Vincenzo Vitale

n esp1

Un ordinamento possibile dei numeri primi

Da una indagine sui criteri di divisibilità
si arriva gradualmente all'ordinamento
dei numeri primi

http://www.integernumbers.org

vincenzovitale@integernumbers.org

“n esp1 - Un ordinamento possibile dei numeri primi”
Codice: edit329022020

vincenzovitale@integernumbers.org
http://www.integernumbers.org

n esp1
Un ordinamento possibile dei numeri primi

Prima parte

Cap. 1	Divisibilità	pag. 1
Cap. 2	Le dimostrazioni	pag. 14
Cap. 3	Le congruenze	pag. 21
Cap. 4	Condizioni di divisibilità	pag. 29
Cap. 5	Criteri di divisibilità	pag. 35
Cap. 6	Altri criteri di divisibilità	pag. 50
Cap. 7	Aggregazioni di numeri primi	pag. 58
Cap. 8	n esp1, il contenitore di tutti i numeri primi	pag. 69

Seconda parte

Cap. 09	Numeri periodici	pag. 91
Cap. 10	Le molecole degli n esp1	pag.107
Cap. 11	Le numerazioni posizionali	pag.151
Cap. 12	Le forme polinomiali delle $(Wn)_b$	pag.184

Il sale, certo, è buono; ma se anche il
sale diventa insipido, con che cosa
si darà sapore?

1. DIVISIBILITA'

1.1 Premesse

In matematica il concetto di divisibilità è legato alla possibilità di scomporre i numeri naturali nel prodotto di fattori.
Trovare i fattori primi dei numeri composti è per i matematici come trovare gli atomi che compongono la materia per i chimici. Ma, mentre per i chimici c'è una famosa tavola che elenca i mattoni con cui è costruita la materia, per i matematici, finora, non si è arrivati a tanto: non esiste una formula che consenta di elencare i numeri primi in successione all'infinito. E' per questo motivo che quando si scopre un nuovo grande numero primo c'è aria di festa.
Per la comprensione dei concetti che saranno esposti in questo volume è essenziale tenere conto delle seguenti

Definizioni

Un numero naturale n si dice:
- composto, se si può scrivere come prodotto di fattori diversi da 1 e da se stesso;
- primo, se non è scomponibile nel prodotto di fattori diversi da 1 e da se stesso.

I numeri naturali composti si dicono multipli dei fattori in cui sono scomponibili, oppure divisibili per i loro fattori.
Ogni numero naturale è divisibile per 1 e per se stesso e multiplo di se stesso.
Il numero 0 è multiplo di ciascun numero naturale.
Nessun numero è divisibile per 0.

[1.1e1] - Esempio

Il numero naturale 35 è composto, perché si può scomporre nel prodotto di fattori: $35 = 5 \cdot 7$
quindi diremo che 35 è multiplo di: 1; 5; 7; 35 oppure che 35 è divisibile per 1; 5;7;35

[1.1e2] - Esempi

- Il numero 17 è primo perché non si può scomporre nel prodotto di fattori. L'unico modo di scriverlo in forma di prodotto è questo:

$$17 = 1 \cdot 17$$

ma il fattore 1 non lo scompone e 17 rimane invariato.
Come per ogni numero primo, si dice che 17 è divisibile solo per 1 e per se stesso.

- Per qualsiasi valore del numero n, si avrà sempre l'uguaglianza:

$$0 \cdot n = 0$$

ne segue che 0 è multiplo di 17 e di ogni altro numero intero.

Nella prima parte di questa trattazione ci occuperemo di un gruppo ristretto di numeri primi e precisamente di quei pochi numeri primi facilmente riconoscibili come fattori di numeri composti.
Il nostro impegno sarà diretto principalmente alla risposta della seguente domanda:
"In che modo è possibile stabilire se un numero naturale n è multiplo di un numero primo p assegnato?"

La risposta più immediata a questa domanda, valida per tutti i numeri naturali, è quella di eseguire la divisione di n per p: se si ottiene un quoziente esatto si concluderà che n è multiplo di p.
In questo caso il risultato è ancora un numero naturale e il resto della divisione è 0.
Alcune volte tuttavia la divisione non è necessaria.
Infatti, come vedremo in seguito, esistono dei semplici criteri di divisibilità che ci faranno riconoscere rapidamente i multipli dei numeri primi:

$$2 \; ; \; 3 \; ; \; 5 \; ; \; 7 \; ; \; 11 \; ; \; 13 \; ; \; 101$$

Successivamente indagheremo in modo più generale sulla divisibilità per gli altri numeri primi.
E' opportuno specificare che un criterio di divisibilità è efficace se ha una caratteristica fondamentale: deve essere di una semplicità tale da risparmiarci l'uso della calcolatrice, o, quanto meno, le sue

procedure di calcolo devono essere più rapide di quelle della divisione.

I manuali di scuola riportano i criteri di divisibilità per i numeri primi 2 , 3 , 5 e 11 saltando abitualmente il 7.
Chi come me ha insegnato matematica si sarà trovato quanto meno a disagio dovere riferire che per questo numero primo non c'è un valido criterio di divisibilità. Per rendere la didattica più fluida e organica sarebbe auspicabile invece una continuità nella sequenza dei numeri primi iniziali, stabilendo un criterio di divisibilità per 7 e, possibilmente, anche per 13.
Certamente saranno stati molti, e tra questi anch'io, coloro che hanno tentato di colmare questo vuoto. Spero che il criterio di divisibilità per 7 che io propongo sia apprezzabile, anche perché riserva qualche bella sorpresa: consente di prendere due piccioni, anzi tre, con una fava soltanto.
Da questo tentativo iniziale si sviluppa progressivamente una ricerca più ampia, estesa ad altri numeri primi; la trattazione di questo volume ne rispecchia la sequenza cronologica.

Espongo qui di seguito due criteri generali di divisibilità e quelli specifici per i numeri primi: 2 , 3 , 5 , 7, 11 , 13 , 101.

1.2 Criteri generali di divisibilità

Questi due criteri valgono per tutti i numeri primi, esclusi il 2 e il 5 per il secondo criterio, e consentono, in molti casi, di riconoscere facilmente alcuni fattori dei numeri composti in esame.

[1.2a] - Dato il numero naturale n, se è possibile staccare le sue cifre in modo tale che tutti i numeri ottenuti siano multipli dello stesso numero primo p, ne seguirà che n è multiplo di p.

[1.2e1] - Esempio
Esaminiamo 1703417.
Staccando opportunamente le cifre, i numeri che si ottengono sono tutti multipli di 17:

1703417 ⟶ 17.0.34.17

Quindi 1703417 è multiplo di 17.

[1.2b] - Dato il numero naturale n, che non sia multiplo né di 2 né di 5, se è possibile staccare le sue prime cifre, o le sue ultime cifre, in gruppi di multipli di uno stesso numero p e non sarà invece possibile formare un multiplo di p con le rimanti cifre, ne seguirà che n non è multiplo di p.

[1.2e2] - Esempio
Esaminiamo 19037
Staccando opportunamente le cifre:

19.0.37

deduciamo immediatamente che questo numero non è multiplo né di 19 né di 37.
Infatti le prime cifre formano due multipli di 19, mentre le rimanenti non formano un multiplo di 19.
Come pure, le ultime cifre formano due multipli di 37 e le prime no.

1.3 Criterio di divisibilità per 2

Il numero 2 è molto particolare: i suoi multipli costituiscono l'insieme dei numeri pari; in contrapposizioni, quelli che non sono multipli di 2 si dicono dispari, per cui un numero naturale o è pari o è dispari.
Basandoci su questa suddivisione dell'insieme N, facciamo la stessa cosa con l'insieme C delle cifre: quelle che coincidono con i multipli di 2 si dicono cifre pari, le rimanenti si dicono cifre dispari.
Si formano in questo modo due sottoinsiemi di C: l'insieme P delle cifre pari e l'insieme D delle cifre dispari:

$$P = \{0\text{-}2\text{-}4\text{-}6\text{-}8\}$$
$$D = \{1\text{-}3\text{-}5\text{-}7\text{-}9\}$$

Fatte queste premesse, enunciamo il noto criterio di divisibilità:

[1.3a] - Per riconoscere se un numero naturale n è divisibile per 2 basta osservare la sua ultima cifra: soltanto se questa è pari, il numero n è divisibile per 2.

[1.3e1] - Esempi
Dati i numeri 23178 e 246081, ci accorgiamo subito che il primo è pari perché termina con 8 che è una cifra pari, mentre il secondo è dispari perché la sua ultima cifra è 1.
Quindi solo 23178 è divisibile per 2.

1.4 Criterio di divisibilità per 3

Anche i multipli del 3 hanno delle caratteristi particolari che ci consentono un semplice criterio di divisibilità.

[1.4a] - Per stabilire la divisibilità per 3 di un numero intero n è sufficiente addizionare le sue cifre: se la somma è 3 o 6 o 9, il numero n è multiplo di 3.
(Nel caso in cui la somma sia un numero con più di una cifra, si potrà reiterare il procedimento fino ad ottenere una cifra soltanto).
Per semplificare i calcoli, grazie ai criteri generali di divisibilità e alla proprietà associativa dell'addizione, si possono eliminare le cifre, anche non vicine, la cui somma è 3 o 6 o 9.

[1.4e1] - Esempi
Stabiliamo se sono divisibili per 3 i numeri 8575878 e 1380584 .

- Addizioniamo le cifre del primo:

$$8+5+7+5+8+7+8=48$$

Reiteriamo il procedimento:

$$4+8=12 \quad ; \quad 1+2=3$$

Poiché la somma finale è 3,
8575878 è multiplo di 3.
Infatti: $8575878 = 3 \cdot 2858626$

- Il secondo numero invece non è multiplo di 3.
Infatti, eliminando le cifre 3 e 0 e le coppie: (1+8) e (5+4), rimane soltanto 8 che non è multiplo di 3.

$$1380584 = 3 \cdot 460194 + 2$$

1.5 Criterio di divisibilità per 5

Come avremo occasione di vedere meglio in seguito, il 5 e il 2 hanno in comune una caratteristica che non ha nessun altro numero primo: ciascuno dei due è sottomultiplo di 10 e, poiché la nostra numerazione è a base 10, ciò determina un criterio di divisibilità molto semplice, valido simultaneamente per entrambi.

[1.5a] - Dato un numero intero n qualsiasi, la sua divisibilità per 2 e per 5 è stabilita dalla sua ultima cifra: se questa è 2 o 4 o 6 o 8, n è multiplo di 2; se è 5, n è multiplo di 5; se è 0, n è multiplo sia di 2 sia di 5. Negli altri casi n non è multiplo né di 2 né di 5.

Ma ecco qui di seguito il criteri di divisibilità specifico del 5.

[1.5b] - Per riconoscere se un numero intero n è divisibile per 5 basta osservare la sua ultima cifra: soltanto se questa è 0 oppure 5, il numero n è divisibile per 5.

[1.5e1] - Esempi
Stabiliamo se sono divisibili per 5 i numeri: 125, 910 e 5555551.

- 125 è multiplo di 5, perché termina con 5;
- 910 è multiplo di 5, perché termina con 0;
- 5555551 non è multiplo di 5, perché non termina né con 5 né con 0.

1.6 Criterio di divisibilità per 7

Al numero 7 associamo altri due numeri primi: 13 e 11. Per tutti e tre suddividiamo la spiegazione dei loro criteri di divisibilità in due fasi: in un primo tempo prenderemo in esame i numeri con tre cifre soltanto; successivamente i criteri di divisibilità saranno estesi agli interi con una qualsivoglia quantità di cifre.

Iniziamo con il numero primo 7.

[1.6a] - Dato un numero n di tre cifre, si elimini quella che delle due cifre agli estremi è più piccola: si sottragga questa cifra a quella maggiore e si addizioni invece a quella al centro.
Se si forma un multiplo di 7, anche il numero n di partenza è multiplo di 7; viceversa, se non si forma un multiplo di 7, nemmeno il numero di partenza n lo è.

[1.6e1] - Esempio
Stabiliamo se 259 è divisibile per 7.

- La cifra più piccola agli estremi di 259 è 2.
- Si elimini la cifra 2,
- si addizioni 2 alla cifra 5,
- si sottragga 2 alla cifra 9.

$$\begin{array}{rr} 5+ & 9- \\ 2 & 2 \\ \hline 7 & 7 \end{array} \qquad 259 \longrightarrow 77$$

Poiché si forma il numero 77,
che è un multiplo di 7, deduciamo che anche 259 è multiplo di 7.

Infatti: $259 = 7 \cdot 37$

[1.6e2] - Esempi
Stabiliamo se 581 e 409 sono divisibili per 7.

- 581 è divisibile per 7, perché, applicando il criterio di divisibilità, si ottiene 49 che è multiplo di 7.

$$\begin{array}{cc} 5- & 8+ \\ 1 & 1 \\ \hline 4 & 9 \end{array} \qquad 581 \longrightarrow 49$$

- 409 invece non è divisibile per 7, perché ad esso corrisponde il numero 45 che non è multiplo di 7.

$$\begin{array}{cc} 0+ & 9- \\ 4 & 4 \\ \hline 4 & 5 \end{array} \qquad 409 \longrightarrow 45$$

1.7 Criterio di divisibilità per 13

Il criterio descritto per il 7 rafforza la sua validità quando ci proponiamo di stabilire un criterio di divisibilità anche per il 13. Ebbene, il criterio di divisibilità per 13 è identico al precedente! La spiegazione di questa coincidenza sarà data in seguito.

[1.7a] - Dato un numero n qualsiasi di tre cifre, si elimini quella che delle due cifre agli estremi è più piccola: si sottragga questa cifra a quella maggiore e si addizioni invece a quella al centro.
Se si forma un multiplo di 13, anche il numero di partenza n è multiplo di 13; viceversa, se non si ottiene un multiplo di 13, nemmeno il numero di partenza n lo è.

[1.7e1] - Esempi
Stabiliamo la divisibilità per 13 di: 949 , 273 , 623 e 601

- Al 949 corrisponde 13, quindi è divisibile per 13.
  Possiamo stabilire nello stesso tempo che non è invece divisibile per 7.

$$\begin{array}{c} -+ \\ 949 \\ 99 \\ \hline 13 \end{array} \qquad 949 \longrightarrow 13 \qquad 949 = 13 \cdot 73$$

- Al 273 corrisponde 91 che è multiplo sia di 13 sia di 7, quindi anche 273 è multiplo sia di 13 sia di 7.

$$\begin{array}{r} +\ - \\ 273 \\ 22 \\ \hline 91 \end{array} \qquad 273 \longrightarrow 91 \qquad 273 = 3 \cdot 7 \cdot 13$$

- Al 623 corrisponde 35, quindi non è multiplo di 13, è invece multiplo di 7.

$$\begin{array}{r} -\ + \\ 623 \\ 33 \\ \hline 35 \end{array} \qquad 623 \longrightarrow 35 \qquad 623 = 7 \cdot 89$$

- Al 601 corrisponde 51, quindi non è multiplo di 13 e nemmeno di 7.

$$\begin{array}{r} -\ + \\ 601 \\ 11 \\ \hline 51 \end{array} \qquad 601 \longrightarrow 51 \qquad 601 \text{ è numero primo}$$

1.8 Criterio di divisibilità per 11

[1.8a] - Dato un numero naturale n di 3 cifre, si addizionino le cifre degli estremi e si sottragga poi al risultato la cifra al centro: se la differenza è un multiplo di 11, è tale anche n; viceversa, se non si ottiene un multiplo di 11, non lo è nemmeno n.

[1.8e1] - Esempi

Stabiliamo se sono divisibili per 11 i numeri: 847 e 593.

Diamo un valore negativo alla cifra al centro ed eseguiamo la somma algebrica delle tre cifre, in entrambi i numeri.

$$847 \longrightarrow 8-4+7=11$$
$$593 \longrightarrow 5-9+3=-1$$

- a 847 corrisponde 11, quindi è multiplo di 11. Infatti: $847 = 11^2 \cdot 7$.
- a 593 corrisponde -1, quindi non è multiplo di 11. Infatti è un numero primo.

1.9 Criterio unico di divisibilità per 7, per 11 e per 13

Come abbiamo potuto constatare, per i numeri interi a tre cifre c'è un unico criterio di divisibilità per 7 e per 13; ma è possibile stabilire un criterio di divisibilità per 7 e per 13 anche per quelli con più di tre cifre ?
Ebbene, si! Anzi, in questo caso, i piccioni da prendere con una fava soltanto diventano tre, perché è possibile stabilire un criterio unico di divisibilità per 7 , 11 e 13.

[1.9a] - Il criterio unico di divisibilità consiste nell'associare al numero intero n, formato da una qualsiasi quantità di cifre, un'altro intero di tre cifre soltanto, seguendo i passaggi indicati di seguito.

1) - Si dividano le cifre di n in classi, staccandole a gruppi di tre, da destra verso sinistra, oppure da sinistra verso destra. Si aggiungano eventualmente degli zeri, affinché anche l'ultimo gruppo sia formato da tre cifre.
2) - si addizionino tra loro le classi di posto pari;
3) - si addizionino tra loro le classi di posto dispari;
4) - si calcoli la differenza tra le due somme;
5) - se la differenza è formata da più di 3 cifre si ritorni al punto 1.

Alla fine si otterrà un numero con non più di tre cifre, al quale si applicherà il criterio di divisibilità per 11 e, in modo unitario, quello per 7 e per 13, così come è stato descritto in: *[1.8a]* , *[1.6a]* , *[1.7a]*.

Quanto sia agevole e utile applicare questo criterio lo si dedurrà dagli esempi qui di seguito riportati.

[1.9e1] - Esempi
Stabiliamo la divisibilità per 7, per 11 e per 13 dei numeri:
41041 ; 8029 ; 53833 ; 8014003

- Sia che stacchiamo le cifre di 41041 da destra verso sinistra che da sinistra verso destra, la differenza tra le due classi è 0.

Cosicché al 41041 si può associare il numero 0, che è multiplo di ogni numero intero.
Deduciamo così che 41041 è multiplo sia di 7, sia di 11, sia di 13. Ricordando poi il 1° criterio generale di divisibilità, possiamo stabilire che è anche multiplo di 41.

Infatti: $41041 = 7 \cdot 11 \cdot 13 \cdot 41$

- Esaminiamo 8029.

Ci conviene staccare le cifre procedendo da destra verso sinistra.

$8.029 \rightarrow 29 - 8 = 21$

La differenza tra le due classi ottenute è 21, che è multiplo di 7, ma non di 11 e di 13, quindi anche 8029 è multiplo di 7, ma non di 11 e nemmeno di 13.

$8029 = 7 \cdot 31 \cdot 37$

Ricordando il 2° criterio generale di divisibilità, possiamo stabilire anche che questo numero non è multiplo neppure di 29.

- Esaminiamo 53833.

Staccando le cifre da sinistra verso destra, possiamo eseguire i calcoli rapidamente e stabilire che 53833 è multiplo di 13, ma non di 7 e nemmeno di 11.

$538.33 \rightarrow 538 - 330 = 208$

$208 \rightarrow 26$ (multiplo di 13, ma non di 7)

$208 \rightarrow 10$ (non è multiplo di 11)

$53833 = 13 \cdot 41 \cdot 101$

- Esaminiamo 134849.

$134.849 \rightarrow 715$

$715 \rightarrow 26 \Rightarrow$ 134849 è multiplo di 13, ma non di 7

$715 \rightarrow 11 \Rightarrow$ 134849 è multiplo di 11

$849 - 134 = 715$

$134849 = 11 \cdot 13 \cdot 23 \cdot 41$

- Esaminiamo 8014003.

8.014.003 ⟶ 3

8014003 = 2003 • 4001

La somma algebrica delle tre classi è 3, per cui 8014003 non è multiplo né di 7, né di 11, né di 13.

- Esaminiamo 7420035266745563:

7.420.035.266.745.563 ⟶ 462

462 ⟶ 28 ⇒ 7420035266745563 è multiplo di 7 e non di 13

462 ⟶ 0 ⇒ 7420035266745563 è multiplo di 11

563 +	745 +	1249 -
266	035	787
420	007	462
1249	787	

7.420.035.266.745.563 = 7 • 11 • 17 • 19 • 59 • 809 • 2309 • 2707

Riflettendo su questo criterio unico di divisibilità si deduce che:

[1.9b] - Ogni numero intero di 6, 12, 18, ..., 6•n,... cifre, tale da formare o classi contigue uguali, o classi simmetriche uguali rispetto ad una linea mediana, è multiplo contemporaneamente di 7, di 11 e di 13. (Si devono considerare classi di 3 cifre).

[1.9e2] - Esempi

In base al criterio descritto accanto, si nota subito che i numeri:

72|072 - 201|201 - 231.231|709.709 - 589.231.709|709.231.589 - 111.111.111|111.111.111 - 1|000.000.001 - 1.001.001|001.001.001

sono multipli sia di 7, sia di 11 sia di 13.

(Aggiungendo opportunamente degli zeri alla loro sinistra, anche i numeri:

- 072.072
- 000000001.000000001
- 001.001.001.001.001.001

si possono ritenere formati da 6•n cifre).

1.10 Criterio di divisibilità per 101

E' interessante riportare un criterio di divisibilità anche per 101, sia per l'estrema semplicità con cui si riconoscono i suoi multipli, sia, soprattutto, per le analogie con il criterio unico di divisibilità descritto prima al punto *[1.9a]*.

[1.10a] - Il metodo consiste nell'associare al numero intero n, formato da una qualsiasi quantità di cifre, un'altro intero di due cifre soltanto, seguendo i passaggi indicati di seguito.

1) - si stacchino le cifre di n a gruppi di due, da destra verso sinistra, oppure da sinistra verso destra, aggiungendo eventualmente uno zero, affinché anche l'ultimo gruppo sia formato da due cifre;
2) - si addizionino tra loro le classi di posto pari;
3) - si addizionino tra loro le classi di posto dispari;
4) - si calcoli la differenza tra le due somme;
5) - se la differenza ha più di due cifre si ritorni al punto 1.

Alla fine si otterrà un numero con non più di due cifre.
Soltanto se il risultato finale è 0, n è multiplo di 101; se invece è un qualunque altro numero di due cifre, n non è multiplo di 101.

[1.10e1] - Esempi
Verifichiamo la divisibilità per 101 dei numeri:
55651 ; 71791 ; 29813862861

- Applichiamo il criterio di divisibilità al numero 55651.

05.56.51 $\quad 51 + 05 = 56 \quad 56 - 56 = 00$

55.65.10 $\quad 55 + 10 - 65 = 0$

55651 = 19 • 29 • 101

Sia che stacchiamo le cifre da destra verso sinistra che da sinistra verso destra, la differenza tra le due classi è 0. Deduciamo così che 55651 è multiplo di 101.

- Applichiamo il criterio di divisibilità al numero 71791:

71.79.10 $\longrightarrow$ 2 $\Rightarrow$ 71791 non è multiplo di 101.
71791 = 17 • 41 • 103

- Applichiamo il criterio di divisibilità al numero 29813862861.

