Stage Urbi et Orbi

Lezione del 21 nov. 2018

Congruenze ++

Università di Roma Tor Vergata

(Giambattista Marini)

Prerequisiti

Assumiamo la conoscenza degli argomenti trattati nelle lezioni precedenti. In particolare, assumiamo

1. un minimo di dimestichezza con le potenze di un binomio;
2. la capacità di risolvere equazioni lineari (e sistemi lineari) di equazioni diofantee.

(Comuqnue, all'occorrenza richiameremo brevemente i risultati utilizzati).

Convenzione

Lavoriamo con numeri interi (cioè con i numeri "**..., -3, -2, -1, 0, 1, 2, 3, 4, 5 ...**"). Questo significa che

scrivendo "consideriamo n" intendiamo "consideriamo un numero intero n";

scrivendo "trovare le soluzioni di ..." intendiamo "trovare le soluzioni intere di ...";

eccetera.

|n| denota il modulo (valore assoluto) del numero **n**.

(si cancella un eventuale segno meno, esempi: $|-7| = 7$, $|-5| = 5$, $|14| = 14$, $|8| = 8$)

Iniziamo con un problema "provocatorio".

Problema 0

Determinare tutte le terne (x, m, z) che soddisfano l'equazione

(0.1)
$$6^{2018^{|z|}} + x \cdot (x+1) + 18m^{|z|} = m^3 - m^2 - 2x + 7^{2018^{|m|}}$$

Soluzione.

Non ce n'è nessuna! Infatti, i numeri sottolineati in blu sono sicuramente pari, quello sotolineato in rosso è sicuramente dispari

$$\underline{6^{2018^{|z|}}} + \underline{x \cdot (x+1)} + \underline{18m^{|z|}} = \underline{m^3 - m^2} - \underline{2x} + \underline{7^{2018^{|m|}}}$$

Per le regole sulle somme di numeri pari e/o dispari ("pari+pari = pari", "pari+dispari = dispari" eccetera), a sinistra abbiamo un numero pari, a destra abbiamo un numero dispari.

Di conseguenza, l'equazione (0.1) non ha soluzioni. ■

In questo caso siamo stato fortunati. Ora, come prima cosa ci domandiamo, cosa significa che un numero è pari, cosa significa che è dispari. La risposta la conosciamo:

"**pari**" significa "il resto della divisione per **2** vale **0**"

"**dispari**" significa "il resto della divisione per **2** vale **1**"

Analizziamo una delle regole che conosciamo, ad esempio la regola "dispari + dispari = pari"
Siano **m** e **n** due numeri dispari, cioè del tipo

m = 2 h + 1 **n = 2 k + 1**

Abbiamo $m + n = 2(h+k) + 1 + 1 = 2(h+k+1)$ (che è un multiplo di 2, ovvero è pari).

A questo punto ci domandiamo:

- il resto della divisione per un numero soddisfa proprietà analoghe?
- in che modo possiamo sfruttarle per risolvere problemi algebrici?

Problema 1

Risolvere l'equazione

(1.1)
$$3^n + 2 = m^2$$

(risolvere significa determinare tutte le coppie (m, n) che la soddisfano)

Soluzione.

Iniziamo con l'osservare che per **n < 0** a sinistra della (1.1) non abbiamo un numero intero, mentre per **n = 0** abbiamo (sempre a sinistra della 1.1) $3^n + 2 = 3$ che non è un quadrato. Di conseguenza non ci sono soluzioni con **n** negativo o nullo. Per questa ragione possiamo assumere, e assumiamo, **n > 0**.

Possiamo scrivere

$$m = 3h + c \quad , \qquad \text{con} \qquad c = 0, 1, 2$$

(cioè, dove c è uno dei tre valori indicati, che sono 0, 1 e 2).

Abbiamo,

$$\begin{aligned} m^2 &= (3h + c)^2 \\ &= 9h^2 + 6hc + c^2 \end{aligned}$$

e, di conseguenza, abbiamo tre possibilità:

$$\begin{aligned} m^2 &= 3 \cdot (3h^2 + 2hc) + 0 \quad , \quad se \ c = 0 ; \\ m^2 &= 3 \cdot (3h^2 + 2hc) + 1 \quad , \quad se \ c = 1 ; \\ m^2 &= 3 \cdot (3h^2 + 2hc) + 4 \\ &= 3 \cdot (3h^2 + 2hc + 1) + 1 \quad , \quad se \ c = 2 . \end{aligned}$$

Queste le possiamo riscrivere come segue:

(1.2)

$$\begin{aligned} m^2 &= 3 \cdot (??) + 0 \quad , \quad se \ c = 0 ; \\ m^2 &= 3 \cdot (??) + 1 \quad , \quad se \ c = 1, 2 . \end{aligned}$$

(il numero tra parentesi è irrilevante). Dalla (1.2) deduciamo che il resto della divisione

$$m^2 : 3$$

può valere solamente **0** oppure **1** .

D'altro canto 3^n è sicuramente un multiplo di **3** (per $n > 0$) ed il resto della divisione

$$3^n + 2 \ : \ 3$$

(3^n + 2 è l'espressione a sinistra della 1.1) vale sicuramente **2** .

