ALGEBRA 1 PB-Z
V. 13 IV 2012

Esercizio 1. Detta $\varphi : \mathbb{N} \to \mathbb{N}$ la funzione di Eulero, si trovino i valori $\varphi(n)$ che essa asssume allorquando n appartiene a $\{37,\ 54,\ 111,\ 360\}$.

Soluzione. Ricordiamo che, dato $n \in \mathbb{N}$, il valore $\varphi(n)$ può esser calcolato a partire dalla decomposizione in fattori primi di n, secondo la formula seguente: se la fattorizzazione di n è $n = p_1^{h_1}...p_s^{h_s}$, allora

$$\varphi(n) = p_1^{(h_1-1)}...p_s^{(h_s-1)}(p_1 - 1)...(p_s - 1).$$

37.
Essendo 37 primo, si ha $\varphi(37) = 37^0(37 - 1)$; ossia, $\varphi(37) = 36$.

54.
Essendo $54 = 2 \cdot 3^3$, si ha $\varphi(54) = \varphi(2 \cdot 3^3) = 2^0 3^2(2 - 1)(3 - 1)$; ossia $\varphi(54) = 18$.

111.
Essendo $111 = 3 \cdot 37$, si ha $\varphi(111) = \varphi(3 \cdot 37) = 3^0 37^0(3 - 1)(37 - 1)$; ossia $\varphi(111) = 72$.

360.
Essendo $360 = 2^3 \cdot 3^2 \cdot 5$, si ha $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 2^2 3^1 5^0(2 - 1)(3 - 1)(5 - 1)$; ossia, $\varphi(360) = 96$.

Esercizio 2. Risolvere le equazioni

$$\bigstar_1 \;\; 14\mathrm{X} \equiv_{24} 2 \qquad \bigstar_2 \;\; 18\mathrm{X} \equiv_3 8 \qquad \bigstar_3 \;\; 96\mathrm{X} \equiv_6 24.$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico *positivo* tra i massimi divisori comuni di a_1 e a_2.

$\bigstar_1$. Poiché $(14, 24) = 2$ e $2|2$, l'equazione è compatibile, ammette $(14, 24) = 2$ soluzioni modulo 24 ed è equivalente a

$$\blacksquare_1 \quad 7\mathrm{X} \equiv_{12} 1.$$

Risolviamo, dunque, $\blacksquare_1$. Un'identità di Bezout per $(7, 12) = 1$ è, ad esempio, la seguente, ottenuta dividendo 12 per 7 (si ha $12 = 1 \cdot 7 + 5$) e, successivamente, 7 per 5 (si ha $7 = 1 \cdot 5 + 2$) e 5 per 2 (si ha $5 = 2 \cdot 2 + 1$):

$$1 = 3 \cdot 12 + (-5) \cdot 7$$

Abbiamo allora

$$1 = 1 \cdot 1 = 1 \cdot (3 \cdot 12 + (-5) \cdot 7) = 3 \cdot 12 + (-5) \cdot 7.$$

Quindi $1 \equiv_{12} (-5) \cdot 7$, così che -5 è una soluzione particolare di $\blacksquare_1$ e, dunque, di $\bigstar_1$. Quindi, l'insieme delle soluzioni di $\blacksquare_1$ (equivalentemente, di $\bigstar_1$) è $-5 + 12\mathbb{Z}$.

Un sistema completo di soluzioni di $\bigstar_1$ è, ad esempio, il seguente $\{-5, -5 + 12\}$; ossia, $\Sigma_1 = \{-5, 7\}$. Un altro sistema completo di soluzioni è, ad esempio, $\mathrm{S}_1 = \{7, 19\}$. Naturalmente, l'insieme delle classi resto modulo 24 degli elementi di Σ_1 e l'insieme delle classi resto modulo 24 degli elementi di S_1 coincidono.

$\bigstar_2$. Poiché $(18, 3) = 3$ e $3 \nmid 8$, l'equazione **non** è compatibile.

