, scritto al rovescio (5, 3, 1, 9, 1, 2) e lo moltiplichiamo scalarmente per la sequenza (1, 3, 2, 6, 4, 5), otteniamo:

$$5 \times 1 + 3 \times 3 + 1 \times 2 + 9 \times 6 + 1 \times 4 + 2 \times 5 = 84 = 70 + 14 = 7 \times (10 + 2)$$

che è divisibile per 7!

Esempio 2.

Il numero 2191 è divisibile per 7?

Se consideriamo il numero, cifra per cifra, scritto al rovescio, ovvero (1, 9, 1, 2), e lo moltiplichiamo per (2, 6, 4, 5), otteniamo:

$$1 \times 2 + 9 \times 6 + 1 \times 4 + 2 \times 5 = 70 = 7 \times 10 \text{ (divisibile per 7!)}$$

o ancora:

$$1 \times 1 + 9 \times 3 + 1 \times 2 + 2 \times 6 = 42 = 7 \times 6 \text{ (divisibile per 7!)}$$

Esempio 3.

Il numero 1753087 è divisibile per 7?

Se consideriamo il numero, cifra per cifra, scritto al rovescio, ovvero (7, 8, 0, 3, 5, 7, 1), e lo moltiplichiamolo per (1, 3, 2, 6, 4, 5, 1), otteniamo:

$$7 \times 1 + 8 \times 3 + 0 \times 2 + 3 \times 6 + 5 \times 4 + 7 \times 5 + 1 \times 1 = 105 = 7 \times 15 \text{ (divisibile per 7!)}$$

b) Un ulteriore criterio consiste nel rovesciare sempre il numero, utilizzando, però, una sequenza più riduttiva, precisamente 1, 3, 2, -1, -3, -2.

Esempi.

Il numero 219135 è divisibile per 7 se e solo se lo è:

$$(5, 3, 1, 9, 1, 2) \times (1, 3, 2, -1, -3, -2) = 5 + 9 + 2 - 9 - 3 - 4 = 0 = 7 \times 0 \text{ (divisibile per 7!)}$$

¹ Dipartimento di Scienze della Comunicazione – Università degli Studi di Teramo
eugenif@tin.it, dtondini@unite.it

Il numero 2191 è divisibile per 7 se e solo se lo è:

$$(1,9,1,2) \times (1,3,2,-1) = 1 + 27 + 2 - 2 = 28 = 7 \times 4 \text{ (divisibile per 7!)}$$

Il numero 1753087 è divisibile per 7 se e solo se lo è:

$$(7,8,0,3,5,7,1) \times (1,3,2,-1,-3,-2,1) = 7 + 24 + 0 - 3 - 15 - 14 + 1 = 0 = 7 \times 0 \text{ (divisibile per 7!)}$$

c) Un altro criterio, attribuito a *David SENCE* (*The Mathematical Gazette*, 1956) anche se, in realtà, era già stato scoperto dal russo *Andrej ZIBOSKI* (cfr. E. Dickson, *History of Theory of Numbers*), consiste nel sottrarre al numero originario, privato della sua ultima cifra, il doppio dell'ultima cifra stessa, iterando il ragionamento fino a quando non si ha la certezza di trovarsi di fronte ad un numero divisibile per 7.

Esempio.

Il numero 2191 è divisibile per 7 se e solo se lo è $219 - 2 \times 1 = 217$ che, a sua volta, è divisibile per 7 se e solo se lo è $21 - 2 \times 7 = 7$ (divisibile per 7!).

Scopo della presente nota è di illustrare, non solo un semplice criterio di divisibilità per 7, a nostro avviso sconosciuto e la cui dimostrazione risulta banale, ma anche una sua estensione, altrettanto facile, a casi più generali (cfr. paragrafo 3).

Possiamo enunciare suddetto criterio, applicabile ad un numero di almeno tre cifre, essendo il caso di due cifre ovvio, nel modo seguente:

Criterio di divisibilità per 7. *Un numero (in rappresentazione decimale) $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 7 se e solo se lo è il numero $C_1 C_0 + 2 \times C_n C_{n-1} \dots C_2$, ovvero la somma tra le ultime due cifre a destra ed il doppio della parte residua.*

Esempio.

Il numero 2191 è divisibile per 7 se solo se lo è $91 + 2 \times 21 = 133$ che, a sua volta, è divisibile per 7 se solo se lo è $33 + 2 \times 1 = 35 = 7 \times 5$ (divisibile per 7!).

