Esercizi di Algebra

3 aprile 2006

1. Sia $n \geq 2$ un intero.

   (a) Trovare due interi $a \geq b > 0$ tali che siano richiesti 5 passi dell'algoritmo euclideo per stabilire che $\mathrm{MCD}(a, b) = n$.

   (b) * Trovare due interi x_n, y_n tali che siano richiesti n passi dell'algoritmo euclideo per stabilire che $\mathrm{MCD}(x_n, y_n) = 1$.

   Soluzione.

   (a) Deve risultare

   $$\begin{aligned} a &= b \times q_1 + r_1 \quad 0 < r_1 < b \\ b &= r_1 \times q_2 + r_2 \quad 0 < r_2 < r_1 \\ r_1 &= r_2 \times q_3 + r_3 \quad 0 < r_3 < r_2 \\ r_2 &= r_3 \times q_4 + \mathbf{n} \quad 0 < r_4 = n < r_3 \\ r_3 &= r_4 \times q_5 + 0. \end{aligned}$$

   Per esempio, potremo scegliere $q_5 = 2$, $q_4 = q_3 = q_2 = q_1 = 1$, e corrispondentemente ottenere $r_3 = 2n$, $r_2 = 3n$, $r_1 = 5n$, $b = 8n$, $a = 13n$.

   (b) Questa volta avremo

   $$\begin{aligned} x_n &= y_n \times q_1 + r_1 \quad 0 < r_1 < y_n \\ y_n &= r_1 \times q_2 + r_2 \quad 0 < r_2 < r_1 \\ r_1 &= r_2 \times q_3 + r_3 \quad 0 < r_3 < r_2 \\ &\vdots \quad\quad \vdots \\ r_{n-3} &= r_{n-2} \times q_{n-1} + \mathbf{1} \quad 0 < 1 < r_{n-2} \\ r_{n-2} &= 1 \times q_n + 0. \end{aligned}$$

   Se scegliamo $q_n = 2$, $q_{n-1} = \cdots = q_2 = q_1 = 1$ è semplice vedere che

ponendo $R_i = r_{n-i}$ $(1 \leq i \leq n-1)$, otteniamo

$$\begin{aligned} R_1 &= 1 \\ R_2 &= 2 \\ R_k &= R_{k-1} + R_{k-2} \quad 2 < k < n \\ y_n &= R_{n-1} + R_{n-2} \\ x_n &= y_n + R_{n-1}. \end{aligned}$$

In altri termini, possiamo prendere come y_n e x_n rispettivamente l'n–esimo e l'$n+1$–esimo numero di Fibonacci.

2. Un generale cinese aveva un esercito di 1000 uomini. Ci fu una battaglia e il generale condusse il suo esercito alla vittoria. Tornato all'accampamento, il generale sapeva di aver perso un numero assai esiguo di soldati e di questo si rallegrava; si chiedeva però anche se potesse rapidamente stabilire quanti fossero effettivamente i caduti. Il generale pensò allora di far disporre i sopravvissuti in riga prima per 5, poi per 7 e infine per 9; così facendo, riscontrò che nell'ultima riga restavano rispettivamente 2, 3 e 7 soldati, e fu quindi certo di aver perso solo 3 soldati. Come mai?

   Soluzione Si tratta di trovare una soluzione del sistema di equazioni congruenziali

$$\begin{cases} X \equiv 2 \bmod 5 \\ X \equiv 3 \bmod 7 \\ X \equiv 7 \bmod 9, \end{cases}$$

   che sia prossima a 1000.

