Vincenzo Vitale

Un ordinamento possibile dei numeri primi

Capitolo 3° - Le congruenze

http://www.integernumbers.org
vincenzovitale@integernumbers.org
tel. +039 3461424768 (WhatsApp)

Sia lode a Gesù Cristo,
unico e vero Maestro

"Wn - Un ordinamento possibile dei numeri primi"
Codice: ed04Wn2019vv (1ª pubblicazione web: 13.04.2008)

Vincenzo Vitale
vincenzovitale@tim.it +039 3461424768 (WhatsApp)
http://www.integernumbers.org
vincenzovitale@integernumbers.org

3.1 Interi congruenti

Il concetto di "congruenza tra interi" nasce dall'idea che in fondo, per stabilire se un intero relativo z sia o no divisibile per un numero primo p, non è strettamente necessario eseguire la divisione, è invece sufficiente limitarsi a calcolare qual è il suo resto. A questo fine si persegue l'obiettivo di studiare quali relazioni intercorrono tra gli interi relativi e i loro resti, rispetto a un determinato intero positivo maggiore di uno.

definizioni

[3.1a] - Si dice divisione euclidea (o elementare) di un intero relativo z per un intero positivo $n \geq 2$, quella il cui resto r è maggiore o uguale a zero e minore del divisore n.
(Si escludono i valori: n=0 perché la divisione per 0 è impossibile; il valore n=1 perché si otterrebbe una identità. z:1=z)

La divisione euclidea è rappresentata dall'uguaglianza:

$$z = g \cdot n + r \;\; ; \;\; 0 \leq r < n \;\; ; \;\; z, g \in Z \;\; ; \;\; n \geq 2$$

[3.1b] - Due numeri interi relativi a e b si dicono congrui tra loro (o congruenti), secondo il modulo n, se le loro divisioni euclidee per lo stesso numero naturale $n > 1$ danno resti uguali.

Rappresentiamo le divisioni euclidee di a e di b per $n > 1$:

$a = g \cdot n + r_1 \;\; , \;\; 0 \leq r_1 < n$

$b = q \cdot n + r_2 \;\; , \;\; 0 \leq r_2 < n$

Se accade che $r_1 = r_2$, denoteremo tale circostanza con la scrittura: $a \equiv b \pmod{n}$
e diremo:
"a è congruo a b, modulo n"
Oppure: "a e b sono congruenti rispetto al modulo n"

[3.1es1] - Esempio
Confrontiamo tra loro 17 e 23 rispetto al numero naturale 3.

Le divisioni euclidee per 3 di 17 e di 23, sono rappresentate dalle uguaglianze:

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

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

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

[3.1es2] - Esempio
Stabiliamo se gli interi relativi –269 , –67 e 139 sono congrui tra loro rispetto al modulo n=17.

Eseguiamo le divisioni euclidee, ricordandoci che $0 \le r < n$

$$-269 = -16 \bullet 17 + 3 \quad ; \quad -67 = -4 \bullet 17 + 1 \quad ; \quad 139 = 8 \bullet 17 + 3$$

Dalle uguaglianze ottenute ci accorgiamo che soltanto –269 e 139 sono congrui tra loro secondo il modulo 17:

$$-269 \equiv 139 \pmod{17} \quad ; \quad -67 \not\equiv -269 \pmod{17} \quad ;$$

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

(Nel caso in cui non facessimo riferimento alla divisione che abbiamo definita "euclidea" , rischieremmo di non accorgerci che –269 è congruo a 139, modulo 17.
Ciò potrebbe accadere, ad esempio, se dovessimo considerare l'uguaglianza –269 = –15•17–14 , anziché quella data dalla divisione euclidea: –269 = –16•17+3 con resto positivo).

[3.1c] - Si dice
sistema completo dei minimi resti positivi, modulo n,
l'insieme A di tutti i resti che si possono ottenere eseguendo le divisioni euclidee degli interi z per il numero naturale n.
Pertanto esso è costituito dai primi n numeri interi positivi:

$$A = \{0 \, , \, 1 \, , \, 2 \, , \, \ldots \, , \, (n-2) \, , \, (n-1)\}$$

[3.1d] - *La divisione euclidea, tra un intero z e un numero naturale n≥2, ci consente di ottenere il minimo resto positivo.*

Tuttavia, similmente a quanto abbiamo convenuto coi numeri misti nel 2° capitolo, paragrafo *[2.4]*, ci può essere utile calcolare un quoziente diverso da quello della divisione euclidea ed ottenere, di conseguenza, un resto che non è quello minimo positivo.
In particolare, in determinate circostanze, sarà opportuno calcolare il resto negativo più piccolo in valore assoluto.
Consideriamo, ad esempio, la divisione di 26 per 7:

$$26 = 3 \bullet 7 + 5 \quad ; \quad 0 < |5| < 7$$

Se però consideriamo il quoziente 4, che è successivo al quoziente 3 della divisione euclidea, otteniamo il risultato:

$$26 = 4 \bullet 7 - 2 \quad ; \quad 0 < |-2| < 7$$

In questo caso la seconda divisione è più vantaggiosa della prima, perché il suo resto, in valore assoluto, è minore dell'altro.

[3.1e] *- La divisione il cui quoziente è il successivo di quello della divisione euclidea, ma nel caso in cui $r \neq 0$, ci consente di ottenere il minimo resto negativo. (Minimo in valore assoluto).*

[3.1f] - Si dice

sistema completo dei minimi resti negativi, modulo n,

l'insieme B degli n numeri interi negativi che, in valore assoluto, sono maggiori o uguali a 0 e minori di n :

$$B=\{0\ ,\ -1\ ,\ -2\ ,\ \ldots\ ,\ -(n-1)\}$$

[3.1es3] - Esempio
Facendo riferimento alla divisione di 29 per 4, prendiamo in considerazione le uguaglianze:

$$29 = 7\bullet 4 + 1 \quad ; \quad 29 = 8\bullet 4 - 3 \quad ; \quad 29 = 6\bullet 4 + 5$$

- La prima uguaglianza ci consente di stabilire quante unità rimangono quando calcoliamo il quoziente utilizzando la divisione euclidea e sodisfa la nostra richiesta di ottenere il minimo resto positivo.

- La seconda uguaglianza ci consente di stabilire quante unità mancano se calcoliamo il quoziente successivo a quello della divisione euclidea e soddisfa la nostra richiesta di trovare il minimo resto negativo (minimo in valore assoluto): $|-3|<|4|$

- La terza uguaglianza è un esempio di divisione con il resto maggiore del divisore.

[3.1es4] - Esempio
Facendo riferimento alla divisioni di – 31 per 7, consideriamo le seguenti uguaglianze.

$-31=-5\bullet 7+4$ minimo resto positivo (divisione euclidea):

$$0<4<7$$

$-31=-4\bullet 7-3$ minimo resto negativo (in valore assoluto):

$$0<|-3|<7$$

$-31=1\bullet 7-38$ resto maggiore, in valore assoluto, del divisore:

$$|-38|>7$$

[3.1g] - Si dice

minimo resto della divisione ,

tra un numero intero z e un numero naturale $n \geq 2$, quello il cui valore assoluto è compreso tra 0 e n/2 :

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

- Nell'esempio *[3.1es3]* il minimo resto della divisione tra 29 e 4 è +1 e coincide col minimo resto positivo.
- Nell'esempio *[3.1es4]* il minimo resto della divisione tra –31 e 7 è –3 e coincide con il minimo resto negativo, in valore assoluto.

[3.1h] - Si dice

sistema completo dei minimi resti, modulo n ,

l'insieme S di tutti i minimi resti che si ottengono eseguendo la divisione tra gli interi z e il numero naturale $n \geq 2$.

$S = \{0 , 1 , 2 , \ldots , (n-1)/2 , -(n-1)/2 , \ldots , -2 , -1\}$ (se n è dispari)

$S = \{0 , 1 , 2 , \ldots , \pm n/2 , \ldots , -2 , -1\}$ (se n è pari)

Come si può notare, l'insieme S è formato sia da numeri interi positivi, sia da numeri interi negativi.

[3.1es5] - Stabiliamo quali sono i sistemi completi dei minimi resti relativamente ai moduli 13 e 10.

Le divisioni euclidee dei numeri interi z per 13 danno origine al sistema completo dei minimi resti positivi, modulo 13:

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

Nel momento in cui, da questi 13 elementi distinti, volessimo ottenere l'insieme S dei minimi resti, sarà sufficiente procedere nel modo seguente:

- 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:

$$S_{13} = \{0 , 1 , 2 , 3 , 4 , 5 , 6 , -6 , -5 , -4 , -3 , -2 , -1\}$$

In modo analogo troviamo quello relativo al modulo 10:

$$S_{10} = \{0 , 1 , 2 , 3 , 4 , \pm 5 , -4 , -3 , -2 , -1\}$$

3.2 Alcune proprietà delle congruenze

[3.2a] - Se due interi relativi a e b sono congruenti, modulo n, ne consegue che la loro differenza è un multiplo di n.

Infatti, data la congruenza:

$$a \equiv b \pmod{n} \quad ; \quad a,b \in Z \ , \ n>1$$

le divisioni euclidee per n di a e di b sono rappresentate dalle uguaglianze:

$$a = g \cdot n + r \quad (0 \le r < n) \ , \ g \in Z$$
$$b = h \cdot n + r \quad (0 \le r < n) \ , \ h \in Z$$

Per definizione di congruenza, r ha lo stesso valore in entrambe, per cui, sottraendo membro a membro, si avrà:

$$a - b = (g - h) \cdot n$$

Questa uguaglianza dimostra la nostra asserzione.

[3.2es1] - Esempio
Le divisioni euclidee per 7 di 36 e di 15 sono rappresentate dalle uguaglianze:

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

per cui 36 e 15 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:

$$36 - 15 = 21 \quad ; \quad (15 - 36 = -21)$$

[3.2es2] - Esempio
Le divisioni euclidee per 117 di –691 e di 245 sono rappresentate dalle uguaglianze:

$$-691 = -6 \cdot 117 + 11$$
$$245 = 2 \cdot 117 + 11$$

per cui gli interi –691 e 245 sono congruenti, rispetto al modulo 117:

$$-691 \equiv 245 \pmod{117}$$

Calcolando la loro differenza, in accordo con le nostre aspettative, otteniamo un multiplo di 117:

$$-691 - 245 = -936 = -8 \cdot 117 \quad ; \quad (245 + 691 = 936)$$

E' valida anche la proposizione inversa della *[3.2a]*.

[3.2b] - Se la differenza di due interi relativi a e b è un multiplo di n>1 , ne consegue che essi sono congruenti, modulo n.

Infatti, data l'uguaglianza

$$a-b=c\bullet n \quad ; \quad a,b,c\in Z \text{ , } n>1$$

le divisioni euclidee per n di a e di b ci danno le uguaglianze:

$$a=g\bullet n+r_1 \quad (0\le r_1<n) \text{ , } g\in Z$$
$$b=h\bullet n+r_2 \quad (0\le r_2<n) \text{ , } h\in Z$$

Sottraendo membro a membro, si avrà quest'altra uguaglianza:

(*) $$a-b=(g-h)\bullet n+(r_1-r_2)$$

Dato che r_1 e r_2 sono entrambi positivi e minori di n, il valore assoluto della loro differenza è certamente compreso tra 0 e n:

$$0\le|r_1-r_2|<n$$

Ma, necessariamente, tale differenza deve essere zero:

$$r_1-r_2=0$$

altrimenti, contradicendo l'ipotesi, a–b non sarebbe multiplo di n. Ciò implica che $r_1=r_2$, per cui è valida la congruenza:

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

Per completare l'analisi, consideriamo il caso in cui la differenza tra due interi relativi non è un multiplo dell'intero positivo n.