$2.98.13.86.28.61 \longrightarrow 0 \quad \Rightarrow \quad 29813862861$ è multiplo di 101

$29813862861 = 3^4 \cdot 23^2 \cdot 83^2 \cdot 101$

61 +	28 +	245-	02-
86	13	43	02
98	02	202	00
245	43		

Riflettendo su questo criterio unico di divisibilità si dedurrà che:

[1.10b] - Ogni numero intero di 4, 8,12, ..., $4 \cdot n$, ... cifre, tale da formare o coppie di cifre contigue uguali o coppie simmetriche uguali rispetto ad una linea mediana, è un multiplo di 101.

[1.10e2] - Esempi

In base al criterio descritto accanto, si nota subito che i numeri:

72.72 - 1.01.02.02.03.03.04.04.05.05

- 87.59.31.09.09.31.59.87
- 11.11.11.11.11.11.11.11.11.11
- 1.00.00.01 - 1.01.01.01.01.01.01.01

sono multipli di 101.

(Aggiungendo opportunamente degli zeri alla loro sinistra, anche i numeri:

- 01.01.02.02.03.03.04.04.05.05
- 01.00.00.01
- 01.01.01.01.01.01.01.01

si possono ritenere formati da $4 \cdot n$ cifre).

2.1 Proprietà fondamentali dei numeri composti

Vediamo adesso di capire come nascono i criteri di divisibilità descritti nel 1° capitolo.
Certamente andare in fondo alla questione è più interessante delle applicazioni, perché è la conoscenza delle strutture dei numeri che ci consente di costruire le loro carte d'identità.
Per dimostrare la validità dei procedimenti descritti, per prima cosa si deve tenere conto di alcune proprietà fondamentali dei numeri composti; esse, nella loro semplicità, stanno alla base, sia di questa trattazione, sia dello studio delle congruenze.

[2.1a] - Se a e b sono multipli di uno stesso numero naturale n, anche la loro differenza è un multiplo di n.

Infatti:

se $a = c \cdot n$ e se $b = d \cdot n$

(sia $a > b$)

si avrà:

$$a-b = c \cdot n - d \cdot n = (c-d) \cdot n$$

[2.1b] - Se il numero a non è multiplo di b, la differenza tra a e un qualsiasi intero m, multiplo di b, non è un multiplo di b.

Infatti:

accertato che a sia primo, o che non abbia b tra i suoi fattori, e che m invece sia un multiplo di b, supponiamo che la differenza a-m sia un multiplo di b:

$$a-m = b \cdot f$$

[2.1e1] - Esempio

Dati i numeri 1891 e 427, entrambi multipli di 61, calcoliamo la loro differenza:

$$1891 - 427 = 1464$$

Dalle uguaglianze:

$$1891 = 31 \cdot 61 \ ; \ 427 = 7 \cdot 61$$

ne segue quest'altra:

$$1891 - 427 = 61 \cdot (31-7) = 61 \cdot 24$$

Come era previsto, il risultato è ancora un multiplo di 61.

[2.1e2] - Esempio

Dato il numero 51 che non è multiplo di 13, sottraiamo da esso un multiplo di 13, ad esempio 39:

$$51-39 = 12$$

Come ci si aspettava, si è ottenuto un numero che, come 51, non è multiplo di 13.

posto $m = b \cdot c$ e sostituendo, si avrà:

$$a - b \cdot c = b \cdot f \implies a = b \cdot f + b \cdot c = b \cdot (f + c)$$

si arriva così alla conclusione contraddittoria che a è multiplo di b.
Resta quindi dimostrato che a-m non può essere un multiplo di b.

[2.1c] - Dato un numero naturale n, se ad alcune sue cifre che formano un multiplo di b si sostituisce un'uguale quantità di zeri, la condizione di divisibilità per b rimarrà invariata.

Questa è una conseguenza delle precedenti proprietà *[2.1a]* e *[2.1b]*.
Infatti, sostituire degli zeri alle cifre di n che formano un multiplo di b, equivale a sottrarre ad n un multiplo di b.

[2.1e3] - Esempio
Sia dato il numero 23597, multiplo di 7.
Osservando che alcune cifre di questo numero formano due multipli di 7 : il 35 e il 7, sottraiamo prima 3500 e poi 7, entrambi multipli di 7. Otteniamo così 20090, dove al posto delle cifre 3, 5 e 7 di 23597 compaiono altrettanti zeri.
Come era nelle nostre aspettative, il risultato 20090 è ancora un multiplo di 7.

Quindi, con questa sostituzione, se n è multiplo di b si otterrà ancora un multiplo di b; se invece n non è multiplo di b, non si otterrà un multiplo di b.

[2.1e4] - Esempio
Scomponiamo nel prodotto di fattori primi il numero 17037.

Osservando che le sue prime due cifre formano il numero 17, sostituiamo ad esse due zeri. Poiché si ottiene 37, che non è multiplo di 17, deduciamo che nemmeno 17037 è multiplo di 17. In modo analogo deduciamo che 17037 non è multiplo neanche di 37.
Applicando il criterio unico di divisibilità, constatiamo rapidamente che non è multiplo nemmeno di 7, di 11 e di 13.
Accertato che invece è multiplo di 3, eseguiamo una prima scomposizione: $17037 = 3^3 \cdot 631$
Verificato che 631 non è multiplo né di 19 né di 23, concludiamo che certamente questo è un numero primo. Cosicché la scomposizione già fatta non subisce variazioni.

2.2 Come si deducono i criteri generali di divisibilità

Tenuto conto delle proprietà fondamentali dei numeri composti, si capisce ora che i due criteri generali di divisibilità *[1.2a]* e *[1.2b]* del capitolo precedente non sono altro che loro applicazioni. Vediamole.

1ª Applicazione

Dato come esempio il numero 220440121, ci si accorge immediatamente che tutte le sue cifre si possono staccare in modo da formare multipli di 11: 22.0.44.0.121.
Applicando la proprietà fondamentale *[2.1c]*, a ciascuno di questi gruppi si può sostituire una quantità uguale di zeri.
Poiché si ottiene 0, che è multiplo di 11, anche il numero di partenza 220440121 è multiplo di 11.

Infatti: $220440121 = 11 \cdot 4099 \cdot 4889$

2ª Applicazione

Dato il numero 3119, staccando le sue cifre a due a due: 31.19, si formano multipli di due numeri diversi, per cui è immediato dedurre che non è multiplo né di 31 né di 19.
Infatti, sostituendo due zeri a 31 si ottiene il numero 19 che non è multiplo di 31; sostituendo due zeri a 19 si ottiene invece 3100 che non è multiplo di 31. Si nota anche subito che non è multiplo di 11.
3119 è un numero primo.

Attenzione a non applicare il criterio di divisibilità *[1.2b]* ai multipli di 2 e di 5: per questi numeri esso non è valido.
Infatti: $1725 = 3 \cdot 5^2 \cdot 23$; $372 = 93 \cdot 2^2$.

2.3 Come si deduce il criterio unico di divisibilità per 7 e per 13, nel caso dei numeri formati da tre cifre soltanto.

Il criterio unico di divisibilità per 7 *[1.6a]* e per 13 *[1.7a]* dei numeri interi a tre cifre è anch'esso una applicazione delle proprietà fondamentali dei numeri composti: il suo utilizzo prevede la sottrazione di un multiplo di 91 dal numero dato.
La scelta del 91 è stata decisa in base alla considerazione che questo è

il minimo comune multiplo di 7 e di 13, cosicché il procedimento vale contemporaneamente per entrambi.

Rivediamo i calcoli degli esempi *[1.6e1], [1.6e2] e [1.7e1]*

Applicando i criteri di divisibilità descritti, praticamente:

- al numero 259 abbiamo sottratto 182, multiplo di 91. $(182 = 2 \cdot 91)$
- al numero 409 abbiamo sottratto 364, multiplo di 91. $(364 = 4 \cdot 91)$
- al numero 949 abbiamo sottratto 819, multiplo di 91. $(819 = 9 \cdot 91)$

259-	409-	949-
182	364	819
077	045	130

A dire il vero l'applicazione delle proprietà fondamentali è stata semplificata nei procedimenti di calcolo.

Per renderci conto in che modo abbiamo sottratto dei multipli di 91 nei nostri esempi dobbiamo porci le seguenti domande:

- si può eseguire la sottrazione in modo diverso da quello usuale?
- si possono scrivere i numeri del sistema decimale in modo diverso da come li scriviamo abitualmente?

La risposta è affermativa in entrambi i casi.

Ad esempio, possiamo scrivere 91 in quest'altra forma:

$$91 \text{ ----------> } 1\overline{1}1$$

Dove $1\overline{1}1$ rappresenta un numero misto, cioè in parte positivo e in parte negativo.

Per proseguire nelle nostre spiegazioni è necessario soffermarci sul concetto di numero misto e su come si possono eseguire le operazioni fondamentali con i numeri naturali scritti in questa forma.

2.4 I numeri misti

Nel sistema di numerazione decimale le unità vengono raggruppate a dieci a dieci e ogni gruppo di dieci unità forma una unità di ordine superiore. Questo ordine è individuato dal posto che ciascuna cifra occupa, andando da destra verso sinistra.

Consideriamo ad esempio il numero: 53468

La prima cifra indica 8 unità, la seconda 6 decine, la terza 4 centinaia,

la quarta 3 migliaia, la quinta 5 decine di migliaia.
Essendo il sistema di numerazione decimale strutturato in questo modo, il numero dato si può scrivere nella forma polinomiale:

$$53468 = 5 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10^1 + 8 \cdot 10^0$$

Più in generale, un qualsiasi numero naturale n con k + 1 cifre, avrà la seguente forma polinomiale:

$$N = a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + , \ldots , + a_1 10 + a_0$$

Rispondiamo adesso a questa domanda:

" Quante unità mancano al numero 53468 affinché le decine siano 7, anziché 6 ?"

Per indicare che ne mancano 2, conveniamo di scrivere così: $5347\overline{2}$ dove il 2 soprassegnato indica una cifra di valore negativo.
La corrispondente scrittura polinomiale sarà:

$$5347\overline{2} = 5 \cdot 10^4 + 3 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10^1 - 2 \cdot 10^0$$

E' chiaro che le due forme di scritture sono equivalenti perché rappresentano la stessa quantità:

$$53468 \equiv 5347\overline{2}$$

Pertanto, nella lettura dei numeri, si dovranno tenere presenti queste

definizioni

Un numero naturale,
scritto con il segno - davanti alla sua prima cifra si dice negativo;
scritto senza alcun segno o con il segno + davanti alla sua prima cifra si dice positivo;
scritto con alcune cifre sopra segnate si dice misto (le cifre sopra segnate sono negative, le altre positive).

Proprietà dei numeri misti

[2.4a] - Ogni numero intero si può trasformare in un numero misto, e, viceversa, ogni numero misto si può trasformare in uno positivo o in uno negativo.

$7 = 1\overline{3}$; $193 = 2\overline{1}3$; $3\overline{6} = 24$; $2\overline{3}5 = 175$; $\overline{6}41 = -559$

[2.4b] - Ogni numero misto ha il valore assoluto uguale al numero misto che si ottiene mutando di segno ciascuna delle sue cifre.

Esempio: $|\overline{6}41| = |64\overline{1}|$ $\qquad \overline{6}41 = -(64\overline{1}) = -559$

[2.4c] - Addizioni e sottrazioni coi numeri misti.

Per addizionare due o più numeri misti basta metterli in colonna e seguire le regole delle operazioni algebriche, tenendo conto del segno di ciascuna cifra. Se due cifre sono di segno uguale, si addizionano i loro valori assoluti e si dà al risultato lo stesso segno; se le due cifre sono di segno opposto, si calcola la differenza dei loro valori assoluti e si dà al risultato il segno della maggiore. Quando c'è un riporto, si deve tenere conto del suo segno.

Anche per la sottrazione si seguono le regole delle operazioni algebriche: sottrarre equivale ad addizionare al primo numero l'opposto del secondo.

[2.4e1] - Esempi

$437 + 21\overline{3} = 644$

$42\overline{6} + 27\overline{5} = 68\overline{1} = 679$

$2\overline{3}1\overline{1} + 10\overline{57} + 3\overline{864} =$
$= 5\overline{212} = 4788$

$437+$	$42\overline{6}+$	$2\overline{3}1\overline{1}+$
$21\overline{3}$	$27\overline{5}$	$10\overline{57}$
644	$68\overline{1}$	$3\overline{864}$
		$5\overline{212}$

$701\text{-}163 = 6\overline{62} = 538$

$8\overline{34} - 41\overline{3} = 4\overline{41} = 359$

$701-$	$8\overline{34}-$
163	$41\overline{3}$
$6\overline{62}$	$4\overline{41}$

Chiarito il concetto, adesso sarà semplice capire in che modo il numero positivo 91 si può trasformare in un numero misto:

$$91 \longrightarrow 1\overline{1}1$$

Nella tabella sono elencati i primi dieci multipli di 91 scritti in forma mista.

91	$= 1\overline{1}1$
182	$= 2\overline{2}2$
273	$= 3\overline{3}3$
364	$= 4\overline{4}4$
455	$= 5\overline{5}5$
546	$= 6\overline{6}6$
637	$= 7\overline{7}7$
728	$= 8\overline{8}8$
819	$= 9\overline{9}9$
910	$= 1\overline{1}10$
...	... ...

[2.4 tab1]

L'osservazione della tabella *[2.4 tab1]* ci fa notare una caratteristica particolare dei primi multipli di 91, scritti in forma mista: essi sono formati da tre cifre uguali nei loro valori assoluti.
Vediamo subito quali vantaggi ne derivano.
Ritorniamo agli esempi *[1.6e1]* e *[1.7e1]* del 1° capitolo.

- Consideriamo il numero 259.

Per stabilire simultaneamente se è multiplo di 7 e di 13, applicando le proprietà dei numeri composti, sottraiamo da esso un multiplo di 91 a tre cifre.
Ricorrendo ai numeri misti, il numero che ci conviene scegliere come sottraendo è facilmente individuato, è $2\overline{2}2$.
La sottrazione tra 259 e il numero misto $2\overline{2}2$ è di immediata esecuzione: si ottiene come risultato 77, che è multiplo di 7 , ma non di 13.
Concludiamo quindi che anche 259 è multiplo di 7, ma non di 13 .

- Consideriamo il numero 949.

A questo numero conviene sottrarre il multiplo di 91 che ha come ultima cifra 9, cioè $9\overline{9}9$.
Eseguendo l'addizione algebrica tra 949 e $9\overline{9}9$ si ottiene 130.
Concludiamo quindi che 949 è multiplo di 13, ma non di 7.

- Consideriamo il numero 601.

A questo numero conviene addizionare algebricamente $1\overline{1}1$.
Poiché si ottiene 510, che non è multiplo né di 7 né di 13, concludiamo che anche 601 non è multiplo né di 7 né di 13 .

259-	949-	601-
$2\overline{2}2$	$9\overline{9}9$	$1\overline{1}1$
077	130	510

2.5 Come si deducono il criterio unico di divisibilità per 7, per 11 e per 13 *[1.9a]* e il criterio di divisibilità per 101 *[1.10a]* ?

Per dedurre questi criteri è necessario fare uno studio preliminare sulle congruenze.
Questo è ciò che ci accingiamo a fare nel prossimo capitolo.

3.1 Definizioni

Ritorniamo al concetto di divisibilità esposto nel paragrafo 1.1 ed estendiamolo a tutti i numeri interi. Se non teniamo conto dei segni, le definizioni fatte in N saranno valide in tutto l'insieme Z degli interi relativi.

Per stabilire se un intero z sia o non sia divisibile per un numero naturale n, non è strettamente necessario eseguire la divisione, è invece sufficiente accertare qual è il suo resto. A questo fine perseguiremo l'obiettivo di ricavare le relazioni che legano tra loro gli interi che danno resti uguali quando eseguiamo le loro divisione elementari per lo stesso numero naturale n.

Definizioni

- Si dice divisione elementare di un intero relativo z per un intero positivo n, quella che da il resto maggiore o uguale a zero e minore del divisore n. (Cioè quella con il minimo resto positivo)
- Diremo che due interi a e b sono congrui tra loro modulo n, se le loro divisioni elementari, per lo stesso numero naturale n, danno resti uguali.

[3.1a] - Eseguendo le divisioni elementari degli interi a e b per il numero naturale n, si otterranno le seguenti uguaglianze:

$a = p \cdot n + r_1 \quad \text{con} \quad 0 \le r_1 < n$

$b = q \cdot n + r_2 \quad \text{con} \quad 0 \le r_2 < n$

Se accade che $r_1 = r_2$
denoteremo tale circostanza con la seguente scrittura:

$$a \equiv b \pmod{n}$$

e diremo:
a è congruo a b modulo n.

[3.1e1] - Esempio

Dati gli interi 17 e 23, stabiliamo se sono congrui tra loro rispetto al modulo 3.

Eseguiamo le loro divisioni elementari per 3:

$$17 = 5 \cdot 3 + 2$$
$$23 = 7 \cdot 3 + 2$$

Poiché i resti sono uguali, diciamo che 17 e 23 sono congrui tra loro secondo il modulo 3 e scriviamo:

$$17 \equiv 23 \pmod{3}$$

[3.1e2] - Esempio
Dati gli interi -67, -31 e 139 stabiliamo se sono congrui tra loro rispetto al modulo 17.

Eseguiamo le loro divisioni elementari per 17:

$-67 = -4 \cdot 17 + 1$
$-31 = -2 \cdot 17 + 3$
$139 = 8 \cdot 17 + 3$

Dalle uguaglianze ottenute si accorgiamo che soltanto -31 e 139 sono congrui tra loro secondo il modulo 17:

$-31 \equiv 139 \pmod{17}$

$-67 \not\equiv -31 \pmod{17}$

$-67 \not\equiv 139 \pmod{17}$

Ia divisione elementare, così come l'abbiamo definita, ci consente di ottenere il minimo resto positivo.
Tuttavia, similmente a quanto abbiamo convenuto con i numeri misti, potrebbe essere utile calcolare un quoziente diverso da quello della divisione elementare ed ottenere, di conseguenza, un resto che non è il minimo positivo.
Facciamo due esempi.

[3.1e3] - Consideriamo la divisione di 29 per 4:

$29 = 7 \cdot 4 + 1$
$29 = 8 \cdot 4 - 3$
$29 = 6 \cdot 4 + 5$

- La prima uguaglianza si ottiene dalla divisione elementare e soddisfa la richiesta di ottenere il minimo resto positivo.
- La seconda uguaglianza ci consente di stabilire quante unità mancano al quoziente successivo a quello della divisione elementare. Questa divisione soddisfa la richiesta di trovare il resto negativo, minimo in valore assoluto: $|-3| < 4$
- La terza uguaglianza è un esempio di divisione con resto maggiore del divisore.

[3.1e4] - Consideriamo le divisioni di -19 per 3:

-19 = -7•3+2 minimo resto positivo: $0 \leq 2 < 3$

-19 = -6•3-1 minimo resto negativo in valore assoluto: $|-1| < 3$

-19 = 1•3-22 resto maggiore del divisore in valore assoluto: $|-22| > 3$

Definizione

Si dice

minimo resto della divisione

tra un numero intero z e un numero naturale n quello il cui valore assoluto è compreso tra 0 e n/2.

$$-\frac{n}{2} \leq r \leq \frac{n}{2}$$

Pertanto, tenuti presenti i due esempi fatti prima, il minimo resto può essere o un numero positivo o un numero negativo:

- nel primo esempio *[3.1e3]* il minimo resto della divisione tra 29 e 4 è 1 e coincide col minimo resto positivo;
- nel secondo esempio *[3.1e4]* il minimo resto della divisione tra -19 e 3 è -1 e coincide con il resto negativo, minimo in valore assoluto.

Definizioni

Si dice

- *sistema completo di resti modulo n,*

l'insieme di tutti i resti che si possono ottenere eseguendo la divisione elementare di un qualsiasi intero z per n.

Pertanto esso è costituito dai primi n numeri interi positivi:

0, 1, 2, ... , (n-1)

Se ai numeri che in questo insieme superano il valore n/2 sostituiamo i minimi resti, otterremo il

- *sistema minimo completo di resti modulo n.*

[3.1e5] - Stabiliamo qual è il sistema completo dei minimi resti relativi al modulo 13.

Se eseguiamo la divisione elementare di un qualsiasi numero intero z per 13 il resto sarà uno dei 13 elementi distinti dell'insieme:

$$A=\{0\ ,\ 1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\ ,\ 7\ ,\ 8\ ,\ 9\ ,\ 10\ ,\ 11\ ,\ 12\}$$

A partire da questi elementi, se vogliamo ottenere l'insieme dei minimi resti, sarà sufficiente procedere in questo modo:

- lasciamo invariati i resti minori di n/2, cioè quelli da 0 a 6.
- calcoliamo le differenze tra ciascun resto maggiore di n/2 e 13:

$7-13=-6\ ;\ 8-13=-5\ ;\ 9-13=-4\ ;\ 10-13=-3\ ;\ 11-13=-2\ ;\ 12-13=-1$

Cosicché, il sistema completo dei minimi resti, modulo 13, è:

$$S=\{0\ ,\ 1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\ ,\ -6\ ,\ -5\ ,\ -4\ ,\ -3\ ,\ -2\ ,\ -1\}$$

3.2 Alcune propietà delle congruenze

Dalle definizioni date sulle congruenze ricaviamo alcune proprietà, indispensabili per la comprensione della nostra trattazione.

[3.2a] - Se due numeri interi a e b sono congrui tra loro, secondo il modulo n, la loro differenza è un multiplo di n.

Infatti, data la congruenza

$$a \equiv b \pmod{n}$$

le divisioni elementari di a e di b per n ci daranno le uguaglianze:

$$a = c\cdot n + r$$
$$b = d\cdot n + r$$

Per la definizione data sulle congruenze, r ha lo stesso valore in entrambe le uguaglianze, per cui, sottraendo membro a membro, si avrà:

$$a-b = (c-d)\cdot n$$

Questa uguaglianza dimostra la nostra asserzione.

[3.2e1] - Esempio

Dati i numeri 36 e 15, le loro divisioni elementari per 7 ci danno le uguaglianze:

$$36=5\cdot 7+1$$
$$15=2\cdot 7+1$$

per cui essi sono congrui tra loro, rispetto al modulo 7:

$$36 \equiv 15 \pmod{7}$$

Calcolando la loro differenza, in accordo con le nostre aspettative, otteniamo un multiplo di 7:

$$36 - 15 = 21$$

E' valida anche la proposizione inversa:

[3.2b] - Se due numeri interi a e b sono tali che la loro differenza è un multiplo di n, ne segue che essi sono congrui tra loro secondo il modulo n.

Infatti, data l'uguaglianza

$$a - b = c \cdot n$$

dalle divisioni elementari di a e di b per n si otterranno le uguaglianze:

$$a = p \cdot n + r_1 \quad (\text{con } 0 \leq r_1 < n)$$

$$b = q \cdot n + r_2 \quad (\text{con } 0 \leq r_2 < n)$$

Sottraendo membro a membro, si avrà:

$$a-b = (p-q) \cdot n + (r_1 - r_2)$$

Considerato che i due resti sono positivi e minori di n, il valore assoluto della loro differenza sarà necessariamente minore di n.

[3.2e2] - Esempio

Dati i numeri 41 e 19, calcoliamo la loro differenza:

$$41-19 = 22 = 2 \cdot 11$$

Da qui si deduce che 41 e 19 sono congrui tra loro secondo il modulo 11.