$\bigstar_3$. Poiché $(96, 6) = 6$ e $6|24$, l'equazione è compatibile, ammette $(96, 6) = 6$ soluzioni modulo 6 ed è equivalente a

$$\blacksquare_3 \quad 16\mathrm{X} \equiv_1 4,$$

cioè, l'insieme delle soluzioni di $\blacksquare_3$ (equivalentemente, di $\bigstar_3$) è l'intero insieme $\mathbb{Z}$ ([1]).

[1] Ricordiamo che la relazione $\equiv_1$ è la relazione di equivalenza totale su $\mathbb{Z}$.

Esercizio 3. Siano $p \in \mathbb{Z}$ un primo e $a \in \mathbb{Z}$ un intero. Si mostri che per ogni $n \in \mathbb{N}$ risulta

$$\square_n. \qquad a^{n(p-1)+1} \equiv_p a.$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico *positivo* tra i massimi divisori comuni di a_1 e a_2.

Osserviamo innanzi tutto che un inverso aritmetico di a modulo p esiste sempre, perché, p essendo primo, risulta $(a, p) = 1$. Quindi, moltiplicando entrambi i membri di $\square_n$ per un tale inverso, possiamo affermare che $a^{n(p-1)+1} \equiv_p a$ è vera se e solo se è vera

$$\triangle_n. \qquad a^{n(p-1)} \equiv_p 1.$$

Dimostreremo la validità di $\triangle_n$ per induzione su $n \in \mathbb{N}$.

Base. Se $n = 0$, allora $\triangle_0$ è vera se e solo se $a^{(p-1)} \equiv_p 1$; ossia, **sempre**, grazie al teorema di Eulero-Fermat.

Passo. Sia ora $n \in \mathbb{N}$, $n \geq 0$ e supponiamo che $\triangle_n$ sia vera: vogliamo dimostrare che, allora, $\triangle_{n+1}$ è anche vera. Ora, $\triangle_{n+1}$ è vera se e solo se $a^{(n+1)(p-1)} \equiv_p 1$; ossia, se e solo se $a^{n(p-1)} \cdot a^{(p-1)} \equiv_p 1$; ossia, **sempre**. Infatti, poiché da una parte $a^{(p-1)} \equiv_p 1$ per ipotesi induttiva e, da un'altra parte per il teorema di Eulero-Fermat $a^{(p-1)} \equiv_p 1$, risulta

$$a^{(n+1)(p-1)} \equiv_p a^{n(p-1)} \cdot a^{(p-1)} \equiv_p 1 \cdot 1 \equiv_p 1.$$

Esercizio 4. Dire se i seguenti elementi sono invertibili e, in caso affermativo, calcolarne l'inverso usando il teorema di Eulero-Fermat.

$$\overline{80} \in \mathbb{Z}_{81}; \qquad \overline{63} \in \mathbb{Z}_{84}; \qquad \overline{181} \in \mathbb{Z}_{360}.$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico *positivo* tra i massimi divisori comuni di a_1 e a_2.

$\overline{\mathbf{80}} \in \mathbb{Z}_{\mathbf{81}}$.
Da $(80, 81) = 1$, si ha che $\overline{80} \in \mathbb{Z}_{81}$ è invertibile. Un inverso aritmetico di 80 modulo 81 è, ad esempio $80^{\varphi(81)-1}$; ossia 80^{53}, essendo $\varphi(81) = \varphi(3^4) = 3^3(3-1) = 54$.

$\overline{\mathbf{63}} \in \mathbb{Z}_{\mathbf{84}}$.
Da $(63, 84) = 7 \neq 1$, si ha che $\overline{63} \in \mathbb{Z}_{84}$ **non** è invertibile.

$\overline{\mathbf{181}} \in \mathbb{Z}_{\mathbf{360}}$.
Da $(181, 360) = 1$, si ha che $\overline{181} \in \mathbb{Z}_{360}$ è invertibile. Un inverso aritmetico di 181 modulo 360 è, ad esempio, $181^{\varphi(360)-1}$; ossia 181^{95}; essendo $\varphi(360) = 96$ ([2]).

[2]Si veda la soluzione dell'esercizio 1.

