$13^{18} + 19^{12} \equiv 1 \bmod 247$

$247 = 13 \cdot 19$

$13^{19-1} + 19^{13-1} \equiv 1 \pmod{13 \cdot 19}$

Σε μια άσκηση εχει δοθεί. Από το θεώρημα Euler έχουμε

$$\begin{cases} m^{\phi(n)} \equiv 1 \bmod n \\ n^{\phi(m)} \equiv 1 \bmod m \end{cases} \rightarrow \begin{cases} n \mid m^{\phi(n)} - 1 \\ m \mid n^{\phi(m)} - 1 \end{cases}$$

$$\Rightarrow m \cdot n \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1)$$

$$\Rightarrow \begin{cases} m \cdot n \mid m^{\phi(n)} \cdot n^{\phi(n)} - (m^{\phi(n)} + n^{\phi(m)} - 1) \\ m \cdot n \mid m^{\phi(n)} n^{\phi(m)} \end{cases}$$

$$\Rightarrow m \cdot n \mid m^{\phi(n)} + n^{\phi(m)} - 1$$

$$\Rightarrow m^{\phi(n)} + n^{\phi(m)} \equiv 1 \bmod (m,n) \quad (1)$$

Τα $p = 13$ και $q = 19$ είναι $(p, q) = 1$

Άρα η (1) παίρνει τη μορφή

$$p^{\phi(q)} + q^{\phi(p)} \equiv 1 \bmod (p \cdot q)$$

$$13^{19-1} + 19^{13-1} \equiv 1 \bmod (247)$$

$$13^{18} + 19^{12} \equiv 1 \bmod (247).$$

(1) Νδο $17 \mid (16!+1) \Leftrightarrow 16!+1 \equiv 0 \bmod 17 \Leftrightarrow$

$16! \equiv -1 \bmod 17$

α' τρόπος

Άρα

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 + 1 \bmod 17$

$1 \cdot 6 \cdot 20 \cdot 42 \cdot 72 \cdot 110 \cdot 156 \cdot 210 \cdot 16 + 1 \bmod 17$

$1 \cdot 6 \cdot 3 \cdot 8 \cdot 4 \cdot 8 \cdot 3 \cdot 6 \cdot 16 + 1$

$6 \cdot 24 \cdot 32 \cdot 18 \cdot 16 + 1$

$6 \cdot 7 \cdot 15 \cdot 1 \cdot 16 + 1$

$8 \cdot 15 \cdot 1 \cdot 16 + 1$

$8 \cdot 15 \cdot 16 + 1$

$8 \cdot 240 + 1$

$8 \cdot 2 + 1$

$16 + 1$

$17 \equiv 0 \bmod 17$

Άρα $17 \mid (16!+1)$.

β' τρόπος Θεώρημα Wilson για $p = 17$

$(p-1)! \equiv -1 \bmod 17$

$16! \equiv -1 \bmod 17$

$17 \mid 16!+1$

Άσκηση 5

Ον. Γκούμας Ευάγγελος
Α.Μ. 14394

Έστω p πρώτος αριθμός. Για κάθε ακέραιο a να δειχθεί ότι

$$p \mid (a^p + a(p-1)!)$$

Λύση

Από το θεώρημα Fermat έχουμε ότι

$$a^p \equiv a \bmod p \quad (1)$$

Από το θεώρημα Wilson έχουμε ότι

$$(p-1)! \equiv -1 \bmod p \Rightarrow a(p-1)! \equiv -a \pmod p \quad (2)$$

(1) + (2)

$$a^p + a(p-1)! \equiv a - a \bmod p$$

$$a^p + a(p-1)! \equiv 0 \bmod p$$

Άρα $p \mid a^p + a(p-1)!$.

(2) Ov. Faoulias Evdoxios
AM: 19399

$5^{2n+1} 2^{n+2} + 3^{n+2} 2^{2n+1} \equiv 0 \bmod 19$

$19 \mid 5^{2n+1} 2^{n+1}$

$19 \mid 3^{n+2} 2^{2n+1}$

$5^2 \equiv 6 \bmod 19$

$5^{2n} \equiv 6^n \bmod 19$

$5^{2n+1} \equiv 6^n \cdot 5 \bmod 19$

$5^{2n+1} \cdot 2 \equiv 6^n \cdot 5 \cdot 2 \bmod 19$

$5^{2n+1} \cdot 2^n \equiv 6^n \cdot 5 \cdot 2^n \bmod 19$

$5^{2n+1} 2^{n+2} \equiv 6^n \cdot 5 \cdot 2^n 4 \bmod 19$

$5^{2n+1} 2^{n+2} \equiv (6 \cdot 2)^n 20 \bmod 19$

$5^{2n+1} 2^{n+2} \equiv (1 \cdot 2)^n \bmod 19$ (1) και (2)

$5^{2n+1} 2^{n+2} \equiv (\cdot 12)^n \bmod 19$

$+ 3^{n+2} 2^{2n+1} \equiv -(12)^n \bmod 19$

$3^n \equiv 3^n \bmod 19$

$3^{n+2} \equiv 3^n \cdot 9 \bmod 19$

$3^{n+2} 2^{2n+1} \equiv 3^n \cdot 9 \cdot 2^n \cdot 2 \bmod 19$

$3^{n+2} 2^{2n+1} \equiv (12)^n \cdot 18 \bmod 19$

$3^{n+2} 2^{2n+1} \equiv (12)^n \cdot -1 \bmod 19$ (2)

$5^{2n+1} 2^{n+2} + 3^{n+2} 2^{2n+1} \equiv 0 \bmod 19$

Άσκηση 6

$X^2 \equiv 152 \bmod 43$ και $x^2 \equiv -154 \bmod 163$

α) Θα υπολογίσω το σύμβολο του Legendre για $X^2 \equiv 152 \bmod 43$

$$\left(\frac{152}{43}\right) = \left(\frac{2 \cdot 76}{43}\right) = \left(\frac{2}{43}\right)\cdot\left(\frac{76}{43}\right) = (-1)^{\frac{43^2-1}{8}} \cdot \left(\frac{76}{43}\right) =$$

$$= (-1)^{231}\left(\frac{33}{43}\right) = (-1)^{231} \cdot (-1)^{\frac{43-1}{2}\cdot\frac{33-1}{2}}\left(\frac{43}{33}\right) =$$

$$= -1 \cdot (-1)^{\frac{42}{2}\cdot\frac{32}{2}}\left(\frac{10}{33}\right) = (-1)\cdot(-1)^{21\cdot 16}\left(\frac{10}{33}\right) =$$

$$= (-1)(-1)^{336}\left(\frac{2\cdot 5}{33}\right) = -\left(\frac{2}{33}\right)\cdot\left(\frac{5}{33}\right) =$$

$$= -1 \cdot (-1)^{\frac{33^2-1}{8}} \cdot (-1)^{\frac{33-1}{2}\cdot\frac{5-1}{2}}\left(\frac{33}{5}\right) =$$

$$= -1\,(-1)^{136} \cdot (-1)^{16\cdot 2} \cdot \left(\frac{3}{5}\right) =$$

$$= -1 \cdot 1 \cdot 1 \left(\frac{3}{5}\right) = -1 \cdot (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\left(\frac{5}{3}\right) =$$

$$= -1 \cdot (-1)^{1\cdot 2}\left(\frac{2}{3}\right) =$$

$$= -1\left(\frac{2}{3}\right) = -1 \cdot (-1)^{\frac{3^2-1}{8}} =$$

$$= -1 \cdot (-1)^{\frac{9-1}{8}} = (-1)(-1)^{\frac{8-1}{8}} =$$

$$= (-1)\cdot(-1) = 1$$

Έχει λύση

b) $X^2 \equiv -154 \bmod 163$

Χαρακτήρας ως ολοκλήρωση Legendre είναι $\left(\frac{-154}{163}\right) = \begin{cases} 1, & -154 \in R_{163} \\ -1, & -154 \in \overline{R}_{163} \end{cases}$

$$\left(\frac{-154}{163}\right) = \left(\frac{-1}{163}\right)\cdot\left(\frac{154}{163}\right) = (-1)^{\frac{163-1}{2}}\cdot\left(\frac{154}{163}\right) =$$

$$= (-1)^{\frac{162}{2}}\cdot\left(\frac{2\cdot 77}{163}\right) = (-1)^{81}\left(\frac{2}{163}\right)\cdot\left(\frac{77}{163}\right) =$$

$$= -1\cdot(-1)^{\frac{163^2-1}{8}}\cdot\left(\frac{77}{163}\right) = (-1)\cdot(-1)\cdot(-1)^{\frac{163-1}{2}\cdot\frac{77-1}{2}}\left(\frac{163}{77}\right)$$

$$= (-1)^{\frac{1620}{2}\cdot\frac{76}{2}}\left(\frac{9}{77}\right) = (-1)^{81\cdot 38}\cdot\left(\frac{3^2}{77}\right) =$$

$$= (-1)^{2592}\cdot 1 = 1.$$

Επαλήθευση.

Άσκηση 1

Δείξτε ότι εάν a, n θετικοί ακέραιοι τ.ώ $\text{ord}_{a^n-1}(a) = n$. και αιτιολογήστε

Να αποδείξετε ότι $n \mid \phi(a^n-1)$

Λύση

Έστω $1 \leq k < n$. Τότε $a^k \not\equiv 1 \pmod{a^n-1}$ καθώς εάν $a^k \equiv 1 \bmod a^n-1$

τότε $a^k - 1 \equiv 0 \pmod{a^n-1} \Rightarrow a^n-1 \mid a^k-1 \Rightarrow a^n-1 \leq a^k-1 \Rightarrow a^n \leq a^k$

Άτοπο καθώς το $k < n$.

Τέρμα ότι επίσης το $a^k \equiv 1 \pmod{a^n-1} \Rightarrow n = \text{ord}_{a^n-1}(a)$ (Α.Δ ορίζω το ελάχιστο ακέραιος k τ.ώ $a^k \equiv 1 \pmod{a^n-1}$)

Άρα $\text{ord}_{a^n-1}(a) = n \mid \phi(a^n-1)$.

A Άσκηση 1

(2) Δείξτε ότι η κλάση $[62]_{155}$ δεν είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{155}$

Λύση

Το $(155, 62) = 31$

Από τον αλγόριθμο του Ευκλείδη για $\alpha = 5$ έχουμε ότι άρα ο $M.K.\Delta(155, 62) = 31$

$$155 = 62 \cdot 2 + 31$$
$$62 = (31) \cdot 2 + 0$$

Το $[62]_{155}$ έχει γενική μορφή $[\alpha]_{155} \Rightarrow \alpha = 62$ και $n = 155$

$(\alpha, n) = 1$ για να αντιστρέφεται

Από τον αλγόριθμο

Επομένως το $[62]_{155}$ δεν Αντιστρέφεται.

(2) Δείξτε ότι η κλάση υπολοίπων $[10]_{21}$ είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{21}$ και βρείτε την αντίστροφη κλάση της.

Λύση

$(10, 21) = 1$

Από αλγόριθμο Ευκλείδη Παρατηρούμε ότι οι αριθμοί $(10, 21)$ είναι σχετικά πρώτοι μεταξύ τους

Άρα $\begin{cases} 21 = 10 \cdot 2 + 1 \\ 10 = (1) 10 + 0 \end{cases}$ Άρα το $[10]_{21}$ αντιστρέφεται στο $\mathbb{Z}_{21}$

$[10]_{21}^{-1}$

$$21 = 2 \cdot 10 + 1 \Rightarrow 1 = 1 \cdot 21 + (-2) \cdot 10 \Leftrightarrow$$
$$[1]_{21} = [21]_{21} + [-2]_{21} \cdot [10]_{21} \Leftrightarrow$$
$$[1]_{21} = 0 + [-2]_{21} \cdot [10]_{21}$$
$$\frac{[1]_{21}}{[10]_{21}} = [-2]_{21} \Leftrightarrow$$
$$[10]_{21}^{-1} = [-2]_{21} \Leftrightarrow$$
$$[10]_{21}^{-1} = [19]_{21}$$

Άσκηση 4.

