

12/2/2025 Θεωρία Αριθμών

Book: Apostol - Δερίζιτης
cvasilak@math.ntua.gr

• Διαμεσότητα:

Έστω $d, n \in \mathbb{Z}$. Λέμε ότι ο d διαμερι-
τον n αν υπάρχει ακέραιος c τ.ω.
 $n = c \cdot d$. Γράφουμε " $d \mid n$ " και λέμε επίσης
ότι ο n είναι πολλαπλάσιο του d ή ότι
ο d είναι διαμέτρης ή παράγοντας του n .
Όταν ο d δεν διαμερι τον n γράφουμε
" $d \nmid n$ ".

Ιδιότητες:

- $n \mid n$ (ταυτοτική)
- $d \mid n, n \mid m \Rightarrow d \mid m$ (μεταβατική)
- * • $d \mid n, d \mid m \Rightarrow d \mid an + bm, \forall a, b \in \mathbb{Z}$ (γραμμικότητα)
- $d \mid n \Rightarrow ad \mid an, \forall a \in \mathbb{Z}$
- $ad \mid an, a \neq 0 \Rightarrow d \mid n$ (νόμος διαγραφής)
- $n \mid 0$
- $0 \mid n \Rightarrow n = 0$
- $n \mid d \Rightarrow n \mid -d, -n \mid d, -n \mid -d, |n| \mid |d|$.

* Proof:

$$n = c \cdot d, m = c' \cdot d \Rightarrow an = ac \cdot d, bm = bc' \cdot d$$

$$an + bm = acd + bc'd = d(ac + bc') \\ \Rightarrow d \mid an + bm$$

- $d \mid n, n \neq 0 \Rightarrow |d| \leq |n|$
- $d \mid n, n \setminus d \Rightarrow |d| = |n|$
- $d \mid n, d \neq 0 \Rightarrow (n/d) \setminus n$
 $\Delta \eta \lambda. \quad n = cd \Rightarrow d \mid n, c \setminus d$

Παράδειγμα:

(N1 Σ03)

Να βρεθούν όλοι οι θετικοί ακέραιοι n για τους οποίους ισχύει ότι $n+1 \mid n^2+1$

Λύση:

Έστω $n^2+1 = a(n+1), a \in \mathbb{Z}$.

$$n^2+1 = n^2-1+2 = (n+1)(n-1)+2$$

$$\begin{aligned} \lambda \rho \alpha \quad a(n+1) - (n+1)(n-1) &= 2 \Leftrightarrow \\ (n+1)(a-n+1) &= 2 \end{aligned}$$

$$\Rightarrow \begin{aligned} n+1=1 & \quad \vee \quad n+1=2 \Rightarrow n=0 \quad \text{✗ (απόρροια)} \\ & \quad \vee \quad \boxed{n=1} \end{aligned}$$

Παράδειγμα: (επιπλοωμένη)

$$\Delta. \sigma. \quad \forall n \in \mathbb{N}, \quad 5 \mid 2^{4n+2} + 1$$

Λύση:

Βάση : Για $n=0, \quad 2^{4 \cdot 0 + 2} + 1 = 2^2 + 1 = 5 \Rightarrow 5 \mid 5 \quad \checkmark \text{ (ισχύει)}$
 Βήμα : Έστω $5 \mid 2^{4n+2} + 1$. Θ.δ.ο. $5 \mid 2^{4(n+1)+2} + 1 = 2^{4n+6} + 1$
 υποθέτουμε: $5 \mid 2^{4n+2} + 1 \Rightarrow 5 \mid (2^{4n+2} + 1) \cdot 2^4 = 2^{4n+2} \cdot 2^4 + 2^4 = 2^{4n+6} + 2^4$
(*)

Επίσης $5 \mid -15 = 1 - 2^4$ (**)

Αντί $(*)$, $(**)$ ^{δρατ.} $\Rightarrow 5 \mid 2^{4n+6} + 2^4 + 1 - 2^4$
 $\Rightarrow 5 \mid 2^{4n+6} + 1$

• Παράδειγμα:

Αν a, b περιττοί ακέραιοι, τότε $8 \mid a^2 - b^2$

• Λύση:

Από a περιττός: $a = 2k + 1, k \in \mathbb{Z}$

$$\leadsto k = 2k_1, k_1 \in \mathbb{Z} \Rightarrow a = 4k_1 + 1 \Rightarrow$$

$$a^2 = 16k_1^2 + 8k_1 + 1 \Rightarrow a^2 = 8(2k_1 + 1)k_1 + 1$$

$$\leadsto k = 2k_2 + 1, k_2 \in \mathbb{Z} \Rightarrow a = 4k_2 + 3$$

$$a^2 = 16k_2^2 + 24k_2 + 9 = 8(2k_2^2 + 3k_2 + 1) + 1$$

Και στις δύο περιπτώσεις $a^2 = 8c + 1$.
 Άρα $a^2 - b^2 = 8c + 1 - 8c' - 1 = 8(c - c') \Rightarrow$
 $8 \mid a^2 - b^2$

• Ευκλείδεια Διαίρεση:

Για $a, b \in \mathbb{Z}, b > 0$, υπάρχουν μοναδικοί
 ακέραιοι q (πηλίκο) και r (υπόλοιπο),
 τέτοιοι ώστε $a = q \cdot b + r, 1 \leq 0 \leq r < b$.

Μέγιστος κοινός διαιρέτης (ΜΚΔ):

• Θεώρημα Bezout:

$(\mathbb{N}^*)$

Για κάθε δύο φυσικούς αριθμούς a, b υπάρχει κοινός τους διαιρέτης d της μορφής $d = xa + yb$ για κάποια $x, y \in \mathbb{Z}$, και κάθε κοινός διαιρέτης του a και b διαιρεί το d .

• Απόδειξη:

Έστω $U = \{k \in \mathbb{N} \mid k = ua + vb, u, v \in \mathbb{Z}\} \subseteq \mathbb{N}$.
Ισχύει $U \neq \emptyset$ αφού $\begin{cases} a = 1 \cdot a + 0 \cdot b \in U \\ b = 0 \cdot a + 1 \cdot b \in U \end{cases}$

Από "αξίωμα ελάχιστου", έχουμε ότι το U έχει ελάχιστο στοιχείο, έστω d . Προφανώς $d = xa + yb$, $x, y \in \mathbb{Z}$. Είναι όμως κοινός διαιρέτης των a, b ?

Αρκεί ν.δ.ο το d διαιρεί κάθε στοιχείο του U .

Έστω άρα, $\exists k \in U$ τ.ω. $d \nmid k$. Από Ευκλείδεια Διαίρεση, έχουμε ότι $k = q \cdot d + r$, $0 < r < d$. Όμως αφού $k \in U$, $\exists u, v \in \mathbb{Z}$ τ.ω. $k = ua + vb \Rightarrow r = k - qd = ua + vb - q(xa + yb) = (u - qx)a + (v - qy)b$, το οποίο $\in U$, αντί της ιδιότητας του d ως ελάχιστο στοιχείο του U και $r < d$ ✗.

Άρα $d \mid k \ \forall k \in U \Rightarrow d \mid a, d \mid b$.

Διαιρεί κάθε κοινός διαιρέτης του a, b το d ?

Έστω $\lambda \mid a$ και $\lambda \mid b \Rightarrow \lambda \mid ax + by \Rightarrow \lambda \mid d$.

• Ορισμός:

Ονομάζουμε Μέγιστο Κοινό Διαιρέτη των $a, b \in \mathbb{Z}$ του μοναδικού d με τις ακόλουθες ιδιότητες.

(i) $d \geq 0$

(ii) $d \mid a, d \mid b$

(iii) $\lambda \mid a, \lambda \mid b \Rightarrow \lambda \mid d$

Τον συμβολίζουμε με (a, b) .

↳ Παρατήρηση:

Ο Bezout εκπληκνύεται και σε πιθανούς αρνητικούς ακέραιους a, b . Αν d ικανοποιεί το Bezout, και ο $-d$ το ικανοποιεί. Οπότε παίρνουμε ως του μοναδικού πέγχο του $|d|$.

• Παρατήρηση:

Αν $(a, b) = 1$, τότε ο a και b είναι πρώτοι μεταξύ τους. Άρα οι μόνοι κοινοί διαιρέτες είναι το ± 1 . Απο Bezout, $\exists x, y \in \mathbb{Z}$ π.ω. $ax + by = 1$. Αντιστοφθα, αν βρεθούν $x, y \in \mathbb{Z}$ π.ω. $ax + by = 1$, τότε $(a, b) \mid a \wedge (a, b) \mid ax + by = 1 \Rightarrow (a, b) \mid 1$.

Δηλαδή για $a, b \in \mathbb{Z} : (a, b) = 1 \Leftrightarrow ax + by = 1$
 $x, y \in \mathbb{Z}$.

• Παράδειγμα:

Δείξτε ότι ο $\sqrt{2}$ άρρητος.

• Λύση:

Έστω ότι $\sqrt{2}$ είναι ρητός. Θα καταλήξω σε άτοπο.

$$\text{Τότε } \sqrt{2} = \frac{a}{b}, a, b \in \mathbb{Z}, (a, b) = 1 \Rightarrow$$

$$ax + by = 1, \quad xy \in \mathbb{Z}.$$

$$\begin{aligned} \text{Άρα } \sqrt{2} &= \sqrt{2} \cdot 1 = \sqrt{2} (ax + by) = \sqrt{2} ax + \sqrt{2} by \\ &= \sqrt{2} \cdot \sqrt{2} b \cdot x + \sqrt{2} \cdot \frac{a}{\sqrt{2}} \cdot y = 2bx + ay \in \mathbb{Z} \quad \text{✗} \end{aligned}$$

• Παράδειγμα:

Δείξτε ότι $(n! + 1, (n+1)! + 1) = 1, \forall n \in \mathbb{N}$.

• Λύση:

Έστω για $n \in \mathbb{N}$, $(n! + 1, (n+1)! + 1) = d$. Άρα
 $d \mid n! + 1 \Rightarrow d \mid (n! + 1)(n+1) = (n+1)! + (n+1)$
 $d \mid (n+1)! + 1$

$$\Rightarrow d \mid (n+1)! + (n+1) - \{(n+1)! + 1\} \Rightarrow d \mid n$$

$$d \mid n \Rightarrow \left. \begin{matrix} d \mid n! \\ d \mid n! + 1 \end{matrix} \right\} d \mid n! + 1 - n! \Rightarrow d \mid 1 \Rightarrow d = 1.$$

13/02/2025

Ιδιότητες ΜΚΔ:

- $(a, b) = (b, a)$ αντιμεταθετικότητα
- $(a, (b, c)) = ((a, b), c)$ προσεταιριστικότητα
- $(ac, bc) = |c| (a, b)$ επηρεριστικότητα

Απόδειξη:

Έστω $d = (a, b)$, $e = (ac, bc)$ Ο.Σ.Ο. $e = k|d|$

Από Bezout έχουμε ότι $d = ax + by$, $x, y \in \mathbb{Z}$
 $\Rightarrow c \cdot d = cax + cby$

Από $e|ac$ } $e|cax + cby \Rightarrow e|cd$
 $e|bc$ }

Από την αλλαγή, $cd|ca$ } $\Rightarrow cd|e$
 $cd|cb$ }

Άρα, από ιδιότητες διαμετόντας: $|c| \cdot d = e$

- $(a, 1) = 1$
- $(a, 0) = |a|$
- $c|(a, b) \Rightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{|c|}$

Απόδειξη:

Από Bezout, $(a, b) = ax + by$, $x, y \in \mathbb{Z}$.
Επίσης, $c|(a, b) \Leftrightarrow c|a, c|b$

Άρα $\frac{a}{c} \cdot x + \frac{b}{c} y = \frac{(a,b)}{c}$.

Άρα την άλλν, $(\frac{a}{c}, \frac{b}{c}) \mid \frac{(a,b)}{c}$
 αφού, όπως στην απόδειξη Βεζουίτ,
 διαφέρει κατά το ίδιο γραμμικό συνδυασμό.

Αφού όπως $\left. \begin{array}{l} \frac{(a,b)}{c} \mid \frac{a}{c} \\ \frac{(a,b)}{c} \mid \frac{b}{c} \end{array} \right\} \Rightarrow \frac{(a,b)}{c} \mid \left(\frac{a}{c}, \frac{b}{c} \right)$

$$\Rightarrow \frac{(a,b)}{|c|} = \left(\frac{a}{c}, \frac{b}{c} \right)$$

• Εξιδιοτέρα: $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1$

• Λήμμα Ευκλείδη:

Αν $a \mid bc$ και $(a,b)=1$, τότε $a \mid c$

• Απόδειξη:

$(a,b)=1 \xRightarrow{\text{Bezout}} ax+by=1. \quad x,y \in \mathbb{Z}$
 $\Rightarrow cax+cby=c$

Όπως (Υπόθεση) $\left. \begin{array}{l} a \mid bcy \\ a \mid acx \end{array} \right\} \Rightarrow a \mid cax+cby=c$

Πιο γενικά, αν $a \mid bc \Leftrightarrow a \mid (a,b)(a,c)$

- $(a, bc) = (a, (a, b)c)$

Απόδειξη:

Επειδή $(a, (a, b)c) \mid (a, b)c$ και γι' αυτό τον $(a, b) \mid c \Rightarrow (ca, cb)$.

Άρα $(a, (a, b)c) \mid bc$ } $\Rightarrow (a, (a, b)c) \mid (a, bc)$
 And $(a, (a, b)c) \mid a$

Όπως $(a, bc) \mid a \Rightarrow (a, bc) \mid ac$ } $\Rightarrow$
 $(a, bc) \mid bc$ δ

$\Rightarrow (a, bc) \mid (ac, bc) = (a, b) \mid c$ } $(a, bc) \mid (a, (a, b)c)$
 $(a, b) \mid a$ } $\checkmark$

- Ειδικότερα, αν $(a, b) = 1$, τότε $(a, bc) = (a, c)$.

Επίσης, αν $(a, b) = (a, c) = 1 \Leftrightarrow (a, bc) = 1$

" $\Rightarrow$ " από πάνω

" $\Leftarrow$ " $\left. \begin{matrix} d \mid a \\ d \mid b \end{matrix} \right\} \Rightarrow d \mid (a, b) \Rightarrow d = 1$

- $(a, b) = 1, a \mid c, b \mid c \Rightarrow ab \mid c$

Απόδειξη:

Υπάρχουν $x, y \in \mathbb{Z}$ π.ω. $ax + by = 1 \Rightarrow$

$cax + cby = c$

Όπως $b \mid c \Rightarrow ab \mid ac$ } $ab \mid cax + cby = c$
 $a \mid c \Rightarrow ab \mid cb$ }

* • $(a,b)=1$, $c|ab \Rightarrow \exists! c_1, c_2 \in \mathbb{Z}$ π.ω. $c=c_1c_2$
 και $c_1|a$, $c_2|b$ με $c_1=(a,c)$, $c_2=(b,c)$

* • Παράδειγμα:

Π.δ.ο. $\forall n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$,
 ισχύει ότι $a|b \Leftrightarrow a^n|b^n$. (Δεδομένου ότι
 $(a,b)^n = (a^n, b^n)$)

• Λύση:

$$" \Rightarrow ": a|b \Rightarrow b = ac \Rightarrow b^n = a^n c^n \Rightarrow a^n|b^n$$

" $\Leftarrow$ ":

$$\text{Έστω ότι } a^n|b^n. \text{ Τότε } \frac{(a,b)^n \cdot a^n \cdot c}{(a,b)^n} = \frac{(a,b)^n \cdot b^n}{(a,b)^n}$$

$$\text{Από νωρίτερα, έχω } \left(\frac{a^n}{(a,b)^n}, \frac{b^n}{(a,b)^n} \right) = 1$$

$$\frac{a^n}{(a,b)^n} \cdot c = \frac{b^n}{(a,b)^n} \Rightarrow \frac{a^n}{(a,b)^n} = 1 \Rightarrow a^n = (a,b)^n \Rightarrow$$

$$\Rightarrow a = (a,b) \Rightarrow a|b$$

• Ευκλείδης Αλγόριθμος

(Για εύρεση και όχι μόνο ύπαρξη)
 ΜΚΔ των a, b

Έστω $0 < b < a$. Τότε $a = qb + r$, $0 \leq r < b$

1^ο Βήμα :

- Αν $r = 0$, δηλαδή $b \mid a$, $(a, b) = b$
- Αν $r \neq 0$, $(a, b) = (b, r)$.

$$\left\{ \begin{array}{l} (a, b) \mid a \\ (a, b) \mid qb \end{array} \right\} \left\{ \begin{array}{l} (a, b) \mid a - qb = r \\ (a, b) \mid b \end{array} \right\} (a, b) \mid (b, r)$$

$$\text{Άρα την αλλαγή, } \left\{ \begin{array}{l} (b, r) \mid b \\ (b, r) \mid qb + r = a \end{array} \right\} (b, r) \mid (a, b) \quad \checkmark$$

Συνεχίζουμε επαναλαμβάνοντας την ίδια διαδικασία, η οποία τερματίζει μετά από πεπερασμένο αριθμό βημάτων ως:

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$\vdots$

$$r_n = \mu \kappa \Delta$$

$$r_{n-1} = q_n r_n + r_{n+1} \quad \circ$$

$\leadsto \circ \mid \mu \kappa \Delta$ των (a, b) είναι το τελευταίο μη μηδενικό υπόλοιπο.

Παρατηρώ, έχουμε ότι :

$$a > b > r_1 > r_2 > \dots > r_n > r_{n+1} = 0 \quad \text{και}$$

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n$$

Πως ξέρω ότι όντως τερματίζει σε η βήματα?

Η ανσπερά φθίνουσα ακολουθία $a, b, r_1, \dots, r_{n+1}$ αποτελείται από φυσικούς αριθμούς, και άρα

από Αξίωμα Ελάχιστου Ινδενίξου.

• Παράδειγμα:

Έστω $a=356$, $b=156$. $\mu\kappa\Delta = ?$

• Λύση:

$$356 = 2 \cdot 156 + 44$$

$$156 = 3 \cdot 44 + 24$$

$$44 = 1 \cdot 24 + 20$$

$$24 = 1 \cdot 20 + 4$$

$$20 = 5 \cdot 4 + 0$$

$$\mu\kappa\Delta(356, 156) = 4$$

• Παρατήρηση:

Χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, μπορούμε, εκτός από τον $\mu\kappa\Delta$ των a, b , μπορούμε να βρούμε και μια (από τις άλλες) παράσταση του $\mu\kappa\Delta$ ως γραμμικό συνδυασμό των a, b .

$$4 = 356x + 156y$$

$$44 = 356 - 2 \cdot 156$$

$$24 = 156 - 3 \cdot 44$$

$$20 = 44 - 1 \cdot 24$$

$$4 = 24 - 1 \cdot 20$$

$$\begin{aligned} \rightarrow 4 &= 24 - 1 \cdot 20 = 24 - (44 - 24) = 2 \cdot 24 - 44 = \\ &= 2(156 - 3 \cdot 44) - 44 = 2 \cdot 156 - 7 \cdot 44 = \end{aligned}$$

$$= 2 \cdot 156 - 7(356 - 2 \cdot 156) =$$

$$= 16 \cdot 156 - 7 \cdot 356$$

Άρα $4 = 356(-7) + 156(16)$
 $x = -7, y = 16$

• Παράδειγμα: $(a, b) = 1, a/bc \Rightarrow a/c$

• Λύση: Δφοῦ $(a, b) = 1$, στον Ευκλείδιο έχουμε

$$b = q_1 a + r_1$$

$$a = q_2 r_1 + r_2$$

⋮

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \rightsquigarrow 1 \rightarrow \text{Υπόθεση}$$

$$r_{n-1} = q_n r_n + r_{n+1}$$

Πολλαπλασιάζω όλα τα μέλη με c

$$cb = cq_1 a + cr_1$$

$$ca = cq_2 r_1 + cr_2$$

⋮

$$cr_{n-2} = cq_{n-1} r_{n-1} + c$$

$$cr_{n-1} = cq_n r_n$$

$$\left. \begin{array}{l} a | cr_1 \\ a | cr_2 \\ \vdots \\ a | c \end{array} \right\} \begin{array}{l} \text{ως παραφ.} \\ \text{συνδυασμοί} \end{array}$$

• Συνεχής Κλάσματα:

• Ορισμός:

Ένα πεπερασμένο συνεχές κλάσμα, είναι μια έκφραση της μορφής :

$$r = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ddots + \frac{1}{a_n}}}}$$

με $a_i \in \mathbb{R}^*$, $i \geq 1$

Συμβολίζουμε $r = \langle a_1, a_2, \dots, a_n \rangle$

Αν $a_1 \in \mathbb{Z}$, $a_i \in \mathbb{Z}_+$, $\forall i \geq 1$, ονομάζεται
αηδὸ πεπερασμένο συνεχὲς κλάσμα.

• Θεώρημα:

Καθε αηδὸ πεπερασμένο συνεχὲς κλάσμα,
εἶναι ἓνας ρητὸς ἀριθμὸς. Αντιστρόφως,
καθε ρητὸς ἀριθμὸς, μπορεῖ νὰ ἀναπαρ-
σταθῇ ὡς αηδὸ πεπερασμένο συνεχὲς
κλάσμα.

19/02/2025

$$t = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots \frac{1}{a_n}}}}$$

$a_1 \in \mathbb{Z}$
 $a_i \in \mathbb{Z}^+, i \geq 1$

Θεώρημα:

Κάθε απλό πεπερασμένο συνεχές κλάσμα είναι ένας ρητός. Αντίστροφα, κάθε ρητός γράφεται ως τέτοιο.

" $\Rightarrow$ " Έστω $t = \langle a_0, a_1, \dots, a_n \rangle$ ένα απλό πεπερασμένο συνεχές κλάσμα. Αφού ο t περιλαμβάνει πεπερασμένο πλήθος πράξεων πολλαπλασιασμών και διαίσεων ακεραίων αριθμών, ο t είναι ρητός αριθμός.

" $\Leftarrow$ " Έστω $r = \frac{a}{b}$ ένας ρητός και έστω $b > 0$ Ευκλείδειδος αλγόριθμος.

$$a = a_0 b + r_1 \quad (1)$$

$$b = a_1 r_1 + r_2 \quad (2)$$

$$r_1 = a_2 r_2 + r_3 \quad (3)$$

$\vdots$

$$r_{n-2} = a_{n-1} r_{n-1} + r_n$$

$$r_{n-1} = a_n r_n + 0, \quad 0 \leq r_i < r_{i-1}$$

$$\frac{a}{b} \stackrel{(1)}{=} \frac{a_0 b + r_1}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} =$$

$$(2) \quad a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} =$$

$$(3) \quad = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = \dots =$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots \frac{1}{a_n}}}}} \quad a_n = \frac{r_{n-1}}{r_n}$$

$$= \langle a_0, a_1, \dots, a_n \rangle \quad \square.$$

• Παρατήρηση:

Αν $a_n = 1$, Θέτοντας $a_n = a_{n-1} + \frac{1}{1}$
 έχουμε ότι $\underbrace{\langle a_0, a_1, \dots, a_n \rangle}_{n+1 \text{ όροι}} = \underbrace{\langle a_0, a_1, \dots, a_{n-1}, 1 \rangle}_n$

Αν $a_n > 1$, Θέτοντας $a_n = a_{n-1} + \frac{1}{1}$
 έχουμε ότι $\underbrace{\langle a_0, \dots, a_n \rangle}_{n+1 \text{ όροι}} = \underbrace{\langle a_0, \dots, a_{n-1}, a_{n-1}, 1 \rangle}_{n+2 \text{ όροι}}$

→ Αυτές οι δύο αναπαραστάσεις είναι οι μοναδικές για έναν ρηζο αριθμό ως συνεχείς κλάσματα.

• Παράδειγμα:

Εκφράζω το $\frac{21}{13}$ ως αλγό πηρασμένο συνεχία κλίση.

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

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

$$\frac{21}{13} = 1 + \frac{8}{13} = 1 + \frac{1}{\frac{13}{8}} =$$

$$= 1 + \frac{1}{1 + \frac{5}{8}} = 1 + \frac{1}{1 + \frac{1}{\frac{8}{5}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{3}{5}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{5}{3}}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}} =$$

Άρα $\frac{21}{13} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}$

$\frac{21}{13} = \langle 1, 1, 1, 1, 1, 2 \rangle$

$\hookrightarrow = \langle 1, 1, 1, 1, 1, 1, 1 \rangle^*$

$2 = 1 + \frac{1}{1}$

• Ορισμός:

Ένα άπειρο συνεχές κλάσμα είναι το όριο μιας αλυσίδας πεπερασμένων συνεχών κλάσματων $\langle a_0 \rangle, \langle a_0, a_1 \rangle, \dots, \langle a_0, a_1, \dots, a_n \rangle, \dots$ αν συγκλίνει ($a_i \in \mathbb{R}^*$). Το συμβολίζουμε ως $\lim_{n \rightarrow \infty} \langle a_0, \dots, a_n \rangle = \langle a_0, a_1, \dots, a_n, \dots \rangle$.

Αν $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{Z}^+$ για $i \geq 1$, τότε το κλάσμα ονομάζεται αλγό άπειρο συνεχές κλάσμα.

• Ορισμός:

Έστω $a_0, a_1, \dots, a_n \in \mathbb{R}$ με $a_i > 0$, $\forall i \geq 1$. Το συνεχές κλάσμα $C_i = \langle a_0, a_1, \dots, a_i \rangle$, $0 \leq i \leq n$, ονομάζεται i -στος συγκλινών του συνεχούς κλάσματος $\langle a_0, \dots, a_n \rangle$. Έτσι έχουμε:

$C_0 = \langle a_0 \rangle$, $C_1 = \langle a_0, a_1 \rangle = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$

$$C_2 = \langle a_0, a_1, a_2 \rangle = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_2 a_1 + 1}$$

Για την απόδειξη αυτών των εφρασεων ορίζουμε επαγωγικά τις εξής δύο ακολουθίες:

$$P_{-1} = 1, \quad P_0 = a_0, \quad P_1 = a_1 P_0 + P_{-1}, \dots, P_n = a_n P_{n-1} + P_{n-2}$$

$$q_{-1} = 0, \quad q_0 = 1, \quad q_1 = a_1 q_0 + q_{-1}, \dots, q_n = a_n q_{n-1} + q_{n-2}$$

$\downarrow$
 a_1

Αντικαθιστώντας παραπάνω (επαγωγικά), ισχύει ότι $C_i = \frac{P_i}{q_i}, \forall i \geq 0$.

Πόρισμα:

Έστω $C_i = \frac{P_i}{q_i}$ ο i -στος συχθέντων του $\langle a_0, \dots, a_k \rangle$,

Τότε ισχύει $P_i q_{i-1} - q_i P_{i-1} = (-1)^{i-1}$

Απόδειξη: (επαγωγικά)

Για $i=1$, έχουμε $P_1 \cdot q_0 - q_1 P_0 = (a_1 a_0 + 1) \cdot 1 - a_1 a_0 = a_1 a_0 + 1 - a_1 a_0 = 1 = (-1)^0$

ε.β: Έστω ότι ισχύει για $i-2$. Δηλαδή:

$$P_{i-1} q_{i-2} - q_{i-1} P_{i-2} = (-1)^{i-2}$$

$$\begin{aligned} P_i q_{i-1} - q_i P_{i-1} &= (a_i P_{i-1} + P_{i-2}) \cdot q_{i-1} - (a_i q_{i-1} + q_{i-2}) P_{i-1} \\ &= \cancel{a_i P_{i-1} q_{i-1}} + P_{i-2} q_{i-1} - \cancel{a_i P_{i-1} q_{i-1}} - q_{i-2} P_{i-1} = \\ &= - (q_{i-2} P_{i-1} - q_{i-1} P_{i-2}) = - (-1)^{i-2} = (-1)^{i-1} \quad \square \end{aligned}$$

Πόρισμα:

Έστω ότι $\langle a_0, \dots, a_n \rangle$ αλγό συνεχές κλειστό.
Τότε οι ακέραιοι P_i, q_i είναι σχετικά
πρώτοι μεταξύ τους. Οποίως $(P_i, P_{i+1})=1$,
 $(q_i, q_{i+1})=1$.