Infatti:

$$41 = 3 \cdot 11 + 8$$

$$19 = 11 + 8$$

quindi:

$$41 \equiv 19 \pmod{11}$$

Se ne deduce quindi che tale differenza non può essere diversa da 0, altrimenti, contradicendo l'ipotesi, a-b non sarebbe multiplo di n. Ciò vuol dire che $r_1 = r_2$, per cui è valida la congruenza:

$$a \equiv b \pmod{n}$$

Quest'ultima proposizioni è quella più pratica da usare per stabilire la congruenza tra due numeri.

Applichiamola per dimostrare le proprietà caratteristiche dei sistemi dei resti modulo n.

[3.2c] - Ciascun sistema dei resti modulo n è tale che due suoi qualsiasi elementi non sono mai congrui tra loro.

Per provare la validità di questa asserzione, basta pensare che la differenza tra due qualsiasi elementi di questo insieme è sempre minore di n, in valore assoluto, e mai zero.

[3.2d] - Un qualsiasi intero che non appartiene all'insieme A dei resti modulo n, è congruo ad uno solo di quelli che vi appartengono.

Infatti, se a è un intero qualsiasi, eseguendo la sua divisione elementare per n, si avrà un resto r_a che appartiene all'insieme A:

$$a = b \cdot n + r_a$$

dall'uguaglianza:

$$a - r_a = b \cdot n$$

ne consegue che:

$$a \equiv r_a \pmod{n}$$

[3.2e3]- Esempio

Calcolare a quale residuo modulo 5 è congruo 41.

Eseguiamo la divisione elementare:

$$41 = 8 \cdot 5 + 1$$

da qui segue che:

$$41 \equiv 1 \pmod{5}$$

L'intero a non può essere congruo a nessun altro residuo di A, perché altrimenti si avrebbe la congruenza tra due elementi di A, contrariamente a quanto abbiamo stabilito in *[3.2c]*.

[3.2e4] - Esempio

Mettiamo a confronto i numeri 29 e 13.

Eseguendo la divisione elementare tra di loro

$$29 = 2 \cdot 13 + 3$$

ne segue che:

$$29 \equiv 3 \pmod{13}$$

[3.2e5] - Esempio

Mettiamo a confronto i numeri 51 e 17.

Eseguendo la divisione elementare tra loro

$$51 = 3 \cdot 17 + 0$$

ne segue che:

$$51 \equiv 0 \pmod{17}$$

Se n è multiplo di p, il resto della loro divisione è zero, per cui è possibile enunciare una nuova definizione del concetto di divisibilità:

Un numero n si dice divisibile per p se è congruo a 0 modulo p.

$$n \equiv 0 \pmod{p} \qquad (\text{per } n = m \cdot p)$$

Il confronto tra i due insiemi A ed S dell'esempio *[3.1e5]* mostra che a ciascun elemento di A corrispondente un elemento in S. Più in generale possiamo enunciare la seguente proposizione.

[3.2e] - a ogni elemento r_A di A, sistema completo dei resti maggiore di n/2, corrisponde un elemento $r_S = r_A - n$ di segno negativo del sistema S dei minimi resti, secondo la relazione:

$$r_A \equiv r_A - n \pmod{n}$$

[3.2f] - La divisione elementare tra due interi n e p (con n > p) ci dà l'uguaglianza:

$$n = a \cdot p + r \qquad (0 \leq r < p)$$

Ne segue la congruenza:

$$n \equiv r \pmod{p}$$

Mentre la divisione con minimo resto negativo ci dà l'uguaglianza:

$$n = (a+1) \cdot p + (r-p) \qquad (|r - p| < p)$$

da cui segue:

$$n - (r-p) = (a+1) \cdot p$$

che implica quest'altra congruenza:

$$n \equiv r-p \pmod{p}$$

quindi: $n \equiv r \equiv r-p \pmod{p}$

[3.2e6] - Esempio

Eseguiamo la divisione elementare tra 127 e 13:

$$127 = 9 \cdot 13 + 10$$

Poiché $10 > 13/2$, calcoliamo il minimo resto congruente:

$$10-13 = -3$$

La divisione corrisponde a questo resto è:

$$127 = 10 \cdot 13 - 3$$

Ne seguono le congruenze:

$$127 \equiv 10 \equiv -3 \pmod{13}$$

Torna utile prendere in considerazione il caso in cui da un qualsiasi numero intero n si sottrae un numero composto m.
A questo proposito, ritornando alle proprietà fondamentali dei numeri composti *[2.1a]* e *[2.1b]*, si deve precisare che esse in realtà costituiscono dei casi particolari di una proprietà più generale.

Dati due numeri interi qualsiasi n e p (con n > p), si avrà:

$$n = c \cdot p + r \qquad (\text{con} \quad 0 \leq r < p)$$

Sottraiamo da entrambi i membri dell'uguaglianza un multiplo di p:

$$n - mp = cp + r - mp$$

Raccogliendo a fattore comune nel secondo membro, si avrà:

$$n - mp = (c-m)p + r$$

Come si può vedere il resto r rimane invariato, per cui perveniamo alla seguente conclusione:

[3.2g] - Se da un numero n sottraiamo un multiplo mp di p la condizione di divisibilità di n rispetto a p non subirà mutamenti.
Tale affermazione è espressa dalle seguenti congruenze:

$$n \equiv n - m \cdot p \equiv r \pmod{p}$$

(dove r è il resto della divisione elementare di n per p)

[3.2e7] - Esempio

Dati i numeri 239 e 23, eseguiamo la loro divisione elementare:

$$239 = 23 \cdot 10 + 9$$

Sottraiamo da 239 un multiplo di 23, ad esempio 92.

$$239 - 92 = 147$$

La divisione elementare di 147 per 23 è data dalla uguaglianza:

$$147 = 6 \cdot 23 + 9$$

Come era nelle nostre aspettative, il resto della divisione è rimasto invariato, per cui possiamo scrivere le congruenze:

$$239 \equiv 147 \equiv 9 \pmod{23}$$

Alle stesse conclusioni si arriva sottraendo a 239 un qualsiasi altro multiplo del modulo 23.

Se n è multiplo di p, si avrà, come caso particolare della *[3.2b]*, la proprietà fondamentale *[2.1a]* enunciata nel 2° capitolo.

$$n - m \cdot p \equiv 0 \pmod{p} \quad (\text{per } n = b \cdot p)$$

Dopo il breve studio preliminare fatto sulle congruenze, riprendiamo la nostra ricerca sulla divisibilità di un numero intero qualsiasi per un numero primo p assegnato.

4.1 Coefficienti di divisibilità

Dato un numero intero A qualsiasi, siano

$$a_K , a_{K-1} , a_{K-2} , a_{K-3} , \dots , a_1 , a_0$$

le sue cifre, rispettivamente dell'ordine:

$$k, k-1, k-2, k-3, \dots , 1, 0$$

Come abbiamo avuto occasione di vedere, A si può scrivere in forma polinomiale:

$$A = a_k 10^k + a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \dots + a_1 10 + a_0 \qquad (*1)$$

[4.1e1] - Esempi

$$237 = 2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$$

$$3.415.792.086 =$$

$$= 3 \cdot 10^9 + 4 \cdot 10^8 + 1 \cdot 10^7 + 5 \cdot 10^6 + 7 \cdot 10^5 + 9 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0$$

Si consideri che in ciascuna di queste uguaglianze il primo membro altro non è che la forma semplificata della scrittura a secondo membro: a primo membro ciascuna potenza di dieci è rappresentata dalla posizione della cifra di uguale ordine.

La forma polinomiale mette in risalto la struttura decimale della nostra numerazione ed è a questa struttura che si deve guardare con attenzione. Combinando tale struttura con il potento strumento delle congruenze analizzeremo in profondità le caratteristiche strutturali dei numeri primi.

Consideriamo le divisioni elementari delle potenze successive di 10 per il generico numero primo p; ciascuna di esse è rappresentata dall'uguaglianza:

$$10^n = m \cdot p + r \qquad 0 < r < p$$

Facciamo le sostituzioni nella forma polinomiale di A (*1):

$$A = a_K(m_K p + r_K) + a_{K-1}(m_{k-1} p + r_{k-1}) + a_{k-2}(m_{K-2} p + r_{K-2}) + \ldots + a_1(m_1 p + r_1) + a_0 =$$
$$= a_K m_K p + a_K r_K + a_{K-1} m_{K-1} p + a_{K-1} r_{K-1} + a_{K-2} m_{K-2} p + a_{k-2} r_{K-2} + \ldots + a_1 m_1 p + a_1 r_1 + a_0$$

Sottraendo da quest'ultima, ad uno ad uno, tutti i multipli di p, per quanto abbiamo stabilito nel capitolo precedente *[3.2g]*, la condizione di divisibilità di A per p rimarrà invariata.
Pertanto possiamo scrivere le seguenti congruenze:

$$A \equiv a_K r_K + a_{K-1} r_{K-1} + a_{K-2} r_{K-2} + \ldots + a_1 r_1 + a_0 \qquad (\text{mod. } p) \qquad (*2)$$
$$r_i \equiv 10^i \quad (\text{mod. } p) \qquad 0 < r_i < p$$

Definizione

Il resto r_i della divisione tra la potenza 10^i e p si dice:

coefficiente di divisibilità per p di ordine i.

Dalla (*2) possiamo dedurre la seguente

condizione generale di divisibilità

[4.1a] - Affinché un numero intero A sia divisibile per il numero primo p è sufficiente che sia divisibile per p la somma dei prodotti di ciascuna cifra di A per il coefficiente di divisibilità per p, di uguale ordine della cifra.

Ciò vuol dire che si deve verificarsi la congruenza:

$$a_K r_K + a_{K-1} r_{K-1} + a_{K-2} r_{K-2} + \ldots + a_1 r_1 + a_0 \equiv 0 \quad (\text{mod. } p)$$

Si badi che, per quanto possa essere elevato il numero di cifre di A, i coefficienti di divisibilità per p sono necessariamente in quantità limitata, perché il valore di ciascuno di essi è minore di p: da un certo punto in poi essi si ripetono tutti ciclicamente nello stesso ordine e la loro quantità è, al massimo, uguale a p-1.
Tutti questi coefficienti, tenuto conto dell'ordine con cui si susseguono, formano un insieme che si chiama:

insieme dei coefficienti di divisibilità per p

[4.1e2] - Esempio
Calcoliamo i coefficienti di divisibilità per 7.

$10^0=1$

$$\begin{array}{r|l} 1 & 7 \\ \hline 1 & 0 \end{array}$$

$10^0=0\cdot 7+1 \Rightarrow 10^0\equiv 1 \pmod 7$

$10^1=10$

$$\begin{array}{r|l} 10 & 7 \\ \hline 3 & 1 \end{array}$$

$10=1\cdot 7+3 \Rightarrow 10^1\equiv 3 \pmod 7$

$10^2=100$

$$\begin{array}{r|l} 100 & 7 \\ \hline 30 & 14 \\ 2 & \end{array}$$

$100=14\cdot 7+2 \Rightarrow 10^2\equiv 2 \pmod 7$

$$\begin{array}{r|l} 1000 & 7 \\ \hline 30 & 142 \\ 20 & \\ 6 & \end{array} \qquad \begin{array}{r|l} 1000 & 7 \\ \hline 30 & 143 \\ 20 & \\ -1 & \end{array}$$

Poiché il minimo resto positivo è maggiore di 7/2 è opportuno considerare anche la divisione con il minimo resto negativo.

$1000=142\cdot 7+6 \Rightarrow 10^3\equiv 6 \pmod 7$

$1000=143\cdot 7-1 \Rightarrow 10^3\equiv -1 \pmod 7$

$10000=1428\cdot 7+4$

$10000=1429\cdot 7-3$

$$\begin{array}{r|l} 10000 & 7 \\ \hline 30 & 1428 \\ 20 & \\ 60 & \\ 4 & \end{array}$$

$10^4\equiv 4\equiv -3 \pmod 7$

$$\begin{array}{r|l} 100000 & 7 \\ \hline 30 & 14285 \\ 20 & \\ 60 & \\ 40 & \\ 5 & \end{array}$$

$10^5\equiv 5\equiv -2 \pmod 7$

$$\begin{array}{r|l} 1000000 & 7 \\ \hline 30 & 142857 \\ 20 & \\ 60 & \\ 40 & \\ 50 & \\ 1 & \end{array}$$

$10^6\equiv 10^0\equiv 1 \pmod 7$

Come si vede, si è ripetuto il resto 1, per cui, da qui in poi, si ripeteranno ciclicamente e nello stesso ordine pure gli altri resti.
Si ripeteranno quindi ordinatamente anche tutti i coefficienti.

Raggruppando i coefficienti di divisibilità per 7 e classificandoli, sia rispetto ai minimi resti positivi, sia rispetto ai minimi resti, otteniamo due insiemi equivalenti:

$$C_7=\{1;3;2;6;4;5\}$$
$$\overline{C}_7=\{1;3;2;-1;-3;-2\}$$

A seconda dei casi, sarà utile servirci o dell'uno o dell'altro insieme.

Adesso che disponiamo dei coefficienti di divisibilità per 7, possiamo applicare la condizione generale di divisibilità *[4.1a]*.

[4.1e3] - Esempi

Stabiliamo se 68.185 e 3.485.022.023 sono divisibili per 7.

Per applicare la condizione di divisibilità enunciata *[4.1a]*, per prima cosa dobbiamo trascrivere i numeri dati in forma polinomiale.

$$68185 = 5 \cdot 10^0 + 8 \cdot 10^1 + 1 \cdot 10^2 + 8 \cdot 10^3 + 6 \cdot 10^4$$

$$3.485.022.023 =$$
$$= 3 + 2 \cdot 10 + 0 \cdot 10^2 + 2 \cdot 10^3 + 2 \cdot 10^4 + 0 \cdot 10^5 + 5 \cdot 10^6 + 8 \cdot 10^7 + 4 \cdot 10^8 + 3 \cdot 10^9$$

Passiamo adesso alle congruenze, sostituendo alle successive potenze di dieci i corrispondenti coefficienti di divisibilità per 7.

$$68185 \equiv 5 \cdot 1 + 8 \cdot 3 + 1 \cdot 2 + 8 \cdot 6 + 6 \cdot 4 \equiv 103 \equiv 3 \cdot 1 + 1 \cdot 2 \equiv 5 \pmod 7$$

Per stabilire la condizione di divisibilità per 7 dell'altro numero, utilizziamo l'insieme dei minimi resti.

$$3.485.022.023 \equiv$$
$$\equiv 3 \cdot 1 + 2 \cdot 3 + 0 \cdot 2 - 2 \cdot 1 - 2 \cdot 3 - 0 \cdot 2 + 5 \cdot 1 + 8 \cdot 3 + 4 \cdot 2 - 3 v 1 \equiv 35 \equiv 0 \pmod 7$$

si deduce così che:

- 68.185 non è divisibile per 7 e la sua divisione per 7 dà come resto 5.
- 3.485.022.023 è divisibile per 7 perché la sua divisione per 7 dà come resto 0.

[4.1e4] - Esempi

Stabiliamo se 68.185 e 3.485.022.023 sono divisibili per 13.

Analogamente a come abbiamo fatto con il numero 7, troviamo i coefficienti di divisibilità per 13.

$$C_{13} = \{1;10;9;12;3;4\}$$
$$\overline{C}_{13} = \{1;-3;-4;-1;3;4\}$$

Applichiamo la condizione di divisibilità usando i minimi resti:

$$68.185 \equiv 5 \cdot 1 - 8 \cdot 3 - 1 \cdot 4 - 8 \cdot 1 + 6 \cdot 3 \equiv -13 \equiv 0 \pmod{13}$$

$$3.485.022.023 \equiv$$
$$\equiv 3 \cdot 1 - 2 \cdot 3 - 0 \cdot 4 - 2 \cdot 1 + 2 \cdot 3 + 0 \cdot 4 + 5 \cdot 1 - 8 \cdot 3 - 4 \cdot 4 - 3 \cdot 1 \equiv -37 \equiv 2 \pmod{13}$$

Deduciamo così che solo 68.185 è divisibile per 13

4.2 La tabella dei coefficienti di divisibilità

Nella tabella che segue *[4.2 tab1]* sono raccolti gli insiemi dei coefficienti di divisibilità di alcuni numeri primi, sia quelli coi minimi resti positivi, sia quelli coi minimi resti.

Nella 4ª colonna è indicato il periodo del sistema dei coefficienti di divisibilità di ciascun numero primo, esso corrisponde alla quantità degli elementi di ciascun insieme.

PRIME OSSERVAZIONI SUI COEFFICIENTI DI DIVISIBILITA'

* L'insieme dei coefficienti di divisibilità di ciascun numero primo p è sempre un sottoinsieme del corrispondente insieme dei resti secondo il modulo p.
* Mentre ogni sistema completo dei resti è ordinato secondo il valore crescente dei numeri naturali da 0 a p-1, ciascun sistema dei coefficienti di divisibilità ha un ordine tutto suo, caratteristico del numero p considerato come modulo.
* Gli insiemi di divisibilità relativi al 2 e al 5 sono gli unici, tra quelli dei numeri primi, ad avere un antiperiodo. Questo accade perché soltanto i numeri primi 2 e 5 sono sottomultipli di 10.
* Escludendo gli insiemi relativi al 2 e al 5, nessun altro insieme ha tra i suoi elementi il coefficiente 0, perché nessuna potenza di 10 è un multiplo degli altri numeri primi.
* Tutti gli insiemi hanno tra i loro elementi il coefficiente 1, ciò perché la potenza 10^0, nella struttura polinomiale di p, è sempre presente e vale 1.
* Se la quantità dei coefficienti di divisibilità è un numero pari, il periodo è minore o uguale a p-1 e l'insieme dei minimi resti si può ripartire in due sottoinsiemi, costituiti da elementi di valore opposto. In questo caso, accanto al periodo completo se ne può considerare uno con valore dimezzato.
* Se la quantità dei coefficienti di divisibilità è un numero dispari, il periodo è minore o uguale a (p-1)/2. Inoltre, considerando solo i valori assoluti, il periodo degli insiemi dei minimi resti non si riduce rispetto a quello dei minimi resti positivi.

[4.2 tab1] SISTEMI DEI COEFFICIENTI DI DIVISIBILITA'

P	Sistema dei minimi resti positivi	Sistema dei minimi resti	periodo
2	0 (con antiperiodo 1)		
3	1	1	1
5	0 (con antiperiodo 1)		
7	1;3;2;6;4;5	1; 3; 2; -1;-3;-2	6 - 3
11	1;10	1; -1	2 - 1
13	1;10;9;12;3;4	1;-3;-4; -1; 3; 4	6 - 3
17	1 ;10;15;14; 4; 6;9; 5; 16; 7; 2; 3;13;11;8;12	1;-7;-2;-3; 4; 6;-8; 5; -1; 7; 2; 3;-4;-6; 8;-5	16 - 8
19	1;10; 5;12; 6; 3;11;15;17; 18; 9;14; 7;13;16; 8; 4; 2	1;-9; 5;-7; 6; 3;-8;-4;-2; -1; 9;-5; 7;-6;-3; 8; 4; 2	18 - 9
23	1;10; 8;11;18;19; 6;14; 2;20;16; 22;13;15;12; 5; 4;17; 9;21; 3; 7	1; 10; 8; 11;-5;-4; 6;-9; 2;-3;-7; -1;-10;-8;-11; 5; 4;-6; 9;-2; 3; 7	22-11
29	1;10;13;14;24; 8;22;17;25;18; 6; 2;20;26; 28;19;16;15; 5;21; 7;12; 4;11;23;27; 9; 3	1; 10; 13; 14;-5; 8;-7;-12;-4;-11; 6; 2;-9;-3; -1;-10;-13;-14; 5;-8; 7; 12; 4; 11;-6;-2; 9; 3	28-14
31	1;10;7;8;18;25;2;20;14;16;5;19; 4;9;28	1;10;7;8;-13;-6;2;-11;14;-15;5;-12; 4;9;-3	15
37	1;10;26	1;10;-11	3
41	1;10;18;16;37	1;10;18;16;-4	5
43	1;10;14;11;24;25;35;6;17;41;23;15; 21;38;36;16;31;9;4;40;13	1;10;14;11;-19;-18;-8;6;17;-2;-20;15; 21;-5;-7;16;-12;9;4;-3;13	21
53	1;10;47;46;36;42;49;13;24;28;15; 44;16	1;10;-6;-7;-17;-11;-4;13;24;-25;15; -9; 16	13
73	1;10; 27; 51;72;63;46;22	1; 10; 27;-22; -1;-10;-27; 22	8 - 4
79	1;10;21;52;46;65;18;22;62;67;38; 64;8	1;10;21;-27;-33;14;18;22;-17;-12;38; -15;8	13
101	1;10;100;91	1; 10; -1;-10	4 - 2
137	1;10;100;41;136;127;37;96	1; 10;-37; 41; -1;-10; 37;-41	8 - 4
239	1;10;100;44;201;98;24	1;10;100;44;-38;98;24	7
271	1;10;100;187;244	1;10;100;-84;-27	5
4649	1;10;100;1000;702;2371;465	1;10;100;1000;702;-2278;465	7

L'osservazione di ciascun sistema dei coefficienti di divisibilità *[4.2 tab1]* , ci consente di dedurre quei facili criteri di divisibilità che abbiamo descritto nel 1° capitolo per alcuni numeri primi.
Completiamo le loro dimostrazioni che momentaneamente avevamo sospeso per occuparci delle congruenze.

5.1 Come nasce il criterio unico di divisibilità per 2 e per 5

I criteri di divisibilità per 2 *[1.3a]* e per 5 *[1.5a]* si deducono dalla condizione generale di divisibilità *[4.1a]*. Le loro particolari semplicità traggono origine da una caratteristica comune ad entrambi: solo essi, tra tutti i numeri primi, sono sottomultipli di 10.
Si osservi la *[4.2 tab.1]*, gli insiemi dei coefficienti di divisibilità di 2 e di 5 sono identici, quindi il criterio di divisibilità è unico per entrambi.
Infatti in ciascuno dei due insiemi il primo coefficiente di divisibilità è 1 (antiperiodo), mentre tutti gli altri coefficienti si ripetono sempre uguali a 0 (periodo), per cui valgono le congruenze:

$$10^0 \equiv 1 \pmod 2 \ , \pmod 5$$

$$10^n \equiv 0 \pmod 2 \ , \pmod 5 \qquad \text{per } n > 0$$

Cosicché, se *a* è il numero intero da esaminare, passando alla sua forma polinomiale e applicando la condizione di divisibilità, sia per 2 sia per 5, la sua ultima cifra, moltiplicata per 1, rimane invariata, mentre tutte le altre, moltiplicate per zero, si annullano. Ne consegue che *a* risulta congruente alla sua ultima cifra, sia rispetto al modulo 2, sia rispetto al modulo 5.
Si conclude così che *a*, se ha come ultima cifra un multiplo di 2, è esso stesso un multiplo di 2, se ha come ultima cifra un multiplo di 5, è esso stesso un multiplo di 5; in particolare, se ha come ultima cifra 0, *a* è multiplo sia di 2 sia di 5.

[5.1e1] - Esempio

Stabiliamo se 1375, 100007 e 45770 sono divisibili per 2 e per 5.