[3.2c] - Se la differenza tra due interi relativi a e b non è un multiplo di n>1, essi non sono congrui tra loro secondo il modulo n.

Infatti, se $a-b\neq c\bullet n$ $(c\in Z)$, dall'uguaglianza (*) ne consegue che $(r_1-r_2)\neq 0$, per cui, necessariamente $r_1\neq r_2$

[3.2es3] - Esempio
Dati i numeri –745 e –791, stabiliamo se sono congrui tra loro rispetto al modulo 23.

Poiché la loro differenza é un multiplo di 23:

$$-745+791=46=2\bullet 23$$

ne consegue che essi sono congruenti, modulo 23:

$$-745\equiv -791 \pmod{23}$$

Infatti:

$$-745=-33\bullet 23+14$$
$$-791=-35\bullet 23+14$$

Unifichiamo i teoremi *[3.2a], [*3.2b*]* e *[*3.2c*]* enunciando una proposizione soltanto.

[3.2d] - Due interi relativi a e b sono congruenti, modulo n, soltanto se la loro differenza è un multiplo di n.

$$a \equiv b \pmod{n} \Leftrightarrow a-b=c \cdot n \quad (a,b,c \in Z\ ;\ n>1)$$

[3.2es4] - Esempio
Calcoliamo la differenza tra 41 e 19:

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

Essendosi ottenuto un multiplo di 11, a motivo della *[3.2d]*, 41 e 19 sono congrui, modulo 11:

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

Infatti, come è nelle nostre previsioni, i resti delle loro divisioni euclidee sono uguali:

$$41=3 \cdot 11+8 \ ; \ 19=11+8$$

[3.2es5] - Esempio
Stabiliamo se gli interi –53 e 71, sono congrui tra loro, modulo 29.

Applicando la *[3.2d]* , calcoliamo la loro differenza:

$$-53-71=-124=-4 \cdot 31$$

Dato che 124 non è un multiplo di 29, il due numeri –53 e 71 non sono congrui, modulo 29.
Sono invece congrui se si considerano i moduli 31 e 4.

$$-53 \not\equiv 71 \pmod{29}$$
$$-53 \equiv 71 \pmod{31}$$
$$-53 \equiv 71 \pmod{4}$$

La proposizioni *[3.2d]* è quella più usata per stabilire la congruenza tra numeri interi.
Applichiamola per dimostrare le proprietà peculiari del sistema dei resti modulo n.

[3.2e] - Ogni sistema completo dei minimi resti positivi A, modulo n, è tale che due suoi qualsiasi elementi non sono mai congruenti.

Infatti, due qualsiasi elementi r_i , r_j dell'insieme A, definito al punto *[3.1c]* , sono sempre distinti ($r_i \neq r_j$) , minori di n e maggiori o uguali a zero.
Da qui ne segue che la loro differenza è, in valore assoluto, minore di n e mai zero ($r_i - r_j \neq 0$) , unico multiplo di n nell'insieme A.
Quindi, per la *[3.2d]* , vale la relazione: $r_i \not\equiv r_j \pmod{n}$

[3.2f] - Un qualsiasi intero relativo z è sempre congruo a uno soltanto degli elementi del sistema completo dei minimi resti positivi A, secondo il modulo n.

Infatti, se z è un intero qualsiasi, il resto r_z della sua divisione euclidea per l'intero positivo n>1 è, per la definizione *[3.1a]* , un elemento dell'insieme A:

$$z = b \bullet n + r_z \quad ; \quad 0 \le r_z < n \; ; \; b \in Z$$

Da questa uguaglianza si ricava quest'altra:

$$z - r_z = b \bullet n$$

Da qui, per la *[3.2d]* , ne consegue la congruenza:

$$z \equiv r_z \pmod{n} \; , \; r_z \in A$$

Dimostriamo che z è congruo a uno soltanto dei residui, modulo n, dell'insieme A.

Se dovessimo supporre che z sia congruo, oltre che a r_z , anche a un altro elemento r_s di A, dalle uguaglianze:

$$z - r_z = b \bullet n \quad ; \quad z - r_s = c \bullet n \qquad (r_z \neq r_s)$$

sottraendo membro a membro, ne seguirebbe quest'altra:

$$r_s - r_z = (b - c) \bullet n$$

Ma cadremmo in contradizione, perché allora sarebbe valida anche la congruenza:

$$r_s \equiv r_z \pmod{n}$$

mentre nella *[3.2e]* affermiamo, al contrario, che due qualsiasi elementi distinti di A non sono mai congruenti, modulo n.

[3.2es6] - Esempio

Calcoliamo a quale elemento del sistema completo dei minimi resti positivi, modulo 13, è congruo 17439.

Eseguiamo la divisione euclidea:

$$17439 = 1341 \bullet 13 + 6$$

Ne consegue che: $17439 \equiv 6 \pmod{13}$

[3.2es7] - Esempio

Mettiamo a confronto gli interi 29 e 13.

Dalla divisione euclidea

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

risulta che 29 non è multiplo di 13 e che vale la relazione:

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

[3.2es8] - Esempio

Mettiamo a confronto gli interi 51 e 17.

Dalla divisione euclidea:

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

risulta che 51 è multiplo di 17 e che vale la relazione:

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

Si osservi che quando z è multiplo di n , il resto della loro divisione euclidea è zero, per cui è possibile enunciare una nuova definizione del concetto di divisibilità.

[3.2g] - Un numero intero relativo z è divisibile per n soltanto se è congruo a zero, modulo n.

$$z \equiv 0 \pmod{n} \quad \Leftrightarrow \quad z = g \bullet n \quad (z, g \in Z \; ; \; n > 1)$$

[3.2h] - Proprietà riflessiva delle congruenze:

$$a \equiv a \pmod{n} \; , \; \forall a \in Z$$

Questa congruenza è sempre valida, qualunque sia il numero relativo a. Infatti la differenza dei suoi due membri è zero ($a - a = 0$) e zero è multiplo del modulo n.

[3.3i] - Proprietà simmetrica delle congruenze:

$$a \equiv b \pmod{n} \; \Rightarrow \; b \equiv a \pmod{n} \; ; \; a, b \in Z \; ; \; n \geq 2$$

Infatti, dalla prima congruenza si ricava l'uguaglianza:

$$a - b = gn \; ; \; g \in Z$$

e cambiando i segni dei suoi termini otteniamo le relazioni:

$$-(a - b) = -gn \; \Rightarrow \; b = -gn + a \; \Rightarrow \; b \equiv a \pmod{n}$$

[3.2j] - Proprietà transitiva delle congruenze:

$$a \equiv b \pmod{n} \; ; \; b \equiv c \pmod{n} \; \Rightarrow \; a \equiv c \pmod{n} \; ; \; a, b, c \in Z$$

Infatti, dalle prime due congruenze ne derivano le uguaglianze:

$$a = g \bullet n + b \; ; \; b = f \bullet n + c$$

e da queste, sommando membro a membro, ne derivano queste altre uguaglianze:

$$a + b = (g + f)n + b + c \; ; \; a = (g + f)n + c$$

Da qui ne consegue la congruenza:

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

[3.2k] - La congruenza è una relazione di equivalenza perché ha le proprietà riflessiva, simmetrica e transitiva.

Non è sempre vera la proposizione inversa della *[3.2j]*:

[3.2ℓ] - $a \not\equiv b \pmod{n} \; ; \; b \not\equiv c \pmod{n} \; \not\Rightarrow \; a \not\equiv c \pmod{n} \; ; \; a, b, c \in Z$

Infatti, date le prime due incongruenze, accade che $a \not\equiv c \pmod{n}$ solo nel caso in cui a, b, c sono congruenti rispettivamente a tre elementi distinti del sistema completo dei minimi resti, i cui elementi, come sappiamo, sono sempre a due a due incongruenti.

[3.2es9] - Esempio
Confrontiamo gli interi 31, 43 e 60 , rispetto al modulo 29.
Poiché:
$31 \equiv 2 \pmod{29}$; $43 \equiv 14 \pmod{29}$; $60 \equiv 2 \pmod{29}$
per la proprietà transitiva ne consegue che: $31 \equiv 60 \pmod{29}$
La proprietà transitiva non vale invece per le incongruenze:
$31 \not\equiv 43 \pmod{29}$, $43 \not\equiv 60 \pmod{29}$, ma $31 \equiv 60 \pmod{29}$

Mettiamo ora a confronto il sistema completo dei minimi resti positivi A, definito in *[3.1c]* , con l'insieme completo dei minimi resti negativi B, definito in *[3.1f]*.

La divisione che ci consente di ottenere il minimo resto positivo è quella euclidea, rappresentata dall'uguaglianza:

$$z = g \cdot n + r \quad (0 \le r < n) \; ; \; z, g \in Z \; ; \; n > 1$$

Da questa, poiché $z - r = g \cdot n$, ne segue la congruenza:

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

Mentre la divisione col minimo resto negativo, secondo la *[3.1e]*, è rappresentata da quest'altra uguaglianza:

$$z = (g+1) \cdot n + (r - n) \quad , \quad r \neq 0$$

Poiché $z - (r - n) = (g+1) \cdot n$, ne consegue la congruenza:

$$z \equiv r - n \pmod{n} \quad , \quad 0 < r < n$$

Accomunando le due congruenze, si avrà:

$$z \equiv r \equiv r - n \pmod{n} \quad , \quad 0 < r < n$$

Pertanto, vale la seguente proposizione.

[3.2m] - Ad ogni elemento $r_A > 0$, del sistema completo dei minimi resti positivi A, corrisponde un elemento $r_B = r_A - n$, del sistema completo dei minimi resti negativi B, secondo la relazione:

$$r_B \equiv r_A - n \pmod{n} \quad , \quad r_A > 0$$

Mentre ad $r_A = 0$ corrisponde $r_B = 0$. Cosicché: $(0 \le |r_B| < n)$

Viceversa, ad ogni elemento $r_B < 0$, del sistema completo dei minimi resti negativi B, corrisponde un elemento $r_A = r_B + n$, del sistema completo dei minimi resti positivi A, secondo la relazione:

$$r_A \equiv r_B + n \pmod{n} \quad , \quad r_B < 0$$

Si osservi che r_B è il minimo resto, in accordo con la definizione *[3.1g]* , solo se ad esso corrisponde $r_A > n/2$.

La scelta che di volta in volta faremo tra $0 \le r_A \le n/2$ e $-n/2 < r_B < 0$ sarà finalizzata ad ottenere un elemento del sistema completo dei minimi resti S, definito in *[3.1h]*.

Allo scopo di facilitare il calcolo si consideri che r_A e il corrispondente r_B sono tali che la somma dei loro valori assoluti è sempre uguale al modulo n: $|r_A|+|r_B|=n$

[3.2es10] - Esempio
Calcoliamo il minimo resto congruente a 23331, modulo 37.