Esercizio 5. Risolvere il sistema

$$\Gamma \quad \begin{cases} \mathrm{X} & \equiv_3 & 2 \\ 2\mathrm{X} & \equiv_5 & 3 \\ 3\mathrm{X} & \equiv_7 & 4 \end{cases}$$

Soluzione. In quanto segue, dati comunque $a_1, a_2 \in \mathbb{Z}$, indicheremo con (a_1, a_2) l'unico *positivo* tra i massimi divisori comuni di a_1 e a_2.

Per affermare che Γ è compatibile è sufficiente la semplice analisi dei suoi coefficienti e dei suoi moduli; infatti, si ha $(3,5) = 1$, $(3,7) = 1$, $(5,7) = 1$ e $(1,3) = 1$ divide 2, $(2,5) = 1$ divide 3, $(3,7) = 1$ divide 4. Inoltre Γ è equivalente al sistema cinese ([3])

$$\mathrm{K} \quad \begin{cases} \mathrm{X} & \equiv_3 & 2 \\ \mathrm{X} & \equiv_5 & 9 \\ \mathrm{X} & \equiv_7 & 20 \end{cases}$$

Al sistema K associamo i tre seguenti sistemi

$$\mathrm{K}^1 \begin{cases} \mathrm{X} & \equiv_3 & 1 \\ \mathrm{X} & \equiv_5 & 0 \\ \mathrm{X} & \equiv_7 & 0 \end{cases} \qquad \mathrm{K}^2 \begin{cases} \mathrm{X} & \equiv_3 & 0 \\ \mathrm{X} & \equiv_5 & 1 \\ \mathrm{X} & \equiv_7 & 0 \end{cases} \qquad \mathrm{K}^3 \begin{cases} \mathrm{X} & \equiv_3 & 0 \\ \mathrm{X} & \equiv_5 & 0 \\ \mathrm{X} & \equiv_7 & 1 \end{cases}$$

Usando identità di Bezout per esprimere $(3, 5\cdot 7) = 1$, $(5, 3\cdot 7) = 1$ e $(7, 3\cdot 5) = 1$, si ha

$$\begin{aligned} \kappa^1 \qquad 1 &= (-1)\cdot(5\cdot 7) + 12\cdot 3 \\ \kappa^2 \qquad 1 &= (1)\cdot(3\cdot 7) + (-4)\cdot 5 \\ \kappa^3 \qquad 1 &= (1)\cdot(3\cdot 5) + (-2)\cdot 7 \end{aligned}$$

Quindi, $-5{\cdot}7 = -35$, $3{\cdot}7 = 21$ e $3{\cdot}5 = 15$ sono soluzioni di K^1, K^2 e, rispettivamente, K^3. Ne segue che $2\cdot(-35) + 9\cdot 21 + 20\cdot 15 = 419$ è soluzione particolare di K e, con esso, del sistema originale Γ.

L'insieme delle soluzioni di Γ è, dunque, $419 + (3\cdot 5\cdot 7)\mathbb{Z}$; ossia, $104 + 105\mathbb{Z}$, essendo $3\cdot 5\cdot 7 = 105$ e $419 = 3\cdot 105 + 104$.

[3] Il sistema K è stato ottenuto calcolando inversi aritmetici di 1, 2 e 3 modulo 3, 5 e, rispettivamente, 7; gli inversi aritmetici qui utilizzati sono 1, 3 e, rispettivamente 5.

Esercizio 6. Determinare le ultime tre cifre decimali di 38^{21}.

Soluzione. Scopo dell'esercizio è quello di determinare il resto della divisione di 38^{21} per 1.000; ossia, quello di risolvere la congruenza $\mathrm{X} \equiv_{1.000} 38^{21}$; ossia, quello di determinare nella classe $[38^{21}]_{1.000} \in \mathbb{Z}_{1.000}$ un elemento $x \in [38^{21}]_{1.000}$ tale che $0 \leq x \lneq 1.000$.