Confrontando le informazioni trovate

$$\text{resto} (m^2 : 3) = 0, 1 \qquad\qquad \text{resto} (3^n + 2 : 3) = 2 \quad (\text{per } n > 0)$$

deduciamo che la (1.1) **NON** ha soluzioni (già sapevamo che non ha soluzioni con **n** negativo o nullo). ■

Definizione 2

Sia $n > 0$. Diremo che **a** è congruo a **b** modulo **n** se

$$a - b \text{ è un multiplo di } n$$

In questo caso scriveremo

$$a \equiv b \mod n$$

Esempi 3

$31 \equiv 19 \mod 4$ infatti $31 - 19 = 12 = 3 \times 4$
$31 \equiv 19 \mod 3$ infatti $31 - 19 = 12 = 4 \times 3$
$27 \equiv 592 \mod 5$ infatti $27 - 592 = -565 = (-113) \times 5$
$31 \equiv 10 \mod 7$ infatti $31 - 10 = 21 = 3 \times 7$

(osserviamo che il multiplo può anche essere negativo, come nel caso del terzo esempio)

Osservazione 4

$$a \equiv b \mod n$$

se solo se

$$\text{resto} (a : n) = \text{resto} (b : n)$$

(cioè le due divisioni **a : n** e **b : n** hanno lo stesso resto).

Nota 5 Sia $n > 0$.

$$\text{resto}(a : n) = r$$

significa che possiamo scrivere

$$a = h\,n + r, \quad 0 \le r \le n-1 \qquad \text{(cioè con } r \text{ compreso tra } 0 \text{ e } n-1\text{)}$$

(Non abbiamo fatto ipotesi sul numero a. Per convenzione, quanto detto sopra si applica anche se a è negativo, ad esempio

$$\text{resto}(-12 : 5) = 3,$$

infatti $-12 = -3 \times 5 + 3$)

Dimostrazione (dell'osservazione 4)

Sia

$$\text{resto}(a : n) = r, \qquad \text{scriviamo} \qquad a = h\,n + r, \quad 0 \le r \le n-1$$

e sia

$$\text{resto}(b : n) = s, \qquad \text{scriviamo} \qquad b = k\,n + s, \quad 0 \le s \le n-1$$

Sottraendo la seconda equazione alla prima troviamo

$$\begin{array}{l} a = h\,n + r \\ b = k\,n + s \\ \hline a - b = (h-k)\,n + r - s \end{array} \qquad \text{dove } |r - s| \le n-1$$

(r ed s sono due numeri compresi tra 0 ed n-1, il modulo della loro differenza non può certo eccedere n-1)

Ne segue che

	$a - b$	è un multiplo di n
se e solo se	$(h-k)\,n + r - s$	è un multiplo di n
se e solo se	$r - s$	è un multiplo di n.

Poiché $|r - s| \le n-1$, l'ultima condizione equivale alla condizione $r - s = 0$, cioè alla condizionee $r = s$. ■

Torniamo al Problema 1. Nelle notazioni appena introdotte, la soluzione diventa

Soluzione # 2 (sempre del Problema 1).

$3^n + 2 \equiv 2 \mod 3$ (per $n > 0$)

$m^2 \equiv 0, 1 \mod 3$ (questo perché $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 1$ modulo 3)

Ne segue che l'equazione data non ha soluzioni. ■

Tutti i calcoli che avevamo fatto nella prima soluzione del problema sono spariti!

Naturalmente le due righe evidenziate vanno giustificate, le giustificheremo tra poco (si veda l'osservazione 14). Prima vediamo qualche problema dove non si vogliono fare, o non è conveniente fare, i conti espliciti.

Problema 6

Calcolare il resto della divisione

(6.1) $2^{2018} : 7$

Soluzione.

Scriviamo

$$\begin{aligned} 2^{2018} &= 2^{2 + 3 \times 672} \\ &= 4 \times 8^{672} \\ &= 4 \times (1+7)^{672} \\ &\equiv 4 \times 1^{672} \mod 7 \\ &= 4 \end{aligned}$$

Quindi il resto della divisione (6.1) è 4. ■

Problema 7

Calcolare il resto della divisione

(7.1) $7135841 : 9$

Soluzione.

Riscriviamo il numero dato nella forma

$$7 \times 10^6 + 2 \times 10^5 + 3 \times 10^4 + 5 \times 10^3 + 8 \times 10^2 + 4 \times 10 + 1$$

$$= (9+1)^6 \quad = (9+1)^5 \quad = (9+1)^4 \quad = (9+1)^3 \quad = (9+1)^2 \quad = (9+1)$$

$$\equiv 1^6 = 1 \quad \equiv 1^5 = 1 \quad \equiv 1^4 = 1 \quad \equiv 1^3 = 1 \quad \equiv 1^2 = 1 \quad \equiv 1$$

(10 e tutte le sue potenze sono congrue a 1 modulo 9)

Da questa espressione otteniamo

$$7\,1\,3\,5\,8\,4\,1 \equiv 7+1+3+5+8+4+1 \quad \text{mod. } 9$$

$$= 29 = 3 \times 9 + 2 \equiv 2 \quad \text{mod. } 9$$

Quindi il resto della divisione (7.1) è **2** .