(1) Δείξτε ότι: Αν $a \equiv b \bmod n_1$ και $b \equiv c \bmod n_2$, τότε $a \equiv c \bmod (n_1, n_2)$

Λύση

$$\begin{cases} a \equiv b \pmod{n_1} \\ b \equiv c \pmod{n_2} \end{cases} \Rightarrow \begin{cases} a - b \equiv 0 \pmod{n_1} \\ b - c \equiv 0 \pmod{n_2} \end{cases} \Rightarrow \begin{cases} n_1 \mid a-b \\ n_2 \mid b-c \end{cases}$$

* Το $(n_1, n_2) = d$ $d \mid n_1$ και $d \mid n_2$

$$\begin{cases} d \mid a-b \\ d \mid b-c \end{cases} \Rightarrow d \mid a-b+b-c \Rightarrow d \mid a-b \Rightarrow a \equiv b \pmod{d}$$ ή $a \equiv b \pmod{(n_1, n_2)}$.

(2) Δείξτε ότι εάν $a, b, n_1, \ldots, n_k \in \mathbb{Z}$ με $n_i \geq 1$ τότε $a \equiv b \bmod n_i$ για κάθε $i = 1, 2, 3, \ldots, k$ εάν και μόνον εάν $a \equiv b \bmod [n_1, n_2, \ldots, n_k]$

Λύση

($\Rightarrow$) Άρα $a \equiv b \bmod n_i \Rightarrow n_i \mid a-b \ \forall i = 1, 2, \ldots, k \Rightarrow [n_1, n_2, \ldots, n_k] \mid a-b$

$\Rightarrow a \equiv b \bmod [n_1, n_2, \ldots, n_k]$

($\Leftarrow$) Έχουμε ότι $a \equiv b \bmod [n_1, n_2, \ldots, n_k] \Rightarrow [n_1, n_2, \ldots, n_k] \mid a-b$

Άρα το $n_1 \mid [n_1, n_2, \ldots, n_k]$, $n_2 \mid [n_1, n_2, \ldots, n_k]$, $\ldots$, $n_k \mid [n_1, n_2, \ldots, n_k]$

Άρα $n_i \mid a-b \Rightarrow a \equiv b \pmod{n_i}$.

Άσκηση 11 14394

Να βρεθούν όλες οι λύσεις των παρακάτω ισοτιμιών

a) $2X \equiv 5 \bmod 7$

b) $3X \equiv 6 \bmod 9$

c) $19X \equiv 30 \bmod 40$

Λύση

a) $2X \equiv 5 \bmod 7$ Το $(2,7)=1$ το $1|5$ άρα υπάρχει μοναδική λύση η οποία είναι η $\bar{X}=6$

- $X=0 \to 2\cdot 0 \not\equiv 5 \bmod 7$
- $X=1 \to 2 \not\equiv 5 \bmod 7$
- $X=2 \to 4 \not\equiv 5 \bmod 7$
- $X \equiv 3 \to 6 \not\equiv 5 \bmod 7$
- $X \equiv 4 \to 8 \equiv 1 \not\equiv 5 \bmod 7$
- $X=5 \to 10 \equiv 3 \not\equiv 5 \bmod 7$
- $X \equiv 6 \to 12 \equiv 5 \bmod 7$

$$X \equiv 6 \pmod 7$$

b) $3X \equiv 6 \bmod 9$ $(3,9)=3$ άρα έχει τρεις λύσεις μοναδικές μ.ε 3/6

Άρα το $X \in \{0,1,2,3,4,5,6,7,8\}$

- για $X=2$
  $3\cdot 2 = 6 \not\equiv \bmod 9$

Άρα $\bar{X}=2$, $\bar{X}=5$ και $\bar{X}=8$

$X \equiv 2 \pmod 9$, $X \equiv 5 \pmod 9$ και $X \equiv 8 \pmod 9$

- $X=5$
  $15 \equiv 6 \bmod 9$

- $X=8$
  $24 \equiv 6 \bmod 9$

c) $19X \equiv 30 \bmod 40$

$(40,19)=1$ το $1|30$ Άρα το πλήθος των λύσεων είναι ακριβώς μία

Παρατηρώ ότι το $\bar{X}=10$ $19\cdot 10 = 190 \equiv 30 \pmod{40}$

Επομένως $X \equiv 10 \pmod{40}$.

Άσκηση 5

Δείξτε ότι (1) $2^{50} \equiv 4 \bmod 7$ και (2) $1! + 2! + 3! + \ldots + 100! \equiv 9 \bmod 12$

Λύση

(1) $2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$

Άρα το $2^5 \equiv 4 \bmod 7 \longrightarrow 10 = 7 \cdot 1 + 3$

$(2^5)^{10} \equiv 4^{10} \bmod 7$

$2^{50} \equiv 4^{10} \pmod 7$

$2^{50} \equiv 4 \pmod 7$

$4^{10} = 4^{7 \cdot 1 + 3} = 4^7 \cdot 4^3 \equiv 4 \cdot 1 \pmod 7$

(2) $1! + 2! + 3! + \ldots + 100! \equiv 9 \bmod 12$

Το

① $\begin{cases} 1! + 2! + 3! \equiv 9 \bmod 12 \\ 4! = 1 \cdot 2 \cdot 3 \cdot 4 \equiv 0 \bmod 12 \\ \text{και } n > 4 \text{ άρα } n! = 4! \cdot 5 \cdot 6 \ldots n \equiv 0 \bmod 12 \end{cases}$

$1! + 2! + 3! + \ldots + 100! \equiv 9 \bmod 12.$

Άσκηση 3

Έστω $\{a_1, a_2, \dots, a_p\}$ και $\{b_1, b_2, \dots, b_p\}$ δύο πλήρη συστήματα υπολοίπων mod p όπου p είναι ένας πρώτος. Να δείξετε ότι αν $p > 2$, τότε το σύνολο $\{a_1 b_1, a_2 b_2, \dots, a_p b_p\}$ δεν είναι πλήρες σύστημα υπολοίπων mod p.

Λύση

Για να είναι πλήρες θα πρέπει το $a_i \equiv 0 \bmod p$ και $b_j \equiv 0 \bmod p$ με $i, j \in \{1, \dots, p\}$

Έστω ότι $a_p \equiv 0 \bmod p$ $(i = p)$

α) Εάν $j \neq p$ τότε $a_j b_j \equiv 0 \bmod p$ και $a_p b_p \equiv 0 \pmod p$

Άρα το $\{a_1 b_1, \dots, a_p b_p\}$ δεν είναι πλήρες mod p

β) Εάν $j = p$ ξεφεύγει το $\{a_1, a_2, \dots, a_p\}$ είναι πλήρες σύστημα υπολοίπων mod p τότε υπάρχει $1-1$ απεικόνιση $\sigma: \{1, 2, \dots, p-1\} \longrightarrow \{a_1, \dots, a_{p-1}\}$ τ.ω. $a_i \equiv \sigma(i) \bmod p$

Άρα $\prod_{i=1}^{p-1} a_i = \prod_{i=1}^{p-1} \sigma(i) = \prod_{i=1}^{p-1} i = 1 \cdot 2 \cdot \dots \cdot (p-1)$

Από wilson theorem

$$a_1 \cdot a_2 \dots a_{p-1} \equiv 1 \cdot 2 \cdot 3 \dots p-1 \equiv (p-1)! \pmod p$$

και

$$b_1 b_2 \dots b_{p-1} \equiv (-1) \bmod p$$

Άρα $a_1 b_1 a_2 b_2 a_3 b_3 \dots a_{p-1} b_{p-1} \equiv 1 \bmod p$

Άρα το $\{a_1 b_1, a_2 b_2, \dots, a_p b_p\}$ δεν είναι πλήρες σύστημα mod p

Γιατί θα έπρεπε $a_1 b_1 a_2 b_2 \dots a_{p-1} b_{p-1} \equiv (-1) \bmod p$ όπως δεν είναι.

Άσκηση 7

Λύση

Έστω $nx_i + my_j \equiv nx_k + my_k \pmod{mn} \Rightarrow mn \mid n(x_i - x_k) + (y_j - y_k)$

Αλλά $m \mid mn$ παίρνουμε ότι

$$\begin{cases} m \mid n(x_i - x_k) + m(y_j - y_k) \\ m \mid m(y_j - y_k) \end{cases} \Rightarrow m \mid n(x_i - x_k)$$

$(m,n) = 1$

$m \mid x_i - x_k$

$\Rightarrow x_i \equiv x_k \pmod{m}$

$$\begin{cases} n \mid n(x_i - x_k) + m(y_j - y_k) \\ n \mid n(x_i - x_k) \end{cases} \Rightarrow n \mid m(y_j - y_k) \Rightarrow$$

$(m,n) = 1$

$\Rightarrow y_j \equiv y_k \pmod{n}$

Δηλαδή αυτών εκφράζουμε το x είναι πλήρες σύστημα υπολοίπων modm και το y πλήρες σύστημα υπολοίπων το modn

Άρα $i = k$ και $j = k$

Άρα το Z είναι πλήρες σύστημα υπολοίπων mod $m.n$

Άσκηση 8

Λύση

- Αν $(m,n)=1$ τότε $(my_i+nx_i, mn) = (nx_i+my_i, m)\cdot(nx_i+my_i, n)$

a) Έστω $d=(nx_i+my_i, m)$, Τότε για $i=1,2,\dots,\phi(mn)$

$$\begin{cases} d \mid nx_i+my_i \\ d \mid m \end{cases} \Rightarrow \begin{cases} d \mid nx_i \\ d \mid mx_i \end{cases} \Rightarrow d \mid (nx_i, mx_i) \Rightarrow d \mid (n,m)x_i$$

$$\Rightarrow d \mid x_i$$

$\Rightarrow d \mid (x_i, n) = 1$ αφού το X είναι περιορισμός σύνολο υπολοίπων modm

άρα $d=1$.

b) Με τον ίδιο τρόπο $(nx_i+my_i, n)=1$

$$\begin{cases} d \mid nx_i+my_i \\ d \mid n \end{cases} \Rightarrow \begin{cases} d \mid my_i \\ d \mid ny_i \end{cases} \Rightarrow d \mid (ny_i, my_i) \Rightarrow d \mid (m,n)y_i$$

$$\Rightarrow d \mid y_i$$

$d \mid (y_i, n) = 1$

Άρα το $(nx_i+my_i, n)=1$

- Έστω $(m,n) \neq 1$

$$nx_i+my_i \equiv nx_k+my_k \pmod{mn}$$

$$\begin{cases} mn \mid n(x_i-x_k)+m(y_i-y_k) \\ m \mid mn \\ n \mid mn \end{cases} \Rightarrow \begin{cases} m \mid n(x_i-x_k)+m(y_i-y_k) \\ n \mid n(x_i-x_k)+m(y_i-y_k) \end{cases}$$

$$\Rightarrow \begin{cases} m \mid n(x_i-x_k) \\ n \mid m(y_i-y_k) \end{cases} \Rightarrow \begin{cases} m \mid x_i-x_k \\ n \mid y_i-y_k \end{cases} \Rightarrow \begin{cases} x_i \equiv x_k \pmod m \\ y_j \equiv y_k \pmod n \end{cases}$$

Άρα $(i,j)=(k,k)$

Επειδή το $X=\{x_1, x_2, \dots, x_{\phi(m)}\}$ είναι περιορισμός σύνολο υπολοίπων modm

και $Y=\{y_1, y_2, \dots, y_{\phi(n)}\}$ είναι περιορισμός σύνολο υπολοίπων modn.