A tal fine, iniziamo riscrivendo 38^{21} nella forma $38^{21} = 54872^7$ ([4]). Ne segue che

$$[38^{21}]_{1.000} = [54872^7]_{1.000} = [54872]^7_{1.000} = [872]^7_{1.000}.$$

Ora, secondo il teorema cinese dei resti, poiché $1.000 = 2^3 \cdot 5^3$, esiste un isomorfismo

$$\begin{array}{rccc} \kappa: & \mathbb{Z}_{1.000} & \longrightarrow & \mathbb{Z}_8 \times \mathbb{Z}_{125} \\ & [\xi]_{1.000} & \longmapsto & (\ [\xi]_8\ ,\ [\xi]_{125}\ ) \end{array}$$

Allora

$$\begin{array}{rcccl} \kappa([38^{21}]_{1.000}) & = & \kappa([872]^7_{1.000}) & = & (\ [872]^7_8\ ,\ [872]^7_{125}\ ) \\ & & & = & (\ [109 \cdot 8]^7_8\ ,\ [7 \cdot 125 - 3]^7_{125}\ ) \\ & & & = & (\ [0]^7_8\ ,\ [-3]^7_{125}\ ) \\ & & & = & (\ [0]_8\ ,\ [-3][729]_{125}\ ) \\ & & & = & (\ [0]_8\ ,\ [-3][6 \cdot 125 - 21]_{125}\ ) \\ & & & = & (\ [0]_8\ ,\ [-3][-21]_{125}\ ) \\ & & & = & (\ [0]_8\ ,\ [63]_{125}\ ) \end{array}$$

Si tratta, allora, di risolvere il seguente sistema cinese

$$\bar{\mathrm{K}} \quad \begin{cases} \mathrm{X} \equiv_8 0 \\ \mathrm{X} \equiv_{125} 63 \end{cases}$$

È immediato verificare che l'insieme delle soluzioni della seconda equzione di $\bar{\mathrm{K}}$ è $63 + 125\mathbb{Z}$; ossia, una soluzione generica x della seconda equazione di $\bar{\mathrm{K}}$ deve essere del tipo $x = 63 + 125y$, con $y \in \mathbb{Z}$.

Ora, sostituendo nella prima equazione di $\bar{\mathrm{K}}$ una soluzione generica $x = 63 + 125y$ della seconda equazione di $\bar{\mathrm{K}}$, troviamo che $x \equiv_8 0$ se e solo se $63 + 125y \equiv_8 0$; ossia, se e solo se([5])

$$\blacksquare \quad -1 + 5y \equiv_8 0.$$

Ne segue che, affinché la congruenza $\blacksquare$ sia verificata, l'intero $y \in \mathbb{Z}$ deve appartenere all'insieme $5 + 8\mathbb{Z}$; ossia, deve essere della forma $y = 5 + 8z$, con $z \in \mathbb{Z}$ qualsiasi ([6]).

---

[4] Infatti, $38^{21} = (38^3)^7$ e $38^3 = 54872$.

[5] Risulta $63 \equiv_8 -1$ e $125 \equiv_8 5$.

[6] Infatti 5 è un inverso aritmetico di 5 modulo 8.

Quindi un intero x che sia soluzione di $\bar{\mathrm{K}}$ (cioè, soluzione simultaneamente della prima e della seconda equazione di $\bar{\mathrm{K}}$) deve essere necessariamente della forma $x = 63 + 125y$, con y un intero della forma $y = 5 + 8z$ e con $z \in \mathbb{Z}$ un intero qualsiasi. Quindi x deve essere della forma $x = 63 + 125y = 63 + 125(5 + 8z)$, con $z \in \mathbb{Z}$ qualsiasi; ossia, deve essere della forma

$$x = 688 + 1.000z, \text{ con } z \in \mathbb{Z} \text{ qualsiasi.}$$

Allora dall'iniettività di κ e da $\kappa([38^{21}]_{1.000}) = \kappa([688]_{1.000})$, si ha che $[38^{21}]_{1.000} = [688]_{1.000}$, così che le ultime tre cifre decimali di 38^{21} coincidono cone le ultime tre cifre decimali di 688. Tali cifre sono dunque 6, 8 e 8.