Ανέκδοξος:

Από προηγούμενο πόρισμα, έχουμε ότι:

$$P_i q_{i-1} - q_i P_{i-1} = (-1)^{i-1} \cdot (-1)^{i+2}$$

$$\Rightarrow P_i q_{i-1} (-1)^{i+1} - q_i P_{i-1} (-1)^{i+2} = 1 \Rightarrow$$

$$\text{Από υπάρχον } \left. \begin{array}{l} x = (-1)^{i+2} q_{i-1} \\ y = (-1)^{i+2} P_{i-1} \end{array} \right\} P_i x + q_i y = 1 \Rightarrow$$

$$(P_i, q_i) = 1$$

□.

Θεώρημα:

Έστω $a_i \in \mathbb{Z}$ με $a_i \geq 1, \forall i \geq 1$. Τότε το αηδίο άπειρο συνεχές κλάσμα $\alpha = \langle a_0, a_1, \dots \rangle$ είναι ένας άρρητος αριθμός. Αντίστροφα, κάθε άρρητος αριθμός μπορεί να παρασταθεί ως ένα αηδίο άπειρο συνεχές κλάσμα με μοναδικό τρόπο.

Απόδειξη:

" $\Rightarrow$ " Επιπλέον αποτελέσματα για τα C_i .

" $\Leftarrow$ ":

Έστω x_i άρρητος αριθμός. Επαγωγικά, ορί-
ζουμε:

$$x_0 = x$$

$$x_{k+1} = \frac{1}{x_k - a_k}, \quad k=0, 1, 2, \dots \text{ με } a_k = [x_k] \text{ το ακέραιο μέρος του } x_k, \text{ δηλαδή μέγιστος ακέραιος } \leq x_k.$$

$$\text{Ο.δ.ο. } x = \langle a_0, a_1, \dots \rangle$$

$\leadsto$ Αφού x άρρητος, τότε x_k άρρητος, αλλιώς από $x_k = \frac{1}{x_{k-1} - [x_{k-1}]}$ θα είχε

$$x_{k-1} = \frac{1}{x_k} + [x_{k-1}] \text{ Θα ήταν ρητός! Απορρο}$$

$\leadsto$ Αφού ο x_k άρρητος, $x_k \neq [x_k] \Rightarrow [x_k] < x_k < [x_k] + 1 \Rightarrow 0 < x_k - [x_k] < 1 \Rightarrow x_{k+1} = \frac{1}{x_k - [x_k]} > 1, \forall k \geq 0$

$\leadsto \sum \alpha_i \delta_{i,k}$, έχουμε:

$$X = X_0 = \lfloor X_0 \rfloor + \frac{1}{X_1} \quad \left\{ \begin{array}{l} X_1 = \frac{1}{X_0 - \lfloor X_0 \rfloor} \Rightarrow X_0 - \lfloor X_0 \rfloor = \frac{1}{X_1} \\ \text{"} \lfloor X_0 \rfloor \text{" } X_1 \end{array} \right.$$

$$\Rightarrow X_0 = \lfloor X_0 \rfloor + \frac{1}{X_1}$$

||

$$X = \lfloor X_0 \rfloor + \frac{1}{X_1} = \lfloor X_0 \rfloor + \frac{1}{\lfloor X_1 \rfloor + \frac{1}{X_2}} =$$

$$= \dots = \langle \lfloor X_0 \rfloor, \lfloor X_1 \rfloor, \dots, \lfloor X_k \rfloor, X_{k+1} \rangle$$

$\leadsto$ Θυμάμαι ότι, αφού $X_k > 1 \quad \forall k \geq 1$,

$$X = \langle \lfloor X_0 \rfloor, \lfloor X_1 \rfloor, \dots, \lfloor X_k \rfloor, X_{k+1} \rangle =$$

$$= \frac{X_{k+1} \cdot p_k + p_{k-1}}{X_{k+1} \cdot q_k + q_{k-1}} \Rightarrow$$

$$\Rightarrow X - C_k := \frac{X_{k+1} \cdot p_k + p_{k-1}}{X_{k+1} \cdot q_k + q_{k-1}} - \frac{p_k}{q_k} =$$

$$= \frac{q_k (X_{k+1} p_k + p_{k-1}) - p_k (X_{k+1} q_k + q_{k-1})}{q_k (X_{k+1} q_k + q_{k-1})} =$$

$$= \frac{\cancel{q_k X_{k+1} p_k} + q_k p_{k-1} - \cancel{p_k X_{k+1} q_k} - p_k q_{k-1}}{q_k (X_{k+1} q_k + q_{k-1})} =$$

$$= \frac{(-1)^{k-1}}{q_k (X_{k+1} q_k + q_{k-1})}$$

$\leadsto$ Αφού $x_{k+1} > [x_{k+1}]$, έχω

$$|x - C_k| = \frac{1}{(x_{k+1}q_k + q_{k-1})q_k} < \frac{1}{([x_{k+1}]q_k + q_{k-1})q_k} = \\ = \frac{1}{q_{k+1} \cdot q_k}$$

και αφού οι ακεραίοι q_k αποτελούν
αύξουσα ακολουθία (από τον ορισμό του),
 $\frac{1}{q_k \cdot q_{k+1}} \xrightarrow{k \rightarrow \infty} 0$ και άρα:

$$q_k \cdot q_{k+1}$$

$$x = \lim_{k \rightarrow \infty} C_k = \langle [x_0], [x_1], [x_2], \dots \rangle.$$

20/02/2025

$$x = \lim_{k \rightarrow \infty} C_k = \langle [x_0], [x_1], [x_2], \dots \rangle$$

αριθμός k-οστος συλλαβισμός αλφαριθμητικό μέρος

$$x_0 = x$$
$$x_k = \frac{1}{x_{k-1} - [x_{k-1}]}$$

Μοναδικότητα με επαγωγή (έστω δύο παρα-
σώσεις αλφ)

Παρατήρηση:

Οι συλλαβισμοί p_n/q_n είναι οι "καλύτερες προσεγγίσεις του x " όπου πιο κοντά στον x από κάθε άλλο ρητό αριθμό με παρονομαστή $\leq q_n$.

Παράδειγμα:

Γράψε τον $\sqrt{2}$ ως αλφ αριθμο συνεχώς κλάσματα.

Λύση:

$$\begin{aligned} & \text{Ξεκινάω με το αλφαριθμητικό μέρος του, } [\sqrt{2}] = 1. \\ & \sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2} - 1}} = 1 + \frac{1}{\frac{\sqrt{2} + 1}{2 - 1}} = \\ & = 1 + \frac{1}{\sqrt{2} + 1}. \text{ Άρα } [\sqrt{2} + 1] = 2 \Rightarrow \end{aligned}$$

$$\sqrt{2} + 1 = 2 + (\sqrt{2} + 1 - 2) = 2 + (\sqrt{2} - 1) =$$

$$= 2 + \frac{1}{\sqrt{2} + 1}$$

Τελικά έχουμε

$$\sqrt{2} = \langle 1, 2, \sqrt{2} + 1 \rangle = \boxed{\langle 1, 2, 2, 2, \dots \rangle}$$

• Παραδείγματα:

Το ίδιο για το $\sqrt{3}$.

• Λύση:

$$\lfloor \sqrt{3} \rfloor = 1$$

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{3} - 1}} = 1 + \frac{1}{\frac{\sqrt{3} + 1}{3 - 1}} =$$

$$= 1 + \overset{a_0}{\frac{1}{\frac{\sqrt{3} + 1}{2}}}$$

$$\frac{\sqrt{3} + 1}{2} = \frac{2 + (\sqrt{3} + 1) - 2}{2} = \frac{2 + \sqrt{3} - 1}{2} =$$

$$= \underbrace{1}_{a_1} + \frac{\sqrt{3} - 1}{2} = 1 + \frac{1}{\sqrt{3} - 1}$$

Θεώρημα:

Έστω $a_1, a_2 \in \mathbb{Z}^*$. Η $a_1x_1 + a_2x_2 = b$ (*)
έχει λύση στο $\mathbb{Z} \iff \text{MCD}(a_1, a_2) \mid b$.
Επιπλέον, αν βρω μια λύση (u_1, u_2) ,
τότε και όλες οι άλλες λύσεις είναι της
μορφής
$$\begin{cases} x_1 = u_1 + k \cdot \frac{a_2}{(a_1, a_2)} \\ x_2 = u_2 - k \cdot \frac{a_1}{(a_1, a_2)} \end{cases}, \quad k \in \mathbb{Z}.$$

Απόδειξη:

" $\Leftarrow$ ":

Έστω ότι $(a_1, a_2) \mid b$, άρα $\frac{b}{(a_1, a_2)} = c \in \mathbb{Z}$.

Από Bezout, $\exists y_1, y_2 \in \mathbb{Z}$, τ.ω.
 $a_1y_1 + a_2y_2 = (a_1, a_2) \Rightarrow \cdot c$

$$ca_1y_1 + ca_2y_2 = c(a_1, a_2) = b.$$

Η (*) έχει λύση τη (y_1c, y_2c)

Υπαρξή λύσης, όχι συγκεκριμένη.

Έστω ότι (u_1, u_2) μια λύση της (*).
Τότε, αντικαθιστώντας τους $x_1 = u_1 + k \frac{a_2}{(a_1, a_2)}$,
 $x_2 = u_2 - k \frac{a_1}{(a_1, a_2)}$, βρίσκω ότι
επαληθεύουν την (*).

$$a_1 \left(u_1 + k \frac{a_2}{(a_1, a_2)} \right) + a_2 \left(u_2 - k \frac{a_1}{(a_1, a_2)} \right) =$$

$$= a_1 u_1 + k \frac{a_1 a_2}{(a_1, a_2)} + a_2 u_2 - k \frac{a_1 a_2}{(a_1, a_2)} =$$

$$= a_1 u_1 + a_2 u_2 = b.$$

" $\Rightarrow$ "

Εστω ότι η $a_1 x_1 + a_2 x_2 = b$ έχει λύση (u_1, u_2) . Καταρχάς $\left. \begin{array}{l} (a_1, a_2) \mid a_1 u_1 \\ (a_1, a_2) \mid a_2 u_2 \end{array} \right\} \Rightarrow$

$$\Rightarrow (a_1, a_2) \mid b$$

Εστω τώρα για άπλη λύση της (*) (x_1, x_2) . Ο.δ.ο. χρειάζεται να αποδείξουμε (u_1, u_2) όπως ορίζουν οι τύποι.

$$\begin{cases} a_1 x_1 + a_2 x_2 = b \\ a_1 u_1 + a_2 u_2 = b \end{cases} \stackrel{(-)}{\Rightarrow} a_1 (x_1 - u_1) = a_2 (u_2 - x_2)$$

$$\Rightarrow \frac{a_1}{(a_1, a_2)} (x_1 - u_1) = \frac{a_2}{(a_1, a_2)} (u_2 - x_2) \quad (1)$$

$$\text{Αλλά είδαμε ότι } \left(\frac{a_1}{(a_1, a_2)}, \frac{a_2}{(a_1, a_2)} \right) = 1.$$

Οπότε από λήμμα Ευκλείδη έχουμε:

$$\frac{a_1}{(a_1, a_2)} \mid u_2 - x_2 \quad \text{ή} \quad \frac{a_2}{(a_1, a_2)} \mid x_1 - u_1$$

$$\hookrightarrow u_2 - x_2 = \frac{a_1}{(a_1, a_2)} \Rightarrow \boxed{x_2 = u_2 - \frac{a_1}{(a_1, a_2)}}$$

Επιστρέφω στην (1):

$$\frac{a_1}{(a_1, a_2)} (x_1 - u_1) = \frac{a_2}{(a_1, a_2)} \left(u_2 - u_2 + \frac{a_1}{(a_1, a_2)} \right) \Leftrightarrow$$

$$= \frac{a_1}{(a_1, a_2)} (x_1 - u_1) = \frac{a_2}{(a_1, a_2)} \cdot \frac{a_1}{(a_1, a_2)} \Rightarrow$$

$$\boxed{x_1 = u_1 + \frac{a_2}{(a_1, a_2)}}$$

• Παράδειγμα:

Να λυθεί η Διοφαντική Εξίσωση:

$$392x_1 - 21x_2 = 14$$

• Λύση:

ΜΚΔ των συντελεστών (αριθμοί το πλην).

$$\begin{aligned} 392 &= 21 \cdot 18 + 14 & (392, 21) &= 7 \mid 14 \\ 18 &= 14 \cdot 1 + 4 & \text{Άρα Δίνεται.} \\ 14 &= 7 \cdot 2 + 0 \end{aligned}$$

Χρειαζόμαστε μια λύση!

Από Ευκλείδειο αλγόριθμο:

$$14 = 392 - 21 \cdot 18$$

$$7 = 21 - 14 \cdot 1$$

$$7 = 21 - 14 \cdot 1 = 21 - 392 + 21 \cdot 18 = 21 \cdot 19 - 392$$

$$2 \cdot 7 = 2 \cdot 21 \cdot 19 - 2 \cdot 392 \Rightarrow 14 = 392(-2) - 21(-2 \cdot 19)$$

Άρα λύση $(-2, -38)$

Από Θεώρημα, όλες οι λύσεις είναι οι

$$\begin{cases} x_1 = -2 + \left(-\frac{21}{7}\right)k \\ x_2 = -38 - \left(\frac{392}{7}\right)k \end{cases} = \begin{cases} x_1 = -2 - 3k \\ x_2 = -38 - 56k \end{cases}, k \in \mathbb{Z}$$

↳ Παρατήρηση:

$$a_1 x_1 + a_2 x_2 = b \Rightarrow x_2 = -\frac{a_1}{a_2} x_1 + \frac{b}{a_2}$$

Είναι μια ευθεία με κλίση $-\frac{a_1}{a_2}$.

Αν $a_1 \cdot a_2 < 0$, η κλίση είναι θετική.
 $\Rightarrow$ αμέτρητο πλήθος θετικών πραγματικών λύσεων. Αν βρω μια θετική ακέραια λύση της εξίσωσης, τότε υπάρχουν αμέτρητες λύσεις.

Αντίθετα, αν $a_1 \cdot a_2 > 0$, τότε η κλίση είναι αρνητική. Άρα, έχω το πολύ πεπερασμένο πλήθος θετικών ακέραιων λύσεων.

~> Προηγούμενο Παράδειγμα:

Παρατηρεί με έλεγχο ότι για $k = -1$, παίρνουμε τη μικρότερη θετική ακέραια λύση $(1, 18)$. Τότε οι λύσεις δίνονται ισόδια-
 ναμα: $(1 - 3k, 18 - 56k)$.

Επίσης αν $k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$. Άρα
έχω $\boxed{(1+3k, 18+56k)}$, $k \in \mathbb{Z}$.

$\leadsto$ Άλλες θετικές ακέραιες λύσεις, που
το y ξερά και από την κλίση $-\frac{21}{392} > 0$.

$\leadsto$ Εναλλακτικά (για την $(1, 18)$)

Ποιος είναι ο μικρότερος θετικός ακέραιος
αριθμός ο οποίος, όταν διαιρεθεί με το
392 και το 21, αφήνει υπόλοιπο 3 και
17 αντίστοιχα.

Λύση:

Έστω x ο ζητούμενος ακέραιος:

$$\begin{cases} x = 392x_1 + 3 \\ x = 21x_2 + 17 \end{cases} \Rightarrow \begin{cases} 392x_1 + 3 = 21x_2 + 17 \\ 392x_1 - 21x_2 = 14 \end{cases}$$

Λύνω τη Διοφαντική: $x = 392 \cdot 1 + 3 = 395$

Παράδειγμα:

Να βρεθεί το πλῆθος των θετικών ακέ-
ραιων λύσεων της $392x_1 + 21x_2 = 14$

Λύση:

Με αντίστοιχο τρόπο με πριν, έχουμε τη
γενική λύση την $(-2+3k, 38-56k)$, $k \in \mathbb{Z}$.

Οι Θέσεις:

$$-2 + 3k > 0 \Rightarrow 3k > 2 \Rightarrow k > 2/3$$

$$38 - 56k > 0 \Rightarrow 56k < 38 \Rightarrow k < 19/20$$

Άρα $k \in \left(\frac{2}{3}, \frac{19}{20} \right)$, αλλά $k \in \mathbb{Z}$ άρα
Αποίτο.

• Παρατήρηση:

Η $a_1 x_1 + \dots + a_n x_n = b$ ανάγεται με επαγωγής
συν δύο μεταβλητές.

• Παράδειγμα:

$$\text{Να λύσει η } 5x_1 + 6x_2 + 3x_3 + 4x_4 = 15$$

• Λύση:

$$(5, 6, 3, 4) = 1, \quad 1 \mid 15 \text{ άρα έχουμε λύση}$$

$$\text{Θέτω } y = 5x_1 + 6x_2, \text{ όπου } (5, 6) = 1.$$

Βρίσκω μια λύση κατασκευάζοντας $t \in \mathbb{Z}$ το
[απλ]: $y = 5(-y) + 6(y) \Rightarrow$ και τη χρησιμοποιώ
στον γενικό τύπο.

$$\begin{cases} x_1 = -y + 6t \\ x_2 = y - 5t \end{cases}, t \in \mathbb{Z}$$

$$\text{Η εξίσωση ανάγεται στην } y + 3x_3 + 4x_4 = 15$$

Τώρα θέλω $z = y + 3x_3$. Ανάλογα:

$$\begin{cases} y = 4z + 3u, & u \in \mathbb{Z} \\ x_3 = -z - u \end{cases}$$

Τέλος, η εξίσωση καταλήγει στην:
 $z + 4x_4 = 15$. Τη λύνω κανονικά:

$$\begin{cases} z = -15 + 2\varphi, & \varphi \in \mathbb{Z} \\ x_4 = 15 - \varphi \end{cases}$$

Συνδυάζοντας τα παραπάνω και έχοντας υπόψιν ότι διαφορετική 2 μεταβλ.
 $1 \rightarrow$ ανίρρα παραφ. $n \rightarrow n-1$ ανίρρα:

Παίρνω συστηματικά:

$$x_4 = 15 - \varphi$$

$$x_3 = -z - u = 15 - 4\varphi - u$$

$$x_2 = y - 5t = 4z + 3u - 5t = -20 + 16\varphi + 3u - 5t$$

$$x_1 = -y + 6t = \dots = 20 - 16\varphi - 3u + 6t$$

5/3/2025

$$5x_1 + 6x_2 + 3x_3 + 4x_4 = 15$$

Άρα η γενική λύση της είναι:

$$x_1 = 60 - 8\varphi - 3u + 6t$$

$$x_2 = -45 + 8\varphi + 3u - 5t \quad t, u, \varphi \in \mathbb{Z}$$

$$x_3 = 13 - 2\varphi - u$$

$$x_4 = 15 - \varphi$$

→ Εναλλακτικός τρόπος επίλυσης γραμμικών Διοφαντικών εξισώσεων (με τη μέθοδο συνεχών κλασμάτων):

Έστω η εξίσωση $a_1x_1 + a_2x_2 = 1$, $(a_1, a_2) = 1$

↳ Ούτως ή άλλως για $a_1x_1 + a_2x_2 = b$
με $d = (a_1, a_2)$, $d|b$
 $\Rightarrow \frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 = \frac{b}{d}$

Λύνω την $\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 = 1$ με

$\left(\frac{a_1}{d}, \frac{a_2}{d}\right) = 1$ και προλίσκω τη λύση με $\frac{b}{d}$

→ Υπολογίζω τον ρητό:

$$\frac{a_1}{a_2} = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \dots + \frac{1}{c_n}}} = \langle c_0, c_1, \dots, c_n \rangle \quad \begin{matrix} c_0 \in \mathbb{Z} \\ c_i \in \mathbb{Z}^+ \end{matrix}$$

Θυμίζω τις αναδρομικές:

$$P_{-1} = 1$$

$$q_{-1} = 0$$

$$P_0 = C_0$$

$$q_0 = 1$$

$\vdots$

$\vdots$

$$P_n = C_n P_{n-1} + P_{n-2}$$

$$q_n = C_n q_{n-1} + q_{n-2}$$

και τους i -σους συνδυασμούς

$$C_i = \frac{P_i}{q_i}$$

$$\text{Άρα } \frac{a_1}{a_2} = \langle C_0, C_1, \dots, C_n \rangle = C_n = \frac{P_n}{q_n}$$

$$\Rightarrow a_1 q_n = a_2 P_n$$

Από Λήμμα Ευκλείδη αφού $a_1 | a_2 P_n$
και $(a_1, a_2) = 1 \Rightarrow a_1 | P_n$. Οφείλει, αφού
 $(q_n, P_n) = 1$, έχουμε $P_n | a_1$, $q_n | a_2 \Rightarrow$
 $\Rightarrow P_n = \pm a_1$, $q_n = \pm a_2$

Αν $a_2 > 0$, αφού $C_n > 0$, έχουμε
 $a_1 = P_n$, $a_2 = q_n$

Επίσης, αποδειχτεί ότι $P_n q_{n-1} - q_n P_{n-1} = (-1)^{n-1}$

$$\text{Άρα } a_1 \cdot q_{n-1} - a_2 \cdot P_{n-1} = (-1)^{n-1}$$

Άρα παίρνω κατευθείαν μια λύση της
Διοφαντικής για να τη χρησιμοποιήσω
στους τύπους. Ειδικότερα, αν:

η περίπτωση: $(-1)^{n-1} = 1$ και η λύση είναι

$$(x_1, x_2) = (q_{n-1}, -P_{n-1})$$

η αριμος: $(-1)^{n-1} = -1$ και $(x_1, x_2) = (-q_{n-1}, p_{n-1})$

Παράδειγμα:

Να υπολογιστεί μια λύση της:
 $63x - 23y = -7$.

Λύση:

$$63x + 23y = 7, \text{ ώστε } a_2 > 0$$

$$\text{Το } \frac{a_1}{a_2} = -\frac{63}{23} = \langle \underbrace{-3}_{c_0}, \underbrace{3}_{c_1}, \underbrace{1}_{c_2}, \underbrace{5}_{c_3} \rangle \rightarrow n=3$$

Χρηάζεται να υπολογιστούν τα p_2, q_2 .
Τα υπολογίζω είτε σταδιακά από τους τύπους τους, είτε από τον 2^ο συχνοδίνοντα:

$$\begin{aligned} c_2 = \frac{p_2}{q_2} &= \langle c_0, c_1, c_2 \rangle = c_0 + \frac{1}{c_1 + \frac{1}{c_2}} = \\ &= -3 + \frac{1}{3 + \frac{1}{1}} = -3 + \frac{1}{4} = -\frac{11}{4} \end{aligned}$$

$$\text{Συνεπώς, έχω } \begin{cases} q_2 = 4 \text{ (} a_2 > 0 \text{)} \\ p_2 = -11 \end{cases}$$

και αφού $n=3$ περικόψω, μια λύση της αρχικής είναι η $(4, 11)$, δηλαδή της $-63x_1 + 23x_2 = 1$ η $(4 \cdot 7, 11 \cdot 7) = (28, 77)$, είναι μια λύση της $-63x_1 + 23x_2 = 7$ $\square$.

(Για να λύσω τη Διοφαντική χρησιμοποιώντας αυτή τη λύση στους τύπους
 $x_1 = u_1 + k \cdot \frac{a_2}{(a_1, a_2)}, \quad x_2 = u_2 - k \cdot \frac{a_1}{(a_1, a_2)}$)

Πρώτοι Αριθμοί

• Ορισμός:

Ένας ακέραιος αριθμός p , λέγεται πρώτος αν $p > 1$ και οι μόνοι θετικοί διαιρετές του είναι το p και το 1 .

π.χ.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31
37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79,
83, 89, 97, 101.

• Θεώρημα:

Κάθε $n > 1$ ακέραιος είναι είτε πρώτος, είτε γινόμενο πρώτων.

↳ Απόδειξη:

• Για $n=2$, ισχύει ότι είναι πρώτος.

• Έστω ότι ισχύει για $k < n$.

Αν n πρώτος ✓

Αν n σύνθετος, θα έχει καίριοιον διαιρετή $d \neq 1, d \neq n$ με $n = c \cdot d$.

Όμως, παρατηρούμε ότι $1 < c, d < n$

και αφού η επαγωγική υπόθεση ισχύει για τα $c, d < n$, και οι δύο είναι πρώτοι, είτε γινόμενο πρώτων. Άρα και το γινόμενο τους γράφεται ως γινόμενο πρώτων.

* Οι πρώτοι αριθμοί, πολλαπλασιαστικά, είναι οι "Θετέλιοι" διότι των φυσικών αριθμών!

Πρόταση:

Αν p πρώτος με $p \nmid a$, τότε $(p, a) = 1$.
Δηλαδή, οι πρώτοι αριθμοί είναι σχετικά πρώτοι με όλους τους άλλους.

Απόδειξη:

Έστω $(a, p) = d$. Τότε $d \mid p \Rightarrow d = 1$ ή $d = p$ είναι αόριστο, γιατί $d \mid a$, άρα $d = 1$.

Πρόταση:

Αν p πρώτος και $p \mid ab$, τότε $p \mid a$ ή $p \mid b$.

Απόδειξη:

Έστω $p \mid ab$. Αν $p \mid a$, τότε ισχύει. Αν $p \nmid a$, τότε $(p, a) = 1$. Λήμμα Ευκλείδη έχουμε $p \mid b$.

Παρατήρηση:

Πιο γενικά, αν p πρώτος και $p \mid a_1 \dots a_n \Rightarrow p \mid a_i$. Αν a_i πρώτοι, τότε $p = a_i$.
Τέλος, προκύπτει ότι αν p πρώτος και $p \mid a$ τότε $p^k \mid a^k$.

• Θεώρημα Ευκλείδη :

Υπάρχουν άπειροι πρώτοι αριθμοί.

• Απόδειξη :

Έστω ότι είναι πεπερασμένοι, $p_1, \dots, p_n$.
Θεωρώ τον $N = 1 + p_1 \cdot p_2 \cdot \dots \cdot p_n$. $N > 1$.
Άρα, N πρώτος ή γινόμενο πρώτων.

$\leadsto$ Αν N πρώτος $\leadsto$ Άτομο, γιατί
 $N > (\Rightarrow \neq)$ όλων των αΐνων πρώτων

$\leadsto$ Έστω ότι είναι γινόμενο πρώτων, άρα
κάποιος p_i . $1 \leq i \leq n$ τον διαιρεί.

$$\left. \begin{array}{l} p_i \mid p_1 \cdot \dots \cdot p_n \\ p_i \mid N \end{array} \right\} p_i \mid N - p_1 \cdot \dots \cdot p_n \Rightarrow p_i \nmid 1 \quad \text{Άτομο}$$

↳ Εναλλακτικά :

Θεωρούμε τον $N = p_1 \cdot \dots \cdot p_n - 1$, $p_1 = 2$

• Παρατήρηση :

Από απόδειξη, αν p_n ο n -στος πρώτος
αριθμός, τότε για κάποιον $m > n+1$, ο
 m -στός πρώτος θα διαιρεί τον
 $2 \cdot 3 \cdot \dots \cdot p_n + 1$ και $p_m \geq p_{n+1}$. Άρα
 $\forall p$ πρώτο, καθορίζεται τουλάχιστον ένας
άλλος μεγαλύτερος πρώτος, διαιρώντας το $2 \cdot 3 \cdot \dots \cdot p + 1$.

π.χ. ο 7 είναι διαμέτρης του $2 \cdot 3 + 1$,
ο 211 του $2 \cdot 3 \cdot 5 \cdot 7 + 1$, αλλά οι
πρώτοι 39 και 509 είναι διαμέτρης
του $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 39 \cdot 509$.

→ Πολλές αποδείξεις υπάρχουν!

(2010):

Έστω $n > 1$ θετικός ακεραίος. Ο n
και ο $n+1$ είναι πρώτοι μεταξύ τους.
Άρα ο $N_2 = n(n+1)$ έχει τουλάχιστον
δύο διαφορετικούς πρώτους διαμέτρης.
Ομοίως, ο N_2 και ο $N_2 + 1$ είναι
πρώτοι μεταξύ τους, άρα $N_3 = N_2(N_2 + 1)$
έχει τουλάχιστον τρεις διαφορετικούς
πρώτους διαμέτρης.

Θέτουμε $N_{k+1} = N_k \cdot (N_k + 1)$, $N_1 = n$
και επαγωγικά ο N_k έχει τουλάχιστον
 k πρώτους παράγοντες. Άρα, το πλῆθος
των πρώτων είναι μεγαλύτερο από κάθε
φυσικό αριθμό.

→ Αριθμοί Fermat:

Θεωρούμε τους αριθμούς $F_n = 2^{2^n} + 1$, για
 $n \in \mathbb{N}$.