Osservazione 8

Essendo **9** un multiplo di **3** , si ha anche $10 \equiv 1$ mod. **3** ed il conto fatto sopra ci dice anche che risulta

$$7\,1\,3\,5\,8\,4\,1 \equiv 2 \quad \text{mod. } 3$$

L'osservazione precedente vale in generale:

Osservazione 9 Sia $n > 0$.

Se

$$n = h \times k \quad , \qquad a \equiv b \quad \text{mod. } n$$

allora valgono anche le congruenze

$$a \equiv b \quad \text{mod. } h$$
$$a \equiv b \quad \text{mod. } k$$

Esempio 10

$$307 \equiv 7 \quad \text{mod. } 15$$ infatti $307 - 7 = 300 = 20 \times 15$

scrivendo $15 = 3 \times 5$ il conto qui sopra ci dice anche che

$$307 \equiv 7 \quad \text{mod. } 3$$ infatti $307 - 7 = 300 = (20 \times 5) \times 3$
$$307 \equiv 7 \quad \text{mod. } 5$$ infatti $307 - 7 = 300 = (20 \times 3) \times 5$

Problema 11

Calcolare il resto della divisione

(11.1) $7\,1\,3\,5\,8\,4\,1 \ : \ 11$

Soluzione.

Riscriviamo il numero dato nella forma

$$7 \times 10^6 + 2 \times 10^5 + 3 \times 10^4 + 5 \times 10^3 + 8 \times 10^2 + 4 \times 10 + 1$$

$$= (11-1)^6 \quad = (11-1)^5 \quad = (11-1)^4 \quad = (11-1)^3 \quad = (11-1)^2 \quad = (11-1)$$

$$\equiv (-1)^6 = 1 \quad \equiv (-1)^5 = -1 \quad \equiv (-1)^4 = 1 \quad \equiv (-1)^3 = -1 \quad \equiv (-1)^2 = 1 \quad \equiv -1$$

($10 \equiv -1$ modulo 11 , le sue potenze dispari continuano ad essere congrue a -1 , quelle pari sono congrue ad **1**, modulo **11**)

Da questa espressione otteniamo

$$7\,1\,3\,5\,8\,4\,1 \equiv 7-1+3-5+8-4+1 \quad \text{mod. } 11$$

(si osservi che qui a destra della congruenza abbiamo la somma alternata delle cifre del numero dato)

$$= 9$$

Quindi il resto della divisione (11.1) è **9** .

Enunciamo i risultati che giustificano i vari passaggi fatti (da quelli della soluzione # 2 del Problema 1 in poi).

Teorema 12 Sia $n > 0$.

Se

$$a_1 \equiv b_1 \mod n \quad \text{e} \quad a_2 \equiv b_2 \mod n$$

allora

- $a_1 + a_2 \equiv b_1 + b_2 \mod n$
- $a_1 \times a_2 \equiv b_1 \times b_2 \mod n$

Corollario 13 Sia $n > 0$.

Se

$$a \equiv b \mod n$$

allora

$$a^k \equiv b^k \mod n \quad \text{(per ogni intero positivo k)}$$

Osservazione 14

Scrivendo, ad esempio, le congruenze

$$3^n + 2 \equiv 2 \mod 3 \quad \text{(soluzione \# 2 del Problema 1)}$$

$$4 \times (1+7)^{672} \equiv 4 \times 1^{672} \mod 7 \quad \text{(soluzione del Problema 6)}$$

$$\ldots + 3 \times 10^4 + \ldots \equiv \ldots + 3 \times 1^4 + \ldots \mod 9 \quad \text{(soluzione del Problema 7)}$$

(sfruttando il fatto che $10 \equiv 1 \mod 9$)

utilizziamo il fatto che in un'espressione dove compaiono somme e prodotti (e potenze), possiamo sostituire un qualsiasi numero che vi compare con un numero ad esso congruo (Teorema 12 e Corollario 13).

Lo stesso discorso vale quando scriviamo

$m^2 \equiv 0, 1 \mod 3$ (questo perché $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 1$ modulo 3) (soluzione # 2 del Problema 1)

infatti, $m^2 \equiv 0, 1, 2$ (uno di questi tre valori) implica $m^2 \equiv 0^2, 1^2, 2^2$, (uno di questi tre valori, ...che essendo 0, 1, 4 si riducono, modulo 3, ai due valori 0 e 1) sempre tutto modulo 3

Voglio sottolineare che questa osservazione giustifica tutti i passaggi fatti (per esercizio, discutere anche quelli non menzionati esplicitamente come, ad esempio, quelli della soluzione del Problema 11).

Dimostrazione (del Teorema 12 e del Corollario 13)

- Viste le ipotesi, possiamo scrivere

$$a_1 - b_1 = k \times n \quad \text{e} \quad a_2 - b_2 = h \times n$$

sommando queste due equazioni troviamo

$$\begin{array}{l} a_1 - b_1 = k \times n \\ a_2 - b_2 = h \times n \\ \hline (a_1 + a_2) - (b_1 + b_2) = (k + h) \times n \end{array}$$

quindi otteniamo

$$a_1 + a_2 \equiv b_1 + b_2 \mod n$$

- Riscrivendo le nostre equazioni nella forma che segue e moltiplicandole abbiamo

$$\begin{array}{l} a_1 = b_1 + k \times n \\ a_2 = b_2 + h \times n \\ \hline a_1 \times a_2 = b_1 \times b_2 + (b_1 \times h + b_2 \times k + k \times h \times n) \times n \end{array}$$

quindi otteniamo

$$a_1 \times a_2 \equiv b_1 \times b_2 \mod n$$

- Il Corollario 13 si ottiene iterando il (o, se preferite, per ragioni induttive dal) Teorema:

$a \equiv b \mod n$ quindi $a^2 \equiv b^2 \mod n$ (si usi il Teorema con $a_1 = a_2 = a$, $b_1 = b_2 = b$) quindi $a^3 \equiv b^3 \mod n$ (si usi il Teorema con $a_1 = a^2$, $a_2 = a$, $b_1 = b^2$, $b_2 = b$)

eccetera!

