22/11/2016

Άπειροι πρώτοι $4k+1$

$n! = 1 \cdot 2 \cdots n$

$(n!)^2 + 1 = N \quad n \geq 2$

$n=2 \quad N = 5 = 4 \cdot 1 + 1$
$n=3 \quad N = 37 = 4 \cdot 9 + 1$

Έστω p πρώτος $/N$ θα δείξουμε ότι $p = 4k+1$

Άσκηση:
Αν $n \neq m \quad ((n!)^2+1, (m!)^2+1) = 1 \quad n > m$

$N = (n!)^2 + 1$ και $p/N \Rightarrow p > n$

Αν $p \leq n \Rightarrow p/n! \Rightarrow \left.\begin{array}{l} p/(n!)^2 \\ p/N \end{array}\right\} \Rightarrow p/N - (n!)^2 = 1$
αδύνατο

$p > n \quad p/N \Rightarrow N \equiv 0 \bmod p$

$(n!)^2 \equiv -1 \bmod p$

$\left((n!)^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod p$

$\underset{1}{\underset{\equiv}{(1)^{p-1}}} \underset{1}{\underset{\equiv}{(2)^{p-1}}} \cdots \underset{1}{\underset{\equiv}{(n)^{p-1}}} \equiv (-1)^{\frac{p-1}{2}} \bmod p \quad \leftarrow$ (θα το δείξουμε παρακάτω)

$(n!)^{p-1} \equiv 1 \bmod p$ και $1 \equiv (-1)^{\frac{p-1}{2}} \bmod p$

άρα $\frac{p-1}{2} = 2k \Rightarrow p = 4k+1$

$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ έχει $(+)$ και $(\cdot)$

η πρόσθεση συμπεριφέρεται καλά
ο πολ/μος προβληματικός, αν n όχι πρώτος

Μια κλάση $[a]_n$ είναι αντιστρέψιμη
(δηλαδή $\exists\, [b]_n$ με $[a]_n \odot [b]_n = [1]_n$)
<u>ανν</u> $(a,n)=1$.

<u>Π.χ.</u> Να βρεθεί αν υπάρχει η αντίστροφη κλάση της $[10]_{33}$

$(10,33)=1 \Leftrightarrow \exists\, [10]^{-1}_{33}$
$2\cdot 5 \quad 3\cdot 11$

Πως θα τη βρούμε;

Ευκλείδιος αλγόριθμος:
$(10,33)=1 \Leftrightarrow 10\cdot x + 33y = 1$

$33 = 10\cdot 3 + 3 \quad \Rightarrow 3 = 33 - 10\cdot 3$
$10 = 3\cdot 3 + 1$
$1 = 10 - 3\cdot 3 = 10 - 3(33 - 10\cdot 3) =$
$= \underbrace{-3}_{y}\cdot 33 + \underbrace{10}_{x}\cdot 10$

$[10]^{-1}_{33} = [10]_{33}$

$10\cdot 10 = 100 = 3\cdot 33 + 1 = 1 \bmod 33$

Ορισμός (Συνάρτηση του Euler)
Ορίζουμε τη συνάρτηση $\phi: \mathbb{N}^* \to \mathbb{N}^*$ με
$\phi(n)$ = το πλήθος των φυσικών ≥ 1 που είναι πρώτοι με το n

$\phi(1)=1$ $\phi(2)=1$ $\phi(3)=2$

$\phi(4)=2$ $\phi(5)=4$ $\phi(6)=2$
$1 \; \cancel{2} \; 3$ $1 \; \cancel{2} \; \cancel{3} \; \cancel{4} \; 5$

Πόσες είναι οι αντιστρέψιμες κλάσεις;
Απάντ: Είναι $\phi(n)$

Πρόταση
Αν p πρώτος, τότε $\phi(p)=p-1$

Πρόταση
Αν p πρώτος, τότε $\phi(p^k)=p^{k-1}(p-1)$

Απόδειξη

Έστω $a < p^k$ με $(a,p^k)=1 \Leftrightarrow (a,p)=1$

Άρα, πρέπει ο a να μην διαιρείται με το p.

Ποια είναι τα πολλαπλάσια του p μέχρι το p^k

Αν $(\kappa p, p)=p$. Όχι κp.

