Παρατήρηση: $[a]_m$ αντιστρέψιμη $\Leftrightarrow (a,m)=1$

το $\mathbb{Z}_7 = \{[0]_7, [1]_7, \ldots, [6]_7\} \rightsquigarrow \varphi(7)=6$

για το $\mathbb{Z}_{14} = \{[0]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$ ← Αντιστρεφ. κλάσεις

$\rightsquigarrow \varphi(14)=6$

οπου γενικά $\varphi(p)=p-1$ όταν $p$ πρώτος!

Επίσης $\varphi(2)=1$ και $\varphi(7)=6 \Rightarrow \varphi(2)\cdot\varphi(7)=6=\varphi(14)$.

ΛΗΜΜΑ: Έστω $\alpha,\beta \in \mathbb{N}$ και $n \in \mathbb{N}$. Τότε εάν $n$ και πρώτος

: $(\alpha+\beta)^n = \alpha^n+\beta^n \bmod n$

Απόδειξη

$$(\alpha+\beta)^n = \sum_{i=0}^{n} \binom{n}{i} \alpha^{n-i}\cdot\beta^i = \alpha^n+\beta^n+\sum_{i=1}^{n-1} \alpha^{n-i}\cdot\beta^i$$

όπου $\binom{n}{i} = \frac{n!}{(n-i)!i!}$

Παρατήρηση: Για το παράδειγμα:

$\alpha=1$ και $\beta=1$ ενώ $n=4$

$(1+1)^4 = 2^4 \equiv 16 \bmod 4 \equiv 0 \bmod 4$ (1)

$(1+1)^4 = 1^4 + \underbrace{\binom{4}{1}1^3\cdot 1}_{\text{διαιρείται με 4}} + \binom{4}{2}1^2\cdot 1^2 + \underbrace{\binom{4}{3}1^3\cdot 1}_{\text{διαιρείται με 4}} + 1^4$

αλλά $\binom{4}{2} = 6 \mod 4 = \underline{\underline{2 \mod 4}}$ (2)

(2) ≠ (1)

Γιατί αυτό; (Δηλ. γιατί δεν εφαρμόζεται το ΛΗΜΜΑ;)

Διότι ο 4 ΟΧΙ πρώτος

Θέλαμε δηλ.

$\binom{4}{i} = \frac{4!}{i!(4-i)!} = (4 \cdot A)$

↓

το 4 αναγκαστικά να μην απλοποιείται από το γινόμενο $i!(4-i)!$ και αυτό έχει μόνο όταν 4 πρώτος φυσικός

Στο σώμα $\mathbb{Z}_7 = \{[0]_7, \dots, [6]_7\}$ πολ/ζω με το 3 και έχω ότι

$\{[0]_7, [3]_7, [6]_7, [9]_7, [12]_7, [15]_7, [18]_7\}$
$= [2]_7, [5]_7, [1]_7, [4]_7$

Για το $\mathbb{Z}_{14}$ αντιστρεψιμων κλάσεων

• πολ/ζω με 2 και παίρνω:

$\{[2]_{14}, [6]_{14}, [10]_{14}, [18]_{14}, [22]_{14}, [26]_{14}\}$ Δεν είναι αντιστρέψιμες
$[4]_{14}, [8]_{14}, [12]_{14}$

• πολ/ζω με 3 και παίρνω:

$\{[3]_{14}, [9]_{14}, [15]_{14}, [27]_{14}, [33]_{14}, [39]_{14}\}$
$[1]_{14}, [13]_{14}, [5]_{14}, [11]_{14}$

Δεν αλλάζει γιατί $(3,14)=1$

Έτσι προκύπτει το αναλογο λημμα

**ΛΗΜΜΑ:** Έστω ότι το σύνολο $\{[a_1]_m, [a_2]_m, \ldots, [a_k]_m\}$ αντιπροσωπεύει όλες τις κλάσεις κατάλοιπων mod m και ο ακέραιος $a$ με $(a,m)=1$. Τότε,

$$\{[aa_1]_m, [aa_2]_m, \ldots, [aa_k]_m\} = \{[a_1]_m, [a_2]_m, \ldots, [a_k]_m\}$$