   Dalla prima equazione abbiamo

$$X = 2 + 5t \quad (t \in \mathbb{Z})$$

   da cui, sostituendo nella seconda,

$$\begin{aligned} 2 + 5t &= 3 + 7n \quad (n \in \mathbb{Z}) \\ 5t &= 1 + 7n \\ 15t &= 3 + 21n \\ t &= 3 + 21n - 14t \\ t &= 3 + 7m \quad (m \in \mathbb{Z}). \end{aligned}$$

   Sarà quindi

$$X = 17 + 35m.$$

   Ora, la terza equazione ci dice

$$\begin{aligned} 17 + 35m &= 7 + 9k \quad (k \in \mathbb{Z}) \\ 36m - m &= -10 + 9k \\ m &= 1 + 9l \quad (l \in \mathbb{Z}). \end{aligned}$$

Dunque in conclusione deve essere

$$X = 52 + 315l.$$

Fra i numeri di tale forma, $997 = 52 + 315 \times 3$ è l'unico ragionevolmente vicino a 1000.

3. Determinare, se esistono, le soluzioni del sistema di equazioni congruenziali

$$\begin{cases} X \equiv 4 \bmod 10 \\ 2X \equiv 4 \bmod 12 \\ 5X \equiv 6 \bmod 14. \end{cases}$$

Soluzione. Le soluzioni della prima equazione sono del tipo

$$X = 4 + 10n.$$

La seconda implica allora,

$$\begin{aligned} 8 + 20n &= 4 + 12m \quad (m \in \mathbb{Z}) \\ 2 + 10n &= 6m \\ 2 + 4n &= 6(m - n) \\ 1 + 2n &= 3k \quad (k \in \mathbb{Z}) \\ 1 &= n - 3n + 3k \\ n &= 1 + 3t \quad (t \in \mathbb{Z}), \end{aligned}$$

e quindi

$$X = 14 + 30t.$$

L'ultima equazione fornisce allora

$$\begin{aligned} 70 + 150t &= 6 + 14l \quad (l \in \mathbb{Z}) \\ 10t &= 6 + 14h \quad (h \in \mathbb{Z}) \\ 5t &= 3 + 7h \\ 15t &= 9 + 21h \\ t &= 2 + 7 - 14t + 21h \\ t &= 2 + 7a \quad (a \in \mathbb{Z}), \end{aligned}$$

dunque in conclusione le soluzioni del sistema dato sono tutti e soli i numeri del tipo

$$X = 74 + 210a \quad (a \in \mathbb{Z}).$$

4. Studiare al variare del parametro $b \in \mathbb{Z}$ il sistema di equazioni congruenziali

$$\begin{cases} X \equiv 3b \bmod 22 \\ X \equiv 1 \bmod 10 \\ X \equiv b \bmod 18. \end{cases}$$

Soluzione. Partiamo questa volta dalla seconda equazione; deve essere

$$X = 1 + 10n \quad (n \in \mathbb{Z}).$$

Sostituendo nella prima equazione si ha

$$10n - 3b + 1 = 22m \quad (m \in \mathbb{Z}).$$

Osserviamo che perchè tale equazione ammetta delle soluzioni necessariamente b deve essere dispari. Sia dunque $b = 2\beta + 1$. Dividendo per due la precedente equazione otteniamo

$$\begin{aligned} 5n &\equiv 3\beta + 1 \bmod 11 \\ -10n &\equiv 6\beta - 2 \bmod 11 \\ n &\equiv -3b + 1 \bmod 11 \\ n &\equiv 8b + 1 \bmod 11. \end{aligned}$$

Le soluzioni delle prime due equazioni (se b è dispari) sono quindi della forma

$$X = 80b + 11 + 110n \quad (n \in \mathbb{Z}).$$

Sostituendo tale espressione nella terza congruenza otteniamo

$$\begin{aligned} 80b + 11 + 110n &\equiv b \bmod 18 \\ 79b + 11 + 2n &\equiv 0 \bmod 18 \\ 7(2\beta + 1) + 11 + 2n &\equiv 0 \bmod 18 \\ 14\beta + 2n &\equiv 0 \bmod 18 \\ 7\beta + n &\equiv 0 \bmod 9 \\ n &\equiv 2\beta \bmod 9 \\ n &\equiv b - 1 \bmod 9. \end{aligned}$$

In conclusione, se $b \equiv 1 \bmod 2$, le soluzioni del sistema dato sono

$$X = 190b - 99 + 990k \quad (k \in \mathbb{Z}).$$

Invece non ci sono soluzioni se b è pari.