$$\begin{cases} 2x \equiv 4 \bmod 8 \\ 3x \equiv 12 \bmod 9 \\ x \equiv 34 \bmod 12 \end{cases}$$

$(9,8) = 1/4$ ✓ $(3,9) = 3/1$ ✓ $(1,12) = 1/34$ ✓

$$\begin{cases} x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 3 \\ x \equiv 34 \bmod 12 \\ x \equiv 10 \bmod 12 \end{cases} \rightarrow \begin{cases} x = 1 \bmod 3 \\ x \equiv 2 \bmod 4 \end{cases}$$

$x \equiv 10 \bmod 12$

$34 \mid 12$
$24 \quad 2$
10

$$\begin{cases} x \equiv 10 \bmod 3 \\ x \equiv 10 \bmod 4 \end{cases} \rightarrow \begin{cases} x = 7 \bmod 3 \\ x \equiv 6 \bmod 4 \end{cases}$$

(12)

$M_1 = \frac{12}{3} = 4$

$M_2 = \frac{12}{4} = 3$

$4x \equiv 1 \bmod 3$

$x = 1$

$3x \equiv 2 \bmod 4$

$x = 2$

$1 \cdot 4 + 2 \cdot 3 = 4 + 6 = 10$

Άρα $x \equiv 10 \bmod 12$

$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ Νδο $\sum_{d/n} \frac{\mu^2(d)}{\tau(d)} = \frac{3^n}{2^n}$

$$\sum_{d/n} \frac{\mu^2(d)}{\tau(d)} = \sum_{d/n} \mu(d) \frac{\mu(d)}{\tau(d)} = \sum_{d/n} \mu(d) f(d) = \prod_{p/n} (1 - f(p))$$

n $f(d)$ έναι πολλαπλασιαστική

$$1 - f(p) = (1 - f(p_1))(1 - f(p_2)) \dots (1 - f(p_m)) = \frac{3^n}{2^n}$$

$$1 - f(p) = 1 - \frac{\mu(d)}{\tau(d)} = 1 - \frac{(-1)}{2} = \frac{3}{2}$$

$$\begin{cases} x \equiv 5 \bmod 6 \\ x \equiv 4 \bmod 11 \\ x \equiv 3 \bmod 17 \end{cases}$$

$(6,11)=1$, $(6,17)=1$, $(11,17)=1$

Άρα $M = 17 \cdot 11 \cdot 6 = 66 \cdot 17 = 1122$

$M_1 = \frac{M}{6} = 187$, $M_2 = \frac{M}{11} = \frac{1122}{11} = 102$, $M_3 = \frac{M}{17} = 66$

$187x \equiv 5 \bmod 6$ $\quad$ $102x \equiv 4 \bmod 11$ $\quad$ $66x \equiv 3 \bmod 17$

~~$x_1 = 1$~~ $\quad$ ~~$x_2 = 4$~~ $\quad$ ~~$x_3 = 9$~~

$x = 5$ $\quad$ $x = 5$ $\quad$ $x = 7$

$M = 187 \cdot 4 \cdot 102 + 8 \cdot 66 = 187 + 408 + 528 = 1123 \bmod M$

$M = 1123 \pmod{1122}$

$M = 187 \cdot 5 + 5 \cdot 102 + 7 \cdot 66 = 935 + 510 + 462$

$= 1907 \pmod{1122}$

$\equiv 785 \pmod{1122}$

$140x \equiv 133 \pmod{302}$ και $34x \equiv 60 \bmod 98$

$(98,34) = 2$ το $2 \mid 60$

$98 = 34$

$\frac{34}{2} x \equiv \frac{60}{2} \bmod \frac{98}{2}$

$17x \equiv 30 \bmod 49 \Rightarrow x = 45$

$(49,17) = 1$ $\quad$ 41

$x \equiv 30\ 17 \bmod 49$

$\phi(49) = \phi(7) \cdot \phi(7) = 6 \cdot 6 = 36 - 1 = 35$

$\phi(49) = \phi(7) = 7^2 - 7^{2-1} = 49 - 7 = 42.$

$\phi(49) - 1 = 42 - 1 = 41$

Άρα $x = 45$

$x = 45 + 49 = 94$

$x^2 \equiv -38 \pmod{13}$

$\left(\frac{-38}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{38}{13}\right) =$

$= (-1)^{\frac{13-1}{2}} \left(\frac{38}{13}\right) =$

$= \left(\frac{38}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{19}{13}\right) =$

$3 \cdot 3 = 9 + 4$

$= (-1)^{\frac{13^2-1}{2}} \left(\frac{19}{13}\right)$

$= (-1)^{\frac{13-1}{2} \cdot \frac{19-1}{2}}$

$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) =$

$= 1 \cdot (-1)^{\frac{13^2-1}{2} \cdot \frac{3-1}{2}} \left(\frac{13}{3}\right) = \left(\frac{4}{3}\right) =$

$= \left(\frac{2^2}{3}\right) = 1.$

$x^2 + 7x + 10 \equiv 0 \pmod{11}$

$4x^2 + 28x + 40 \equiv 0 \pmod{11}$

$\underbrace{(2x+7)}_{y}{}^2 - 9 \equiv 0 \pmod{11}$

$y = 9 \pmod{11}$

$\left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = 1.$

Άσκηση 4 (εφαρμογή)

(1) για τον 2,3 στο mod11

Η συνάρτηση $\phi(11)$ Euler-function $\phi(11) = 11-1 = 10$

οι διαιρέτες του $\phi(11) = 10$ είναι το 2 και 5.

α $2^{\frac{\phi(11)}{2}} = 2^5 = 32 \not\equiv 1 \bmod 11$

και $2^{\frac{\phi(11)}{5}} = 2^2 = 16 \not\equiv 1 \bmod 11$

Άρα $ord_{11}(2) = 10 = \phi(11)$

για $a = 3$

α [illegible]

$3^{\frac{\phi(11)}{2}} = 3^5 = 243 \equiv 1 \bmod 11$ Αλλά δεν έχει πρωταρχική ρίζα στο mod(11) Άρα ~~$ord_{11}(3)$~~

(2) στο mod9

$\phi(9) = \phi(3^2) = 3^2 - 3^{2-1} = 9-3 = 6$ → 2,3 οι πρώτοι διαιρέτες του 6.

$(2,9) = 1$

$2^{\frac{\phi(9)}{2}} = 2^{\frac{6}{2}} = 2^3 = 8 \not\equiv 1 \bmod 9$

και $2^{\frac{\phi(9)}{3}} \equiv 2^{\frac{6}{3}} = 2^2 = 4 \not\equiv 1 \bmod 9$

Άρα το $ord_9(2) = 6 = \phi(9)$

[illegible]

$3^{\frac{\phi(9)}{2}} = 3^{\frac{6}{2}} = 3^3 = 27 \equiv 0 \not\equiv 1 \bmod 9$

και $3^{\frac{\phi(9)}{3}} = 3^{\frac{6}{3}} = 3^2 = 9 \equiv 0 \not\equiv 1 \bmod 9$

Άρα 3 είναι πρωταρχική ρίζα (mod9)

Άσκηση 4 (Ανδρίτσος)

(1) $\Rightarrow$ (2)

Από υπόθεση έχουμε ότι το a είναι πρωτογενής ρίζα mod n

Άρα $\text{ord}_n(a) = \phi(n)$ και $a^k \not\equiv 1 \bmod n$ $\forall$

για $1 \le k < \phi(n)$ και p διαιρέτες του $\phi(n)$ δηλ. $p \mid \phi(n)$. Άρα $k = \frac{\phi(n)}{p}$ $\forall$

$\phi(n) = k \cdot p$

Από $\forall \Rightarrow (\forall)$ $a^{\frac{\phi(n)}{p}} \not\equiv 1 \bmod n$

(2) $\Rightarrow$ (1)

Αν υποθέσουμε ότι $a^{\frac{\phi(n)}{p}} \not\equiv 1 \bmod n$ για τους πρώτους διαιρέτες p του $\phi(n)$

Και αν υποθέσουμε ότι το a δεν είναι πρωτογενής ρίζα του n. Άρα $\text{ord}_n(a) \mid \phi(n)$

και $\text{ord}_n(a) < \phi(n)$. Έστω $\text{ord}_n(a) = \pi$ θα έχουμε $\frac{\phi(n)}{\pi} > 1$. Έστω p

πρώτος διαιρέτης του $\frac{\phi(n)}{\pi}$ Τότε $\frac{\phi(n)}{\pi} = p \cdot m \Rightarrow \frac{\phi(n)}{p} = \pi \cdot m$

$\rightarrow a^{\frac{\phi(n)}{p}} = a^{\pi m} = (a^{\pi})^m = 1^m \equiv 1 \pmod n$ Άτοπο

Άρα ο a είναι όντως πρωτογενής ρίζα mod n.

$7 \mid (3^{2n+1} + 2^{n+2})$

$3^0 = 1 \equiv 2 \bmod 7$

$3^{2n} \equiv 2^n \bmod 7$

$3^{2n} 3 \equiv 2^n 3 \bmod 7$

$\boxed{3^{2n+1} \equiv 2^n 3 \bmod 7}$

$2^0 = 1 \equiv 4 \bmod 7$

$2^m \equiv 4^n \bmod 7$

$2^n \cdot 2^2 \equiv 4^n 4 \bmod 7$

$2^{n+2} \equiv 2^n 4 \bmod 7$

$3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 2^n 4 = 7 \cdot 2^n = 0 \bmod 7$

$\boxed{7 \mid 3^{2n+1} + 2^{n+2}}$

$24x + 138y = 18$

Apo

$138 = 24 \cdot 5 + 18$

$24 = 18 \cdot 1 + 6$

$18 = 6 \cdot 3 + 0$

$6 = (24, 138)$ ως $6 \mid 18$

$6 = 24 - 18(1) = 24 - 1 \cdot 18 =$

$24 - 1(138 - 24 \cdot 5) =$

$= 24 - 138 + 24 \cdot 5 =$

$= 6 \cdot 24 - 138 =$

$\boxed{24 \cdot (6) + 138(-1) = 6}$

αρα και

επ(3)

$\boxed{24 \cdot (18) + 138(-3) = 18}$

$\begin{cases} x = x_0 + \frac{b}{d} t \\ y = y_0 - \frac{a}{d} t \end{cases} \Rightarrow \begin{cases} x_0 = 18 + \frac{138}{6} t = 18 + 23t \\ y = -3 - \frac{24}{6} t = -3 - 4t \end{cases}$

$t \in \mathbb{Z}$ συν. απ.

Vδο $42 \mid n^7 - n$

$n^7 \equiv n \bmod 42$ $\quad 6 \cdot 7 = 42$

* $n^{\phi(7)} \equiv 1 \bmod 7 \quad 7 \nmid n$

$n^6 \equiv 1 \bmod 7$

~~$(n^{6-1}) \equiv 1 \bmod 7$~~

~~$n^{42} \equiv 1 \bmod 7$~~

$n^6 \cdot n \equiv n \bmod 7$

$\boxed{n^7 \equiv n \bmod 7}$

$6 = 2 \cdot 3$

$n^{\phi(3)} \equiv 1 \bmod 3$

$(n^2)^3 \equiv 1 \bmod 3$

$\boxed{n^7 \equiv n \bmod 3}$

$42 \mid n^7 - n$

2·2·2·2·2·2

Να λύσετε την ισοτιμία.

