

Θεώρημα: $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{για } n=1 \\ 0 & \text{διαφορετικά} \end{cases}$

Απόδειξη: Η μ είναι πολλαπλασιαστική. Ορίζουμε την $f(n) = \sum_{d|n} \mu(d)$. Η f είναι επίσης πολλαπλασιαστική.

$$f(1) = \sum_{d|1} \mu(d) = \mu(1) = 1 \oplus$$

$$f(p^k) = \sum_{d|p^k} \mu(d) = \underbrace{\mu(1)}_1 + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_0 + \dots + \underbrace{\mu(p^k)}_0 = 0$$

$$d|p^k \Rightarrow d = 1, p, p^2, p^3, \dots, p^k$$

$$f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = f(p_1^{k_1}) \dots f(p_r^{k_r})$$

$$f(p_1 p_2) = \sum_{d|p_1 p_2} \mu(d) = \underbrace{\mu(1)}_1 + \underbrace{\mu(p_1)}_{-1} + \underbrace{\mu(p_2)}_{-1} + \underbrace{\mu(p_1 p_2)}_1 = f(p_1) f(p_2) = 0$$

$$f(p_1) = \sum_{d|p_1} \mu(d) = \mu(1) + \mu(p_1) = 1 + (-1) = 0$$

Άρα, ισχύει ότι $\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$

Θεώρημα: (Τύπος αντιστροφής του Mobius) Έστω $f: \mathbb{N}^* \rightarrow G$ με τύπο $F(n) = \sum_{d|n} f(d)$, τότε $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$

Απόδειξη: Αν $d|n$, τότε και το $\frac{n}{d} | n$. $\sum_{d|n} F(d) \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \sum_{c|d} f(c)$

και $F(d) = \sum_{c|d} f(c)$

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

$$= \sum_{c|n} f(c) \sum_{\substack{d|n \\ c|\frac{n}{d}}} \mu(d). \text{ Για να είναι το } \sum_{d|n} \mu(d) = 1 \text{ πρέπει } \frac{n}{c} = 1 \Rightarrow n=c \quad (+)$$

$$= \sum_{c=n} f(c) = f(n). \text{ Άρα, } \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = f(n)$$

$$\Rightarrow \underline{\text{Πόρισμα}}: \sum_{d|n} \sigma(d) \mu\left(\frac{n}{d}\right) = n$$

Απόδειξη: Από το προηγούμενο για $\sigma(d) = F(d) = \sum_{c|d} c$

$$f(c) = c \text{ ή } f(n) = n$$

$$\text{Άρα, } f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) \text{ και } f(n) = n$$

$$\text{Συμμενώς, } \boxed{\sum_{d|n} \sigma(d) \mu\left(\frac{n}{d}\right) = n}$$

$$\Rightarrow \underline{\text{Πόρισμα}}: \text{ Γνωρίζουμε ότι } n = \sum_{d|n} \phi(d) \text{ Άρα, } \phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$

Απόδειξη: Από το προηγούμενο για $F(n) = n$ και $f(n) = \phi(n)$
θα έχουμε ότι $\phi(n) = f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$

Ισχύει και το αντίστροφο.

$$\Rightarrow \underline{\text{Θεώρημα}} \text{ Αν } f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) \text{ τότε } F(n) = \sum_{d|n} f(d)$$

$$\textcircled{5} \underline{\text{Άσκηση}}: \phi(m) = \phi(n \cdot m), n > 1 \rightarrow n = 2 \quad m = 2^{\ell+1}$$

Κάθε αριθμός (φυσικός) γράφεται $m = 2^k (2\ell+1)$ με $k \geq 0$.

$$n = 2^k (2\ell+1) \quad \phi(m) = 2^{k-1} \phi(2\ell+1)$$

Έστω $k \geq 0$

$$\text{Τότε } \phi(mn) = \phi(2^{k+k'}(2l+1)(2l'+1)) = 2^{k+k'-1} \phi(2l+1)(2l'+1)$$

$$2^{k-1} \phi(2l+1) = 2^{k+k'-1} \phi(2l+1)(2l'+1)$$

$$\text{και } \phi(2l+1) \leq \phi((2l+1)(2l'+1))$$

$$\phi(2l+1) = 2^{k'} \phi(2l+1)(2l'+1) \quad \mu\epsilon \quad k'=0 \quad \underline{\text{ατόπο}}$$

Άρα, μπορεί κτο και $k'=0$ ή $k=0$ και $k'=0$

$$\rightarrow \kappa\tau\omicron \text{ και } \kappa'=0$$

$$\text{Τότε } 2^{k-1} \phi(2l+1) = 2^{k-1} \phi(2l+1)(2l'+1)$$

$$\phi(2l+1) = \phi(2l+1)(2l'+1)$$

Επειδή $n > 1 \Rightarrow \exists 2l'+1 > 1$ και περικό

$$\text{Άρα, } \phi(2l+1) < \phi(2l+1)(2l'+1) \quad \underline{\text{Ατόπο}}$$

$$\rightarrow \kappa=0 \text{ και } \kappa' \geq 1$$

$$\phi(2l+1) = 2^{k'-1} \phi((2l+1)(2l'+1)) \quad \text{Άρα, } k'=1 \text{ και θα πρέπει}$$

$$\phi(2l+1) = \phi((2l+1)(2l'+1)) \quad \text{Πρέπει να δείξουμε ότι } 2l'+1=1$$

$$\text{Αν } 2l'+1 > 1 \Rightarrow \phi(2l+1) < \phi((2l+1)(2l'+1)) \quad \underline{\text{Αδύνατο}}$$