Ancora il numero 219135 è divisibile per 7 se e solo se lo è $35 + 2 \times 2191 = 4417$ che, a sua volta, è divisibile per 7 se e solo se lo è $17 + 2 \times 44 = 105$ che, iterando il ragionamento, è divisibile per 7 se e solo se lo è $5 + 2 \times 1 = 7$ (divisibile per 7!).

Nel paragrafo 2, dopo aver richiamato i classici criteri di divisibilità, derivanti dal cosiddetto *Criterio Generale di Divisibilità*, che denomineremo *I Criterio*, ci soffermeremo sulle difficoltà che siamo costretti ad affrontare più frequentemente.

Nel paragrafo 3, invece, dopo aver dimostrato il criterio di divisibilità per 7, ci concentreremo sulle sue generalizzazioni, sì da giungere a quello che chiameremo *II Criterio Generale di Divisibilità*.

Nel paragrafo 4, infine, porremo in risalto le varie conseguenze che ne discendono, illustrando anche ulteriori criteri di divisibilità.

2. – Com'è ben noto, se $X = 0, 1, 2, \dots, 9$ è la base per la numerazione decimale, allora ogni numero naturale N si esprime, in modo unico, nella forma seguente:

$$N = (C_n C_{n-1} \dots C_2 C_1 C_0)_{10} = C_n 10^n + C_{n-1} 10^{n-1} + \dots + C_2 10^2 + C_1 10 + C_0$$

Nel presente paragrafo richiameremo la teoria della divisibilità rispetto ad una base di numerazione così come essa si deduce dalla teoria delle congruenze e del gaussiano. Allo scopo ricordiamo alcune definizioni.

Siano dati i numeri naturali m, a ed a' . Allora scrivere che

$$a \equiv a' \pmod{m} \quad (\text{si legge } a \text{ congruo ad } a' \text{ modulo } m)$$

significa dire che a ed a' , divisi per m , hanno lo stesso resto.

Ciò premesso ricordiamo che si chiama *gaussiano in base a di m* il numero:

$$g(m, a) = \text{gauss}(m, a) = \{ \min x \text{ t.c. } a^x \equiv 1 \pmod{m} \}$$

Sia data ora la successione:

$$1, a, a^2, a^3, \dots, a^n, \dots$$

e sia

$$R_0 = 1, R_1, R_2, \dots, R_n, \dots$$

la successione dei resti della divisione per m di tali numeri.

Se m_1 è il più grande divisore di m costituito da fattori primi di a (in altre parole i fattori primi di a , comuni ad m , ma elevati all'esponente massimo con cui dividono m), allora:

Teorema 1. *La successione dei resti sopra indicati è in generale periodico-mista con antiperiodo A e periodo G dati rispettivamente da:*

$$A = \{ \min x \text{ t.c. } a^x \equiv 0 \pmod{m_1} \}$$

$$G = \text{gauss} \left(\frac{m}{m_1}, a \right)$$

N.B. Se a ed m sono primi tra loro allora $m_1 \equiv 1, A = 0, G = g$; la sequenza dei resti arriva fino all'indice $g - 1$ ed inizia a ripetersi in corrispondenza dell'indice g , essendo $R_{g+h} = R_{0+h}$. Segue, in tal caso, che i resti che formano il periodo sono esattamente:

$$R_0 = 1, R_1, R_2, \dots, R_{g-1}$$

Osservazione. Nel caso in cui sia $a = 10$ (base decimale), allora (R) è:

- periodica semplice se m è primo con 2 ovvero con 5;
- periodico-composta se m è divisibile per 2 ovvero per 5.

Vediamo due esempi significativi:

a) Sia $m=3$ ed $a=10$. Poiché $(3;10)=1$ occorre calcolare $g = g(m,a) = g(3,10)$ ovvero $\{\min x \text{ t.c. } 10^x \equiv 1 \pmod{3}\}$. Poiché $10^1 - 1 = 9$ segue che è $g=1$ e che il periodo è costituito dal solo $R_0 = 1$.

b) Sia $m=4$ ed $a=10$. Risulta $m_1 = 4$, per cui dobbiamo calcolare:

$$A = \{\min x \text{ t.c. } 10^x \equiv 0 \pmod{4}\}$$

$$G = \text{gauss}(1,10) = \{\min x \text{ t.c. } 10^x \equiv 1 \pmod{1}\}$$

Quindi: $A = x = 2$ e $G = x = 1$. I resti sono: 1, 2, 0, 0, 0, ...