Passando alle congruenze, si avranno questi risultati:

- $1375 \equiv 1 \cdot 5 + 0 \cdot 7 + 0 \cdot 3 + 0 \cdot 1 \equiv 5 \pmod{2}, \pmod{5}$
  ne segue che 1375 è multiplo di 5, ma non di 2.
- $45770 \equiv 0 \pmod{2}, \pmod{5}$
  quindi 45770 è multiplo sia di 2 sia di 5.
- $100007 \equiv 7 \pmod{2}, \pmod{5}$
  quindi 100007 non è multiplo né di 2 né di 5.

5.2 Come nasce il criterio di divisibilità per 3

Anche per il numero primo 3 le cose sono molto semplici. Infatti il quoziente della divisione per 3 di 10^n ($n \in N$) genera sempre ed unicamente il resto 1.
Ciò implica che l'insieme dei coefficienti di divisibilità per 3 è costituito da un solo elemento e per giunta questo è l'elemento neutro della moltiplicazione. Vale quindi la congruenza:

$$10^n \equiv 1 \pmod{3} \qquad n \in N$$

Ciò vuol dire che nello sviluppo polinomiale del numero intero *a*, quando si passa alle congruenze, ciascuna potenza di 10, essendo sostituita dal fattore 1, di fatto viene soppressa. Cosicché rimane la congruenza che si ottiene soltanto dalla somma delle cifre del numero dato.

[5.2e1] -Esempio
Stabiliamo se 4231 è divisibile per 3.

Passiamo allo sviluppo polinomiale:

$$5231 = 5 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 1 \cdot 10^0$$

Poiché $10^n \equiv 1 \pmod{3}$ $n \in N$
si avrà la congruenza:

$$5231 \equiv 5 + 2 + 3 + 1 \equiv 11 \equiv 2 \pmod{3}$$

Quindi 5231 non è multiplo di 3, perché la sua divisione per 3 ha come resto 2.

E' da questa congruenza che nasce il criterio di divisibilità per 3, esposto nel 1° capitolo, e ad esso, applicando le proprietà dell' addizione, si aggiungono quest'altre facilitazioni:

- la somma delle cifre si può eseguire senza rispettare il loro ordine sequenziale;
- le cifre che, da sole o addizionate, formano dei multipli di 3 si possono sopprimere.

Nella nostra trattazione stiamo considerando prevalentemente la divisibilità per i numeri primi.
Tuttavia vale la pena tenere presente che anche l'insieme dei coefficienti di divisibilità per 9 è formato soltanto dal coefficiente 1, per cui il criterio di divisibilità per i numeri 3 e 9 è unico.

[5.2e2] - Esempi

Stabiliamo se 9183 e 32168547 sono divisibili per 3 e per 9.

Passiamo alle congruenze:

$$9183 \equiv 9+1+8+3 \equiv 3 \pmod{3}, \pmod{9}$$
$$32168547 \equiv (3+6)+(2+7)+(1+8)+(5+4) \equiv 0 \pmod{3}, \pmod{9}$$

Ne segue che:

- 9183 è multiplo di 3 ma non di 9.
- 32168547 è multiplo sia di 3 sia di 9.

5.3 Come nasce il criterio di divisibilità per 7

Al contrario di ciò che accade con il numero 3, applicare meccanicamente la condizione generale di divisibilità per 7, così come abbiamo fatto nell'esempio *[4.1e3]*, non è molto vantaggioso.
Solo con il rimaneggiamento delle procedure di calcolo e con l'osservazione riusciremo ad ottenere anche per questo numero primo un semplice criterio di divisibilità.

Abbiamo già constatato che le divisioni delle successive potenze di dieci per 7 producono una periodicità illimitata di 6 resti, così ordinati:

1; 3; 2; 6; 4; 5

Una prima elaborazione di questi dati possiamo farla sostituendo agli ultimi tre resti, maggiori di 7/2, i minimi resti:

6 ---> -1 ; 4 ---> -3 ; 5 ---> -2

Facendo ciò, non solo si riduce il valore assoluto dei coefficienti, ma si ottiene anche una caratteristica strutturale interessante:

1 ; 3 ; 2
-1 ; -3 ; -2

L'insieme dei coefficienti di divisibilità per 7, configurato in questo modo, si divide in due sottoinsiemi con caratteristiche comuni:

- ciascun sottoinsieme è costituito da tre coefficienti uguali, nei loro valori assoluti, a quelli dell'altro sottoinsieme;
- l'ordine di successione dei tre valori assoluti è lo stesso in entrambi. (Ad ogni coefficiente del primo sottoinsieme corrisponde il coefficiente di segno opposto nell'altro).

In base a queste osservazioni possiamo asserire che l'insieme dei coefficienti di divisibilità per 7, quando consideriamo solo i valori assoluti, si riduce a 3 elementi.

Vediamo quali vantaggi si ottengono quando si considera l'insieme ridotto dei coefficienti di divisibilità, anziché quello completo.

Sia dato un generico numero intero *A* , formato da k cifre:

*[5.3*1]* $A = a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1$

Applichiamo la condizione di divisibilità, scrivendo *A* in forma polinomiale e moltiplicando ciascuna delle sue cifre per il corrispondente coefficiente di divisibilità per 7:

*[5.3*2]*

$$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot a_1 + 3 \cdot a_2 + 2 \cdot a_3 - 1 \cdot a_4 - 3 \cdot a_5 - 2 \cdot a_6 + 1 \cdot a_7 + \ldots \quad (\text{mod.}7)$$

Raccogliamo a fattore comune, mettendo in evidenza i coefficienti di divisibilità, ma in modo tale che questi compaiano tutti con il segno positivo:

*[5.3*3]*

$$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot (a_1 - a_4 + a_7 - \ldots) + 3 \cdot (a_2 - a_5 + a_8 - \ldots) + 2 \cdot (a_3 - a_6 + a_9 \ldots) \quad (\text{mod.}7)$$

Calcoliamo le tre somme algebriche racchiuse dentro le parentesi:

$$s_1 = a_1 - a_4 + a_7 - a_{10} + \ldots$$
$$s_2 = a_2 - a_5 + a_8 - a_{11} + \ldots$$
$$s_3 = a_3 - a_6 + a_9 - a_{12} + \ldots$$

e sostituendole nella congruenza *[5.3*3]*, avremo:

*[5.3*4]* $a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot (s_1) + 3 \cdot (s_2) + 2 \cdot (s_3)$ (mod.7)

Sostituiamo ai coefficienti di divisibilità di quest'ultima le prime 3 potenze di 10 da cui hanno avuto origine:

*[5.3*5]* $a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 10^0 \cdot s_1 + 10^1 \cdot s_2 + 10^2 \cdot s_3$ (mod.7)

Eseguendo i calcoli a secondo membro di quest'ultima congruenza otterremo un numero intero *A*' congruente al numero *A* di partenza. Sicuramente *A*' è minore di *A*, perché, applicando la condizione di divisibilità per 7, a ciascuna potenze di dieci abbiamo sostituito un coefficiente di valore inferiore.
Nel caso in cui *A*' risultasse formato da un numero di cifre superiore a tre, sarà necessario ripetere le procedure seguite per *A* :

*[5.3*6]* $A' \equiv 1 \cdot (t_1) + 3 \cdot (t_2) + 2 * (t_3) \equiv 1 \cdot (t_1) + 10 \cdot (t_2) + 100 \cdot (t_3)$ (mod.7)

Continuando otterremo un numero *A*'' con non più di tre cifre.

*[5.3*6]* $A'' \equiv 1 \cdot (r_1) + 3 \cdot (r_2) + 2 * (r_3) \equiv 1 \cdot (r_1) + 10 \cdot (r_2) + 100 \cdot (r_3) = r_3 r_2 r_1$
(mod.7) $(0 \le r_i < 10)$

$A'' = r_3 r_2 r_1$ (r_1 indica le unità, r_2 le decine e r_3 le centinaia di *A*").

A conclusione di questo lavoro possiamo asserire che:

[5.3a] - al generico numero intero A, con un numero qualsivoglia di cifre, è sempre possibile associarne uno, ad esso congruente secondo il modulo 7, di non più di tre cifre.

Per stabilire la divisibilità per 7 di quest'ultimo numero relativo *A*'', anziché continuare con la condizione di divisibilità, è preferibile applicare il criterio unico di divisibilità per 7 e per 13, descritto nel 1° capitolo per i numeri con 3 cifre soltanto *[1.6a]*.

A questo punto il nostro obiettivo è raggiunto, perché era nostro proposito dimostrare che:

i coefficienti di divisibilità per 7 non sono necessari.

Infatti, anche se ci hanno accompagnati fino qui, nella realtà dei fatti questi coefficienti non li abbiamo utilizzati.
E' essenziale invece la struttura del loro insieme, così come l'abbiamo configurato, cioè suddiviso in 2 classi di 3 elementi.

[5.3b]

$$\begin{matrix} 1;\ 3;\ 2; \\ -1;\ -3;\ -2 \end{matrix} \xrightarrow[\text{coefficienti di divisibilità per 7}]{\text{struttura dell'insieme dei}} \begin{matrix} \alpha;\ \beta;\ \gamma; \\ -\alpha;\ -\beta;\ -\gamma \end{matrix}$$

[5.3e1] - Esempio

Verifichiamo la divisibilità per 7 di 798201879011782.

La condizione di divisibilità per 7 ci fornisce queste congruenze:

$$798.201.879.011.782 \equiv$$
$$\equiv 1\cdot 2+3\cdot 8+2\cdot 7-1\cdot 1-3\cdot 1-2\cdot 0+1\cdot 9+3\cdot 7+2\cdot 8-1\cdot 1-3\cdot 0-2\cdot 2+1\cdot 8+3\cdot 9+2\cdot 7 \equiv$$
$$\equiv 1\cdot(2-1+9-1+8)+3\cdot(8-1+7-0+9)+2\cdot(7-0+8-2+7) \equiv$$
$$\equiv 1\cdot 17+3\cdot 23+2\cdot 20 \equiv 10^0\cdot 17+10^1\cdot 23+10^2\cdot 20 \equiv 2247 \pmod 7$$

Ripetiamo il procedimento:

$$2247 \equiv 1\cdot(7-2)+3\cdot 4+2\cdot 2 \equiv 10^0\cdot 5+10^1\cdot 4+10^2\cdot 2 \equiv 245 \pmod 7$$

Ottenuta la congruenza del numero dato con un numero a tre cifre, applichiamo a quest'ultimo il criterio di divisibilità descritto nel 1° capitolo *[1.6a]*, riducendo la congruenza ad un numero a sole due cifre, facilmente riconoscibile:

$$798.201.879.011.782 \equiv 2247 \equiv 245 \equiv 63 \equiv 0 \pmod 7$$

Quindi 798.201.879.011.782 è divisibile per 7.

Queste procedure ci sono servite essenzialmente per comprendere le proprietà strutturali dei multipli di 7, ma in realtà i calcoli si possono eseguire molto più rapidamente.
Poiché nelle congruenze possiamo sostituire alternativamente i coefficienti di divisibilità con le corrispondenti potenze di 10, eseguiamo i calcoli secondo il modulo 7 in quest'altro modo:

$$798.201.879.011.782 \equiv$$
$$\equiv 1\cdot 2+3\cdot 8+2\cdot 7-1\cdot 1-3\cdot 1-2\cdot 0+1\cdot 9+3\cdot 7+2\cdot 8-1\cdot 1-3\cdot 0-2\cdot 2+1\cdot 8+3\cdot 9+2\cdot 7 \equiv$$
$$\equiv 1\cdot(2+9+8)+10\cdot(8+7+9)+100\cdot(7+8+7)-1\cdot(1+1)-10\cdot(1+0)-100\cdot(0+2)$$

Da qui si evince che, anziché addizionare le unità, le decine e le centinaia dei vari ordini separatamente, conviene addizionarle direttamente per classi.
Cosicché possiamo ottenere i risultati precedenti in modo più semplice e veloce seguendo questi passaggi:

1) - diviso il numero dato in classi di tre cifre, si addizionano tra loro sia le classi di posto pari sia quelle di posto dispari.
2) - si calcola la differenza delle due somme;
3) - si ripetono eventualmente le procedure fino ad ottenere un numero di tre cifre soltanto;
4) - si applica il criterio unico di divisibilità per 7 e per 13 *[1.6a]*

1)

782 +	
879	011 +
798	201
2459	212

2)

2459-
212
2247

3)

247-
2
245

4)

$245 \equiv 63 \equiv 0 \pmod 7$

[5.3e2] - Esempi

Verifichiamo la divisibilità per 7 dei numeri:
1005320413695117802, 1492001 , 1001001002001 e 110346001

- Dividiamo il primo numero in classi di 3 cifre e seguiamo i passaggi dei punti 1 ; 2 ; 3 e 4.
1.005.320.413.695.117.802

1)

802 +	
695	117 +
320	413
1	005
1818	535

2)

1818-
535
1283

3)

283-
1
282

4)

$282 \equiv 100 \equiv 2 \pmod 7$

Quindi 1.005.320.413.695.117.802 non è multiplo di 7, perché la sua divisione per 7 dà come resto 2.

- Dividiamo in classi di 3 cifre il secondo numero: 1.492.001
Questa volta i calcoli sono davvero facili, è un multiplo di 7 :

$$1.492.001 \equiv 490 \equiv 0 \pmod 7$$

- Anche il numero 1001001002001 è multiplo di 7.

Infatti, con un rapido calcolo mentale, arriviamo alla congruenza:

$$1.001.001.002.001 \equiv 0 \pmod{7}$$

- Il numero 110346001 invece non è multiplo di 7.

Infatti un calcolo immediato ci dà le congruenze:

$$110.346.001 \equiv -235 \equiv -53 \equiv 3 \pmod{7}$$

L'ultima di queste congruenze ci serve solo per sapere qual è il resto della divisione, mentre per la divisibilità è sufficiente considerare il solo valore assoluto dei numeri ottenuti.

5.4 Come nasce il criterio di divisibilità per 13

I coefficienti di divisibilità per 13 sono in ordine:

$$1;\ 10;\ 9;\ 12;\ 3;\ 4$$

Se applichiamo meccanicamente la condizione di divisibilità per 13, così come abbiamo fatto nell'esempio *[4.1e4]*, non ne trarremo alcun vantaggio. Ma, elaborando opportunamente le procedure di calcolo e facendo le dovute osservazioni, sarà possibile dedurre anche per questo numero un semplice criterio di divisibilità.

Anzitutto sostituiamo i minimi resti ai tre coefficienti maggiori di 13/2, calcolando la differenza di ciascuno di questi con il 13:

$$10 \dashrightarrow -3\ ;\ 9 \dashrightarrow -4\ ;\ 12 \dashrightarrow -1$$

E' d'immediata constatazione l'analogia con il sistema dei coefficienti di divisibilità per 7: l'insieme dei coefficienti di 13, anch'esso formato da sei elementi, si può dividere in due sottoinsiemi che hanno caratteristiche uguali, così come è mostrato nel riquadro *[5.4a]*.

[5.4a]

1;	-3;	-4;	*struttura dell'insieme dei* $\longrightarrow$	$\alpha;\ \beta;\ \gamma;$
-1;	3;	4	*coefficienti di divisibilità per 13*	$-\alpha;\ -\beta;\ -\gamma$

In questi due sottoinsiemi gli elementi sono uguali in valore assoluto e si susseguono nello stesso ordine, per cui, come è accaduto per il 7, anche per il 13 l'insieme dei coefficienti di divisibilità si riduce a tre valori assoluti soltanto.

Cosicché, confrontando la *[5.4a]* con la *[5.3b]*, ci accorgiamo che le strutture dei coefficienti di divisibilità per 7 e per 13 coincidono.

A questo punto dobbiamo supporre che anche per il 13 la struttura abbia il sopravvento sul valore dei coefficienti.

Facciamone una verifica concreta, ripetendo i passaggi seguiti per il numero 7 nel paragrafo *[5.3]*.

Riprendiamo il generico numero intero *A* formato da k cifre *[5.3*1]*:

$$A = a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1$$

Applichiamo la condizione di divisibilità: scriviamo *A* in forma polinomiale, moltiplicando ciascuna delle sue cifre per il corrispondente coefficiente di divisibilità per 13.

$$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot a_1 - 3 \cdot a_2 - 4 \cdot a_3 - 1 \cdot a_4 + 3 \cdot a_5 + 4 \cdot a_6 + 1 \cdot a_7 - \ldots \pmod{13}$$

Raccogliamo a fattore comune, mettendo in evidenza i coefficienti di divisibilità nel modo seguente:

*[5.4*1]*

$$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_3 a_2 a_1 \equiv 1 \cdot (a_1 - a_4 + a_7 - \ldots) - 3 \cdot (a_2 - a_5 + a_8 - \ldots) - 4 \cdot (a_3 - a_6 + a_9 \ldots) \pmod{13}$$

Mettendo a confronto la *[5.4*1]* con la corrispondente *[5.3*3]* del numero 7, si può constatare che le tre somme algebriche racchiuse dalle parentesi sono le stesse. Pertanto, se nella *[5.4*1]* ai tre coefficienti di divisibilità per 13 sostituiamo le prime tre potenze di 10 ad essi congruenti e facciamo ripetutamente i calcoli, otteniamo gli stessi numeri *A*' e A'' che figurano nelle congruenze del paragrafo *[5.3]*.

Possiamo scrivere quindi:

$$A \equiv A' \equiv A'' \pmod{7}, \pmod{13}$$

asserendo così che il criterio di divisibilità per 7 vale simultaneamente anche per il 13.

Le conclusioni per il 13 sono le stesse di quelle fatte per il 7:

i coefficienti di divisibilità per 13, non sono necessari.

[5.4a] - Al generico numero intero A, con un numero qualsivoglia di cifre, è sempre possibile associarne uno, ad esso congruente secondo il modulo 13, di non più di tre cifre.

Per stabilire la divisibilità per 13 di quest'ultimo numero relativo a tre cifre, anziché applicare ancora la condizione di divisibilità, è preferibile continuare con il criterio unico di divisibilità per 7 e per 13, descritto nel 1° capitolo *[1.6a]*.

[5.4e1] - Esempio

Verifichiamo la divisibilità per 13 di 798201879011782.

Poiché si tratta dello stesso numero dell'esempio *[5.3e1]*, i calcoli sono già fatti:

$$798.201.879.011.782 \equiv 2247 \equiv 245 \equiv 63 \qquad (\text{mod. } 13)$$

Quindi il numero dato non è un multiplo di 13.

5.5 Come nasce il criterio unico di divisibilità per 7, 11 e 13

Il successo ottenuto mettendo a confronto gli insiemi dei coefficienti di divisibilità per 7 e per 13, ci spinge ad indagare sugli insiemi degli altri numeri primi, alla ricerca di altre strutture uguali.
Passando in rassegna i sistemi di divisibilità disponibili *[4.2 tab.1]*, in un primo tempo sembra che non ci siano strutture uguali a quelle del 7 e del 13, ma, con l'elaborazione dei dati e con l'osservazione, troveremo quello che cerchiamo.
Tra tutti i sistemi esaminati desta la nostra attenzione l'insieme ridotto dei coefficienti di divisibilità per 11.

Le divisioni per 11 delle potenze successive di dieci producono una periodicità illimitata di 2 resti, nell'ordine:

$$1 \; ; \; 10$$

Sostituendo al coefficiente 10 il minimo resto ad esso congruente, l'insieme si riduce ad un solo valore assoluto:

$$C_{11} = [1 \; ; \; -1]$$

Quindi, poiché l'insieme dei coefficienti di divisibilità è ciclico, i valori 1 e -1 si alterneranno all'infinito:

$$1;-1;+1;-1+1;-1;+1;-1;+1;-1; \ldots.$$

Tenendo d'occhio la struttura dei coefficienti del 7, al fine di crearne una simile, prendiamo i primi sei elementi di questa stringa e disponiamoli in 2 gruppi, così come è mostrato nel riquadro *[5.5a]*

[5.5a]

$$\begin{array}{cc} 1; & -1; +1; \\ -1; +1; & -1 \end{array} \xrightarrow[\text{coefficienti di divisibilità per 11}]{\text{struttura dell'insieme dei}} \begin{array}{c} \alpha; \ \beta; \ \gamma; \\ -\alpha; -\beta; -\gamma \end{array}$$

Confrontando la *[5.5a]* con l'analoga *[5.3b]* del numero 7, riteniamo di essere riusciti nel nostro intento, perché le due strutture sono uguali.

Per accertarci che la struttura creata artificiosamente dia effettivamente i frutti sperati, ritorniamo a considerare il generico numero intero *A* formato da k cifre *[5.3*1]*.

$$A = a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1$$

Applichiamo la condizione di divisibilità per 11: scriviamo *A* in forma polinomiale, moltiplicando ciascuna delle sue cifre per il corrispondente coefficiente di divisibilità.

$$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot a_1 - 1 \cdot a_2 + 1 \cdot a_3 - 1 \cdot a_4 + 1 \cdot a_5 - 1 \cdot a_6 + 1 \cdot a_7 - \ldots \pmod{11}$$

Coerentemente con la struttura che abbiamo ideato, mettiamo in evidenza i coefficienti di divisibilità in questo modo:

*[5.5*1]*

$$a_k a_{k-1} a_{k-2} \ldots a_3 a_2 a_1 \equiv 1 \cdot (a_1 - a_4 + a_7 - \ldots) - 1 \cdot (a_2 - a_5 + a_8 - \ldots) + 1 \cdot (a_3 - a_6 + a_9 \ldots) \pmod{11}$$

Confronto la *[5.5*1]* con la corrispondente *[5.3*3]* del numero 7, si può constatare che le tre somme algebriche racchiuse dentro le parentesi sono le stesse. Cosicché, se nella *[5.5*1]* ai tre coefficienti di divisibilità per 11 sostituiamo le prime tre potenze di 10 ad essi congruenti e facciamo i calcoli, otteniamo gli stessi numeri *A*' e A'' che compaiono nelle congruenze del paragrafo *[5.3]*.

Possiamo scrivere quindi:

$$A \equiv A' \equiv A'' \pmod{7}, \pmod{13}, \pmod{11}$$

asserendo così che il criterio di divisibilità per il 7 vale simultaneamente anche per i numeri 13 e 11.

Le conclusioni per 11 sono le stesse di quelle fatte per il 7 e il 13:

i coefficienti di divisibilità per 11, non sono necessari.

[5.5b] - al generico numero intero A, con un numero qualsivoglia di cifre, è sempre possibile associarne uno, ad esso congruente secondo il modulo 11, di non più di tre cifre.

Dopo, per stabilire la divisibilità per 11 del numero relativo di tre cifre, si continuerà con il criterio che abbiamo descritto nel 1° capitolo al punto *[1.8a]*.

Quest'ultimo criterio è stato ricavato considerando che l'insieme ridotto dei coefficienti di divisibilità per 11 è formato dal solo valore assoluto 1, elemento neutro della moltiplicazione. Quindi il criterio di divisibilità di *A*'' per 11 si riduce alla somma algebrica delle sue tre cifre, dopo avere dato un valore negativo alla cifra centrale.