Osservazione 15

Il numero scelto nel Problema 7 (ovvero nel Problema 11) non ha nulla di speciale, gli stessi identici conti ci danno un criterio per stabilire qual è il resto della divisione per **9** (ovvero per **11**) di un numero arbitrario **m**:

$$m \equiv \text{"somma delle cifre di } m\text{"} \quad \text{mod. } 9$$
$$m \equiv \text{"somma alterna delle cifre di } m\text{"} \quad \text{mod. } 11$$

(dove "somma alterna" significa "si prende la cifra delle unità, si sottrae quella decine, si somma quella delle centinaia, si sottrae quella delle migliaia eccetera")

Naturalmente, vista l'osservazione 8 (o meglio, la 9) abbiamo anche

$$m \equiv \text{"somma delle cifre di } m\text{"} \quad \text{mod. } 3$$

Sono convinto che in molti sanno che un numero è divisibile per 3 se e solo se lo è la somma delle sue cifre, ma credo che in pochi abbiano mai riflettuto sul fatto che dividendo per 3 un numero e dividendo per 3 la somma delle sue cifre si ottiene lo stesso identico resto.

Esercizio 16

Stabilire un criterio di divisibilità per **101**.

Suggerimento

Dato un numero, scriverlo come somma di potenze di **100**. Ad esempio, scriveremo il numero **7235841** nella forma

$$7\ 23\ 58\ 41 = 7 \times 100^3 + 23 \times 100^2 + 58 \times 100 + 41$$

Problema 17

Calcolare il resto della divisione

(17.1) $2\,7\,4\,5\,8\,2\,9\,3\,4 : 7$

Soluzione.

Riscriviamo il numero dato nella forma

$$2 \times 10^8 + 7 \times 10^7 + 4 \times 10^6 + 5 \times 10^5 + 8 \times 10^4 + 2 \times 10^3 + 9 \times 10^2 + 3 \times 10 + 4$$

$10^8 \equiv 2$ $10^7 \equiv 3$ $10^6 \equiv 1$ $10^5 \equiv 5$ $10^4 \equiv 4$ $10^3 \equiv 6$ $10^2 \equiv 2$ $10 \equiv 3$

Osserviamo che

$10^0 \equiv 1$ $= 1$ ←
$10^1 \equiv 3$ $= 3$
$10^2 = 10 \times 10 \equiv 3 \times 3 = 9 \equiv 2$ $= 2$
$10^3 = 10^2 \times 10 \equiv 2 \times 3 = 6$ $= 6$
$10^4 = 10^3 \times 10 \equiv 6 \times 3 = 18 \equiv 4$ $= 4$
$10^5 = 10^4 \times 10 \equiv 4 \times 3 = 12 \equiv 5$ $= 5$
$10^6 = 10^5 \times 10 \equiv 5 \times 3 = 15 \equiv 1$ $= 1$ ← Osserviamo che da questo punto in poi si ritrovano (ordinatamente) gli stessi numeri già trovati
$10^7 \equiv$ 3
$10^8 \equiv$ 2

Osserviamo che potremmo scrivere anche $10^6 = 10^2 \times 10^4 \equiv 2 \times 4 = 8 \equiv 1$,

....ma anche $10^6 = 10^3 \times 10^3 \equiv 6 \times 6 = 36 = 35 + 1 \equiv 1$,

...ovviamente ottenendo sempre lo stesso risultato!

A questo punto abbiamo

$$2\,7\,4\,5\,8\,2\,9\,3\,4 \equiv 2 \times 2 + 7 \times 3 + 4 \times 1 + 5 \times 5 + 8 \times 4 + 2 \times 6 + 9 \times 2 + 3 \times 3 + 4 \times 1$$

(in arancione, abbiamo i numeri calcolati sopra)

$$= 4 + 21 + 4 + 25 + 32 + 12 + 18 + 9 + 4 = 129 \equiv 3 \quad \text{mod. } 7$$

Quindi il resto della divisione (17.1) è **3**.