La divisione euclidea ci fornisce le seguenti uguaglianze:

$$23331=630 \cdot 37+21 \;\; ; \;\; 23331-21=630 \cdot 37$$

Per cui: $23331 \equiv 21 \pmod{37}$

Tuttavia questo non è il residuo minimo, perché $21>37/2$.
Lo è invece il minimo resto negativo della divisione che ha il quoziente successivo a quello della divisione euclidea:

$$23331=631 \cdot 37-16$$

per cui: $23331 \equiv -16 \pmod{37}$

In base alla *[3.2m]* , il minimo resto negativo si può ricavare in modo più semplice sottraendo da quello positivo il modulo 37:

$$21 \equiv 21-37 \equiv -16 \pmod{37}$$

[3.2es11] - Esempio
Calcoliamo il minimo resto congruente a –178331, modulo 89.

Eseguiamo prima la divisione euclidea considerando il dividendo positivo; poi, sistemando i segni, otteniamo quella non euclidea col minimo resto negativo:

$$-178331=-2003 \cdot 89-64$$

Per cui: $-178331 \equiv -64 \pmod{89}$

Ma $|-64|>89/2$, per cui dobbiamo trovare il minimo resto.
Lo possiamo ricavare calcolando il quoto precedente di quello della divisione già effettuata:

$$-178331=-2004 \cdot 89+25 \quad \text{(Divisione euclidea)}$$

Per cui: $-178331 \equiv 25 \pmod{89}$

Ma, in base alla *[3.2m]* , possiamo ottenere questo resto dal precedente, più rapidamente, sottraendo 64 dal modulo 89:

$$-64 \equiv 89-64 \equiv 25 \pmod{89}$$

3.3 Operazioni tra congruenze

[3.3a] - Se a entrambi i membri di una congruenza si sottrae o si addiziona lo stesso intero z, si ottiene una nuova congruenza rispetto allo stesso modulo n:

$$f \equiv t \pmod{n} \Rightarrow (f \pm z) \equiv (t \pm z) \pmod{n} \quad , \quad (z \in Z)$$

Dimostrazione

$$f \equiv t \pmod{n} \Rightarrow f = g \cdot n + t \quad , \quad g \in Z$$

Sottraiamo ad entrambi i membri dell'uguaglianza un intero z:

$$f - z = g \cdot n + t - z$$

Da questa, poiché $(f-z)-(t-z) = g \cdot n$, ne consegue la congruenza:

$$(f-z) \equiv (t-z) \pmod{n}$$

Analogamente, se addizioniamo, otteniamo la congruenza:

$$(f+z) \equiv (t+z) \pmod{n}$$

Nelle applicazioni della *[3.3a]*, torna vantaggioso sottrarre o addizionare un intero z del primo o del secondo membro della congruenza data. Vediamo alcuni casi particolari.

Data la congruenza $f \equiv t \pmod{n}$, sottraendo o t o f da entrambi i membri, otteniamo rispettivamente le relazioni:

$$f \equiv t \pmod{n} \Rightarrow f - t \equiv 0 \pmod{n} \; ; \; t - f \equiv 0 \pmod{n}$$

Agendo analogamente, otteniamo quest'altre implicazioni:

$$f + z \equiv t + z \pmod{n} \Rightarrow f \equiv t \pmod{n}$$

$$f - z \equiv t - z \pmod{n} \Rightarrow f \equiv t \pmod{n}$$

$$a + g + m \equiv b + h + g \pmod{n} \Rightarrow a + m \equiv b + h \pmod{n}$$

Cosicché possiamo enunciare le due proposizioni che seguono.

[3.3b] - E' possibile il trasporto di un termine da un membro all'altro di una congruenza cambiandolo di segno.

[3.3c] - E' valida la proposizione inversa della *[3.3a]*:

$$(f \pm z) \equiv (t \pm z) \pmod{n} \Rightarrow f \equiv t \pmod{n} \quad (f, t, z \in Z)$$

Dimostriamo ora quest'altra proposizione.

[3.3d] - Date le congruenze $f \equiv t \pmod{n}$; $h = j \pmod{n}$, se le addizioniamo membro a membro, otteniamo una nuova congruenza rispetto allo stesso modulo n:

$$f \equiv t \pmod{n} \;\; ; \;\; h \equiv j \pmod{n} \;\Rightarrow\; f+h \equiv t+j \pmod{n}$$

Dimostrazione

Consideriamo le uguaglianza $f=d \bullet n+t$, $h=g \bullet n+j$ che derivano dalle congruenze date e addizioniamole membro a membro:

$$f+h=(d+g) \bullet n+(t+j)$$

Da quest'ultima uguaglianza ne segue la tesi:

$$f+h \equiv (t+j) \pmod{n}$$

[3.3es1] - Esempio

Data la congruenza $5104 \equiv 41 \pmod{83}$, addizioniamo a entrambi i suoi membri l'intero 17:

$$5121 \equiv 58 \pmod{83}$$

Come era nelle nostre aspettative, si è ottenuto una nuova congruenza rispetto allo stesso modulo 83.

Si osservi tuttavia che:

$$5121 \not\equiv 5104 \pmod{83} \;\; ; \;\; 58 \not\equiv 41 \pmod{83}$$

[3.3es2] - Esempio

Data la congruenza $787619 \equiv -300 \pmod{863}$, addizioniamo a entrambi i suoi membri l'intero 11219:

$$798838 \equiv 10919 \pmod{863}$$

Come era nelle nostre aspettative, si è ottenuto una nuova congruenza rispetto allo stesso modulo 863.

Ma questa volta, contrariamente a quanto abbiamo osservato nell'esempio precedente, si verificano le congruenze:

$$787619 \equiv 798838 \pmod{863} \;\; ; \;\; -300 \equiv 10919 \pmod{863}$$

[3.3es3] - Esempio

Data la congruenza $20792 \equiv 91 \pmod{163}$, sottraiamo a entrambi i suoi membri l'intero 481:

$$20311 \equiv -390 \pmod{163}$$

Come era nelle nostre aspettative, si è ottenuta una nuova congruenza rispetto allo stesso modulo 163.

Si osservi tuttavia che:

$$20792 \not\equiv 20311 \pmod{163} \;\; ; \;\; 91 \not\equiv -390 \pmod{163}$$

Gli esempi precedenti ci inducono alla riflessione.
Infatti, data la congruenza:

$$f \equiv t \pmod{n},$$

ci chiediamo in quali circostanze accade che:

$$f \equiv f \pm z \equiv t \pmod{n}\ ,\ z \in Z$$

Come ci accingiamo a dimostrare con la proposizione seguente, queste congruenze sono vere solo per degli specifici valori di z .

[3.3e] - Sia data la congruenza:

$$f \equiv t \pmod{n},$$

se ad f si sottrae (o si addiziona) un intero z, multiplo del modulo n ($z = g \cdot n$) , $f \pm z$ è congruo ad f , e quindi anche a t , rispetto allo stesso modulo n:

$$f \pm gn \equiv f \equiv t \pmod{n}\ ,\ g \in Z$$

D*imostrazione*

Se sottraiamo (o addizioniamo) l'intero $z = g \cdot n$ a entrambi i membri della congruenza $f \equiv t \pmod{n}$, avremo le relazioni:

$$f \pm gn \equiv t \pm gn \pmod{n} \Rightarrow f \pm gn = kn + (t \pm gn)\ ,\ k \in Z$$

e quindi: $f \pm gn = (k \pm g)n + t \Rightarrow f \pm gn \equiv t \pmod{n}$

Come si vede, il secondo membro di quest'ultima congruenza è rimasto invariato rispetto alla congruenza di partenza, quindi, per la proprietà transitiva, le congruenze della tesi sono vere.

[3.3f] - Data la congruenza $f \equiv t \pmod{n}$, se ad f si sottrae (o si addiziona) un intero k che non sia multiplo del modulo n, l'intero $f \pm k$ non è congruo ad f , e nemmeno a t , modulo n:

$$f \equiv t \pmod{n}\ ,\ k \neq gn \Rightarrow f \pm k \not\equiv f \pmod{n}\ ,\ f \pm k \not\equiv t \pmod{n}$$

Dimostrazione

- Supponiamo che $f \pm k \equiv f \pmod{n}$ con $k \neq gn$

In questo caso, sottraendo f dai due membri della congruenza data, ne seguirebbe che $k \equiv 0 \pmod{n}$
Ma ciò è impossibile, perché quest'ultima congruenza è vera solo se $k = gn$, in contraddizione con l'ipotesi.

- Supponiamo che $f \pm k \equiv t \pmod{n}$ con $k \neq gn$

Anche in questo caso cadremmo in contradizione con l'ipotesi, perché, essendo $f \equiv t \pmod{n}$, per la proprietà transitiva, ne seguirebbe ancora la congruenza $k \equiv 0 \pmod{n}$.

Unifichiamo la *[3.3e] e* la *[3.3f]* in una sola proposizione.

[3.3g] - Data la congruenza f≡t (mod. n), soltanto se ad f si sottrae (o si addiziona) un multiplo z di n, la differenza (o la somma) è un intero congruente ad f, e quindi anche a t , rispetto allo stesso modulo n *(si consideri che in questo caso z≡0 , mod. n)* :

$$f \pm z \equiv f \equiv t \pmod{n} \Leftrightarrow z = g \bullet n \ , \ g \in Z$$

Ritornando ai principi fondamentali della divisibilità, enunciati ai punti *[2.1a]* e *[2.1b]* del secondo capitolo, si capisce adesso che essi sono in realtà delle applicazioni della proprietà *[3.3g]* .

Infatti, poiché $n \equiv n \pm m \bullet p \pmod{p}$, sottraendo (o addizionando) al numero intero n un multiplo di p, la condizione di divisibilità di n rispetto a p non subisce alcun mutamento.

[3.3es4] - Esempio

Mettiamo a confronto n=138567877 con p=127.

Dalla divisione euclidea ne risultano le relazioni:

$138.567.877 = 1091085 \bullet 127 + 82 \Rightarrow 138.567.877 \equiv 82 \pmod{127}$

Poiché 82>127/2 , calcoliamo il minimo resto.

Tenendo conto della *[3.2m]*, sottraiamo 127 ai due membri della congruenza:

$$138.567.877 - 127 \equiv 82 - 127 \pmod{127}$$

Per la *[3.3a]*, otteniamo una nuova congruenza, modulo n:

$$138567750 \equiv -45 \pmod{127}$$

Avendo sottratto un multiplo del modulo, per la *[3.3e]*, ne segue anche la congruenza:

$$138.567.877 \equiv 138.567.750 \pmod{127}$$

Quindi, per la proprietà transitiva:

$$138.567.877 \equiv -45 \pmod{127}$$

[3.3es5] - Esempio

Stabiliamo se n=289983 è divisibile per p=29.

Addizioniamo 17 a n: $289983 + 17 = 290000$

Da qui deduciamo che: $289983 \not\equiv 0 \pmod{29}$

Infatti, avendo addizionato un intero che non è multiplo di 29, abbiamo ottenuto 290000 che è invece multiplo di 29.

Pertanto: $29 \nmid 289983$

[3.3es6] - Esempio
Stabiliamo se il numero p=397 è primo o composto.