$$\text{Άρα, } n=2 \text{ και } m=2l+1.$$

* Άσκηση 8: Αν $(m, n) = d$, τότε $\phi(mn) \phi(d) = d \phi(m) \phi(n)$

$$d = p_1^{k_1} \dots p_\ell^{k_\ell}$$

$$m = p_1^{k_1'} \dots p_\ell^{k_\ell'} q_1^{m_1} \dots q_s^{m_s}$$

όπου p_i και q_j πρώτοι διαφορετικοί μεταξύ τους

$$\text{Επίσης, } n = p_1^{k_1''} \dots p_\ell^{k_\ell''} r_1^{a_1} \dots r_{s'}^{a_{s'}}$$

p_i, q_j, r_v όλοι διαφορετικοί

$$k_i = \min(k_i', k_i'')$$

$$m \cdot n = p_1^{k_1' + k_1''} \dots p_\ell^{k_\ell' + k_\ell''} q_1^{m_1} \dots q_s^{m_s} r_1^{a_1} \dots r_{s'}^{a_{s'}}$$

$$\phi(mn) = p_1^{k_1' + k_1'' - 1} \dots p_\ell^{k_\ell' + k_\ell'' - 1} q_1^{m_1 - 1} \dots q_s^{m_s - 1} r_1^{a_1 - 1} \dots r_{s'}^{a_{s'} - 1}$$

$$= (p_1 - 1) \dots (p_\ell - 1) (q_1 - 1) \dots (q_s - 1) (r_1 - 1) \dots (r_{s'} - 1)$$

$$\phi(mn) = \prod_{i=1}^{\ell} p_i^{k_i' + k_i'' - 1} (p_i - 1) \prod_{j=1}^s q_j^{m_j - 1} (q_j - 1) \prod_{v=1}^{s'} r_v^{a_v - 1} (r_v - 1)$$

και

$$\phi(d) = \prod_{i=1}^{\ell} p_i^{k_i - 1} (p_i - 1)$$

$$\text{Άρα } \phi(mn) \phi(d) = \prod_{i=1}^{\ell} p_i^{k_i + k_i' + k_i'' - 1 - 1} (p_i - 1)^2 \prod_{j=1}^s q_j^{m_j - 1} (q_j - 1) \prod_{v=1}^{s'} r_v^{a_v - 1} (r_v - 1)$$

$$\phi(m) = \prod_{i=1}^{\ell} p_i^{k_i' - 1} (p_i - 1) \prod_{j=1}^s q_j^{m_j - 1} (q_j - 1)$$

$$\phi(n) = \prod_{i=1}^{\ell} p_i^{k_i'' - 1} (p_i - 1) \prod_{v=1}^{s'} r_v^{a_v - 1} (r_v - 1)$$

$$d = \prod_{i=1}^{\ell} p_i^{k_i}$$

$$= \prod_{i=1}^r (x_i^{e_i-1} + x_i^{e_i-2} + \dots + 1) (p_i-1)^{e_i} \prod_{j=1}^s q_j^{m_j-1} (q_j-1) \prod_{v=1}^t r_v^{d_v-1} (r_v-1)$$

* Άσκηση ④: Για $m=n$ έχουμε ότι $(m,n)=m$
 Από το προηγούμενο έχουμε $\phi(mn)\phi(d)=d\phi(m)\phi(n) \rightarrow$
 $\Rightarrow \phi(m^2)\phi(m) = m(\phi(m))^2 \Rightarrow \phi(m^2) = m\phi(m)$

* Άσκηση ⑤: $2^{2^n} \equiv 1 \pmod{3}$
Νόο
 $\phi(3)=2 \Rightarrow 2^{\phi(3)} = 2^2 \equiv 1 \pmod{3}$
 $2^2 \equiv 1 \pmod{3} \Rightarrow (2^2)^n \equiv 1^n \pmod{3} \Rightarrow 2^{2^n} \equiv 1 \pmod{3}$

$$2^{3^n} \equiv 1 \pmod{7}$$

$$2^3 = 8 \equiv 1 \pmod{7} \Rightarrow (2^3)^n \equiv 1^n \pmod{7} \Rightarrow 2^{3^n} \equiv 1 \pmod{7}$$

$$\text{ord}_7(2) = 3 \mid \phi(7) = 6$$

$$2^{20} \equiv 1 \pmod{41}$$

$$\phi(41) = 40$$

$$2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 \equiv (-9) \pmod{41}$$

$$2^{10} \equiv 81 \pmod{41} \equiv (-1) \pmod{41}$$

$$2^{20} = (2^{10})^2 \equiv (-1)^2 \pmod{41} \equiv 1 \pmod{41}$$

$$\text{Αρα, } \text{ord}_{41}(2) = 20$$

Άσκηση ⑨: $\frac{1}{5}a^5 + \frac{1}{3}a^3 + \frac{7}{15}a \in \mathbb{Z}, \forall a \in \mathbb{Z}$. (πρόβλημα είναι ότι διαφύ με το 5, 3 και 15)

$$\frac{1}{15} (3a^5 + 5a^3 + 7a) \in \mathbb{Z} \Leftrightarrow (3a^5 + 5a^3 + 7a) \equiv 0 \pmod{15}$$

$$\Rightarrow a (3a^4 + 5a^2 + 7) \equiv 0 \pmod{5}$$

Κάθε αριθμός αναπαρίσταιται με:

$$a = 3l$$

$$\text{ή } a = 3l + 1$$

$$\text{ή } a = 3l + 2$$

$$\rightarrow a = 3l$$

$$3l(3(3l)^4 + 5(3l)^2 + 7) \equiv$$

$$3l^5 + 15l^3 + 7l$$

$$3l(3l^4 + 5 \cdot 3l + 7)$$

$$3^5 l^4 + 5 \cdot 3l + 7 \equiv 0 \pmod{5}$$

διαίπεται με το 5

$$3l^4 + 7 \equiv 0 \pmod{5}$$

$$\underbrace{3}_2 \cdot \underbrace{1}_2 \equiv 0 \pmod{5}$$

$$\rightarrow a = 3l + 1$$

$$3l + 1(3(3l + 1)^4 + 5(3l + 1)^2 + 7)$$

$$[3(3l + 1)^4 + 5(3l + 1)^2 + 7] \pmod{15}$$

$$3l(3(3l + 1)^4 + 5(3l + 1)^2 + 7) \equiv 3(3l + 1)^4 + 5(3l + 1)^2 + 7$$

$$3(3l^4 + 4 \cdot 3l^3 + 6 \cdot 3l^2 + 4 \cdot 3l + 1 + 5(3l^2 + 2 \cdot 3l + 1) + 7)$$

$$3 \cdot 1 + 5 \cdot 1 + 7 \equiv 0 \pmod{15}$$

$$3^5 l^4 + 4 \cdot 3^4 l^3 + 6 \cdot 3^3 l^2 + 4 \cdot 3^2 l$$

$$5 \cdot 3(3l^2 + 2l) \equiv 0 \pmod{15}$$

$$\text{Άρα } 3^5 l^4 + 4 \cdot 3^4 l^3 + 6 \cdot 3^3 l^2 + 4 \cdot 3^2 l \equiv 0 \pmod{15}$$

Να δείξετε το ίδιο για $a = 3l + 2$

* Άσκηση ① $\text{ord}_{11}(2) = ;$

$$\text{ord}_{11}(2) \mid \phi(11) = 10 \quad \text{Πιθανές: } 2, 5, 10$$

$$2^2 = 4$$

$$2^4 = 5 \pmod{11}$$

$$2^5 = 10 \pmod{11} \equiv (-1) \pmod{11}$$

$$2^{10} \equiv 1 \pmod{11}$$

$$\text{Άρα, } \text{ord}_{11}(2) = 10$$

$$\text{ord}_{17}(3) = ; \quad \text{ord}_{17}(3) \mid \phi(17) = 16 \quad \text{Πιθανές } 2, 4, 8, 16$$

$$3^2 = 9$$

$$3^4 = 81 \pmod{17} \equiv 13 \equiv -4 \pmod{17}$$

$$3^8 \equiv (-4)^2 \pmod{17} \Rightarrow \text{ord}_{17}(3) = 16 \quad \text{Άρα, 3 πρωταρχική ρίζα}$$

και

$$\text{ord}_{11} 8^{2015} \quad \phi(11) = 10 \Rightarrow a^{10} \equiv 1 \pmod{11}$$

$$8^{2015} = 8^{2010} \cdot 8^5 = 8^{10 \cdot 201} \cdot 8^5$$

$$8^{2015} \pmod{11} \equiv 1 \cdot (2^3)^5 \equiv 1 \cdot 2^{15} \equiv 1 \cdot 2^5 \equiv 1 \cdot 2^5 \pmod{11}$$

$$8^{2015} \equiv 2^5 \pmod{11} \quad \text{και } \text{ord}_{11}(2) = 10 \Rightarrow \text{ord}_{11}(2^5) = 2$$

* Άσκηση ②: $n, 2^n \equiv 4 \pmod{17}$ Γνωρίζουμε ότι το 3 είναι πρωταρχική ρίζα $\pmod{17}$. Άρα, $\exists k \mu \epsilon 7 = 3^k$ και $\exists \lambda \mu \epsilon 4 = 3^\lambda \pmod{17}$

$$\text{Τότε } 7^n \equiv 3^{kn} \equiv 3^\lambda \pmod{17}$$

①

②

③

④

$$3 \quad 3^2 = 9 \quad 3^3 = 27 \equiv 10 \pmod{17} \quad 3^0 \equiv 1 \equiv -4 \pmod{17}$$

$$-12 \equiv 5 \quad 15 \equiv -2 \quad -6 \quad -18 \equiv -1 \quad -3 \quad -9 \equiv 8 \quad 24 \equiv 7$$

⑤

⑥

⑦

⑧

⑨

⑩

⑪

$$\text{Αρα, } 7 \equiv 3^{11} \pmod{17} \quad \text{και } 4 \equiv 3^{12} \pmod{17}$$

$$\frac{21 \equiv 4}{12}$$

$$\text{Συνοψως, } 3^{11n} \equiv 3^{12} \pmod{17}$$

$$3^{\phi(17)} = 3^{16} \equiv 1 \pmod{17}$$

$$3^{11n} \equiv 3^{12} \cdot 3^{16k} \pmod{17} \Rightarrow 3^{11n} \equiv 3^{16k+12} \pmod{17}$$

$$\text{Βρε } s \text{ η } \omega \sigma \tau \epsilon \quad 11n = 16k + 12 \Rightarrow \boxed{11n \equiv 12 \pmod{16}}$$

$\epsilon \nu \epsilon \dot{\omega} \eta, (11, 16) = 1 \Rightarrow \text{έχει μοναδική λύση. Βρείτε την}$

$$(*) \text{ Άσκηση } : n = 2l + 1 \rightarrow 2^n + 3^n \not\equiv 0 \pmod{17}$$

$$\text{As υποθέσουμε ότι } 2^n \equiv -3^n \pmod{17} \equiv (-3)^n \pmod{17}.$$

$$\text{ord}_{17}(2) = 16$$

$$\text{Ποσές } 2, 4, 8, 16$$

$$2 \cdot 4 \cdot 16 \equiv -1 \pmod{17}$$

$$1 \cdot 2 \cdot 3 \cdot 4$$

$$2^8 \equiv 1 \pmod{17} \quad \text{Αρα, } \text{ord}_{17}(2) = 8$$

$$\text{προσέχουμε ότι } \text{ord}_{17}(3) = 16 \Rightarrow 3^8 \equiv -1 \pmod{17}$$

$$2^8 \equiv 1 \pmod{17} \quad -3^8 \equiv 1 \pmod{17}$$

$$2^8 \equiv -3^8 \pmod{17} \quad , \quad 2^8 \neq 3^8 \equiv 0 \pmod{17}$$

$$2^{8+16k} \equiv 3^{8+16k} \pmod{17} \quad \text{Για να 16 έχει αυτό πρέπει το}$$