Nota 18

Dopo la lezione mi è stato chiesto se fosse possibile dimostrare il criterio che segue utilizzando le congruenze. Il criterio è questo:

Dato un numero **n** , si ha che

(18.1) **n** è divisibile per **7** **se e solo se** il numero ottenuto sottraendo il doppio della cifra delle unità al numero costituito dalle cifre rimenenti è divisibile per **7**

ad esempio, dato il numero **336** , scriviamo **33 - 2 x 6 = 33 - 12 = 21** che è divisibile per **7** , quindi lo è anche **336**

(l'ultima cifra è **6** , il numero "rimanente", cioè ottenuto cancellando il **6**, è **33**)

La risposta alla domanda posta naturalemente è **si** . Prima di dimostrare l'affermazione fatta osserviamo quanto segue:

il criterio ci dice che una volta scritto **n** nella forma **n = 10 a + u** (con **a** intero)

(si osservi che **u** è la cifra delle unità di **n** ed **a** è il numero costituito dalle rimanenti cifre)

si ha che

(18.2) $n \equiv 0 \mod 7$ **se e solo se** $a - 2u \equiv 0 \mod 7$

Dimostrazione (della (18.2), che come già osservato è la traduzione in formule della (18.1))

Premessa: $a - 2u \equiv 0 \mod 7$ **se e solo se** $10 \times (a - 2u) \equiv 0 \mod 7$

(questo perché 10 non contiene il fattore 7)

Risulta

$$10 \times (a - 2u) = 10a + u - 21u = n - 21u \equiv n \mod 7$$

cioè

$$10 \times (a - 2u) \equiv n \mod 7$$

Vista la premessa ciò conclude la dimostrazione. ■

C'è un commento che voglio fare. L'affermazione (18.1) è decisamente inutile (e l'archivierei come curiosità e non come criterio). Questo per due motivi:

- ci dice se un numero è divisibile per **7** ma **non** ci dice qual è il resto della sua divisione per **7**
  (questo perché "moltiplicando un numero per 10 il resto della divisione per 7 cambia", cfr. premessa);
- con numeri di tre cifre tutto sommato funziona, però, se ad esempio si parte da un generico numero di 20 cifre, la (18.1) riconduce la sua divibilità per **7** alla divisibilità per **7** di un numero di 19 cifre, questo significa che per avere la risposta finale dovremo applicare la (18.1) moltissime volte ...si fa decisamente prima a fare la divisione!

Col problema che segue introduciamo come l'osservazione 9 si inverte e come utilizzare tale "inversa".

Problema 19

Calcolare il resto della divisione

(19.1) $2^{2019} : 105$

Soluzione.

Fattorizziamo il numero **105** :

$$105 = 3 \times 5 \times 7$$

Quindi osserviamo che

$$2^{2019} = 2^{1 + 2 \times 1009} = 2 \times 4^{1009} = 2 \times (3+1)^{1009} \equiv 2 \times 1^{1009} = 2 \mod 3$$

$$2^{2019} = 2^{1 + 2 \times 1009} = 2 \times 4^{1009} = 2 \times (5-1)^{1009} \equiv 2 \times (-1)^{1009} = -2 \equiv 3 \mod 5$$

$$2^{2019} = 2^{3 \times 673} = 8^{673} = (1+7)^{673} \equiv 1 \mod 7$$

Sia dunque **r** il resto della divisione (19.1) , cioè la soluzione dell'equazione

(19.2) $2^{2019} \equiv r \mod 105$

soddisfacente l'ulteriore condizione

(♠) $0 \leq r \leq 104$

Alla alla luce dell'osservazione (9), quanto visto sopra ci dice che

$$(19.3)\qquad \begin{cases} r \equiv 2 \mod 3 \\ r \equiv 3 \mod 5 \\ r \equiv 1 \mod 7 \end{cases}$$

Risolvendo quest'ultimo sistema di equazioni (si tratta del classico sistema lineare diofanteo che avete imparato a risolvere nella lezione precedente) troviamo

$r = \ldots, 8, 113, 218, 323, \ldots$

Tra tutte queste soluzione scegliamo la soluzione $r = 8$ (evidenziata in verde), che è la soluzione soddisfacente la condizione (♠)

(cioè compresa tra 0 e 104).

In definitiva, il resto della divisione (19.1) è 8.

Come dicevamo, il valore r soddisfacente sia la (19.2) che (♠) soddisfa anche la (19.3), poiché quest'ultima ha una sola soluzione nell'intervallo da 0 a 104, questa deve necessariamente essere la soluzione cercata. Sembrerebbe che siamo stati fortunati (a priori la (19.3) è solamente una coseguenza della (19.2) e avrebbe potuto avere più soluzioni nell'intervallo (♠)), non è stata solamente fortuna:

Il teorema che segue ci dice che l'equazione (19.2) ed il sistema (19.3) sono equivalenti. Ciò giustifica la strategia adottata.

Teorema 20 (Cinese del resto)

Siano $n_1, \ldots, n_k$ interi strettamente positivi **a due a due coprimi**. Sia inoltre $n = n_1 \times \ldots \times n_k$ (il prodotto degli n_i).

Fissati dei numeri $b_1, \ldots, b_k$, si ha che esiste un unico valore b, con $0 \le b \le n-1$, tale che il sistema lineare nell'incognita x

$$(20.1)\qquad \begin{cases} x \equiv b_1 \mod n_1 \\ \vdots \\ x \equiv b_k \mod n_k \end{cases}$$

è equivalente all'equazione

$$(20.2)\qquad x \equiv b \mod n$$

Vediamo subito un'altra applicazione del Teorema.

Problema 21

Un sindaco, volendo contare le persone presenti in piazza, chiedo loro di ...

...mettersi in fila per 7, si accorge che ne avanzano 5
...mettersi in fila per 11, si accorge che ne avanzano 8
...mettersi in fila per 13, si accorge che ne avanzano 7

Sapendo che la piazza **non** può contenere più di 1000 persone, stabilire quante sono.