Nel seguito conviene, per le prime potenze del 10, effettuare le divisioni per $m = 2, 3, 4, 5, 6, \dots$ per ottenere la tabella che segue dalla quale si deducono vari criteri di divisibilità. Accanto al resto R porremo anche $R - m$ nel caso in cui questi sia, in valore assoluto, inferiore ad R , essendo:

$$R - m \equiv R \pmod{m}$$

In realtà il ricorso al Teorema 1 occorre solo se l'analisi procede per molti numeri, specie nei casi di gaussiano di grandi dimensioni.

TABELLA

<u>Resti mod 2:</u> $(R) = 1, 0, 0, 0, \dots, 1, [0]$	\Rightarrow <i>antiperiodo</i> = (1); <i>periodo</i> = (0)
<u>Resti mod 3:</u> $(R) = 1, 1, 1, 1, \dots, 1, [1]$	\Rightarrow <i>periodo</i> = (1)
<u>Resti mod 4:</u> $(R) = 1, 2, 0, 0, \dots, [0]$	\Rightarrow <i>antiperiodo</i> = (1, 2); <i>periodo</i> = (0)
<u>Resti mod 5:</u> $(R) = 1, 0, 0, 0, \dots, 1, [0]$	\Rightarrow <i>antiperiodo</i> = (1); <i>periodo</i> = (0)
<u>Resti mod 6:</u> $(R) = 1, 4, 4, 4, \dots, 4, [4]$	\Rightarrow <i>antiperiodo</i> = (1); <i>periodo</i> = (4) = (-2)
<u>Resti mod 7:</u> $(R) = 1, 3, 2, 6, 4, 5, \dots$	\Rightarrow <i>periodo</i> = (1, 3, 2, 6, 4, 5)
ovvero $(R) = 1, 3, 2, -1, -3, -2, \dots$ utilizzando anche resti negativi $(m - R)$	
<u>Resti mod 8:</u> $(R) = 1, 2, 4, 0, 0, 0, \dots$	\Rightarrow <i>antiperiodo</i> = (1, 2, 4); <i>periodo</i> = (0)
ovvero $(R) = 1, 3, 2, -1, -3, -2, \dots$ utilizzando anche resti negativi $(m - R)$	
<u>Resti mod 9:</u> $(R) = 1, 1, 1, 1, \dots, 1, [1]$	\Rightarrow <i>periodo</i> = (1)
<u>Resti mod 10:</u> $(R) = 1, 0, 0, 0, \dots, 1, [0]$	\Rightarrow <i>antiperiodo</i> = (1); <i>periodo</i> = (0)
<u>Resti mod 11:</u> $(R) = 1, 10, 1, 10, 1, 10, \dots$	\Rightarrow <i>periodo</i> = (1, 10)
ovvero $(R) = 1, -1, 1, -1, 1, -1, \dots$ utilizzando anche resti negativi $(m - R)$	
<u>Resti mod 12:</u> $(R) = 1, 10, 4, 4, 4, 4, \dots$	\Rightarrow <i>antiperiodo</i> = (1, 10); <i>periodo</i> = (4)
ovvero $(R) = 1, -2, 4, 4, 4, 4, \dots$ utilizzando anche resti negativi $(m - R)$	
<u>Resti mod 13:</u> $(R) = 1, 10, 9, 12, 3, 4, \dots$	\Rightarrow <i>periodo</i> = (1, 10, 9, 12, 3, 4)
ovvero $(R) = 1, -3, -4, -1, 3, 4, \dots$ utilizzando anche resti negativi $(m - R)$	

Se ora vogliamo individuare dei criteri affinché un altro numero naturale m sia un divisore di:

$$N = (C_n C_{n-1} \dots C_2 C_1 C_0)_{10} = C_n 10^n + C_{n-1} 10^{n-1} + \dots + C_2 10^2 + C_1 10 + C_0$$

dobbiamo, in generale, studiare il comportamento degli elementi della successione

$$1, 10, 10^2, \dots, 10^{n-1}, 10^n, \dots$$

qualora ciascuno di essi venga diviso per m , ed in particolare, valutare la successione dei resti della divisione di tali elementi per l'intero m .