$2x \equiv 5 \pmod 7 \quad (2,7) = 1$ άρα ακριβώς μία λύση

$x = 5\, 2^{\phi(7)-1} \pmod 7$

$x \equiv 5\, 2^{6-1} \bmod 7$

$x \equiv 5 \cdot 32 \bmod 7$

$\boxed{x \equiv 6 \bmod 7}$

64 | 7
32 | 9
28
40
35
5

$n^{13} \equiv n \pmod{1365}$

$1365 = 3 \cdot 5 \cdot 7 \cdot 13$

Ex- $3 \nmid n$ Then $n^{\phi(3)} \equiv 1 \bmod 3$ (Fermat)

$n^2 \equiv 1 \bmod 3$

$n^{12} \equiv 1 \bmod 3$

$\boxed{n^{13} \equiv n \bmod 3}$ (1)

Ans: (1), (2), (3), (4)

$3 \cdot 5 \cdot 7 \cdot 13 \mid n^{13} - n$

$\Rightarrow 1365$

$5 \nmid n$ $n^{\phi(5)} \equiv 1 \bmod 5$

$n^4 \equiv 1 \bmod 5$

$n^{12} \equiv 1 \bmod 5$

$\boxed{n^{13} \equiv n \bmod 5}$ (2)

Primitive roots

$7 \nmid n$ $n^{\phi(7)} \equiv 1 \bmod 7$

$n^6 \equiv 1 \bmod 7$

$n^{12} \equiv 1 \bmod 7$

$\boxed{n^{13} \equiv n \bmod 7}$ (3)

$13 \nmid n$ $n^{12} \equiv 1 \bmod 13$

$\boxed{n^{13} \equiv n \bmod 13}$ (4)

Διοφαντική εξίσωση

$286x + 528 = \dots$

$(286, 528) = 22$

Δεν διαιρεί το σωστό

(c)

Άλλα είναι ομοιό

$528 = 286(1) + 242$

$286 = 242(1) + 44$

$242 = 44 \cdot 5 + 22$

$44 = 22(2) + 0$

$22 = 242 - 44 \cdot 5 =$

$= 242 - (286 - 242) \cdot 5 =$

$= 242 - 286 \cdot 5 + 242 \cdot 5 =$

$= 6 \cdot 242 - 286 \cdot 5 =$

$= -286 \cdot 5 + 6 \cdot 242 =$

$= 286(-5) + 6(528 - 286)$

$= -5286 + 6 \cdot 286 + 6 \cdot 528$

$-11\,286 + 5 \cdot 528$

$$22 = 286(-11) + 6528(5)$$

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} = \begin{cases} x = -11 + \frac{528}{22}t \\ y = 6 - \frac{286}{22}t \end{cases}$$

1124

$11 \quad 13$

$$\begin{cases} x = -11 + 24t \\ y = 6 - 13t \end{cases}$$

14394

Άσκηση 12

Βρείτε έναν αριθμό ο οποίος είναι πολλαπλάσιο του 11 και δίνει υπόλοιπο 1 όταν διαιρεθεί με τους αριθμούς 2, 3, 5 και 7

Λύση

Άρα καταλήγω στο σύστημα

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod{11} \end{cases}$$

$(2, 3, 5, 7, 11) = 1$

Τα 2, 3, 5, 7, 11 είναι σχετικά πρώτοι ανά δύο

Chinese remainder theorem

$$M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$

$$M_1 = \frac{M}{2} = 1155 \,, \quad M_2 = \frac{M}{3} = 770 \,, \quad M_3 = \frac{M}{5} = 462 \,, \quad M_4 = \frac{M}{7} = 330$$

και $M_5 = \frac{M}{11} = 210$

$1155 x_1 \equiv 1 \pmod 2 \Rightarrow x_1 \equiv 1 \pmod 2 \Rightarrow x_1 = 1$

$770 x_2 \equiv 1 \pmod 3 \Rightarrow 2x_2 \equiv 1 \pmod 2 \Rightarrow x_2 = 2$

$462 x_3 \equiv 1 \pmod 5 \Rightarrow 2x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 3$

$330 x_4 \equiv 1 \pmod 7 \Rightarrow x_4 \equiv 1 \pmod 7 \Rightarrow x_4 = 1$

$210 \cdot x_5 \equiv 0 \pmod 7 \Rightarrow x_5 \equiv 0 \pmod 7 \Rightarrow x_5 = 0$

Άρα $x_0 = 1155 + 2 \cdot 770 + 462 \cdot 3 + 330 \cdot 1 + 0 \pmod{2310}$

$\Rightarrow x_0 \equiv 4411 \pmod{2310}$

Όπου $x \equiv 2101 \pmod{2310}$

Και αλλά το $2101 = 11 \cdot 191 + 0$ Άρα ο $x = 2101$.

Να δείξετε ότι:

$$\sum_{k|n} \sigma(k)\left|\mu\left(\frac{n}{k}\right)\right| = n$$

Απόδειξη

Γράφουμε ότι $\sigma(n) = \sum_{k|n} k = \sum_{k|n} \frac{n}{k} = n\sum_{k|n} \frac{1}{k}$

Άρα: $\sigma(n) = \sum_{k|n} k \quad (2)$

Ο γενικός τύπος αντιστροφής του Möbius είναι:

$$F(n) = \sum_{k|n} f(k) \Longrightarrow f(n) = \sum_{k|n} F(k)\left|\mu\left(\frac{n}{k}\right)\right| \quad (1)$$

Άρα $(2) \xrightarrow{(1)} F(n) = \sigma(n)$, $f(k) = k$

$$n = \sum_{k|n} \sigma(k)\cdot\left|\mu\left(\frac{n}{k}\right)\right| \quad \square.$$

Να δείξετε ότι

$$\sum_{k|n} T(k)\left|\mu\left(\frac{n}{k}\right)\right| = 1$$

Γνωρίζουμε από την θεωρία ότι $T(n) = \sum_{k|n} 1$

το $f(k) = 1$ (σταθερή συνάρτηση)

$$F(n) = T(n)$$

Άρα βάσει του αντίστροφου μετασχηματισμού Möbius γίνεται

$$f(n) = \sum_{k|n} F(k)\left|\mu\left(\frac{n}{k}\right)\right|$$

$$1 = \sum_{k|n} T(k)\left|\mu\left(\frac{n}{k}\right)\right| \quad \square.$$

Να υπολογιστούν τα αθροίσματα a) $\sum_{k/n} \frac{\mu(k)}{k}$, b) $\sum_{k/n} \mu(k)T(k)$, c) $\sum_{k/n} \mu(k)\sigma(k)$

και d) $\sum_{k/n} k\mu(k)$.

Λύση.

a) Το $\phi(n) = \sum_{k/n} \mu(k)\frac{n}{k} = n\sum_{k/n}\frac{\mu(k)}{k}$ Από θεωρία (Βασικό - Apostol)

Άρα $\phi(n) = n\sum_{k/n}\frac{\mu(k)}{k} \Rightarrow$

$$\boxed{\sum_{k/n}\frac{\mu(k)}{k} = \frac{\phi(n)}{n}}$$

για $n = p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_r^{a_r}$

Αν $n=1 \Rightarrow \sum_{k/1}\frac{\mu(k)}{k} = \frac{\phi(1)}{1} = \frac{1}{1} = 1.$

b) $\sum_{k/n}\mu(k)T(k) = (1-T(p_1))\cdot(1-T(p_2))\cdot\ldots\cdot(1-T(p_m)) = (-1)^m$

c) $\sum_{k/n}\mu(k)\sigma(k) = (1-\sigma(p_1))\cdot(1-\sigma(p_2))\cdot\ldots(1-\sigma(p_m)) =$

$= (1-(p_1+1))\cdot(1-(p_2+1))\cdot\ldots\cdot(1-(p_m+1)) =$

$= (-1)^m p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_m$

d) $\sum_{k/n} k\mu(k) = (1-f(p_1))\cdot(1-f(p_2))\cdot\ldots\cdot(1-f(p_m)) =$

$= (1-p_1)\cdot(1-p_2)\cdot\ldots\cdot(1-p_m)$ □

Άσκηση 4

(1) Για τις τιμές του $n \in \mathbb{N}$ ο αριθμός $\phi(n)$ είναι περιττός.

Για $n=1$ και $n=2$

$$\begin{cases} \phi(1)=1 \\ \phi(2)=1 \end{cases}$$ Προφανώς

Εάν $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

Άρα το $\phi(n) = n\left(1-\frac{1}{a_1}\right)\cdot\left(1-\frac{1}{a_2}\right)\cdot \cdots \cdot\left(1-\frac{1}{a_k}\right)$ -2)

Παρατηρώ πως εάν οι αριθμοί των αναγράφονται στην παραγοντική ανάλυση του $n = m \cdot k$, $(m,k)=1$ τότε το $\phi(n)$ είναι άρτιο

δηλαδή $\phi(n) = 2k$ πχ $\phi(15) = \phi(3\cdot 5) = \phi(3)\cdot\phi(5) = 2\cdot 4 = 8$:K

Εάν τώρα $n = 2^m k$ με k περιττός με $m \geq 1$

Έστω $k=1 \Rightarrow n = 2^m$

$$\phi(n) = \phi(2^m) = 2^m\left(1-\frac{1}{2}\right) = 2^{m-1}$$

Άρα ο $\phi(n)$ πάλι άρτιος

Εάν το $k \geq 3$ και $(2^m, k) = 1$ Άρα $\phi(2^m, k) = \phi(2^m)\cdot\phi(k)$ είναι πολλαπλασιαστική

άρτιος.

Άρα ο τύπος αριθμών των οποίων περιττό αριθμό είναι το $n = 1, 2$

Άσκηση 4

(2) Να δείξετε ότι υπάρχουν άπειροι n τ.ω $\phi(n) = 2, 4, 6, 8, 10, 12$

Λύση

Έχουμε ότι για το $\phi(n) = 2$

Άρα το n μπορεί να είναι $n = 3, 4, 6$

Διότι
$\phi(3) = 3 - 1 = 2$
$\phi(4) = 4 \cdot \left(1 - \frac{1}{2}\right) = 4 \cdot \frac{1}{2} = 2$
$\phi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6\left(\frac{1}{2}\right) \cdot \left(\frac{2}{3}\right) = 2$

Όταν το $\phi(n) = 4$
$\phi(5) = 4$
$\phi(8) = 4$

Όταν το $\phi(n) = 6$
$\phi(7) = 6$
$\phi(9) = 6$
$\phi(14) = 6$
$\phi(18) = 6$
$\phi(20) = 6$

$\phi(n) = 8$
$\phi(16) = 8$
$\phi(15) = 8$
$\phi(24) = 8$
$\phi(30) = 8$

$\phi(n) = 10$
$\phi(11) = 10$
$\phi(22) = 10$

$\phi(n) = 12$
$\phi(13) = 12$
$\phi(26) = 12$
$\phi(28) = 12$

α' τρόπος

Γενικά το $\phi(n)$ όπως το n δεν είναι πρώτος αριθμός $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_l^{n_l}$

το ~~εκφράσαμε~~ εκφράσαμε και ως $\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_l}\right)$ (1)

αλλα καλως είναι: $\phi(n) = p_1^{n_1-1}\cdot p_2^{n_2-1}\cdot\ldots\cdot p_l^{n_l-1}\cdot(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_l-1)$ (2)

Θα χρησιμοποιήσουμε την (2)

Άρα $k = p_1^{m_1} p_2^{m_2}\cdot\ldots\cdot p_k^{m_k}$ και το $n = p_1^{n_1}\cdot\ldots\cdot p_k^{n_k} p_{k+1}^{n_{k+1}}\cdot\ldots\cdot p_l^{n_l}$ *

Το $\phi(k) = p_1^{m_1-1} p_2^{m_2-1} p_k^{m_k-1}(p_1-1)\cdot\ldots\cdot(p_k-1)$

και $\phi(n) = p_1^{n_1-1} p_2^{n_2-1}\cdot\ldots\cdot p_k^{n_k-1}(p_1-1)\ldots(p_k-1)p_k^{n_{k+1}-1}\ldots p_l(p_{k+1}-1)\ldots(p_l-1)$

* $n_i \geq m_i$ $1\leq i\leq k$ και $n_i \geq 1$ για $k+1<i<l$

Άρα παίρνουμε το αποτέλεσμα ότι το $\phi(k) \mid \phi(n)$ από το γεγονός ότι $n_i \geq m_i, 1\leq i\leq k$.