[5.5e1] - Esempi

Verifichiamo la divisibilità per 7, per 11 e per 13 di:
1792160394037 ; 1001001001 ; 3321800437 ;
632469583210629075694053 7

- Dividiamo il primo numero in classi di 3 cifre ed eseguiamo i calcoli.
1.792.160.394.037

037 +	394 +	186-
160	792	1
1	1186	185
198		

198-
185
13

1792160394037 ≡ 13 (mod.7) , (mod.11) , (mod.13)

Quindi 1.792.160.394.037 è multiplo di 13; non è multiplo invece né di 7 né di 11.

- Il secondo numero è multiplo di 7, di 11 e di 13.
Infatti, con calcolo immediato, si ottiene la congruenza:

1.001.001.001 ≡ 0 (mod.7) , (mod.11) , (mod.13)

- Il numero 3.321.800.437 non è multiplo di nessuno dei tre, infatti si ottiene rapidamente la congruenza:

3.321.800.437 ≡ 45 (mod.7) , (mod.11) , (mod.13)

- Il numero 6.324.695.832.106.290.756.940.537 è formato da venticinque cifre, ma con due semplici addizioni riusciamo a stabilire che è divisibile per 11 e per 13, ma non per 7.

537 +	
756	940 +
106	290
695	832
6	324
2100	2386

6.324.695.832.106.290.756.940.537 ≡ -286 (mod.7),(mod.11),(mod.13)

-286 ≡ 0 (mod.11) , (mod.13) -286 ≡1 (mod.7)

5.6 Come nasce il criterio di divisibilità per 101

Nel primo capitolo, paragrafo 1.10, abbiamo descritto un semplice criterio di divisibilità per 101, vediamo ora da cosa si deduce.
Se osserviamo la tabella *[4.2 tab.1]* ci accorgiamo che l'insieme dei coefficienti di divisibilità per 101 è formato da 4 elementi, riducibili a due se si considerano solo i valori assoluti. Cosicché è possibile disporre questi coefficienti come è mostrato nel riquadro *[5.6a]*

[5.6a]

1; 10;	*struttura dell'insieme dei*	→	α; β;
-1; -10;	*coefficienti di divisibilità per 101*		−α; −β

L'insieme dei coefficienti di divisibilità per 101, così strutturato, si divide in due sottoinsiemi con caratteristiche comuni:
- ciascun sottoinsieme è formato da due coefficienti uguali, nei loro valori assoluti, a quelli dell'altro sottoinsieme;
- l'ordine di successione dei valori assoluti è lo stesso in entrambi, cosicché ad ogni coefficiente del primo sottoinsieme corrisponde il coefficiente di segno opposto nell'altro.

Vediamo quali vantaggi possiamo trarre da questa struttura quando dobbiamo stabilire la condizione di divisibilità di un numero intero qualsiasi per 101.

Sia dato un generico numero intero *A* , formato da k cifre:

*[5.6*1]* $A = a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1$

Applichiamo la condizione di divisibilità per 101.
Scritto *A* in forma polinomiale, moltiplichiamo ciascuna delle sue cifre per il corrispondente coefficiente di divisibilità:

*[5.6*2]*

$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot a_1 + 10 \cdot a_2 - 1 \cdot a_3 - 10 \cdot a_4 + 1 \cdot a_5 + 10 \cdot a_6 - \ldots \pmod{101}$

Raccogliamo a fattore comune, mettendo in evidenza i coefficienti di divisibilità, ma in modo tale che questi compaiano tutti con il segno positivo:

*[5.6*3]*

$a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot (a_1 - a_3 + a_5 - \ldots) + 10 \cdot (a_2 - a_4 + a_6 - \ldots) \pmod{101}$

Eseguiamo le due somme algebriche racchiuse dentro le parentesi:

$$s_1 = a_1 - a_3 + a_5 - a_7 + \ldots$$
$$s_2 = a_2 - a_4 + a_6 - a_8 + \ldots$$

e sostituiamole nella congruenza *[5.6*3]*:

*[5.6*4]* $a_k a_{k-1} a_{k-2} a_{k-3} \ldots a_4 a_3 a_2 a_1 \equiv 1 \cdot (s_1) + 10 \cdot (s_2) \pmod{101}$

Eseguendo i calcoli a secondo membro di quest'ultima congruenza otterremo un numero intero *A*' congruente al numero *A* di partenza, secondo il modulo 101.

*[6*5.3]* $A \equiv A' = 1 \cdot (s_1) + 10 \cdot (s_2) \pmod{101}$

Sicuramente *A*' avrà una quantità di cifre inferiore a quelle di *A*, perché, applicando la condizione di divisibilità per 101, a ciascuna potenza di dieci con esponente maggiore di 1, abbiamo sostituito un coefficiente di valore inferiore .
Nel caso in cui *A*' risultasse formato da un numero di cifre superiore a due, ripetendo le procedure seguite per *A*, alla fine, e rapidamente, si otterrà un numero *A*'' con non più di due cifre.

*[6*5.3]* $A \equiv A' \equiv A'' = 1 \cdot (r_1) + 10 \cdot (r_2) \pmod{101} \qquad (0 \leq r_i < 10)$

$A'' = r_2 r_1$ è un numero di due cifre
(r_1 rappresenta le unità ed r_2 le decine di *A*")

A conclusione di questo lavoro possiamo asserire che:

[5.6a] - al generico numero intero A, con un numero qualsivoglia di cifre, è sempre possibile associarne uno, ad esso congruente secondo il modulo 101, di non più di due cifre.

Poiché tutti i multipli di 101, escluso lo 0, sono formati da più di 2 cifre, quest'ultimo numero *A''*, sarà 0 se il numero *A* di partenza è un multiplo di 101, sarà diverso da 0 se *A* non è multiplo di 101.

A questo punto il nostro obiettivo è raggiunto, perché era nostro proposito dimostrare che:

i coefficienti di divisibilità per 101, non sono necessari.

Infatti, anche se ci hanno accompagnati fino qui, nella realtà dei fatti questi coefficienti non li abbiamo utilizzati. E' essenziale invece la struttura del loro insieme, così come l'abbiamo configurato, cioè suddiviso in 2 classi di 2 elementi.

[5.6e1] - Esempio

Verifichiamo la divisibilità per 101 dei numeri 1556760167, 1007273 e 2034817

- Se volessimo scomporre 1556760167 in fattori, senza l'aiuto di un computer, l'impresa non sarebbe affatto semplice, ma almeno uno dei suoi fattori sarebbe possibile individuarlo facilmente.

Dividiamolo in classi di due cifre: 15.56.76.01.67

Addizioniamo le classi di posto pari e quelle di quelle di posto dispari; successivamente calcoliamo la differenza delle due somme:

67 +			
76	58-	01 +	57-
15	1	56	57
158	57	57	00

Si deduce così che 1556760167 è multiplo di 101.

- Anche per gli altri due numeri è possibile dedurre la loro condizione di divisibilità per 101 con rapidi calcoli fatti a mente:

1.00.72.73 è multiplo di 101, mentre 2.03.48.17 non lo è.

In questo capitolo indagheremo sui numeri primi successivi al 13, alla ricerca di altri facili criteri di divisibilità.
Come è accaduto con i precedenti criteri, troveremo quello che cerchiamo osservando ed elaborando gli insieme dei coefficienti di divisibilità dei numeri primi presi in esame.
I numeri primi, successivi al 13, che ci permettono di raggiungere dei risultati interessanti sono: 17, 19, 29, 37.

6.1 Criterio di divisibilità per 19

Basta dare una rapida occhiata ai coefficienti di divisibilità per 19, per dedurre un semplice criterio di divisibilità.

[6.1a] - Dato il numero intero n, si moltiplichi per 2 la sua prima cifra a destra e si addizioni il prodotto alla seconda cifra; si moltiplichi il risultato per 2 e si addizioni il prodotto alla terza cifra; si continui così fino all'ultima cifra.
Se il risultato ottenuto con questo procedimento è multiplo di 19, è tale anche il numero n di partenza, se invece non è un multiplo di 19, non lo è nemmeno n.

[6.1e1] - Esempio.
Stabiliamo se 437 è un multiplo di 19.

- Applicando il criterio di divisibilità descritto, con facili calcoli, eseguibili a mente, otteniamo il risultato:

$$(7 \cdot 2 + 3) \cdot 2 + 4 = 38$$

e, successivamente, reiterando il procedimento:

$$2 \cdot 8 + 3 = 19$$

Pertanto possiamo affermare che 437 è multiplo di 19.

Reiterano il procedimento, ogni volta si otterrà un valore minore del precedente, fino a quando diverrà minore o uguale a 19; se il numero n di partenza è multiplo di 19, il risultato finale sarà 19.
Applicando il procedimento allo stesso 19 si ottiene ancora 19, applicandolo ad un numero minore di 19, si ottiene un risultato ancora minore di 19.

[6.1e2] - Esempi

Verifichiamo se sono divisibili per 19 i numeri:

8931 , 238545 e 38266848851317313200163.

I calcoli saranno più rapidi se ci aiuteremo con le congruenze.

- Applichiamo il criterio di divisibilità per 19 al primo numero:

$$(((2\cdot 1+3)\cdot 2+9)\cdot 2+8) \equiv 0\cdot 2+8 \equiv 8 \pmod{19}$$

Pertanto 8931 non è multiplo di 19.

Attenzione però a non concludere che anche 8931 è congruo a 8 secondo il modulo 19. Infatti la congruenza corretta è quella che si ottiene moltiplicando alla fine per 10^3:

$$8931 \equiv (((2\cdot 1+3)\cdot 2+9)\cdot 2+8)\cdot 10^3 \equiv 8\cdot 12 \equiv 1 \pmod{19}$$

In generale: l'esponente del fattore finale 10, da aggiungere alla congruenza, è k-1, essendo k il numero delle cifre di N.

- Applichiamo il criterio di divisibilità al secondo numero:

$$((((2\cdot 5+4)\cdot 2+5)\cdot 2+8)\cdot 2+3)\cdot 2+2 \equiv$$

$$\equiv (((-5\cdot 2+5)\cdot 2+8)\cdot 2+3)\cdot 2+2 \equiv (-2\cdot 2+3)\cdot 2+2 \equiv 0 \pmod{19}$$

ne segue che: $238545 \equiv 0 \pmod{19}$

- Il terzo numero è formato da 23 cifre, per cui conviene sostituirlo con uno di 9 cifre ad esso congruente, secondo il modulo 19. Ciò sarà possibile considerando che l'insieme ridotto dei coefficienti di divisibilità per 19 è caratterizzato dal periodo 9. Si veda la tabella *[4.2 tab.1]*.

$$38266.848851317.313200163 \equiv$$

$$\equiv 38266 + 313200163 - 848851317 \equiv -535612888 \pmod{19}$$

Applicando al valore assoluto di quest'ultimo numero il criterio di divisibilità, dedurremo che il numero iniziale è multiplo di 19.

$$(((((((2\cdot 8+8)\cdot 2+8)\cdot 2+2)\cdot 2+1)\cdot 2+6)\cdot 2+5)\cdot 2+3)\cdot 2+5 \equiv$$

$$\equiv ((((((5\cdot 2+8)\cdot 2+2)\cdot 2+1)\cdot 2+6)\cdot 2+5)\cdot 2+3)\cdot 2+5 \equiv$$

$$\equiv (((((-2+2)\cdot 2+1)\cdot 2+6)\cdot 2+5)\cdot 2+3)\cdot 2+5 \equiv$$

$$\equiv (((2+6)\cdot 2+5)\cdot 2+3)\cdot 2+5 \equiv (2\cdot 2+3)\cdot 2+5 \equiv 19 \equiv 0 \pmod{19}$$

6.2 Criterio di divisibilità per i numeri della forma 10·n-1

L'osservazione della tabella *[4.2 tab.1]* ci suggerisce che il criterio di divisibilità per 19 si può generalizzare a tutti gli interi che terminano con la cifra 9, cioè a tutti gli interi della forma:

$$A = 10 \cdot n - 1 \qquad \forall\, n \in N$$

Cosicché, se *A* è formato da K cifre, sarà valida la congruenza:

*[6.2*1]* $A \equiv ((...(((a_1 \cdot n + a_2) \cdot n + a_3) \cdot n + a_4) \cdot n + \ ... \ + a_{k-1}) \cdot n + a_k) \cdot 10^{K-1}$

Applicando questa formula:
- per n = 1, ne seguirà il noto criterio di divisibilità per 9;
- per n = 2, si otterrà il criterio di divisibilità per 19 descritto prima;
- per n = 3 avremo il corrispondente criterio di divisibilità per 29.

[6.2a] - Dato il numero intero n, si moltiplichi per 3 la sua prima cifra a destra e si addizioni il prodotto alla seconda cifra; si moltiplichi il risultato per 3 e si addizioni il prodotto alla terza cifra; si continui così fino all'ultima cifra.
Se il risultato ottenuto con questo procedimento è multiplo di 29, è tale anche il numero n di partenza, se invece non è un multiplo di 29, non lo è nemmeno n.
Reiterano il procedimento, ogni volta si otterrà un valore minore del precedente; se il numero n di partenza è multiplo di 29, il risultato finale sarà 29.

[6.2e1] - Esempio.
Stabiliamo se 841 e 517 sono multipli di 29.

- Applicando il criterio di divisibilità per 29 ai due numeri, con facili calcoli, eseguibili a mente, otteniamo i risultati:

$$(1 \cdot 3 + 4) \cdot 3 + 8 = 29$$

$$(7 \cdot 3 + 1) \cdot 3 + 5 \equiv -7 \cdot 3 + 5 \equiv -16 \equiv$$
$$\equiv 13 \pmod{29}$$

Ne segue che 841 è multiplo di 29, mentre 517 non lo è.

Per 841 la congruenza, modulo 29, è immediata; per 517 invece la congruenza si avrà solo moltiplicando il risultato finale per 10^2.

$$841 \equiv 0 \pmod{29}$$

$$517 \equiv 13 \cdot 100 \equiv 24 \pmod{29}$$

Esempio [6.2*e*2]

Verifichiamo se sono divisibili per 29 i numeri:

$$7801\ ;\ 16783\ ;\ 43957929$$

I calcoli saranno più rapidi se ci aiuteremo con le congruenze.

- Applichiamo il criterio di divisibilità per 29 al primo numero:

$$((3\cdot 1+0)\cdot 3+8)\cdot 3+7 \equiv -12\cdot 3+7 \equiv 0 \pmod{29}$$

Pertanto 7801 è multiplo di 29.

- Applichiamo il criterio di divisibilità per 29 al secondo numero:

$$(((3\cdot 3+8)\cdot 3+7)\cdot 3+6)\cdot 3+1 \equiv (0\cdot 3+6)\cdot 3+1 \equiv 19 \pmod{29}$$

Pertanto 16783 non è multiplo di 29: $16783 \equiv 21 \pmod{29}$

- Applichiamo il criterio di divisibilità per 29 al terzo numero:

$$(((3\cdot 9+2)\cdot 3+9)\cdot 3+7)\cdot 3+5)\cdot 3+9)\cdot 3+3)\cdot 3+4 \equiv 25 \pmod{29}$$

Pertanto 43957929 non è multiplo di 29.

Però, se si osserva che 43957929 termina con 29, i calcoli si potranno fare più rapidamente. Infatti è valida la congruenza:

$$43957929 \equiv 439579\cdot 10^2 \pmod{29}$$

Ricordando poi le proprietà del paragrafo 2.1, si potranno semplificare ulteriormente i calcoli passando a quest'altra congruenza:

$$4.39.5.79.29 \equiv 41055\cdot 10^3 \pmod{29}$$

Cosicché si potrà applicare il criterio di divisibilità per 29 al 41055 anziché al 43957929, eseguendo i calcoli a mente:

$$(((3\cdot 5+5)\cdot 3+0)\cdot 3+1)\cdot 3+4 \equiv 25 \pmod{29}$$

Per $n \geq 4$ la formula *[6.2*1]* ci darà il corrispondente criterio di divisibilità, ma le applicazioni saranno via via sempre più difficoltosi.

Ad esempio, per stabilire se il numero 39737 è multiplo di 79, applicando più volte la formula *[6.2*1]* per $n = 8$, si avrà:

$$39737 > > 30731 > > 6083 > > 2054 > > 2370 > > 474 > > 316 > > 395$$

Applicando il criterio al 395 otteniamo ancora 395, per cui la reiterazione si conclude: $395 = 5\cdot 79$.

6.3 Criterio di divisibilità per 37

Se diamo un rapido sguardo alla tabella *[4.2 tab.1]*, anche per il numero primo 37 possiamo formulare un criterio di divisibilità davvero facile da applicare.
Da quanto abbiamo appreso nel cap. 5, la struttura dei coefficienti di divisibilità ha il sopravvento sui valori degli stessi coefficienti, di conseguenza ciò che realmente ci interessa sapere è la loro quantità. Dato che l'insieme dei coefficienti di divisibilità per 37 è formato da tre elementi soltanto, ogni multiplo n di 37, in modo analogo a quanto abbiamo dimostrato per 7 e per 13, è tale da potersi ridurre ad uno congruente di non più di tre cifre. Questa volta però bisogna stare attenti a considerare tutte positive le classi a tre cifre di n.

[6.3a] - Dato il numero intero n, iniziando da destra, si stacchino le sue cifre a gruppi di 3 e si calcoli la somma di tutte le classi.
Si ripeta la procedura fino ad ottenere un numero t con non più di tre cifre.
Se t è formato da tre cifre uguali, il numero n di partenza è multiplo di 37.
In questo caso n è congruo a t secondo il modulo 37.
Se t non è formato da tre cifre uguali, si moltiplichi per 3, riducendo eventualmente il prodotto a non più di tre cifre.
Se si ottiene adesso un numero con tre cifre uguali, il numero n di partenza è multiplo di 37, in caso contrario non lo è.

[6.3e1] - Esempi.

Stabiliamo se 34521 e 41567081 sono multipli di 37.

- Riduciamo il primo numero.

$$34.521 \equiv 555 \pmod{37}$$

Poiché si è ottenuto un numero a tre cifre uguali, ne segue che 34.521 è multiplo di 37
Infatti: $34521 = 37 \cdot 933$

- Riduciamo il secondo numero.

$$41.567.081 \equiv 689 \pmod{37}$$

Poiché non si è ottenuto un numero a tre cifre uguali, moltiplichiamo questo per 3:

$$689 \cdot 3 = 2.067 \text{ -----> } 69$$

Neanche adesso si è ottenuto un numero a tre cifre uguali, quindi 41567081 non è multiplo di 37.

Si tenga anche presente che

$$41567081 \not\equiv 69 \pmod{37}$$

Riflettendo su questo criterio, dedurremo che i criteri di divisibilità per 3 e per 37 si possono unificare.

[6.3b] - Dato l'intero n, si addizionino tutte le sue classi di tre cifre, ripetendo la procedura fino ad ottenere un numero t di non più di tre cifre.
Se le cifre di t sono tre e tutte uguali, il numero n è multiplo sia di 3 sia di 37.
In caso contrario si verifichi la divisibilità di t per 3.
Se t è divisibile per tre, dedurremo che n è divisibile per 3, ma non per 37.
Se t non è multiplo di tre, si moltiplichi per 3. Se questo prodotto si può ridurre a tre cifre uguali, n è multiplo di 37, altrimenti non lo è.

[6.3e2] - Esempio.

Stabiliamo la divisibilità per 3 e per 37 di 167351.

Riducendo a tre cifre, si avrà:

$167.351 \equiv 518 \pmod 3;(\text{mod.}37)$

Il numero ottenuto non ha le cifre uguali e non è multiplo di 3; dobbiamo fare un'altra prova, moltiplicandolo per 3:

$518 \cdot 3 = 1.554$ ------> 555

Adesso si è avuto un numero con tre cifre uguali, quindi 167351 è multiplo di 37, ma non di 3.

[6.3e3] - Esempi.

Stabiliamo la divisibilità per 3 e per 37 dei numeri:

110889, 163380911 e 1001010001000011

- Riduciamo 110889 :

$110.889 \equiv 999 \pmod 3 ; (\text{mod.}37)$

Si tratta quindi di un multiplo di 9 e di 37: $110.889 = 3^4 \cdot 37^2$

- Riduciamo 163380911 :

$163.380.911 \equiv 1454 \equiv 455 \pmod 3 ; (\text{mod.}37)$

Moltiplichiamo per 3: $455 \cdot 3 = 1.365$ -------> 366

Pertanto 163380911 non è multiplo né di 3 né di 37.

- Riduciamo 1001010001000011:

$1.001.010.001.000.011 \equiv 24 \pmod 3 ; (\text{mod.}37)$

Si è ottenuto un multiplo di 3 che non ha tre cifre uguali, quindi 1001010001000011 è multiplo di 3, ma non di 37.

$1001010001000011 = 3 \cdot 41 \cdot 101 \cdot 2713 \cdot 29700389$

6.4 Criterio di divisibilità per 17

La ricerca di un criterio di divisibilità per 17 non è immediato, ma l'elaborazione dei dati ci consentirà di ottenerne uno anche per questo numero.

Osservando la tabella *[4.2 tab.1]*, ci accorgiamo che i coefficienti di divisibilità per 17 hanno delle particolarità: essi formano un insieme ridotto di 8 cifre e sono distribuiti in modo tale da suggerire il seguente criterio.

[6.4a] - Dato il numero n, si proceda come è indicato di seguito.
La direzione sarà sempre da destra verso sinistra.

1) - Si stacchino le sue cifre a gruppi di 8.
Indicando con segno negativo le classi di posto pari, si calcoli la loro somma algebrica.
Si ripeta eventualmente la procedura fino ad ottenere un numero n_1 con non più di 8 cifre.

2) - Si stacchino le cifre di n_1 in due gruppi di 4.
Si moltiplichi per 4 la seconda classe e si addizioni il prodotto alla prima.
Si ripeta eventualmente la procedura fino ad ottenere un numero n_2 con non più di 4 cifre.

3) - Si stacchino le cifre di n_2 in due gruppi di 2.
Si moltiplichi per 2 la seconda classe e si sottragga il prodotto dalla prima.
Si ripeta eventualmente la procedura fino ad ottenere un numero n_3 con non più di 2 cifre.

4) - Se n_3 è multiplo di 17, lo è anche il numero n di partenza.
Viceversa, se n_3 non è multiplo di 17, non lo è neanche n.
Tutti i multipli di 17 a due cifre sono: 34, 51, 68, 85, facilmente riconoscibili perché divisibili pure o per 2, o per 3, o per 5.

Si tenga presente che vale sempre la congruenza:

$$n \equiv n_3 \pmod{17}$$

[6.4e1] - Esempio.
Stabiliamo la divisibilità per 17 di:

$$4097 - 5403 - 13481 - 83688565318023$$

- Poiché 4097 è formato da 4 cifre, applicheremo il criterio di divisibilità per 17 considerando solo il punto 3.
Riduciamolo ad uno congruente di non più di due cifre:

$$97-2\cdot 40 = 17$$

per cui valgono le congruenze:

$$40.97 \equiv 17 \equiv 0 \pmod{17}$$

Quindi 4097 è multiplo di 17.

- Anche 5403 è formato da quattro cifre, riduciamolo:

$$3-2\cdot 54 = -105 \text{ -----> } -(5-2) = -3$$

cosicché valgono le congruenze:

$$54.03 \equiv -3 \equiv 14 \pmod{17}$$

quindi 4097 non è multiplo di 17.