Βρες τα πολλαπλάσια του p
$p, 2p, 3p, \ldots, p^{k-1} \cdot p = p^k$

Από το πλήθος όλων των αριθμών μεταξύ 1 και p^k αφαιρούμε το πλήθος των πολλαπλασίων : $p^k - p^{k-1}$

<u>Θεώρημα</u>
Αν $(m,n)=1$, τότε $\phi(m,n) = \phi(m)\cdot\phi(n)$

<u>Απόδειξη</u>

$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ ← # αντιστρέψιμων $\phi(m)$ και

$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ ← # αντιστρεψ. $\phi(n)$

$\mathbb{Z}_{mn} = \{[0]_{mn}, [1]_{mn}, \ldots, [mn-1]_{mn}\}$ # αντιστρεψ. $\phi(mn)$

Θα δείξαμε ότι
$\mathbb{Z}_{mn} = \{[an+bm] \mid 0 \leq a \leq m-1, \ 0 \leq b \leq n-1\}$

για $a=0$
ισχύει $\mathbb{Z}_n = \{[m\cdot 0]_n, [m\cdot 1]_n, \ldots, [m(n-1)]_n\}$ γιατί $(m,n)=1$

$b=0$: $\mathbb{Z}_m = \{ \ldots \}$

Υπάρχουν $m\cdot n$ το πλήθος $[an+bm]$ για όλες τις επιλογές $0 \leq a \leq m-1$, $0 \leq b \leq n-1$

Αν $[an+bm]_{mn} = [a'n+b'm]_{mn} \Leftrightarrow an+bm - (a'n+b'm) = kmn$

$(a-a')n + (b-b')m = kmn$

$\left.\begin{array}{l} m \mid kmn \\ m \mid (b-b')m \end{array}\right\} \Rightarrow \left.\begin{array}{l} m \mid kmn - (b-b')m = (a-a')n \\ (m,n)=1 \end{array}\right\} \Rightarrow$

$\Rightarrow m | a - a'$

$$\left.\begin{array}{l} a \equiv a' \bmod m \\ a, a' \leq m-1 \end{array}\right\} \Rightarrow a = a'$$

Για τον ίδιο λόγο $b = b'$.
Άρα, το σύνολο $\{[an+bm]_{mn} | \ldots\}$ είναι ακριβώς το $\mathbb{Z}_{mn}$

Θα δείξουμε
$[an+bm]_{mn}$ αντιστρέψιμη $\Leftrightarrow [a]_m$ και $[b]_n$ αντιστρέψιμοι.
Αν το δείξουμε αυτό έχουμε τελειώσει.

$(a,m) = 1$ Άρα $[a]_m$ αντιστρέφεται
$(b,n) = 1$ $[b]_n$ "

Θέλουμε $(an+bm, mn) = 1$
Υποθέτουμε ότι $\exists$ p πρώτος $| (an+bm, mn)$

$$\left.\begin{array}{l} \Rightarrow p | mn \Rightarrow p | m \text{ ή } p | n \\ \qquad (m,n) = 1 \end{array}\right\} \text{ άρα, διαιρεί μόνο τον έναν}$$

Υποθέτουμε ότι $p | m \Rightarrow$
$$\left.\begin{array}{l} p | bm \\ p | (an+bm, mn) \end{array}\right\} \Rightarrow p | (an+bm-bm, mn) = (an, mn)$$
$\Rightarrow$ $p \nmid n$

$$\Rightarrow \begin{array}{l} p | a \\ p | m \end{array} \circledast \ \underline{\text{αδύνατο}}$$

Η άλλη κατεύθυνση

Έστω ότι $(an+bm, mn)=1$

Υποθέτουμε ότι $p \mid (a,m) \Rightarrow$

$$p \mid (an, mn) \Rightarrow p \mid (an+bm, mn)=1$$

$$\Uparrow$$

Γιατί $p \mid m \Rightarrow p \mid bm$ **Αδύνατο**

άρα $(a,m)=1$ και $(b,n)=1$

Π.χ.

$$\left.\begin{array}{l}\phi(6)=\phi(2\cdot 3)\\ (2,3)=1\end{array}\right\} = \phi(2)\cdot\phi(3) = (2-1)\cdot(3-1)=2$$

$$\phi(15)=\varphi(3\cdot 5)=\varphi(3)\cdot\varphi(5)=(3-1)(5-1)=8$$

$$\phi(45)=\phi(5\cdot 9)=\phi(5)\phi(9)=$$
$$=(5-1)\phi(3^2)=4\cdot 3(3-1)=24$$

$\mathbb{Z}_{45}$ έχει $24=\phi(45)$ αντιστρέψιμες κλάσεις.

Πόρισμα

Αν $n=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$ με p_i πρώτοι διαφορετικοί, τότε

$$\phi(n)=\prod_{i=1}^{m} p_i^{k_i-1}(p_i-1)$$

Θεώρημα (Τύπος του Gauss χωρίς απόδειξη)

Για $n \in \mathbb{N}^*$ έχουμε $n = \sum_{d|n} \varphi(d)$

Πάρε όλους τους διαιρέτες του n. Βρες τα ϕ και άθροισέ τα θα πάρεις το n.