Soluzione.

Sia x il numero delle persone presenti in piazza. Le condizioni poste si traducono nel sistema

$$(21.1)\qquad \begin{cases} x \equiv 5 \mod 7 \\ x \equiv 8 \mod 11 \\ x \equiv 7 \mod 13 \\ x \le 1000 \quad \text{(e, naturalmente, } x \text{ positivo)} \end{cases}$$

Osserviamo che il prodotto degli n_i è il numero $n = 7 \times 11 \times 13 = 1001$.

Il Teorema ci dice che esiste **un unico** valore b, con $0 \le b \le 1000$ $(n-1 = 7 \times 11 \times 13 - 1 = 1000)$, tale che

$$(21.2)\qquad x \equiv b \mod 1001$$

(questo significa che il numero delle persone presenti in piazza **può** essere calcolato a partire dai dati a disposizione).

Per calcolare x si deve risolvere il sistema (21.1) (cosa che, trattandosi di un sistema diofanteo, sappiamo fare).

Per comodità del lettore svolgiamo esplicitamente il conto. Dalla prima equazione abbiamo che x è del tipo

$x = 7k + 5$ che, sostituito nella seconda equazione, ci dà $7k + 5 \equiv 8 \mod 11$

ovvero $k \equiv 2 \mod 11$ (il calcolo lo lasciamo per esercizio)

cioè k del tipo $k = 11h + 2$ (quindi x del tipo $7 \times (11h + 2) + 5$) che, sostituito nella terza equazione, ci dà

$7 \times (11h + 2) + 5 \equiv 7 \mod 13$ ovvero $h \equiv -1 \mod 13$ (il calcolo lo lasciamo per esercizio)

Posto $h = -1$ troviamo $x = -58$ (sostituiamo $h = -1$ nell'equazione $x = 7 \times (11h + 2) + 5$)

$x = -58$ è **una** soluzione della (21.2), la soluzione generica è del tipo $1001 \times m - 58$

e, per $m = 1$ si trova nell'intervallo desiderato (l'intervallo che va da 0 a 1000).

In definitiva, $x = 1001 - 58 = 943$

Dimostrazione (del Teorema 20 "Cinese del resto")

***Passo* 1** Trattiamo il caso dove le equazioni sono 2. Cioè un sistema del tipo

$$(\heartsuit) \qquad \begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

Osserviamo che a meno di sommare ad a un multiplo opportuno di n e sommare a b un multiplo di m possiamo assumere

$$0 \le a \le n-1 \qquad 0 \le b \le m-1$$

A questo punto "risolviamo" il sistema come se fosse un sistema esplicito, cioè scriviamo

$$(\spadesuit) \qquad x = k\,n + a \quad \text{ed} \quad x = h\,m + b$$

Dal confronto di queste due equazioni troviamo

$$k\,n + a = h\,m + b$$

ovvero

$$k\,n + h'\,m = b - a \qquad (\text{essendo } h' = -h)$$

Essendo n ed m coprimi (per ipotesi), questa equazione **può** essere risolta (qui usiamo ciò che sappiamo sulle equazioni diofantee), il che sostituendo in $(\spadesuit)$ ci dà **una** soluzione del sistema di partenza $(\heartsuit)$.

***Passo* 2** Modifichiamo la soluzione trovata in modo che sia nel range desiderato (cioè tra 0 e $n \times m - 1$).

A meno di sommare ad x un multiplo di $m \times n$ (cosa che non inficia la validità delle equazioni $(\heartsuit)$) possiamo assumere

$$0 \le x \le n \times m - 1$$

***Passo* 3** Proviamo che nel range tra 0 e $n \times m - 1$ non ci sono altre soluzioni.

Se x_1 e x_2 fossero due soluzioni (distinte) nel range desiderato, cioè soddisfacenti

$$0 \le x_1 \le n \times m - 1 \qquad 0 \le x_2 \le n \times m - 1$$

si avrebbe anche

$$x_1 \equiv a \pmod{n}, \quad x_2 \equiv a \pmod{n} \quad \text{quindi} \quad x_1 - x_2 \equiv 0 \pmod{n}$$
$$x_1 \equiv b \pmod{m}, \quad x_2 \equiv b \pmod{m} \quad \text{quindi} \quad x_1 - x_2 \equiv 0 \pmod{m}$$

con $0 \le |x_1 - x_2| \le n \times m - 1$.

Questo è impossibile perché $|x_1 - x_2|$ è un multiplo sia di n che di m (che sono coprimi tra loro).

***Passo* 4** Ci si riconduce al caso dove le equazioni sono solamente 2.

Sapendo trattare il caso dove le equazioni sono **2**, partendo da un sistema di k equazioni ($k \ge 3$), possiamo ridurlo ad un sistema di $k-1$ equazioni (sostituiamo le prime due equazioni con una sola equazione). Quindi lo riduciamo ad un sistema di $k-2$ equazioni, eccetera (o, se preferite, concludiamo per ragioni induttive).

...i dettagli di quest'ultimo passo li lasciamo per esercizio! ■

Introduciamo un altro risultato molto utile.

Problema 22

Calcolare il resto della divisione

(22.1) $$3^{1804} : 601$$

Soluzione.