η να έχει μορφή $8 \pmod{16}$ το οποίο είναι άρτιο. Αρα, για να 16 έχει ότι $2^n + 3^n \not\equiv 0 \pmod{17}$.

$$A \mid a-b \text{ και } 5 \mid b \Rightarrow 5 \mid a-b+b=a$$

Επαναληπτικές Ασκήσεις

11/11/16

Ανάλυση επαγωγής

Πρόταση $p(n)$ η οποία εξαρτάται από το $n \in \mathbb{N}$
(πολλές φορές $n \geq a$)

Θα δείξουμε ότι είναι αληθής για $n \geq a$.

1) Εξετάζουμε την αλήθεια για $p(a)$

2) Υποθέτουμε ότι είναι αληθής για $n=k$ και θδo
η $p(k+1)$ είναι αληθής

④ Άσκηση: Δείξτε ότι $5 \mid 3 \cdot 7^n + 2 \cdot 2^n$ για $n \geq 0$

Η $P(n) = 3 \cdot 7^n + 2 \cdot 2^n$ είναι πολλαπλάσιο του 5

$$P(0) = 3 \cdot 7^0 + 2 \cdot 2^0 = 5 \text{ διαιρείται από το } 5$$

$$P(1) = 3 \cdot 7 + 2 \cdot 2 = 25 \text{ διαιρείται από το } 5.$$

Υποθέτουμε ότι είναι αληθής η $p(k)$ και θα αποδείξουμε ότι
 $p(k+1)$ είναι αληθής.

$$3 \cdot 7^k + 2 \cdot 2^k = 5\lambda \text{ και θέλουμε να δείξουμε ότι } 3 \cdot 7^{k+1} + 2 \cdot 2^{k+1} = 5\lambda'$$

$$3 \cdot 7^{k+1} + 2 \cdot 2^{k+1} = 3 \cdot 7 \cdot 7^k + 2 \cdot 2 \cdot 2^k = 3 \cdot 7 \cdot 7^k + 2 \cdot 2 \cdot 2^k = 21 \cdot 7^k + 4 \cdot 2^k$$

$$= 21 \cdot 7^k + 4 \cdot 2^k - 2(3 \cdot 7^k + 2 \cdot 2^k) \text{ διαιρείται με το } 5$$

$$15 \cdot 7^k = 5 \cdot 3 \cdot 7^k \text{ διαιρείται}$$

$$\text{και } 3 \cdot 7^k + 2 \cdot 2^k = 5\lambda \text{ (υπόθεση) διαιρείται}$$

④ Άσκηση: Νδo το 15 διαιρεί το $3n^5 + 5n^3 + 7n$ για $n \geq 1$

$$\text{Για } n=1: 3 \cdot 1^5 + 5 \cdot 1^3 + 7 \cdot 1 = 3 + 5 + 7 = 15 \text{ 16 χύει}$$

$$\text{Για } n=2: 3 \cdot 2^5 + 5 \cdot 2^3 + 7 \cdot 2 = 3 \cdot 32 + 5 \cdot 8 + 7 \cdot 2 = 150 \text{ 16 χύει}$$

Υποθέτουμε ότι 16 χύει για k . $15 \mid 3k^5 + 5k^3$ και θδo $15 \mid 3(k+1)^5 + 5(k+1)^3 + 7(k+1)$

* Άσκηση 3: Αν το 7 διαιρεί το $2m+n$ τότε διαιρεί και το $100m+n$
 Τα m και n είναι ακέραιοι

Δεν μπορώ να χρησιμοποιήσω επαγωγή.

$$2m+n=7\lambda \Rightarrow 100m+n=7\lambda'$$

$$50(2m+n)=7 \cdot 50\lambda \Rightarrow 100m+50n=7 \cdot 50\lambda$$

$$100m+50n=7\lambda''$$

Αν το $100m+50n - (100m+n)$ διαιρείται με το 7
 τότε και το $100m+n$ διαιρείται με το 7

$$49n = 7 \cdot 7n \text{ ισχύει}$$

* Άσκηση 4: Να γράψετε το 310 στη δεκαδική και δυαδική του μορφή

$$310 = 3 \cdot 10^2 + 10 = 3 \cdot 10^2 + 1 \cdot 10 + 0$$

$$(3 \ 1 \ 0)_{10}$$

$$310 = 1 \cdot 256 + 54 = 1 \cdot 2^8 + 54$$

$$2^6=64 \quad 2^7=128 \quad 2^8=256$$

$$54 = 1 \cdot 32 + 22 = 1 \cdot 2^5 + 22$$

$$22 = 1 \cdot 2^4 + 6$$

$$6 = 1 \cdot 2^2 + 2$$

$$2 = 1 \cdot 2^1$$

$$\text{Άρα, } 310 = 1 \cdot 2^8 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

$$(1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0)_2$$

⑤ Άσκηση: Να βρεθούν ζεύγη ακεραίων (a, b) με $a^6 + b^{14} = 2$
Πόσα ζευγάρια υπάρχουν;