A riguardo, denotata la successione dei resti e quella delle cifre rispettivamente con:

$$(R) = R_0 = 1, R_1, R_2, \dots, R_{n-1}, R_n, \dots$$

e quella delle cifre con:

$$(C) = C_0, C_1, C_2, \dots, C_{n-1}, C_n, \dots$$

possiamo richiamare il seguente Teorema, oramai ben noto in letteratura, la cui dimostrazione è banale.

Teorema 2 (Primo Criterio Generale di Divisibilità). *Dato il numero naturale:*

$$N = C_n C_{n-1} \dots C_2 C_1 C_0 = C_n 10^n + C_{n-1} 10^{n-1} + \dots + C_2 10^2 + C_1 10 + C_0$$

risulta che N è divisibile per m se e solo se lo è l'intero

$$(C) \times (R) = C_0 R_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n.$$

N.B. Ogni singolo R_h può banalmente sostituirsi con $R_h - m$.

Esempio 1. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 2 (ovvero per 5, ovvero per 10) se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 0, 0, 0, \dots, 0, \dots$ cioè se e solo se lo è C_0 .

Esempio 2. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 3 (ovvero per 9) se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 1, 1, 1, \dots, 1, \dots$, cioè se e solo se lo è la somma delle cifre.

Esempio 3. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 4 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 2, 0, 0, \dots, 0, \dots$, cioè se e solo se è divisibile per 4 il complesso delle ultime due cifre a destra, che lo è se lo è il numero $C_0 + 2C_1$.

Esempio 4. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 6 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 4, 4, 4, \dots, 4, \dots$, cioè se e solo se lo è la somma tra l'ultima cifra a destra e quattro volte la somma delle rimanenti, ovvero $C_0 + 4(C_1 + C_2 + \dots + C_n)$.

Esempio 5. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 7 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 3, 2, -1, -3, -2, \dots$

Esempio 6. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 8 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, 2, 4, 0, 0, 0, \dots$, cioè se e solo se lo è il complesso delle ultime tre cifre a destra, che lo è se lo è il numero $C_0 + 2C_1 + 4C_2$.

Esempio 7. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 11 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, -1, 1, -1, \dots$, cioè se e solo se lo è la somma delle cifre pari meno quella delle cifre dispari.

Esempio 8. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 12 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, -2, 4, 4, 4, 4, \dots$

Esempio 9. $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 13 se e solo se lo è:

$$C_0 + C_1 R_1 + C_2 R_2 + \dots + C_{n-1} R_{n-1} + C_n R_n$$

con $(R) = 1, -3, -4, -1, 3, 4, \dots$

Osserviamo che gli esempi 1, 2, ..., 7 rappresentano proprio i criteri citati in premessa, ivi compreso il criterio di divisibilità per 7; gli esempi 8 e 9, invece, esprimono i complicati criteri di divisibilità per 12 e per 13, derivanti dal primo criterio di divisibilità.

3. – Nel presente paragrafo dimostreremo il criterio di divisibilità per 7, già enunciato nel paragrafo 1. In realtà, però, proveremo un po' di più, precisamente il seguente:

Teorema (Secondo criterio generale di divisibilità). *Sia dato un numero naturale N rappresentato, rispetto ad una base $X = 0, 1, \dots, X-1$, da:*

$$N = (C_n C_{n-1} \dots C_2 C_1 C_0)_X = C_n X^n + C_{n-1} X^{n-1} + \dots + C_2 X^2 + C_1 X + C_0$$

Allora N è divisibile per m se e solo se lo è l'intero:

$$M = (X^r - km)(C_n C_{n-1} \dots C_{r+1})_X + (C_r C_{r-1} \dots C_2 C_1 C_0)_X$$

dove k è un intero arbitrario, quindi, in particolare, il più grande intero tale:

$$X^r - km > 0 \quad \Rightarrow \quad k = \left\lfloor \frac{X^r}{m} \right\rfloor$$

Dimostrazione.

Sia m un divisore di N . Allora:

$$N = hm = C_n X^n + C_{n-1} X^{n-1} + \dots + C_r X^r + C_{r-1} X^{r-1} + \dots + C_2 X^2 + C_1 X + C_0 =$$

$$= X^r [C_n X^{n-r} + C_{n-1} X^{n-r-1} + \dots + C_r] + (C_{r-1} \dots C_2 C_1 C_0)_X$$

$$hm - km(C_n C_{n-1} \dots C_r)_X = (C_n C_{n-1} \dots C_2 C_1 C_0)_X - km(C_n C_{n-1} \dots C_r)_X =$$

$$= X^r (C_n C_{n-1} \dots C_r)_X + (C_n C_{n-1} \dots C_r)_X - km(C_n C_{n-1} \dots C_r)_X =$$

$$= (X^r - km)(C_n C_{n-1} \dots C_r)_X + (C_n C_{n-1} \dots C_r)_X = M$$

Dunque m è un divisore di M .