1) Δ.ό. είναι ανά δύο σχετικά πρώτοι
μεταξύ τους.

Οι αριθμοί αυτοί ικανοποιούν τη σχέση:
 $F_n = f_0 \cdot f_1 \cdot \dots \cdot f_{n-1} + 2$.

$$\text{Για } n=1: \left. \begin{array}{l} F_0 = 2 + 1 = 3 \\ F_1 = 4 + 1 = 5 \end{array} \right\} f_1 = f_0 + 2$$

Αν ισχύει για n , δείχνουμε ότι ισχύει για $n+1$.

$$F_0 \cdot F_1 \cdot \dots \cdot F_{n-1} \cdot F_n = f_{n-2} \cdot F_n = (f_n - 2) \cdot F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

Τώρα, αν $d|f_k$ και $d|f_\ell$ κοινό διαμέρισμα (με $k < \ell$), τότε $d|f_\ell - (f_0 \cdot f_1 \cdot \dots \cdot f_{k-1} \cdot \dots \cdot f_{\ell-1}) \Rightarrow d|2 \Rightarrow d=1$ ή $d=2$, αλλά όλοι οι f_n περιζω, άρα $d=1 \Rightarrow (f_k, f_\ell) = 1 \forall k, \ell$.

- 2) Τους χρησιμοποιώ για να δείξω την απουσία των πρώτων. Κάθε f_i έχει τουλάχιστον έναν πρώτο διαμέρισμα, ο οποίος δεν διαμερίζει κανέναν άλλο f_j , $j \neq i$. Συνεπώς, για κάθε n , υπάρχουν τουλάχιστον $n+1$ διακεκριμένοι πρώτοι αριθμοί (οι διαμέρισμα των $f_0, \dots, f_n$). Άλλωστε τέτοιοι $\Rightarrow$ άπειροι πρώτοι.

• Παρατήρηση:

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, F_3 , F_4 είναι πρώτοι. Ο F_5 δεν είναι. Η εκκασία του Fermat ότι όλοι οι f_n είναι πρώτοι

κατέγραψε αυτό του Euler το 1739.
Ακόμα αναπάντητο: είναι ο F_4 ο
μεγαλύτερος πρώτος του Fermat?
Αν όχι, είναι άπειροι οι F_n πρώτοι.

→ Ευκλείδους κατασκευές: (Gauss 1801)
Αν το πλάθος των πλευρών ενός
κανονικού πολυγώνου είναι $2^k \cdot f_{m_2} \dots f_{m_r}$
όπου f_{m_i} διακ. πρώτοι αριθμοί Fermat,
τότε, μπορεί να κατασκευαστεί με κανόνα
και διαβήτη, και αντίστροφα.

12/03/2025

Θεώρημα: (Θεμελιώδες Θεώρημα της Αριθμητικής)

Κάθε φυσικός αριθμός $n > 1$, μπορεί να παρασταθεί ως γινόμενο πρώτων παραγόντων, κατά μοναδικό τρόπο.

Απόδειξη: (Με επαγωγή στο n)

$n=2$ ξετριμένα

Έστω. ότι αληθεύει $\forall k < n$. Θ.δ.ο. ισχύει για το n .

$\hookrightarrow$ Αν n πρώτος ✓

$\sim$ Αν n σύνθετος, από προηγούμενο Θεώρημα, ισχύει ότι γράφεται ως γινόμενο πρώτων. Έστω ότι έχουμε δύο τέτοιες παραγοντοποιήσεις

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s = q_1 \cdot q_2 \cdot \dots \cdot q_t.$$

Θ.δ.ο. $s=t$ και ότι $p_i = q_j$ $\forall i$, για κάποιο j

Αφού ο p_1 πρώτος και $p_1 \mid q_1 \cdot q_2 \cdot \dots \cdot q_t$, τότε ο p_1 διαιρεί κάποιον από αυτούς και μάλιστα είναι ίσος με αυτόν και έχουμε $p_1 = q_1$. Διαγράφοντας τους στην ανάλυση, έχουμε ότι $\frac{n}{p_1} = p_2 \cdot \dots \cdot p_s = q_2 \cdot \dots \cdot q_t$.

Όμως $\frac{n}{p_1} < n$, άρα από επαγωγή υπόθεση, έχουμε ότι οι δύο παραγοντοποιήσεις του $\frac{n}{p_1}$ ταυτίζονται

Άρα $s=t$ και $p_i = q_j, \forall i, j$. $\square$

↳ Αν είχαμε συμπεριλάβει το 1 στους πρώτους, θα έπρεπε να επαναδιατυπώσουμε. (π.χ. $1 \cdot 5 \cdot 7 = 5 \cdot 7$).

Αντιπαράδοξα:

Υπάρχουν άλλα σύνολα αριθμών, που δεν ικανοποιούν το αντίστοιχο θεώρημα μοναδικής παραγοντοποίησης.

π.χ. άρτιοι αριθμοί $2\mathbb{Z} = \{\dots, -2, 0, 2, \dots\}$
με διαμετρούτητα β/α αν υπάρχει $\gamma \in 2\mathbb{Z}$ τ.ω. $\alpha = \beta\gamma$.

π.χ. $2 \mid 4$ αλλά $2 + 2 (1 \notin 2\mathbb{Z})$

Αντίστοιχα, ένα στοιχείο p λέγεται πρώτος αν $\nexists \alpha, \beta \in 2\mathbb{Z}$ τ.ω. $p = \alpha \cdot \beta$.

π.χ. $2, 6, 10, 18, \dots$

$\rightarrow 2 \mid 2 \cdot 2$ αλλά $2 + 2$, άρα δεν ισχύει το λήμμα του Ευκλείδη.

$\rightarrow 2 \cdot 18 = 6 \cdot 6$ (δεν ισχύει το θεμελιώδες)

Παρατήρηση:

Στην παραγοντοποίηση του n σε πρώτους, κάποιος p μπορεί να εμφανίζεται παραπάνω από μια φορές. Αν $p_1, p_2, \dots, p_r$ είναι οι διάφοροι πρώτοι παράγοντες και κάθε p_i εμφανίζεται a_i -φορές, τότε μπορούμε να γράψω $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r} = \prod_{i=1}^r p_i^{a_i}$ με $0 < a_i$ για

την ανάλυσή του σε πρώτους. Τότε, το σύνολο των Θετικών Διαμερισμάτων του n είναι το σύνολο των αριθμών της μορφής: $\prod_{i=1}^r p_i^{c_i}$, όπου $0 \leq c_i \leq a_i$.

• Σημείωση:

Αν παίρουμε τους πρώτους αριθμούς κατά αύξουσα σειρά $p_1=2, p_2=3, p_3=5, \dots$

$p_n = n$ -οστός πρώτος, τότε μπορεί να γράψω $n = \prod_{i=1}^{\infty} p_i^{a_i}$ με $0 \leq a_i$. Ισοδύναμα, $n = \prod_{p \in P} p^{a_p}$, $0 \leq a_p$, όπου $P = \{\text{όλοι οι πρώτοι}\}$.

Φυσικά, πρόκειται για πεπερασμένο γινόμενο. Δηλαδή μόνο ένα πεπερασμένο πλήθος εκθετών a_p είναι $\neq 0$, ακόμα και αν το P είναι άπειρο σύνολο.

(*) Συχνά, οι εκθέτες a_i ή a_p συμβολίζονται με $v_p(n)$. Π.χ. 600:

600	2	$\rightarrow 600 = 2^3 \cdot 3 \cdot 5^2$
300	2	
150	2	
75	3	
25	5	$v_2(600) = 3$
5	5	$v_3(600) = 1$
		$v_5(600) = 2$

Ακριβέστερα, $\gamma = v_p(n) \Leftrightarrow p^\gamma | n$, αλλά $p^{\gamma+1} \nmid n$.

• Πρόταση:

Για $m, n \in \mathbb{N}^+$, ισχύουν:

$$1) \quad \text{Up}(n) = 0 \quad \forall p \Leftrightarrow n = 1$$

$$2) \quad \text{Up}(m \cdot n) = \text{Up}(m) + \text{Up}(n)$$

Ειδικότερα: $\text{Up}(n^k) = k \cdot \text{Up}(n)$

$$\underbrace{\left(\prod_{i=1}^{\infty} p_i^{a_i} \right)}_n^k = \prod_{i=1}^{\infty} (p_i^{a_i})^k = \prod_{i=1}^{\infty} p_i^{a_i \cdot k}$$

$$3) \quad \Delta \nu \quad m | n \Leftrightarrow \text{Up}(m) \leq \text{Up}(n) \\ m = n \Leftrightarrow \text{Up}(m) = \text{Up}(n).$$

$$4) \quad [\text{ΜΚΔ}]$$

$$\text{Για } d = (m, n), \quad \text{Up}(d) = \min \{ \text{Up}(m), \text{Up}(n) \}.$$

↳ Proof:

Θ. Σ. Θ. $d = \prod_{p \in P} p^c$, $c = \min \{ \text{Up}(m), \text{Up}(n) \}$
έχει τις χαρακτηριστικές ιδιότητες του
ΜΚΔ των m, n .

- $d > 0$

- $d | m$, ισχύει $0 \leq \min \{ \text{Up}(m), \text{Up}(n) \} \leq \text{Up}(m)$

- $d | n$, —||— $0 \leq \min \{ \text{Up}(m), \text{Up}(n) \} \leq \text{Up}(n)$

- Έστω $e \neq d$ με $e | m$ και $e | n$.

$$\begin{array}{ll} \text{Τότε } \text{Up}(e) \leq \text{Up}(m) & \text{αφού τους} \\ \text{Up}(e) \leq \text{Up}(n) & \text{διαιρεί.} \end{array}$$

Άρα Up μικρότερος και του δύο $\Rightarrow$
 $\text{Up}(e) \leq \min \{ \text{Up}(m), \text{Up}(n) \} \quad \forall p$ πρώτο.
Άρα $e | d$.

• Παρατήρηση:

Για $n = \prod_{i=1}^r p_i^{u_i(n)}$, έχουμε ότι σίγουρα

οι $p_1^0, p_1^1, \dots, p_1^{u_1(n)}$ διαμορούν τον n .

$$\hookrightarrow \# U_{p_1}(n) + 1$$

Αφού ένας Θετικός Διαρέτης n είναι πάντα της μορφής $p_1^{k_1} \dots p_r^{k_r}$ $0 \leq k_i \leq u_i(n) \forall r$, το συνολικό άθροισ των διαρέτων του n είναι ίσο με $\prod_{p \in P} (u_p(n) + 1) = \tau(n)$.

Μάλιστα, προκύπτει ότι αν $(m, n) = 1$, τότε $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$. Αυτό σημαίνει ότι η συνάρτηση $\tau: \mathbb{N}^+ \rightarrow \mathbb{N}$ που ορίζεται όπως επάνω, είναι μια πολλαπλασιαστική αριθμητική συνάρτηση.

• Παράδειγμα:

Δείξτε ότι αν μια δύναμη ρητού είναι ακέραιος, τότε ο αρχικός ρητός είναι ακέραιος. π.χ. $\left(\frac{3}{5}\right)^n \notin \mathbb{Z} \forall n$.

• Λύση:

Έστω ότι $\left(\frac{a}{b}\right)^n \in \mathbb{Z}$, για κάποιο

$n \in \mathbb{N}$, δηλαδή $b^n \mid a^n$. Τότε

$$0 \leq v_p\left(\frac{a^n}{b^n}\right) = v_p(a^n) - v_p(b^n) =$$

$$= n \cdot \text{ur}(a) - n \cdot \text{ur}(b) = n(\text{ur}(a) - \text{ur}(b)).$$

Αφού $n > 0$, έχω $\text{ur}(a) \geq \text{ur}(b)$
 $\forall p$ πρώτο. Άρα $b|a$ και $\frac{a}{b} \in \mathbb{Z}$.

Παράδειγμα:

Το γινόμενο τριών διαδοχικών φυσικών αριθμών δεν μπορεί να είναι δύναμη κάποιου φυσικού αριθμού.

Λύση:

Έστω ότι ο φυσικός αριθμός $(n-1) \cdot n \cdot (n+1) = n(n^2-1)$ είναι η m -οστή δύναμη ενός φυσικού k .

$$\text{Αλλά αν } d|n \Rightarrow d|n^2 \quad \left\{ \begin{array}{l} d|n^2 - n^2 + 1 \Rightarrow d=1 \\ \text{και αν } d|n^2-1 \end{array} \right.$$

Άρα $(n, n^2-1) = 1$, άρα δεν έχουν κανένα κοινό πρώτο αριθμό στην ανάλυσή τους.

$$\text{Άρα } n(n^2-1) = (p_1^{a_1} \cdots p_r^{a_r})(q_1^{b_1} \cdots q_s^{b_s}) \text{ με } p_i \neq q_j \quad \forall i, j.$$

$$\text{Έστω ότι αυτό το γινόμενο ισούται με } k^m = (s_1^{c_1} \cdots s_t^{c_t}) = s_1^{c_1 \cdot m} \cdots s_t^{c_t \cdot m}.$$

Από μοναδικότητα σε ανάλυση πρώτων αριθμών, έχουμε

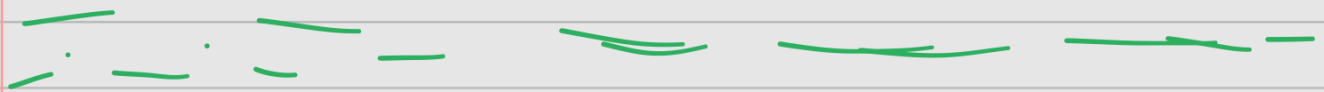
$$p_i^{a_i} = s_n^{c_n \cdot m} \quad , \quad q_j^{b_j} = s_v^{c_v \cdot m}$$

Συνεπώς και οι δύο αριθμοί, n , n^2-1 ,
γράφονται ως m -οστές συνάρσεις οι ίδιοι.

$$(\cdot \cdot \cdot)$$

Αυτό δεν είναι δυνατόν να ισχύει
για δύο διαδοχικούς φυσικούς. Πράγμα-
τα, θεωρώντας την $f: \mathbb{N} \rightarrow \mathbb{N}$
 $a \mapsto a^m$

βλέπουμε ότι $f(a+1) = (a+1)^m > a^m + 1$.



Αριθμητικές Συναρτήσεις

• Ορισμός:

Μια συνάρτηση $f: \mathbb{N}^* \rightarrow \mathbb{R}$ ή $\mathbb{C}$ ή $\mathbb{N}$,
ονομάζεται αριθμητική συνάρτηση.

• Ορισμός:

Η συνάρτηση Möbius ορίζεται ως εξής

$$\mu(n) = \begin{cases} 1, & \text{αν } n=1 \\ (-1)^k, & \text{αν } \nu_p(n)=1 \ \forall p \text{ στο } n = \prod_{i=1}^k p_i \\ 0, & \text{else} \end{cases}$$

Δηλαδή, $\mu(n)=0 \Leftrightarrow 0 < n$ έχει έστω
και έναν παράγοντα > 1 που είναι
τέλειο τετράγωνο.

n	{	1	}	2	}	3	}	4	}	5	}	6	}	-	-	...
$\mu(n)=1$	}	1	}	-1	}	-1	}	0	}	-1	}	1	}			

14/03/2025

$$\mu(n) = \begin{cases} 1, & n=1 \\ (-1)^k, & \text{αν } \nu_p(n)=1 \\ 0, & \text{else} \end{cases}$$

• Θεώρημα: (Άθροισμα Διαφερών)

$$\text{Αν } n \geq 1, \text{ τότε } \sum_{d|n} \mu(d) = \left[\frac{1}{n} \right] = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$$

• Απόδειξη: (Θυμάμαι Διωνυμικό Θεώρημα)

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \dots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

$$\text{Για } n=1: \sum_{d|1} \mu(d) = \mu(1) = 1$$

Για $n>1$, $n = p_1^{a_1} \dots p_k^{a_k}$ και $\sum_{d|n} \mu(d)$ οι μόνοι μη μηδενικοί όροι αυτοί για $d=1$ και αυτοί για τους διαφύτες που είναι γινόμενο διαφύτων πρώτων. Οπότε:

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \dots + \mu(p_k) + \mu(p_1 p_2) + \\ &\quad + \mu(p_1 p_2) + \dots + \mu(p_1 p_k) + \dots + \mu(p_{k-1} p_k) \\ &\quad + \mu(p_1 p_2 p_3) + \dots + \mu(p_1 p_2 \dots p_{k-1} p_k) = \\ &= 1 + \binom{k}{1} (-1)^1 + \binom{k}{2} (-1)^2 + \dots + \binom{k}{k} (-1)^k = \\ &= (1-1)^k = 0 \quad \square \end{aligned}$$

• Ορισμός:

Για $n \geq 1$, η "ολική" συνάρτηση Euler $\phi(n)$, ορίζεται ως το πλήθος των θετικών ακεραίων που δεν ξυμπερνούν τον n και είναι πρώτοι με αυτόν:

$$\phi(n) = 1 + \dots + 1 = \sum_{1 \leq i \leq n, (i,n)=1} 1$$

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

→ Παρατηρώ ότι αν p πρώτος, το $\varphi(p) = p-1$, αφού p σχετικώς πρώτος με όλους τους αριθμούς μικρότερους από αυτόν

* Και εδώ μας ενδιαφέρει το άθροισμα των διαιρετών να δίνεται από έναν τύπο.

↳ Θεώρημα: (Τύπος Gauss)

$$\text{Αν } n > 1, \text{ τότε } \sum_{d|n} \varphi(d) = n$$

• Απόδειξη:

Για φεγγαρισμένο $n > 1$, θεωρώ το σύνολο $S = \{1, 2, \dots, n\}$. Φαράνω μια διαμέριση του S παίρνοντας για κάθε $d|n$ το σύνολο $A(d) = \{k \mid (k, n) = d, 1 \leq k \leq n\}$, δηλαδή εκείνους τους αριθμούς μικρότερους του n με ΜΚΔ τον n ακριβώς τον d . Αυτό το χρίσμα αποτελεί διαμέριση:

• Τα σύνολα είναι ξένα μεταξύ τους:
Εστω $\ell \in A(d) \cap A(d')$, $d \neq d'$, τότε

$$\left. \begin{array}{l} (\ell, n) = d \\ (\ell, n) = d' \end{array} \right\} \text{Απονο}$$

• Η ένωση τους, δίνει το S .

$\bigcup_{d|n} A(d) = S$, αφού έχω ένα τέτοιο σύνολο για κάθε διαιρετή του n .

π.χ. $n=6$ $S = \{1, 2, 3, 4, 5, 6\}$
 $d|6 \leadsto d=1, d=2, d=3, d=6$

$$A(1) = \{k \mid (k, 6) = 1\} = 1, 5$$

$$A(2) = \{k \mid (k, 6) = 2\} = 2, 4$$

$$A(3) = \{k \mid (k, 6) = 3\} = 3$$

$$A(6) = \{k \mid (k, 6) = 6\} = 6$$

Άρα $n = |S| = \left| \bigcup_{d|n} A(d) \right| = \sum_{d|n} |A(d)|$ (*)

Γνωρίζω ότι $(k, n) = d \iff \left(\frac{k}{d}, \frac{n}{d}\right) = 1$ και επίσης ισχύει ότι $0 \leq k \leq n \iff 0 \leq \frac{k}{d} \leq \frac{n}{d}$.

Ορίζω μια 1-1 και επί αντιστοιχία:

$$\begin{array}{ccc} A(d) & \longrightarrow & \{0 < q < \frac{n}{d} \mid (q, \frac{n}{d}) = 1\} \\ \nwarrow & \searrow & \nearrow \\ & \frac{k}{d} & \end{array}$$

Συνεπώς, τα δύο σύνολα έχουν τον ίδιο πληθυσμό, $|A(d)|$ και $\varphi\left(\frac{n}{d}\right)$ αντιστοιχα. Άρα έχω:

$$(*) \quad n = \sum_{d|n} |A(d)| = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

Αλλά, παρατηρώ ότι αυτή η σχέση είναι ισοδύναμη με το ζητούμενο.

Γιατί? Όταν το d διατρέχει τους διαφύτες του n , το ίδιο ακριβώς συμβαίνει με το $\frac{n}{d}$. (Δυσικός τρόπος σκέψης)

$n > n \cdot x$

Για $n=6$:

$$\sum_{d|6} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$$

$$\begin{aligned} \sum_{d|6} \varphi\left(\frac{6}{d}\right) &= \varphi\left(\frac{6}{1}\right) + \varphi\left(\frac{6}{2}\right) + \varphi\left(\frac{6}{3}\right) + \varphi\left(\frac{6}{6}\right) \\ &\quad \quad \quad d=1 \quad \quad \quad d=2 \quad \quad \quad d=3 \quad \quad \quad d=6 \\ &= \varphi(6) + \varphi(3) + \varphi(2) + \varphi(1) = 2 + 2 + 1 + 1 = 6 \end{aligned}$$

• Θεώρημα: (Συνδυασμός φ και μ)

$$\text{Αν } n \geq 1, \text{ τότε } \varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}.$$

• Απόδειξη:

$$\text{Αφού } \left[\frac{1}{(n, k)} \right] = 0 \text{ για όλα τα } k \text{ εκτός από αυτά που έχουν } (n, k) = 1.$$

Μπορώ να γράψω:

$$\varphi(n) = \sum_{\substack{1 \leq i \leq n \\ (i, n) = 1}} 1 = \sum_{k=1}^n \left[\frac{1}{(n, k)} \right].$$

$$\begin{aligned} \text{Άρα έχω } \varphi(n) &= \sum_{k=1}^n \left[\frac{1}{(n, k)} \right] = \sum_{k=1}^n \sum_{d|(n, k)} \mu(d) \\ &= \sum_{k=1}^n \sum_{\substack{d|n \\ d|k}} \mu(d). \end{aligned} \text{ Πρέπει να εμφανιστούν } \text{όσο } \frac{n}{d}.$$

Για έναν συγκεκριμένο διαμέριση d του n ,
 η αθροισμα γίνεται για όλους τους
 ακεραίους $1 \leq k \leq n$ που είναι πολλαπλασιασμοί
 του d , $k = d \cdot q$. Επίσης, $0 < k \leq n \iff$
 $0 < q \leq \frac{n}{d}$, οπότε προκύπτει $\rightarrow 1 \leq k \leq n \iff$
 $1 \leq q \leq \frac{n}{d}$.

$$\begin{aligned} \text{Άρα } \varphi(n) &= \sum_{d|n} \sum_{q=1}^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{\frac{n}{d}} 1 = \\ &= \sum_{d|n} \mu(d) \cdot \frac{n}{d} \quad \square. \end{aligned}$$

• Θεώρημα: (Πολλαπλασιαστικός τύπος)

$$\text{Για } n \geq 1, \quad \varphi(n) = n \prod_{\substack{p|n \\ p \text{ πρώτος}}} \left(1 - \frac{1}{p}\right)$$

$\leadsto p$ οι
πρώτοι διαμερίτες
του n

• Απόδειξη:

• $n=1$ $\varphi(1)=1$

• $n > 1$, έστω $p_1, p_2, \dots, p_r$ οι πρώτοι,

$$\begin{aligned} \text{Έχουμε } \prod_{p|n} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) = \\ &= \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right) = \\ &= \left(1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 p_2}\right) \left(1 - \frac{1}{p_3}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right) = \\ &= \left(1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 p_2} - \frac{1}{p_3} + \frac{1}{p_1 p_3} + \frac{1}{p_2 p_3} - \frac{1}{p_1 p_2 p_3}\right) \\ &\quad \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

$$= \dots = 1 - \sum_{i=1}^r \frac{1}{p_i} + \sum_{\substack{i=1 \\ j=1 \\ i \neq j}}^r \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \dots \\ + \frac{(-1)^r}{p_1 p_2 \dots p_r} \star$$

Όπου π.χ. στον όρο $\frac{1}{p_i p_j p_k}$ έχουμε ένα
 τα 3ηδη γινόμενο διαφόρων
 πρώτων παραγόντων του n . Παρατηρώ ότι
 όλοι οι όροι είναι της μορφής $\pm \frac{1}{d}$ με
 δηλ γινόμενο διαφόρων πρώτων.
 Άρα ο αριθμητής είναι αριθμός $\mu(d)$.

- Αν σε αθροισμα υπάρχει όρος με
 παρονομαστή κίνηση διαρέτη του n
 όχι αυτής της μορφής ($p_i p_j p_k$) τότε
 το μ του θα μηδενίζεται εξ'όριστου.

$$\star = \sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n} \Rightarrow \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

π.χ.

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

$$\varphi(7) = 7 \left(1 - \frac{1}{7}\right) = 7 - 1 = 6$$

• Ιδιότητα της φ :

- $\varphi(m) \leq m-1 \Leftrightarrow$ Όντως

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \leq m \left(1 - \frac{1}{p} \text{ πρώτος}\right) = m - \frac{m}{p} \leq m-1$$

$\frac{m}{p} \geq 1$

$$\bullet \varphi(p^a) = p^a - p^{a-1}, \quad a \geq 1, \quad p \text{ primes}$$

$$\varphi(p^a) = p^a \prod_{q|p^a} \left(1 - \frac{1}{q}\right) = p^a \left(1 - \frac{1}{p}\right) = p^a - p^{a-1} \quad \square.$$

18/03/2025

$$\varphi(n) = n \cdot \prod_{\substack{p|n \\ p \text{ πρώτος}}} \left(1 - \frac{1}{p}\right)$$

$$\bullet \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}, \quad d = (m, n)$$

$$\frac{\varphi(n)}{n} = \prod_{\substack{p|n \\ p \text{ πρώτος}}} \left(1 - \frac{1}{p}\right) \Rightarrow \frac{\varphi(m \cdot n)}{m \cdot n} = \prod_{\substack{p|m \cdot n \\ p \text{ πρώτος}}} \left(1 - \frac{1}{p}\right) = \frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n} \cdot \frac{d}{\varphi(d)}$$

$$\begin{aligned} &= \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)=d} \left(1 - \frac{1}{p}\right)} = \\ &= \frac{\frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}} = \frac{\varphi(m) \cdot \varphi(n) \cdot d}{m \cdot n \cdot \varphi(d)} \Rightarrow \end{aligned}$$

$$\Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}$$

Ειδικά, αν $d=1 \Rightarrow \varphi(m) \cdot \varphi(n) = 1$

• Αν $a|b$, τότε $\varphi(a)|\varphi(b)$ (Άσκηση)

• Για $n \geq 3$, $\varphi(n)$ άρτιο. Μαάλιστα, αν ο n έχει r διαφορετικούς πρώτους πριμογοντες, τότε $2^r | \varphi(n)$.

(> Ουτως, για $n=3$, $\varphi(n)=2$ ✓
Για $n=2^a$, $a \geq 2$, $\varphi(2^a) = 2^a - 2^{a-1} \Rightarrow \varphi(n)$ άρτιος

Αν n έχει έναν τουλάχιστον περιττό
 πρώτο, τότε: $\varphi(n) = n \cdot \prod_{p|n} \frac{p-1}{p} \Rightarrow$ είναι ένας άρτος

$$\varphi(n) = \frac{n}{\prod_{p|n} p} \cdot \prod_{p|n} (p-1) = k \cdot \prod_{p|n} (p-1)$$
για $k \in \mathbb{Z}$.

Άρα $\varphi(n)$ άρτος. Μάλιστα, κάθε
 περιττός πρώτος παράγοντας $p|n$, δίνει
 ακόμα ένα πολλαπλάσιο του 2 στο γινό-
 μενο $\prod (p-1)$. Άρα $2' | \varphi(n)$.

• Έτσι, καθιστούμε όλους τους n , αφού
 είτε θα έχουν μόνο το 2 στην ανάλυση
 πρώτων παραγόντων (2^a), είτε θα έχουν
 κάποιον άλλο παράγοντα, ο οποίος είναι
 περιττός.

• Παράδειγμα:

Το πλήθος των $\frac{a}{b}$ αναγώνων γνησίων
 κλασμάτων ($0 \leq a \leq b$) και έχουν $b \leq n$, ισούται
 με το $\sum_{i=2}^n \varphi(i)$. $\varphi(8) = 4$

Δηλαδή για $n=8$:

$\frac{1}{8}$	$\frac{3}{8}$	$\frac{5}{8}$	$\frac{7}{8}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$
$\frac{4}{7}$	$\frac{5}{7}$	$\frac{6}{7}$	$\frac{1}{6}$	$\frac{5}{6}$	$\frac{1}{5}$	$\frac{2}{5}$
$\frac{3}{5}$	$\frac{4}{5}$	$\frac{1}{4}$	$\frac{3}{4}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{1}{2}$

Που το πλήθος τους είναι ακριβώς

$$\sum_{i=2}^8 \varphi(i) = \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) + \varphi(7) + \varphi(8)$$

Ορισμός :

Αν f και g δύο αριθμητικές συναρτήσεις, τότε το κατά Dirichlet γινόμενο τους (ή συνένδυση Dirichlet) είναι η αριθμητική συνάρτηση $(f+g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right)$.