Έχει λύση γιατί $(6, 14) = 2 \mid 2$

Μια λύση με τον αλγόριθμο του Ευκλείδη

$$14 = 2 \cdot 6 + 2 \Rightarrow \boxed{2 = 14 - 2 \cdot 6}$$

Μια λύση λοιπόν είναι η $(a = -2, b = 1)$ έχει άλλες;;

Η εξίσωση αυτή είναι Διοφαντική

Βρες πρώτα μια $(-2, 1)$

Υπολογισες $a = -2 + 14t, t \in \mathbb{Z}$

$$b = 1 - 6t$$

Πρέπει να ισχύει $6a + 14b = 2$

$$6(-2 + 14t) + 14(1 - 6t) = -12 + 14 = 2, \text{ ισχύει}$$

④ Εφαρμογή: Βρες τον αντίστροφο του 3 στο $\text{mod } 17$
 $(3, 17) = 1 \Rightarrow \exists a \text{ και } b \text{ ακέραιοι με } 3a + 17b = 1 \Rightarrow$

$$(3a + 17b) \text{ mod } 17 \equiv 1 \Rightarrow 3a \equiv 1 \text{ mod } 17 \Rightarrow \boxed{a^{-1} \equiv 3 \text{ mod } 17}$$

④ Παράδειγμα: Να βρεθεί η τάξη του 3 στο $\text{mod } 11$ και στο $\text{mod } 22$

$3^{\text{ord}(3)} \equiv 1 \text{ mod } 11$: μικρότερος φυσικός $(3, 11) = 1$ και $\text{ord}(3) \mid \phi(11) = 10$
πιθανές τιμές 2, 5, 10

πχ. $6 \text{ mod } 15$

$$6^2 \equiv 6 \text{ mod } 15$$

$$6^3 \equiv 6 \cdot 6 \equiv 6 \text{ mod } 15$$

Πρέπει $(6, 15) = 1$, άτοπο

γιατί $(6, 15) = 3$

$$3^3 \equiv 6 \equiv 5, 3^4 \equiv 15 \equiv 4 \text{ και}$$

$$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 1 \text{ mod } 11$$

$$\text{Άρα } \boxed{\text{ord}(3) = 5}$$

$(3, 22) = 1$ και $\text{ord}(3) \mid \phi(22) = \phi(2)\phi(11) = 10$

$$3, 3^2 = 9, 3^3 = 27, 3^4 = 15 \equiv -7, 3^5 = -21 \equiv 1$$

$$\text{Άρα } \boxed{\text{ord}(3) = 5}$$

* Παράδειγμα: Αν το γινόμενο δύο πρώτων p και q είναι $n = pq = 1147$ και $\phi(1147) = 1080$, να βρεθούν οι πρώτοι p και q .

1ος τρόπος $\phi(pq) = \phi(p) \cdot \phi(q) = \tau \ 1080 = (p-1)(q-1) = pq - p - q + 1 = \tau$

$$\Rightarrow 1080 = 1147 - p - q + 1 \Rightarrow p + q = 1147 - 1080 + 1 = 68$$

Άρα, $p + q = 68 \Rightarrow p = 68 - q \Rightarrow p = \dots$

$$pq = 1147 \Rightarrow (68 - q)q = 1147 \Rightarrow q = \dots$$

2ος τρόπος

$$pq = 1147$$

$$p, q \leq \sqrt{1147} \approx 33.8$$

Βρες τους πρώτους από το 3 μέχρι το 35 και διαίρεσε

* Παράδειγμα: Να λυθεί η $2x \equiv 10 \pmod{12}$
έχει λύση $(2, 10) | 12$

Όχι μοναδική λύση. Βρες μια

$H x \equiv 5 \pmod{12}$ είναι μια λύση

$$\frac{5 + 12}{(2, 10)} = 5 + 6 \pmod{12}$$

* Παράδειγμα: Να λυθεί η $4x \equiv 12 \pmod{20}$

έχει λύση $(4, 12) | 20$

Όχι μοναδική λύση. Βρες μια

$$H x \equiv 3 \pmod{20}$$

$$\left(3 + \frac{20}{2}\right) \pmod{20}, \left(3 + \frac{20}{3}\right) \pmod{20}, \left(3 + \frac{20}{4}\right) \pmod{20}$$

Ⓐ Άσκηση: Λύσε το σύστημα
$$\begin{aligned} 2x &\equiv 10 \pmod{12} \\ 4x &\equiv 12 \pmod{20} \end{aligned}$$

Ζυνδυάζουμε τις λύσεις των εξισώσεων

$$\left. \begin{aligned} x &\equiv 5 \pmod{12} \\ x &\equiv 3 \pmod{20} \end{aligned} \right\} \Rightarrow x = 5 + 12k \quad \left\{ \begin{aligned} 5 + 12k &\equiv 3 \pmod{20} \end{aligned} \right.$$

$$\Rightarrow 12k \equiv -2 \pmod{20} \Rightarrow 12k \equiv 18 \pmod{20} \quad (12, 18) | 20$$

6 | 20 όχι λύση

Ⓑ Άσκηση:

Να λυθεί: $x \equiv 3 \pmod{37}$. Θ. Euler: Αν p πρώτος και a φυσικός με $(a, p) = 1$
 $\Rightarrow a^{\phi(p)} \equiv 1 \pmod{p}$

$$\begin{aligned} x^{\phi(37)-1} &\equiv 3 \pmod{37} \Rightarrow x^{\phi(37)} \equiv 3x \pmod{37} \Rightarrow \\ &\Rightarrow 1 \equiv 3x \pmod{37} \Rightarrow 3x \equiv 1 \pmod{37} \end{aligned}$$

$$12 \cdot 3x \equiv 12 \pmod{37} \Rightarrow (-1)x \equiv 12 \pmod{37} \Rightarrow x \equiv -12 \pmod{37} \equiv 25 \pmod{37}$$