5. Calcolare:
   (a) l'ultima cifra decimale di 321123^{123321};
   (b) le ultime due cifre decimali di 1234^{4321};
   (c) le ultime tre cifre decimali di 111^{111}.

   Soluzione.

(a) Bisogna trovare quale intero $0 \leq X \leq 9$ soddisfa la congruenza

$$X \equiv 321123^{123321} \bmod 10.$$

Osserviamo che

$$321123^{123321} \quad \equiv \quad 3^{123321} \bmod 10.$$

Sappiamo inoltre che $3^4 \equiv 1 \bmod 10$ (infatti $4 = \varphi(10)$). Quindi

$$3^{123321} \equiv 3^{123320} \cdot 3 \equiv (3^4)^{30830} \cdot 3 \equiv 3 \bmod 10.$$

Dunque

$$X = 3.$$

(b) Bisogna trovare quale intero $0 \leq Y \leq 99$ soddisfa la congruenza

$$Y \equiv 1234^{4321} \bmod 100.$$

Osserviamo che

$$1234^{4321} \quad \equiv \quad 34^{4321} \bmod 100.$$

Per il teorema cinese del resto, possiamo risolvere equivalentemente il sistema di congruenze

$$\begin{cases} Y \equiv 34^{4321} \bmod 4 \\ Y \equiv 34^{4321} \bmod 25. \end{cases}$$

Visto che $34 \equiv 2 \bmod 4$, $34 \equiv 9 \bmod 25$ e $\varphi(25) = 20$, avremo

$$\begin{cases} Y \equiv 2^{4321} \equiv 0 \bmod 4 \\ Y \equiv 9^{4321} \equiv (9^{20})^{216} \cdot 9 \equiv 9 \bmod 25. \end{cases}$$

Deve quindi essere

$$Y = 84.$$

(c) Bisogna trovare quale intero $0 \leq Z \leq 999$ soddisfa la congruenza

$$Z \equiv 111^{111} \bmod 1000.$$

Per il teorema cinese del resto, possiamo risolvere equivalentemente il sistema di congruenze

$$\begin{cases} Z \equiv 111^{111} \equiv (-1)^{111} \equiv -1 \bmod 8 \\ Z \equiv 111^{111} \equiv (-14)^{111} \bmod 125. \end{cases}$$

Ora, $\varphi(125) = 100$, quindi

$$(-14)^{111} \equiv (-14)^{11} \equiv -(14)^{11} \bmod 125.$$

Ora $14^{11} = 14 \cdot 14^2 \cdot ((14^2)^2)^2$, inoltre

$$\begin{aligned} 14^2 &\equiv 71 \bmod 125 \\ 71^2 &\equiv 41 \bmod 125 \\ 41^2 &\equiv 56 \bmod 125, \end{aligned}$$

quindi

$$(14)^{11} \equiv 14 \cdot 71 \cdot 56 \equiv 4 \cdot 14^2 \cdot 71 \equiv 4 \cdot 41 \equiv 39 \bmod 125.$$

e

$$\begin{cases} Z \equiv -1 \bmod 8 \\ Z \equiv 86 \bmod 125. \end{cases}$$

Sarà allora

$$Z = 711.$$

6. (a) Sia $b > 1$ un intero. Mostrare che per ogni coppia di interi $n, m \geq 0$

$$\mathrm{MCD}(b^m - 1, b^n - 1) = b^{\mathrm{MCD}(m,n)} - 1.$$

[Suggerimento: procedere per induzione sul massimo fra m ed n; osservare che se $n \geq m$ allora

$$(b^{n-m} - 1) = (b^n - 1) - b^{n-m}(b^m - 1)$$

e dedurre che

$$\mathrm{MCD}(b^m - 1, b^n - 1) = \mathrm{MCD}(b^m - 1, b^{n-m} - 1).]$$

(b) Dedurre che se un primo p divide $b^n - 1$ allora o divide $b^d - 1$ per qualche divisore proprio d di n oppure $p \equiv 1 \bmod n$ (e più in particolare, se n e p sono dispari $p \equiv 1 \bmod 2n$).