- Applichiamo il criterio di divisibilità al 13481, iniziando dal punto 2.
Riduciamolo prima ad uno congruente di non più di 4 cifre:

$$1\cdot 4 + 3481 = 3485$$

Riduciamolo poi ad uno congruente di non più di 2 cifre:

$$3485 \text{ -----> } 85-2\cdot 34 = 17$$

Quindi 13481 è multiplo di 17, perché valgono le congruenze:

$$1.3481 \equiv 34.85 \equiv 17 \pmod{17}$$

- Stabiliamo la divisibilità per 17 di 83688565318023.
1) Sostituiamo ad esso uno congruente di non più di 8 cifre:
$836885.65318023 \text{ ------> } 65318023-836885 = 64481138$
2) Sostituiamone uno di non più di 4 cifre:
$6448.1138 = 4\cdot 6448 + 1138 = 26930 \text{ -----> } 6938$
3) Sostituiamone uno di 2 cifre:

$$38-2\cdot 69 = -100 \text{ ----> } 2$$

Valgono quindi le congruenze:

$$836885.65318023 \equiv 69.38 \equiv -1.00 \equiv 2 \pmod{17}$$

Quindi 83688565318023 non è multiplo di 17.

7. AGGREGAZIONI DI NUMERI PRIMI

I benefici che abbiamo conseguito nei capitoli precedenti raggruppando sotto un'unica struttura i numeri primi 7, 11 e 13, ci incoraggiano a sviluppare ulteriormente questa prospettiva. Infatti sorge spontaneo il quesito se sia possibile aggregare ad essi qualche altro numero primo, ma anche, e soprattutto, se siano possibili delle altre aggregazioni di numeri primi.

7.1 I numeri primi 3 e 37

La ricerca di altri numeri primi da associare a 7, 11 e 13 ci induce a indagare sul 37 e sul 3, identificati come probabili per la quantità dei loro coefficienti di divisibilità: il 37 ne ha tre e il 3 soltanto uno. (Si veda la tabella *[4.2 tab1]*).

Dato l'intero n, se volessimo stabilire la sua divisibilità per 37 applicando la condizione di divisibilità, dovremmo staccare le sue cifre a gruppi di 3, perché 3 sono i coefficienti di divisibilità di 37. Successivamente potremmo ridurre n a un numero congruente di non più di 3 cifre, modulo 37, addizionando le classi ottenute.
E' da sottolineare che in questo caso dovremmo considerare le classi tutte positive.
Come abbiamo avuto modo di constatare nel paragrafo 5.3, le classi di tre cifre che si devono formare nella congruenza modulo 7 vanno invece considerate, alternativamente, positive e negative.
Pertanto la riduzione di n a tre cifre, nelle due congruenze, porta a risultati diversi, rendendo impossibile l'aggregazione di 37 al 7.
Analogamente accade per il numero primo 3, esso non si può associare al 7, perché le classi che si devono formare con le cifre dell'ipotetico n, si devono considerare tutte positive.

[7.1e1] - Esempio
Stabiliamo la divisibilità per 7 e per 37 di 380193093.

- Per verificare la divisibilità di 380193093 per 7, stacchiamo le sue cifre in classi di 3, considerandole, alternativamente, positive e negative: $380.\overline{193}.093$
Calcoliamo la loro somma algebrica:

$$380-193+093=280$$

Si ottiene così la congruenza:

$$380193093 \equiv 280 \equiv 0 \pmod{7}$$

- Per verificare la divisibilità di 380193093 per 37, stacchiamo le sue cifre ancora in classi di 3, ma questa volta le dobbiamo considerare tutte positive.
Calcoliamo la loro somma:

$$380+193+093=666$$

A questo numero possiamo applicare o la condizione di divisibilità: $666 \equiv 6 \cdot 26 + 6 \cdot 10 + 6 \cdot 1 \equiv 6 \cdot 37 \pmod{37}$
o, più semplicemente, il criterio di divisibilità descritto nel paragrafo 6.3. In ogni caso, sarà valida la congruenza:

$$380193093 \equiv 666 \equiv 0 \pmod{37}$$

Come era previsto, la riduzione a tre cifre di 380193093 nelle due congruenze, mod. 7 e mod. 37, ha dato risultati differenti, confermando così l'impossibilità di accorpare i numeri primi 7 e 37.

Il numero 3, avendo un solo coefficiente di divisibilità, si può aggregare facilmente a molti numeri primi, ma l'unione che gli si addice di più, come si constaterà meglio in seguito, è col 37.
E' possibile ampliare artificiosamente il periodo del 3, ripetendo tre volte il suo unico coefficiente, e creare così una struttura periodica di tre elementi, simile a quella del 37, i cui coefficienti sono realmente tre. (Si osservino le tabelle *[7.1a]* e *[7.1b]* seguenti).
Inoltre le classi che si formano con questo periodo artificioso sono da considerare tutte positive, così come sono tutte positive quelle relative al 37.
Ne segue che la riduzione a non più di tre cifre di un dato numero

n, sia secondo il modulo 37, sia secondo il modulo 3, porta allo stesso risultato e ciò rende possibile l'accorpamento di 3 e di 37.

[7.1a]

1 ; 10 ; 26 $\xrightarrow[\text{coefficienti di divisibilità per 37}]{\text{struttura periodica dell'insieme dei}}$ α; β; γ

[7.1b]

1 ; 1 ; 1 $\xrightarrow[\text{coefficienti di divisibilità per 3}]{\text{struttura periodica artificiosa dei}}$ α; β; γ

[7.1e2] - Esempio

Stabiliamo la divisibilità per 3 e per 37 di 10976605877603.

Possiamo verificare la divisibilità di 10.976.605.877.603 per 3 e per 37 simultaneamente staccando le sue cifre a gruppi di 3 e addizionando tutte le classi ottenute.

603 +
877
605
976
10
3071 ⟶ 074

La riduzione a tre cifre ci porta al numero 74 che è multiplo di 37, ma non di 3; quindi anche 10976605877603 è multiplo di 37, ma non di 3.

$10976605877603 \equiv 74 \pmod{3}, \pmod{37}$

$10976605877603 = 37 \cdot 59 \cdot 1433 \cdot 877 \cdot 4001$

7.2 Altri accorpamenti di numeri primi

Riflettendo sugli accorpamenti finora realizzati, dedurremo facilmente che l'aggregazioni tra due o più numeri primi è possibile se:
- le quantità dei loro coefficienti di divisibilità sono uguali;
- la quantità dei coefficienti di divisibilità di uno è un multiplo della quantità dei coefficienti di divisibilità di tutti gli altri.

In base a queste considerazioni, osservando la tabella *[4.2 tab1]*, possiamo formare questi altri raggruppamenti di numeri primi:

(3, 11) se si considerano classi di 2 cifre;
(3, 11, 101) se si considerano classi di 4 cifre;
(3, 7, 11, 13, 37) se si considerano classi di 6 cifre;
(3, 11, 73, 101, 137) se si considerano classi di 8 cifre.

[7.2e1] - Esempio
Scomponiamo 28594728019 in fattori primi.

1) - Accorpando i numeri primi 3, 7, 11, 13 e 37 possiamo pensare ad un'unica struttura periodica di 6 elementi.
Dividiamo 28594.728019 in classi di 6 cifre e addizioniamole:

$$28594 + 728019 = 756613$$

Otteniamo così una riduzione a 6 cifre secondo le congruenze:

$28594728019 \equiv 756613 \pmod{3},\pmod{7},\pmod{11},\pmod{13},\text{md.37}$

a) Se limitiamo poi l'accorpamento a 7, 11 e 13, sottraendo le due classi: 613-756 = -143 , possiamo ridurre ulteriormente a 3 cifre.

$$28594728019 \equiv -143 \pmod{7}, \pmod{11}, \pmod{13}$$

Da qui si deduce che 28594728019 è multiplo di 11 e di 13.

b) Se accorpiamo invece solo 3 e 37, possiamo ridurre a tre cifre addizionando le due classi: 613 + 756 = 1369 ----> 370

$$28594728019 \equiv 370 \pmod{3}, \pmod{37}$$

Da qui si deduce che 28594728019 è multiplo di 37.

2) Accorpando i numeri primi 11, 101, 73, e 137, possiamo pensare ad un'unica struttura periodica di 8 elementi.
Dividiamo 285.94728019 in classi di 8 cifre e addizioniamole:

$$285 + 94728019 = 94728304$$

Otteniamo così una riduzione a 8 cifre secondo le congruenze:

$28594728019 \equiv 94728304 \pmod{11}, \pmod{101}, \pmod{73}, \pmod{137}$

a) Se limitiamo poi l'accorpamento a 73 e 137, sottraendo le classi: 9472-8304 = 1168, possiamo ridurre ulteriormente a 4 cifre.

$$9472.8304 \equiv 1168 \pmod{73}, \pmod{137}$$

Da qui si deduce che 28594728019 è multiplo di 73.

b) Se accorpiamo invece solo 11 e 101, possiamo ridurre a 4 cifre addizionando le due classi: 9472 + 8304 = 17776 -----> 7777

$$9472.8304 \equiv 7777 \equiv 0 \pmod{101}, \pmod{11}$$

da qui si deduce che 28594728019 è multiplo di 101 e di 11.

Ecco allora la scomposizione completa:

$$28594728019 = 11 \cdot 13 \cdot 37 \cdot 73 \cdot 101 \cdot 733$$

7.3 Numeri primi sincroni

I risultati finora ottenuti avvalorano l'ipotesi che, per stabilire la divisibilità per un numero primo qualsiasi, non importa sapere quali siano i suoi coefficienti di divisibilità, ma quanti essi siano.

Per rendere l'esposizione più scorrevole, è opportuno semplificare alcuni concetti con delle definizioni.

- Diremo che sono "*sincroni*" i numeri interi che hanno la stessa quantità di coefficienti di divisibilità.
In modo equivalente, sono sincroni gli interi che generano numeri decimali periodici con la stessa quantità di cifre periodiche.

[7.3e1] - Esempi
Tenuto conto delle definizioni, diciamo che:
- i numeri primi 7 e 13 sono sincroni, di ordine 6;
- 37 è di ordine 3;
- 41 e 271 sono sincroni, di ordine 5.

- Diremo che un numero intero p che ha n coefficienti di divisibilità è di ordine n.
Dicendo che "*p è di ordine n*" intenderemo asserire che l'inverso del numero intero p genera un numero decimale illimitato periodico, il cui periodo è formato da n cifre.

La caratteristica fondamentale della matematica è il numero, il quale esprime una "*quantità*".
Adesso è la stessa quantità che diventa oggetto delle nostre osservazioni e le proprietà che via via emergeranno si dovranno esprimere in termini numerici.
Si consideri infatti che la caratteristica comune ai numeri interi sincroni è un numero intero, per cui, indagare sulle proprietà di questi numeri, è come seguire il filo che si avvolge su sé stesso in una matassa.
Qual è il suo bandolo?
Per trovarlo dobbiamo andare alla ricerca di un principio di semplificazione, simile a quello che si incontra in altre situazioni matematiche, che potremmo definire:

"*passaggio ad esponente*"

Per fare progredire la nostra ricerca ci occorrono altri numeri primi sincroni, ma è necessario snellire le procedure seguite finora per ottenerli.
Continuare a calcolare i coefficienti di divisibilità, per poi confrontare le potenze degli insiemi ottenuti, sarebbe un lavoro lungo, che oltretutto non è nemmeno necessario. Infatti la quantità dei coefficienti di divisibilità di ciascun numero primo p coincide con la quantità delle cifre periodiche che si ottengono dalla divisione per p di una qualsiasi potenza di 10, compresa la potenza 10^0.
Cosicché, in pratica, è sufficiente calcolare il reciproco del numero primo p in considerazione e contare le cifre del suo periodo.

[7.3e2] - Esempio
Stabiliamo l'ordine di 41 e 271.

Per calcolare la quantità dei coefficienti di divisibilità dei numeri primi 41 e 271 basta eseguire le divisioni:

$$1:41 = 0,\overline{02439} \quad ; \quad 1:271 = 0,\overline{00369}$$

Sia 41, sia 271 danno origine a numeri periodici con periodi di 5 cifre. Diciamo quindi che 41 e 271 sono sincroni, di ordine 5.
La caratteristica numerica che accomuna questi due numeri primi è il numero 5.

E' evidente che la ricerca dell'ordine di ciascun numero intero dipende dalla potenza di calcolo dello strumento di cui si dispone, tanto è vero che, passando in rassegna i numeri primi, si arriva rapidamente a periodi molto lunghi.
Se volessimo stabilire, ad esempio, l'ordine di 1801, per trovarlo dovremmo calcolare ben 900 cifre decimali!
Ma la difficoltà maggiore si incontrerebbe nel momento in cui volessimo trovare i numeri primi di ordine assegnato.
Qual'è, ad esempio, il numero primo di ordine 93?
Il procedimento di calcolo per arrivare a questo numero:
900900900900900900900900900900990990990990990990990990990991
formato da 60 di cifre, è molto più complesso del caso precedente.

7.4 I numeri n esp1

Vediamo quali numeri sincroni possiamo trovare con l'utilizzo di strumenti facilmente reperibili: una calcolatrice a 10 cifre e una tavola di numeri primi inferiori a 10.000.
Calcolando gli inversi di tutti questi numeri primi, nei limiti imposti dalla nostra calcolatrice, troveremo le coppie sincrone della tabella *[7.4 tab1]* seguente.
Il numeretto in basso alla parentesi tonda indica la caratteristica di ciascuna coppia, cioè la quantità che abbiamo definito *"ordine"*.

$(41\ ;\ 271)_5$	;	$(7\ ;\ 13)_6$	*[7.4 tab1]*
$(239\ ;\ 4649)_7$	;	$(73\ ;\ 137)_8$	

Verifichiamo se anche per questi numeri primi sincroni sono valide le proprietà riscontrate nei precedenti raggruppamenti.

[7.4e1] - Esempio
Stabiliamo se sono multipli di 41 e di 271 i numeri:

14306827943 ; 241801078171 ; 6720619062459529

Considerando che gli interi 41 e 271 sono entrambi di ordine 5 (vedi la *[7.4 tab1])*, li accorpiamo. Cosicché, ripetendo con questa coppia di sincroni i ragionamenti fatti nel 5° capitolo col 7 e col 13, riduciamo i numeri dati a 5 cifre, senza preoccuparci di stabilire quali siano i coefficienti di divisibilità per 41 e per 271.
Stacchiamo le cifre di ciascuno dei numeri dati a gruppi di 5 e addizioniamo le classi ottenute.
Avremo così le congruenze:

$$1.43068.27943 \equiv 71012 \quad (\text{mod. } 41)\ ,\ (\text{mod.}271)$$
$$24.18010.78171 \equiv 96205 \quad (\text{mod. } 41)\ ,\ (\text{mod.}271)$$
$$6.72061.90624.59529 \equiv 22222 \quad (\text{mod. } 41)\ ,\ (\text{mod.}271)$$

Adesso, anche con la nostra ordinaria calcolatrice a 10 cifre, ci è possibile stabilire che il primo numero è multiplo di 41, il secondo di 271 e il terzo di entrambi.

Osserviamo i calcoli di quest'ultimo esempio: nella congruenza relativa al terzo numero, a secondo membro, le cinque cifre sono tutte uguali.
Questo evento, in un tale genere di calcoli coi numeri sincroni, apparirà ricorrente, per cui dobbiamo chiederci, ragionevolmente, se esso sia casuale oppure no.
Al fine di avere una risposta a questo quesito, si cambino i dati dell'esercizio *[7.4e1]* e si rifacciano i calcoli: sicuramente, ogni qualvolta il numero in esame sarà multiplo contemporaneamente di 41 e di 271, l'evento si verificherà ancora: le cinque cifre della corrispondente congruenza risulteranno uguali.

A questo punto è importante stabilire se questa circostanza si manifesta anche con altri primi sincroni.
Facciamo delle verifiche con le coppie della tabella *[7.4 tab1]*.

$41 \cdot 271 = 11111$
$239 \cdot 4649 = 1111111$
$7 \cdot 13 = 91$
$73 \cdot 137 = 10001$

L'evento si verifica nuovamente con la coppia $(239 ; 4649)_7$.
Non si verifica invece con le coppie: $(7 ; 13)_6$ e $(73 ; 137)_8$

Se consideriamo anche gli accorpamenti trovati in precedenza nel paragrafo 7.2 , possiamo constatare che l'evento si verifica ancora con la coppia (3 ; 37).
Si verifica anche se si aggregano:
- alla coppia $(7;13)_6$, il 3, il 37 e l' 11;
- alla coppia $(73; 137)_8$, l' 11 e il 101.

$3 \cdot 37 = 111$
$7 \cdot 13 \cdot 3 \cdot 37 \cdot 11 = 111111$
$73 \cdot 137 \cdot 11 \cdot 101 = 11111111$

Per indagare più a fondo sulla questione, sono necessari altri dati, ma occorre uno strumento di calcolo più potente della nostra calcolatrice a 10 cifre. Proviamo allora con la calcolatrice di Windows, che mette a disposizione ben 32 cifre decimali.
Troveremo così i raggruppamenti della tabella *[7.4 tab2]* seguente.

[7.4 tab2]

$(53; 79)_{13}$; $(43; 1933)_{21}$;
$(23; 4093; 8779)_{22}$; $(29; 281)_{28}$
$(211; 241; 2161)_{30}$

Questi nuovi dati rivelano un evento che non si era ancora verificato: i numeri sincroni possono essere più di 2.

Eseguendo i calcoli con questi raggruppamenti, nessun risultato però è quello sperato, cioè con le cifre tutte uguali.
Si veda la tabella accanto.

$53 \cdot 79 = 4187$
$43 \cdot 1933 = 83119$
$23 \cdot 4093 \cdot 8779 = 826446281$
$29 \cdot 281 = 8149$
$211 \cdot 241 \cdot 2161 = 109889011$

Cosicché il ricorso alla calcolatrice di Windows è deludente: sia le 32 cifre decimali, sia i numeri primi inferiori a 10000, risultano insufficienti a farci progredire nella nostra ricerca.
Del resto ci dobbiamo rendere conto che i numeri sincroni trovati finora sono casi molto particolari, perché la divisione per un numero intero n può dare origine a n resti distinti.
L'avere trovato il periodo 5 con i numeri 41 e 271 è stato sicuramente un evento fortuito. Se 41 avesse avuto ordine 40 e 271 ordine 270, con i mezzi ordinari i calcoli sarebbero stati impossibili.

Data la difficoltà a trovare altri indizi a favore delle nostre ipotesi, proviamo ad aggirare l'ostacolo: invertendo il senso di marcia, scomponiamo i numeri a cui pensavamo di arrivare.
Forniamoci di un programma di scomposizione in fattori primi e andiamo avanti. (Per il lettore è disponibile il programma di scomposizione, utilizzabile con Excel, allegato alla presente opera).
Troveremo così i risultati della tabella *[7.4 tab3]* seguente.

Anche questa volta si arriverà ben presto al limite del nostro strumento di calcolo: con Excel non è possibile andare oltre le 15 cifre.
Tuttavia coi risultati trovati avremo delle certezze in più.
Infatti, mettendo a confronto questi nuovi dati con i precedenti, le vaghe impressioni iniziali appariranno più consistenti.
Se analizziamo la tabella *[7.4 tab3]*, ci accorgeremo che tra i fattori di alcune scomposizioni sono inclusi i numeri primi sincroni trovati precedentemente per altra via.
Ad esempio, i numeri sincroni della coppia $(53 ; 79)_{13}$, presente nella tabella *[7.4 tab2]* , li ritroviamo nella scomposizione di indice 13

della tabella *[7.4 tab3]* , ma ad essi si aggiunge ora un terzo numero primo, il 265371653.
Per indagare su questo accorpamento dobbiamo stabilire qual è l'ordine di quest'altro primo.
Facendo il calcolo con la calcolatrice di Windows, ci accorgeremo che anche 265371653, alla stessa stregua di 53 e 79, ha ordine 13.
Quindi questa scomposizione ci ha dato tre primi sincroni.

Anche gli altri accorpamenti di numeri primi, individuati dalle scomposizioni, presentano situazioni simili.
Adesso non ci resta altro da fare che elaborare i dati ottenuti.
Ci faremo così un'idea più precisa e completa sul modo in cui si aggregano i numeri primi.

Nel prossimo capitolo dimostreremo le deduzioni tratte dalle nostre osservazioni.

[7.4 tab3]

$^{3}1 = 111 = 3 \cdot 37$
$^{4}1 = 1111 = 11 \cdot 101$
$^{5}1 = 11111 = 41 \cdot 271$
$^{6}1 = 111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$
$^{7}1 = 1111111 = 239 \cdot 4649$
$^{8}1 = 11111111 = 11 \cdot 73 \cdot 101 \cdot 137$
$^{9}1 = 111111111 = 3 \cdot 3 \cdot 37 \cdot 333667$
$^{10}1 = 1111111111 = 11 \cdot 41 \cdot 271 \cdot 9091$
$^{11}1 = 11111111111 = 21649 \cdot 513239$
$^{12}1 = 111111111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$
$^{13}1 = 1111111111111 = 53 \cdot 79 \cdot 265371653$
$^{14}1 = 11111111111111 = 11 \cdot 239 \cdot 4649 \cdot 909091$
$^{15}1 = 111111111111111 = 3 \cdot 31 \cdot 37 \cdot 41 \cdot 271 \cdot 2906161$
$^{16}1 = 1111111111111111 = ?$

Per facilitare la lettura dei numeri della tabella, abbiamo indicato ad esponente, a sinistra, quante volte si ripete la cifra 1.
In inglese tali numeri sono indicati col termine "*repunit*" per rimarcare la ripetitività della cifra 1.

Noi, nella nostra trattazione, li denomineremo invece *"numeri n esp1"*, specificando con n quante volte si ripete la cifra 1.
Si è preferito il termine *"esp"* in accordo con la semplificazione esponenziale usata.
E' bene informare il lettore che al nostro vocabolo *"ordine"* corrisponde in inglese la frase: *"period length of the decimal expansion"*.

Le caratteristiche dei raggruppamenti di numeri primi ci offrono la divertente applicazione dell'esempio seguente.

[7.4e2] - Esempio
Dato il numero 1860790044610366931061 di 22 cifre, si stacchino le cifre a gruppi di 7 e si addizionino le classi.
Si ripeta eventualmente più volte la procedura, fino ad ottenere un numero con 7 cifre soltanto.
1.8607900.4461036.6931061

```
 6931061 +
 4461036
 8607900
       1
--------
19999998  > > 9999999
```

Il risultato finale è un numero con 7 cifre uguali.

Si rifacciano i calcoli staccando le cifre, progressivamente, in classi di 6, 5, 4, 3 e 2.

```
 931061 +
 610366
 790044
   1860
-------
2333331  > > 333333
```

```
 31061 +
 03669
 04461
 60790
    18
-------
99999  > > 99999
```

```
 61 +
 10
 93
 66
 03
 61
 44
 00
 79
 60
 18
----
495  > > 99
```

```
 1061 +
 6693
 6103
 0044
 6079
   18
-------
19998  > > 9999
```

```
 061 +
 931
 366
 610
 044
 790
 860
   1
------
3663  > > 666
```

Come si può notare, i risultati hanno sempre le cifre uguali.