**Απόδειξη**

1) Πρέπει $[aa_i]_m$ να είναι αντιπροσωπευτικό

2) Τα σύνολα να είναι ίσα

1) Έαν $[aa_i]_m$ όχι αντιπροσωπευτικό τότε $(aa_i, m) \neq 1$. Άρα, υπάρχει $p$ πρώτος ώστε $p|m$ & $p|aa_i \Rightarrow p|m$ και $(p|a$ ή $p|a_i)$
$(p|m$ και $p|a)$ ή $(p|m$ και $p|a_i)$ Αδύνατο
$(a,m)=1$ $(a_i,m)=1$

2) Αρκεί $[aa_i]_m \neq [aa_j]_m$
Αν $[aa_i]_n = [aa_j]_m \Leftrightarrow aa_i - aa_j$ διαιρ. από το $m$
$a(a_i - a_j)$ διαιρείται από το $m$
Αν $p$ πρώτος: $p|m$ και $p|a(a_i - a_j)$
Τότε $p|m$ και $p|a$ αδύνατο $(a,m)=1$
ή $p|m$ και $p|a_i - a_j$. Άλλά $[a_i]_n \neq [a_j]$
διαπιστώνεται πλάσμα αδύνατο.

**Θεώρημα:** Έστω $(m,n)=1$ και $m,n \in \mathbb{N}$
Τότε $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

**Απόδειξη**

Έστω $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ και
$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

και

$$\mathbb{Z}_{m\cdot n} = \{[an+\beta m]_{m\cdot n} \mid 0 \leq a \leq m-1 \ \& \ 0 \leq \beta \leq n-1\}$$

Το σύνολο $\mathbb{Z}_{m\cdot n}$ περιέχει $m \cdot n$ στοιχεία. Αρκεί αυτά να είναι $\neq$ mod $m \cdot n$

Αν υποθέσαμε ότι $[\alpha\nu+\beta m]_{nm} = [\alpha'\nu+\beta' m]_{nm} \Leftrightarrow$

$\Leftrightarrow \alpha\nu+\beta m - \alpha'\nu-\beta' m$ διαιρ. απ' το $m\cdot\nu$

$(\alpha-\alpha')\nu + (\beta-\beta')m$ διαιρ. από το $m\cdot\nu$ (1)

Γνωρίζαμε ότι

$[\alpha]_m \neq [\alpha']_m$ & $[\beta]_\nu \neq [\beta']_\nu$ και $(\nu,m)=1$

άρα (1) $(\alpha-\alpha')\nu+(\beta-\beta')m = k m\nu \equiv 0 \bmod m\nu \Leftrightarrow$

$$\left.\begin{array}{l}(\alpha-\alpha')\nu+(\beta-\beta')m \equiv 0 \bmod m \\ (\beta-\beta')m \equiv 0 \bmod m\end{array}\right\} \Rightarrow \left\{\begin{array}{l}(\alpha-\alpha')\nu \equiv 0 \bmod m \quad (*) \\ (\nu,m)=1\end{array}\right.$$

Το ότι $(\nu,m)=1 \Rightarrow \exists\, \delta$ ώστε: $\nu\cdot\delta \equiv 1 \bmod m$

πολ/ζω την (*) με $\delta$ και έχω:

$(\alpha-\alpha')\nu\delta \equiv 0\cdot\delta \bmod m \Rightarrow (\alpha-\alpha') \equiv 0 \bmod m$

δηλ. $\alpha = \alpha'$ μ.α. αυτό είναι άτοπο από την αρχική υπόθεση.