Παρατήρηση :

Προς το παρόν, απλά μια διευκρίνιση επί του συνόλου των αριθμητικών συναρτήσεων. Αν $M = \{f \mid f: \mathbb{N}^* \rightarrow \mathbb{R} \text{ συνάρτηση}\}$, τότε $*$: $M \times M \rightarrow M$ (κλειστότητα)

$$\begin{aligned} \text{π.χ. } (f+g)(6) &= \sum_{d|6} f(d) g\left(\frac{6}{d}\right) = \\ &= f(1) \cdot g(6) + f(2) g(3) + f(3) g(2) + f(6) g(1). \end{aligned}$$

Παράδειγμα :

Έστω η αριθμητική συνάρτηση $N: \mathbb{N} \rightarrow \mathbb{N} \subset \mathbb{R}$ με $N(n) = n \quad \forall n \in \mathbb{N}$ η σταθερή συνάρτηση στο n . Τότε, το αποτέλεσμα "σύνδεση μεταξύ φ και μ ", που αποδείξαμε, $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$, γίνεται:

$\varphi(n) = \mu * N$

• Πρόταση:

Ο πολλαπλός κατά Dirichlet είναι αντιμεταθετικός.

↳ Απόδ. Πρέπει ν.δ.ο. $f * g = g * f, \forall f, g \in \mathcal{M}$

$$(f * g)(n) = \sum_{d|n} \underbrace{f(d)g\left(\frac{n}{d}\right)}_{a \cdot b = n} = \sum_{\substack{a, b \\ a \cdot b = n}} f(a) \cdot g(b) =$$

Όταν ο d διατρέχει τους διαιρέτες του n , τότε και το $\frac{n}{d}$ τους διατρέχει
 $= \sum_{\substack{a, b \\ a \cdot b = n}} g(b) \cdot f(a) = (g * f)(n).$

• Ορισμός:

Η αριθμητική συνάρτηση $I(n) = \left[\frac{1}{n} \right] = \begin{cases} 1, n=1 \\ 0, n>1 \end{cases}$ ονομάζεται ταυτοτική αριθμητική συνάρτηση.

• Θεώρημα:

Έστω f αριθμητική συνάρτηση $f(1) \neq 0$. Τότε υπάρχει μοναδική αριθμητική συνάρτηση f^{-1} , η Dirichlet αντιστροφή της f , τέτοια ώστε $f * f^{-1} = f^{-1} * f = I$

• Απόδειξη:

Για $n=1$, δεδομένης της f , λύνα ως προς f^{-1} την $(f * f^{-1})(1) = I(1) = 1 \Rightarrow f(1) \cdot f^{-1}(1) = 1 \Rightarrow f^{-1}(1) = \frac{1}{f(1)}$, αφού $f(1) \neq 0$.

Με επαγωγή, έστω ότι $n > 1$ οι τιμές $f^{-1}(k)$ για $k < n$ έχουν προσδιοριστεί μονοσήμαντα. Τότε, δίνω την $(f * f^{-1})(n) = I(n) \Rightarrow$

$$\Rightarrow \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \Rightarrow f(1) f^{-1}(n) + \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

$$\Rightarrow f^{-1}(n) = - \frac{1}{f(1)} \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d).$$

• Παράδειγμα:

Ορίζοντας την αριθμητική μοναδιαία συνάρτηση $u(n) = 1 \quad \forall n \in \mathbb{N}$, εκφράζουμε το αποτέλεσμα "αθροισμα διαμεριζών" για τη μ , $\sum_{d|n} \mu(d) = \left[\frac{1}{n} \right]$ ως:

$$u = \mu^{-1} \text{ και } \mu = u^{-1}, \text{ αφού } \mu * u = I.$$

• Θεώρημα:

Το σύνολο $\mathcal{M}$ των αριθμητικών συναρτήσεων f με $f(1) \neq 0$, αποτελεί αβελιανή ομάδα ως το γινόμενο Dirichlet.

(> Απόδειξη:

Κλειστότητα?: Από την και αν $f(1) \neq 0$ $g(1) \neq 0$ τότε $(f * g)(1) = f(1)g(1) \neq 0$

Ουδέτερο?: Ταυτοτική

Συμμετρικό?: Η και η Dirichlet αντιστροφή

Προσδιοριστική :

$$(f * (g * h))(n) \stackrel{?}{=} ((f * g) * h)(n)$$

$$(f * (g * h))(n) = \sum_{\substack{a, b \\ a \cdot b = n}} f(a) (g * h)(b) =$$

$$= \sum_{\substack{a, b \\ a \cdot b = n}} f(a) \cdot \left(\sum_{\substack{c, d \\ c \cdot d = b}} g(c) \cdot h(d) \right) =$$

$$= \sum_{\substack{a, b \\ a \cdot b = n}} \sum_{\substack{c, d \\ c \cdot d = b}} f(a) \cdot g(c) \cdot h(d) = \sum_{\substack{a, c, d \\ a \cdot c \cdot d = n}} f(a) g(c) h(d) =$$

$$= \dots = ((f * g) * h)(n).$$

19/03/2025

Ορισμός:

Μια αριθμητική συνάρτηση ονομάζεται πολλαπλασιαστική αν $f(1)=1$ και $f(m \cdot n) = f(m) \cdot f(n)$, όταν $\gcd(m, n) = 1$. ($f(m) \neq 0 \forall m$).

Λέγεται πλήρως πολλαπλασιαστική, όταν $f(m \cdot n) = f(m) \cdot f(n) \quad \forall m, n \in \mathbb{N}^*$.

Παράδειγμα:

Έχουμε δείξει ότι $\tau(n) = \prod_{p \in P} (U_p(n) + 1)$ και φ του Euler είναι πολλαί. Επίσης, $f_a(n) = n^a$, αφο είναι πλήρως πολλαί. Ομοίως και η ταυτοτική $I(n) = \left\lfloor \frac{1}{n} \right\rfloor$, όπως και η $N(n) = n$.

Παρατήρηση:

$$f \text{ πολλαί} \iff f(p_1^{a_1} \dots p_k^{a_k}) = f(p_1^{a_1}) \dots f(p_k^{a_k})$$

" $\implies$ ": ορισμός

" $\impliedby$ ": διακριτοί πρώτοι $\rightarrow$ ανάλυση πρώτων παραγ.

$$f \text{ πλήρως πολλαί} \iff f(p^a) = f(p)^a.$$

Θεώρημα:

Το σύνολο των πολλαίων συναρτήσεων είναι υπό-ομάδα της $(\mathcal{M}, *, I)$.

Δηλαδή f, g πολλαί, $f * g$ πολλαί,
 g πολλαί, g^{-1} πολλαί

Μάθημα η κατά Dirichlet αντιστροφή μιας
πλήρως πολλαπλής συνάρτησης δίνεται από
εύκολο τύπο.

• Θεώρημα:

Έστω f πολλαπλή. Τότε η f είναι πλήρως πολλαπλή αν
και μόνο αν $f^{-1}(n) = \mu(n) \cdot f(n) \quad \forall n \geq 1$

• Απόδειξη:

" $\Rightarrow$ ": Έστω f πλήρως πολλαπλή. Θέσω $g = \mu \cdot f$ και υπολογίζω
το Dirichlet γινόμενο $g * f$.

$$(g * f)(n) = \sum_{d|n} (\mu \cdot f)(d) \cdot f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f\left(d \cdot \frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot f(n) =$$

$$= f(n) \cdot \sum_{d|n} \mu(d) = f(n) \cdot I(n) = I(n)$$

γιατί $f(1) \cdot I(1) = 1, \quad n > 1, \quad f(n) \cdot I(n) = f(n) \cdot 0 = 0$

Άρα $f^{-1} = \mu \cdot f$

" $\Leftarrow$ ": Έστω $f^{-1}(n) = \mu(n) \cdot f(n)$. Θ.δ.ο. $f(p^a) = f(p)^a$.

Ξέρω ότι $(f^{-1} * f)(n) = I(n) \Rightarrow \sum_{d|n} \mu(d) f(d) \cdot f\left(\frac{n}{d}\right) = 0 \quad \forall n > 1$

$$\text{Για } n = p^a : \sum_{d|p^a} \mu(d) \cdot f(d) \cdot f\left(\frac{p^a}{d}\right) = \mu(1) \cdot f(1) \cdot f(p^a) +$$

$$+ \mu(p) \cdot f(p) \cdot f(p^{a-1}) + \mu(p^2) \cdot f(p^2) \cdot f(p^{a-2}) =$$

$$= 1 \cdot 1 \cdot f(p^a) + (-1) f(p) \cdot f(p^{a-1}) = 0 \Rightarrow$$

$$f(p^a) = f(p) \cdot f(p^{a-1})$$

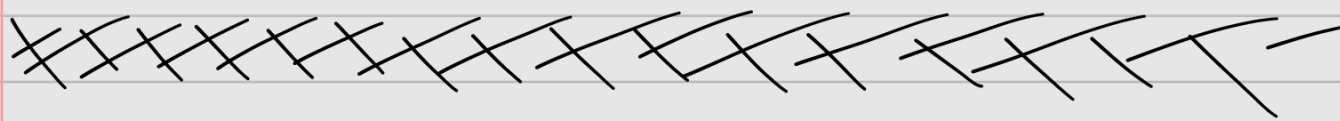
Άρα επαγωγικά $f(p^a) = f(p)^a \quad \square$.

• Παράδειγμα: (Dirichlet αντιστροφή της φ)

Αφού $\varphi = \mu * N$, ξέρω ότι $\varphi^{-1} = \mu^{-1} * N^{-1}$. Αλλά, η N
είναι πλήρως πολλαπλή, άρα $N^{-1} = \mu \cdot N$.

Άρα $\varphi^{-1} = \mu^{-1} \underset{\rightarrow \mu}{*} \mu \cdot N = \mu * \mu \cdot N$ και έχω

$$\varphi^{-1}(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \mu(d) \cdot N(d) = \sum_{d|n} d \cdot \mu(d)$$



ΙΣΟΔΥΝΑΜΙΕΣ

• Ορισμός:

Έστω οι ακέραιοι a, b, m με $m > 0$. Λέμε ότι ο a είναι ισοδύναμος modulo m με το b $a \equiv b \pmod{m}$ αν $m \mid a-b$. Ο m ονομάζεται μέτρο ισοδυναμίας. Άλλως, όταν $m \nmid a-b$ γράφουμε $a \not\equiv b \pmod{m}$.

Ειδιοσότητες: 1) $a \equiv 0 \pmod{m} \Leftrightarrow m \mid 0$

2) $a \equiv b \pmod{m} \Leftrightarrow m \mid a-b \Leftrightarrow a-b \equiv 0 \pmod{m}$.

3) $m \mid a-b \Leftrightarrow -m \mid a-b$

• Παράδειγμα:

$$19 \equiv 7 \pmod{12}$$

$$1 \equiv -1 \pmod{2}$$

$$1 \not\equiv 13 \pmod{7}$$

$$13 \equiv -26 \pmod{7}$$

$$3^2 \equiv -1 \pmod{5}$$

$$n \text{ άρτος} \Leftrightarrow n \equiv 0 \pmod{2}$$

$$n \text{ περιττός} \Leftrightarrow n \equiv 1 \pmod{2}$$

$$a \equiv b \pmod{1} \quad \forall a, b \in \mathbb{Z}$$

• Αν $a \equiv b \pmod{m}$ και $c \mid m$ τότε $a \equiv b \pmod{c}$

Απόδειξη: Αφού $c \mid m$ και $m \mid b-a \Rightarrow c \mid b-a$

• Παρατήρηση:

Η ισότητα ($\equiv$) είναι σχέση ισοδυναμίας, αφού

$$\bullet a \equiv a \pmod{m} \Leftrightarrow m \mid 0$$

$$\bullet a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m} \text{ αφού } m \mid a-b \Leftrightarrow m \mid b-a$$

$$\bullet \text{ Αν } a \equiv b \pmod{m} \text{ και } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$\text{γιατί } \left. \begin{array}{l} m \mid a-b \\ m \mid b-c \end{array} \right\} m \mid a-b+b-c = a-c$$

• Πρόταση:

$a \equiv b \pmod{m} \Leftrightarrow a, b$ αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με m .

• Λογική:

Έχουμε από Ευκλείδεια Διάρθρωση:

$$a = m \cdot q + r \quad 0 \leq r < m \quad \left\{ \begin{array}{l} a - b = m(q - q') + (r - r') \\ b = m \cdot q' + r' \quad 0 \leq r' < m \end{array} \right.$$

$$\text{Άρα } m \mid a - b \Leftrightarrow m \mid r - r'$$

Όμως $|r - r'| < m$, οπότε ο m δεν μπορεί να διαιρεί τη διαφορά, εκτός αν είναι αυτή 0.

$$\text{Άρα } a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \Leftrightarrow |r - r'| = 0 \Leftrightarrow r = r' \quad \square.$$

• Παρατήρηση:

Από μοναδικότητα υπολοίπου της διαίρεσης, έχουμε ότι $\forall a \in \mathbb{Z}, \exists! r \in \mathbb{Z}$ π.ω. $a \equiv r \pmod{m}$ και $0 \leq r < m$.

• Παρατήρηση:

Αφού η σχέση $\equiv \pmod{m}$ είναι ισοδυναμία επί των ακεραίων, αυτή ορίζει κάποιες κλάσεις ισοδυναμίας, οι οποίες είναι ξένες μεταξύ τους, και η ένωσή τους μας δίνει όλο το $\mathbb{Z}$.

• Ορισμός:

Για ένα ορισμένο μέτρο m , ονομάζω το σύνολο των ακεραίων x με την ιδιότητα $x \equiv a \pmod{m}$, τοξή ή κλάση υπολοίπων $a \pmod{m}$. Συμβολίζεται με $\bar{a}^m$ ή $[a]_m$ ή $\bar{a} = \{a + mk \mid k \in \mathbb{Z}\}$.

• Ιδιότητες: (Διατήρησης)

$$\bullet \bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$$

$$\bullet \text{αν } x \in \bar{a} \wedge y \in \bar{a}, \text{ τότε } x \equiv y \pmod{m}$$

$$\bullet \text{Οι } \bar{1}^m, \bar{2}^m, \dots, \overline{m-1}^m, \bar{m}^m = 0 \text{ είναι ξένες μεταξύ τους και η ένωσή τους } \bar{0} \cup \bar{1} \cup \dots \cup \overline{(m-1)} = \mathbb{Z}.$$

• Όταν $0, 1, \dots, m$ είναι μη κοινόδοιο με m και $\forall x \in \mathbb{Z}$ λείπει ότι το υπόλοιπο r της $x = mq + r$, είναι κάποιος από αυτούς $x \in \bar{r}$.

Ορισμός:

Ονομάζουμε πλήρες σύστημα υπολοίπων $\bmod m$ ένα σύνολο από m αντιπροσώπους, έναν από κάθε μία από τις τάξεις υπολοίπων $\overline{0}, \overline{1}, \dots, \overline{m-1}$.

Π.χ.

Κάθε σύνολο m ακεραίων που δεν είναι ισοϋπόδεικτοι με m , αποτελεί ένα τέτοιο σύστημα, όπως για παράδειγμα $\{0, 1, \dots, m-1\}$, $\{1, 2, \dots, m-1, m\}$, $\{1, m+2, 2m+3, \dots, m^2\}$.

Αν m περιζώδ, τότε:

$$\left\{ -\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \frac{m-3}{2}, \frac{m-1}{2} \right\}.$$

Το σύνολο $\{1^2, 2^2, 3^2, \dots, m^2\}$ ΔΕΝ είναι πλήρες σύστημα υπολοίπων $\bmod m$, αφού

$$(m-1)^2 \equiv 1^2 \bmod m \quad \text{γιατί:}$$

$$(m-1)^2 - 1 = m^2 - 2m = m(m-2) \quad \text{και το } m \text{ το διαιρεί,}$$

άρα τα στοιχεία του είναι διγώτερα του m .

20/03/2025

Θεώρημα:

Αν $(k, m) = 1$ και $\{a_1, a_2, \dots, a_m\}$ είναι ένα ισοπλάγιο σύστημα υπολοίπων $\text{mod } m$, τότε $\{ka_1, ka_2, \dots, ka_m\}$ είναι επίσης ένα ισοπλάγιο σύστημα υπολοίπων $\text{mod } m$.

Απόδειξη:

Έστω ότι δεν είναι. Τότε θα έχουμε ότι $ka_i \equiv ka_j \pmod{m}$ για κάποια a_i, a_j .
 $\Rightarrow m \mid ka_i - ka_j \Rightarrow m \mid k(a_i - a_j) \xrightarrow{\text{ίστη}} \xRightarrow{\text{Ευκλ. δ.}}$
 $\Rightarrow m \mid a_i - a_j$ άρα $a_i \equiv a_j \pmod{m}$ ~~✗~~

Άρα, όλα τα ka_i είναι μη ισοδύναμα $\text{mod } m$ και m το πλήθος άρα ισχύει.

Πρόταση: (Ιδιότητες ισοδυναμιών)

Αν $a \equiv b \pmod{m}$ και $c \equiv d \pmod{m}$

$$1) ax + cy = bx + dy \pmod{m} \quad \forall x, y \in \mathbb{Z}$$

$$\begin{aligned} \text{Θα έχουμε} \quad \left. \begin{array}{l} m \mid a-b \\ m \mid c-d \end{array} \right\} & \begin{aligned} m \mid x(a-b) + y(c-d) &= \\ &= xa + yc - xb - yd = \\ &= ax + cy - (bx + dy) \end{aligned} \end{aligned}$$

$$2) ac \equiv bd \pmod{m} \quad (\text{νόμος του κανονιστικού})$$

Ουτως $ac - bd = ac + bc - bc - bd =$
 $\underbrace{c(a-b)}_{m \cdot x} + \underbrace{b(c-d)}_{m \cdot x} \equiv 0 \pmod{m}$

3) $a^n \equiv b^n \pmod{m}$

Ουτως, από (2) έχω $a \cdot a \equiv b \cdot b \pmod{m} \Rightarrow$
 ... επαναληπτικά.

4) $f(a) \equiv f(b) \pmod{m} \quad \forall$ πολυώνυμο f με
 ακέραιους συντελεστές

Ουτως, χρησιμοποιώντας τις 1, 2, 3 και
 επαναληπτικά στον βαθμό του f .

• Παράδειγμα:

Ποιό είναι το υπόλοιπο του αθροίσματος
 $S = 1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5$ δια του 4.

• Λύση:

Κάθε αριθμός στο $\mathbb{Z}$ ανήκει σε μια από
 τις τέσσερις υποδοιότητες $\pmod{4}$, δηλαδή
 σε μια από τις $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ (γιατί
 αυτές είναι ένα πλήρες σύστημα υποδοιότητων
 $\pmod{4}$). Επομένως από 1 έως 100 $\exists$ 25 αριθμοί
 ισοδύναμοι με κάθε έναν $\pmod{4}$.
 Επίσης $3 \equiv -1 \pmod{4}$.

Λίγο ως ιδιότητες που δείξαμε, έχουμε:

$$S = 25 \cdot 0^5 + 28 \cdot 1^5 + 25 \cdot 2^5 + 25 \cdot (-1)^5 \Rightarrow \\ S' = 25 \cdot 2^5 = 25 \cdot 4 \cdot 2^3 \equiv 0 \pmod{4}$$

• Παράδειγμα:

Ποιο είναι το υπόλοιπο της διαίρεσης του $N = (n^2 - 1)^{1001} (n^2 + 1)^{1001}$ με το n ?

• Λύση:

$$\begin{aligned} \text{Ξέρω } n^2 &\equiv 0 \pmod{n} \Rightarrow n^2 - 1 \equiv -1 \pmod{n} \Bigg\} \Rightarrow \\ &\Rightarrow n^2 + 1 \equiv 1 \pmod{n} \end{aligned}$$

$$\Rightarrow \begin{cases} (n^2 - 1)^{1001} \equiv -1^{1001} \equiv -1 \pmod{n} \\ (n^2 + 1)^{1001} \equiv 1^{1001} \equiv 1 \pmod{n} \end{cases}$$

$$\text{Άρα } N = (n^2 - 1)^{1001} (n^2 + 1)^{1001} \equiv (-1)(1) = -1 \pmod{n}$$

Άρα το υπόλοιπο είναι $n-1$.

• Παράδειγμα:

Για κάθε πρώτο $p > 3$, ο $p^2 + 2$ είναι σύνθετος.

• Λύση:

Θα σου δείξω $\text{mod } 3$. ^{intuitive} Έχω $2 \equiv -1 \text{ mod } 3$.
Κάθε πρώτος μεγαλύτερος του 3 ικανοποιεί
 $p \equiv (\pm 1) \text{ (mod } 3)$, γιατί αν $p \equiv 0 \text{ mod } 3$ δεν
θα ήταν πρώτος.

$$\text{Άρα } p^2 \equiv 1 \text{ mod } 3 \Rightarrow p^2 + 2 = 2 + 1 = 3 \equiv 0 \text{ mod } 3.$$

Άρα $3 \mid p^2 + 2$ και άρα $p^2 + 2$ σύνθετος.

• Παράδειγμα:

$$\bigcirc F_5 = 2^{2^5} + 1 \text{ είναι σύνθετος.}$$

• Λύση:

Χωρίς να υπολογίσουμε τον $2^{32} + 1$, Θ.δ.ο.
ο 641 τον διαιρεί. Εξαιτίας του ως διδο-
χικές διαίρεσης του 2, $\text{mod } 641$

$$2^2 \equiv 4 \text{ mod } 641$$

$$2^4 \equiv 4^2 \text{ mod } 641 \equiv 16 \text{ mod } 641$$

$$2^8 \equiv 16^2 \text{ mod } 641 \equiv 256 \text{ mod } 641$$

$$2^{16} \equiv 256^2 \text{ mod } 641 \equiv 65536 \text{ mod } 641 \equiv 154 \text{ mod } 641$$

$$2^{32} \equiv 154^2 \text{ mod } 641 \equiv 23716 \equiv 640 \text{ mod } 641$$

$$\text{Άρα } 2^{32} + 1 = 640 + 1 = 641 \equiv 0 \text{ mod } 641$$

$$\text{Άρα } 641 \mid F_5.$$

• Παράδειγμα: (Διαμεττότητα με το 9)

Ένας ακέραιος $n > 0$ διαμετρείται με το 9 αν το άθροισμα των ψηφίων του διαμετρείται με το 9.

• Λύση:

Έστω $n = a_0 + 10a_1 + 10^2a_2 + \dots + 10^ka_k$, όπου a_i τα ψηφία του αριθμού στο δεκαδικό σύστημα. Έχουμε ότι:

$$\left. \begin{array}{l} 10 \equiv 1 \pmod{9} \\ 10^2 \equiv 1 \pmod{9} \\ \vdots \\ 10^k \equiv 1 \pmod{9} \end{array} \right\} \Rightarrow n = a_0 + \dots + 10^ka_k \equiv a_0 + a_1 + \dots + a_k \pmod{9}$$

Ειδικά αν $9 | a_0 + \dots + a_k \Leftrightarrow 9 | n$.

Πιο γενικά, χράφοντας την παράσταση ενός αριθμού ως προς μια βάση B , έχουμε τα εξής κριτήρια:

• Θεώρημα:

Έστω $n = \sum_{i=0}^k a_i B^i$, $B, a_i \in \mathbb{N}$, $B > 1$ τότε

1) Αν $d | B - 1$, τότε $d | n \Leftrightarrow d | \sum_{i=0}^k a_i$ (π.χ. 9, 3)

2) Αν $d | B$ και $j < k$, τότε $d^j | n \Leftrightarrow d^j | \sum_{i=0}^j a_i B^i$ (π.χ. 2, 5)

$\hookrightarrow$ n.x. για $j=1$, τότε

$d|n \Leftrightarrow d|a_0$ (τελευταίο ψηφίο)

$$3) \text{ Αν } d|B+1, \quad d|n \Leftrightarrow d|\sum_{i=0}^K (-1)^i a_i$$

n.x. ένας αριθμός διαιρείται με το 11
ανν το $11 | a_0 - a_1 + a_2 - \dots + (-1)^k a_k$

Απόδειξη (2):

Αφού $B \equiv 0 \pmod{d}$, τότε $B^j \equiv 0 \pmod{d^j}$,
 $B = d \cdot c \Rightarrow B^j = d^j c^j$ $\forall j$

$$\text{Άρα } \sum_{i=0}^K a_i B^i = a_0 + a_1 B + a_2 B^2 + \dots + a_j B^j + a_{j+1} B^{j+1} + \dots + a_k B^k$$

$$= a_0 + a_1 B + \dots + a_{j-1} B^{j-1} = \sum_{i=0}^{j-1} a_i B^i \pmod{d^j}$$

$$\text{Άρα όπως } d^j | n \Leftrightarrow n \equiv 0 \pmod{d^j} \Leftrightarrow d^j | \sum_{i=0}^{j-1} a_i B^i$$

• Παράδειγμα:

Να βρεθεί το x για το οποίο ισχύει:
 $(52817) \cdot (3212146) = 169655 \underline{x} 15282$

• Λύση:

Θα δουλέψω $\pmod{11}$ χρησιμοποιώντας το
εναλλασόμενο αθροισμα του ψηφίου.

$$7-1+8-2+5 = 17 \equiv 6 \pmod{11}$$

$$6-4+1-2+1-2+3 = 3 \pmod{11}$$

Άρα στα αριστερά έχω $3 \cdot 6 = 18 \equiv 7 \pmod{11}$

Άρα Θέλω

$$2-8+2-5+1-x + 5-5+6-9+6-1 = 7 \Rightarrow -6-x \equiv 7 \pmod{11}$$

$$\Rightarrow x \equiv -13 \equiv -2 \pmod{11} = 9 \pmod{11}$$

Άρα $x = 9$.

• Παρατήρηση:

Πρέπει να επιδείξω διαίρεση με αριθμό > 9 ,
έτσι ώστε οι κλάσεις υπολοίπων $0, 1, 2, 3, 4, 5, 6,$
 $7, 8$ να είναι διαίρετες (ξένες μεταξύ τους).

• Πισω σε γενικές ιδιότητες :

* Πρόταση:

Αν $c > 0$, τότε $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$.

↳ Απόδειξη:

Ισχύει από διαμεσότητα ότι :

$$m|a-b \Leftrightarrow cm|c(a-b)$$

↳ Προσοχή!

Ο κοινός παράγοντας που διαγράφουμε, βρίσκεται και στο μέτρο.

π.χ. $48 \equiv 18 \pmod{10} \not\Rightarrow 8 \equiv 3 \pmod{10}$ ~~XXXX~~

Όταν δυν υπάρχει τέτοιος κοινός παράγοντας, μπορεί να χρησιμοποιηθεί το παρακάτω:

• Πρόταση: (Νόμος Διαγραφής)

Αν $ac \equiv bc \pmod{m}$ και $d = (m, c)$, τότε ισχύει $a \equiv b \pmod{\frac{m}{d}}$, δηλαδή διαγράφω κοινό παράγοντα c διακρίνοντας το μέτρο m με τον ΜΚΔ τους.

↳

Ισχύει $8 \equiv 3 \pmod{5} \rightarrow \frac{10}{2}$ αφού $2 = (10, 5)$.

Ειδικότερα, οποιoσδήποτε παράγοντας, πρώτος με το μέτρο, απαλείφεται! Αφού $(m, c) = 1$.

↳ Απόδειξη:

Αν $m | c(a-b) \Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$.

Αλλά $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, άρα αργό

Λίγα βελτίωση $\Rightarrow \frac{m}{d} \mid a-b$.