(c) Fattorizzare $2^{13} - 1$ e $3^{11} - 1$.

Soluzione.

(a) Procediamo per induzione sul massimo fra n ed m. Possiamo supporre che sia $n \geq m$ (scambiando n ed m se necessario). Se $n = 1$, non c'è nulla da dimostrare. Ora, per il passo induttivo, possiamo supporre che $n > m$ (infatti l'affermazione è banalmente vera se $n = m$). Come suggerito, vale l'uguaglianza

$$(b^{n-m} - 1) = (b^n - 1) - b^{n-m}(b^m - 1),$$

che implica da un lato che ogni divisore comune di $b^n - 1$ e $b^m - 1$ è anche un divisore di $b^{n-m} - 1$ e dall'altro che ogni divisoare comune di $b^{n-m} - 1$ e $b^m - 1$ è anche un divisore di $b^n - 1$. Questo in effetti prova che

$$\mathrm{MCD}(b^m - 1, b^n - 1) = \mathrm{MCD}(b^m - 1, b^{n-m} - 1).$$

Usando l'ipotesi induttiva abbiamo ora che

$$\mathrm{MCD}(b^m-1, b^n-1) = \mathrm{MCD}(b^m-1, b^{n-m}-1) = b^{\mathrm{MCD}(m,n-m)}-1.$$

Ma, come subito si verifica,

$$\mathrm{MCD}(m, n-m) = \mathrm{MCD}(m, n).$$

(b) Se $p|b^n-1$, per il piccolo teorema di Fermat vale anche

$$p|b^{p-1}-1.$$

Dunque

$$p|\mathrm{MCD}(b^n-1, b^{p-1}-1) = b^{\mathrm{MCD}(n,p-1)}-1.$$

Se $\mathrm{MCD}(n, p-1) < n$ allora in effetti $p|b^d-1$ con d divisore proprio di n; altrimenti sarà $\mathrm{MCD}(n, p-1) = n$, e quindi

$$p \equiv 1 \bmod n.$$

Infine, se p ed n sono dispari

$$\begin{cases} p \equiv 1 \bmod 2 \\ p \equiv 1 \bmod n \end{cases} \implies p \equiv 1 \bmod 2n.$$

(c) L'unico divisore proprio di 13 è 1 dunque, i primi che eventualmente dividano $2^{13}-1$ devono soddisfare

$$p \equiv 1 \bmod 26.$$

Inoltre, $\sqrt{2^{13}-1} = 90,504\ldots$; quindi se $2^{13}-1$ non è primo deve avere un fattore primo minore di 91. Ora, ci sono solo due numeri primi congrui ad 1 modulo 26 minori di 91: 53 e 89. Come subito si verifica nessuno dei due divide $2^{13}-1$. Pertanto $8191 = 2^{13}-1$ è un primo (di Mersenne).
Chiaramente $2 = 3^1-1$ divide $3^{11}-1$. Ragionando come sopra si vede che ogni fattore primo p di $88573 = \frac{3^{11}-1}{2}$ deve soddisfare

$$p \equiv 1 \bmod 22.$$

In effetti 23 divide 88573, e risulta

$$88573 = 23 \cdot 3851.$$

Osservando che $\sqrt{3851} = 62,056\ldots$, che 23 è l'unico primo minore di 63 congruo a 1 modulo 22, e verificando che 23 non divide 3851, deduciamo che la fattorizzazione richiesta è

$$3^{11}-1 = 2 \cdot 23 \cdot 3851.$$