Se p fosse composto, dovrebbe avere qualche divisore primo p minore o uguale a 19, essendo $19<\sqrt{397}<23$.
Andiamo alla ricerca di suoi eventuali divisori primi.

Se al numero p sottraiamo 7 si ottiene 390 che non è multiplo di 7, di conseguenza neanche 397 è multiplo di 7.

Pur non avendo sottratto un multiplo di 13, la differenza è però 390, multiplo di 13, quindi 397 non è multiplo di 13.

Non è multiplo neanche di 17 e di 19, perché, sottraendo 17, si ottiene 380 che è multiplo di 19.
Si può constatare con facilità che 397 non è multiplo neppure dei rimanenti numeri primi minori di 19, quindi è primo.

[3.3es7] - Esempio
Calcoliamo il minimo resto positivo di n=37061, modulo 37.

Data la congruenza $37061\equiv x \pmod{37}$, se sottraiamo 61 ai suoi due membri, per la *[3.3a]* , otteniamo questa altre congruenza rispetto allo stesso modulo 37:

$$37000\equiv x-61\equiv 0 \pmod{37}$$

Ma: $37061\not\equiv 37000 \pmod{37}$
perché abbiamo sottratto 61 che non è multiplo di 37.

Tuttavia: $x-61\equiv 0 \pmod{37} \Rightarrow x\equiv 61-37\equiv 24 \pmod{37}$
Quindi il minimo resto positivo è 24.

[3.3es8] - Esempio
Calcoliamo il minimo resto positivo del numero n=81273, secondo il modulo 91.

Sottraendo 273 a n, poiché $273=3\cdot 91$, contrariamente a quanto è avvenuto nell'esempio precedente, vale la congruenza:

$$81273\equiv 81000 \pmod{91}$$

Dato che: $81000\equiv -10\cdot 10^3\equiv -100\cdot 100\equiv -9\cdot 9\equiv 10 \pmod{91}$
ricaviamo la congruenza cercata:

$$81273\equiv 10 \pmod{91}$$

Quindi il minimo resto di n, modulo 91, è 10.

[3.3h] - Siano dati due interi f e t , non necessariamente distinti, e il modulo $n \geq 2$.

a) - Se la loro differenza è un multiplo di n, come abbiamo già dimostrato nella *[3.2d]* , certamente f e t sono congrui, modulo n.

b) - Se la loro somma è un multiplo di n, f e t sono congrui, modulo n, soltanto quando si verificano queste due circostanze:
* entrambi sono congrui a 0, modulo n ;
* entrambi sono congrui all'intero n/2 , ammesso che n sia pari.

Dimostriamo la b)

Dati gli interi f e t, dalle loro divisioni euclidee per n, ricaviamo le relazioni:

$$f = gn + r_1 \quad 0 \leq r_1 < n \quad ; \quad t = hn + r_2 \quad 0 \leq r_2 < n$$

per cui: $f + t = (g+h)n + r_1 + r_2$

Dato che, per ipotesi, $f + t = m \bullet n$, ne consegue

o che $r_1 + r_2 = 0$ oppure che $r_1 + r_2 = n$

* la circostanza $r_1 + r_2 = 0$ si può verificare solo se $r_1 = r_2 = 0$
cioè solo nel caso in cui f e t sono entrambi multipli di n.

* la circostanza $r_1 + r_2 = n$, con $r_1 \neq r_2$, ha molte soluzioni, ma, come abbiamo dimostrato al punto *[3.2e]* , $r_1 \not\equiv r_2 \pmod{n}$, per cui: $f \not\equiv t \pmod{n}$

* la circostanza $r_1 + r_2 = n$, con $r_1 = r_2$, ha invece una soluzione soltanto: $r_1 = r_2 = n/2$, sempre che n/2 sia intero, la qual cosa accade esclusivamente quando n è pari.

Questo è l'unico caso in cui f e t , pur non essendo multipli del modulo pari n, sono congruenti.

[3.3es9] - Esempi

* $711 - 321 = 390 \Rightarrow 711 \equiv 321 \pmod{13}$
* $89 + 41 = 130$, ma $89 \not\equiv 41 \pmod{13}$
* $26 + 39 = 65 = 5 \bullet 13 \Rightarrow 26 \equiv 39 \pmod{13}$
perché sia 26, sia 39, sono multipli di 13
* $45 + 27 = 72 = 18 \bullet 4 \Rightarrow 45 \equiv 27 \pmod{18}$
perché sia 45, sia 27 sono multipli di $n/2 = 9$
* $15 \not\equiv 0 \pmod{10}$, ma $15 + 5 \equiv 0 \pmod{10}$
ciò perché $5 = n/2$ e $15 \equiv 5 \pmod{10}$

[3.3i] - Data la congruenza $f \equiv t \pmod{n}$, se si moltiplicano entrambi i suoi membri per un intero z , si ottiene una nuova congruenza rispetto allo stesso modulo n.

$$f \equiv t \pmod{n} \Rightarrow f \cdot z \equiv t \cdot z \pmod{n} \ , \ z \in Z$$

Dimostrazione

Consideriamo l'uguaglianza $f=g \cdot n+t$ che deriva dalla congruenza data e moltiplichiamo entrambi i suoi membri per un intero z .

$$f \cdot z=(g \cdot n+t) \cdot z$$

da questa ne segue la tesi:

$$f \cdot z-t \cdot z=h \cdot n \Rightarrow f \cdot z \equiv t \cdot z \pmod{n}$$

Si consideri però che il più delle volte:

$$f \not\equiv f \cdot z \pmod{n} \ , \ z \in Z$$

[3.3es10] - Esempio

Data la congruenza $983 \equiv 29 \pmod{53}$

moltiplicando per 10 entrambi i suoi membri, si ottiene una nuova congruenza, rispetto allo stesso modulo 53:

$$9830 \equiv 290 \pmod{53}$$

però: $9830 \not\equiv 983 \pmod{53}$; $290 \not\equiv 29 \pmod{53}$

[3.3j] - Date le congruenze $f \equiv t \pmod{n}$; $h \equiv j \pmod{n}$, se si moltiplicano tra loro membro a membro, si ottiene una nuova congruenza rispetto allo stesso modulo n:

$$f \equiv t \pmod{n} \ ; \ h \equiv j \pmod{n} \Rightarrow f \cdot h \equiv t \cdot j \pmod{n}$$

Dimostrazione

Consideriamo le uguaglianza $f=d \cdot n+t$, $h=g \cdot n+j$ che derivano dalle congruenze date e moltiplichiamole tra loro membro a membro.

$$fh=dgn^2+djn+gtn+tj=n(ndg+dj+gt)+tj$$

Da qui ne segue la tesi: $f \cdot h \equiv t \cdot j \pmod{n}$

[3.3es11] - Esempio

Date le congruenze $24 \equiv 2 \pmod{11}$; $15 \equiv 4 \pmod{11}$, moltiplichiamole tra loro membro a membro.

Come si può constatare facilmente, si ottiene ancora una congruenza, modulo 11: $360 \equiv 8 \pmod{11}$

Si noti però che: $360 \not\equiv 24 \pmod{11}$; $8 \not\equiv 4 \pmod{11}$

Data la congruenza $f \equiv t \pmod{n}$ ci chiediamo ora se, e in quali circostanze, possa accadere che $f \equiv f \cdot z \equiv t \pmod{n}$, $z \in Z$.

Come dimostreremo con la proposizione seguente, queste congruenze sono vere solo per determinati valori dell'intero z .

[3.3k] - Sia data la congruenza:

$$f \equiv t \pmod{n} \quad ; \quad f \not\equiv 0 \pmod{n}$$

Il prodotto $f \cdot z$ è un intero congruo ad f, e quindi anche a t, rispetto allo stesso modulo n, soltanto se $z \equiv 1 \pmod{n}$:

$$f \cdot z \equiv f \equiv t \pmod{n} \Leftrightarrow z \equiv 1 \pmod{n} \ , \ z \in Z$$

Dimostrazione

Data la congruenza:

$$f \equiv t \pmod{n} \ ; \ f \not\equiv 0 \pmod{n}$$

* supponiamo che $f \cdot z \equiv f \equiv t \pmod{n}$, $z \in Z$

In questo caso saranno valide le seguenti relazioni.

$$f \cdot z \equiv f \pmod{n} \Rightarrow f \cdot z - f \equiv 0 \pmod{n} \Rightarrow f \cdot (z-1) \equiv 0 \pmod{n}$$

Da qui, poiché abbiamo posto $f \not\equiv 0 \pmod{n}$, necessariamente deve essere $z \equiv 1 \pmod{n}$.

Ciò dimostra la proposizione diretta della tesi.

* supponiamo che $z \equiv 1 \pmod{n}$

Considerato che: $f \equiv t \pmod{n} \Rightarrow f = g \cdot n + t$, ($t \neq 0$ per ipotesi)

moltiplichiamo per l'intero z i due membri dell'uguaglianza:

$$f \cdot z = (g \cdot n + t) \cdot z = h \cdot n + t \cdot z \ , \ z \in Z$$

Per ipotesi risulta anche l'uguaglianza $z = d \cdot n + 1$, per cui, sostituendo, si avranno le relazioni:

$$f \cdot z = h \cdot n + t \cdot (dn+1) \Rightarrow f \cdot z = (h + td) \cdot n + t \Rightarrow f \cdot z \equiv t \pmod{n}$$

Pertanto, per la proprietà transitiva, ne segue la proposizione inversa della tesi: $f \cdot z \equiv t \equiv f \pmod{n}$

[3.3ℓ] - In modo evidente, tenuto conto della *[3.3k]* , sono valide le seguenti implicazioni.

$$f \equiv 0 \pmod{n} \Rightarrow f \equiv f \cdot z \equiv 0 \pmod{n} \ , \ \forall z \in Z$$

$$z \not\equiv 1 \ , \ f \not\equiv 0 \pmod{n} \Rightarrow f \not\equiv f \cdot z \pmod{n} \ , \ z \in Z$$

$$f \equiv 0 \ , \ z \equiv 1 \pmod{n} \Rightarrow f \equiv f \cdot z \pmod{n^2} \ , \ z \in Z$$

[[3.3es12] - Esempio
Si data la congruenza $25 \equiv 8 \pmod{17}$
* Moltiplichiamo entrambi i suoi membri per 18.
Per la *[3.3i]* si ottiene una nuova congruenza, modulo 17:

$$450 \equiv 144 \pmod{17}$$

In questo caso: $450 \equiv 25 \pmod{17}$; $144 \equiv 8 \pmod{17}$
Ciò accade perché $18 \equiv 1 \pmod{17}$, in accordo con la *[3.3k].*
* Moltiplichiamo entrambi i suoi membri per 4.
Si ottiene una nuova congruenza, ancora modulo 17:

$$100 \equiv 32 \pmod{17}$$

Ma: $25 \not\equiv 100 \pmod{17}$; $8 \not\equiv 32 \pmod{17}$
Ciò accade perché: $4 \not\equiv 1 \pmod{17}$
in accordo con la *[3.3k].*

Stabiliamo ora se è valida la proposizione inversa della *[3.3i].*
A questo fine, data la congruenza $a \equiv b \pmod{n}$, consideriamo il caso in cui a e b non sono coprimi $(a,b) \neq 1$ e sia d^m $(m \geq 1)$ un loro divisore comune. Si avrà quindi:

$$c \cdot d^m \equiv e \cdot d^m \pmod{n} \ ; \ m \geq 1$$

Ci proponiamo di capire se sia lecito dividere entrambi i membri di questa congruenza per d^m
Esaminiamo l'uguaglianza che deriva dalla congruenza data:

***)** $$c \cdot d^m - e \cdot d^m = g \cdot n \ ; \ g \in Z$$

Poiché il primo membro è divisibile per d^m , necessariamente anche il secondo membro $g \cdot n$ deve essere divisibile per d^m
Distinguiamo le due situazioni differenti che si possono verificare.