26/03/2025

• Νόμος Διαγραφής:

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$$

• Παράδειγμα:

$$\textcircled{O} \quad F_5 = 2^2 + 1 \quad \text{είναι σύνθετος}$$

• Λύση:

$$\textcircled{O} \text{ δ.ο. } 641 | F_5$$

Παρατηρώ ότι ο $640 \equiv (-1) \pmod{641}$
αναλύεται σε πρώτους παρρισοντες ως
 $640 = 2^7 \cdot 5 \Rightarrow (2^7 \cdot 5)^4 = 2^{28} \cdot 5^4 \equiv 1 \pmod{641} \quad (1)$

$$\text{Αλλά έχουμε ότι } 641 = 5^4 + 2^4 \Rightarrow -2^4 \equiv 5^4 \pmod{641} \quad (2)$$

$$\text{Αλλά } (1) \times (2) \Rightarrow -2^{32} \cdot 5^4 \equiv 5^4 \pmod{641} \Rightarrow$$

$$\begin{array}{l} \text{Νόμος} \\ \Rightarrow \\ \text{Διαγραφής} \end{array} \quad -2^{32} \equiv 1 \pmod{641} \Rightarrow 641 | 2^{32} + 1 = F_5$$

(*) Σαν ειδική περίπτωση του Ν. Διαφρ. παίρνουμε και μια ιδιότητα που μοιάζει με την $ab=0 \Rightarrow a=0 \text{ ή } b=0$.

$$\begin{array}{l} \bullet \text{ Αν } ab \equiv 0 \pmod{m}, (a,m)=1 \Rightarrow \\ \Rightarrow b \equiv 0 \pmod{m}, (a \not\equiv 0 \pmod{m}) \end{array}$$

• Πρόταση:

Αν $a \equiv b \pmod{m}$ τότε $(a, m) = (b, m)$.

• Απόδειξη:

Έστω $d = (a, m)$, $e = (b, m)$. Αφού $a - b = cm \Rightarrow b = a - cm$.

Έχω $\left. \begin{matrix} d|a \\ d|m \end{matrix} \right\} \Rightarrow d|a - cm \Rightarrow d|b \left\{ \begin{matrix} \text{και} \\ d|m \end{matrix} \right\} \Rightarrow d|e$

Αντιστοίχα $e|d \Rightarrow e = d$.

• Πρόταση:

Αν $a \equiv b \pmod{m}$ και $a \equiv b \pmod{n}$, αν $(m, n) = 1$, τότε $a \equiv b \pmod{m \cdot n}$.

• Απόδειξη:

$\left. \begin{matrix} m|a-b \Rightarrow a-b = k \cdot m \\ n|a-b \Rightarrow a-b = \lambda \cdot n \end{matrix} \right\} \Rightarrow k \cdot m = \lambda \cdot n, k, \lambda \in \mathbb{Z}$.

Εκτίδως
Αφού $m|\lambda n$ και $(m, n) = 1 \Rightarrow m|\lambda \Rightarrow m \cdot n | \lambda n = (a-b)$.

(*) Πιο γενικά, ισχύει για $(m_i)_{i=1}^k$ ομογενή α-
 πρώτων μεταξύ τους αριθμών,
 $a \equiv b \pmod{m_i} \forall i \Leftrightarrow a \equiv b \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_k}$.
 Από πάνω δείξαμε το " $\Rightarrow$ ". Το " $\Leftarrow$ "
 ισχύει για οποιονδήποτε Στοιχείο του $\mathbb{Z}$.

Για παράδειγμα $a \equiv b \pmod{108} \Leftrightarrow a \equiv b \pmod{4}$
 και $a \equiv b \pmod{27}$ (αφού $(4, 27) = 1$).

Πολλή Βασική Ιδιότητα για το Κινέζικο
 Θέλημα.

Ειδικότερα, αν $m = \prod_{\substack{p \text{ prime} \\ p|m}} p^{u_p(m)}$ η πρωτογενής

ανάλυση του, τότε:

$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{p^{u_p(m)}} \forall p$ πρώτο
 Στοιχείο του m $(p^u, q^v) = 1$.

Οι κλάσεις υπολοίπων modulo συνά-
 μων πρώτων αριθμών, είναι οι Θυέταλοι
 Αιότοι για όλες τις κλάσεις του αλφαίου.

• Παράδειγμα:

Δ.ο. $\forall n \in \mathbb{N} \quad 42 | n^7 - n$.

• Λύση:

Η ανάλυση του $42 = 2 \cdot 3 \cdot 7$, Θ.δ.ο.

$n^7 \equiv n \pmod{42}$, δείχνοντας ότι:

$\left. \begin{array}{l} n^7 \equiv n \pmod{2} \\ n^7 \equiv n \pmod{3} \\ n^7 \equiv n \pmod{7} \end{array} \right\}$ έτσι θα ισχύει το αποτέλεσμα

• Αν n άρτος, n^7 άρτιος και $n^7 - n$ άρτιος,
άρα $n^7 \equiv n \pmod{2}$

Αν n περιττός, τότε n^7 περιττός και
 $n^7 - n$ άρτιος, άρα $n^7 \equiv n \pmod{2}$

• Από Fermat, ισχύει ότι $n^3 \equiv n \pmod{3}$ και
έχω $n^7 \equiv (n^3)^2 \cdot n = n^2 \cdot n = n^3 \equiv n \pmod{3}$
 $\hookrightarrow n \pmod{3}$

• Από Fermat, $n^7 \equiv n \pmod{7}$ $\square$

Γραμμικές Ισοδυναμίες :

Εξετάζουμε λύσεις της $f(x) \equiv 0 \pmod{m}$
για πολυώνυμα f με ακέραιους συντελεστές,
για $x \in \mathbb{Z}$. ($f(x) \in \mathbb{Z}$). Φυσικά, $x \equiv y \pmod{m}$
 $\Rightarrow f(x) \equiv f(y) \pmod{m}$. Άρα, αν έχω μια
έχω άπειρες λύσεις στο $\mathbb{Z}$. Θεωρούμε ως
διακριτές τις μη-ισοδύναμες $\pmod{m}$ (δηλ.
αυτές που ανήκουν σε ένα πλήρες σύστη-
μα υπολοίπων του $\pmod{m}$). Άρα έχω το
πολύ m λύσεις.

Παραδείγματα :

• $2x \equiv 3 \pmod{4}$ είναι αδύνατη, γιατί ο
 $2x - 3$ είναι περιττός και άρα το 4 δεν
το διαιρεί.

- $x^2 \equiv 1 \pmod{8}$ έχει τέσσερις λύσεις, το $1, 3, 5, 7$, (ψαχτεί).

• Θεώρημα:

Αν $(a, m) = 1$, τότε $ax \equiv b \pmod{m}$, έχει μοναδική λύση.

• Απόδειξη:

Αρκεί να δοκιμάσουμε τους $0, 1, 2, \dots, m-1$, καθώς αυτοί σχηματίζουν ένα πλήρες σύστημα υπολοίπων $\pmod{m}$. Από προηγούμενη πρόταση, τα $0, a, 2a, 3a, \dots, (m-1)a$, σχηματίζουν ένα πλήρες σύστημα $\pmod{m}$, αφού $(a, m) = 1$. Αυτό σημαίνει ότι μόνο ένα από αυτά (αφού είναι ξένα μεταξύ τους και καλύπτουν το $\mathbb{Z}$) είναι ισοδύναμο με $b \pmod{m}$, το οποίο είναι η λύση της ισοτιμίας. $\square$

• Παρατήρηση:

Το παραπάνω δίνει μόνο την ύπαρξη της μοναδικής λύσης. Για τον υπολογισμό θα χρησιμοποιήσουμε ειδικές μεθόδους.

• Ορισμός:

Ονομάζουμε αντιστροφή ή αντιστροφή κλάση του $a \pmod{m}$ τη μοναδική λύση της $ax \equiv 1 \pmod{m}$ όταν $(a, m) = 1$. Όταν η

$a \pmod{m}$ είναι αντιστρέψιμη, ή αντιστοίχο $a' \pmod{m}$, τότε η μοναδική λύση της $ax \equiv b \pmod{m}$ είναι $x \equiv a'b \pmod{m}$.

Παρατήρηση:

Στην πραγματικότητα, $ax \equiv 1 \pmod{m}$ έχει λύση αν και μόνο αν $(a, m) = 1$. Το Θεώρημα δίνει την " $\Leftarrow$ ". Το " $\Rightarrow$ ", αν $\exists \beta \in \mathbb{Z}$ τέω. $a\beta \equiv 1 \pmod{m}$ τότε $m \mid a\beta - 1 \Rightarrow a\beta - 1 = \lambda m \Rightarrow a\beta - \lambda m = 1$. Από Bezout, για $\beta, -\lambda \in \mathbb{Z}$, παίρνουμε $(a, m) = 1$.

Άρα σκέψομαι αντιστρέψιμες κλάσεις $\pmod{m}$ είναι οι $a \pmod{m}$ με $(a, m) = 1$.

Παραδείγματα:

- Αν $a\beta \equiv 0 \pmod{m}$ και a αντιστρέψιμο τότε $\beta \equiv 0 \pmod{m}$.

Αντιπαράδειγμα: $3 \cdot 4 \equiv 0 \pmod{12}$, $3, 4 \not\equiv 0 \pmod{12}$, κανένα δεν είναι αντιστρέψιμο $\pmod{12}$.

- Έστω $m = 12$. Οι μόνες κλάσεις $\pmod{12}$ που είναι αντιστρέψιμες, είναι οι $1, 5, 7, 11 \pmod{12}$, γιατί είναι πρώτες με το 12.

$1' \equiv 1 \pmod{12}$ (πάντα), αλλά τυχαίνει και $5' \equiv 5 \pmod{12} \rightarrow 5 \cdot 5 = 25 \equiv 1 \pmod{12}$, $7' \equiv 7 \pmod{12}$, $11 \dots$

Μπορούμε να χρησιμοποιήσουμε τον
Ευκλείδιο αλγόριθμο για να προσδιορίσουμε
την αντίστροφη κλάση.

π.χ. για το $8'(\text{mod } 21)$ ψάχνω $a, b \in \mathbb{Z}$:

$$8a + 21b = 1. \quad 21 = 2 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

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

$$\begin{array}{c} a \qquad b \\ \downarrow \quad \downarrow \\ \Rightarrow 8 \cdot 8 + 21(-3) = 1 \end{array} \quad \begin{array}{c} \text{mod } 21 \\ \Rightarrow 8 \cdot 8 + 0 \equiv 1 \text{ mod } 21 \Rightarrow \\ 8' \equiv 8 \text{ mod } 21. \end{array}$$

Ορισμός:

Ένα σύνολο $\{a_1, \dots, a_k\}$ ακεραίων λέγεται
αλληλόμορφο σύστημα υπολοίπων $\text{mod } m$ ή
πλήρες σύστημα αντιπροσωπευτικών κλάσεων $\text{mod } m$
αν $\forall 1 \leq i \leq k \quad (a_i, m) = 1$ και $a_i \not\equiv a_j (\text{mod } m)$
 $\forall 1 \leq i, j \leq k$.

Βλέπω ότι είναι το πλήθος $\varphi(m)$!

27/03/2025

$\{a_1, \dots, a_k\}$ ανηγμένο σύστημα υπολοίπων $\text{mod } m$
 $\varphi(m)$ το πλήθος.

Παράδειγμα:

Το $\{1, 2, 4, 5, 7, 8\}$ (οι αντιστ. κλάσεις $\text{mod } 9$) είναι ένα
ανηγμένο σύστημα υπολοίπων $\text{mod } 9$ με πλήθος:
$$\varphi(9) = 9 \cdot \prod_{\substack{p|9 \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = 9 \cdot \left(1 - \frac{1}{3}\right) = 9 - 3 = 6$$

Παράδειγμα:

Εναλλακτική αιτιολόγηση ότι $\varphi(m)$ άρτιος για $m \geq 3$.
Αν $a(\text{mod } m)$ είναι μια αντιστρέψιμη κλάση, τότε
και η $-a(\text{mod } m)$ είναι αντιστρέψιμη με $(-a)' \equiv -a \text{mod } m$.
Άρα, οι αντιστρέψιμες κλάσεις είναι πάντα σε
ζεύγη, αφού $a \not\equiv -a(\text{mod } m)$, αλλιώς $m|2a \Rightarrow$
 $\Rightarrow m|2$ ~~$\times$~~ , $m \geq 3$.

Άρα, κάθε ανηγμένο σύστημα υπολοίπων $\{a_1, \dots, a_{\varphi(m)}\}$,
διατερίζεται σε ζεύγη $\Rightarrow$ η τάξη του συνόλου
 $\varphi(m)$ είναι άρτιος.

Θεώρημα:

Αν $\{a_1, \dots, a_{\varphi(m)}\}$ ανηγμένο σύστημα υπολοίπων $\text{mod } m$
και $(b, m) = 1$, τότε $\{ba_1, \dots, ba_{\varphi(m)}\}$ είναι επίσης
σύστημα υπολοίπων $\text{mod } m$.

Απόδειξη:

Αυτές είναι $\varphi(m)$ το ισθός. Πράγμα, αν :

$$ba_i \equiv ba_j \pmod{m} \Rightarrow a_i \equiv a_j \pmod{m} \quad (b, m) = 1.$$

Άρα, όλοι οι κανονισμοί μη ισοδυναμικοί $\pmod{m}$.
Επίσης, όλοι είναι αντιστρέψιμοι $\pmod{m}$. Άρα
 $(a_i, m) = 1, (b, m) = 1$, τότε $(ba_i, m) = 1, \forall i$.

Πράγμα, αν $a = \prod p_i^{s_i}, b = \prod q_i^{r_i}, m = \prod u_i^{t_i} \Rightarrow$
 $a, b = \prod p_i^{s_i} q_i^{r_i}$ αλλιώς $p_i \neq u_i, q_j \neq u_i \quad \forall i, j$.

Θεώρημα!!:

Αν $(a, m) = d$ και $d \mid b$, τότε η $ax \equiv b \pmod{m}$ (1)
έχει ακριβώς d λύσεις $\pmod{m}$. Αυτές είναι οι:
 $b, b + \frac{m}{d}, b + \frac{2m}{d}, \dots, b + \frac{(d-1)m}{d}$, όπου b η
μοναδική λύση $\pmod{\frac{m}{d}}$ της $\frac{d}{d}x \equiv \frac{a}{d} \pmod{\frac{m}{d}}$ (2).

Παρατήρηση: (Τότε είναι αδύνατη η (1))

Η (1) έχει λύσεις αν και μόνο αν $d \mid b$. Πράγμα:
" $\Rightarrow$ ": έχω ότι $d \mid m$ και $m \mid ax - b \Rightarrow d \mid ax - b$ αλλιώς
και $d \mid a \Rightarrow d \mid b$.

" $\Leftarrow$ ": έχω ότι αν $d \mid b$, τότε σχηματίζω την
 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, η οποία έχει μοναδική

λύση, από προηγούμενο Θεώρημα, μιας και
 $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$. Η λύση της $\pmod{\frac{m}{d}}$, είναι

και λύση της $ax \equiv b \pmod{m}$.

Άρα η (1) αδύνατη $\Leftrightarrow d \nmid b$.

- Απόδειξη:

Η (1) είναι ισοδύναμη (αφού ψάχνω x τ.ω. $m|ax-b$) με τη Διοφαντική $ax-my=b$, με συντελεστές $a, -m \in \mathbb{Z}$. Από Θεωρία, γνωρίζω πως όταν $d=(a,m)|b$, έχουμε απεριόριστε λύσεις στο $\mathbb{Z}$:

$$x = x_0 + k \frac{(-m)}{d}, \quad y = y_0 - k \frac{a}{d}, \quad (x_0, y_0) \text{ ist ein Punkt}$$

Ψάχνω certo τις λύσεις του x τις μη ισοδυναμίες $\text{mod } m$, για να λύσω την (1). Έστω $x_1 = x_0 - \frac{m}{2} k_1$ και $x_2 = x_0 - \frac{m}{2} k_2$, $k_1, k_2 \in \mathbb{Z}$, δύο λύσεις του x της Διοφαντικής. Ισχύει ότι

$$x_1 \equiv x_2 \pmod{m} \Leftrightarrow k_1 \equiv k_2 \pmod{d}.$$

Quers, $x_1 - x_2 = \frac{m}{d} (k_2 - k_1)$. Av $d/k_1 - k_2$, zöze

$$m \mid x_1 - x_2, \text{ gazi} \quad k_2 - k_1 = d \cdot C \Rightarrow x_1 - x_2 = \frac{m}{d} \cdot d \cdot C = m \cdot d$$

$$\Delta v \quad m|x_1 - x_2, \quad z \in \mathbb{Z} \quad \cancel{m \cdot e} = \frac{\cancel{m}}{d} (k_2 - k_1) \rightarrow d \mid k_2 - k_1.$$

Άρα $x_1 \not\equiv x_2 \pmod{m} \Leftrightarrow k_1 \not\equiv k_2 \pmod{d}$. Άρα το πλήθος των διακριτών $\pmod{m}$ λύσεων της (1) είναι το ίδιο με το πλήθος των μη ισοδύναμων κλάσεων $\pmod{d}$, δηλαδή αριθμός d .

Τέλος, αν θεωρήσουμε ως χ_0 τη λύση t της (2) που ξέρω ότι είναι και λύση της (1), και παίρνουμε το π αντίστοιχα συστήματα υπολοίπων mod $\Sigma = \{-(d-1), -(d-2), \dots, -2, -1, 0\}$.

Τότε, μια ειδική μη λυόμενη λύση της (1) είναι, από τον $x = b - \frac{m}{d} \cdot k$ οι εξής:

$$t, t + \frac{m}{d}, t + \frac{2m}{d}, \dots, t + \frac{(d-1)m}{d}$$

↓

↓

1

.

1

—



Παρατήρηση:

Μια λύση x της (1) είναι και λύση της (2) και η μοναδική λύση z της (2) είναι και λύση της (1). Όλες οι αναγραφόμενες διακριτές λύσεις της (1) mod m "πέρχονται" στην ίδια κλάση της μοναδικής $z \bmod \left(\frac{m}{d}\right)$ της (2).

Παραδείγματα:

1) $15x \equiv 3 \pmod{35}$

Το $(15, 35) = 5$. Αφού $d \neq 1$, δεν έχω μοναδική λύση. Η 5 η καμία λύση. Αλλά το $5 \nmid 3$, άρα δεν έχω καμία λύση.

2) $7x \equiv 3 \pmod{10}$

$d(7, 10) = 1 \Rightarrow$ μοναδική λύση $x \equiv 3 \cdot 7' \pmod{10}$, όπου $7'$ η αντίστροφη. Αλλά $7' = 3 \Rightarrow x \equiv 9 \pmod{10}$.

3) $42x \equiv 84 \pmod{63}$

Αλλά $21 \mid 84$, έχω 21 λύσεις!

$$d(42, 63) = 21 = 3 \cdot 7$$

$$\begin{array}{l} \hookrightarrow 3 \cdot 3 \cdot 7 \\ \hookrightarrow 2 \cdot 3 \cdot 7 \end{array}$$

Οι λύσεις είναι οι :

$$t, t + \frac{63}{21}, t + 2 \cdot \frac{63}{21}, \dots, t + 20 \cdot \frac{63}{21}$$

$$\text{Όπου } t \text{ η μοναδική λύση της } \frac{42}{21}x \equiv \frac{84}{21} \pmod{\frac{63}{21}}$$

$$\Rightarrow 2x \equiv 4 \pmod{3} \Rightarrow 2x \equiv 1 \pmod{3} \Rightarrow x \equiv 2 \pmod{3}$$

Άρα $t = 2$.

Επομένως οι 21 λύσεις της αρχικής είναι οι $2, 5, 8, \dots, 62 \pmod{63}$.

4) Εναλλακτικά το $ax+by=(a,b) \quad (*)$

Σχηματίζω τη γραμμική ισοτιμία $ax \equiv (a,b) \pmod{b}$ η οποία έχει λύσεις γιατί $(a,b) \mid (a,b)$. Άρα, μπορώ να έχω $b \mid ax-(a,b) \Rightarrow \exists k \text{ π.μ. } ax-(a,b)=kb \Rightarrow ax-kb=(a,b)$. Άρα βρήκα τα $x \in \mathbb{Z}, -k \in \mathbb{Z}$ που ικανοποιούν την $(*)$.

28/03/2025

• Θεώρημα: (Euler-Fermat)

Αν $(a, m) = 1$, τότε $a^{\varphi(m)} \equiv 1 \pmod{m}$
 $\hookrightarrow a$ αντιστρέφεται mod m .

• Απόδειξη:

Αν $\{b_1, b_2, \dots, b_{\varphi(m)}\}$ ανηγμένο σύστημα υπολοίπων mod m , αφού $(a, m) = 1$, τότε $\{ab_1, ab_2, \dots, ab_{\varphi(m)}\}$ είναι και αυτό ένα ανηγμένο σύστημα υπολοίπων mod m . Άρα, το γινόμενο όλων των στοιχείων του ενός συνόλου, ισούται με το γινόμενο όλων των στοιχείων του αΐσλου συνόλου mod m , γιατί ξέρω ότι $b_i \equiv ab_j \pmod{m}$, για κάποια i, j , και πολλαπλαζω κατά μέλη. Δηλαδή:

$$b_1 \cdot b_2 \cdot \dots \cdot b_{\varphi(m)} \equiv ab_1 \cdot ab_2 \cdot \dots \cdot ab_{\varphi(m)} \pmod{m} \Rightarrow$$
$$\Rightarrow \text{Ν. Διαφρ} + (b_i, m) = 1 \quad \forall i \Rightarrow 1 \equiv a \cdot a \cdot \dots \cdot a \pmod{m} \Rightarrow$$
$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad \square$$

• Παρατήρηση:

Ισχύει και το αντιστρόφιο, δηλαδή αν $a \in \mathbb{Z}$ και $a^{\varphi(m)} \equiv 1 \pmod{m}$, τότε $(a, m) = 1$. Οντως, έχω $m \mid a^{\varphi(m)} - 1$ και Θ.Σ.Ο. $(a, a^{\varphi(m)} - 1) = 1$. Άρα, αναγκαστικά $(a, m) = 1$. Για να το δείξω, βάλνω ότι αν

$$\left. \begin{array}{l} d \mid a^{\varphi(m)} - 1 \\ d \mid a \Rightarrow d \mid a^{\varphi(m)} \end{array} \right\} \Rightarrow d = 1.$$

• Πόρισμα:

Αν $(a, m) = 1$, τότε η μοναδική λύση της $ax \equiv b \pmod{m}$ δίνεται από τη $x \equiv ba^{\varphi(m)-1} \pmod{m}$.

Απόδειξη:

Αφού $a^{\varphi(m)} \equiv 1 \pmod{m}$ για α αντιστρέφεται mod m, ισχύει ότι $a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$, άρα $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$ και άρα $x \equiv ba^{\varphi(m)-1} \pmod{m}$.

Παραδείγματα:

1) $5x \equiv 3 \pmod{24}$

$(5, 24) = 1$ μοναδική λύση

$x \equiv 3 \cdot 5^{\varphi(24)-1} \pmod{24} \Rightarrow 3 \cdot 5 \pmod{24} \equiv 15 \pmod{24}$

$\Rightarrow \varphi(24) = \varphi(3 \cdot 8) = \varphi(3) \cdot \varphi(8) = 2 \cdot 4 = 8$

$\Rightarrow 5^7 \pmod{24}$ υπολογίζω τις πρώτες δυνάμεις:

$5^2 = 25 \equiv 1 \pmod{24}$. Άρα $5^7 = 5^6 \cdot 5 = (5^2)^3 \cdot 5 \equiv 5 \pmod{24}$

2) $25x \equiv 15 \pmod{120}$

$(25, 120) = 5$, $5 \nmid 15 \Rightarrow$ έχω 5 λύσεις mod 120.

Για να βρω την t, $5x \equiv 3 \pmod{24}$. Άρα, ξέρω ότι $t=15$ ($x \equiv 15 \pmod{24}$)

Άρα, έχω τις 5 λύσεις:

$x = 15 + 24k$, $k=0, 1, 2, 3, 4 \Rightarrow x \equiv 15, 39, 63, 87, 111 \pmod{120}$.

Πρόταση:

Αν p πρώτος με p τα, τότε $a^{p-1} \equiv 1 \pmod{p}$.

Απόδειξη:

Από Euler-Fermat, αφού $\varphi(p) = p-1$ και $(a, p) = 1$, έχει p τα.

Πρόταση: (Μικρό Θεώρημα Fermat)

Για κάθε $a \in \mathbb{Z}$ και πρώτο p, $a^p \equiv a \pmod{p}$

• Ανάλυση:

Αν $p|a$, είναι άμεσο, πόλιντας με a κατά μέλη.
Αν $p \nmid a$, έχουμε ότι $a \equiv (0 \bmod p)$, αλλά και επίσης $a^p \equiv 0 \bmod p$. Άρα, ούτως $a^p \equiv a \bmod p$.

• Euler-Fermat: εύκολος υπολογισμός υπολοίπων μεγάλων δυνάμεων δια φυσικών.

• Παράδειγμα:

Υπόλοιπο διαίρεσης του 35^{506} δια 24.

• Λύση:

$$\begin{aligned}\varphi(24) &= 8 \Rightarrow 506 = 8 \cdot 63 + 2 \Rightarrow 35^{506} \equiv (35^8)^{63} \cdot 35^2 \pmod{24} \\ &\equiv 35^2 \pmod{24} \equiv (5 \cdot 7)^2 \pmod{24} \equiv 5^2 \cdot 7^2 \pmod{24} = 25 \cdot 49 \pmod{24} \\ &\equiv 1 \pmod{24}\end{aligned}$$

Άρα τελικά $35^{506} \equiv 1 \pmod{24}$. Άρα το υπόλοιπο είναι 1.

• Παράδειγμα:

Να υπολογιστούν τα 2 τελευταία ψηφία του 1993^{1993} .

• Λύση:

Ουσιαστικά μας ζητείται το υπόλοιπο της διαίρεσης του 1993^{1993} με το 100.

$$\varphi(100) = \varphi(4) \cdot \varphi(25) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40$$

Διαφύ τω δύναμη με το $\varphi(100)$

$$1993 = 40 \cdot 49 + 33$$

$$\text{Άρα } 1993^{1993} = (1993^{40})^{49} \cdot 1993^{33} \equiv 1993^{33} \pmod{100}$$

$$\begin{aligned}\text{Αλλά } 1993^{33} &= \underbrace{(1900 + 93)}_{\text{πολ/οις } 100}^{33} = \underbrace{1900^{33}}_{\text{Διωνυμικό}} + \underbrace{\binom{33}{1} 1900^{32} \cdot 93}_{\text{Ολική τιμή}} + \dots + \binom{33}{2} 1900^{32} \cdot 93^2 + 93^{33}\end{aligned}$$

$$\begin{aligned} \equiv 93^{33} \pmod{100} &\equiv (-7)^{33} \pmod{100} \equiv -7^{33} \pmod{100} \equiv \\ &\equiv -(7^4)^8 \cdot 7 \pmod{100} \equiv -7 \pmod{100} \equiv 93 \pmod{100} \end{aligned}$$

$$7 \equiv 7 \pmod{100}$$

$$7^2 \equiv 49 \pmod{100}$$

$$7^3 \equiv 43 \pmod{100}$$

$$7^4 \equiv 301 \pmod{100} \equiv 1 \pmod{100}$$

Άρα, τα τελευταία
2 ψηφία του 1993^{1993}
είναι το 93.

• Παράδειγμα:

Να δείξετε ότι $\forall a \in \mathbb{Z}, a^{81} \equiv a \pmod{935}$.

• Λύση:

$$a \equiv b \pmod{m_i}, 1 \leq i \leq k, (m_i, m_j) = 1, \forall i, j \Leftrightarrow a \equiv b \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_k}$$

Η ανάλυση του μέτρου σε πρώτους: $1935 = 5 \cdot 11 \cdot 17$.

$$\text{Άρα } a^{81} \equiv a \pmod{5 \cdot 11 \cdot 17} \Leftrightarrow a^{81} \equiv a \pmod{5}$$

$$a^{81} \equiv a \pmod{11}$$

$$a^{81} \equiv a \pmod{17}$$

$$\begin{aligned} \text{Αλλά } a^{81} &= \underbrace{(a^5)^{16}}_{\text{u.o.f.}} \cdot a \equiv a^{16} \cdot a \pmod{5} \equiv a^{17} \pmod{5} \equiv \\ &\equiv (a^5)^3 \cdot a^2 \pmod{5} \equiv a^3 \cdot a^2 \pmod{5} \equiv a \pmod{5} \end{aligned}$$

$$a^{81} = (a^{11})^7 \cdot a^4 \equiv a^7 \cdot a^4 \pmod{11} \equiv a \pmod{11}$$

$$a^{81} = (a^{17})^4 \cdot a^{13} \equiv a^4 \cdot a^{13} \equiv a^{17} \equiv a \pmod{17}. \quad \square$$

02/04/2025

Σε κάποια αναλογία με το Θεμελιώδες Θεώρημα Άλγεβρας (κάθε πολυ βαθμού n έχει n λύσεις στο $\mathbb{C}$) που δεν ισχύει γενικά, έχουμε το παρακάτω — μόνο για modulo πρώτων αριθμών:

• Θεώρημα: (Lagrange)

Έστω p πρώτος και $f(x) = a_0 + a_1x + \dots + a_nx^n$ με $a_i \in \mathbb{Z}$ και $a_n \not\equiv 0 \pmod{p}$. Τότε η $f(x) \equiv 0 \pmod{p}$ έχει το πολύ n λύσεις στο $\mathbb{Z}$.

