Aritmetica, Tutorato 2

DV 2.64 Per ogni primo p esiste $n \in \mathbb{N}$ t.c.

$$6n^2+5n+1 \equiv 0 \pmod p.$$

dim. Riscriviamo la congruenza come

$$(3n+1)(2n+1) \equiv 0 \pmod p.$$

Pertanto, è sufficiente trovare $n \in \mathbb{N}$ che risolva una tra le due congruenze

(i) $3n+1 \equiv 0 \ (p) \rightsquigarrow 3n \equiv -1 \ (p)$,

(ii) $2n+1 \equiv 0 \ (p) \rightsquigarrow 2n \equiv -1 \ (p)$.

Se $p=2$, la (i) ha soluzione, perché $3 \equiv 1$ è invertibile $\pmod 2$ (equiv., $(3,p)=1$ se $p=2$); se $p=3$, la (ii) ha soluzione per lo stesso motivo e, se $p \neq 2,3$, entrambe (i) e (ii) hanno soluzione.

Notiamo che, a voler essere pedanti, questo garantisce l'esistenza di $n \in \mathbb{Z}$ con le proprietà volute ma, se $n \notin \mathbb{N}$, è sufficiente considerare $n-np$ per ottenere un numero naturale che risolve ancora la congruenza iniziale. $\square$

DN 3.7.10 Siano, per $n \in \mathbb{N}$,

$$F_n := 2^{2^n}+1$$

i numeri di Fermat. Mostrare che

(i) F_5 non è primo;

(ii) se $n \neq m$, $(F_n, F_m) = 1$;

(iii) esistono infiniti numeri primi distinti.

dim. (i) Mostro che $641 \mid F_5$. Scrivo

$$641 = 2^4+5^4$$
$$= 1+5 \cdot 2^7,$$

cioè

$$(1) \qquad 5^4 \equiv -2^4 \ (641),$$

$$(2) \qquad 5 \cdot 2^7 \equiv -1 \ (641).$$

Elevando alla quarta la (2) si ottiene

$$5^4 \cdot 2^{28} \equiv 1 \ (641)$$

e sostituendo 5^4 via la (1) si ha

$$-2^4 \cdot 2^{28} \equiv 1 \ (641),$$

cioè

$$2^{32} \equiv -1 \ (641)$$

$$\Longrightarrow \mathcal{F}_5 \equiv 0 \ (641).$$

(ii) Supponiamo wlog che $n > m$, per cui $2^n = 2^m \cdot 2^r$ con $r > 0$.

Se per assurdo $(\mathcal{F}_n, \mathcal{F}_m) \neq 1$, sia p un primo che divide entrambi $\mathcal{F}_n$ e $\mathcal{F}_m$: allora

$$(i) \quad 2^{2^n} + 1 \equiv 0 \ (p) \longrightarrow 2^{2^m \cdot 2^s} \equiv -1 \ (p)$$

$$(ii) \quad 2^{2^m} + 1 \equiv 0 \ (p) \longrightarrow 2^{2^m} \equiv -1 \ (p)$$

e sostituendo (ii) in (i) si ottiene

$$(-1)^{2^s} \equiv -1 \ (p)$$

cioè, poiché $s > 0$,

$$1 \equiv -1 \ (p) \Longrightarrow 2 \equiv 0 \ (p).$$

Pertanto, dev'essere $p = 2$, ma $2 \nmid \mathcal{F}_n, \mathcal{F}_m$ $\not\subset$.

(iii) Supponiamo che esistano solo finiti primi distinti, e sia $\mathbb{P}$ l'insieme dei primi.

Consideriamo un insieme $C = \{N_1, N_2, \dots\} \subset \mathbb{N}$ di numeri a due a due coprimi e tutti diversi da $0, \pm 1$. Allora, per ogni i, esiste $p_i \in \mathbb{P}$ tale che $p_i \mid N_i$: poiché $(N_i, N_j) = 1$ per ogni $j \neq i$, dev'essere $p_i \neq p_j$ per ogni $i \neq j$. Pertanto, la funzione $C \to \mathbb{P}$, $N_i \mapsto p_i$ è iniettiva, da cui segue che se $\mathbb{P}$ è finito anche C lo è.

D'altra parte, abbiamo costruito in (ii) un insieme infinito di numeri a due a due coprimi, ie $\{\mathcal{F}_n \mid n \in \mathbb{N}\}$, perciò P dev'essere infinito. $\square$

DN 3.7.11 (i) Risolvere l'eq. diofantea

$$40x + 252y = 44$$

(ii) Esistono sol (x,y) con $x \equiv 0 \ (7)$? Con $x \equiv 0 \ (13)$?

dim (i) Notiamo che l'equazione proposta è equivalente a

$$10x + 63y = 11.$$

Ricordo che una diofantea lineare $ax+by=c$ ha soluzione se e solo se $(a,b) \mid c$.

In questo caso, usando l'algoritmo di Euclide

$$(10,63) = (63,10) = (10,3)$$
$$= (3,1) = 1,$$

pertanto la diofantea ha soluzione.

Inoltre, l'algoritmo per la risoluzione di una diofantea lineare è

① trovare una soluzione particolare "srotolando" l'algoritmo di Euclide;

② risolvere l'equazione omogenea associata.