Il fenomeno osservato nella soluzione del **Proplema 17**, dove le potenze di **10**, modulo **7**, si ripetevano, vale anche per le potenze **3**, modulo **601**. Il problema è capire quand'è che iniziano a ripetersi. Nel nostro caso, essendo **601** un numero primo, il teorema di Fermat enunciato sotto (Teorema 24) ci dice quanto segue:

(22.2) $$3^{600} \equiv 1 \pmod{601}$$

A questo punto la strada per risolvere il nostro problema è in discesa, si ha:

$$3^{1804} = 3^{3\times600+4} = 3^{600} \times 3^{600} \times 3^{600} \times 3^4$$
$$\equiv 3^4 = 81 \pmod{601}$$

■

Esempio 23

Scriviamo le potenze di **3** modulo **7**:

	3^0	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	3^{13}	
≡	1	3	2	6	4	5	1	3	2	6	4	5	1	3	mod. 7

Attenzione! Anche le potenze di **2** modulo **20** a un certo punto si ripetono, ma **1** non lo ritroviamo mai:

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	
≡	1	2	4	8	16	12	4	8	16	12	4	8	16	12	mod. 20

Il fenomeno di cui sopra è immediato (o meglio segue dalle proprietà delle congruenze): scrivendo in sequenza le potenze di un numero facciamo sempre la stessa operazione (ogni volta moltiplichiamo per quel numero) e, una volta che ritroviamo un numero già incontrato... (lasciamo le dovute riflessioni per esercizio).

Il teorema che segue ci dice che, se p è primo, allora dopo $p-1$ passi ritroviamo $a^0 = 1$

Teorema 24 (di Fermat)

Sia **a** un numero e **p** un numero primo. Assumendo che **a** **non** sia un multiplo di **p** si ha

(24.1) $$a^{p-1} \equiv 1 \mod p$$

Avvertenza. Non si esclude la possibilità di ritrovare **1** (anche) prima. Ad esempio, scrivendo le potenze di **2** modulo **7** troviamo

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	
≡	1	2	4	1	2	4	1	2	4	1	2	4	1	2	mod. 7

Il Teorema ci dice che dopo **6** passi ritroviamo **1**, in realtà lo ritroviamo già dopo solo **3** passi. Vale la pena osservare quanto segue: visto che i numeri che troviamo "si ripetono", allora: se ritroviamo **1** dopo **q** passi (e non prima), lo ritroveremo "ogni **q** passi", cioè ogni volta che avremo effettuato un multiplo di **q** passi, d'altro canto, dovendolo ritrovare dopo **p-1** passi, si deve necessariamente avere che **q** è un divisore di **p-1**.
Nel caso dell'esempio, ritroviamo **1** dopo **3** passi, in accordo con l'osservazione abbiamo che **3** è un divisore di **6** (**= 7-1 = p-1**).

Dimostrazione (del Teorema di Fermat)

Passo 1 Scriviamo tutti i numeri da **1** a **p - 1**

$$1,\ 2,\ 3,\ 4,\ \ldots,\ p-1$$

ed osserviamo che moltiplicandoli per **a** si ottengono, modulo **p**, di nuovo gli stessi numeri (in ordine differente), cioè risulta

(♠) $$\{1,\ 2,\ 3,\ 4,\ \ldots,\ p-1\} = \{a,\ 2a,\ 3a,\ 4a,\ \ldots,\ (p-1)a\} \quad \text{(mod. p)}$$

(ricordiamo che, per ipotesi, il numero **a** non è un multiplo di **p**)

Per dimostrare (♠), ragioniamo come segue:

i) se **x** ed **y** sono due numeri differenti dell'insieme a sinistra, moltiplicati per **a** restano differenti (anche modulo **p**);
(questo perché, per ipotesi, il numero a non è un multiplo di p)

ii) per quanto osservato al punto i), a destra della formula (♠) abbiamo p-1 "classi di resto modulo **p**" differenti e non nulle,
(quanto alla nozione di "classe di resto", si pensi ai possibili resti della divisone per p, che sono i numeri tra 0 e p-1)
ovvero abbiamo esattamente, come nell'insieme a sinistra, tutte le classi di resto modulo **p** non nulle.

Passo 2 In (♠), a destra e sinistra abbiamo, modulo **p**, gli stessi numeri (sebbene, lo ripetiamo, in ordine differente), in particolare il prodotto π dei numeri a sinistra deve essere uguale, modulo p, al prodotto dei numeri a destra (che, come si evince raccogliendo a fattore tutte le **a**, è uguale a $a^{p-1} \times \pi$)

cioè si deve avere

(24.2) $$\pi \equiv a^{p-1} \times \pi \mod p$$

Passo 3 Poiché π non è un multiplo di **p** (essendo **p** primo e π il prodotto dei numeri che precedono **p**), esiste **y** tale che

$$\pi \times y \equiv 1 \mod p$$

(in questo senso **y** è "l'inverso di π mod. **p**").

Nota: questo risultato segue di nuovo da (♠): tra i numeri $\{\pi, 2\pi, 3\pi, \ldots, (p-1)\pi\}$ ci deve essere 1.