↳ Αντιστοίχισμα:

$x^2 \equiv 1 \pmod{8}$ έχει 4 λύσεις, $x = 1, 3, 5, 7 \pmod{8}$.

• Απόδειξη:

Με επαγωγή στον βαθμό n .

Για $n=1$, παίρνουμε γραμμική $a_0 + a_1x \equiv 0 \pmod{p} \Rightarrow a_1x \equiv -a_0 \pmod{p}$.

• Αφού p πρώτος, $(a_1, p) = 1$ και η ισοδυναμία έχει μοναδική λύση.

• Έστω ότι ισχύει για πολυώνυμα βαθμού $n-1$.

Έστω ότι δεν ισχύει για το $f(x)$, δηλαδή έστω ότι η $f(x) \equiv 0 \pmod{p}$ έχει $n+1$ λύσεις, μη ισοδύναμες $\pmod{p}$, τις $x_1, x_2, \dots, x_{n+1}$.

$$\begin{aligned} \text{Σχηματίζω } f(x) - f(x_1) &= a_nx^n + a_{n-1}x + \cancel{a_0} - a_nx_1^n - \dots - a_1x_1 - \cancel{a_0} \\ &= a_n(x^n - x_1^n) + a_{n-1}(x^{n-1} - x_1^{n-1}) + \dots + a_1(x - x_1) = \\ &= (x - x_1) \cdot g(x), \text{ όπου } g(x) \text{ πολυών.} \end{aligned}$$

για: ακέραιοι συν.

και ο μεγιστοβ.

βαθμού $n-1$, οπότε ισχύει η συνεξίστη.

επαγωγική υπόθεση.

$$a_n \equiv 0 \pmod{p}$$

Αφού $f(x_{n+1}) = f(x_1) \equiv 0 \pmod{p}$, ισχύει ότι $f(x_{n+1}) - f(x_1) = (x_{n+1} - x_1)g(x_{n+1}) \equiv 0 \pmod{p}$.

Έχουμε όμως υποθέσει ότι $x_{n+1} - x_1 \not\equiv 0 \pmod{p} \Rightarrow g(x_{n+1}) \equiv 0 \pmod{p}$.

Αυτό σημαίνει πως βρήκατε άλλη μια και άρα η μη ισοδύναμη λύση της $g(x) \equiv 0 \pmod{p}$, το οποίο αντάρχη την επαγωγική υπόθεση. $\square$

Πόρισμα:

Αν $f(x)$ αείροιο πολυώνυμο βαθμού n και περισσοτέρη από η λύση $\pmod{p}$, p πρῶτος τότε κάθε συντέλεστής του f διαρῖται με το p .

Απόδειξη:

Αν κάποιος συντέλεστής ἔστω a_k ο μεγαλύτερος δεν διαρῖται με το p , $1 \leq k \leq n$, τότε η ισοδύναμη $a_0 + a_1x + \dots + a_kx^k \equiv 0 \pmod{p}$ ἔχει περισσότερες από $k < n$ λύσεις, γιατί $\cancel{a_kx^k} + \dots + \cancel{a_1x} \equiv 0 \pmod{p}$ ἄρα, αφού πλῆι για $j > k$.
↳ από Lagrange.

Θεώρημα: (Wilson)

Για κάθε πρῶτο p , ἔχουμε $(p-1)! \equiv (-1) \pmod{p}$

Απόδειξη:

Θεωρῶ το πολυώνυμο:

$$f(x) = (x-1)(x-2) \dots (x-p+1) - x^{p-1} + 1$$

Ο βαθμός του $f(x)$ είναι $p-2$. Επίσης, ο σταθερός ὅρος του είναι ο $(p-1)! + 1$. Θα χρησιμοποιήσω το πόρισμα του Lagrange για να δείξω ότι ο $p \mid (p-1)! + 1$. Θεωρῶ το $(x-1)(x-2) \dots (x-p+1)$ και παρατηρῶ ότι οι ὁρίθοι $1, 2, 3, \dots, p-1$ είναι ρίζες του (και γενικά ἄλλα και $\pmod{p}$, αφού είναι μη ισοδύναμοι $\pmod{p}$). Όσοι όμως είναι και πρῶτοι με τον p , αφού είναι μικρότεροι και ἄρα από

Euler-Fermat ικανοποιούν την $x^{p-1} \equiv 1 \pmod{p}$. Άρα $1, 2, \dots, p-1$ ρίζες και του $(-x^{p-1} + 1) \pmod{p}$. Συνεπώς, οι $p-1$ αυτοί αριθμοί είναι και ρίζες της $f(x) \equiv 0 \pmod{p}$ που έχει βαθμό $p-1$. Συνεπώς από Lagrange ο p διαιρεί κάθε συντελεστή του και ειδικότερα τον σταθερό όρο. Άρα $p \mid (p-1)! + 1 \Rightarrow (p-1)! \equiv (-1) \pmod{p}$.

• Παρατήρηση:

Ισχύει και το αντίστροφο, δηλαδή αν $(n-1)! \equiv (-1) \pmod{n}$ τότε το n είναι πρώτος. Γιατί αν δεν ήταν θα είχε κάποιον διαιρέτη $q < n$. Αναγκαστικά, ο q θα ήταν από τους αριθμούς στο παραγοντικό. Άρα:

$$\left. \begin{array}{l} q \mid (n-1)! \\ q \mid n \Rightarrow q \mid (n-1)! + 1 \\ (n-1)! + 1 \equiv 0 \pmod{n} \end{array} \right\} \begin{array}{l} q=1 \text{ άτονο.} \\ \text{άρα } n \text{ πρώτος} \end{array}$$

$$\Rightarrow n \mid (n-1)! + 1$$

• Παράδειγμα:

Να υπολογιστεί το $(12 \cdot 13 \cdot \dots \cdot 20 \cdot 21) \pmod{11}$

• Λύση:

Γενικά, αν $a_1, \dots, a_{p-1}$ είναι $p-1$ διαδοχικοί ακέραιοι που διαιρούνται από έναν πρώτο p , τότε αποτελούν ένα ανηγμένο σύστημα υπολοίπων $\pmod{p}$, όπως είναι και $1, 2, \dots, p-1$. Άρα, σαν κλάσεις $\pmod{p}$ ταυτίζονται ανά δύο, άρα μπορεί να πάρω το γινόμενο τους, πολλαπλασιάζοντας κατά μέλη:

$$1 \cdot 2 \cdot \dots \cdot p-1 \equiv a_1 \cdot \dots \cdot a_{p-1} \pmod{p}.$$

Ειδικότερα, οι διαδοχικοί αριθμοί $12, \dots, 21$, δεν διαιρούνται με το 11 , άρα

$$12 \cdot 13 \cdot \dots \cdot 21 \equiv (p-1)! \equiv (-1) \pmod{11} \text{ από Willson.}$$

• Παράδειγμα:

N.S.O. $61! + 1 \equiv (63! + 1) \pmod{71}$

• Λύση:

Από Willson ισχύει ότι $70! \equiv (-1) \pmod{71}$. Όπως

έχουμε $63! \cdot 64 \cdot \dots \cdot 70 \equiv 63! \cdot (-7) \cdot \dots \cdot (-1) \equiv (-1)^7 63! \cdot 7! \pmod{71}$

και $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 70 \cdot 72 \equiv (-1)(1) \pmod{71} \equiv -1 \pmod{71}$.

Άρα $-1 \equiv 70! \equiv (-1) \cdot 63! \cdot (-1) \equiv 63! \pmod{71}$. Άρα
 $71 \mid 63! + 1$.

Επίσης $62 \cdot 63 \equiv (-9)(-8) \equiv 72 \equiv 1 \pmod{71}$.

Οπότε $61! + 1 \equiv (61!) \cdot 1 + 1 \equiv 61! \cdot 62 \cdot 63 + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$

Άρα ισχύει $61! + 1 \equiv 63! + 1 \pmod{71}$.

03/04/2025

Κριτήριο Θεώρημα - Συστήματα Γραμμικών Ισοδυν.:

Γενικά, ένα σύστημα γραμμικών ισοδυναμιών, δεν έχει κατ' ανάγκη λύση, ακόμα και αν η κάθε ισοδυναμία έχει.

π.χ.
$$\begin{cases} x \equiv 1 \pmod{2} \Rightarrow x \text{ περιττός} & (2,4) \neq 1 \\ x \equiv 0 \pmod{4} \Rightarrow x \text{ πολ/σις του } 4 \end{cases}$$

Παράδειγμα:

$$\begin{cases} 3x \equiv 7 \pmod{23} \\ 15x \equiv 12 \pmod{18} \end{cases}$$
 Τις λύσεις ξεχωρίζω:

1) $(3, 23) = 1 \leadsto$ μοναδική λύση $x \equiv 10 \pmod{23}$

2) $(15, 18) = 3$, $3 | 12 \leadsto 3$ λύσεις: $x \equiv 2, 8, 14 \pmod{18}$

Οι κοινές λύσεις είναι οι αριθμοί που ανήκουν στην τομή των αντιστοίχων κλάσεων:

π.χ.
$$\begin{cases} x \equiv 10 \pmod{23} \\ x \equiv 2 \pmod{18} \end{cases}$$

Από την (1) ξέρω ότι $x = 23k + 10$, $k \in \mathbb{Z}$.

Για την (2), καθορίζω τα k για τα οποία:

$23k + 10 \equiv 2 \pmod{18} \Rightarrow$

$5k \equiv -8 \pmod{18} \Rightarrow 5k \equiv 10 \pmod{18} \Rightarrow k \equiv 10 \cdot 11 \pmod{18} \Rightarrow$

$k \equiv 2 \pmod{18}$

Άρα οι λύσεις αυτές είναι:

$$\begin{aligned} x &= 23 \cdot 10 + 10 \stackrel{(2)}{\equiv} 56 \pmod{18} \text{ αλλά και } \left\{ \begin{aligned} x &\stackrel{(1)}{\equiv} 56 \pmod{23} \end{aligned} \right. \Rightarrow \end{aligned}$$

$\Rightarrow x \equiv 56 \pmod{(18 \cdot 23)} \Rightarrow x \equiv 56 \pmod{414}$

$23k + 10 = 18\alpha + 2$
Διόφαντος?

Αρτιστοιχα, θα εδωνα

$$\begin{cases} x \equiv 10 \pmod{23} \\ x \equiv 8 \pmod{18} \end{cases} \text{ και } \begin{cases} x \equiv 10 \pmod{23} \\ x \equiv 14 \pmod{18} \end{cases}$$

Γιο γενικα, ακολουθαμε τη μεθοδο λογικη της ισοπα-
καζω αποδωξης:

• Θεωρημα: (Κινεζικο Θεωρημα υπολοιπου η Νικολαχου)

Εστω τα μετρα $m_1, m_2, \dots, m_k$ θετικοι ακειροι αριθμοι
μεταξυ τους κανει δυο, δηλ. $(m_i, m_j) = 1 \ \forall i \neq j, 1 \leq i, j \leq k$.

Για $b_1, \dots, b_k$ τυχαious ακειρους, το σιστημα:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \text{ εχει ακριβως 1 λυση } \pmod{m_1 \cdot \dots \cdot m_k}$$

• Αποδωξη:

Εστω $M = m_1 \cdot \dots \cdot m_k$ και εστω $M_i = \frac{M}{m_i}$. Τότε
παρτηρω οτι $(M_i, m_i) = 1$.

Οποτε, καθε M_i εχει μοναδικο αντιστοιχο
 $M_i' \pmod{m_i}$. ($M_i M_i' \equiv 1 \pmod{m_i}$)

Εστω $x = b_1 \cdot M_1 M_1' + b_2 \cdot M_2 M_2' + \dots + b_k \cdot M_k M_k'$

Θ.δ.θ. το x ειναι λυση ολων των ισοδυναμιων
του συστηματος και παλιστα οτι ειναι μοναδικη $\pmod{M}$.

• Για καθε $1 \leq i \leq k$, δουλειοντας $\pmod{m_i}$ εχουμε:

$$x = b_1 \cancel{M_1 M_1'} + \dots + b_i \overset{1}{M_i M_i'} + \dots + b_k \cancel{M_k M_k'} \pmod{m_i}$$

Αρα $x \equiv b_i \pmod{m_i}$.

Οποτε το x κανοιποιει την τυχαία ισοδυναμια, ορα
οτις του συστηματος. ▼

• Έστω x, y δύο λύσεις του συστήματος. Τότε
 $x \equiv y \pmod{m_i}$ $\forall i$ και επειδή όλα τα m_i είναι πρώτοι
 μεταξύ τους, από ιδιότητα παίρνω $x \equiv y \pmod{m_1 \dots m_k}$
 $\Rightarrow x \equiv y \pmod{M}$. $\square$

• Παράδειγμα:

$$\begin{cases} x \equiv 11 \pmod{15} \\ x \equiv 5 \pmod{8} \\ x \equiv 12 \pmod{13} \end{cases}$$

$$23r + 10 = 181 + 2 \Rightarrow$$

$$23r - 181 = -8 \Rightarrow$$

$$181 - 23r = 8$$

$$x_1 = 72 + 23m$$

$$x_2 = 56 + 18n$$

• Λύση:

$(15, 8) = (8, 13) = (15, 13) = 1$. Άρα υπάρχουν αντίστοιχοι

Ορίζω $M = 8 \cdot 13 \cdot 15$

$$M_1 = 8 \cdot 13 = 104$$

$$M_2 = 15 \cdot 13 = 195$$

$$M_3 = 18 \cdot 8 = 120$$

Αντιστοίχοι:

$$104 M_1' \equiv 1 \pmod{15} \Rightarrow 14 M_1' \equiv 1 \pmod{15} \Rightarrow (-1) M_1' \equiv 1 \pmod{15} \Rightarrow$$

$$M_1' \equiv -1 \pmod{15} \Rightarrow M_1' \equiv 14 \pmod{15}$$

$$195 M_2' \equiv 1 \pmod{8} \Rightarrow 3 M_2' \equiv 1 \pmod{8} \Rightarrow M_2' \equiv 3 \pmod{8}$$

$$120 M_3' \equiv 1 \pmod{13} \Rightarrow 3 M_3' \equiv 1 \pmod{13} \Rightarrow M_3' \equiv 9 \pmod{13} \equiv -4 \pmod{13}$$

Η μοναδική λύση $\pmod{M}$ είναι η:

$$x = b_1 M_1 M_1' + b_2 M_2 M_2' + b_3 M_3 M_3' =$$

$$= 11(-104) + 5 \cdot 195 \cdot 3 + 12 \cdot 120(-4) = \dots = -3979 \equiv -859 \pmod{1560}$$

$$\Rightarrow x \equiv 701 \pmod{1560}$$

• Πρόταση:

Αν $m_1, \dots, m_k$ είναι αμοιβά δύο σχετικά πρώτοι μεταξύ

τους και $b_1, \dots, b_k$ τυχαίοι ακέραιοι, για κάποιους

$a_1, \dots, a_k$ τ.λ. $(a_i, m_i) = 1$, $\forall 1 \leq i \leq k$, τότε το:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases} \text{ έχει μοναδική λύση } \pmod{m_1 \dots m_k}$$

• Απόδειξη:

Αφού $(a_i, m_i) = 1$, και θz $a_i x \equiv b_i \pmod{m_i}$ είναι ισοδύναμη με τη $x \equiv b_i a_i'$ για a_i' την αντίστροφη modulo του $a_i \pmod{m_i}$. Έντα Κινέζικο.

• Παράδειγμα:

Βρίξει την ηθικία που διαρκύμεν με το :

3 έχει υπόλοιπο 1

5 — 11 — 2

7 — 11 — 2

• Λύση:

Έστω x η ηθικία:

$$x \equiv 1 \pmod{3}$$

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

$$x \equiv 2 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$72 \cdot 56 \pmod{424}$$

Άρα μοναδική λύση $\pmod{105} \rightarrow 3 \cdot 5 \cdot 7$

$$u_1 = 35, \quad u_1' \equiv 2 \pmod{3} \equiv -1 \pmod{3}$$

$$u_2 = 21, \quad u_2' \equiv 1 \pmod{5}$$

$$u_3 = 15, \quad u_3' \equiv 1 \pmod{7}$$

$$\text{Άρα } x = 1 \cdot 35(-1) + 2 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 37 \pmod{105}$$

Άρα η ηθικία είναι 37.

Πιο γενικά, για τυχαίο υπόλοιπο

$$x \equiv u_1 \pmod{3} \quad x = u_1(-35) + u_2 \cdot 21 + u_3 \cdot 15 \pmod{105}$$

$$x \equiv u_2 \pmod{5}$$

$$x \equiv u_3 \pmod{7}$$

• Παράδειγμα:

Το σύστημα
$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$
 λύση του οποίου
επίκειται στο ιθαίδικον.

• Εναλλακτική απόδειξη: (Κινέζικου)

Έστω $\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \dots, \overline{n-1} \}$. Ορίζουμε $M = m_1 \dots m_k$
και ορίζουμε την: $f: \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$
 $x \pmod{M} \mapsto (x \pmod{m_1}, \dots, x \pmod{m_k})$.

Η f είναι καλά ορισμένη (πάντα όταν έχω κλάσματα
με ανυποσυνήκτους), αφού $x \equiv y \pmod{M}$, τότε
 $x \equiv y \pmod{m_i} \quad \forall 1 \leq i \leq k$, καθώς $\forall i, m_i | M$.

Η f είναι 1-1 αφού αν $(x \pmod{m_1}, \dots, x \pmod{m_k}) =$
 $(y \pmod{m_1}, \dots, y \pmod{m_k}) \Rightarrow x \equiv y \pmod{m_i} \quad \forall 1 \leq i \leq k$ και
αφού $(m_i, m_j) = 1, i \neq j \Rightarrow x \equiv y \pmod{m_1 \dots m_k}$

Η f είναι επί, αφού $|\mathbb{Z}_M| = M = |\mathbb{Z}_{m_1}| \cdot \dots \cdot |\mathbb{Z}_{m_k}| =$
 $= |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}|$.

Συνεπώς για κάθε $(b_1 \pmod{m_1}, \dots, b_k \pmod{m_k})$ υπάρχει
μοναδικό $x \pmod{M}$ π.ω. η f το στέλνει, δηλαδή
ικανοποιούνται όλες οι εξισώσεις ταυτόχρονα. $\square$

08/04/2025

Πολυωνυμική Ισοδυναμία

Για $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ με $a_i \in \mathbb{Z}$, λύνουμε $f(x) \equiv 0 \pmod{m}$ στο $\mathbb{Z}$ για m σύνθετο αριθμό.

Θεώρημα: (εφαρμογή Κινέζικου)

Έστω f πολυώνυμο με ακέραιους συντελεστές και $m_1, \dots, m_k$ πρώτοι ανά δύο μεταξύ τους. Αν $M = m_1 \dots m_k$, τότε $f(x) \equiv 0 \pmod{M}$ ⁽¹⁾ έχει λύση $\Leftrightarrow$ κάθε $f(x) \equiv 0 \pmod{m_i}$ ⁽²⁾ έχει λύση.

Επίσης, αν $v(M)$ και $v(m_i)$ το πλήθος των λύσεων αντίστοιχα των (1) και (2), τότε $v(M) = v(m_1) \dots v(m_k)$.

Απόδειξη:

" $\Rightarrow$ " Αν a λύση της (1), τότε $f(a) \equiv 0 \pmod{M} \Rightarrow f(a) \equiv 0 \pmod{m_i}$. Άρα κάθε λύση της (1) είναι και της (2).

" $\Leftarrow$ " Έστω a_i μια λύση κάθε μιας εξίσωσης από τη (2). Άρα $a_i \equiv 0 \pmod{m_i}$. Για αυτές τις κλάσεις $a_i \equiv 0 \pmod{m_i}$, από Κινέζικο υπάρχει μοναδικός $a \in \mathbb{Z}$ τέω. $a \equiv a_i \pmod{m_i} \forall i$. Άρα $f(a) \equiv f(a_i) \pmod{m_i} \Rightarrow f(a) \equiv 0 \pmod{m_i} \forall i$. Αφού $(m_i, m_j) = 1 \forall i, j$, ισχύει ότι $f(a) \equiv 0 \pmod{M}$ και άρα η (1) έχει λύση.

Γνωρίζουμε από Κινέζικο ότι κάθε k -άδα λύσεων $(a_1, \dots, a_k)$ των εξισώσεων (2), δίνει μοναδικό ακέραιο $\pmod{M}$ που τελικά ικανοποιεί την (1). Πόσες τέτοιες περιπτώσεις?

$$(a_1, \dots, a_k) \longleftrightarrow a$$

$$\overset{\uparrow}{v(m_1)} \quad \overset{\uparrow}{v(m_k)} \quad \longleftrightarrow \quad v(m_1) \cdot \dots \cdot v(m_k) = v(M).$$

επιλογές

• Παρατήρηση:

Η επίλυση μιας πολυωνυμικής ισοδυναμίας modulo έναν σύνθετο M , ανάγεται σε αντίστοιχες επιλύσεις ισοδυναμιών modulo δυνατών πρώτων, καθώς από Θεμελιώδες Θεώρημα $M = p_1^{a_1} \dots p_k^{a_k}$ και όλοι αυτοί οι παράγοντες είναι πρώτοι μεταξύ τους. Δηλαδή δίνεται $f(x) \equiv 0 \pmod{M} \Leftrightarrow f(x) \equiv 0 \pmod{p_i^{a_i}}$.

• Παράδειγμα:

Βρείτε τις λύσεις της $x^2 - 1 \equiv 0 \pmod{12}$

• Λύση:

Η πρωτογενής ανάλυση είναι $12 = 2^2 \cdot 3$. Άρα ψάχνω τις λύσεις $\begin{cases} x^2 - 1 \equiv 0 \pmod{2^2} \text{ με λύσεις } 1 \pmod{4}, 3 \pmod{4} \\ x^2 - 1 \equiv 0 \pmod{3} \text{ με λύσεις } 1 \pmod{3}, 2 \pmod{3} \end{cases}$

Άρα η αρχική έχει $2 \cdot 2 = 4$ λύσεις. Δίνονται αυριβώς από τις λύσεις:

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{3} \end{cases}, \begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases}, \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{3} \end{cases}, \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases}$$

Από Κινέζικο, οι λύσεις είναι $1 \pmod{12}, 5 \pmod{12}, 7 \pmod{12}, 11 \pmod{12}$.

• Σκοπός:

Ψάχνω έναν μεθοδικό τρόπο να ιεραρώ από λύσεις της $f(x) \equiv 0 \pmod{p^{k+1}}$ σε λύσεις της $f(x) \equiv 0 \pmod{p^k}$, ώστε να φτάσω τελικά σε λύσεις της $f(x) \equiv 0 \pmod{p}$.

Έστω μια λύση της (2), $a \in \{0, 1, \dots, p^{k-1}\}$. Τώρα, όλοι οι $a + t \cdot p^k$ για $0 \leq t \leq p-1$ είναι ισοδύναμοι $\pmod{p^k}$ αλλά όχι ισοδύναμοι $\pmod{p^{k+1}}$. Από την άλλη, αν ο β είναι λύση της (1), τότε είναι και λύση της (2), αφού $p^k \mid p^{k+1}$. Θεωρώντας ότι

$\beta < p^{k+1}$, εκτελώ την διαίρεση του β με το p^k και παίρνω: $\beta = p^k \cdot t + \alpha$ για $0 \leq t \leq p-1$ και $0 \leq \alpha \leq p^k - 1$. Τότε έχω $\beta \equiv \alpha \pmod{p^k} \Rightarrow f(\alpha) \equiv 0 \pmod{p^k}$ ($f(p) \equiv 0 \pmod{p^k}$). Γνωρίζοντας μια λύση της (2), ελέγχω για ποιά t οι αριθμοί $p^k t + \alpha$ είναι λύσεις της (1).

• Παράδειγμα:

Να λυθεί η $x^3 - 2x + 1 \equiv 0 \pmod{5^2}$.

• Λύση:

Θεωρώ την $x^3 - 2x + 1 \equiv 0 \pmod{5}$ και βρίσκω τις λύσεις $1 \pmod{5}$, $2 \pmod{5}$. Άρα, οι πιθανές λύσεις της αρχικής είναι και οι $5t+1$ ή $5t+2$ για $t=0,1,2,3,4$.
 $\rightarrow 5t+1$: $(5t+1)^3 - 2(5t+1) + 1 \stackrel{\text{Θέλω}}{=} 5^2 \gamma, \gamma \in \mathbb{Z}$.

$$\Rightarrow \dots \Rightarrow t = 5(-5t^3 - 3t^2 + \gamma), \quad 0 \leq t \leq 4, \gamma \in \mathbb{Z}.$$

Μόνο για $t=0$ ισχύει.

$$\text{π.χ. } t=1: \quad 1 = 5(-5 - 3 + \gamma) = 1 = 5(-8 + \gamma) \Rightarrow 1 = -40 + 5\gamma \quad \text{X}.$$

$\rightarrow 5t+2$: (...) καμία λύση.

• Λήμμα Hensel:

Έστω a μια λύση της $f(x) \equiv 0 \pmod{p^k}$ με $0 \leq a \leq p^k - 1$. Τότε:

1) Αν $f'(a) \not\equiv 0 \pmod{p}$, τότε υπάρχει μοναδική λύση της $f(x) \equiv 0 \pmod{p^{k+1}}$ της μορφής $p^k t + a \pmod{p^{k+1}}$ για κάποιο $t=0, \dots, p-1$.

2) Αν $f'(a) \equiv 0 \pmod{p}$ τότε

i) αν $f(a) \not\equiv 0 \pmod{p^{k+1}}$, η $f(x) \equiv 0 \pmod{p^{k+1}}$ είναι αδύνατη

ii) αν $f(a) \equiv 0 \pmod{p^{k+1}}$, υπάρχουν p λύσεις της $f(x) \equiv 0 \pmod{p^{k+1}}$ και είναι οι $p^k t + a \pmod{p^{k+1}}$ για κάθε $t=0, 1, \dots, p-1$.

10/04/2025

Παράδειγμα:

$$4x^4 + 9x^3 - 5x^2 - 21x + 61 \equiv 0 \pmod{125}$$

Λύση:

$$125 = 3^2 \cdot 5^3, f(x) = 4x^4 + 9x^3 - 5x^2 - 21x + 61$$

$$\text{Αντι: } f(x) \equiv 0 \pmod{3^2 5^3} \rightarrow \begin{cases} f(x) \equiv 0 \pmod{3^2} & (1) \\ f(x) \equiv 0 \pmod{5^3} & (2) \end{cases}$$

και δίνω εξωποισαί.

$$f'(x) = 16x^3 + 27x^2 - 10x - 21 \quad \text{για να ελέγξω Hensel}$$

$$1) f(x) \equiv 0 \pmod{3} \rightarrow 1 \pmod{3}, 2 \pmod{3}$$

Τώρα, $f(x) \equiv 0 \pmod{3^2}$ είναι τες μορφές $1+3t, 2+3t, t=0,1,2$.

$$\underline{1 \pmod{3}}: f'(1) = 16 + 27 - 10 - 21 = 12 \equiv 0 \pmod{3} \quad \text{αρα}$$

εφασι $\alpha \equiv 2 \pmod{3}$ Hensel

Αρα $f(1) = 48 \not\equiv 0 \pmod{3^2}$, δεν υπάρχει λύση της μορφής $1+3t$ για την $f(x) \equiv 0 \pmod{3^2}$

$$\underline{2 \pmod{3}}: f'(2) \equiv 0 \pmod{3} \quad \text{και} \quad f(2) \equiv 0 \pmod{3^2} \quad \text{έχουμε}$$

3 λύσες, ως $2+3 \cdot 0, 2+3 \cdot 1, 2+3 \cdot 2 \pmod{3^2}$

2) Για το άλλο σκέλος έχω $f(x) \equiv 0 \pmod{5^3}$ και ξεκινάω με την $f(x) \equiv 0 \pmod{5}$. Ο, λύσεις είναι οι $2 \pmod{5}$ και $3 \pmod{5}$.