Vediamo ①:

$$63 = 6 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1$$
$$\Rightarrow \quad 1 = 10 - 3 \cdot 3$$
$$= 10 - 3(63 - 6 \cdot 10)$$
$$= 19 \cdot 10 - 3 \cdot 63,$$

da cui, moltiplicando per 11,

$$11 = 209 \cdot 10 - 33 \cdot 63,$$

cioè $(209, 33)$ è una sol. particolare.

Passiamo a ②:

$$10x + 63y = 0$$

$$\Leftrightarrow 10x = -63y$$

e, poiché $(10, 63) = 1$, dev'essere $10 \mid y$, cioè $y = 10k$, quindi

$$\cancel{10}x = -63 \cdot \cancel{10}k$$

$$\Rightarrow \begin{cases} x = -63k \\ y = 10k \end{cases}.$$

In conclusione, le soluzioni dell'equazione iniziale sono esattamente le coppie della forma $(209 - 63k, 33 + 10k)$ al variare di $k \in \mathbb{Z}$.

(ii) Se $x \equiv 0$ (7), dev'essere

$$209 - 63k \equiv 0 \ (7)$$

cioè, poiché $209 \equiv 6$ (7) e $63k \equiv 0$ (7) (per ogni k),

$$6 \equiv 0 \ (7) \ ⚡$$

quindi non esistono sol. di questa forma.

Analogamente,

$$x \equiv 0 \ (13)$$

$$\Leftrightarrow 209 - 63k \equiv 0 \ (13)$$

$$\Leftrightarrow 1 + 2k \equiv 0 \ (13)$$

$$\Leftrightarrow 2k \equiv -1 \ (13).$$

Poiché 2 è invertibile (mod 13), esistono soluzioni, e sono esattamente

$$k \equiv -7 \ (13)$$

poiché 7 è l'inverso molt. di 2 (mod 13). Quindi, $x = 209 - 63k$ è $\equiv 0 (13) \Leftrightarrow k \equiv -7 (13)$. $\square$

DN 3.7.12 Risolvere

$$341x \equiv 15 \quad (912).$$

dim. Notiamo che

$$(341, 912) = (912, 341) = (341, 230)$$

$$= (230, 111) = (111, 8) = 1,$$

quindi l'eqz. ha sol. La fatt in primi di 912 è

$$912 = 2^4 \cdot 3 \cdot 19,$$

e per il TCR l'eqz. è equ. al sistema

$$\begin{cases} 341x \equiv 15 \ (16) \\ 341x \equiv 15 \ (3) \\ 341x \equiv 15 \ (19) \end{cases}$$

che si semplifica in

$$\begin{cases} 5x \equiv -1 \ (16) \\ -x \equiv 0 \ (3) \\ -x \equiv 15 \ (19) \end{cases}$$

e, tenendo conto che 13 è l'inverso di 5 (mod 16), perché

$$13 \cdot 5 = 65 \equiv 1 \ (16),$$

in

$$\begin{cases} x \equiv 3 \ (16) & \leftarrow -13 \equiv 3 \\ x \equiv 0 \ (3) \\ x \equiv 4 \ (19) & \leftarrow -15 \equiv 4 \end{cases}$$

A questo punto

Modo 1

$$\begin{cases} x = 3 + 16k, \ k \in \mathbb{Z} \\ 3 + 16k \equiv 0 \ (3) \\ x \equiv 4 \ (19) \end{cases} \iff \begin{cases} \text{——} \\ k \equiv 0 \ (3) \iff k = 3h, h \in \mathbb{Z} \\ 3 + 16 \cdot 3h \equiv 4 \ (19) \end{cases}$$

$$\iff \begin{cases} \text{——} \\ \text{——} \\ 10h \equiv 1 \ (19) \iff h \equiv 2 \ (19) \iff h = 2 + 19\ell, \ \ell \in \mathbb{Z} \end{cases}$$

$\uparrow$ 2 è l'inv. di 10 (mod 19)

da cui

$$x = 3 + 16k$$
$$= 3 + 16 \cdot 3h$$
$$= 3 + 16 \cdot 3(2 + 19\ell)$$
$$= 3 + 96 + 912\ell$$

ie.

$$x \equiv 99 \ (912)$$

è la sol. del sistema.

Modo 2 Sappiamo che esiste un'unica sol. (mod 912): listiamo allora tutte le soluzioni della congruenza (mod 19) [perché 19 è > 3, 16 ⇒ meno numeri] minori di 912 finché troviamo quella giusta:

4 NO 23 NO 42 NO 61 NO 80 NO

99 SÌ ⇒ FINE :).

Modo 3 La soluzione di

$$\begin{cases} x \equiv 3 \ (16) \\ x \equiv 0 \ (3) \end{cases}$$

è unica (mod 48) e chiaramente 3 funziona, quindi il sistema iniziale equivale a

$$\begin{cases} x \equiv 3 \ (48) \\ x \equiv 4 \ (19) \end{cases}$$

Procedendo come in 2 listiamo le sol (mod 48):

3 NO 51 NO 99 SÌ ⇒ FINE (ma più veloce)
:))

□