1)* Nella *) il modulo n e d siano coprimi: $(n,d)=1$
In questo caso, necessariamente g sarà divisibile per d^m , per cui valgono le relazioni:

$$c \cdot d^m - e \cdot d^m = g \cdot n \ \Rightarrow \ c - e = (g/d^m) \cdot n \ \Rightarrow \ c \equiv e \pmod{n}$$

2)* Nella *) il modulo n e d non siano coprimi: $(n,d) \neq 1$
In quest'altra circostanza la situazione è più complessa, perché potrebbe accadere che, oltre ad n, anche il fattore g sia divisibile per una potenza della base d.

Valutiamo allora cosa accade nella congruenza

$$c \bullet d^m \equiv e \bullet d^m \pmod{n} \;;\; m \geq 1$$

quando si verifica che:

$$(n,d) \neq 1 \;;\; d^s \mid g \;,\; s \geq 0$$

- Se $s \geq m$, valgono le relazioni:

$$c \bullet d^m - e \bullet d^m = g \bullet n \;\Rightarrow\; c - e = (g/d^m) \bullet n \;\Rightarrow\; c \equiv e \pmod{n}$$

Cosicché, visto che $d^m \mid g$, si ottiene ancora una congruenza rispetto allo stesso modulo n.

- Se invece $0 \leq s < m$, eseguendo la cancellazione, si ottengono delle congruenze il cui modulo non è più quello di partenza, perché certamente n sarà diviso per qualche fattore di d^m.
Tra queste congruenze ci sono anche le seguenti.

posto $(d^m, n) = a \;;\; a \nmid g \;;\; m \geq 1$

$$c \bullet d^m - e \bullet d^m = g \bullet n \;\Rightarrow\; c - e = (g \bullet n)/d^m = t \bullet (n/a) \;\Rightarrow\; c \equiv e \pmod{n/a}$$

posto $d = n \;;\; n^m \nmid g$

$$c \bullet n^m - e \bullet n^m = g \bullet n \;\Rightarrow\; c - e = (g \bullet n)/n^m = t \bullet (n/n) \;\Rightarrow\; c \equiv e \pmod{1}$$

Ma questa espressione non ha significato, perché, per definizione, il modulo di una congruenza è maggiore o uguale a 2.

Conclusione

[3.3m] - Data la congruenza:

$$c \bullet d^m \equiv e \bullet d^m \pmod{n} \;;\; m \geq 1$$

$$(n,d) = 1 \;\Rightarrow\; c \equiv e \pmod{n}$$

Se invece $(n,d) \neq 1$
la cancellazione del fattore comune d^m dà come risultato una congruenza il cui modulo non sempre è n, per cui, di volta in volta, è necessario fare una verifica.

[3.3es13] - Esempio
Data la congruenza $8591 \equiv 44 \pmod{37}$
Poiché: $8591 = 11 \bullet 781 \;;\; 44 = 11 \bullet 4$
e verificato che: $(11, 37) = 1$
Possiamo dividere i due membri della congruenza per 11, certi di ottenere un'altra congruenza rispetto allo stesso modulo n.

$$8591 \equiv 44 \pmod{37} \;\Rightarrow\; 781 \equiv 4 \pmod{37}$$

Si noti però che: $8591 \not\equiv 781 \pmod{37} \;;\; 44 \not\equiv 4 \pmod{37}$

[3.3es14] - Esempio
Data la congruenza $136 \equiv 56 \pmod{10}$
si constata facilmente che:

$$136 = 8 \bullet 17 \ ; \ 56 = 8 \bullet 7$$

Poiché 8 e il modulo non sono coprimi $(8, 10) \neq 1$, dividendo entrambi i membri della congruenza data per il loro fattore comune, non possiamo essere certi dell'esito.
Verifichiamo la validità della congruenza:

$$17 \equiv 7 \pmod{10}$$

Poiché $17 - 7 = 10$, ne segue che la congruenza è vera.
Quindi, come abbiamo constatato facilmente, pur avendo diviso per un fattore non coprimo col modulo 10, si è ottenuto una congruenza ancora modulo 10.
Ciò accade perché nell'uguaglianza $a - b = gn$, che deriva dalla congruenza $a \equiv b \pmod{n}$, anche il fattore g è divisibile per 8.
Infatti: $136 - 56 = 8 \bullet 10$

[3.3es15] - Esempio
Data la congruenza $1484 \equiv 21 \pmod{77}$
Poiché: $1484 = 7 \bullet 212 \ ; \ 21 = 7 \bullet 3$
e constatato che: $(7, 77) \neq 1$
dividendo i due membri per il loro divisore comune 7, non possiamo essere certi di potere ottenere una congruenza rispetto allo stesso modulo 77: l'esito della cancellazione dipende dal fattore g.
Quindi, eseguite le divisioni, è necessario fare una verifica.

$$1484 \equiv 21 \pmod{77} \Rightarrow 212 \equiv 3 \pmod{x}$$

Poiché $212 - 3 = 209 = 11 \bullet 19$
ne seguono le relazioni:

$$212 \not\equiv 3 \pmod{77} \ ; \ 212 \equiv 3 \pmod{11} \ ; \ 212 \equiv 3 \pmod{19}$$

Come si vede, la cancellazione del fattore comune 7 , non coprimo col modulo 77 , ha prodotto delle congruenze che non hanno più il modulo 77 di partenza.
Si noti che il modulo 11 è dato dalla divisione del modulo di partenza per il fattore comune 7, mentre il modulo 19 è del tutto imprevedibile.

[3.3es16] - Esempio
Data la congruenza $4473 \equiv 142 \pmod{71}$
Poiché: $4473 = 71 \cdot 63 \ ; \ 142 = 71 \cdot 2$
Dividendo i due membri per il loro fattore comune 71, si nota subito che la congruenza

$$63 \equiv 2 \pmod{71}$$ è falsa.

Ciò accade perché abbiamo diviso per 71 che è il modulo della congruenza data e il fattore g , in questo caso 61 , non è divisibile per 71. $(4473 - 142 = 61 \cdot 71)$
La cancellazione del fattore comune dà origine a una congruenza che ha un modulo diverso da quello di partenza:

$$63 \equiv 2 \pmod{61}$$

Si noti che l'espressione:

$$63 \equiv 2 \pmod{1}$$

è priva di significato, perché la definizione di congruenza stabilisce che il modulo sia $n \geq 2$.

[e3.3es17] - Esempio
Data la congruenza

$$18259 \equiv 10571 \pmod{31}$$

Poiché:

$$18259 = 31^2 \cdot 19 \ ; \ 10571 = 31^2 \cdot 11$$

dopo avere diviso i due membri per il fattore comune 31, uguale al modulo, è necessario verificare se l'espressione:

$$589 \equiv 341 \pmod{31}$$

è una congruenza valida.
Dal calcolo:

$$589 - 341 = 248 = 31 \cdot 8$$

ci accorgiamo che la congruenza ottenuta è ancora valida rispetto allo stesso modulo di partenza 31.

Diverso è il risultato se dividiamo per il fattore comune 31^2:

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

Infatti: $19 - 11 = 8$
Quindi, in questo caso, si ottiene una nuova congruenza con un modulo imprevedibile, diverso da quello di partenza:

$$19 \equiv 11 \pmod{8}$$

[3.3n] - Se si elevano alla stessa potenza entrambi i membri di una congruenza, si ottiene una nuova congruenza rispetto allo stesso modulo n:

$$f \equiv t \pmod{n} \Rightarrow f^m \equiv t^m \pmod{n} \ , \ m \in N$$

Dimostrazione

Consideriamo due volte la congruenza data:

$$f \equiv t \pmod{n} \ ; \ f \equiv t \pmod{n}$$

moltiplicando membro a membro, per la *[3.3j]* ne segue che:

$$f^2 \equiv t^2 \pmod{n}$$

Cosicché, moltiplicando questa nuova congruenza per quella di partenza e ripetendo la procedura m volte, ne seguirà la tesi.

[3.3es18] - Esempio

Sia data la congruenza $5 \equiv 19 \pmod{7}$

* Eleviamo a 3 i due membri della congruenza.

Come si può verificare facilmente, otteniamo un'altra congruenza rispetto allo stesso modulo 7:

$$5^3 \equiv 19^3 \pmod{7}$$

Tuttavia è opportuno osservare che:

$$5^3 \not\equiv 5 \pmod{7} \ ; \ 19^3 \not\equiv 19 \pmod{7}$$

* Eleviamo a 7 i due membri della congruenza.

Anche questa volta otteniamo una nuova congruenza rispetto allo stesso modulo 7:

$$5^7 \equiv 19^7 \pmod{7}$$

Ma, come si può constatare, questa volta, contrariamente a quanto è accaduto prima, succede che:

$$5^7 \equiv 5 \pmod{7} \ ; \ 19^7 \equiv 19 \pmod{7}$$

Stimolati da questi esempi, ci chiediamo in quali circostanze accade che:

$$f \equiv f^m \pmod{n} \ ; \ f \neq 0,1 \ ; \ m \neq 1$$

Una risposta concreta all'interrogativo ci viene data dal concetto: "periodo di n nella base f", sempre esistente.

(Nel mio libro "Wn - Un ordinamento possibile dei numeri primi" faccio un'approfondita trattazione su questo complesso argomento).

Il concetto di “periodo” è dato dalla seguente proposizione.

[3.3o] - Dato il modulo $n \geq 2$, sia $f > 1$ un intero tale che $(n,f)=1$

Il più piccolo valore $0<k<n$ tale che $f^k \equiv 1 \pmod{n}$, si dice periodo di n nella base f.

(In algebra k definisce l’ordine di f , modulo n).

Dal concetto di periodo ne consegue la risposta da noi cercata:

[3.3p] $f^k \equiv 1 \pmod{n} \Rightarrow f^{k+1} \equiv f \pmod{n}$

[3.3es19] - Esempio
Dato il modulo primo 41, scegliamo come base un qualsiasi intero coprimo con esso, ad esempio 10: $(41 , 10)=1$
Calcolando tutte le potenze di 10 in successione, cominciando dall’esponente zero, otteniamo le seguenti congruenze rispetto al modulo 41.

$10^0 \equiv 1 \pmod{41}$; $10^1 \equiv 10 \pmod{41}$; $10^2 \equiv 18 \pmod{41}$;
$10^3 \equiv 16 \pmod{41}$; $10^4 \equiv 37 \pmod{41}$; $10^5 \equiv 1 \pmod{41}$;
$10^6 \equiv 10 \pmod{41}$; . . .

A questo punto il calcolo può terminare, perché è chiaro che dall’esponente 5 in poi i valori di queste congruenze si ripeteranno sempre le stesse, ciclicamente.