β' τρόπος

Γενικά στην αριθμοθεωρία και πολλά βιβλία στην θεωρία συναρτήσεων φ του Euler

Ξέρουμε ότι είναι πολλαπλασιαστική συνάρτηση μια βασική ιδιότητα είναι ότι

$$\phi(kn) = \phi(k)\cdot\phi(n) \quad \text{με } (k,n) = 1.$$

Αλλά θα ~~χρη~~ υπάρχει και μια πιο γενική σχέση η εξής

$$\phi(kn) = \phi(k)\phi(n)\left(\frac{d}{\phi(d)}\right) \quad d = (k,n) \text{ **}$$

(φαίνεται πανεύκολο, άχρηστο σαν ιδέα αλλά θα την χρησιμοποιήσουμε να το δείξουμε)

Ξέρουμε ότι το k/n τι σημαίνει αυτό δηλαδή $n = ck$ με $1\leq c\leq n$

Αν το $c=n$ και $k=1$. Είναι το τετριμμένο

Έστω ότι $c<n$. Άρα από την ** έχουμε ότι $\phi(n) = \phi(ck) =$

$$= \phi(c)\cdot\phi(k)\cdot\frac{d}{\phi(d)} = d\,\phi(c)\cdot\frac{\phi(k)}{\phi(d)} \quad (3)$$

ξέρουμε ότι το $\phi(1)=1$ (πάντα!)

Να δειχθεί ότι $\sum_{k|n} \sigma(k^{h-1})\,\phi(k) = n^h$

Λύση

Γνωρίζουμε ότι $\sigma_h(n) = \sum_{k|n} k^h$

$F(n) = \sigma_h(n)$

$f(k) = k^h$

Από θεώρημα αντιστροφής του Möbius έχουμε ότι

$$k^h = \sum_{k|n} \sigma(k^{h-1})\,\mu(n)\,\frac{k}{n} = \sum_{k|n} \sigma(k^{n-1}) \cdot \phi(k).$$

Το $\phi(m)/\phi(c)$ αφού m/c Από την (3) έχουμε ότι το δεξί μέλος πολλαπλασιάζεται με το $\phi(n)$ όπως το $\varphi(n)/\phi(n)$ Άρα έχουμε αυτό που θέλαμε να δείξουμε.

6. Άσκηση 6

Θυμίζουμε ότι ένας φυσικός αριθμός n καλείται τέλειος εάν είναι ίσος με το άθροισμα των γνησίων διαιρετών του. Αν n είναι ένας τέλειος άρτιος αριθμός να δείξετε ότι

$$\sum_{m/n} \frac{1}{m} = 2.$$

Λύση

Γνωρίζουμε ότι ο n είναι ένας τέλειος αριθμός άρα

$$\sigma(n) = 2n \Rightarrow \sum_{m/n} m = 2n \Rightarrow n\left(\sum_{m/n} \frac{1}{m}\right) = 2n$$

$$\Rightarrow \sum_{m/n} \frac{1}{m} = 2.$$

Άσκηση 7

Να δείξετε ότι:

$$\sum_{m/n} \frac{\mu^2(m)}{\phi(m)} = \frac{n}{\phi(m)}$$ (εδώ υπάρχει λάθος τυπογραφικό)

Το πολλαπλό n $\phi(m)$ ← Δεν μπορεί να είναι $\phi(m)$ αλλά $\phi(n)$

Άρα η σωστή διατύπωση της Άσκησης είναι

$$\sum_{m/n} \frac{\mu^2(m)}{\phi(m)} = \frac{n}{\phi(n)}$$

Λύση

$$\sum_{m/n} \frac{\mu^2(m)}{\phi(m)} = \prod_{i=1}^{k} \sum_{j=0}^{a_i} \frac{\mu^2(p_i^j)}{\varphi(p_i^j)} = \prod_{i=1}^{k} \left(1 + \frac{1}{p_i - 1}\right) = \prod_{i=1}^{k} \frac{1}{1 - \frac{1}{p_i}} = \frac{n}{\varphi(n)}$$

$m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$.

Ον. Γκούμας Ευάγγελος

Άσκηση

(1) Έστω m,n δύο φυσικοί αριθμοί έτσι ώστε $(m,n)=1$. Δείξτε ότι $m^{\phi(n)}+n^{\phi(m)} \equiv 1 \bmod m\cdot n$

Λύση

Από το Θεώρημα Euler-Fermat $a^{\phi(n)} \equiv 1 \pmod n$

$$\begin{cases} m^{\phi(n)} \equiv 1 \bmod n \\ \text{και} \\ n^{\phi(m)} \equiv 1 \bmod m \end{cases} \iff \begin{cases} m^{\phi(n)}-1 \equiv 0 \bmod n \\ \\ n^{\phi(m)}-1 \equiv 0 \bmod n \end{cases} \iff \begin{cases} n \mid m^{\phi(n)}-1 \\ \\ m \mid n^{\phi(m)}-1 \end{cases}$$

$$n\cdot m \mid (m^{\phi(n)}-1)\cdot(n^{\phi(m)}-1) = m^{\phi(n)}n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1 =$$

$$= m^{\phi(n)}n^{\phi(m)} - (m^{\phi(n)} + n^{\phi(m)} - 1)$$

$$\to m\cdot n \mid m^{\phi(n)} + n^{\phi(m)} - 1 \quad \text{Άρα } m^{\phi(m)}+n^{\phi(m)} \equiv 1 \bmod (m\cdot n)$$

(2) Έστω p,q δύο πρώτοι όπου $p \neq q$. Δείξτε ότι

(a) $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$

(b) $(p-1) \mid (q-1)$ και $(a, pq) = 1$ τότε $a^{q-1} \equiv 1 \bmod pq$

Λύση

(a) Απλά για $m=p$ και $n=q$

$\phi(p) = p-1$ και $\phi(q) = q-1$ Με βάση το (1) έχουμε ότι

$$p^{\phi(q)} + q^{\phi(p)} = p^{q-1} + q^{p-1} \equiv 1 \pmod{p\cdot q}$$

Επομένως $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$

(b) Το $(p-1)/(q-1) \Rightarrow q-1 = (p-1)\cdot K.$, $(p,q)=1$

$(q,pq) = 1 \Rightarrow (a,p)\cdot(a,q) = 1$ $\begin{cases} (a,p)=1 & p \nmid a \\ (a,q)=1 & q \nmid a \end{cases}$

Από Θεώρημα Fermat.

$$\begin{cases} a^{p-1} \equiv 1 \bmod p \\ a^{q-1} \equiv 1 \bmod q \end{cases} \Rightarrow a^{(p-1)\cdot K} \equiv 1^K \pmod p \Rightarrow \begin{cases} \boxed{a^{q-1} \equiv 1 \bmod p} \to p \mid a^{q-1}-1 \\ a^{q-1} \equiv 1 \bmod q \to q \mid a^{q-1}-1 \end{cases}$$

Τα $(p,q)=1$ Άρα $p\cdot q \mid a^{q-1}-1 \Rightarrow$

$$\Rightarrow a^{q-1} \equiv 1 \bmod p\cdot q$$

Ασκηση 14

14394

Α.

$m_1 = 3,\ m_2 = 5,\ m_3 = 7$

$(3,5,7) = 1$

$M = 3 \cdot 5 \cdot 7 = 15 \cdot 7 = 105$

$$\begin{cases} x \equiv a_1 \bmod 3 \\ x \equiv a_2 \bmod 5 \\ x \equiv a_3 \bmod 7 \end{cases}$$

Chinese remainder theorem

(Κινέζικο Θεώρημα)

$M_1 = \frac{M}{m_1} = \frac{3 \cdot 5 \cdot 7}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{3 \cdot 5 \cdot 7}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{3 \cdot 5 \cdot 7}{7} = 15$

Αρα $x_0 35 \equiv 2 \bmod 3$

$x_0 21 \equiv 1 \bmod 5$

$x_0 15 \equiv 1 \bmod 7$

$$\begin{cases} 35 x_0 \equiv 1 \bmod 3 \\ 21 x_0 \equiv 1 \bmod 5 \\ 15 x_0 \equiv 1 \bmod 7 \end{cases} \rightarrow \begin{cases} 2 x_0 \equiv 1 \bmod 3 \\ x_0 \equiv 1 \bmod 5 \\ x_0 \equiv 1 \bmod 7 \end{cases}$$

$$x \rightarrow \begin{cases} x_0 \equiv -1 \bmod 3 \\ x_0 \equiv 1 \bmod 5 \\ x_0 \equiv 1 \bmod 7 \end{cases}$$

Αρα το $x_0 = -2 \cdot 35 a_1 + 21 a_2 + 15 a_3 = -35 a_1 + 21 a_2 + 15 a_3$ (mod 105)

Ασκηση 20

Δείξτε ότι για κάθε $n \in \mathbb{N}$ ο αριθμός $\frac{1}{5} n^5 + \frac{1}{3} n^3 + \frac{7}{15} n$ είναι ακέραιος

Λύση

$\frac{1}{5} n^5 + \frac{1}{3} n^3 + \frac{7}{15} n = \frac{3n^5}{15} + \frac{5n^3}{15} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15} \in \mathbb{Z} \Rightarrow A$

Αρκεί $15 \mid 3n^5 + 5n^3 + 7n$

$3n^5 + 5n^3 + 7n$ ο 3 αρκεί αριθμός $\forall n \in \mathbb{Z}$

$A = 3(n^5 + 2n^3 + 2n) - (n^3 - n)$

$n^3 \equiv n \pmod 3 \rightarrow \begin{cases} 3 \mid n^3 - n \\ 3 \mid 3 \cdot (n^5 + 2n^3 + 2n) \end{cases} \rightarrow 3 \mid A$

$A = 5(n^5 + n^3 + n) - 2(n^5 - n)$ ο 5 αρκεί

$n^5 \equiv n \pmod 5 \rightarrow \begin{cases} 5 \mid n^5 - n \\ 5 \mid 5 \cdot (n^5 + n^3 + n) \end{cases} \rightarrow 5 \mid A$

Αρα $15 \mid A \Rightarrow 15 \mid 3n^5 + 5n^3 + 7n$ και Αρα $\frac{1}{5} n^5 + \frac{1}{3} n^3 + \frac{7}{15} n \in \mathbb{Z}$.

$(3,5) = 1$

Άσκηση 13

Λύση

14394

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 5 \\ x \equiv 5 \bmod 6 \\ x \equiv 0 \bmod 7 \end{cases}$$

$x \equiv 3 \bmod 6 \Rightarrow x \equiv 3 \bmod 2 \cdot 3$

$\Downarrow$

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \end{cases}$$

$x \equiv 3 \bmod 4 \Rightarrow x \equiv 1 \bmod 2$

$\Rightarrow$ Το Νέο σύστημα είναι

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 5 \\ x \equiv 0 \bmod 7 \end{cases}$$

$M = 3 \cdot 4 \cdot 5 \cdot 7 = 420$

$M_1 = \frac{M}{3} = \frac{420}{3} = 140$, $M_2 = \frac{M}{4} = \frac{420}{4} = 105$, $M_3 = \frac{M}{5} = \frac{420}{5} = 84$

$M_4 = \frac{M}{7} = 60$

$140 x_1 \equiv 2 \bmod 3$, $105 x_2 \equiv 3 \bmod 4$, $84 x_3 \equiv 4 \bmod 5$, $60 x_4 \equiv 0 \bmod 7$

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

$2 x_1 \equiv 2 (\bmod 3)$ $\quad x_2 \equiv 3 (\bmod 4)$ $\quad 4 x_3 \equiv 4 (\bmod 5)$ $\quad 4 x_4 \equiv 0 (\bmod 7)$

$x_1 = 1$ $\quad x_2 = 3$ $\quad x_3 = 1$ $\quad x_4 = 0$

$x_0 = 140 + 3 \cdot 105 + 84 = 539$

$x_0 \equiv 539 (\bmod 420) \Rightarrow x \equiv 119 (\bmod 420)$

Άρα ο ελάχιστος αριθμός αρχών είναι 119 αυτά ήταν τα καλάδια.