ΙΔΙΑ ΘΕΩΡΗΜΑΤΟΣ

ΘΔΟ εαν $[a]_m$ & $[\beta]_n$ είναι αντιστρέψιμες κλάσεις mod m και mod n αντίστοιχα, τοτε η κλάση $[\alpha n+\beta m]_{mn}$ είναι αντιστρέψιμη και αντιστροφος. Τότε, το πλήθος των αντιστρεψιμων κλάσεων mod mn, θα ισούται με το γινόμενο του πλήθους των αντιστρεψιμων κλάσεων mod m επι το αντίστοιχο πλήθος mod n. Δηλ. θα εχουμε δείξει οτι

$\varphi(mn) = \varphi(m)\cdot\varphi(n)$

($\Rightarrow$): $[a]_m$ και $[\beta]_n$ αντιστρεψιμες $\Leftrightarrow (a,m), (\beta,n), (m,n) = 1$

Εστω οτι η $[\alpha n+\beta m]_{mn}$ <u>οχι</u> αντιστρεψιμη $\Leftrightarrow$

$\Leftrightarrow (\alpha n+\beta m, mn) \neq 1$. Αρα, θα ∃ πρωτος p με

$p \mid m\cdot n$ και $p \mid \alpha n+\beta m$

Τοτε θα ειχαμε $p \mid m$ <u>ή</u> $p \mid n$

Εστω $p \mid m$ και $p \mid \alpha n+\beta m \Rightarrow \left\{ \begin{array}{l} p \mid m \ \& \ p \mid \alpha n \\ p \nmid n \end{array} \right| \Rightarrow$

$\Rightarrow p \mid a$ και $p \mid m$ Αδύνατο

ομοιως και για $p \mid n$.

($\Leftarrow$): Εστω $[\alpha n+\beta m]$ αντιστρεψιμη $\Leftrightarrow (\alpha n+\beta m, mn) = 1$

Θελουμε $(a,m)=1=(\beta,n)$

Εστω ότι ∃ πρωτος $p \mid (a,m)$

($[a]_m$ οχι αντιστρεψιμη, και θελουμε <u>ατοπο</u>)

Επειδη $p \mid (a,m) \Rightarrow p \mid (an, m) \Rightarrow p \mid (\alpha n+\beta m, m) \Rightarrow$

$\Rightarrow p \mid (\alpha n+\beta m, mn) = 1$

πχ (πάνω στην παρακάτω πρόταση)

$\varphi(4) = \varphi(2^2) = 2 = 2^{2-1}\cdot(2-1)$

$\varphi(2^3) = 4 = 2^2(2-1)$ $\{[0],[1],[2],[3],[4],[5],[6],[7]\}$

δεν παίρνω πολλ/σια του 2

$0, 1\cdot 2, 2\cdot 2, 3\cdot 2$

$2^3$ αριθμοί − πολλ/σια του 2 από 0 έως $2^3-1$

ΠΡΟΤΑΣΗ

Έστω ρ πρώτος, τότε $\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1-\frac{1}{p}\right)$

ΑΠΟΔΕΙΞΗ

Ψάχνουμε τους αριθμούς μεταξύ του 1 και $p^k-1$ που δεν θα διαιρούνται από τον ρ

Άρα από όλους αυτούς τους αριθμούς πρέπει να αφαιρέσουμε τα πολλ/σια του ρ.

$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right) = p^{k-1}(p-1)$

ΠΡΟΤΑΣΗ

Έστω $n = p_1^{k_1}\cdots p_\mu^{k_\mu}$ με $p_i$ πρώτοι και $0<k_i$ φυσικοί

Τότε:

$$\varphi(n) = n\prod_{i=1}^{\mu}\left(1-\frac{1}{p_i}\right)$$

ΑΠΟΔΕΙΞΗ

Αφού $(p_i^{k_i}, p_j^{k_j}) = 1$ για $i\neq j$ θα έχουμε ότι

$\varphi\left(p_i^{k_i}\cdot p_j^{k_j}\right) = \varphi\left(p_i^{k_i}\right)\cdot\varphi\left(p_j^{k_j}\right) = p_i^{k_i}\left(1-\frac{1}{p_i}\right)\cdot p_j^{k_j}\left(1-\frac{1}{p_j}\right)$

Άρα, το ίδιο ισχύει και για περισσότερους πρώτους

ΘΕΩΡΗΜΑ (ΤΥΠΟΣ GAUSS)