Poiché 5 è il più piccole esponente della base 10 con cui si ripete il valore iniziale 1 di queste congruenze, diciamo:
“5 è il periodo in base 10 del numero 41”
Oppure: “5 è l’ordine di 10, modulo 41”
Si badi che il valore del periodo varia al variare della base.
Ad esempio, nella base 2 il periodo di 41 è 20, e non 5.
Infatti: $2^i \not\equiv 1 \pmod{41}$, $0<i<20$, mentre $2^{20} \equiv 1 \pmod{41}$

[3.3es20] - Esempio
Calcoliamo il periodo del numero composto 91 in base 3, considerato che $(91,3)=1$

$3^0 \equiv 1 \pmod{91}$; $3^1 \equiv 3 \pmod{91}$; $3^2 \equiv 9 \pmod{91}$;
$3^3 \equiv 27 \pmod{91}$; $3^4 \equiv 81 \pmod{91}$; $3^5 \equiv 61 \pmod{91}$;
$3^6 \equiv 1 \pmod{91}$ . . .

Quindi: “6 è il periodo in base 3 del numero 91”

Pur essendo la *[3.3p]* una risposta esauriente al quesito che ci siamo posti, tuttavia dobbiamo tenere presente che non è facile stabilire qual è il periodo di un intero q, perché non esiste una formula che lo determini.
Per questo motivo, nelle applicazioni, si aggira l'ostacolo facendo ricorso ad alcuni teoremi che in qualche modo sfruttano la peculiarità del periodo.

Fondamentale è un teorema di Laplace sui gruppi, dal quale si deduce che il periodo dell'intero positivo q è un divisore di $\phi(q)$.

$\phi(q)$, nota come funzione di Eulero, indica quanti sono gli interi positivi $0<a<q$ tali che $(a,q)=1$.
Si deve considerare che il numero 1 è sempre presente nel calcolo e quando q è numero primo $\phi(q)=q-1$
Esempi: $\phi(15)=8$; $\phi(17)=16$

Questi altri teoremi si possono dedurre dal teorema di Laplace.

* Piccolo teorema di Fermat
Se p è primo necessariamente deve valere la congruenza:

$$a^p \equiv a \pmod{p} \; ; \; (0<a<p)$$

* Teorema di Eulero
Se q è un intero qualsiasi , vale la congruenza:

$$a^{\phi(q)+1} \equiv a \pmod{q} \; ; \; (a, q)=1$$

(Si deve osservare che quando q è primo, il teorema di Eulero coincide con "il piccolo teorema di Fermat").

* Teorema VV
Se q è dispari e a è residuo quadratico, vale la congruenza:

$$a^{(\phi(q)/2)+1} \equiv a \pmod{q} \; ; \; (a, q)=1$$

Io stesso ho dimostrato quest'ultimo teorema e l'ho pubblicato nel mio sito personale:

www.integernumbers.org/vv.pdf

Finora i docenti professionisti ai quali mi sono rivolto hanno disdegnato di dialogare con me, per cui non mi è stato possibile accertare l'originalità e il pregio di questo teorema.

Il lettore verificherà da sé la validità delle deduzioni da me addotte a sua dimostrazione.
Sarò grato a chi volesse darmi un suo parere.

[3.3es21] - Esempio
Calcoliamo il minimo valore positivo della congruenza:

$$10^{49} \equiv x \pmod{13} \quad ; \quad 0<x<13$$

Il periodo di 13 nella base 10 è 6, quindi: $10^7 \equiv 10 \pmod{13}$

Cosicché, applicando la *[3.3p]* , il calcolo diventa semplice.
Scomponiamo l'esponente e passiamo alle congruenze.

$$10^{49} = 10^{7 \cdot 7} \equiv 10 \pmod{13}$$

[3.3es22] - Esempio
Calcoliamo la congruenza:

$$8^{130} \equiv x \pmod{43}$$

Se non si sa qual è il periodo di 43 in base 8, trattandosi di un modulo primo, per risolvere questa congruenza si può applicare il "piccolo teorema di Fermat": $8^{43} \equiv 8 \pmod{43}$

Per cui, scomposto l'esponente, calcoliamo le congruenze:

$$8^{130} = 8^{3 \cdot 43+1} = 8 \cdot 8^3 \equiv 8^4 \equiv 21^2 \equiv 11 \pmod{43}$$

Questo è il minimo valore positivo che risolve la congruenza.
Infatti, in base alla *[3.2f]* , 3^{130} è congruo a uno solo dei valori compresi tra 0 e 43.

Si osservi che nelle applicazioni si preferisce servirsi della congruenza $a^k \equiv 1 \pmod{p}$, anziché $a^{k+1} \equiv a \pmod{p}$, per facilitare il calcolo, dato che 1 è l'elemento neutro della moltiplicazione.

[3.3es23] - Esempio
Risolviamo la congruenza

$$7^{3130} \equiv x \pmod{12} \quad ; \quad 0<x<12$$

Considerato che 7 e 12 sono coprimi, per il teorema di Eulero, vale la congruenza: $7^{\phi(12)} \equiv 1 \pmod{12}$

Pertanto, essendo $\phi(12)=4$, si ha: $7^4 \equiv 1 \pmod{12}$

Cosicché il calcolo è immediato:

$$7^{3130} \equiv 7^{728 \cdot 4+2} \equiv 7^2 \equiv 1 \pmod{12}$$

Da qui ne segue anche che il periodo di 12, in base 7, è 2.

[3.3es24] - Esempio
Risolviamo la congruenza

$$4^{317} \equiv x \pmod{11} \quad ; \quad 0 \le x < 11$$

Considerato che 4 è residuo quadratico e 11 numero primo, per il Teorema VV, vale la congruenza: $4^5 \equiv 1 \pmod{11}$

per cui: $4^{317} \equiv 4^{63 \cdot 5+2} \equiv 4^2 \equiv 5 \pmod{11}$

[3.3es25] - Esempio
Risolviamo la congruenza

$$7^{1259} \equiv x \pmod{15} \quad ; \quad 0 \le x < 15$$

Per il Teorema VV, solo nel caso in cui il modulo p sia primo e la base sia un non residuo quadratico, accade che:

$a^{\phi(p)/2} \equiv -1 \pmod{p}$ (vedi: www.integernumbers.org/vv.pdf)

Pertanto, dato che 15 non è primo ma composto e (7, 15)=1,

vale la congruenza: $7^{\phi(15)/2} \equiv 1 \pmod{15}$

Cosicché il calcolo è immediato.

Essendo $\phi(15)=8$, ne segue che $7^4 \equiv 1 \pmod{15}$

Quindi: $7^{1259} = 7^{4 \cdot 314+3} \equiv 7^3 \equiv 4 \cdot 7 \equiv 13 \pmod{15}$

[3.3es26] - Esempio
Stabiliamo se p=17447 sia primo o composto.

- Supponiamo che p sia primo.

In questo caso $\phi(p)=(p-1)$, quindi, per il teorema VV , deve valere la congruenza:

$$2^{8723} \equiv \pm 1 \pmod{17447}$$

L'incertezza del segno è dovuta all'impossibilità di stabilire subito se la base 2 sia o no un residuo quadratico.

Ma, in entrambi i casi, la congruenza è falsa, perché dal calcolo risulta:

$$2^{8723} \equiv 8691 \pmod{17447}$$

Ne consegue così che 17447 sicuramente è composto.

Infatti: $17447 = 73 \cdot 239$

3.4 Applicazione delle proprietà

[3.4a] - Data una espressione polinomiale

$$a_1^{k_1} \bullet a_2^{k_2} + a_3^{k_3} \bullet a_4^{k_4} + a_5^{k_5} \bullet a_6^{k_6} + \ldots \quad (a_i \in Z \ ; \ k_j \geq 0)$$

se ad alcuni o a tutti i suoi termini si sostituiscono degli interi ad essi congruenti, modulo n, si ottiene un polinomio congruente, rispetto allo stesso modulo n.

Infatti, dato un intero n, ogni termine $a_i^{k_j}$ del polinomio si può scrivere nella forma:

$$a_i^{k_j} = n \bullet g_i + r_i \ ; \ g_i , \ r_i \in Z$$

Dove r_i , in valore assoluto, non deve essere necessariamente minore del modulo n.

Cosicché possiamo scrivere il polinomio nel modo seguente:

$$a_1^{k_1} \bullet a_2^{k_2} + a_3^{k_3} \bullet a_4^{k_4} + a_5^{k_5} \bullet a_6^{k_6} + \ldots =$$

$$= (n \bullet g_1 + r_1)(n \bullet g_2 + r_2) + (n \bullet g_3 + r_3)(n \bullet g_4 + r_4) + \ldots$$

Passiamo poi alle congruenze, considerando che $n \bullet g_i \equiv 0$ (mod. n).

$$a_1^{k_1} \bullet a_2^{k_2} + a_3^{k_3} \bullet a_4^{k_4} + a_5^{k_5} \bullet a_6^{k_6} + \ldots \equiv r_1 \bullet r_2 + r_3 \bullet r_4 + r_5 \bullet r_6 + \ldots \ (\text{mod. n})$$

Si consideri che nel generico prodotto $a_h^{k_s} \bullet a_t^{k_c}$ sono valide anche le implicazioni:

$$a_t^{k_c} \equiv 0 \ (\text{mod. n}) \ \Rightarrow \ a_h^{k_s} \bullet a_t^{k_c} \equiv 0 \ (\text{mod. n})$$

$$a_t^{k_c} \equiv 1 \ (\text{mod. n}) \ \Rightarrow \ a_h^{k_s} \bullet a_t^{k_c} \equiv a_h^{k_s} \ (\text{mod. n})$$

[3.4es1] - Esempio

Calcoliamo il minimo valore positivo della congruenza, modulo 31, del polinomio:

$$p = 41^{17} \bullet 5^4 + 13^{20} \bullet 10^{31} + 29 \bullet 11^2 + 37$$

Stabiliamo prima la validità delle seguenti uguaglianze:

$41^{17} = 84326460241960491232378654 \bullet 31 + 7$; $5^4 = 20 \bullet 31 + 5$;

$13^{20} = 6130633475767999818 96 \bullet 31 + 25$;

$10^{31} = 32258064516129032258064516129 0 \bullet 31 + 10$;

$29 = 0 \bullet 31 + 29$; $121 = 3 \bullet 31 + 28$; $37 = 31 + 6$

Poi facciamo le dovute sostituzioni nel polinomio e passiamo alle congruenze, considerando che $a \bullet 31 \equiv 0$ (mod.31) , $a \in Z$.

$p \equiv 7 \bullet 5 - 6 \bullet 10 + (-2) \bullet (-3) + 6 \equiv -13 \equiv 18$ (mod. 31)

[3.4es2] - Esempio
Risolviamo la congruenza:

$$3900137270000265131 \equiv x \pmod{13} \quad , \quad 0 \le x < 13$$

Come si intuisce facilmente, alle cifre contigue che formano un multiplo di 13 si può sostituire un'eguale quantità di zeri. Per convincercene basta scrivere il numero dato in forma polinomiale e passare alle congruenze.