Άσκηση 2

Δείξτε ότι αν $a, n \in \mathbb{Z}$ με $n \geq 1$ τότε το σύνολο $\{a, a+1, \ldots, a+n+1\}$ αποτελεί ένα πλήρες σύστημα υπολοίπων mod n

Λύση

$0 \leq i \leq j \leq n-1$ Το $a+i \equiv a+j \pmod n$

$\Rightarrow n \mid a+i-a-j \Rightarrow n \mid i-j \Rightarrow n \mid j-i$

Εάν $j-i \neq 0$, $n \leq j-1$ το οποίο δεν αληθεύει. γιατί $j < n$ και $i \geq 0$

Άρα $i=j$ Άρα το Είναι πλήρες σύστημα. ως mod n.

Άσκηση 6

Εάν ο m είναι σύνθετος ακέραιος με $m > 4$ δείξτε ότι $(m-1)! \equiv 0 \pmod m$

Λύση

Άρα το $m = a \cdot b$

Αν $a=b$ τότε $m = a \cdot b = a \cdot a = a^2 \Rightarrow m = a^2$

Το $m \mid (m-1)! \Rightarrow a^2 \mid (m-1)!$

Άρα το $(m-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot a \cdot \ldots \cdot (m-a) \cdot \ldots \cdot (m-1) \equiv 0 \pmod n$

Ενώ εάν $a \neq b$ τότε $m \mid (m-1)!$

$m = a \cdot b \Rightarrow a \cdot b \mid (m-1)!$ $\begin{cases} a \mid (m-1)! & \text{για } a < b \\ b \mid (m-1)! \end{cases}$

$(m-1)! = 1 \cdot 2 \cdot 3 \ldots a \cdot b \cdot m-1 \Rightarrow m \mid a \cdot b \mid (m-1)!$

$\text{ord}_7 \in \{0, 1, 2, 3, 6\}$

a) $\text{ord}_7(4) = 3$

→ $4^1 \equiv 4 \bmod 7$

$4^2 = 16 \equiv 2 \bmod 7$

$4^3 \equiv 1 \bmod 7$

b) $\text{ord}_{11}(4) = 5$ $\quad \text{ord}_{11}(4) \in \{1, 2, 5, 10\}$

$4 \equiv 4 \bmod 11$

$16 \equiv 5 \bmod 11$

$1024 \equiv 1 \bmod 11$

c) $\text{ord}_{13}(5) = 4$ $\quad \text{ord} \in \{1, 2, 3, 4, 6, 12\}$

$5^2 = 25 = 12 \bmod 13$

$5^3 = 125 \equiv 8 \bmod 13$

$n=4$ $\quad 625 \equiv 1$

d) $\text{ord}_{18}(7) = 3$ $\quad \text{ord} \in \{1, 2, 3, 6\}$

$\phi(18) = 6$

$7^{\phi} \equiv 7 \bmod \bmod 18$

$49 \equiv 13 \bmod 18$

$343 \equiv 1 \bmod 18$

e) $\text{ord}_{18}(17) = 2$ $\quad \text{ord} \in \{1, 2, 3, 6\}$

$17 \equiv 17 \bmod 18$

$289 \equiv 1 \bmod 18$

Άσκηση 6

Υπολογίστε τα $\left(\frac{1234}{4567}\right)$ και $\left(-\frac{520}{3}\right)$

Λύση

$$\left(\frac{1234}{4567}\right) = \left(\frac{2\cdot 617}{4567}\right) = \left(\frac{2}{4567}\right)\left(\frac{617}{4567}\right) = (-1)^{\frac{4567^2-1}{8}}\left(\frac{617}{4567}\right) =$$

$$= (-1)^{\frac{4567^2-1}{8}}(-1)^{\frac{4567-1}{2}\cdot\frac{617-1}{2}}\left(\frac{4567}{617}\right) = \left(\frac{248}{617}\right) =$$

$$= \left(\frac{2}{617}\right)^3\left(\frac{31}{617}\right) = (-1)^{\frac{617^2-1}{8}}\cdot\left(\frac{31}{617}\right) =$$

$$= (-1)^{\frac{617^2-1}{8}}(-1)^{\frac{617-1}{2}\cdot\frac{31-1}{2}}\left(\frac{617}{31}\right) =$$

$4567 \equiv 248 \bmod(617)$

$$= \left(\frac{248}{31}\right) = \left(\frac{2^3\cdot 7}{31}\right) = \left(\frac{2^2}{31}\right)\left(\frac{7}{31}\right) =$$

$$= (-1)^{\frac{31^2-1}{8}}\cdot(-1)^{\frac{31-1}{2}\cdot\frac{7-1}{2}}\left(\frac{31}{7}\right) =$$

$$= -\left(\frac{3}{7}\right) = -(-1)^{\frac{7-1}{2}\cdot\frac{3-1}{2}}\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(-\frac{520}{3}\right) = \left(-\frac{1}{3}\right)\left(\frac{520}{3}\right) = (-1)^{\frac{3-1}{2}}\left(\frac{520}{3}\right) = (-1)^{\frac{3}{2}}\left(\frac{520}{3}\right) =$$

$$= -\left(\frac{520}{3}\right) = -\left(\frac{4\cdot 10\cdot 13}{3}\right) = -\left(\frac{4\cdot 2\cdot 5\cdot 13}{3}\right) =$$

$$= -\left(\frac{2}{3}\right)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{2}{3}\right)\left(\frac{5}{3}\right)\left(\frac{13}{3}\right) =$$

$$= -(-1)\cdot(-1)\cdot(-1)\cdot(-1)\cdot 1 = -(1)\cdot(1)\cdot(1) = -1$$

$$\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = (-1)^{\frac{9-1}{8}} = (-1)^{\frac{8}{8}} = -1$$

$$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Για το $x^2 \equiv -154 \bmod 163$ $\left(\frac{-154}{163}\right) = 1$. $154 R_{163}$.

$$\left(\frac{-154}{163}\right) = \left(\frac{-1}{163}\right)\cdot\left(\frac{154}{163}\right) = (-1)^{\frac{163-1}{2}}\left(\frac{154}{163}\right) = (-1)^{81}\left(\frac{154}{163}\right) =$$

$$= -1\cdot\left(\frac{154}{163}\right) = -1\left(\frac{2\cdot 7\cdot 11}{163}\right) = -1\left(\frac{2}{163}\right)\cdot\left(\frac{7}{163}\right)\cdot\left(\frac{11}{163}\right) =$$

$$= -1\cdot(-1)^{\frac{163^2-1}{8}}\cdot(-1)^{\frac{7-1}{2}\cdot\frac{163-1}{2}}\left(\frac{163}{7}\right)\cdot(-1)^{\frac{163-1}{2}\cdot\frac{11-1}{2}}\left(\frac{163}{11}\right) = (-1)\cdot(-1)^{3321}$$

$$\cdot(-1)^{3\cdot 81}\left(\frac{163}{7}\right)\cdot(-1)^{81\cdot 5}\left(\frac{163}{11}\right) = (-1)\cdot(-1)\cdot(-1)^{243}\left(\frac{163}{7}\right)\cdot(-1)^{405}\left(\frac{163}{11}\right) =$$

$$= (1)(-1)\left(\frac{163}{7}\right)\cdot(-1)\left(\frac{163}{11}\right) = (-1)\cdot(-1)\left(\frac{163}{7}\right)\left(\frac{163}{11}\right) = \left(\frac{163}{7}\right)\left(\frac{163}{11}\right) =$$

$$= \left(\frac{2}{7}\right)\cdot\left(\frac{9}{11}\right) = \left(\frac{2}{7}\right)\cdot\left(\frac{3}{11}\right)\cdot\left(\frac{3}{11}\right) = (-1)^{\frac{7^2-1}{8}}\cdot(-1)^{\frac{11-1}{2}\cdot\frac{3-1}{2}}\left(\frac{11}{3}\right)(-1)^{\frac{11-1}{2}\cdot\frac{2-1}{2}}\left(\frac{11}{3}\right) = \text{πρότυπο}$$

ΠΑΡΑΔΕΙΓΜΑ 1 Να λυθεί η ισοδυναμία $5x \equiv 3 \pmod{24}$.

Λύση

Από το ότι $(5, 24) = 1$, έπεται ότι υπάρχει μοναδική λύση. Χρησιμοποιώντας τη (10), βρίσκουμε

$$x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^7 \pmod{24}$$

διότι $\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4$. Modulo 24 έχουμε $5^2 \equiv 1$, και

$$5^4 \equiv 5^6 \equiv 1, \qquad 5^7 \equiv 5, \text{ οπότε } x \equiv 15 \pmod{24}.$$

ΠΑΡΑΔΕΙΓΜΑ 2 Να λυθεί η ισοδυναμία $25x \equiv 15 \pmod{120}$.

Λύση

Από το ότι $d = (25, 120) = 5$ και $d \mid 15$, έπεται ότι η ισοδυναμία έχε
ακριβώς πέντε λύσεις modulo 120. Για να τις βρούμε, διαιρούμε με τον
και λύνουμε την ισοδυναμία $5x \equiv 3 \pmod{24}$. Χρησιμοποιώντας το Πα
ράδειγμα 1 και το Θεώρημα 5.14, βρίσκουμε ότι οι πέντε λύσεις δίνοντ
από την $x = 15 + 24k$, $k = 0, 1, 2, 3, 4$, δηλ.

$$x \equiv 15, 39, 63, 87, 111 \pmod{120}.$$

(α) Να δείξω $\sum_{k=1}^{n} \mu(k!) = 1$ $n \geq 3$.

$\mu(1!) = \mu(1) = 1$

$\mu(2!) = \mu(2) = (-1)^1 = -1$

$\mu(3!) = \mu(1 \cdot 2 \cdot 3) = (-1)^2 = 1$

$\mu(4!) = \mu(1 \cdot 2 \cdot 3 \cdot 4) = \mu(2^3 \cdot 3) = 0$

Άρα για $n \geq 3$ το $2^2 / n!$ και άρα $\mu(n!) = 0$

Επομένως $\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) + \ldots + \mu(4!)$

$= 1 + (-1) + 1 + 0 + \ldots + 0 = 1.$

Αυτό που ήθελα να δείξω.

(43)

$ord_{43}(a) \in \{1, 2, 3, 6, 7, 14, 21, 42\}$

$\phi(43) = 42 - 1$.

$3^7 \equiv -6 \bmod 43$

$3^{14} \equiv 36 \bmod 43$

$3^{21} \equiv -1 \bmod 43$

$3^{42} \equiv 1 \bmod 43$

$\hookrightarrow ord_{43}(3) = 42 = \phi(43)$

11 / 10! + 1

$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 + 1$

$1 \cdot 12 \cdot 12 \cdot 45 \cdot 56 \cdot 10 + 1$

$1 \quad 1 \quad 1 \quad 1 \quad (-1) + 1 = 0$ (mod 11)

$11 / 10! + 1.$

$\frac{5^{100}}{7}$

5^{100}

$5^{\phi(7)} \equiv 1 \bmod 7$ $\quad (5,7)=1$ $\quad 7 \nmid 5$

$5^6 \equiv 1 \bmod 7$

$100 \mid 6$
$\frac{6}{40}$
$\frac{36}{4}$

$(5^6)^{16} \equiv 1 \bmod 7$

$(5^6)^{16} \cdot 5^4 \equiv 5^4 \bmod 7$

$5^{100} \equiv 2 \bmod 7$

25^2
$625 \mid 7$

42

$\frac{6^{2000}}{11} \Rightarrow$

$6^{\phi(11)} \equiv 1 \bmod 11$

$\phi(11) = 10$

$6^{10} \equiv 1 \bmod 11$

$6^{1000} \equiv 1 \bmod 11$

Άσκηση 1. (1) *Να λυθεί η γραμμική Διοφαντική εξίσωση:*

$$13521x + 732y = 11225 \tag{1}$$

(2) *Να βρεθούν:* (α) *όλες οι λύσεις, και* (β) *όλες οι θετικές λύσεις, της γραμμικής Διοφαντικής εξίσωσης*

$$17x + 19y = 23 \tag{2}$$

Λύση. (1) *Από την Θεωρία γνωρίζουμε ότι η διοφαντική εξίσωση* (1) *έχει λύση αν και μόνον αν* $d \mid 11225$, *όπου* $d = (13521, 732)$.