Supponiamo ora che m divida M . Allora:

$$M = sm = (X^r - km)(C_n C_{n-1} \dots C_r)_X + (C_n C_{n-1} \dots C_r)_X$$

da cui segue:

$$M + km(C_n C_{n-1} \dots C_r)_X = sm + km(C_n C_{n-1} \dots C_r)_X = X^r (C_n C_{n-1} \dots C_r)_X + (C_n C_{n-1} \dots C_r)_X = N$$

Dunque l'asserto è verificato.

Osserviamo, in ultima analisi che il precedente teorema vale, non solo per una base qualsiasi, e quindi in particolare per la base 10, ma anche per un indice qualsiasi $r \geq 2$ e per un k qualsiasi, quindi anche per la suddetta parte intera.

4. – Nuovi Criteri

a) Criterio di divisibilità per 7. Per $X - 1 = 9$, $m = 7$, $r = 2$ e $k = 14$, ritroviamo il teorema enunciato nel primo paragrafo, essendo $(10^2 - k7) = 2 > 0$.

b) Criterio di divisibilità per 13. Per $X - 1 = 9$, $m = 13$, $r = 2$ e $k = 7$, otteniamo $(10^2 - k13) = 9 > 0$; per $k = 8$, invece, abbiamo $(10^2 - k13) = -4 < 0$. Possiamo, quindi, enunciare il criterio di divisibilità per 13 nel modo seguente:

Un numero (in rappresentazione decimale) $N = C_n C_{n-1} \dots C_2 C_1 C_0$ è divisibile per 13 se e solo se lo è il numero $C_1 C_0 + 9 \times C_n C_{n-1} \dots C_2$ [somma tra le ultime due cifre a destra e nove volte la parte residua], ovvero se e solo se lo è il numero $C_1 C_0 - 4 \times C_n C_{n-1} \dots C_2$ [differenza tra le ultime due cifre a destra e quattro volte la parte residua].

Esempi.

$$X - 1 = 9; m = 7; r = 2; k = \left\lfloor \frac{X^2}{m} \right\rfloor = 14 > 13 \text{ (si parte allora dal successivo!!!)}$$

$$X - 1 = 9; m = 8; r = 2; k = \left\lfloor \frac{X^2}{m} \right\rfloor = 12; (X^2 - km) = 4; C_1 C_0 + 4C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 9; r = 2; k = \left\lfloor \frac{X^2}{m} \right\rfloor = 11; (X^2 - km) = 1; C_1 C_0 + C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 10; r = 2; k = 10; (X^2 - km) = 0; C_1 C_0$$

$$X - 1 = 9; m = 11; r = 2; k = 9; (X^2 - km) = 1; C_1 C_0 + C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 12; r = 2; k = 8; (X^2 - km) = 4; C_1 C_0 + 4C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 13; r = 2; k = 7; (X^2 - km) = 9 = -4; C_1 C_0 + 9C_n C_{n-1} \dots C_2 = C_1 C_0 - 4C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 14; r = 2; k = 7; (X^2 - km) = 2; C_1 C_0 + 2C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 15; r = 2; k = 6; (X^2 - km) = 10 = -5; C_1 C_0 - 5C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 16; r = 2; k = 6; (X^2 - km) = 4; C_1 C_0 + 4C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 17; r = 2; k = 5; (X^2 - km) = 15 = -2; C_1 C_0 - 2C_n C_{n-1} \dots C_2$$

$$X - 1 = 9; m = 18; r = 2; k = 5; (X^2 - km) = 10 = -8; C_1 C_0 - 8C_n C_{n-1} \dots C_2$$