Λήμμα

Έστω $\{[a_1]_m, [a_2]_m, \ldots [a_{\phi(m)}]_m\}$

όλες οι αντιστρέψιμες κλάσεις στο mod m.

Αν $(a,m)=1$, τότε

$$\{[aa_1]_m, [aa_2]_m, \ldots, [aa_{\phi(m)}]_m\} =$$

$$= \{[a_1]_m, [a_2]_m, \ldots, [a_{\phi(m)}]\}$$

Π.χ. $\{[1]_5, [2]_5, [3]_5, \underset{\phi(5)}{[4]_5}\}$ $(3,5)=1$

$\{[3]_5, [3\cdot 2]_5 = [1]_5, [3\cdot 3]_5 = [4]_5, [4\cdot 3]_5 = [2]_5\}$

Θεώρημα (Τύπος Wilson)

Ο φυσικός $p > 1$ είναι πρώτος ανν
$$(p-1)! \equiv -1 \bmod p \equiv (p-1) \bmod p$$

Αν m σύνθετος με $m \neq 4$, τότε
$$(m-1)! \equiv 0 \bmod m$$

π.χ. $\bmod 7$

$$(7-1)! = \underbrace{1 \cdot 2}_{1 \bmod 7} \cdot 3 \cdot \overset{1 \bmod 7}{4} \cdot 5 \cdot \underbrace{6}_{-1 \bmod 7}$$
$1 \bmod 7$

Απόδειξη

"$\Leftarrow$" Δηλαδή
$$(p-1)! \equiv -1 \bmod p \Rightarrow p \text{ πρώτος}.$$

Υποθέτουμε ότι p όχι πρώτος. Άρα, υπάρχει q πρώτος $/p$ και $q < p$

$$q \quad 1 \cdot 2 \cdot \ldots \cdot (p-1) \Rightarrow q/(p-1)!$$
$$q/p$$

$$(p-1)! \equiv -1 \bmod p \Rightarrow (p-1)! + 1 \equiv 0 \bmod p \Leftrightarrow p/(p-1)! + 1$$

άρα $\left.\begin{array}{l} q/p/(p-1)! + 1 \\ q/(p-1)! \end{array}\right\} \Rightarrow q/1$ αδύνατο

" $\Longrightarrow$ "

Έστωμε p πρώτος περιττός. Θέλουμε $(p-1)! \equiv -1 \bmod p$

Έστω $(p-1)! = A \Rightarrow A^2 = 1^2 \cdot 2^2 \cdots (p-1)^2 \equiv 1 \bmod p$

γιατί για κάθε a θα υπάρχει ο αντίστροφος

$A^2 \equiv 1 \bmod p \Rightarrow A^2 - 1 \equiv 0 \bmod p$

$(A-1)(A+1) \equiv 0 \bmod p$

p πρώτος $\Rightarrow$ δεν έχει μηδενοδιαιρέτες

$\Rightarrow A-1 \equiv 0 \bmod p$ ή $A+1 \equiv 0 \bmod p$

Αν $A \equiv 1 \bmod p$.

$\forall\ 1 < a < p-1$ υπάρχει ο αντίστροφος διαφορετικός από τον a ή ταυτίζεται με τον εαυτό του.

δεν υπάρχει

$1 \cdot 2 \cdot 3 \ldots a \ldots p-1$

Αν $[a]_p^{-1} = [b]_p$ $\qquad a \neq b$ $\qquad$ Αν $a = b$

$a \cdot b = 1 \bmod p$

Αν $a = b \Rightarrow 1 \cdot 2 \ldots a \ldots (p-1) > a(p-1)$

Δηλαδή $A \not\equiv 1 \bmod p$.

Άρα, τελικά $A \equiv -1 \bmod p$

Έστω $m = pq$ $(p,q)=1$ σύνθετο

1) $p \neq q$
2) $p = q$

$p, q < m-1 \Rightarrow pq \mid (m-1)!$

$m = p \cdot q \mid (m-1)! \Rightarrow (m-1)! \equiv 0 \bmod m$

2) $m = p^2$ $(m-1)! = 1 \cdot 2 \cdots p(p+1) \cdots 2p(2p+1) \cdots (p^2-1) \Rightarrow$

$\Rightarrow m = p^2 \mid (m-1)! \Rightarrow (m-1)! \equiv 0 \bmod p.$