Με χρήση του αλγόριθμου του Ευκλείδη, υπολογίζουμε:

$$\begin{aligned} 13521 &= 18 \cdot 732 + 345 \\ 732 &= 2 \cdot 345 + 42 \\ 345 &= 8 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 1 \cdot 3 + 0 \end{aligned}$$

και επομένως $d = (13521, 732) = 3$.

Επειδή προφανώς $3 \nmid 11225$, *έπεται ότι η Διοφαντική εξίσωση* (1) *δεν έχει ακέραιες λύσεις.*

(2) *Από την Θεωρία γνωρίζουμε ότι η διοφαντική εξίσωση* (2) *έχει λύση αν και μόνον αν* $d \mid 23$, *όπου* $d = (19, 17)$. *Επειδή προφανώς* $d = (19, 17) = 1$ *και* $1 \mid 23$, *έπεται ότι η Διοφαντική εξίσωση* (2) *έχει ακέραιες λύσεις.*

Γνωρίζουμε ότι αν (x_0, y_0) *είναι μια ακέραια λύση μιας Διοφαντικής εξίσωσης* $ax + by = c$, *όπου* $d \mid (a, b)$, *τότε όλες οι λύσεις της* (2) *δίνονται από τους τύπους:*

$$x = x_0 + \frac{b}{d}t \quad \& \quad y = y_0 - \frac{a}{d}t, \qquad t \in \mathbb{Z}$$

Για την εύρεση μιας λύσης (x_0, y_0) *της* (2), *εργαζόμαστε ως εξής.*

Με χρήση του αλγόριθμου του Ευκλείδη, υπολογίζουμε:

$$\begin{aligned} 19 &= 1 \cdot 17 + 2 \\ 17 &= 2 \cdot 8 + 1 \\ 8 &= 1 \cdot 8 + 0 \end{aligned}$$

Από τις παραπάνω σχέσεις, θα έχουμε:

$$1 = 17 - 2 \cdot 8 = 17 - 8 \cdot (19 - 17) = 17 \cdot 9 + 19 \cdot (-8)$$

και τότε

$$23 = 23 \cdot 1 = 23 \cdot (17 \cdot 9 + 19 \cdot (-8)) = 17 \cdot (23 \cdot 9) + 19 \cdot (-8 \cdot 23) = 17 \cdot 207 + 19 \cdot (-184)$$

Επομένως, θέτοντας $x_0 = 207$ & $y_0 = -184$

αποκτούμε μια λύση της (2).
Από την παραπάνω ανάλυση, έπεται ότι όλες οι ακέραιες λύσεις της (2) είναι οι εξής:

$$x = 207 + 19t \quad \& \quad y = -184 - 17t, \quad t \in \mathbb{Z}$$

Για την εύρεση όλων των θετικών λύσεων της (2), εργαζόμαστε ως εξής. Η λύση (x, y) είναι θετική αν και μόνον αν, εξ' ορισμού, ισχύει $x > 0$ και $y > 0$. Επομένως

$$207 + 19t > 0 \quad \& \quad -184 - 17t > 0 \implies -\frac{207}{19} < t < -\frac{184}{17}$$

Επειδή $\frac{207}{19} = 10.82...$ και $\frac{184}{17} = 10.89....$ θα έχουμε

$$-10.82... < t < -10.89...$$

Επειδή οι θετικές ακέραιες λύσεις της (2) δίνονται από το σύνολο

$$\{(207 + 19t, -184 - 17t) \mid -10.82... < t < -10.89...\} \cap \mathbb{Z}$$

το οποίο είναι προφανώς κενό, έπεται ότι η (2) δεν έχει θετικές ακέραιες λύσεις (κάτι το οποίο μπορούσε να διαπιστωθεί εύκολα από την αρχή λόγω της μορφής της Διοφαντικής εξίσωσης). □

Άσκηση 2. *Να βρεθούν τα υπόλοιπα των διαιρέσεων:*

$$\frac{17^{2241}}{8700} \qquad \& \qquad \frac{n^{257} - n}{255}, \quad n \in \mathbb{Z}$$

Λύση. (1) *Εύκολα βλέπουμε ότι η πρωτογενής ανάλυση του αριθμού* 8700 *είναι:*

$$8700 = 2^2 \cdot 3 \cdot 5^2 \cdot 29$$

απ' όπου βλέπουμε άμεσα ότι:
(α') $(8700, 17) = 1$.
(β') $\phi(8700) = \phi(2^2 \cdot 3 \cdot 5^2 \cdot 29) = \phi(2^2) \cdot \phi(3) \cdot \phi(5^2)\phi(\cdot 29) = 2240$.
Επειδή $(8700, 17) = 1$, *από το Θεώρημα του Euler, τότε θα έχουμε:*

$$17^{\phi(8700)} \equiv 1 \,(\mathrm{mod}\, 8700) \implies 17^{2240} \equiv 1 \,(\mathrm{mod}\, 8700)$$

Πολλαπλασιάζοντας την τελευταία ισοτιμία με 17, *θα έχουμε*

$$17^{2241} \equiv 17 \,(\mathrm{mod}\, 8700)$$

και επομένως το υπόλοιπο της διαίρεσης του αριθμού 17^{2241} *με τον αριθμό* 8700 *είναι* 17.

(2) *Θα δείξουμε ότι το υπόλοιπο της διαίρεσης του αριθμού* $n^{257} - n$ *με τον αριθμό* 255 *είναι* 0 *ή ισοδύναμα θα δείξουμε ότι:*

$$n^{257} \equiv n \,(\mathrm{mod}\, 255) \qquad (*)$$

Εύκολα υπολογίζουμε ότι η πρωτογενής ανάλυση του αριθμού 255 *είναι:*

$$255 = 3 \cdot 5 \cdot 17$$

Επειδή οι αριθμοί $2, 5, 17$ *είναι ανα δύο πρώτοι μεταξύ τους,για να δείξουμε την σχέση* $(*)$, *αρκεί να δείξουμε ότι:*

$$3 \mid n^{257} - n \quad \& \quad 5 \mid n^{257} - n \quad \& \quad 17 \mid n^{257} - n \qquad (**)$$

Η απόδειξη τών σχέσεων διαιρετότητας $(**)$ *είναι παρόμοια:*

- *Διακρίνουμε περιπτώσεις:*
  (α') *Αν* $3 \mid n$, *τότε* $n \equiv 0 \,(\mathrm{mod}\, 3)$ *και άρα* $n^{257} \equiv 0 \,(\mathrm{mod}\, 3) \equiv n (\mathrm{mod}\, 3)$. *Επομένως* $3 \mid n^{257} - n$.

(β') *Αν* $3 \nmid n$, *τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:*

$$n^{\phi(3)} \equiv 1 \pmod 3 \implies n^2 \equiv 1 \pmod 3$$

και τότε

$$(n^2)^{128} \equiv n^{256} \equiv 1 \pmod 3 \implies n^{257} \equiv n \pmod 3$$

Άρα αν $3 \nmid n$, *πάλι θα έχουμε ότι* $3 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$3 \mid n^{257} - n \tag{a}$$

- *Διακρίνουμε περιπτώσεις:*

  (α') *Αν* $5 \mid n$, *τότε* $n \equiv 0 \pmod 5$ *και άρα* $n^{257} \equiv 0 \pmod 5 \equiv n \pmod 5$. *Επομένως* $5 \mid n^{257} - n$.

  (β') *Αν* $5 \nmid n$, *τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:*

$$n^{\phi(5)} \equiv 1 \pmod 5 \implies n^4 \equiv 1 \pmod 5$$

και τότε

$$(n^4)^{64} \equiv n^{256} \equiv 1 \pmod 5 \implies n^{257} \equiv n \pmod 5$$

Άρα αν $5 \nmid n$, *πάλι θα έχουμε ότι* $5 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$5 \mid n^{257} - n \tag{b}$$

- *Διακρίνουμε περιπτώσεις:*

  (α') *Αν* $17 \mid n$, *τότε* $n \equiv 0 \pmod{17}$ *και άρα* $n^{257} \equiv 0 \pmod{17} \equiv n \pmod{17}$. *Επομένως* $17 \mid n^{257} - n$.

  (β') *Αν* $17 \nmid n$, *τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:*

$$n^{\phi(17)} \equiv 1 \pmod{17} \implies n^{16} \equiv 1 \pmod{17}$$

και τότε

$$(n^{16})^{16} \equiv n^{256} \equiv 1 \pmod{17} \implies n^{257} \equiv n \pmod{17}$$

Άρα αν $17 \nmid n$, *πάλι θα έχουμε ότι* $17 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$17 \mid n^{257} - n \tag{c}$$

Από τις σχέσεις $(a), (b)$ *και* (c), *έπεται ότι*

$$3 \cdot 5 \cdot 17 = 255 \mid n^{257} - n$$

Επομένως το υπόλοιπο της διαίρεσης του αριθμού $n^{257} - n$ *με τον αριθμό* 255 *είναι* 0. □

Άσκηση 6. (1) *Αν ο n είναι περιττός και $3 \nmid n$, τότε:* $n^2 \equiv 1 \pmod{24}$.
(2) *Αν* $(a, 35) = 1$, *δείξτε ότι:* $35 \mid a^{12} - 1$.

Λύση. (1) *Επειδή* $3 \nmid n$, *από το μικρό Θεώρημα του Fermat, έπεται ότι* $n^{\phi(3)} \equiv n^2 \equiv 1 \pmod{3}$. *Επομένως θα έχουμε*

$$3 \mid n^2 - 1 \qquad (a)$$

Από την άλλη πλευρά επειδή ο αριθμός n είναι περιττός, θα έχουμε $n = 2k + 1$, για κάποιον ακέραιο k. Τότε

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \implies n^2 - 1 = 4k(k+1)$$

Επειδή, όπως γνωρίζουμε το γινόμενο δύο διαδοχικών ακεραίων διαιρείται από το 2, θα έχουμε $2 \mid k(k+1)$ Τότε όμως η παραπάνω σχέση δίνει ότι:

$$8 \mid n^2 - 1 \qquad (b)$$

Επειδή $(3, 8) = 1$, *από τις σχέσεις (a) και (b) έπεται ότι*

$$3 \cdot 8 = 24 \mid n^2 - 1$$

και επομένως $$n^2 \equiv 1 \pmod{24}$$

(2) Επειδή $(a, 35) = 1$, θα έχουμε προφανώς

$$(a, 5) = 1 = (a, 7)$$

και τότε από το μικρό Θεώρημα του Fermat θα έχουμε:

$$a^{\phi(5)} \equiv a^4 \equiv 1 \pmod 5 \implies (a^4)^3 \equiv a^{12} \equiv 1 \pmod 5 \qquad (a)$$

και

$$a^{\phi(7)} \equiv a^6 \equiv 1 \pmod 7 \implies (a^6)^2 \equiv a^{12} \equiv 1 \pmod 7 \qquad (b)$$

Οι σχέσεις (a) και (b) γράφονται ισοδύναμα ως εξής:

$$5 \mid a^{12} - 1 \quad \& \quad 7 \mid a^{12} - 1$$

Επειδή $(5, 7) = 1$ οι παραπάνω σχέσεις δίνουν το ζητούμενο

$$5 \cdot 7 = 35 \mid a^{12} - 1 \qquad \square$$

Άσκηση 7. *Αν p είναι ένας πρώτος με $p > 5$, δείξτε ότι ο αριθμός*

$$(p-1)! + 1$$

έχει τουλάχιστον δύο πρώτους διαιρέτες.