39.00.13.7.27.0000.26.5.13.1=

$$=39\cdot10^{17}+13\cdot10^{13}+7\cdot10^{12}+27\cdot10^{10}+26\cdot10^{4}+5\cdot10^{3}+13\cdot10+1$$

Considerato che $a\cdot31\equiv0 \pmod{13}$; $a\in Z$, ne segue che:

$$3900137270000265131\equiv7\cdot10^{12}+27\cdot10^{10}+5\cdot10^{3}+1 \pmod{13}$$

cioè: $3900137270000265131\equiv7270000005001 \pmod{13}$

si consideri anche che $10^{12}\equiv1 \pmod{13}$ (teorema di Fermat), quindi:

$$7\cdot1+1\cdot10^{10}+5\cdot10^{3}+1\equiv7+(-3)^{3\cdot3+1}+5\cdot(-3)^{3}+1\equiv$$
$$\equiv8+(-3)\cdot(-1)-5\equiv6 \pmod{13}$$

[3.4es3] - Esempio
Risolviamo la congruenza:

$$23713 \equiv x \pmod{10} \quad , \quad 0 \le x < 10$$

Scriviamo il numero in forma polinomiale:

$$23713=2\cdot10^{4}+3\cdot10^{3}+7\cdot10^{2}+10+3$$

Poiché: $10^{i}\equiv0 \pmod{10}$, $(i\ge1)$

facendo le sostituzioni, il risultato è immediato.

$$23713\equiv3 \pmod{10}$$

[3.4es4] - Esempio
Risolviamo la congruenza:

$$690827 \equiv x \pmod{7} \quad , \quad 0 \le x < 7$$

Scriviamo il numero in forma polinomiale:

$$690837=6\cdot10^{5}+9\cdot10^{4}+0\cdot10^{3}+8\cdot10^{2}+2\cdot10^{1}+7\cdot10^{0}$$

Poiché: $10^{0}\equiv1$, $10\equiv3$, $10^{2}\equiv2 \pmod{7}$

$$10^{3}\equiv-1 \ , \ 10^{4}\equiv4\equiv-3 \ , \ 10^{5}\equiv5\equiv-2 \pmod{7}$$

sostituendo, otteniamo con facilità il risultato cercato.

$$(-1)\cdot(-2)+2\cdot(-3)+0+1\cdot2+2\cdot3+0\equiv2+1+2-1\equiv4 \pmod{7}$$

[3.4es5] - Esempio
Calcoliamo il minimo resto positivo di 21507119, modulo 17.

Dato che il 17 è formato da 2 cifre, è opportuno scrivere il numero dato in questa forma polinomiale:

$$21507119=19+71\cdot10^2+50\cdot10^4+21\cdot10^6$$

e poiché: $10^2\equiv(-7)^2\equiv49\equiv-2 \pmod{17}$

$10^4\equiv(-2)^2\equiv4$, $10^6\equiv(-2)^3\equiv-8 \pmod{17}$

$19\equiv2$, $71=51+20\equiv3$, $50\equiv-1 \pmod{17}$

$21\equiv4 \pmod{17}$

Ne segue: $21\cdot10^6+50\cdot10^4+71\cdot10^2+19\equiv4\cdot(-8)+(-1)\cdot4+3\cdot(-2)+2\equiv$

$\equiv-32-4-6+2\equiv-6\equiv11 \pmod{17}$

Quindi: $21507119\equiv11 \pmod{17}$

[3.4es6] - Esempio
Calcoliamo il minimo resto del numero $n=43\cdot10^{32}+1$ rispetto al modulo p=241.

Considerato che a nostra disposizione abbiamo la calcolatrice di Windows a sole 32 cifre, scriviamo n in quest'altra forma polinomiale:

$$n=430\cdot10^{31}+1$$

e poiché: $430\equiv-52$, $10^{31}\equiv10 \pmod{241}$

ne segue che: $43\cdot10^{32}+1\equiv-520+1\equiv-37 \pmod{241}$

[3.4es7] - Esempio
Risolviamo la seguente congruenza:

$$233^{910}\equiv x \pmod{911} \ ; \ 0\le x<911$$

Considerato che a nostra disposizione abbiamo la calcolatrice di Windows a sole 32 cifre, procediamo coi calcoli nel seguente modo.

Scomponiamo l'esponente e passiamo alle congruenze.

$233^{910}=233^{2\cdot5\cdot7\cdot13}=(233^{10})^{7\cdot13}\equiv577^{7\cdot13}\equiv491^{13}\equiv491^{11+2}\equiv$

$\equiv491^2\cdot491^{11}\equiv577\cdot30\equiv1 \pmod{911}$

Quindi: $233^{910}\equiv1 \pmod{911}$

[3.4es8] - Esempio
Stabiliamo se n ed m sono divisibili per p=1091
n=18.455.672.443.580.719.048.776.608.897.526.141
m=3.200.144.676.877.659.890.713.254.667.710.015.497.808.317

Considerato che abbiamo a disposizione la calcolatrice di Windows a sole 32 cifre e il numero n invece è formato da 35 cifre, trasformiamo n nella seguente forma polinomiale.

$$1845.567244358071904877660889752614 1 =$$

$$=1845 \cdot 10^{31} + 567244358071904877660889752614 1 \equiv$$

$$\equiv 754 \cdot 599 + 28 \equiv 451674 \equiv 0 \pmod{1091}$$

Ne segue che: $1091 \mid n$

Facciamo la verifica con m, formato da 43 cifre.

$$m = 320014467687 \cdot 10^{31} + 765989071325466771001549780831 7 \equiv$$
$$\equiv 946 \cdot 599 + 817 = 567471 \equiv 151 \pmod{1091}$$

Ne segue che: $1091 \nmid m$

[3.4es9] - Esempio
Risolviamo la congruenza:

$$900001 \equiv x \pmod{41} \quad , \quad 0 \le x < 41$$

Si sa che nella numerazione decimale il numero primo 41 ha periodo 5, per cui: $10^5 \equiv 1 \pmod{41}$
Cosicché, scrivendo il numero in forma polinomiale, la congruenza si risolve facilmente:

$$900001 = 9 \cdot 10^5 + 1 \equiv 10 \pmod{41}$$

[3.4es10] - Esempio
Risolviamo la congruenza:

$$620000027 \equiv x \pmod{31} \quad , \quad 0 \le x < 31$$

Osservando che le prime due cifre formano il numero 62, multiplo del modulo 31, è opportuno fare riferimento alla seguente forma polinomiale:

$$620000027 = 62 \cdot 10^7 + 27$$

Cosicché, essendo $62 \equiv 0 \pmod{31}$, il risultato è immediato:

$$620000027 \equiv 27 \pmod{31}$$

3.5 Criteri di divisibilità

[3.5es1] - Esempio
Risolviamo la congruenza
$17.325.397.127.453.192.168.315.367 \equiv x \pmod{37}$; $0 \le x < 37$

Considerato che 37 nella numerazione decimale ha periodo 3, e quindi $10^3 \equiv 1 \pmod{37}$, ci conviene raggruppare le cifre del numero dato in classi di tre elementi, a iniziare da destra, e scriverlo nella seguente forma polinomiale.
Successivamente passeremo alle congruenze, modulo 37.

$$367+315\cdot 10^3+168\cdot(10^3)^2+192\cdot(10^3)^3+453\cdot(10^3)^4+127\cdot(10^3)^5+$$
$$+397\cdot(10^3)^6+325\cdot(10^3)^7+17\cdot(10^3)^8\equiv$$
$$\equiv 367+315+168+192+453+127+397+325+17\equiv$$
$$\equiv 2361\equiv 361+2\cdot 10^3\equiv 363\equiv -1\cdot 10+3\equiv -7\equiv 30 \pmod{37}$$

Riflettendo sull'esempio *[3.5es1]* , è evidente che il procedimento seguito per il suo svolgimento si può generalizzare a un qualsiasi modulo q , così come viene esposto nel seguente enunciato.

[3.5a] - Sia dato un intero z, formato da t cifre, e un modulo q di periodo k nella base B, con $k<t$.
Raccolte le cifre di z in gruppi di k elementi a iniziare da destra, la somma delle classi così formate è un intero congruo a z, secondo il modulo q.

Dimostrazione
Sia dato l'intero $z=a_t \dots a_2 a_1$ in base B, formato da t cifre.
(a_n è la cifra di z di posto n, andando da destra verso sinistra).
Iniziando dalla cifra a_1 , raggruppiamo le cifre di z in gruppi di k elementi ($k<t$) con l'eventualità che l'ultimo gruppo possa avere una quantità di cifre inferiore a k.
Trasformiamo quindi z nella seguente forma polinomiale.

$$z=(a_k\dots a_2 a_1)+(a_{2k}\dots a_{k+2}a_{k+1}\cdot B^k)+(a_{3k}\dots a_{2k+2}a_{2k+1}\cdot B^{2k})+\dots a_t\cdot B^{mk}$$

Per ipotesi: $B^k \equiv 1 \pmod{q} \Rightarrow B^{nk}\equiv 1 \pmod{q}$, $n \ge 0$

Da qui ne segue la tesi:

$$z\equiv(a_k\dots a_2 a_1)+(a_{2k}\dots a_{k+2}a_{k+1})+(a_{3k}\dots a_{2k+2}a_{2k+1})+\dots a_t \pmod{q}$$

Così come espongo nel libro “Wn - Un ordinamento possibile dei numeri primi”, in cui faccio un’ampia trattazione sul “periodo”, quando nella base B il periodo k di un numero primo p è pari, vale la congruenza:

$$B^{k/2} \equiv -1 \pmod{p}$$

In questo caso la *[3.5a]* si può ridurre a una più semplice.

[3.5b] - Dato un intero $z = a_t \dots a_2 a_1$, formato da t cifre, e un modulo p primo il cui periodo k sia pari nella base B, con $k/2 < t$.
Staccate le cifre di z a gruppi di k/2 elementi, iniziando da destra, la somma algebrica delle classi così formate, considerandole, alternativamente, positive e negative, è un intero congruo a z, modulo p.

Dimostrazione

Iniziando dalla cifra a_1 , stacchiamo le cifre di z in modo da formare classi di k/2 elementi e scriviamo z in forma polinomiale.

$$z = (a_{k/2} \dots a_2 a_1) + (a_k \dots a_{k/2+2} a_{k/2+1} \cdot B^{k/2}) + (a_{3k/2} \dots a_{k+2} a_{k+1} \cdot B^k) +$$
$$+ (a_{2k} \dots a_{3k/2+2} a_{3k/2+1} \cdot B^{3(k/2)}) + \dots$$

Per ipotesi, si ha:

$$B^{k/2} \equiv -1 \pmod{p} \ , \ B^k \equiv 1 \pmod{p}$$

quindi:

$$B^{h \cdot k/2} \equiv (-1)^h \pmod{p} \ , \ h \geq 0$$

Da qui ne segue la tesi:

$$z \equiv (a_{k/2} \dots a_2 a_1) - (a_k \dots a_{k/2+2} a_{k/2+1}) + (a_{3k/2} \dots a_{k+2} a_{k+1}) - a_{2k} \dots \pmod{p}$$

[3.5es2] - Esempio
Stabiliamo se z=1009200057 è divisibile per 3 e per 9

Nella numerazione decimale sia il 3, sia il 9 hanno periodo k=1, per cui:

$$10^n \equiv 1 \pmod{3}, \pmod{9} \ ; \ \forall n \geq 0$$

Cosicché conviene scrivere z in forma polinomiale considerando le sue cifre singolarmente. Passeremo poi alle congruenze.

$$z = 7 \cdot 10^0 + 5 \cdot 10^1 + 2 \cdot 10^5 + 9 \cdot 10^6 + 1 \cdot 10^9 \equiv$$
$$\equiv 7 + 5 + 2 + 9 + 1 \equiv 24 \equiv 2 + 4 \equiv 6 \pmod{3}, \pmod{9}$$

Poiché $6 \equiv 0 \pmod{3}$, ne segue che z è divisibile per 3.
Poiché $6 \not\equiv 0 \pmod{9}$, ne segue che z non è divisibile per 9.