8.1 Definizioni e concetti

In questo capitolo vedremo quali proprietà si possono dedurre elaborando i dati della tabella *[7.4 tab3]*.
Per rendere più scorrevole la trattazione è opportuno però sintetizzare alcuni concetti con delle definizioni.

I numeri che hanno tutte o molte cifre consecutive uguali possiamo indicarli in modo più sintetico con le seguenti notazioni.
Scriviamo la cifra una sola volta e indichiamo ad esponente, alla sua sinistra, quante volte si ripete.
esempi:
$1111111 = {}^{7}1$ (leggi: 7 esp1)
$99999999 = {}^{8}9$ (8 esp9)
$234000000000000000000071 = 234^{19}071$ (234, 19 esp0, 71)

- L'insieme di tutti i numeri primi il cui prodotto è un n esp1 si dirà:
sistema n dei numeri primi
o, più semplicemente,
sistema n.
-il sottinsieme del sistema n, formato solo dai primi di ordine n, si dirà:
sistema dei primi di ordine n
- *ogni* sottinsieme del sistema n che forma un sistema di ordine inferiore a n si dirà:
sistema sub-n
- ogni primo del sistema n, il cui prodotto con tutti i primi di ordine n è un numero della forma $10^n + 1$, si dirà:
ausiliare dei primi di ordine n.

[8.1e1] - Esempio
Sia dato il numero 6 esp1:
${}^{6}1 = 111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 3$
- Il sistema 6 è:
${}^{6}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\}$
- Il sistema dei primi di ordine 6 è il sottinsieme:
${}^{6}S = \{7\text{-}13\}$
- I sottinsiemi:
${}^{3}\overline{S} = \{3\text{-}37\}$; ${}^{2}\overline{S} = \{11\}$
sono sistemi sub-6.
- 11 è ausiliare dei primi di ordine 6:
$11 \cdot 7 \cdot 13 = 10^3 + 1$

8.2 Proprietà degli n esp1

[8.2a] - *Ogni numero della forma* $^{n}1$ *ha ordine n.*

La dimostrazione è immediata se esaminiamo i coefficienti di divisibilità per $^{n}1$.

Le divisioni delle successive potenze di 10 per $^{n}1$ generano i resti:

$$1 ; 10 ; 10^2 ; \ldots ; 10^{n-1} ; 1 \ldots$$

Tra tutte quindi si deve prendere in considerazione la divisione:

$$10^n = 9 \cdot {}^{n}1 + 1$$

la quale ci fornisce la congruenza:

$$10^n \equiv 1 \pmod{{}^{n}1}$$

Dato che 10^n è la prima potenza di 10 a ripetere il resto 1, l'insieme dei coefficienti di divisibilità per $^{n}1$ è formato da n elementi:

$$1 ; 10 ; 10^2 ; \ldots ; 10^{n-1}$$

Di conseguenza l'ordine di $^{n}1$ è n.

[8.2e1] - Esempi

Stabiliamo quale ordine hanno 1111111 e 111111111111.

Poiché questi sono numeri n esp1, per stabilire il loro ordine è sufficiente contare le cifre di ciascuno di essi.

Se li scriviamo in forma sintetica, visualizzeremo i loro ordine ad esponente:

$1111111 = {}^{7}1$ questo numero ha ordine 7

$111111111111 = {}^{12}1$ questo numero ha ordine 12

Possiamo averne una conferma calcolando i loro inversi:

$1 :{}^{7}1 = 0,\overline{0000009}$ il periodo è formato da 7 cifre

$1 :{}^{12}1 = 0,\overline{000000000009}$ il periodo è formato da 12 cifre

Le divisioni elementari ci danno le seguenti congruenze.

$$10^7 = 9 \cdot {}^{7}1 + 1 \quad \Rightarrow \quad 10^7 \equiv 1 \pmod{{}^{7}1}$$

$$10^{12} = 9 \cdot {}^{12}1 + 1 \quad \Rightarrow \quad 10^{12} \equiv 1 \pmod{{}^{12}1}$$

[8.2b] - *Ogni* $^{n}1$ *è multiplo di ciascun numero intero p di ordine n.*

La dimostrazione è semplice.

Dato il generico numero $^{n}1$, sia p un intero che abbia n coefficienti di divisibilità: $a_1,a_2,....,a_n$, cioè tanti quanti sono le cifre di $^{n}1$.

Applichiamo a $^{n}1$ la condizione di divisibilità per p (vedi *[4.1a]).*

$$111...111 \equiv 1 \cdot a_1 + 1 \cdot a_2 + ... + 1 \cdot a_n \quad (\text{mod. } p)$$

Dato che le n cifre di $^{n}1$ sono tutte uguali ad 1, il secondo membro di questa congruenza è uguale alla somma di tutti i coefficienti di divisibilità per p:

$$111...111 \equiv a_1 + a_2 + ... + a_n \quad (\text{mod. } p)$$

Ma

la somma dei coefficienti di divisibilità per p è un multiplo di p,

cosicché $111...111 \equiv m \cdot p \quad (\text{mod. } p)$

quindi $^{n}1 \equiv 0 \quad (\text{mod.p})$ per qualunque p di ordine n.

Ciò dimostra il teorema.

[8.2e2] - Esempio

Verifichiamo che $^{5}1 = 11111$ è multiplo di ogni intero di ordine 5.

Nella *[7.4 tab1]* troviamo due primi di ordine 5: il 41 e il 271.

La verifica che 11111 è multiplo sia di 41 sia di 271 è immediata:

$$11111 = 41 \cdot 271$$

E' evidente che non ci può essere qualche altro primo di ordine 5, perché, se ci fosse, anch'esso sarebbe un divisore di 11111.

Ma che ci sia un altro divisore primo di $^{5}1$, oltre a 41 e 271, è impossibile, perché la scomposizione in fattori primi è unica.

L'unico numero composto di ordine 5 è lo stesso $^{5}1$.

Non ci possono essere altri numeri composti di ordine 5 perché, se ci fossero, dovrebbero dividere $^{5}1$, ma l'unico numero composto, divisore di $^{5}1$, è lo stesso $^{5}1$.

Cosicché possiamo concludere che la scomposizione di $^{5}1$ in fattori ci consente di trovare tutti gli interi di ordine 5, sia quelli primi, sia quelli composti.

[8.2e3] - Esempio
Dati i numeri 21 e 3367 stabiliamo se sono divisori di qualche numero della forma ${}^{n}1$.

Calcolando gli inversi:

$$1:21 = 0,\overline{047619} \quad ; \quad 1:3367 = 0,\overline{000297}$$

ci accorgiamo facilmente che entrambi sono di ordine 6, per cui, sia 21 sia 3367 dividono ${}^{6}1$.

Infatti: $111111 = 5291 \cdot 21 = 33 \cdot 3367$

La scomposizione di ${}^{6}1$, ci fornisce il sistema di ordine 6:

$$111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \quad \Rightarrow \quad {}^{6}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\}$$

Poiché 21 e 3367, pur essendo entrambi di ordine 6, non fanno parte del sistema 6 dei numeri primi, deduciamo che:
- non sono numeri primi;
- sono multipli di alcuni numeri primi del sistema 6.

Infatti: $21 = 3 \cdot 7 \quad ; \quad 3367 = 7 \cdot 13 \cdot 37$

[8.2c] - Dato il numero ${}^{n}1$, se n è composto, sia d un divisore di n.
Ogni intero di ordine d è divisore di ${}^{n}1$.

Anche in questo caso la dimostrazione è semplice.
L'esponente n indica quante sono le cifre di ${}^{n}1$ e, per l'ipotesi fatta, è un numero composto.
Se d è un divisore di n, possiamo formare n/d classi di cifre uguali, possiamo cioè staccare le cifre di ${}^{n}1$ e formare n/d volte ${}^{d}1$.
Per la *[1.2a]*, ${}^{n}1$ è divisibile per ${}^{d}1$, per cui vale l'uguaglianza:

$${}^{n}1 = m \cdot {}^{d}1$$

Per il teorema precedente ${}^{d}1$ è divisibile per ogni intero di ordine d, per cui, indicando con k_d uno qualsiasi di questi divisori di ordine d, l'uguaglianza precedente si trasforma in quest'altra:

$${}^{n}1 = m \cdot k_d \cdot b$$

Cosicché il teorema è dimostrato.

[8.2e4] - Esempio
Dato $^{6}7$, verifichiamo che esso è multiplo di tutti gli interi che hanno come ordine un divisore dell'esponente 6.

L' insieme dei divisori di 6: $D_6 = \{1\text{-}2\text{-}3\text{-}6\}$, ci indica che le cifre di 777777 si possono staccare in classi uguali in tutti questi modi:

7.7.7.7.7.7 (Si formano 6 classi, ciascuna uguale a 1 esp7)
77.77.77 (Si formano 3 classi, ciascuna uguale a 2 esp7)
777.777 (Si formano 2 classi, ciascuna uguale a 3 esp7)
777777 (Si forma 1 classe 6 esp7)

cosicché $^{6}7$ è divisibile per: $^{1}7$, $^{2}7$, $^{3}7$, $^{6}7$

$^{1}7$ è divisibile per 7, per cui $^{6}7$ è multiplo di 7.

Conviene eliminare il fattore 7 da $^{6}7$ e ridurre il numero alla forma $^{6}1$, cosicché possiamo leggere i fattori dei sistemi n esp1 sulla tabella *[8.3 tab1]*.
Per evitare di ripetere gli stessi fattori, tuttavia è preferibile considerare solo i divisori di ordine proprio elencati nella *[8.3 tab2]* .

$^{2}1$ è divisibile per 11, per cui $^{6}1$ è multiplo di 11;
$^{3}1$ è divisibile per 3 e per 37, per cui $^{6}1$ è multiplo di 3 e di 37;
$^{6}1$ è divisibile per 7 e per 13, per cui $^{6}1$ è multiplo di 7 e di 13.

Infatti: $777777 = 3 \cdot 7^{2} \cdot 11 \cdot 13 \cdot 37$

[8.2d] - *Ogni sistema n di numeri primi è un insieme chiuso.*

Abbiamo scelto il termine "*sistema*" perché i numeri primi si combinano tra loro in modo tale che il prodotto di ciascuno dei loro raggruppamenti formi un numero n esp1.
Con il termine "*chiuso*" invece abbiamo voluto indicare che l'ordine di ciascun divisore di $^{n}1$ non è mai maggiore di n.
Infatti:
- l'ordine di ogni fattore primo del sistema $^{n}1$ è n o un divisore di n;
- l'ordine del prodotto di due o più elementi differenti di $^{n}1$ è uguale al minimo comune multiplo dei loro ordini.

[8.2e5] - Esempio
Dato l'esp $^{12}1$, il sistema 12 dei numeri primi è:

$$^{12}\overline{S} = \{3 ; 7 ; 11 ; 13 ; 37 ; 101 ; 9901\}$$

- $^{12}1$ ha ordine 12, uguale al minimo comune multiplo di tutti gli ordini del sistema;
- 3 e 11 hanno rispettivamente ordine 1 e 2 e il loro prodotto 33 ha ordine 2, uguale al m.c.m. degli ordini 2 e 1;
- 7 e 13 hanno entrambi ordine 6 e così pure il loro prodotto 91;
- 37 ha ordine 3 e 9901 ordine 12, il loro prodotto 366337 ha ordine 12;
- 37 e 101 hanno ordine 3 e 4, primi tra loro; il loro prodotto 3737 ha ordine 12, uguale al prodotto dei loro ordini;
- 7 ha ordine 6 e 101 ordine 4, il loro prodotto 707 ha ordine 12;
- il prodotto $28207949 = 7 \cdot 11 \cdot 37 \cdot 9901$ ha ordine uguale al m.c.m. degli ordini dei suoi fattori, cioè 12.

In ogni caso il prodotto di due o più elementi di $^{12}\overline{S}$ non può avere un ordine maggiore dell'ordine 12 di $^{12}1$.

Nota bene: diverso è il caso in cui si moltiplica un elemento del sistema n per sé stesso: in questo caso l'ordine della potenza si ottiene moltiplicando l'ordine della base per la base.
es.: 101^2 ha ordine 404 ($404 = 4 \cdot 101$) ; 7^2 ha ordine 42 ($42 = 6 \cdot 7$)

[8.2e] - *Dato $^n1$, se n è primo, i suoi divisori sono tutti* di ordine *n*.

Questo è un caso particolare del teorema *[8.2c]*.
Poiché n è primo, gli unici divisori di n sono 1 ed n stesso, di conseguenza $^n1$ è divisibile solo per gli esp: $^1 1$ e $^n1$.
L'unico elemento del sistema 1 è la base di $^n1$, mentre gli elementi del sistema n devono avere o ordine n o ordine divisore di n, ma n è primo quindi devono avere, necessariamente, ordine n.
Pertanto i divisori di $^n1$ sono i numeri primi di ordine n e i multipli che si ottengono come prodotto di questi primi.
Questi multipli, dovendo avere ordine uguale al m. c. m. degli ordini dei loro fattori, sono necessariamente anch'essi di ordine n.

[8.2e6] - Esempio.
Dato $^{7}1$, scomponiamolo in fattori primi: $1111111 = 239 \cdot 4649$
Poiché il suo esponente è un numero primo, $^{7}1$ non è divisibile per nessun altro esp1 con esponente diverso da 1 e da 7.
Quindi il sistema 7 è privo di sistemi sub-7 e coincide con il sistema dei primi di ordine 7:

$$^{7}\overline{S} = {}^{7}S = \{239 - 4649\}$$

Ne segue che i due fattori di $^{7}1$ hanno necessariamente ordine 7.
Infatti: $1 : 239 = 0,\overline{0041841}$; $1 : 4649 = 0,\overline{0002151}$
L'unico numero multiplo, divisore di $^{7}1$, è lo stesso $^{7}1$, il quale, come sappiamo dalla *[8.2a]* , ha ordine 7.

[8.2e7] - Esempio.
Dato $^{13}1$, scomponiamolo in fattori primi: $^{13}1 = 53 \cdot 79 \cdot 265371653$
Poiché l'esponente 13 è primo, non ci sono sistemi sub-13, cosicché il sistema 13 coincide col sistema dei primi di ordine 13:

$$^{13}\overline{S} = {}^{13}S = \{53 ; 79 ; 265371653\}$$

Ne segue che tutti i divisori primi di $^{13}1$ hanno ordine 13.
I numeri multipli, divisori di $^{13}1$, sono quelli che si ottengono moltiplicando tra loro i numeri primi del sistema:

$53 \cdot 79 = 4187$; $53 \cdot 265371653 = 14064697609$
$79 \cdot 265371653 = 20964360587$; $53 \cdot 79 \cdot 265371653 = {}^{13}1$

Questi multipli hanno ordine uguale al m.c.m. degli ordini dei loro fattori, quindi hanno anch'essi ordine 13.

[8.2f] - Il teorema [8.2e] ci dice che ogni sistema n di numeri primi, con n primo, è formato solo da numeri primi di ordine n.
Se accade che $^{n}1$ sia un numero primo, il sistema n di numeri primi avrà un solo elemento di ordine n e coincide con lo stesso $^{n}1$.

E' un esempio il sistema 19: $^{19}\overline{S} = \{{}^{19}1\}$

Questo è *formato dal solo numero primo $^{19}1$, il quale, ovviamente, ha ordine 19.*

[8.2g] - Condizione necessaria e sufficiente affinché p sia primo è che appartenga al sistema dei primi di ordine n, essendo n l'ordine di p.

Nel caso di p primo, si consideri che:

a) n è uguale a p-1 o ad un divisore di p-1;
b) p divide $^{n}1$.

La validità di queste asserzioni deriva dai teoremi precedenti.

[8.2e8] - Esempio.
Stabiliamo se 31 e 1356437 sono numeri primi o multipli.

- 31 ha ordine 15 e il teorema *[8.2b]* ci assicura che divide $^{15}1$.
Poiché 31 fa parte del sistema dei primi di ordine 15, esso è primo. (Si veda la tabella *[8.3 tab2]).*
Se non avessimo avuto la possibilità di conoscesse l'ordine di 31, avremmo potuto considerarlo uguale a 30 (n = p-1).
In questo caso, dato che la divisione $^{30}1/31$ è possibile, la conclusione sarebbe stata la stessa, perché avremmo trovato il 31 nel sistema 30 dei numeri primi. (Si veda la tabella *[8.3 tab1]).*

- 1356437 ha ordine 24, ma, poiché non fa parte del sistema dei primi di ordine 24, esso non è primo. Il teorema *[8.2b]* ci assicura comunque che esso divide $^{24}1$, per cui dobbiamo dedurre che è multiplo di alcuni primi del sistema 24:

$$^{24}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\text{-}73\text{-}101\text{-}137\text{-}9901\text{-}99990001\}$$

Infatti: $1356437 = 137 \cdot 9901$

Per trovare l'ordine di 31 e di 1356437 basta calcolare i loro inversi con la calcolatrice di Windows:

$1/31 = 0{,}032258064516129032258064516129032....$
il periodo è 032258064516129 ed è formato da 15 cifre, quindi l'ordine di 31 è 15.

$1/1356437 = 0{,}000000737225540146722627000000737225 54.....$
il periodo è formato da 24 cifre, quindi l'ordine di 1356437 è 24.

Ci si può servire anche del programma allegato alla presente opera, installandolo su excel; esso fornisce direttamente l'ordine del numero intero inserito.

[8.2e9] - Esempio.
Stabiliamo se 4226364059 è numero primo.

4226364059 ha ordine 14, per cui divide $^{14}1$.
Poiché l'esponente è pari, si ha l'uguaglianza:

$$^{14}1 = {}^{7}1 \cdot (10^7 + 1)$$

Per cui 4226364059 è primo solo se divide 10000001, ma, in modo evidente, ciò è impossibile, quindi è composto.

Cerchiamo i suoi fattori.
L'esponente di $^{14}1$ ha i divisori:

$$D_{14} = \{1, 2, 7, 14\}$$

Tenuto conto di questi divisori, possiamo asserire che:
- non è possibile che i fattori cercati abbiano tutti ordine 7;
- tra essi ci deve essere o uno di ordine 2 o uno di ordine 14.

Quindi tra i fattori di 4226364059 ci deve essere o 11 o 909091.

Infatti: $4226364059 = 4649 \cdot 909091$

[8.2e10] - Esempio.
Stabiliamo se 264307843 è numero primo.

Per calcolare l'ordine di questo numero la calcolatrice di Windows è inadeguata; se utilizziamo invece il programma allegato a questa opera, si troverà subito che il suo ordine è 43.
Quindi 264307843 divide $^{43}1$.
Poiché l'esponente di $^{43}1$ è un numero primo, tutti gli elementi del sistema 43, sono di ordine 43:

$$^{43}\overline{S} = \{173\text{-}1527791\text{-}1963506722254397\text{-}21409920153955266 41\}$$

Il nostro numero non si trova tra questi, per cui è composto e i suoi fattori sono alcuni di essi.

Dato che 264307843 è formato da sole 9 cifre, non può che essere multiplo di 173 e di 1527791.

Infatti: $264307843 = 173 \cdot 1527791$

[8.2e11] - Esempio.
Stabiliamo se 10838689, 20951185837 e 5593186232871 sono primi o multipli.

L'ordine di tutti e tre è 21, per cui ciascuno di essi divide $^{21}1$.
Le nostre ricerche vanno quindi fatte all'interno del sistema 21:

$$^{21}\overline{S} = \{3\text{-}37\text{-}43\text{-}239\text{-}1933\text{-}4649\text{-}10838689\}$$

Osservando questo sistema, ci accorgiamo che 10838689 è numero primo, mentre gli altri due sono composti.

- Cerchiamo i fattori primi di 20951185837
Stabilito che i divisori dell'esponente 21 di $^{21}1$ sono:

$$D_{21} = \{1,3,7,21\}$$

eseguiamo la divisione $^{21}1/(^{3}1 \cdot ^{7}1)$
e otteniamo l'uguaglianza: $^{21}1 = ^{3}1 \cdot ^{7}1 \cdot 900900990991$
dove 900900990991 è il prodotto di tutti i primi di ordine 21.
Poiché il nostro numero divide 900900990991:

$$900900990991 : 20951185837 = 43$$

ne segue che esso è multiplo degli altri due di ordine 21:

$$^{21}S = \{43\text{-}1933\text{-}10838689\}$$

$$20951185837 = 10838689 \cdot 1933$$

- Cerchiamo i fattori primi di 5593186232871.
In modo evidente, esso non divide 900900990991, per cui i divisori cercati non possono essere tutti di ordine 21; del resto non possono essere neanche tutti di ordine 3, né tutti di ordine 7.
I criteri di divisibilità ci dicono che è divisibile per 3 e per 37:

$$5593186232871/111 = 50389065161$$

Provando con qualche altra divisione tra quest'ultimo numero e quelli del sistema 21, infine avremo la scomposizione completa:

$$5593186232871 = 3 \cdot 37 \cdot 4649 \cdot 10838689$$

I numeri del tipo: $10^n + 1$; 9090...91 ; 900900....990991 ; ...
sono alcuni dei contenitori di numeri primi di ordine n; la loro scomposizione ci fa risparmiare la scomposizione molto più complessa del corrispondente $^{n}1$ di cui sono sottomultipli.

[8.2h] - Dato ${}^n1$*, indicando con a,b, ..., k tutti i suoi divisori primi, si avranno le uguaglianze:*

$$ {}^n1 = (10^n - 1)/9 $$

$$ 10^n = {}^n1 \cdot 9 + 1 = a \cdot b \cdot .... \cdot k \cdot 9 + 1 $$

Dividendo per uno di questi fattori, ad esempio per k, si avrà:

$$ 10^n/k = a \cdot b \cdot .... \cdot 9 + 1/k $$ (formula della matassa)

Da quest'ultima uguaglianza si evince che, dividendo la potenza 10^n *per uno o più elementi del sistema n, otteniamo un numero decimale periodico con le seguenti caratteristiche: la parte intera ha come fattori primi tutti e soltanto gli altri elementi del sistema n e in più il fattore 9; le sue cifre sono, ordinatamente, le stesse del periodo.*

[8.2e12] - Esempio.

Dato ${}^{20}1$, scomponendolo in fattori primi, avremo il sistema 20:

$$ {}^{20}\overline{S} = \{11\text{-}41\text{-}101\text{-}271\text{-}3541\text{-}9091\text{-}27961\} $$

Dividiamo 10^{20} per un elemento di ${}^{20}\overline{S}$, ad esempio per 9091:

$$ 10^{20}/9091 = 1099989000109989\overline{9,0001099989000109989} $$

Scomponiamo in fattori primi la parte intera:

$$ 1099989000109989 = 9 \cdot 11 \cdot 41 \cdot 101 \cdot 271 \cdot 3541 \cdot 27961 $$

Come era previsto, questa scomposizione ha restituito, assieme al fattore 9, tutti gli elementi del sistema ${}^{20}\overline{S}$, eccetto 9091.

Si osservi che il periodo di 20 cifre, multiplo di quello reale, ripete ordinatamente le cifre significative della parte intera.

[8.2e13] - Esempio.