$$\begin{aligned}
& X-1=9; m=19; r=2; k=5; (X^2-km)=5; C_1C_0+5C_nC_{n-1}\dots C_2 \\
& X-1=9; m=20; r=2; k=5; (X^2-km)=0; C_1C_0 \\
& X-1=9; m=21; r=2; k=4; (X^2-km)=16; C_1C_0-5C_nC_{n-1}\dots C_2 \\
& X-1=9; m=22; r=2; k=4; (X^2-km)=12; C_1C_0-10C_nC_{n-1}\dots C_2 \\
& X-1=9; m=23; r=2; k=4; (X^2-km)=8; C_1C_0+8C_nC_{n-1}\dots C_2 \\
& X-1=9; m=24; r=2; k=4; (X^2-km)=4; C_1C_0+4C_nC_{n-1}\dots C_2 \\
& X-1=9; m=25; r=2; k=4; (X^2-km)=0; C_1C_0 \\
& X-1=9; m=26; r=2; k=3; (X^2-km)=22; C_1C_0-4C_nC_{n-1}\dots C_2 \\
& X-1=9; m=27; r=2; k=3; (X^2-km)=19; C_1C_0-8C_nC_{n-1}\dots C_2 \\
& X-1=9; m=28; r=2; k=3; (X^2-km)=16; C_1C_0-12C_nC_{n-1}\dots C_2 \\
& X-1=9; m=29; r=2; k=3; (X^2-km)=13; C_1C_0+13C_nC_{n-1}\dots C_2 \\
& X-1=9; m=30; r=2; k=3; (X^2-km)=10; C_1C_0+10C_nC_{n-1}\dots C_2 \\
& X-1=9; m=31; r=2; k=3; (X^2-km)=7; C_1C_0+7C_nC_{n-1}\dots C_2 \\
& X-1=9; m=32; r=2; k=3; (X^2-km)=4; C_1C_0+4C_nC_{n-1}\dots C_2 \\
& X-1=9; m=33; r=2; k=3; (X^2-km)=1; C_1C_0+C_nC_{n-1}\dots C_2 \\
& X-1=9; m=34; r=2; k=2; (X^2-km)=32; C_1C_0-2C_nC_{n-1}\dots C_2 \\
& X-1=9; m=35; r=2; k=2; (X^2-km)=30; C_1C_0-5C_nC_{n-1}\dots C_2 \\
& X-1=9; m=36; r=2; k=2; (X^2-km)=28; C_1C_0-8C_nC_{n-1}\dots C_2 \\
& X-1=9; m=37; r=2; k=2; (X^2-km)=26; C_1C_0-11C_nC_{n-1}\dots C_2 \\
& X-1=9; m=38; r=2; k=2; (X^2-km)=24; C_1C_0-14C_nC_{n-1}\dots C_2 \\
& X-1=9; m=39; r=2; k=2; (X^2-km)=22; C_1C_0-17C_nC_{n-1}\dots C_2 \\
& X-1=9; m=40; r=2; k=2; (X^2-km)=20; C_1C_0+20C_nC_{n-1}\dots C_2 \\
& X-1=9; m=41; r=2; k=2; (X^2-km)=18; C_1C_0+18C_nC_{n-1}\dots C_2 \\
& X-1=9; m=42; r=2; k=2; (X^2-km)=16; C_1C_0+16C_nC_{n-1}\dots C_2 \\
& X-1=9; m=43; r=2; k=2; (X^2-km)=14; C_1C_0+14C_nC_{n-1}\dots C_2 \\
& X-1=9; m=44; r=2; k=2; (X^2-km)=12; C_1C_0+12C_nC_{n-1}\dots C_2 \\
& X-1=9; m=45; r=2; k=2; (X^2-km)=10; C_1C_0+10C_nC_{n-1}\dots C_2 \\
& X-1=9; m=46; r=2; k=2; (X^2-km)=8; C_1C_0+8C_nC_{n-1}\dots C_2 \\
& X-1=9; m=47; r=2; k=2; (X^2-km)=6; C_1C_0+6C_nC_{n-1}\dots C_2 \\
& X-1=9; m=48; r=2; k=2; (X^2-km)=4; C_1C_0+4C_nC_{n-1}\dots C_2 \\
& X-1=9; m=49; r=2; k=2; (X^2-km)=2; C_1C_0+2C_nC_{n-1}\dots C_2 \\
& X-1=9; m=50; r=2; k=2; (X^2-km)=0; C_1C_0
\end{aligned}$$