Generalizziamo i calcoli eseguiti nell'esempio *[3.5es2]* enunciando il seguente

criterio di divisibilità per 3

[3.5c] - Per stabilire se un qualsiasi intero z è divisibile per 3 basta addizionare le sue cifre: soltanto se la loro somma è un intero congruo a 0, modulo 3, z è divisibile per 3.

Reiterando questo criterio sulle somme via via ottenute, alla fine si otterrà un intero congruente a z, modulo 3, di una sola cifra. Soltanto se questa cifra è 3 o 6 o 9, z è divisibile per 3.

[3.5es3] - Esempio
Stabiliamo se z=307532071 è divisibile per il numero primo 11.

Nella numerazione decimale 11 ha periodo k=2, per cui:

$$10^{2n} \equiv 1 \pmod{11}\ ,\ \forall n \geq 0$$

Tenuto conto di ciò, ci conviene scrivere z in forma polinomiale staccando le sue cifre in classi di due elementi, iniziando da destra. Passeremo poi alle congruenze.

$$3.07.53.20.71 \equiv 71 \cdot 10^0 + 20 \cdot 10^2 + 53 \cdot 10^4 + 7 \cdot 10^6 + 3 \cdot 10^8 \equiv$$
$$\equiv 71 + 20 + 53 + 7 + 3 \equiv 154 \equiv 54 + 1 \equiv 0 \pmod{11}$$

Però il periodo k di 11 è pari, quindi valgono pure le relazioni:

$$10^{k/2} \equiv -1 \pmod{11} \Rightarrow 10^{n \cdot (k/2)} \equiv (-1)^n \pmod{11}\ ,\ n \geq 0$$

Cosicché possiamo scrivere z in forma polinomiale considerando le sue cifre anche singolarmente.

$$1 \cdot 10^0 + 7 \cdot 10^1 + 2 \cdot 10^3 + 3 \cdot 10^4 + 5 \cdot 10^5 + 7 \cdot 10^6 + 3 \cdot 10^8 \equiv$$
$$\equiv 1 - 7 - 2 + 3 - 5 + 7 + 3 \equiv 0 \pmod{11}$$

In entrambi i casi deduciamo che z è divisibile per 11.

Generalizzando i due procedimenti dell'esempio *[3.5es3]* possiamo scegliere tra i due seguenti

criteri di divisibilità per 11

[3.5d] - Per stabilire se un intero z è divisibile per 11 basta addizionare le classi formate dalle sue cifre, raggruppate a due a due a iniziare da destra.
Soltanto se la loro somma è un intero congruo a 0, modulo 11, z è multiplo di 11.

[3.5e] - Per stabilire se un intero z è divisibile per 11 basta addizionare le sue cifre, considerandole, alternativamente, positive e negative. Solo se la loro somma algebrica è un intero congruo a 0, modulo 11, z è multiplo di 11.

Ciascuno di questi due criteri si può ripetere sulle somme via via ottenute. Soltanto se, alla fine, si otterrà un numero formato da due cifre uguali, oppure zero, z è divisibile per 11.

[3.5es4] - Esempio
Stabiliamo se z=408632053 è multiplo del numero primo 101.

Nella numerazione decimale 101 ha periodo k=4, per cui:

$$10^{2n} \equiv (-1)^n \pmod{101} \quad , \quad n \geq 0$$

Tenuto conto di questa relazione, ci conviene scrivere z in forma polinomiale staccando le sue cifre a gruppi di 2 elementi, iniziando da destra. Passeremo poi alle congruenze.

$$4.08.63.20.53 \equiv 53 \cdot 10^0 + 20 \cdot 10^2 + 63 \cdot 10^4 + 8 \cdot 10^6 + 4 \cdot 10^8 \equiv$$

$$\equiv 53 - 20 + 63 - 8 + 4 \equiv 92 \pmod{101}$$

Poiché: $92 \not\equiv 0 \pmod{101}$

ne segue che z non è multiplo di 101.

Generalizzando il procedimento dell'esempio *[3.5es4]* possiamo stabilire il seguente

criterio di divisibilità per 101

[3.5f] - Per stabilire se un qualsiasi intero z è divisibilità per 101 basta raggruppare le sue cifre a due a due iniziando da destra e considerare le classi così formate, alternativamente, positive e negative. Soltanto se la loro somma algebrica è un intero congruo a 0, modulo 101, z è multiplo di 101.

Reiterando il procedimento sulle somme via via ottenute, alla fine si otterrà un numero congruente a z, modulo 101, formato da una o due cifre.
Solo se questo numero è 0, z è divisibile per 101.

Ritorniamo indietro all'esempio *[3.5es1]* per osservare il procedimento che abbiamo usato allo scopo di stabilire la divisibilità per 37 del numero dato e generalizziamolo a un qualsiasi altro intero z.

Criterio di divisibilità per 37

[3.5g] - Per stabilire se un qualsiasi intero z è divisibile per 37 basta raggruppare le sue cifre a tre a tre iniziando da destra. Soltanto se la somma delle classi così formate è un intero congruo a 0, modulo 37, z è multiplo di 37.

Reiterando il procedimento sulle somme via via ottenute, alla fine si otterrà un intero congruente a z, modulo 37, formato da non più di tre cifre.

[3.5es5] - Esempio
Stabiliamo se z=54110873720369 è multiplo di 7.

Nella numerazione decimale il numero primo 7 ha periodo k=6, per cui vale la relazione:

$$10^{n\cdot 3} \equiv (-1)^n \pmod 7 \quad , \quad n \geq 0$$

Cosicché ci conviene scrivere z in forma polinomiale raggruppando le sue cifre in classi di 3 elementi, a iniziare da destra. Passeremo poi alle congruenze.

$$54.110.873.720.369 =$$
$$= 369 \cdot 10^0 + 720 \cdot 10^3 + 873 \cdot 10^{2\cdot 3} + 110 \cdot 10^{3\cdot 3} + 54 \cdot 10^{4\cdot 3} \equiv$$
$$\equiv 369 - 720 + 873 - 110 + 54 \equiv 466 \equiv 46 \cdot 10 + 6 \equiv -3 \cdot 3 + 6 \equiv -3 \pmod 7$$

Poiché $-3 \not\equiv 0 \pmod 7$, ne segue che z non è multiplo di 7

In generale vale il seguente

criterio di divisibilità per 7

[3.3h] - Per stabilire se un qualsiasi intero z è divisibilità per 7 basta raggruppare le sue cifre a tre a tre iniziando da destra e considerare le classi così formate, alternativamente, positive e negative. Soltanto se la loro somma algebrica è un intero congruo a 0, modulo 7, z è multiplo di 7.

Reiterando il procedimento sulle somme via via ottenute, alla fine si otterrà un numero congruente a z, modulo 7, formato da non più di tre cifre.

Nella numerazione decimale accade che il 13 ha periodo k=6, uguale a quello del 7, per cui il criterio di divisibilità per 13 è identico a quello per il 7.

Criterio di divisibilità per 13

[3.3i] - Per stabilire se un qualsiasi intero z è divisibilità per 13 basta raggruppare le sue cifre a tre a tre iniziando da destra e considerare le classi così formate, alternativamente, positive e negative. Soltanto se la loro somma algebrica è un intero congruo a 0, modulo 13, z è multiplo di 13.

Reiterando il procedimento sulle somme via via ottenute, alla fine si otterrà un intero congruente a z, modulo 13, formato da non più di tre cifre.

Per dei motivi particolari che espongo nel mio libro "Wn - un ordinamento possibile dei numeri primi", l'intero ottenuto con questo procedimento è congruo a z riguardo anche al modulo 11, oltre che ai moduli 7 e 13.

Per cui, se alla fine delle reiterazioni del procedimento si ottiene zero, z è divisibile sia per 7, sia per 11, sia per 13.

[3.5es6] - Esempi
Stabiliamo se sono divisibili per 7, per 11 e per 13 i numeri:
g=1.557.900.303.007.111
t=10.756.061.737.166.186.863.538.809.153.461

Così come risulta dalla *[3.3i]* i numeri primi 7, 11 e 13 hanno un unico criterio di divisibilità determinato dalla congruenza:

$$10^{n\cdot 3} \equiv (-1)^n \pmod{7},\ \pmod{11},\ \pmod{13}\ ;\ n \geq 0$$

Cosicché, staccate le cifre del numero in considerazione a tre a tre, iniziando da destra, addizioniamo le classi ottenute considerandole, alternativamente, positive e negative.

$g \equiv 111-7+303-900+557-1 \equiv 63 \pmod{7},\pmod{11},\pmod{13}$

Da qui ne segue che:

$63 \equiv 0 \pmod{7} \Rightarrow 7 \mid z$

$63 \not\equiv 0 \pmod{11} \Rightarrow 11 \nmid z$

$63 \not\equiv 0 \pmod{13} \Rightarrow 13 \nmid z$

$t \equiv 461-153+809-538+863-186+166-737+61-756+10 \equiv$
$\equiv 0 \pmod{7},\ \pmod{11},\ \pmod{13}$

Ne consegue che t è divisibile sia per 7, sia per 11, sia per 13.

Appare evidente che i criteri di divisibilità che abbiamo esposto fin qui sono facili da applicare perché il periodo k dei moduli considerati è inferiore a 5.
Tuttavia, anche se la loro efficacia diminuisce man mano che il valore del periodo k aumenta, ciò non toglie che possano essere utili quando si ha a che fare con numeri di grandi dimensioni.

[3.5es7] - Esempio
Stabiliamo se z=5112.70021.00090.82021.91671.99873.40097 è divisibile per 41 e per 271.

La calcolatrice di windows a nostra disposizione non ci consente di operare direttamente con questo numero di 34 cifre, per cui dobbiamo fare ricorso ai criteri di divisibilità stabiliti prima.

Nella numerazione decimale accade che sia 41 sia 271 hanno lo stesso periodo k=5, di conseguenza applicheremo per entrambi lo stesso criterio di divisibilità .

Raggruppate le cifre di z a cinque a cinque, iniziando da destra, sommiamo le classi ottenute.

$$z \equiv 40097+99873+91671+82021+90+70021+5112 \equiv 388885 \equiv$$
$$\equiv 88885+3 \equiv 88888 \pmod{41}, \pmod{271}$$

Poiché il risultato finale è un intero con cinque cifre uguali ne consegue che z è sicuramente divisibile sia per 41 sia per 271.

Potete trovare una valida motivazione di quest'ultima asserzione nel mio libro

"Wn - Un ordinamento possibile dei numeri primi"