(Αν τις βρω, χρησιμοποιώ και αλγεβρικές μεθόδους για $f(x) = (x-2)(x-3)(2x^2-3x+18) \pmod{5}$ και βλέπω ότι δεν έχω άλλες

Τώρα ελέγχω πιθανές λύσεις του $f(x) \equiv 0 \pmod{5^2}$. Αν υπάρχουν, είναι τες μορφές $2+5b, b=0,1,2,3,4$.

$$\underline{2 \pmod{5}}: f'(2) = 195 \equiv 0 \pmod{5}$$

$$f(2) = 135 \not\equiv 0 \pmod{5^2} \quad \text{δεν έχω λύση και}$$

αρα ούτε για $\pmod{5^3}$

$3 \bmod 5$: $f'(3) = 624 \not\equiv 0 \bmod 5$, είπαμε σε 1^η Hensel,
μοναδική ρίζα $3+5t$, $t=0,1,2,3,4 \bmod 5^2$

Για $t=4$: $f(5+3 \cdot 4) = f(23) = \dots = 0 \bmod 5^2$.

Άρα το $23 \bmod 5^2$ η μοναδική λύση της
 $f(x) \equiv 0 \bmod 5^2$

Προχωράω στην $f(x) \equiv 0 \bmod 5^3$

Αφού $f'(23) \not\equiv 0 \bmod 5$, έχω πάλι μοναδική λύση
της μορφής $23+5^2t$, $t=0,1,2,3,4$. Για $t=2$:

$$f(23+5^2 \cdot 2) = f(73) \equiv 0 \bmod 5^3.$$

Άρα η $73 \bmod 5^3$ η μοναδική λύση της μορφής
 $f(x) \equiv 0 \bmod 5^3$.

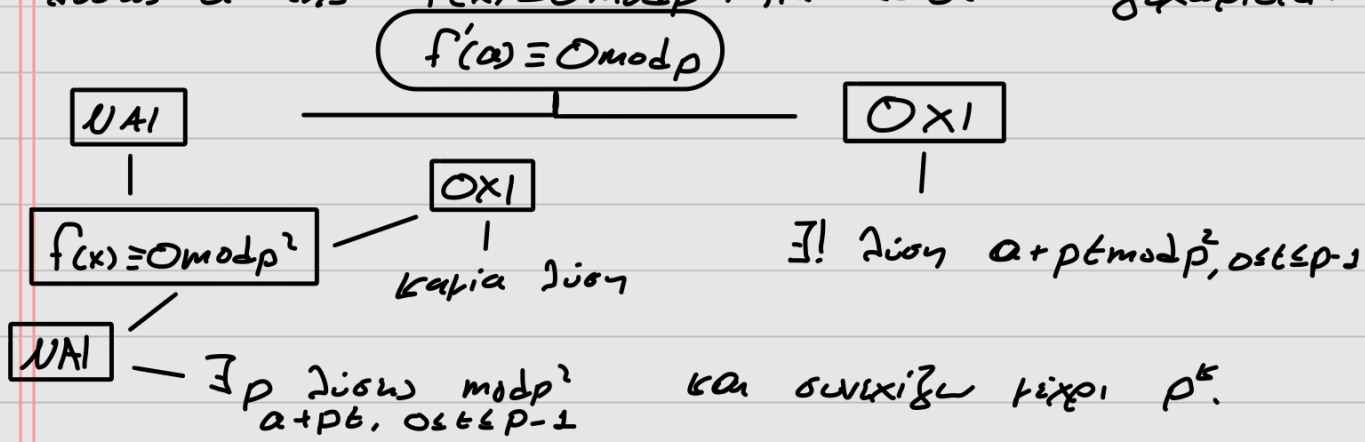
Τέλος, η (1) έχει τρεις λύσεις, τις $2, 5, 8 \bmod 3^2$ και
η (2) έχει μία λύση, την $73 \bmod 5^3$. Άρα η
 $f(x) \equiv 0 \bmod 3^2 5^3$ έχει $1 \cdot 3 = 3$ λύσεις, τις οποίες
βρίσκω με κινέζικο.

$$\begin{cases} x \equiv 73 \bmod 5^3 \\ x \equiv 2 \bmod 3^2 \end{cases}, \begin{cases} x \equiv 73 \bmod 5^3 \\ x \equiv 5 \bmod 3^2 \end{cases}, \begin{cases} x \equiv 73 \bmod 5^3 \\ x \equiv 8 \bmod 3^2 \end{cases}$$

Λύνοντας αυτά, έχουμε τις ρίζες:
 $323, -52, -427 \bmod 1125$.

Μεθοδολογία Hensel:

Για τις λύσεις της $f(x) \equiv 0 \bmod p^k$, ξεκινάω από τις
λύσεις α της $f(x) \equiv 0 \bmod p$. Για κάθε α ξεκινάω:



ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ - ΤΕΤΡΑΓΩΝΙΚΗ ΑΝΤΙΣΤΡΟΦΗ

Προηγουμένως, $f(x) \equiv 0 \pmod{n}$ για σύνθετο n ανάχεται σε πολυωνυμικές ισοδυναμίες modulo πρώτους αριθμούς και στο ζεύγος συστήματα γραμμικών ισοδυναμιών.

Για $f(x) \equiv 0 \pmod{p}$, πηγαίμε ψαχτά. Γενικά, μια μέθοδος για εύρεση τέτοιων ριζών παραμένει ανοιχτό πρόβλημα στη Θεωρία Αριθμών.

- Για $f(x)$ πρώτου βαθμού (γραμμικές ισοδυναμίες) έχουμε γενικές λύσεις της $f(x) \equiv 0 \pmod{p}$. Δηλαδή, για $F(x) = ax + b$ ($p \nmid a$ αλλιώς $a < p$) τότε $x \equiv a^{-1}(-b) \pmod{p}$ (αν $p \mid b$ τότε $x \equiv 0 \pmod{p}$ λύση).
- Για $f(x)$ δεύτερου βαθμού, δηλ. $a_2x^2 + a_1x + a_0 \equiv 0 \pmod{p}$ το πρόβλημα ύπαρξης έχει λυθεί ήδη ως αλλιώς και πάλι χωρίς γενική μέθοδο για τον υπολογισμό της.

Ξεκινάμε μελετώντας τετραγωνικές ισοαμίες της μορφής $x^2 \equiv n \pmod{p}$, για p περιττό πρώτο. (για $p=2$, $x \equiv 0$ ή $x \equiv 1$ εύκολα λύσεις). $\text{spr}(n \equiv 0 \pmod{p})$

Από Lagrange, η $x^2 - n \equiv 0 \pmod{p}$ έχει το πολύ δύο λύσεις, όσοι ο βαθμός του πολυωνύμου. Επίσης, ισχύει ότι αν x είναι λύση, τότε ο $(-x)$ είναι λύση. Άρα, η $x^2 \equiv n \pmod{p}$ έχει ή 0 ή 2 λύσεις.

Ορισμός:

Αν η $x^2 \equiv n \pmod{p}$ έχει λύση, τότε λέμε ότι ο n είναι τετραγωνικό υπόλοιπο $\pmod{p}$ και γράφουμε $n \in \mathbb{R}_p$ ή $n \in \mathbb{T}\mathbb{U} \pmod{p}$. Αλλιώς, λέμε ότι n είναι τετραγωνικό μη-υπόλοιπο $\pmod{p}$ και γράφουμε $n \notin \mathbb{R}_p$ ή $n \notin \mathbb{T}\mathbb{U} \pmod{p}$.

~> Βασικά Προβλήματα:

- I) Για συγκεκριμένο p , ποιές κλάσεις του είναι η
είναι $TY_{mod p}$ και ποιές $TM_{mod p}$.
- II) Για συγκεκριμένο n , ποιοι είναι οι πρώτοι p για τους
οποίους $nTY_{mod p}$ και ποιοι $nTM_{mod p}$.

• Παράδειγμα: $TY_{mod 11}?$

• Λύση:

Παίρνω όλες τις μη μηδενικές κλάσεις $mod 11$, υπολο-
γίζω τα τετράγωνα και έχω:

$$1^2 \equiv 1 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 4^2 \equiv 5 \pmod{11}, \quad 5^2 \equiv 3 \pmod{11}, \\ 6^2 \equiv 3 \pmod{11}, \quad 7^2 \equiv 5 \pmod{11}, \quad 8^2 \equiv 9 \pmod{11}, \quad 9^2 \equiv 4 \pmod{11}, \quad 10^2 \equiv 1 \pmod{11}$$

Όμως, $6 \equiv -5 \pmod{11}$, άρα $6^2 \equiv (-5)^2 \equiv 3 \pmod{11}$ χωρίς
να το ξαναυπολογίσω.

Καταλαύουμε στο ότι τα $1, 4, 5, 9, 3$ είναι τετράγωνα
υπόλοιπα $mod 11$, ενώ τα $2, 6, 7, 8, 10$ είναι $TM_{mod 11}$.
(δηλ. δεν φτιάχνονται από κανένα τετράγωνο αριθμοί
 $mod 11$).

Παρατηρώ ότι τα κατασκευάζω, υπολογίζοντας τα
 $1^2, 2^2, 3^2, 4^2, 5^2$ μόνο!
 $\hookrightarrow \frac{p-1}{2}$

• Θεώρημα:

Έστω p πρώτος αριθμός ($p \geq 3$). Τότε κάθε ανήκοντο
σύστημα υπολοίπων (για να μην έχω μέσα το 0),
περιέχει ακριβώς $\frac{p-1}{2}$ $TY_{mod p}$ και $\frac{p-1}{2}$ $TM_{mod p}$.
Τα $TY_{mod p}$ είναι οι κλάσεις των $1^2, 2^2, \dots, (\frac{p-1}{2})^2$.

Απόδειξη:

Πρώτον, οι αριθμοί αυτοί είναι διαφορετικοί μεταξύ τους $\text{mod } p$. Ουτως, αν $x^2 \equiv y^2 \text{mod } p \Rightarrow (x-y)(x+y) \equiv 0 \text{mod } p$

Αλλά, $1 \leq x, y \leq \frac{p-1}{2}$, ισχύει ότι $2 \leq x+y \leq p-1$ ή $1 < x+y < p$, άρα $x-y \equiv 0 \text{mod } p \Rightarrow x \equiv y \text{mod } p$, αφού ο p πρώτος.

Τώρα, αφού $(-x)^2 \equiv (p-x)^2 \equiv (x)^2 \text{mod } p$, εκτός από το $x \text{mod } p$ είναι ένας από αυτούς.

30/04/2025

• Παράδειγμα:

	$p=3$	$p=5$	$p=7$	$p=13$
TY	1	1, 4	1, 4, 2	1, 4, 9, 3, 12, 10
TUY	2	2, 3	3, 5, 6	2, 5, 6, 7, 8, 11

→ Σύμβολο Legendre:

Δ_n $n \not\equiv 0 \pmod p$ και p πρώτος:

$$(n|p) = \begin{cases} 1 & , n \in TY \pmod p \\ -1 & , n \in TUY \pmod p \end{cases}$$

$$\Delta_n \quad n \equiv 0 \pmod p \rightarrow (n|p) = 0$$

Π.χ.

• $(1|p) = 1$ αφού 1 είναι $TY \pmod p$

• $(m^2|p) = 1$ εξ' ορισμού

• $(7|11) = -1$ αφού $7 \in TUY \pmod{11}$

• $(22|11) = 0$, αφού $11|22$

• $(n|p) = (m|p)$ όταν $n \equiv m \pmod p$ καθώς είναι και τα δύο $TY \pmod p$ ή όχι.

• $\sum_{a=1}^{p-1} (a|p) = 0$, αφού από Θεώρημα $\exists \frac{p-1}{2} \in TY \pmod p$ και $\frac{p-1}{2} \in TUY \pmod p$. Άρα $\sum_{a=1}^{p-1} (a|p) = \sum_{a \in TY} (a|p) + \sum_{a \in TUY} (a|p) = (+1) \left(\frac{p-1}{2} \right) + (-1) \left(\frac{p-1}{2} \right) = 0$

• $\prod_{a=1}^{p-1} (a|p) = \underbrace{(+1)(+1) \dots}_{\frac{p-1}{2}} \cdot \underbrace{(-1)(-1) \dots}_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$

→ Από Euler-Fermat, $n^{p-1} \equiv 1 \pmod p$, $p \nmid n$. Τότε για $p > 3$:

$$(n^{p-1} - 1) \equiv 0 \pmod p \Rightarrow (n^{\frac{p-1}{2}} + 1)(n^{\frac{p-1}{2}} - 1) \equiv 0 \pmod p$$

Τότε, αφού p πρώτος: $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ που ισχύει γενικά.

• Θεώρημα: (Κριτήριο Euler)

Έστω p πρώτος. Τότε, $\forall n$ έχουμε
 $(n|p) \equiv n^{\frac{p-1}{2}} \pmod{p}$. Άρα, $n \text{ TY} \pmod{p} \Rightarrow n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
 $n \text{ TUX} \pmod{p} \Rightarrow n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

• Απόδειξη:

Αν $n \equiv 0 \pmod{p}$, τότε και τα δύο μέρη είναι 0.
 $\rightarrow$ Έστω $(n|p) = 1$, άρα $\exists x$ με $p \nmid x$ με $x^2 \equiv n \pmod{p}$
 $\Rightarrow n^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} \Rightarrow n^{\frac{p-1}{2}} = x^{p-1} \equiv \underbrace{1}_{\text{HWP}} \pmod{p}$

Άρα $n^{\frac{p-1}{2}} \equiv (n|p) \pmod{p}$.

Έστω $(n|p) = -1$. Θεωρώ το $f(x) = x^{\frac{p-1}{2}} - 1$ με βαθμό $\frac{p-1}{2}$, άρα από Lagrange, η $f(x) \equiv 0 \pmod{p}$ έχει το πολύ $\frac{p-1}{2}$ λύσεις.

Οπως όλα τα TY είναι λύσεις της!

π.χ. $m \equiv y^2 \pmod{p} \Rightarrow f(m) = (y^{\frac{p-1}{2}})^2 - 1 = y^{p-1} - 1 \equiv 0 \pmod{p}$.

Άρα τα $\text{TY} \pmod{p}$ είναι ακριβώς $\frac{p-1}{2}$ το πολύ, άρα αναγκαστικά τα $\text{TUX} \pmod{p}$ δεν είναι λύσεις της.

Οπότε για το αρχικό n , $f(n) \not\equiv 0 \pmod{p} \Rightarrow n^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$.

Από παρατήρηση $\Rightarrow n^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Rightarrow n^{\frac{p-1}{2}} \equiv (n|p) \pmod{p}$.

π.χ. Για $p=29$, $(2|29)$

$$\begin{aligned} \text{Από Euler: } 2^{\frac{29-1}{2}} &= 2^{14} = (2^7)^2 = (2^5 \cdot 2^2)^2 = (32 \cdot 2^2)^2 = \\ &= (3 \cdot 2^2)^2 = 12^2 = 144 \equiv 28 \equiv -1 \pmod{29} \end{aligned}$$

Το $(2|29) = -1$ άρα $2 \text{ TUX} \pmod{29}$, δηλαδή η $x^2 \equiv 2 \pmod{29}$ δεν έχει λύση.

$\rightarrow$ Εναλλακτική απόδειξη Κριτηρίου Euler για $n \text{ TUX} \pmod{p}$:
Παρατηρώ ότι $\forall i \in \{1, 2, \dots, p-1\}$ υπάρχει $j \in \{1, 2, \dots, p-1\}$ c.t.
 $i \cdot j \equiv n \pmod{p}$. Οπότε $i(i' \cdot n) \equiv n \pmod{p}$ αφού i είναι αντιστρέψιμος (αφού p πρώτος).

Επίσης, αν $n \nmid p$, τότε $i \neq j \pmod p$ γιατί
αλλιώς θα είχα $i \equiv i \cdot n \pmod p \Rightarrow i \cdot i \equiv n \pmod p \Rightarrow i^2 \equiv n \pmod p$
Από το

Οπότε $\exists$ ακριβώς $\frac{p-1}{2}$ ζεύγη αριθμών
και πολλές φορές τις ισότητες $ij \equiv n \pmod p$
 $1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv n^{\frac{p-1}{2}} \pmod p \Rightarrow n^{\frac{p-1}{2}} \equiv (-1) \pmod p \quad \square$

Π.χ. Δ.δ. το -1 είναι $T \pmod p$ αν και μόνο αν
 $p \equiv 1 \pmod 4$ ($-1 \equiv (p-1) \pmod p$)

$-1 \pmod p \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p \Rightarrow \frac{p-1}{2}$ άρτιος,
δηλαδή $\frac{p-1}{2} = 2k \Rightarrow p-1 = 4k \Rightarrow p \equiv 1 \pmod 4$

Αντιστοίχα, μπορεί v.δ.ο. $-1 \pmod p \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$
 $\Leftrightarrow \frac{p-1}{2}$ περιττός $\Leftrightarrow \frac{p-1}{2} = 2k+1 \Rightarrow p-1 = 4k+2 \Rightarrow p \equiv 3 \pmod 4$

Θεώρημα:

Το σύμβολο Legendre ορίζει μια πράσινη πράσινη
αριθμητική συνάρτηση $\mathbb{N} \xrightarrow{(-1)^{\frac{p-1}{2}}} \mathbb{N}$, $n \mapsto (n|p)$.

Απόδειξη:

- Θ.δ.ο. $(n|p)(m|p) = (n \cdot m|p) \quad \forall n, m \in \mathbb{N}$ p πρώτος
- Αν $p|n$ ή $p|m \Rightarrow p|n \cdot m \Rightarrow (n \cdot m|p) = 0$
και αντίστροφα $p|n \cdot m \Rightarrow p|m$ ή $p|n$ ή και τα δύο.
 - Αν $p \nmid n$ και $p \nmid m$ τότε $p \nmid n \cdot m$ και έχουμε
 $(n \cdot m|p) \equiv (n \cdot m)^{\frac{p-1}{2}} = n^{\frac{p-1}{2}} \cdot m^{\frac{p-1}{2}} \equiv (n|p)(m|p) \pmod p$

$\leadsto$ Αυτό όμως δεν είναι αρκετό για απλή και όχι
 $\pmod p$ ισότητα δύο αριθμών γενικά.

Όμως, κάθε ένα από αυτά είναι είτε 1 είτε -1
οπότε για την (απλή, όχι $\pmod p$) διαφορά τους,
έχουμε: $(m \cdot n|p) - (m|p)(n|p) = \begin{cases} 2 \\ -2 \end{cases} (\neq 1)$

Υπολογίζοντας mod p βλέπω ότι οι περιπτώσεις 2 και -2 απορρίπτονται γιατί $2, -2 \not\equiv 0 \pmod{p}$ αφού $p \geq 3$. Άρα είμαστε στην πρώτη περίπτωση (*) και άρα $(m \cdot n \mid p) = (m \mid p)(n \mid p)$

π.χ.

$$(-520 \mid 3)$$

$$520 = 2^3 \cdot 5 \cdot 13 \quad \text{άρα:}$$

$$(-520 \mid 3) = (-1 \mid 3)(2^3 \mid 3)(5 \mid 3)(13 \mid 3)$$

$$(-1 \mid 3) \equiv -1, \text{ αφού } p \equiv 3 \pmod{4}$$

$$(2^3 \mid 3) = (2 \mid 3)^3 \equiv (-1)$$

$$(5 \mid 3) = (2 \mid 3) = -1$$

$$(13 \mid 3) = (1 \mid 13) = 1$$

$$\text{Άρα } (-520 \mid 3) = (-1)(-1)(-1)(1) = -1 \quad \text{άρα } -520 \text{ τετ. mod } 3.$$

02/05/2025

• Πρόταση ^(IE): (note $2 \nmid \chi \bmod p$)

Για p περιττό πρώτο, $(2|p) = (-1)^{\frac{p^2-1}{8}}$, άρα
$$(2|p) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

• Απόδειξη:

Φαίνου ένα σύστημα $\frac{p-1}{2}$ ισοδυναμίες

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

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

$$p-3 \equiv 3(-1)^3 \bmod p$$

$$4 \equiv 4(-1)^4 \bmod p$$

$\vdots$

$$t \equiv \frac{p-1}{2} (-1)^{\frac{p-1}{2}} \bmod p \quad \text{όπου } t = p - \frac{p-1}{2} \text{ ή } t = \frac{p-1}{2},$$

ανάλογα ποιος είναι άρτιος

Παρατηρώ ότι στα αριστερά μέλη έχω μόνο άρτιους αριθμούς.

π.χ. για $p=11$

$$10 \equiv (-1) \bmod 11$$

$$2 \equiv 2 \bmod 11$$

$$8 \equiv (-3) \bmod 11$$

$$4 \equiv 4 \bmod 11$$

$$6 \equiv (-5) \bmod 11$$

Πολλαπλασιάζοντας όλες τις ισοδυναμίες κατά μέλη,

παίρνω:

$$2 \cdot 4 \cdot \dots \cdot (p-3)(p-1) \equiv \left(\frac{p-1}{2}\right)! (-1)^{1+2+\dots+\frac{p-1}{2}} \bmod p$$

$\begin{matrix} \text{"} & \text{"} & \text{"} & \text{"} \\ 2 \cdot 1 & 2 \cdot 2 & 2(\frac{p-1}{2}-1) & 2(\frac{p-1}{2}) \end{matrix}$

$$\begin{aligned} & \rightarrow 2^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2} - 1\right) \left(\frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \Rightarrow \\ & \Rightarrow 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (-1)^{\frac{(\frac{p-1}{2})(\frac{p-1}{2}+1)}{2}} \bmod p \end{aligned}$$

$\Rightarrow$

$$\Rightarrow 2^{\frac{p-1}{2}} \left(\frac{p-1}{2} \right)! \equiv \left(\frac{p-1}{2} \right)! (-1)^{\frac{p^2-1}{8}} \pmod{p} \Rightarrow$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p} \stackrel{\text{Euler}}{\Rightarrow} (2|p) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Άρα και τα δύο μέλη είναι $\pm 1 \Rightarrow$

$$(2|p) \equiv (-1)^{\frac{p^2-1}{8}}. \quad \square$$

Παράδειγμα:

$$(2|11) = \begin{cases} 2^{\frac{11-1}{2}} = 2^5 = 2 \pmod{11} \text{ από Euler (χρυσόβερρο)} \\ \text{αντιθέτως από πρόταση είναι } -1, \text{ αφού} \\ 11 \equiv 3 \pmod{8} \end{cases}$$

Άρα $2 \nmid 11 \pmod{11}$

* Αν και το κριτήριο του Euler δίνει "εύνο" για τον υπολογισμό καίθε $(n|p)$, ο υπολογισμός μπορεί να είναι πολύ δύσκολος (π.χ. για μεγάλο n ή p). Το παρακάτω αποτέλεσμα του Gauss δίνει έναν πιο απλό υπολογισμό.

Λήμμα Gauss:

Έστω $n \not\equiv 0 \pmod{p}$. Θεωρούμε τις εξής $\frac{p-1}{2}$ κλάσεις πολλαπλασίων $n \pmod{p}$.

$$n, 2n, 3n, \dots, \left(\frac{p-1}{2} \right) n \pmod{p}.$$

Αν m το n ηθος εκκίνων που είναι $> \frac{p}{2}$, τότε $(n|p) = (-1)^m$

Απόδειξη:

Κατ' αρχάς, όλες αυτές οι κλάσεις είναι μη ισοδύναμες $\pmod{p}$, γιατί αλλιώς θα είχαμε:

$$k \equiv \ell \pmod{p} \stackrel{\text{νόμος}}{\Rightarrow} k \equiv \ell \pmod{p} \quad \text{✗}$$

Τις ξεχωρίζουμε σε δύο ξένα μεταξύ τους σύνολα, βάσει του αν είναι $> \frac{p}{2}$ ή $< \frac{p}{2} \pmod{p}$.

$$A = \{a_1, \dots, a_k\} \text{ με } a_i \equiv t \cdot n \pmod{p}, \quad 1 \leq t \leq \frac{p-1}{2}, \quad 0 < a_i < \frac{p}{2}$$

$$B = \{b_1, \dots, b_m\} \text{ με } b_j \equiv s \cdot n \pmod{p}, \quad 1 \leq s \leq \frac{p-1}{2}, \quad 0 < b_j < p$$

Αναγκαστικά, από τις ταξίδια των συνόλων, έχουμε ότι $k+m = \frac{p-1}{2}$.

Σχηματίζουμε τώρα το σύνολο:

$$C = \{c_1, \dots, c_m\} \text{ με } c_i = p - b_i.$$

Για αυτό τα c_i είναι όσα και τα b_i . Άρα $0 < c_i < \frac{p}{2}$. Όμως τα A και C είναι ξένα μεταξύ τους, γιατί:

$$\text{Έστω } c_i \equiv a_j \pmod{p} \text{ για κάποια } i, j. \Rightarrow$$

$$\Rightarrow p - b_i \equiv a_j \pmod{p} \Rightarrow -s \cdot n \equiv t \cdot n \pmod{p} \Rightarrow$$

$$\Rightarrow t \cdot n + s \cdot n \equiv 0 \pmod{p} \Rightarrow n(t+s) \equiv 0 \pmod{p} \Rightarrow$$

$t+s \equiv 0 \pmod{p}$, αφού όπως $t+s < p$, δεν μπορεί να έχω $t+s=p$, άρα άτοπο.

Συνεπώς, η ένωση $A \cup C = \{a_1, \dots, a_k, c_1, \dots, c_m\}$ περιέχει διακεκριμένους $m+k = \frac{p-1}{2}$ αριθμούς, που βρίσκονται στο ακέραιο διάστημα $[1, \frac{p-1}{2}]$.

Άρα αναγκαστικά $A \cup C = \{1, 2, \dots, \frac{p-1}{2}\}$. Παιρνοντας τα γινόμενα, έχουμε $a_1 \dots a_k \cdot c_1 \dots c_m = (\frac{p-1}{2})! \Rightarrow$
 $\Rightarrow (\frac{p-1}{2})! = a_1 \dots a_k \cdot \underbrace{(p-b_1) \dots (p-b_m)}_{-b_1}$ και δουλεύουμε $\pmod{p}$:

$$\left(\frac{p-1}{2}\right)! \equiv a_1 \dots a_k \cdot (-b_1) \dots (-b_m) \pmod{p} \Rightarrow$$

$$\left(\frac{p-1}{2}\right)! \equiv a_1 \dots a_k \cdot b_1 \dots b_m \cdot (-1)^m \pmod{p} \Rightarrow$$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^m \cdot n(2n)(3n) \dots \left(\frac{p-1}{2} \cdot n\right) \pmod{p} \Rightarrow$$

$$\Rightarrow \left(\frac{p-1}{2}\right)! \equiv (-1)^m \cdot n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \Rightarrow$$

$\Rightarrow 1 \equiv (-1)^m \cdot n^{\frac{p-1}{2}} \pmod{p}$, άρα πρέπει και οι δύο όροι στα δεξιά να είναι 1 ή $-1 \pmod{p}$ ζευγάρους
άρα είναι ίσα $\pmod{p} \Rightarrow$

$$n^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p} \xRightarrow{\text{Euler}} (n/p) \equiv (-1)^m \pmod{p}. \quad \square$$

• Παράδειγμα:

Είναι το $5 \text{ TY} \pmod{11}$?