Dato ${}^{14}1$, scomponiamolo in fattori primi:

$$ 11111111111111 = 11 \cdot 239 \cdot 4649 \cdot 909091 $$

Dividiamo 10^{14} per 217272749, prodotto di $239 \cdot 909091$:

$$ 10^{14}/217272749 = 460251,\overline{00000000460251} $$

Scomponiamo in fattori primi la parte intera (o il periodo):

$$ 460251 = 9 \cdot 11 \cdot 4649 $$

Anche questa volta le nostre aspettative non sono state deluse: la scomposizione ha restituito, oltre al 9, tutti gli altri fattori di ${}^{14}1$.

8.3 Le applicazioni

Vediamo adesso, con qualche esempio, in che modo si può procedere nella compilazione della tabella dei sistemi n dei numeri primi *[8.3 tab1] e* della tabella dei primi di ordine n *[8.3 tab2]*.

[8.3e1] - Esempio
Supponiamo che la tabella in nostro possesso non vada oltre il sistema 25 e ci occorra calcolare il sistema 26.

Stabiliamo quali sono i divisori dell'esponente 26 di $^{26}1$:

$$D_{26} = \{1 ; 2 ; 13 ; 26\}$$

Leggiamo nella tabella *[8.3 tab2]* i primi propri dei sistemi:

$$^{1}S \ ; \ ^{2}S \ ; \ ^{13}S$$

escludendo il sistema ^{26}S che riteniamo incognito.

$^{1}1$ ----> 1 (la base è 1)
$^{2}1$ ----> 11
$^{13}1$ ----> 53 - 79 - 265371653
$^{26}1$ ----> K (incognita da calcolare)

Questi numeri primi e K sono tutti divisori di $^{26}1$; K potrebbe essere o primo di ordine 26, o multiplo di tutti i primi di ordine 26.

$$^{26}1 = 11 \cdot 53 \cdot 79 \cdot 265371653 \cdot K$$

$$K = {}^{26}1/(11 \cdot 53 \cdot 79 \cdot 265371653) = 909090909091$$

I numeri primi di ordine 26, propri del sistema 26, certamente non si trovano nei sistemi precedenti; l'unico modo di trovarli è quello di scomporre il contenitore 909090909091 in cui sono annidati tutti.
Col programma in Visual basic allegato a questa opera, affidando il calcolo ad Excel, in pochi istanti, avremo il risultato:

$$909090909091 = 859 \cdot 10583113049$$

Adesso il sistema 26 e il sottinsieme dei primi di ordine 26 sono completi:

$^{26}\overline{S} = \{11\text{-}53\text{-}79\text{-}859\text{-}265371653\text{-}1058313049\}$
$^{26}S = \{859\text{-}1058313049\}$

Dato che l'esponente del sistema 26 è pari, si può arrivare al contenitore dei primi di ordine 26 in modo più rapido.
Vale infatti l'uguaglianza:

$$^{26}1 = {}^{2\cdot 13}1 = {}^{13}1\cdot(10^{13}+1) = {}^{13}1\cdot 11\cdot 909090909091$$

(11 è sempre un ausiliare dei primi di ordine n quando $10^{n/2}+1$, come accade in questo caso, ha l'esponente dispari).

Come è programmato Excel

Per scomporre i contenitori dei primi di ordine n si può utilizzare un procedimento diverso da quello abituale, impostando il problema nel modo descritto di seguito.
Assegnato il valore q, ci proponiamo di trovare i primi di ordine q.
Dato che ogni intero p, di ordine q, è della forma:

$$p = q\cdot n + 1 \quad \text{con} \quad n \in N$$

compiliamo un programma che affidi al computer il compito di trovare tutti i numeri di questo tipo, imponendo la restrizione che essi siano divisori del contenitore di tutti i primi di ordine q.
(In mancanza di uno minore, si può prendere il più grande dei contenitori dei primi di ordine q , cioè $^{q}1$).
I risultati restituiti dal compilatore saranno i primi di ordine q e i multipli di questi primi, ma noi visualizzeremo solo quelli primi.

[8.3e2] - Esempio
Scomponiamo il contenitore 900900990991 dei numeri primi di ordine 21. (Vedi esempio *[8.2e11]*).

Cerchiamo tutti i primi di ordine 21, applicando la formula:

$$M = 2\cdot n\cdot 21 + 1 \quad \text{con} \quad n \in N$$

I valori validi di M sono solo quelli che dividono il contenitore.
Il programma inserito in Excel in pochi istanti ci dà i risultati:

43 - 1933 - 10838689

Tra i valori di M ci sono anche i numeri composti di ordine 21, ma, poiché questi sono multipli dei primi trovati assieme ad essi, lo stesso programma li seleziona, lasciando alla nostra visualizzazione solo quelli primi.

Scomposizione in negativo

[8.3e3] - Esempio
Scomponiamo 29140076347 e 179202798430900296939037

- Calcoliamo l'ordine di 29140076347, scegliendo come esponente di 10, per comodità, il numero delle cifre del divisore, meno 1.

$$10^{10} : 29140076347 = 0,\overline{343170000000000}$$

Stabilito che questo numero ha ordine 15 ed è composto, cerchiamo i suoi fattori primi, ma in modo diverso da come abbiamo fatto finora: tenendo conto della *[8.2h]*, seguiamo un procedimento che definiamo "*scomposizione in negativo*".
Tolti gli zeri, consideriamo solo la parte significativa del periodo:

$$0,\overline{343170000000000} \text{ ------> } 34317$$

dividiamo per 9: $34317 : 9 = 3813$
Anche 3813 ha ordine 15 e non è primo; i suoi divisori e quelli dello stesso 29140076347 sono da ricercare nel sistema 15:

$$^{15}\overline{S} = \{3\text{-}31\text{-}37\text{-}41\text{-}271\text{-}2906161\}$$

Stabiliamo quali sono i divisori di 3813:
3 è un divisore e implica che 37 non lo è; 31 è un divisore; 41 è un divisore e implica che 271 non lo è; 2906161, in modo evidente, non è un divisore.

All'esito negativo della divisibilità di 3813 corrisponde, al contrario, un esito positivo per 29140076347: i fattori del sistema 15 che non dividono 34317, dividono invece 29140076347.

Infatti: $29140076347 = 37 \cdot 271 \cdot 2906161$

- Stabiliamo quali sono i fattori di 179202798430900296939037
Questo numero di 24 cifre ha ordine 29 ed è composto:

$10^{29}/179202798430900296939037 = 558027,00000000000000000000005...$

Dividiamo la parte intera del quoziente per 9: $558027/9 = 62003$
Poiché 62003 è primo, deduciamo che il nostro numero è multiplo di tutti gli altri numeri primi del sistema 29:

$179202798430900296939037 = 3191 \cdot 16763 \cdot 43037 \cdot 77843839397$

[8.3e4] - Esempio

Scomponiamo: 5964848081 ; 918191 ; 786782848151848938631

- Stabilito che il periodo di 59648488081 è 40, poiché esso si trova nel sistema dei primi di ordine 40, è un numero primo.

$10^9/5964848081 = 0{,}167648863209999999999983235113679...$

$^{40}S = \{1676321 - 5964848081\}$

- 918191 ha ordine 20 ed è composto.

$10^5/918191 = 0{,}10890980199108900000\ 108909801991...$

I divisori possibili di 918191 sono quelli del sistema 20:

$^{20}\overline{S} = \{11\text{-}41\text{-}101\text{-}271\text{-}3541\text{-}9091\text{-}27961\}$

I criteri di divisibilità ci indicano che uno dei divisore è 101; dividendo, abbiamo la scomposizione cercata:

$918191:101 = 9091$

- 786782848151848938631 ha ordine 30. Dividendo per 9 il periodo privo degli zeri, si ottiene: 1270998729/9 = 141222081

In questo caso ci conviene scomporre 141222081, anziché il numero 786782848151848938631 che ha 21 cifre.

I divisori primi possibili di entrambi sono quelli del sistema 30:

$^{30}\overline{S} = \{\underline{3}\text{-}\underline{7}\text{-}\underline{11}\text{-}\underline{13}\text{-}\underline{31}\text{-}\underline{37}\text{-}\underline{41}\text{-}211\text{-}241\text{-}271\text{-}2161\text{-}9091\text{-}2906161\}$

Applicando i criteri di divisibilità, avremo:

$141222081 \equiv 0 \pmod{7}, \pmod{13}, \pmod{11}$

dividiamo per 1001: 141222081/1001 = 141081

$141081 \equiv 0 \pmod{3}, \pmod{37}$

dividiamo per 111: 141081/111 = 1271

poiché 1271 ha ordine 15, non è divisibile per i primi di ordine 30: 211; 241; 2161 e nemmeno per quello di ordine 10: 9091

Tra quelli rimasti, gli unici divisori primi possibili sono: 41 e 31.

Avremo così la scomposizione al completo:

$141222081 = (7 \cdot 11 \cdot 13) \cdot (3 \cdot 37) \cdot (31 \cdot 41)$

Tolti questi primi dal sistema 30, tutti gli altri sono i fattori primi del numero dato:

$786782848151848938631 = 211 \cdot 241 \cdot 271 \cdot 2161 \cdot 9091 \cdot 2906161$

Ordinamento dei numeri primi

Da quanto abbiamo esposto prima è evidente che la scomposizione in fattori primi, così come l'abbiamo proposta, è strettamente legata alle tabelle *[8.3 tab1]* e *[8.3 tab2]* .
Dato il numero p, calcolata la lunghezza del periodo generato dal suo inverso, queste tavole ci consentono di stabilire subito se esso è primo e, in caso contrario, di trovare con facilità i suoi fattori primi.
La formazione illimitata dei sistemi n delle tabelle dipende comunque dalla scomposizione in fattori primi degli n esp1 e, come si sa, man mano che le cifre aumentano, aumentano anche le difficoltà di scomposizione: chi possiede i mezzi più potenti potrà raggiungere i traguardi più elevati.
Tuttavia, nei casi in cui l'indice n non sia primo, è possibile ridurre la lunghezza dei numeri da scomporre, individuando i contenitori più piccoli dei primi di ordine n, cioè i sottomultipli degli n esp1 nei quali sono annidati tutti e soli i primi di ordine n.
In effetti, per formare ciascun sistema n, di volta in volta, si devono calcolare soltanto i primi propri di ogni esp1, perché tutti gli altri primi formano degli esp1 sub-n le cui scomposizioni sono già presenti nei sistemi precedenti.
Con questo modo di procedere si prospetta un avanzamento continuo dell'orizzonte dei numeri primi: raggiunto un traguardo, c'è ne sarà uno immediatamente successivo da raggiungere, perché i numeri primi sono infiniti.
I numeri $^{n}1$ sono i contenitori di tutti i numeri primi: al variare di n, le loro scomposizioni ci danno in successione i sistemi $^{n}\overline{S}$ di aggregazione dei numeri primi e in ciascuno di questi sistemi c'è il sottinsieme ^{n}S di quelli che generano periodi di uguale lunghezza n.
Se n è primo, ^{n}S e $^{n}\overline{S}$ coincidono, perché, in questo caso, $^{n}1$ è il prodotto di tutti e soli i numeri primi che generano il periodo n.
In definitiva possiamo asserire che:
i sistemi dei primi di ordine n della tabella [8.3 tab2], uno dopo l'altro, ci elencano in ordine tutti i numeri primi, senza saltarne alcuno.

L'ordinamento così proposto inverte una situazione abituale.
I numeri primi sono distribuiti in N in modo casuale e finora non ci è possibile prevedere la posizione di ciascuno di essi nella sequenza dei naturali.
Ordinandoli secondo il periodo generato da ciascuno di essi, i numeri primi acquistano la centralità loro dovuta e i numeri composti si dovranno cercare, come loro possibili prodotti, all'interno di ciascun sistema di numeri primi.

Un ulteriore vantaggio offerto da questo ordinamento, sicuramente di notevole importanza, è la possibilità di *una produzione illimitata di numeri primi, certi che quelli trovati dopo saranno sempre diversi dai precedenti*.

Nelle pagine seguenti sono riportate la tabella *[8.3 tab1] dei sistemi n dei numeri primi e la tabella [8.3 tab2] dei primi propri di ogni sistema n*.
Chi volesse delle tabelle più estese potrà trovarle nei siti internet:
- http://www.h4.dion.ne.jp/~rep/
- swox.com/~tege/repunit/html
Ci sono altri siti simili a questi e in alcuni viene data la possibilità di contribuire attivamente all'incremento delle tavole.
Altri siti internet di sicuro interesse sono:
www.alpertron.com.ar/ECM.HTM
www.alpertron.com.ar/BIGCALC.HTM
In questi ultimi sono disponibili potenti calcolatrici che consentono calcoli e scomposizioni anche con numeri di centinaia di cifre.
Per avere altre notizie su questi argomenti su internet si può cercare alle voci "repunit" e "period", ma si tratta quasi sempre di documentazione in lingua inglese.
Qualcosa in italiano si trova sull'enciclopedia di Wikipedia:
htpp://it.wikipedia.org/wiki/Repunit
In queste pagine si legge, tra l'altro, che il termine "repunit" (repeated unit) è stato coniato nel1964 da Albert H. Beiler nel suo libro:
Ricreation in the Theory of Numbers.

[8.3 tab1] SISTEMI DI NUMERI PRIMI

1	$^{1}\overline{S} = 1$
2	$^{2}\overline{S} = \{11\}$
3	$^{3}\overline{S} = \{3 - 37\}$
4	$^{4}\overline{S} = \{11 - 101\}$
5	$^{5}\overline{S} = \{41 - 271\}$
6	$^{6}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\}$
7	$^{7}\overline{S} = \{239\text{-}4649\}$
8	$^{8}\overline{S} = \{11\text{-}73\text{-}101\text{-}137\}$
9	$^{9}\overline{S} = \{3^{2}\text{-}37\text{-}333667\}$
10	$^{10}\overline{S} = \{11\text{-}41\text{-}271\text{-}9091\}$
11	$^{11}\overline{S} = \{21649\text{-}513239\}$
12	$^{12}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\text{-}101\text{-}9901\}$
13	$^{13}\overline{S} = \{53\text{-}79\text{-}265371653\}$
14	$^{14}\overline{S} = \{11\text{-}239\text{-}4649\text{-}909091\}$
15	$^{15}\overline{S} = \{3\text{-}31\text{-}37\text{-}41\text{-}271\text{-}2906161\}$
16	$^{16}\overline{S} = \{11\text{-}17\text{-}73\text{-}101\text{-}137\text{-}5882353\}$
17	$^{17}\overline{S} = \{2071723\text{-}5363222357\}$
18	$^{18}\overline{S} = \{3^{2}\text{-}7\text{-}11\text{-}13\text{-}19\text{-}37\text{-}52579\text{-}333667\}$
19	$^{19}\overline{S} = \{\ ^{19}1\ \}$
20	$^{20}\overline{S} = \{11\text{-}41\text{-}101\text{-}271\text{-}3541\text{-}9091\text{-}27961\}$
21	$^{21}\overline{S} = \{3\text{-}37\text{-}43\text{-}239\text{-}1933\text{-}4649\text{-}10838689\}$
22	$^{22}\overline{S} = \{11^{2}\text{-}23\text{-}4093\text{-}8779\text{-}21649\text{-}513239\}$
23	$^{23}\overline{S} = \{\ ^{23}1\ \}$
24	$^{24}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}37\text{-}73\text{-}101\text{-}137\text{-}9901\text{-}99990001\}$
25	$^{25}\overline{S} = \{41\text{-}271\text{-}21401\text{-}25601\text{-}182521213001\}$
26	$^{26}\overline{S} = \{11\text{-}53\text{-}79\text{-}859\text{-}265371653\text{-}1058313049\}$
27	$^{27}\overline{S} = \{3^{3}\text{-}37\text{-}757\text{-}333667\text{-}440334654777631\}$
28	$^{28}\overline{S} = \{11\text{-}29\text{-}101\text{-}239\text{-}281\text{-}4649\text{-}909091\text{-}121499449\}$
29	$^{29}\overline{S} = \{3191\text{-}16763\text{-}43037\text{-}62003\text{-}77843839397\}$
30	$^{30}\overline{S} = \{3\text{-}7\text{-}11\text{-}13\text{-}31\text{-}37\text{-}41\text{-}211\text{-}241\text{-}271\text{-}2161\text{-}9091\text{-}2906161\}$
31	$^{31}\overline{S} = \{\ 2791\text{-}6943319\text{-}57336415063790604359\}$
32	$^{32}\overline{S} = \{11\text{-}17\text{-}73\text{-}101\text{-}137\text{-}353\text{-}449\text{-}641\text{-}1409\text{-}69857\text{-}5882353\}$
33	$^{33}\overline{S} = \{3\text{-}37\text{-}67\text{-}21649\text{-}513239\text{-}1344628210313298373\}$
34	$^{34}\overline{S} = \{11\text{-}103\text{-}4013\text{-}2071723\text{-}5363222357\text{-}21993833369\}$
35	$^{35}\overline{S} = \{41\text{-}71\text{-}239\text{-}271\text{-}4649\text{-}123551\text{-}102598800232111471\}$

$^{36}\overline{S}$ = {3^2-7-11-13-19-37-101-9901-52579-333667-999999000001}
$^{37}\overline{S}$ = {2028119-247629013-2212394296770203368013}
$^{38}\overline{S}$ = {11-909090909090909091-^{19}1}
$^{39}\overline{S}$ = {3-37-53-79-265371653-900900900900990990990991}
$^{40}\overline{S}$ = {11-41-73-101-137-271-3541-9091-27961-1676321-5964848081}
$^{41}\overline{S}$ = {83-1231-538987-201763709900322803748657942361}
$^{42}\overline{S}$ = {3-7^2-11-13-37-43-127-239-1933-2689-4649-459691-909091-10838689}
$^{43}\overline{S}$ = {173-1527791-1963506722254397-2140992015395526641}
$^{44}\overline{S}$ = {11^2-23-89-101-4093-8779-21649-513239-1052788969-1056689261}
$^{45}\overline{S}$ = {3^2-31-37-41-271-238681-333667-2906161-4185502830133110721}
$^{46}\overline{S}$ = {11-47-139-2531-549797184491917-^{23}1}
$^{47}\overline{S}$ = {35121409-316362908763458525001406154038726382279}
$^{48}\overline{S}$ = {3-7-11-13-17-37-73-101-137-9901-5882353-99990001- - 9999999900000001}
$^{49}\overline{S}$ = {239-4649-505885997-19767301445981909635680230146793333}
$^{50}\overline{S}$ = {11-41-251-271-5051-9091-21401-25601-182521213001- - 78875943472201}
$^{51}\overline{S}$ = {3-37-613-210631-2071723-52986961-5363222357}
$^{52}\overline{S}$ = {11-53-79-101-521-859-265371653-1058313049- - 1900381976777332243781}
$^{53}\overline{S}$ = {107-1659431-1325815267337711173- - 47198858799491425660200071}
$^{54}\overline{S}$ = {3^3-7-11-13-19-37-757-52579-333667-70541929-14175966169- - 440334654777631}
$^{55}\overline{S}$ = {41-271-1321-21649-62921-513239-83251631- - 1300635692678058358830121}
$^{56}\overline{S}$ = {11-29-73-101-137-239-281-4649-7841-909091-121499449- - 127522001020150503761}
$^{57}\overline{S}$ = {3-37-21319-10749631-^{19}1-39311230223051293779765 19}
$^{58}\overline{S}$ = {11-59-3191-16763-43037-62003-77843839397- - 1540832049306625577812018 49}
$^{59}\overline{S}$ = {2559647034361- - 434087628565746021214453428992855982675574 6751}
$^{60}\overline{S}$ = {3-7-11-13-31-37-41-61-101-211-241-271-2161-3541-9091-9901- - 27961-2906161-4188901-39526741}
$^{61}\overline{S}$ = {733-4637-329401-974293-1360682471-106007173861643- - 7061709990156159479}

[8.3 tab2] SISTEMI DEI PRIMI DI ORDINE N

1	$^{1}S = \{3\}$
2	$^{2}S = \{11\}$
3	$^{3}S = \{37\}$
4	$^{4}S = \{101\}$
5	$^{5}S = \{41\text{-}271\}$
6	$^{6}S = \{7\text{-}13\}$
7	$^{7}S = \{239\text{-}4649\}$
8	$^{8}S = \{73\text{-}137\}$
9	$^{9}S = \{333667\}$
10	$^{10}S = \{9091\}$
11	$^{11}S = \{21649\text{-}513239\}$
12	$^{12}S = \{9901\}$
13	$^{13}S = \{53\text{-}79\text{-}265371653\}$
14	$^{14}S = \{909091\}$
15	$^{15}S = \{31\text{-}2906161\}$
16	$^{16}S = \{17\text{-}5882353\}$
17	$^{17}S = \{2071723\text{-}5363222357\}$
18	$^{18}S = \{19\text{-}52579\}$
19	$^{19}S = \{\ ^{19}1\ \}$
20	$^{20}S = \{3541\text{-}27961\}$
21	$^{21}S = \{43\text{-}1933\text{-}10838689\}$
22	$^{22}S = \{23\text{-}4093\text{-}8779\}$
23	$^{23}S = \{\ ^{23}1\ \}$
24	$^{24}S = \{99990001\}$
25	$^{25}S = \{21401\text{-}25601\text{-}182521213001\}$
26	$^{26}S = \{859\text{-}1058313049\}$
27	$^{27}S = \{757\text{-}440334654777631\}$
28	$^{28}S = \{29\text{-}281\text{-}121499449\}$
29	$^{29}S = \{3191\text{-}16763\text{-}43037\text{-}62003\text{-}77843839397\}$
30	$^{30}S = \{211\text{-}241\text{-}2161\}$
31	$^{31}S = \{2791\text{-}6943319\text{-}57336415063790604359\}$
32	$^{32}S = \{353\text{-}449\text{-}641\text{-}1409\text{-}69857\}$
33	$^{33}S = \{67\text{-}1344628210313298373\}$
34	$^{34}S = \{103\text{-}4013\text{-}21993833369\}$
35	$^{35}S = \{71\text{-}123551\text{-}102598800232111471\}$

^{36}S = {999999000001}
^{37}S = {2028119-247629013-2212394296770203368013}
^{38}S = {909090909090909091}
^{39}S = {9009009009009909909909991}
^{40}S = {1676321-5964848081}
^{41}S = {83-1231-538987-201763709900322803748657942361}
^{42}S = {127-2689-459691}
^{43}S = {173-1527791-1963506722254397-2140992015395526641}
^{44}S = {89-1052788969-1056689261}
^{45}S = {238681-4185502830133110721}
^{46}S = {47-139-2531-549797184491917}
^{47}S = {35121409-316362908763458525001406154038726382279}
^{48}S = {9999999900000001}
^{49}S = {505885997-19767301445981909635680230146793333}
^{50}S = {251-5051-78875943472201}
^{51}S = {613-210631-52986961-13168164561429877}
^{52}S = {521-1900381976777332243781}
^{53}S = {107-1659431-1325815267337711173-47198858799491425660200071}
^{54}S = {70541929-14175966169}
^{55}S = {1321-62921-83251631-1300635692678058358830121}
^{56}S = {7841-127522001020150503761}
^{57}S = {21319-10749631-3931123022305129377976519}
^{58}S = {59-154083204930662557781201849}
^{59}S = {2559647034361-434087628565746021214453428992855982675574675 1}
^{60}S = {61-4188901-39526741}
^{61}S = {733-4637-329401-974293-1360682471-106007173861643- - 7061709990156159479}

Seconda parte