$$\begin{aligned}
& X-1=9; m=51; r=2; k=1; (X^2-km)=49; C_1C_0-2C_nC_{n-1}\dots C_2 \\
& X-1=9; m=52; r=2; k=1; (X^2-km)=48; C_1C_0-4C_nC_{n-1}\dots C_2 \\
& X-1=9; m=53; r=2; k=1; (X^2-km)=47; C_1C_0-6C_nC_{n-1}\dots C_2 \\
& X-1=9; m=54; r=2; k=1; (X^2-km)=46; C_1C_0-8C_nC_{n-1}\dots C_2 \\
& X-1=9; m=55; r=2; k=1; (X^2-km)=45; C_1C_0-10C_nC_{n-1}\dots C_2 \\
& X-1=9; m=56; r=2; k=1; (X^2-km)=44; C_1C_0-12C_nC_{n-1}\dots C_2 \\
& X-1=9; m=57; r=2; k=1; (X^2-km)=43; C_1C_0-14C_nC_{n-1}\dots C_2 \\
& X-1=9; m=58; r=2; k=1; (X^2-km)=42; C_1C_0-16C_nC_{n-1}\dots C_2 \\
& X-1=9; m=59; r=2; k=1; (X^2-km)=41; C_1C_0-18C_nC_{n-1}\dots C_2 \\
& X-1=9; m=60; r=2; k=1; (X^2-km)=40; C_1C_0-20C_nC_{n-1}\dots C_2 \\
& X-1=9; m=61; r=2; k=1; (X^2-km)=39; C_1C_0-22C_nC_{n-1}\dots C_2 \\
& X-1=9; m=62; r=2; k=1; (X^2-km)=38; C_1C_0-24C_nC_{n-1}\dots C_2 \\
& X-1=9; m=63; r=2; k=1; (X^2-km)=37; C_1C_0-26C_nC_{n-1}\dots C_2 \\
& X-1=9; m=64; r=2; k=1; (X^2-km)=36; C_1C_0-28C_nC_{n-1}\dots C_2 \\
& X-1=9; m=65; r=2; k=1; (X^2-km)=35; C_1C_0-30C_nC_{n-1}\dots C_2 \\
& X-1=9; m=66; r=2; k=1; (X^2-km)=34; C_1C_0-32C_nC_{n-1}\dots C_2 \\
& X-1=9; m=67; r=2; k=1; (X^2-km)=33; C_1C_0+33C_nC_{n-1}\dots C_2 \\
& X-1=9; m=68; r=2; k=1; (X^2-km)=32; C_1C_0+32C_nC_{n-1}\dots C_2 \\
& X-1=9; m=69; r=2; k=1; (X^2-km)=31; C_1C_0+31C_nC_{n-1}\dots C_2 \\
& X-1=9; m=70; r=2; k=1; (X^2-km)=30; C_1C_0+30C_nC_{n-1}\dots C_2 \\
& X-1=9; m=71; r=2; k=1; (X^2-km)=29; C_1C_0+29C_nC_{n-1}\dots C_2 \\
& X-1=9; m=72; r=2; k=1; (X^2-km)=28; C_1C_0+28C_nC_{n-1}\dots C_2 \\
& X-1=9; m=73; r=2; k=1; (X^2-km)=27; C_1C_0+27C_nC_{n-1}\dots C_2 \\
& X-1=9; m=74; r=2; k=1; (X^2-km)=26; C_1C_0+26C_nC_{n-1}\dots C_2 \\
& X-1=9; m=75; r=2; k=1; (X^2-km)=25; C_1C_0+25C_nC_{n-1}\dots C_2 \\
& X-1=9; m=76; r=2; k=1; (X^2-km)=24; C_1C_0+24C_nC_{n-1}\dots C_2 \\
& X-1=9; m=77; r=2; k=1; (X^2-km)=23; C_1C_0+23C_nC_{n-1}\dots C_2 \\
& X-1=9; m=78; r=2; k=1; (X^2-km)=22; C_1C_0+22C_nC_{n-1}\dots C_2 \\
& X-1=9; m=79; r=2; k=1; (X^2-km)=21; C_1C_0+21C_nC_{n-1}\dots C_2 \\
& X-1=9; m=80; r=2; k=1; (X^2-km)=20; C_1C_0+20C_nC_{n-1}\dots C_2 \\
& X-1=9; m=81; r=2; k=1; (X^2-km)=19; C_1C_0+19C_nC_{n-1}\dots C_2 \\
& X-1=9; m=82; r=2; k=1; (X^2-km)=18; C_1C_0+18C_nC_{n-1}\dots C_2
\end{aligned}$$