Για $n\in\mathbb{N}^*$ έχουμε

$$n = \sum_{d/n}\varphi(d)$$

Δηλ. αθροίζουμε ως προς τους διαιρέτες του n

## ΘΕΩΡΗΜΑ (Wilson)

Ο φυσικός $p>1$ είναι πρώτος αν

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

### ΑΠΟΔΕΙΞΗ

$p=2 \Rightarrow 1! \equiv -1 \bmod 2 \equiv 1 \bmod 2$

$p$ περιττός

($\Leftarrow$): $(p-1)! \equiv -1 \bmod p$. Ας υποθέσουμε ότι $p$ όχι πρώτος

Άρα θα $\exists$ πρώτος $q<p$ ο οποίος θα τον διαιρούσε

$(p-1)! = 1 \cdot 2 \cdot 3 \cdots q \cdots (p-1)$, $q \le p-1$

Έτσι, το $q \mid (p-1)!$ και $q \mid p$ και $p \mid (p-1)!+1$ $\Rightarrow$ $q \mid (p-1)!$ και $q \mid (p-1)!+1$ $\Rightarrow$

$\Rightarrow q \mid 1$ Άδυνατο

($\Rightarrow$) Έστω $p$ πρώτος άρα $\{[1]_p, \ldots, [p-1]_p\}$ αντιστρέψιμες

Ας πάμε πχ:

$\mathbb{Z}_5 = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ ← Αντιστρέψιμες υπάρχουν

Έχουμε, $([1]_5)^{-1} = [1]_5$, $([2]_5)^{-1} = [3]_5$, $([3]_5)^{-1} = [2]_5$

και $([4]_5)^{-1} = [4]_5$

οπότε εάν πολ/ω με τον εαυτό του τότε θα έχω τα στοιχεία

$[1]_5, [2]_5, [3]_5, [4]_5, [1]_5, [2]_5, [3]_5, [4]_5 \equiv 1 \bmod 5$

Άρα, $([1]_p, \ldots, [p-1]_{p-1})^2 \equiv 1 \bmod p$

Έχουμε, $A^2 \equiv 1 \bmod p \Leftrightarrow p \mid A-1$ ή $p \mid A+1$

$A = kp-1 \equiv -1 \bmod p$ ή $A = kp+1 \equiv 1 \bmod p$

το $A$ δεν μπορεί να είναι

(Άρα, $A \equiv -1 \bmod p \equiv (p-1) \bmod p$) $1 \bmod p$

Πχ

ΝΔΟ $12 \cdot 13 \cdot \ldots \cdot 21 \equiv -1 \bmod 11$

ΛΥΣΗ

$12 \cdot 13 \cdot \ldots \cdot 21 = 1 \bmod 11 \cdot 2 \bmod 11 \cdot \ldots \cdot 10 \bmod 11$

Ο 11 πρώτος. Άρα $\frac{21!}{11!} \equiv -1 \bmod 11$

(Αφού $12 \cdots 21 = 1 \cdots 10 \bmod 11 \overset{\text{Wilson}}{\equiv} (-1) \bmod 11$)

ΘΕΩΡΗΜΑ (Euler)

Έστω $a, m \in \mathbb{N}^*$ με $(a,m)=1$. Τότε $a^{\varphi(m)} \equiv 1 \bmod m$

ΑΠΟΔΕΙΞΗ

$\varphi(m)$ = πλήθος αντιστρέψιμων υπολοίπων

$\{[a_1]_m, \ldots, [a_{\varphi(m)}]_m\} = A$

$(a,m)=1 \Rightarrow a \bmod m = [a]_m \in A$

$[a]_m = [a_i]_m$

Αρκεί νδο ο $a_i^{\varphi(m)} = 1 \bmod m$

$(a_i, m) = 1 \Rightarrow \{[a_i \cdot a_1]_m, \ldots, [a_i a_{\varphi(m)}]_m\} = A$

Έαν πολλ/με όλα τα στοιχεία θα έχουμε

$a_i \cdot a_1 \, a_i \cdot a_2 \ldots a_i a_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)} \bmod m$

$a_i^{\varphi(m)} \cdot a_1 \ldots a_{\varphi(m)} - a_1 a_2 \ldots a_{\varphi(m)} \equiv 0 \bmod m$