Passo 4 Moltiplicando la (24.2) a destra e sinistra per **y** si ottiene

$$\pi \times y \equiv a^{p-1} \times \pi \times y \mod p$$

ovvero, sostiutendo $\pi \times y$ con **1** (passo 3), abbiamo

$$1 \equiv a^{p-1} \mod p$$

Definizione 25

Dato un numero **n** (che assumiamo maggiore o uguale a **2**), si definisce la Funzione di Eulero $\varphi(n)$ ponendo

$$\varphi(n) := \text{"numero dei coprimi con } n \text{ compresi tra } 1 \text{ e } n-1\text{"}$$

(ricordiamo che due numeri si dicono coprimi quando non hanno fattori in comune).

Esempio 26

$\varphi(12) = 4$ (i coprimi con 12 sono 1, 5, 7, 11)

$\varphi(28) = 12$ (i coprimi con 28 sono 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27)

Proposizione 27

La funzione di Eulero soddifa le proprietà che seguono:

i) se p è primo risulta $\varphi(p) = p - 1$

ii) se $n = p^k$ è la potenza di un primo risulta $\varphi(n) = p^k - p^{k-1}$ $\left(\text{che è uguale a } p^{k-1} \times (p-1)\right)$

iii) se n ed m sono coprimi risulta $\varphi(n \times m) = \varphi(n) \times \varphi(m)$

Dimostrazione (cenno)

La i) è immediata: tutti i numeri compresi tra 1 e $p - 1$ sono coprimi con p.

La ii) segue dal fatto che se scriviamo i numeri compresi tra 1 e p^k in gruppi di p numeri coprimi con p, cioè scriviamo

1, ... p-1, p, p+1, ... 2p-1, 2p 2p+1, ... 3p-1, 3p 3p+1, ... 4p-1, 4p . . . ..., p^k,

abbiamo p^{k-1} insiemi in ognuno dei quali ci sono $p - 1$ coprimi con p, ovvero con p^k (essere coprimo con p^k equivale a essere coprimo con p).

La iii) segue dal fatto che se si scrivono ordinatamente i numeri compresi tra 1 ed $n \times m$ in una tabella di n righe e m colonne, quindi si cancellano i numeri che **non** sono coprimi con $n \times m$, ci si accorge che restano esattamente $\varphi(m)$ colonne e che, in ciascuna di queste restano esattamente $\varphi(n)$ numeri (suggeriamo di scrivere gli esempi $60 = 12 \times 5$, $120 = 8 \times 15$, $120 = 15 \times 8$).

Esempio 28

Si ha $\varphi(10000) = \varphi(2^4 \times 5^4) = \varphi(2^4) \times \varphi(5^4) = (2^4 - 2^3) \times (5^4 - 5^3) = (16 - 8) \times (625 - 125) = 8 \times 500 = 4'000$

(usiamo la iii) (usiamo la ii))

La iii) si generalizza al prodotto di più di due termini (sempre coprimi tra loro), basta iterarla, ad esempio:

$$\varphi(540'000) = \varphi(2^5 \times 3^3 \times 5^4) = \left(\varphi(2^5 \times 3^3)\right) \times \varphi(5^4) = \varphi(2^5) \times \varphi(3^3) \times \varphi(5^4)$$

$$= (64 - 32) \times (27 - 9) \times (625 - 125) = 32 \times 18 \times 500 = 288'000$$

Nota 29

L'esempio non ha nulla di speciale:

siamo in grado di calcolare il valore della funzione di Eulero di ogni numero

(basterà decomporlo, quindi usare le regole ii) e iii) della Proposizione 27).

Problema 30

Determinare le ultime quattro cifre del numero

(30.1) $$37^{10^{2019}}$$

Soluzione.

Trovare le ultime quattro cifre di un numero n equivale a trovare il resto della divisione di n per $10'000$.

Purtroppo $10'000$ non è un numero primo e non possiamo applicare il teorema di Fermat. In compenso possiamo applicare il teorema di Eulero enunciato sotto (Teorema 31). Si deve avere (cfr. Esempio 28):

$$37^{4'000} \equiv 1 \quad \text{mod. } 10'000$$

A questo punto siamo in grado di concludere rapidamente: 10^{2019} è sicuramente un multiplo di $4'000$ (10^{2019} contiene i fattori 2 e 5 migliaia di volte, e a noi basta che sia un multiplo di $4'000 = 2^5 \times 5^3$).

Di conseguenza, posto $10^{2019} = m \times 4000$ possiamo scrivere:

$$37^{10^{2019}} = 37^{4'000 \times m} = \left(37^{4'000}\right)^m \equiv 1 \quad \text{mod. } 10'000$$

Teorema 31 (di Eulero)

Siano a ed n coprimi (cioè, senza fattori in comune). Si ha

(31.1) $$a^{\varphi(n)} \equiv 1 \quad \text{mod. } n$$

dove $\varphi(n)$ denota la funzione di Eulero (cfr. Definizione 25).

Questo Teorema non lo dimostreremo.

Nota 32

Per $n = p$ primo, l'ipotesi che n ed a siano coprimi si traduce nell'ipotesi che a non sia un multiplo di p, risulta $\varphi(p) = p - 1$. Queste considerazioni ci dicono che

il teorema di Eulero generalizza il teorema di Fermat

(il teorema di Fermat si ottiene da quello di Eulero per $n = p$ primo).