Άρα, $x \equiv 25 \pmod{37}$

13/1/16

Θεωρία Αριθμών

Ασκηση 9

$$1) \quad 2x \equiv 2 \pmod{4}$$

Εξαι. Δίνει: $(2, 4) | 2 \Leftrightarrow$

$$2x - 2 \equiv 4 \Leftrightarrow (2x - 4k) = 2$$

$\nwarrow$ $\nearrow$
 M.K.D

$$(2, 4) = 2 \Rightarrow \text{Εξαι. Δίνει}$$

$$2x \equiv 2 \pmod{4} \quad (\Leftrightarrow \quad 2x - 2 \equiv 4k \quad (\Leftrightarrow \quad x - 1 = 2k$$

$$2^{-1}, 2^{-1}, \text{όπου} \pmod{4} \text{ (δεν έχει οπρ.)} \quad / \quad \text{Αρα οπρ. } x \equiv 1 \pmod{2}$$

$$x \equiv 1 \pmod{4}$$

$$x \equiv (1 + 4/2) \pmod{4} \\ \equiv 3 \pmod{4}$$

2)

$$15 | 3n^5 + 5n^3 + 7n, \quad n \geq 1$$

$$n=1 \quad 3 \cdot 1^5 + 5 \cdot 1^3 + 7 \cdot 1 = 15 \quad \text{Ισχύει}$$

$$n=2 \quad 3 \cdot 2^5 + 5 \cdot 2^3 + 7 \cdot 2$$

$$96 + 40 + 14 = 150 \quad \text{Ισχύει}$$

Υποθέτουμε ότι ισχύει για k
 $N.A.O$

$$15 | 3k^5 + 5k^3 + 7k$$

$$15 | 3(k+1)^5 + 5(k+1)^3 + 7(k+1)$$

$$3 \left[k^5 + \sum_{i=1}^5 \binom{5}{i} k^{5-i} 1^i \right] + 5 \left[k^3 + \sum_{i=1}^3 \binom{3}{i} k^{3-i} 1^i \right] + 7(k+1)$$

$$\Leftrightarrow 3 \left[k^5 + \sum_{i=1}^5 \binom{5}{i} k^{5-i} 1^i + 1^5 \right] + 5 \left[k^3 + \sum_{i=1}^3 \binom{3}{i} k^{3-i} 1^i + 1^3 \right] + 7k + 7$$

$$= \underbrace{3k^5 + 5k^3 + 7k}_{15} + \underbrace{3+5+7}_{15} + \underbrace{\sum_{i=1}^5 3 \binom{5}{i} k^{5-i}}_{15} + \underbrace{\sum_{i=1}^3 5 \binom{3}{i} k^{3-i}}_{15}$$

Αρα όλα διαπερνάει με το 15. Αρα το αθροισμα διαπερνάει

15. Αρα

$$= 15$$

Να βρεθεί το n ώστε:

$$3^{6n} + 3^n + 2 \equiv 0 \pmod{7}$$

$$3^{6n} + 3^n \equiv -2 \pmod{7}$$

$$3^{6n} + 3^n \equiv 5 \pmod{7}$$

$$(3^6)^n + 3^n \equiv 5 \pmod{7}$$

$$(3^6)^n + 3^n \equiv 5 \pmod{7}$$

$$1 + 3^n \equiv 5 \pmod{7}$$

$$3^n \equiv 4 \pmod{7} \equiv -3 \pmod{7}$$

7 πρώτος $\Rightarrow$ υπάρχει ηρωταρχική ρίζα.

α ηρωταρχική ρίζα $\pmod{7} \Rightarrow \text{ord}_7(a) = \varphi(7) = 6$

$$2, 4, 8 \equiv 1 \Rightarrow \text{ord}_7(2) = 3$$

$$3, 9 \equiv 2, 6, 18 \equiv 4, 12 \equiv 5, 15 \equiv 1$$

$\text{ord}_7(3) = 6 = \varphi(7) \Rightarrow 3$ ηρωταρχική ρίζα.

$$3^n \equiv 4 \pmod{7} = 3^4 \pmod{7} \Rightarrow n \equiv 4 \pmod{\varphi(7)}$$

$$4+6 \Rightarrow 3^{4+6} = 3^4 \cdot 3^6 = 3^4 \cdot 1 \pmod{7}$$

$$n \equiv 4 \pmod{6}$$

Οφείλω:

$$2^n \equiv 4 \pmod{7} \Rightarrow (3^2)^n \equiv 4 \pmod{7} \Rightarrow$$

Βρίσκω την ηρωταρχική ρίζα 3^2 .

$$\Rightarrow 3^{2n} \equiv 3^4 \pmod{7} \Rightarrow 2n \equiv 4 \pmod{6} \Rightarrow n \equiv 2 \pmod{3}$$

$$n \equiv 3 \pmod{6} \text{ ή } (3+5) \pmod{6} \equiv 2 \pmod{6}$$

Τετραγωνικά υπόλοιπα

$$x^2 \pmod{p}$$

$$\text{Π.Χ.} \begin{array}{c|c} 1, 2^2, 3^2, 4^2 \pmod{5} \\ 4 \quad 4 \quad 1 \end{array}$$

Άρα τα τετραγωνικά υπόλοιπα $\pmod{5}$

είναι μόνο τα 1, 4.