$(a_i^{\varphi(m)} - 1)(a_1 \ldots a_{\varphi(m)}) \equiv 0 \bmod m$ } $\Rightarrow$

Επειδή, $(a_1 \ldots a_{\varphi(m)})(a_1 \ldots a_{\varphi(m)}) \equiv 1 \bmod m$

$\Rightarrow a_i^{\varphi(m)} - 1 \equiv 0 \bmod m \Leftrightarrow a_i^{\varphi(m)} \equiv 1 \bmod m$

ΘΕΩΡΗΜΑ: Έστω $p$ πρώτος και $a \in \mathbb{N}$ με $(a,p)=1$

τότε $a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^p \equiv a \bmod p$

## ΕΦΑΡΜΟΓΕΣ / ΠΑΡΑΔΕΙΓΜΑΤΑ:

πχ 1

ΝΔΟ $2^{50}+3^{50} \equiv 0 \mod 13$

ΛΥΣΗ

Το 13 είναι πρώτος τότε μπορούμε να εφαρμόσουμε το προηγούμενο θεώρημα

$(2,13)=(3,13)=1$ τότε

$2^{12} \equiv 1 \mod 13$ και $3^{12} \equiv 1 \mod 13$

$50 = 4 \cdot 12 + 2$

Άρα $2^{50} = 2^{4 \cdot 12+2} = (2^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 4 \mod 13 \rightsquigarrow$

$\rightsquigarrow 2^{50} \equiv 4 \mod 13$

Ενώ, $3^{50} = 3^{4 \cdot 12+2} = (3^{12})^4 \cdot 3^2 \equiv 1 \cdot 9 \mod 13$

Άρα $2^{50}+3^{50} \equiv (4+9) \mod 13 \equiv 0 \mod 13$

άρα ο αριθμός $2^{50}+3^{50}$ διαιρείται του 13.

πχ 2

$3^{372} \equiv x \mod 37$ να βρεθεί το $x=;$

ΛΥΣΗ

37 πρώτος με $(3,37)=1$

$3^{36} \equiv 1 \mod 37$

Με $372 = 36 \cdot 10 + 12$

άρα $3^{372} = (3^{36})^{10} \cdot 3^{12} \equiv 13^{12} \mod 37$

Πως βρίσκω το $13^{12}$;;

Γνωστό ότι: $3^1=3$, $3^2=9$, $3^3=27$, $3^4=81$

$3^4 = 81 \equiv 7 \mod 37$

$3^{12} = (3^4)^3 \equiv 7^3 \mod 37 \equiv 7 \cdot 7^2 \mod 37 \equiv 7 \cdot 12 \mod 37 \equiv$

$\equiv 84 \mod 37 \equiv 10 \mod 37$

Ασκ 3

ΝΔΟ $7 \nmid n^2+1$

Λύση

Έστω ότι $7 \mid n^2+1 \Leftrightarrow n^2+1 \equiv 0 \bmod 7 \Leftrightarrow n^2 \equiv -1 \bmod 7$

$\Rightarrow n^4 \equiv 1 \bmod 7 \Rightarrow n^2 \cdot n^4 \equiv (-1)\cdot 1 \bmod 7 \Rightarrow$

$\Rightarrow n^6 \equiv -1 \bmod 7$ . Αν $(n,7)=1 \Rightarrow n^6 \equiv 1 \bmod 7$ Άτοπο

Άρα, εάν $(n,7) \neq 1$ τότε θα ∃ πρώτος που θα τους διαιρεί έστω ρ αυτός ο πρώτος με $(n,7)$ διαφέτει από το ρ, άλλα 7 πρώτος άρα αναγκαστικά είναι

$\rho = 7 \Rightarrow 7 \mid (n,7) \Rightarrow n = k \cdot 7 \quad k \in \mathbb{Z}$

$\Rightarrow n^2 = k^2 \cdot 7^2 \Rightarrow \cdot \quad k^2 \cdot 7^2 + 1$

Αν $7 \mid n^2+1 \Rightarrow 7 \mid 1$ άρα $7 \mid n^2 = k^2 \cdot 7^2$