Λύση. *Χρειάζεται να δείξουμε ότι για πρώτο $p > 5$, ο ακέραιος $(p-1)! + 1$ δεν είναι δύναμη πρώτου. Ας υποθέσουμε ότι*

$$(p-1)! + 1 = q^k$$

για κάποιον πρώτο q και θετικό ακέραιο k και θα καταλήξουμε σε αντίφαση. Από το Θεώρημα Wilson $p \mid (p-1)! + 1 = q^k$, έτσι πρέπει να έχουμε $q = p$, δηλαδή $(p-1)! + 1 = p^k$.

Από την τελευταία σχέση έπεται ότι

$$p^k = (p-1)! + 1 < (p-1)^{p-1} < p^{p-1},$$

άρα $k < p - 1$. Αφού ο p είναι πρώτος μεγαλύτερος του 5 ο $p - 1$ είναι σύνθετος αριθμός μεγαλύτερος του 4, έτσι από την Άσκηση 7 του Φυλλαδίου 6 έχουμε ότι

$$0 \equiv (p-2)! \bmod (p-1).$$

Επίσης έχουμε

$$(p-1)! = p^k - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + p + 1)$$

που, χρησιμοποιώντας ότι $p \equiv 1 \bmod (p-1)$ συνεπάγεται ότι

$$0 \equiv (p-2)! = p^{k-1} + p^{k-2} + \cdots + p + 1 \equiv 1 + 1 + \cdots + 1 \equiv k \bmod (p-1).$$

Έτσι έχουμε $0 < k < p - 1$ και $p - 1 \mid k$ που είναι αντίφαση. Επομένως ο αριθμός $(p-1)! + 1$ έχει τουλάχιστον δύο πρώτους διαιρέτες. $\square$

Άσκηση 8. *Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού*

$$\sum_{k=1}^{2013} 7^k$$

με τον αριθμό 100.

Λύση. *Σε αυτή την άσκηση ο συμβολισμός* $[a]$ *σημαίνει* $[a]_{100}$. *Έχουμε*

$$[7^2] = [49], \qquad [7^3] = [343] = [43], \qquad [7^4] = [7][43] = [301] = [1]$$

Επομένως, αφού $[7^4] = [1]$, *με επαγωγή στο* k *έχουμε*

$$[7^{4k+i}] = [7^i]$$

για κάθε $k \geq 0$ *και* $1 \leq i \leq 4$. *Παρατηρούμε ότι* $2013 = 4 \cdot 503 + 1$. *Σαν συνέπεια*

$$\sum_{k=1}^{2013} 7^k \bmod 100 = \left(503(7 + 7^2 + 7^3 + 7^4) + 7\right) \pmod{100}$$

Αλλά

$$\left[7 + 7^2 + 7^3 + 7^4\right] = [7 + 49 + 43 + 1] = [100] = [0].$$

Επομένως

$$[\sum_{k=1}^{2013} 7^k] = [7]$$

και άρα το υπόλοιπο της διαίρεσης του $\sum_{k=1}^{2013} 7^k$ *με τον αριθμό* 100 *είναι ίσο με* 7. □

Άσκηση 9. *Αν* $n \geq 2$ *είναι ένας θετικός ακέραιος, δείξτε ότι:*

$$n \nmid 2^n - 1$$

Λύση. *Αν ο* n *είναι άρτιος, τότε η πρόταση ισχύει γιατί το* $2^n - 1$ *είναι περιττός. Υποθέτουμε ότι ο* n *είναι περιττός και* $n \mid 2^n - 1$ *και θα καταλήξουμε σε αντίφαση. Επειδή* $n \geq 2$, *ο αριθμός* n *έχει έναν πρώτο διαιρέτη. Έστω* p *ο μικρότερος πρώτος που διαιρεί το* n. *Ο συμβολισμός* $[a]$ *στα ακόλουθα σημαίνει* $[a]_p$. *Τότε* $(n, p-1) = 1$ *και άρα υπάρχουν ακέραιοι* a_1, b_1 *τέτοιοι ώστε* $a_1 n + b_1(p-1) = 1$. *Επομένως για κάθε ακέραιο* t *έχουμε*

$$1 = a_1 n + b_1(p-1) = na_1 - (p-1)(-b_1) = n(a_1 + (p-1)t) - (p-1)(-b_1 + nt)$$

Για κατάλληλα μεγάλο t *έχουμε* $a_1 + (p-1)t > 0$ *και* $-b_1 + nt > 0$. *Θέτοντας* $a = a_1 + t(p-1)$ *και* $b = -b_1 + nt$ *έχουμε ότι* $a, b > 0$ *και*

$$1 = an - b(p-1) \tag{1}$$

Αφού $2^n \equiv 1 \bmod n$ *έχουμε* $n \mid 2^n - 1$, *και επειδή* $p \mid n$, *έπεται ότι* $p \mid 2^{n-1}$, *δηλαδή:* $2^n \equiv 1 \bmod p$. *Επομένως* $[2^n] = [1]$ *και άρα* $[2^{an}] = [2^n]^a = [1]^a = [1]$. *Χρησιμοποιώντας την ισότητα (1) έχουμε ότι* $[2^{(1+b(p-1))}] = [2^{an}] = [1]$, *το οποίο συνεπάγεται ότι*

$$[2][2^{p-1}]^b = [1]. \tag{2}$$

Από το Θεώρημα Euler-Fermat έχουμε $[2^{p-1}] = [1]$ *και άρα* $[2^{p-1}]^b = [1]$, *οπότε η ισότητα (2) συνεπάγεται ότι* $[2] = [1]$ *στο σύνολο* $\mathbb{Z}_n$ *που είναι αντίφαση διότι* $n \geq 2$. *Επομένως* $n \nmid 2^n - 1$. □

Άσκηση 10. *Να λυθεί το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} x \equiv 3 \pmod{34} \\ x \equiv 5 \pmod{107} \\ x \equiv 3 \pmod{1111} \\ x \equiv 8 \pmod{38} \end{cases}$$

Λύση. *Έχουμε* $34 = 2 \cdot 17$ *και* $38 = 2 \cdot 19$. *Επομένως* $(34, 38) = 2$. *Αφού* $2 \nmid 3 - 8 = -5$ *από την Θεωρία το σύστημα είναι αδύνατο.*

Άσκηση 11. *Έστω $m_1, m_2, \cdots, m_n$ θετικοί ακέραιοι οι οποίοι είναι πρώτοι μεταξύ τους ανα δύο. Να δείξετε ότι η μοναδική λύση $(\mathrm{mod}\, m_1 m_2 \cdots m_n)$ του συστήματος γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} x \equiv a_1 \,(\mathrm{mod}\, m_1) \\ x \equiv a_2 \,(\mathrm{mod}\, m_2) \\ \quad \vdots \\ x \equiv a_n \,(\mathrm{mod}\, m_n) \end{cases}$$

είναι:

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_n M_n^{\phi(m_n)} \,(\mathrm{mod}\, M)$$

όπου

$$M = m_1 m_2 \cdots m_n \quad \& \quad M_i = \frac{M}{m_i}, \quad 1 \le i \le n$$

Λύση. *Αφού τα m_j είναι πρώτα ανά δύο, έχουμε $(M_j, m_j) = 1$ για όλα τα j, και $(M_i, m_j) = m_j$ για $i \neq j$. Επομένως, από το Θεώρημα Euler-Fermat έχουμε για κάθε j*

$$M_j^{\phi(m_j)} \equiv 1 \,\mathrm{mod}\, m_j.$$

Σαν συνέπεια, για κάθε j έχουμε

$$[x] = [a_1 M_1^{\phi(m_1)} + \cdots + a_j M_j^{\phi(m_j)} + \cdots + M_n^{\phi(m_n)}] = [0] + [0] + \cdots + [a_j \cdot 1] + [0] + \cdots + [0] = [a_j]$$

όπου για ακέραιο a ο συμβολισμός $[a]$ σημαίνει $[a]_{m_j}$. Επομένως το x ικανοποιεί το σύστημα, και άρα από το Κινέζικο Θεώρημα Υπολοίπων είναι η μοναδική λύση $\mathrm{mod}\, M$. □

Να λυθεί η τετραγωνική ισοτιμία

$x^2 + 7x + 10 \equiv 0 \pmod{11}$

Ισοτιμία $x^2 + 7x + 10 \equiv 0 \pmod{11}$ είναι ισοδύναμη με

$4x^2 + 28x + 40 \equiv (2x+7)^2 - 9 \equiv 0 \pmod{11}$

γιατί $(4, 11) = 1$ θέτουμε $y = 2x + 7$ και λύνουμε

την ισοτιμία $y^2 \equiv 9 \pmod{11}$

Προφανείς $y \equiv 3 \pmod{11}$ και $y \equiv -3 \pmod{11}$

Αρκεί λοιπόν να λύσουμε τις

$2x + 7 \equiv 3 \pmod{11}$ και $2x + 7 \equiv -3 \pmod{11}$

ισοδύναμα

$2x \equiv -4 \equiv 7 \pmod{11}$ και $2x \equiv -10 \equiv 1 \pmod{11}$

Οι λύσεις είναι $x \equiv 9 \pmod{11}$ και $x \equiv 6 \pmod{11}$

Να λυθεί η γραμμική ισοτιμία $70x \equiv 16 \pmod{41}$

$(70, 41) = 1$ άρα η 1/16 θα έχει μοναδική λύση

$70 = 41(1) + 29$

$41 = 29(1) + 12$

$29 = 12(2) + 5$

$12 = 5 \cdot (2) + 2$

$5 = 2 \cdot (2) + 1$

$2 = 1 \cdot (2) + 0$

$70x \equiv 16 \pmod{41} \Leftrightarrow$

$x = 16\, 70^{\phi(41)-1} \pmod{41}$

$x \equiv 16 \cdot 70^{40-1} \pmod{41}$

$x \equiv 16 \cdot 70^{39} \pmod{41}$

Άρα $\boxed{x \equiv 26 \pmod{41}}$

15 Prove that $13 \mid 4^{2n+1} + 3^{n+2}$ for all non-negative integers n

$4 \equiv 4 \bmod 13$

$4^2 \equiv 4^2 \equiv 16 \equiv 3 \bmod 13$

$4^2 \equiv 3 \bmod 13$

$4^{2n} \equiv 3^n \bmod 13$

$4^{2n} \cdot 4 \equiv 3^n \cdot 4 \bmod 13$

$\boxed{4^{2n+2} \equiv 3^n 4 \bmod 13}$ 1*

$16 \equiv 13 \cdot (1) + 3$ 1*

$9 = 13 \cdot (1) + (-4)$ 2*

$3 \equiv 3 \bmod 13$

$3^n \equiv 3^n \bmod 13$

$3^n \cdot 3^2 \equiv 3^n \cdot 9 \bmod 13$

$\boxed{3^{n+2} \equiv 3^n \cdot 9 \bmod 13 \equiv 3^n (-4) \bmod 13}$ 2*

$4^{2n+1} + 3^{n+2} \equiv 4 \cdot 3^n - 4 \cdot 3^n \bmod 13 \Leftrightarrow$

$\boxed{13 \mid 4^{2n+1} + 3^{n+2}}$