Είναι το 3 τετραγωνικό υπόλοιπο $\pmod{5}$;,, ΟΧΙ! Δεν υπάρχει

$$1 \leq a \leq 4 \text{ με } 3 = a^2 \pmod{5}$$

$$x^2 \equiv 3 \pmod{5} \text{ der } x \in \mathbb{Z} \text{ } \Delta \text{ } 0 \text{ } 1$$

$$x^2 \equiv 4 \pmod{5} \text{ der } x \in \mathbb{Z} \text{ } 2 \text{ } 3 \text{ } 4 \text{ } 0$$

$$\text{Euler: } (a, p) = 1$$

$$a \text{ ist ein T.Y. mod } p \text{ av-v:}$$

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

$$\text{Av } p = 4k + 3, \text{ zöc} \quad a^{k+1} \text{ anotelei } \Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \quad x^2 \equiv a \pmod{p}, \text{ av } a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\text{Na } \Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \quad x^2 \equiv 23 \pmod{11}$$

$$x^2 \equiv 23 \pmod{11} \equiv 1 \pmod{11}$$

$$x \equiv 1 \text{ in } -1 \equiv -10 \pmod{11}$$

$$\text{En } \Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \text{ } 4 \text{ } 5 \text{ } 6 \text{ } 7 \text{ } 8 \text{ } 9 \text{ } 10$$

$$(1 + 11k)^2 \equiv 23 \pmod{11^2} \text{ opes } k$$

$$1 + 2 \cdot 11k \equiv 23 \pmod{11^2}$$

$$2 \cdot 11k \equiv 22 \pmod{11^2} \Rightarrow 2k \equiv 2 \pmod{11^2}$$

$$k \equiv 1. \text{ Ape } \text{pro } \Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \text{ } 4 \text{ } 5 \text{ } 6 \text{ } 7 \text{ } 8 \text{ } 9 \text{ } 10 \text{ } 11 \text{ } 12 \text{ } 13 \text{ } 14 \text{ } 15 \text{ } 16 \text{ } 17 \text{ } 18 \text{ } 19 \text{ } 20 \text{ } 21 \text{ } 22 \text{ } 23 \text{ } 24 \text{ } 25 \text{ } 26 \text{ } 27 \text{ } 28 \text{ } 29 \text{ } 30 \text{ } 31 \text{ } 32 \text{ } 33 \text{ } 34 \text{ } 35 \text{ } 36 \text{ } 37 \text{ } 38 \text{ } 39 \text{ } 40 \text{ } 41 \text{ } 42 \text{ } 43 \text{ } 44 \text{ } 45 \text{ } 46 \text{ } 47 \text{ } 48 \text{ } 49 \text{ } 50 \text{ } 51 \text{ } 52 \text{ } 53 \text{ } 54 \text{ } 55 \text{ } 56 \text{ } 57 \text{ } 58 \text{ } 59 \text{ } 60 \text{ } 61 \text{ } 62 \text{ } 63 \text{ } 64 \text{ } 65 \text{ } 66 \text{ } 67 \text{ } 68 \text{ } 69 \text{ } 70 \text{ } 71 \text{ } 72 \text{ } 73 \text{ } 74 \text{ } 75 \text{ } 76 \text{ } 77 \text{ } 78 \text{ } 79 \text{ } 80 \text{ } 81 \text{ } 82 \text{ } 83 \text{ } 84 \text{ } 85 \text{ } 86 \text{ } 87 \text{ } 88 \text{ } 89 \text{ } 90 \text{ } 91 \text{ } 92 \text{ } 93 \text{ } 94 \text{ } 95 \text{ } 96 \text{ } 97 \text{ } 98 \text{ } 99 \text{ } 100$$

$$\Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \text{ } 4 \text{ } 5 \text{ } 6 \text{ } 7 \text{ } 8 \text{ } 9 \text{ } 10 \text{ } 11 \text{ } 12 \text{ } 13 \text{ } 14 \text{ } 15 \text{ } 16 \text{ } 17 \text{ } 18 \text{ } 19 \text{ } 20 \text{ } 21 \text{ } 22 \text{ } 23 \text{ } 24 \text{ } 25 \text{ } 26 \text{ } 27 \text{ } 28 \text{ } 29 \text{ } 30 \text{ } 31 \text{ } 32 \text{ } 33 \text{ } 34 \text{ } 35 \text{ } 36 \text{ } 37 \text{ } 38 \text{ } 39 \text{ } 40 \text{ } 41 \text{ } 42 \text{ } 43 \text{ } 44 \text{ } 45 \text{ } 46 \text{ } 47 \text{ } 48 \text{ } 49 \text{ } 50 \text{ } 51 \text{ } 52 \text{ } 53 \text{ } 54 \text{ } 55 \text{ } 56 \text{ } 57 \text{ } 58 \text{ } 59 \text{ } 60 \text{ } 61 \text{ } 62 \text{ } 63 \text{ } 64 \text{ } 65 \text{ } 66 \text{ } 67 \text{ } 68 \text{ } 69 \text{ } 70 \text{ } 71 \text{ } 72 \text{ } 73 \text{ } 74 \text{ } 75 \text{ } 76 \text{ } 77 \text{ } 78 \text{ } 79 \text{ } 80 \text{ } 81 \text{ } 82 \text{ } 83 \text{ } 84 \text{ } 85 \text{ } 86 \text{ } 87 \text{ } 88 \text{ } 89 \text{ } 90 \text{ } 91 \text{ } 92 \text{ } 93 \text{ } 94 \text{ } 95 \text{ } 96 \text{ } 97 \text{ } 98 \text{ } 99 \text{ } 100$$

$$\text{Na } \Delta \text{ } 0 \text{ } 1 \text{ } 2 \text{ } 3 \quad 3x^2 + 6x \equiv 66 \pmod{11^2}$$