$$\begin{aligned}
X-1=9; m=83; r=2; k=1; (X^2-km)=17; C_1C_0+17C_nC_{n-1}\dots C_2 \\
X-1=9; m=84; r=2; k=1; (X^2-km)=16; C_1C_0+16C_nC_{n-1}\dots C_2 \\
X-1=9; m=85; r=2; k=1; (X^2-km)=15; C_1C_0+15C_nC_{n-1}\dots C_2 \\
X-1=9; m=86; r=2; k=1; (X^2-km)=14; C_1C_0+14C_nC_{n-1}\dots C_2 \\
X-1=9; m=87; r=2; k=1; (X^2-km)=13; C_1C_0+13C_nC_{n-1}\dots C_2 \\
X-1=9; m=88; r=2; k=1; (X^2-km)=12; C_1C_0+12C_nC_{n-1}\dots C_2 \\
X-1=9; m=89; r=2; k=1; (X^2-km)=11; C_1C_0+11C_nC_{n-1}\dots C_2 \\
X-1=9; m=90; r=2; k=1; (X^2-km)=10; C_1C_0+10C_nC_{n-1}\dots C_2 \\
X-1=9; m=91; r=2; k=1; (X^2-km)=9; C_1C_0+9C_nC_{n-1}\dots C_2 \\
X-1=9; m=92; r=2; k=1; (X^2-km)=8; C_1C_0+8C_nC_{n-1}\dots C_2 \\
X-1=9; m=93; r=2; k=1; (X^2-km)=7; C_1C_0+7C_nC_{n-1}\dots C_2 \\
X-1=9; m=94; r=2; k=1; (X^2-km)=6; C_1C_0+6C_nC_{n-1}\dots C_2 \\
X-1=9; m=95; r=2; k=1; (X^2-km)=5; C_1C_0+5C_nC_{n-1}\dots C_2 \\
X-1=9; m=96; r=2; k=1; (X^2-km)=4; C_1C_0+4C_nC_{n-1}\dots C_2 \\
X-1=9; m=97; r=2; k=1; (X^2-km)=3; C_1C_0+3C_nC_{n-1}\dots C_2 \\
X-1=9; m=98; r=2; k=1; (X^2-km)=2; C_1C_0+2C_nC_{n-1}\dots C_2 \\
X-1=9; m=99; r=2; k=1; (X^2-km)=1; C_1C_0+C_nC_{n-1}\dots C_2
\end{aligned}$$

Si noti che se un numero $N = C_n \dots C_0$ non è divisibile per m allora il resto della divisione di N per m è dato dal risultato dell'ultima divisione effettuata.

Esempio.

Il numero 1123 non è divisibile per 7. Operando con il criterio di divisibilità per 7, considerando che $2 \times 11 + 23 = 45$ e che $45 = 6 \times 7 + 3$, risulta $1123 = \rho \times 7 + 3$ con $\rho = 160$.

5. – Divisibilità per 3

Notiamo che un numero è divisibile per 3 se, comunque ripartito, il doppio della somma delle cifre della ripartizione di sinistra meno la somma delle cifre della ripartizione di destra è divisibile per 3.

Dimostrazione.

Sappiamo che un numero $N = C_n \dots C_0$ è divisibile per 3 se e solo se lo è la somma delle sue cifre (decimali), cioè se e solo se lo è il numero $M = C_n + \dots + C_2 + C_1 + C_0$. Consideriamo l'identità:

$$\begin{aligned}
2(C_n + \dots + C_2 + C_1 + C_0) &= 2(C_n + \dots + C_i) + 2(C_{i-1} + \dots + C_1 + C_0) = \\
&= 2(C_n + \dots + C_i) - (C_{i-1} + \dots + C_1 + C_0) + 3(C_{i-1} + \dots + C_1 + C_0)
\end{aligned}$$

che chiaramente prova l'asserto.

Esempio.

Il numero 845322 (con $8+4+5+3+2+2=24$; $2+4=6!$) è divisibile per 3: ripartito, infatti, in 84 e 5322, risulta: $2(8+4)-(5+3+2+2)=24-12=12$, che è divisibile per tre.

Bibliografia

F. EUGENI – M.A. GARZIA – D. TONDINI, *La divisibilità nell'anello degli interi relativi*, in: www.apav.it (vedi: Comunicazione, Scienze e Società, voce numeri).

A. CHIellini – R. GIANNARELLI, *L'esame orale di Matematica nei concorsi a cattedre di scuole*, Libreria Eredi Virgilio Veschi, Roma, 1962.