$$3x^2 + 6x = 3(x^2 + 2x) = 3(x^2 + 2x + 1 - 1)$$

$$3(x+1)^2 - 3$$

$$3x^2 + 6x = 3(x+1)^2 - 3 \equiv 66 \pmod{11^2}$$

$$3(x+1)^2 \equiv 69 \pmod{11^2} \quad (1)$$

$$(3, 121) = 1$$

$$121 = 40 \cdot 3 + 1 \Rightarrow 1 = 121 - 40 \cdot 3$$

$$3^{-1} \pmod{11^2} = -40 \equiv 81 \pmod{11^2}$$

$$(1) \Rightarrow -40 \cdot 3(x+1)^2 \equiv -40 \cdot 69 \pmod{11^2}$$

$$(x+1)^2 \equiv -276 \pmod{121}$$

$$\equiv -34 \pmod{11^2}$$

$$(x+1)^2 \equiv 87 \pmod{11^2}$$

$$x+1 = y \Rightarrow y^2 \equiv 87 \pmod{11^2} \Rightarrow \underline{\underline{1124}}$$

Ασκήσεις

4) Έστω p, q πρώτοι αριθμοί και $(a, pq) = 1 \Rightarrow a^{\frac{\phi(pq)}{2}} \equiv 1 \pmod{pq}$

$$\phi(pq) = \phi(p) \cdot \phi(q) = (p-1)(q-1) \Rightarrow \frac{\phi(pq)}{2} = \frac{(p-1)(q-1)}{2}$$

$$(a, pq) = 1 \Rightarrow (a, p) = 1 \text{ και } (a, q) = 1 \quad (*)$$

$$a^{\frac{\phi(p)}{2}} \equiv 1 \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow (a^{p-1})^{\frac{q-1}{2}} \equiv 1 \pmod{p}$$

$$(*) \Rightarrow a^{(p-1)\frac{q-1}{2}} \equiv 1 \pmod{q}$$

$$\text{Ανάλυση: } \left(\begin{matrix} a^{\frac{\phi(pq)}{2}} \equiv 1 \pmod{p} \\ a^{\frac{\phi(pq)}{2}} \equiv 1 \pmod{q} \end{matrix} \right) \Rightarrow \left. \begin{matrix} a^{\frac{\phi(pq)}{2}} - kp = 1 \\ a^{\frac{\phi(pq)}{2}} - kq = 1 \end{matrix} \right\}$$

$$\Rightarrow \begin{cases} a^{\frac{\phi(pq)}{2}} - 1 = kp \\ a^{\frac{\phi(pq)}{2}} - 1 = k'q \end{cases} \text{ Άρα } p \text{ και } q \text{ διαγουν το } a^{\frac{\phi(pq)}{2}} - 1$$

$$\text{Άρα } pq \text{ διαγουν το } a^{\frac{\phi(pq)}{2}} - 1 \Leftrightarrow a^{\frac{\phi(pq)}{2}} \equiv 1 \pmod{pq}$$

SOS SOS

$$3x \equiv 7 \pmod{17} \Rightarrow x \equiv 4^2 \pmod{17} \equiv 8 \pmod{17}$$

$$2^2 \equiv 6 \pmod{17} \Rightarrow 3 \cdot 6 \equiv 1 \pmod{17}$$

Να λύσει το σύστημα: $3 \cdot 3 \equiv 5^{-1}$

$$5x \equiv 3 \pmod{7} \Rightarrow 3 \cdot 5x \equiv 9 \pmod{7} \Rightarrow x \equiv 8 \pmod{7}$$

$$4x \equiv 2 \pmod{5} \Rightarrow 4 \cdot 4x \equiv 8 \pmod{5} \Rightarrow x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{3}$$

7, 5, 3 πρώτοι $\Rightarrow$ Κ.Θ.

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

Λύση $\pmod{7 \cdot 5 \cdot 3} = \pmod{105}$

$$\frac{M}{7} \cdot a \equiv 1 \pmod{7} \Rightarrow 15 \cdot a \equiv 1 \pmod{7} \Rightarrow a \equiv 1 \pmod{7}$$

$$\frac{M}{5} \cdot \beta \equiv 1 \pmod{5} \Rightarrow 2\beta \equiv 1 \pmod{5} \Rightarrow \beta \equiv 3 \pmod{5}$$

$$\frac{M}{3} \cdot \delta \equiv 1 \pmod{3} \Rightarrow 35\delta \equiv 1 \pmod{3} \Rightarrow 2\delta \equiv 1 \pmod{3} \Rightarrow \delta \equiv 2 \pmod{3}$$

$$\text{Lösung} \left(\frac{M}{7} \cdot 1 \cdot 2 + \frac{M}{5} \cdot 4 \cdot 5 + \frac{M}{3} \cdot 2 \cdot 2 \right) \pmod{105}$$

Na $\beta p w$ zu N wäre $\forall a \in \mathbb{Z}$:

$$y(n) = t/e \cdot n$$

$$n = 2^{k_1} 3^{k_2} \dots p_{\ell}^{k_{\ell}}$$

$$y(n) = 2^{k_1-1} \cdot 3^{k_2-1} \cdot \dots \cdot p_{\ell}^{k_{\ell}-1} (p_{\ell}-1)$$

$$= t/e \cdot 2^{k_1} \cdot 3^{k_2} \cdot \dots \cdot p_{\ell}^{k_{\ell}}$$

$$= t/e \cdot 2^{k_1} \cdot 3^{k_2} \cdot \dots \cdot p_{\ell}^{k_{\ell}}$$

$$k_1 \in \mathbb{N} \quad k_1 \geq 1 \quad k_{\ell} = \dots = k_{\ell} = 0$$

$$\ln 105 \quad n = 2^{k_1}$$

$$y(pq) = (p-1)(q-1)$$

$$y(p^2 q^3) = p(p-1) q^2 (q-1)$$