• Λύση:

Από Λήμμα Gauss, $(5/11) = (-1)^m \pmod{11}$, όπου m είναι το ημίθλος των κλάσεων $1 \cdot 5, 2 \cdot 5, 3 \cdot 5, 4 \cdot 5, 5 \cdot 5 \pmod{11}$ που είναι μεγαλύτεροι του 5 (μας νοιάζει αν το ημίθλος τους είναι άρτιο ή περιττό).

$$1 \cdot 5 \equiv 5 \pmod{11} \leq 5 \quad \times$$

$$2 \cdot 5 \equiv 10 \pmod{11} > 5 \quad \checkmark$$

$$3 \cdot 5 \equiv 4 \pmod{11} \leq 5 \quad \times$$

$$4 \cdot 5 \equiv 9 \pmod{11} > 5 \quad \checkmark$$

$$5 \cdot 5 \equiv 3 \pmod{11} \leq 5 \quad \times$$

} Άρα $(5/11) = (-1)^2 \equiv 1 \pmod{11} \Rightarrow$
 $5 \text{ TY} \pmod{11}$

• Θεώρημα: (αρτιότητας του m)

Για το m που εμφανίζεται στο Λήμμα του Gauss,

έχουμε:

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{t \cdot n}{p} \right] + (n-1) \frac{p-1}{8} \pmod{2}.$$

Ειδικότερα, αν η περιζωδός $(n-1) \frac{p-1}{8} \equiv 0 \pmod{2}$, άρα

$$m \equiv \sum_{t=1}^{\frac{p-1}{2}} \left[\frac{t \cdot n}{p} \right]$$

Παράδειγμα:

Για $n=5$, $p=11$:

$$m = \sum_{t=1}^5 \left\lfloor \frac{5 \cdot t}{11} \right\rfloor \bmod 2$$

$$\begin{aligned} m &= \left\lfloor \frac{5}{11} \right\rfloor + \left\lfloor \frac{5 \cdot 2}{11} \right\rfloor + \left\lfloor \frac{5 \cdot 3}{11} \right\rfloor + \left\lfloor \frac{5 \cdot 4}{11} \right\rfloor + \left\lfloor \frac{5 \cdot 5}{11} \right\rfloor = \\ &= 0 + 0 + 1 + 1 + 2 = 4 \equiv 0 \bmod 2. \end{aligned}$$

Άρα $(5|11) \equiv (-1)^0 \equiv 1 \Rightarrow 5 \text{ ΤΥ} \bmod 11$.

Νέος Τετραγωνικός Αυστοστροφής

→ Μέχρι τώρα, Euler και Gauss δίνουν λύσεις του
πρώτου προβλήματος I. Τα προβλήματα τύπου II,
είναι δύσκολα. $\eta \text{ ΤΥ} \rightarrow$ για ποιά p ?
_{1) συγχερίσιμα}

[Euler, Legendre, Gauss ~ 1796]

→ Ιδια Θεωρήματα:

$(p|q) = (q|p)$ για $p \neq q$ πρώτοι
εκτός αν $p \equiv q \equiv 3 \bmod 4$ οπότε και $(p|q) = -(q|p)$.

Ανταδίδει, συσχετίζει με ακριβή τρόπο τις λύσεις
της $x^2 \equiv q \bmod p$ με τις λύσεις της $x^2 \equiv p \bmod q$:
και οι δύο είναι ταυτόχρονα επιλύσιμες (ή ταυτόχρονα
μη επιλύσιμες) αν έστω και ένας από τους δύο
πρώτους είναι της μορφής $4n+1$. Αν όχι και οι
δύο πρώτοι είναι της μορφής $4n+3$, τότε η μία
είναι και η άλλη δεν είναι επιλύσιμη.

• Παράδειγμα: ($p=5, p=7$)

Για $p=5 (=4 \cdot 1 + 1)$, ξέρω ότι τα 1 και 4 είναι $\text{TY}_{\text{mod } 5}$. Δηλαδή για οποιονδήποτε πρώτο $q \neq 5$, η $x^2 \equiv q \pmod{5}$ έχει λύση αν $q \equiv 1 \pmod{5}$ ή $q \equiv 4 \pmod{5}$. Ποιος αντιστοίχως? 1-| $x^2 \equiv 5 \pmod{q}$ για τα παραπάνω q έχει πάντα λύση, δηλ. $5 \text{TY}_{\text{mod } q}$.

Για $p=7 (=4 \cdot 1 + 3)$, ξέρουμε ότι τα 1, 2, 4 είναι $\text{TY}_{\text{mod } 7}$. Ποιος αντιστοίχως? Για $q \neq 7$, παίρνουμε:
 $\leadsto$ αν $q \equiv 1/2/4 \pmod{7}$ και $q = 4n+1 \Rightarrow 7 \text{TY}_{\text{mod } q}$
 $\leadsto$ αν $q \equiv 1/2/4 \pmod{7}$ και $q = 4n+3 \Rightarrow 7 \text{NTY}_{\text{mod } q}$
 $\leadsto$ αν $q \equiv 3/3/6 \pmod{7}$ και $q = 4n+3 \Rightarrow 7 \text{TY}_{\text{mod } q}$

• Θεώρημα: (Νόμος Τετραγωνικής Αντιστοίχως)

Αν p, q διαφορετικοί περιζωτοί πρώτοι:

$$(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

$\leadsto$ Παρατηρώ ότι αν $p, q \equiv 3 \pmod{4} \Rightarrow$

$$\Rightarrow \frac{(4k+3-1)(4\lambda+3-1)}{4} = \frac{(4k+2)(4\lambda+2)}{4} = \frac{2 \cdot 2(2k+1)(2\lambda+1)}{4} =$$

$$= 4k\lambda + 2k + 2\lambda + 1 = 2(2k\lambda + k + \lambda) + 1.$$

$$\lambda \rho \alpha \quad (p|q)(q|p) = (-1)^{2k\lambda+2k+2\lambda+1} = (-1) \Rightarrow (p|q) = -(q|p).$$

$$\text{Αλλά } p=4k+1, \quad \frac{(4k+1-1)(q-1)}{4} = \frac{4k(q-1)}{4} \text{ άρτιος}$$

$$(p|q)(q|p) = (-1)^{\text{άρτιος}} = 1.$$

07/05/2025

$$(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Απόδειξη:

Από Λήμμα Gauss και ζήνο για m , έχουμε

$$(p|q) = (-1)^m, \quad m = \sum_{t=1}^{q-1} \left[\frac{tp}{q} \right] \pmod{2}$$

$$(q|p) = (-1)^n, \quad n = \sum_{s=1}^{p-1} \left[\frac{sq}{p} \right] \pmod{2}$$

$$\text{Άρα } (p|q)(q|p) = (-1)^{m+n} \quad \text{Ο.δ.ο. } m+n = \frac{q-1}{2} \cdot \frac{p-1}{2} \quad (*)$$

Θεωρώ τη συνάρτηση $f(x,y) = px - qy$ με $1 \leq x \leq \frac{q}{2}, 1 \leq y \leq \frac{p}{2}$.

Βλίνω ότι $f(x,y) \neq 0$ για $x,y \neq 0$.

Για τις τιμές $x \in \{1, 2, \dots, \frac{q-1}{2}\}, y \in \{1, 2, \dots, \frac{p-1}{2}\}$ η $f(x,y)$ παίρνει $\frac{q-1}{2} \cdot \frac{p-1}{2}$ διαφορετικές τιμές, άρα:

$$\begin{aligned} f(x,y) - f(x',y') &= px - qy - px' + qy' = p(x-x') - q(y-y') = \\ &= f(x-x', y-y') \neq 0, \text{ αν } x-x' \neq 0, y-y' \neq 0. \end{aligned}$$

Ποιες από αυτές τις τιμές είναι θετικές και ποιες αρνητικές?

Αν φιξάσουμε το x , $f(x,y) > 0 \Leftrightarrow px - qy > 0 \Leftrightarrow$

$$y < \frac{px}{q}$$

ή αλλιώς $y \leq \left[\frac{px}{q} \right]$. Άρα ισχύει για

$$y = 1, 2, \dots, \left[\frac{px}{q} \right].$$

Συνολικά, το πλήθος των θετικών τιμών είναι:

$$\sum_{x=1}^{\frac{q-1}{2}} \left[\frac{px}{q} \right] \sim y, \text{ για κάθε τιμή του } x.$$

$$\text{Ομοίως, τα αρνητικά } y \text{ είναι } \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{qy}{p} \right]$$

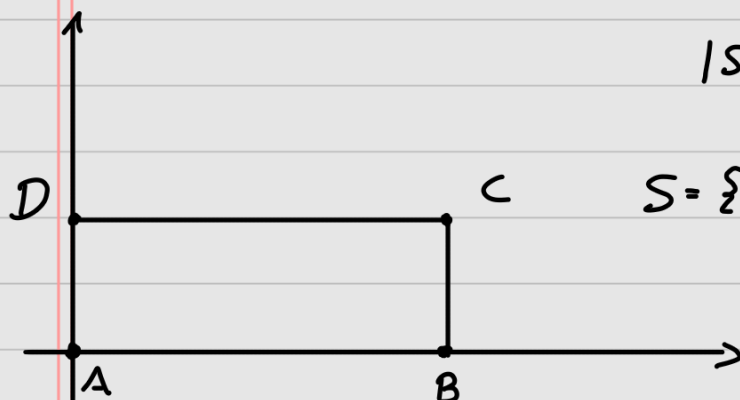
Άρα, όπως οι τιμές, είναι συνολικά:

$$\sum + \sum = \frac{q-1}{2} \cdot \frac{p-1}{2} \quad (*) \quad \square$$

→ Ένα ενδιαφέρουσα Απόδειξη:

Παίρνω τη σφαίρα

$$A(0,0), B(\frac{q}{2},0), C(\frac{q}{2},\frac{p}{2}), D(0,\frac{p}{2})$$



$$|S| = \frac{q-1}{2} \cdot \frac{p-1}{2},$$

$$S = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq x \leq \frac{q-1}{2}, 1 \leq y \leq \frac{p-1}{2}\}$$

$$\ominus. \text{δ.ο. } |S| = \Sigma + \Sigma.$$

Πρώτα, έστω ε η ευθεία που διέρχεται από το A και C με εξίσωση $y = \frac{p}{q}x \Rightarrow qy = px$.

Αφού $\frac{p}{q}$ ανάγωγο και $(p,q)=1$, κανένα σημείο του S δεν είναι πάνω στην ε : αλλιώς, θα ισχυε

$y_0 = \frac{p}{q}x_0$ για $(x_0, y_0) \in S$, άρα θα είχατε $x = ky$ για $k \in \mathbb{Z}$, που είναι άτοπο, γιατί $x_0 < \frac{q}{2}$.

Εξαιρίζουμε τα σημεία κάτω από την ευθεία ε , δηλαδή $(x,y) \in S$ με $qy < px$. Για σταθερή τετμημένη, είναι τα $(x,1), (x,2), \dots, (x, \lfloor \frac{px}{q} \rfloor)$ που είναι $\lfloor \frac{px}{q} \rfloor$ το πλήθος. Άρα για όλες τις μηδενικές τετμημένες, έχουμε σύνολα σημείων $\sum_{x=1}^{\frac{q-1}{2}} \lfloor \frac{px}{q} \rfloor$.

Αναλόγως, τα σημεία του S πάνω από την ε είναι το πλήθος $\sum_{y=1}^{\frac{p-1}{2}} \lfloor \frac{qy}{p} \rfloor$ $\square$

→ Παρατήρηση:

Στο κομμάτι της απόδειξης του (*) χρησιμοποιήσαμε μόνο ότι $(p,q)=1$, όχι ότι είναι πρώτοι.

Παράδειγμα:

Το 219 είναι TY ή $TY \pmod{383}$?

Λύση:

$$(219|383) = (3 \cdot 73|383) = (3|383)(73|383)$$

$$\leadsto (3|383) = -(383|3) = -(2|3) = -(-1) = 1$$

$$\leadsto (73|383) = (383|73) = (18|73) = (2|73)(3^2|73) = 1 \cdot 1 = 1$$

Άρα $(219|383) = 1 \cdot 1 = 1$, άρα 219 είναι $TY \pmod{383}$.

Παράδειγμα:

Να προσδιοριστούν οι περιττοί πρώτοι για τους οποίους ο 3 είναι $TY \pmod{p}$.

Λύση:

Από νόμο αντιστροφής, έχουμε για $p \neq 3$

$$(3|p) = (p|3) (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{(p-1)x}{4}} \cdot (p|3)$$

καθορίζεται από το $p \pmod{3} \leadsto \begin{matrix} 1 & TY \pmod{3} \\ 2 & TY \pmod{3} \end{matrix}$

$$\left(\begin{cases} p = u_1 \pmod{3} \\ p = u_2 \pmod{4} \end{cases} \right)$$

Συνεπώς, εξετάζω το $p \pmod{12}$. Για p περιττός πρώτος, έχω μόνο ως $1, 5, 7, 11 \pmod{12}$. Γιατί αν $p = 2, 4, 6, 8, 10 \pmod{12}$ ο p θα ήταν άρτιος, ενώ αν $p = 3, 9 \pmod{12}$ δεν θα ήταν πρώτος
π.χ. αν $p = 3 \pmod{12} \Rightarrow p = 12k + 3 = 3(4k + 1)$

$$p \equiv 1 \pmod{12} \Leftrightarrow \left\{ \begin{array}{l} p \equiv 1 \pmod{3} \Rightarrow (p|3) = +1 \\ p \equiv 1 \pmod{4} \Rightarrow \frac{p-1}{2} \text{ άρτιος} \end{array} \right\} \Rightarrow \\ \Rightarrow (3|p) = 1.$$

$$\begin{aligned}
 p \equiv 5 \pmod{12} &\Leftrightarrow \begin{cases} p \equiv 2 \pmod{3} \Rightarrow (p|3) = -1 \\ p \equiv 1 \pmod{4} \Rightarrow \frac{p-1}{2} \text{ άρτιο} \end{cases} \Rightarrow (3|p) = -1 \\
 p \equiv 7 \pmod{12} &\Leftrightarrow \begin{cases} p \equiv 1 \pmod{3} \Rightarrow (p|3) = 1 \\ p \equiv 3 \pmod{4} \Rightarrow \frac{p-1}{2} \text{ περιττός} \end{cases} \Rightarrow (3|p) = -1 \\
 p \equiv 11 \pmod{12} &\Leftrightarrow \begin{cases} p \equiv 2 \pmod{3} \Rightarrow (p|3) = -1 \\ p \equiv 3 \pmod{4} \Rightarrow \frac{p-1}{2} \text{ περιττός} \end{cases} \Rightarrow (3|p) = 1
 \end{aligned}$$

$$\text{Άρα } (3|p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{12} \\ -1, & p \equiv \pm 5 \pmod{12} \end{cases}$$

Παράδειγμα:

Είναι ο 1729 πρώτος?

Λύση:

Εδώχω για παράδειγμα, αν το κριτήριο του Euler και ο νόμος τετραγωνικής αντιστροφής, δίνουν το ίδιο αποτέλεσμα.

$$\begin{aligned}
 &\sim (11|1729) = (1729|11) = (2|11) = -1 \\
 &\quad \text{4n+3} \quad \text{4k+1} \quad \frac{1729-1}{2} \\
 &\rightarrow (11|1729) = 11^{\frac{1729-1}{2}} \pmod{1729} = (\dots) = +1 \\
 &\quad \downarrow \\
 &\quad \text{Euler}
 \end{aligned}$$

Άρα όχι πρώτος (7·13·17)

Συνοψίζοντας:

Για p, q περιττοι πρώτοι:

- $(1|p) = 1$
- $(-1|p) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv -1 \pmod{4} \end{cases}$
- $(2|p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$
- $(3|p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{12} \\ -1, & p \equiv \pm 5 \pmod{12} \end{cases}$
- $(n|p) = (m|p), n \equiv m \pmod{p}$
- $(nm|p) = (n|p)(m|p) \quad \forall n, m$
- $(nm^2|p) = (n|p)$

$$\bullet (p|q) = (q|p) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Αν $a = \pm 2^{t_1} \cdot 3^{t_2} \cdot \dots \cdot p_s^{t_s}$, p_i πρώτοι αριθμοί τότε

$$(a|p) = (\pm 1|p) (2|p)^{t_1} \cdot \dots \cdot (p_s|p)^{t_s}$$

Παράδειγμα:

Έχει λύση η πολυωνυμική ισοδυναμία
 $x^2 - 299 \equiv 0 \pmod{359}$, όπου 359 πρώτος.

Λύση:

$$\begin{aligned} (299|359) &= (13|359) (23|359) && (2^2|13) = 1 \\ (13|359) &= (359|13) = (8|13) = (2^3|13) = (2|13) = -1 && \xrightarrow{(2^2|13)=1} \\ &&& \text{1 mod 4} \qquad \qquad \qquad \text{5 mod 8} \\ (23|359) &= - (359|23) = - (14|23) = - (2|23) (7|23) = && \\ &&& \text{3 mod 4} \quad \text{3 mod 4} \\ &= - (+1) (-1) (23|7) = (2|7) = +1 \end{aligned}$$

Άρα $(299|359) = (-1)(+1) = -1$.

Άρα $299 \nmid 359$, συνεπώς η $x^2 - 299 \equiv 0 \pmod{359}$
 δεν έχει λύση.

08/05/2025

~> Πώς συνδέουμε για $\text{TY}_{\text{mod } P}$, P σύνθετος?

Ορισμός:

Αν P θετικός περιττός ακέραιος με πρωτογενή ανάλυση $\prod_{i=1}^r p_i^{a_i}$, τότε το σύμβολο του Jacobi ορίζεται για κάθε ακέραιο n ως:

$(n|P) := \prod_{i=1}^r (n|p_i)^{a_i}$ όπου $(n|p_i)$ το σύμβολο Legendre
Ορίζουμε $(n|1) = 1$.

• Οι δυνατές τιμές του $(n|P)$ είναι $\pm 1, 0$, όπου $(n|P) = 0$ αν $(n, P) > 1$ (δηλαδή κάποιος στο γινόμενο εμφανίζεται το $(0|p)$).

~> Είναι σαν να επεκτείνουμε τον Legendre σε μη πρώτους, χρησιμοποιώντας την ήδη πολλαπλασιαστικότητα του.

• Αν η $x^2 \equiv n \pmod{P}$ έχει λύση, τότε $x^2 \equiv n \pmod{p_i}$ $\forall i$ (από αρχικές ιδιότητες των mod, αφού $\forall p_i | P$).
Άρα, $(n|p_i) = 1 \ \forall p_i$ πρώτο στην παραγοντοποίηση του P , $\Rightarrow (n|P) = 1$.

* Προσοχή!

Το αντίστροφο δεν ισχύει. Αν $(n|P) = 1$, μπορεί να εμφανίζεται άρτος αριθμός $(n|p_i) = -1$ στο $(n|P) = \prod_{i=1}^r (n|p_i)^{a_i}$. Άρα η $\text{TY}_{\text{mod } p_i}$ δε κάποια p_i και έτσι όχι αναγκαστικά η $\text{TY}_{\text{mod } P}$. (αφού δε μπορεί να χρησιμοποιήσω το $x^2 \equiv n \pmod{p_i} \ \forall p_i$, $(p_i, p_j) = 1 \Rightarrow x^2 \equiv n \pmod{P}$).

Παράδειγμα:

$$(1|15) = (1|3)(1|5) = 1 \cdot 1 = 1 \quad \text{όπως } 1 \pmod{15}$$

Αλλά $(2|15) = (2|3)(2|5) = (-1)(-1) = 1$ αλλά

$$x^2 \equiv 2 \pmod{15} \text{ δεν έχει λύση} \rightarrow 2 \not\equiv \pmod{15}$$

Πρόταση:

Αν P, Q θετικοί περιττοί ακέραιοι, τότε:

$$\bullet (m|P)(n|P) = (m \cdot n|P)$$

$$\bullet (n|P)(n|Q) = (n|P \cdot Q)$$

$$\bullet (m|P) = (n|P) \Rightarrow m \equiv n \pmod{P}$$

$$\bullet (a^2 n|P) = (n|P) \text{ , αν } (a, P) = 1.$$

$$\bullet (-1|P) \text{ και } (2|P) \text{ είναι όπως του Legendre.}$$

Απόδειξη: $(-1|P) = (-1)^{\frac{P-1}{2}}$

Έστω $P = p_1 \cdot \dots \cdot p_m$ όχι αναγκαστικά διαδοχικοί μεταξύ τους:

$$(-1|P) = \prod_{i=1}^m (-1|p_i) = \prod_{i=1}^m (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^m \frac{p_i-1}{2}} \quad \star$$

$$\begin{aligned} \text{Παρατηρώ ότι } P &= \prod_{i=1}^m p_i = \prod_{i=1}^m (1 + (p_i - 1)) = \\ &= 1 + (p_1 - 1) + \dots + (p_m - 1) + (p_1 - 1)(p_2 - 1) + \dots + (p_1 - 1)(p_m - 1) + \\ &+ \dots + (p_{m-1} - 1)(p_m - 1) = 1 + \sum_{i=1}^m (p_i - 1) + \sum_{i < j} (p_i - 1)(p_j - 1) \end{aligned}$$

Θμω, κάθε $(p_i - 1)$ είναι άρτιος, άρα $(p_i - 1)(p_j - 1)$ πολλαπλάσιο του 4. Άρα:

$$P \equiv 1 + \sum_{i=1}^m (p_i - 1) \pmod{4} \Rightarrow P - 1 \equiv \sum_{i=1}^m (p_i - 1) \pmod{4} \Rightarrow$$

$$\frac{P-1}{2} \equiv \sum_{i=1}^m \frac{p_i-1}{2} \pmod{2}$$

Άρα, στο $\star$ παίρνω ότι $(-1|P) = (-1)^{\sum \frac{p_i-1}{2}} = (-1)^{\frac{P-1}{2}}$, αφού σημασία έχει μόνο αν ο εκθέτης είναι άρτιος ή περιττός, δηλαδή η τιμή του mod 2.

• Θεώρημα: (Νόμος Τετραγωνικής Αντιστροφής Jacobi)
 Αν P, Q Θετικοί περιττοί ακέραιοι με $(P, Q)=1$,
 τότε :
$$(P|Q)(Q|P) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

• Απόδειξη:

Έστω $P = p_1 \cdots p_m$, $Q = q_1 \cdots q_n$ με

$$(P|Q)(Q|P) = \prod_{i=1}^m \prod_{j=1}^n (p_i|q_j)(q_j|p_i) = (-1)^r, \quad r = ?$$

Με τετραγωνική αντιστροφή :

$$r = \sum_{i=1}^m \sum_{j=1}^n \frac{1}{2} (p_i-1)(q_j-1) = \sum_{i=1}^m \frac{1}{2} (p_i-1) \sum_{j=1}^n \frac{1}{2} (q_j-1)$$

Άρα, όπως πριν $r \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2} \quad \square$.

• Παράδειγμα:

Υπολογίστε το $(335|2999)$

• Λύση:

Με ενδιαφέρει αν και οι δύο είναι περιττοί και
 πρώτοι μεταξύ τους. Ουτως $(335|2999)=1$.

Άρα

$$\begin{aligned} (335|2999) &= (-1)(2999|335) = -(319|335) = -(-16|335) \\ &= -(-1|335)(16|335) = (-1)(-1) = +1 \end{aligned}$$

• Παράδειγμα:

Είναι ο $888 \pmod{1999}$, όπου 1999 πρώτος ?

• Λύση:

$$\begin{aligned} (888|1999) &= (2^3 \cdot 111|1999) = (2^3|1999)(111|1999) = \\ &= (2|1999)(111|1999) = (-1)(111|1999) \stackrel{(2|1999)}{=} \\ &= -1 \pmod{8} \end{aligned}$$

$$\ast \alpha' \text{ τρόπος: } = (3|1999)(37|1999) = \dots$$

$$\text{Jacobi } (111|1999) = 1.$$

$$\beta' \text{ τρόπος: } = (111|1999) = (-1)(1999|111) = -(11|11) = -1$$

Άρα $888 \pmod{1999}$.

ΠΡΩΤΟΙ ΣΕ ΑΡΙΘΜΗΤΙΚΕΣ ΠΡΟΟΔΟΥΣ :

Θυμόμαστε ότι μια αριθμητική πρόοδος με πρώτο όρο h και (κοινή) διαφορά k αποτελείται από όλους τους αριθμούς της μορφής $kn+h$ με $n=0,1,\dots$. Εναλλακτικά, $a_{n+1} = a_n + k$ (αναδρομικά) που δίνει $a_{n+1} = kn + a_0$. Μας ενδιαφέρει πόσοι πρώτοι αριθμοί εμφανίζονται σε μια αριθμητική πρόοδος.

→ Αν $d|h$ και $d|k$, τότε d διαφέρει κάθε όρο της πρόοδου, οπότε για $d > 1$, έχουμε το πρόβλημα να είναι πρώτος αριθμός της πρόοδου - του h , αν είναι πρώτος.

→ Η πρόοδος $kn+h$ έχει άπειρους πρώτους όρους $\Rightarrow (h,k)=1$

Ο Dirichlet έδειξε το αντίστροφο (1837):

$(h,k)=1 \Rightarrow$ η αριθμητική πρόοδος $kn+h$ έχει άπειρους πρώτους όρους.

Θεώρημα :

Υπάρχουν άπειροι πρώτοι της μορφής $4n-1$.

Απόδειξη :

- Έστω ότι οι πρώτοι της μορφής $4n-1$ είναι πεπερασμένοι στο πλήθος και έστω p ο μεγαλύτερος

από αυτούς. Θεωρούμε τον φυσικό αριθμό $N = (2^2 \cdot 3 \cdot 5 \cdot \dots \cdot p) - 1$, που στο γινόμενο έχει όλους τους περιττούς πρώτους, μέχρι του p .

Αφού ο N είναι της μορφής $4n-1$, δηλαδή όρος της προόδου, δεν μπορεί να είναι πρώτος, αφού $N > p$. Επίσης, κανένας πρώτος αριθμός $\leq p$ δεν μπορεί να διαιρεί το N (γιατί αλλιώς θα διαιρούσε το 1).

Άρα, στην ανάλυση πρώτων παραγόντων του N , έχω όλους τους πρώτους αναγκαστικά μεγαλύτερους του p . Αφού κάθε τέτοιος πρώτος παράγοντας είναι περιττός, θα είναι είτε $1 \pmod{4}$ είτε $(-1) \pmod{4}$. Γίνεται όλοι οι πρώτοι παράγοντες του N να είναι στην κλάση $1 \pmod{4}$, δηλαδή της μορφής $4n+1$? Όχι, γιατί $(4n+1)(4k+1) = 4(\dots) + 1$, άτοπο.

Άρα, έστω και ένας πρώτος παράγοντας, θα είναι της μορφής $4n-1$. Αλλά, είναι και αυτός όρος της προόδου και μεγαλύτερος του p . Άρα άτοπο.

13/05/2025

• Θεώρημα:

Υπάρχουν άπειροι πρώτοι της μορφής $4n+1$.

• Απόδειξη:

Έστω τυχαίος ακέραιος $N > 1$. Ο.δ.ο. $\exists p > N$ με $p \equiv 1 \pmod{4}$, συνεπώς υπάρχουν άπειροι τέτοιοι πρώτοι. Έστω $m = (N!)^2 + 1$, άρα m περιττός και $m > 1$. Παίρνοντας την πρωταγενή ανάλυση του m , θεωρή τον ελάχιστο πρώτο παράγοντα p .

$\rightarrow$ Αφού $2, 3, 4, \dots, N \mid N!$, δεν μπορούν να διαιρούν τον m , γιατί τότε θα διαιρούσαν το 1. Άρα $p > N$.

$\rightarrow$ Ισχύει ότι $(N!)^2 \equiv -1 \pmod{m}$ και αφού $p \mid m$
 $(N!)^2 \equiv -1 \pmod{p} \Rightarrow ((N!)^{\frac{p-1}{2}})^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \Rightarrow$
 $\Rightarrow (N! \mid p)^2 \equiv (-1 \mid p) \Leftrightarrow +1 \equiv (-1 \mid p) \Rightarrow p \equiv 1 \pmod{4}$.

Άρα $p = 4k+1$, $k \in \mathbb{Z}$ $\square$

• Παρατήρηση:

Η προηγούμενη μέθοδος για $4n-1$ (μέθοδος "Ευκλείδης"), δεν μπορεί να χρησιμοποιηθεί για $4n+1$. Όντως, έστω ότι όλοι οι πρώτοι της μορφής $4n+1$ ήταν πεπερασμένοι το πλήθος, p ο μεγαλύτερος από αυτούς και έστω $N = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1$. Σε αντίθεση με πριν, εδώ θα μπορούσαν όλοι οι πρώτοι παράγοντες του N , να είναι της μορφής $4n-1$, γιατί άρτιο πλήθος αυτών δίνει όντως $4n+1$. Οπότε, δεν μπορώ να καταλήξω σε άτοπο.

Εναλλακτικά, θεωρούμε τον $M = 4(p_1 \cdot \dots \cdot p_n)^2 + 1$, όπου $p_1, \dots, p_n$ είναι οι πεπερασμένοι το πλήθος πρώτοι της μορφής $4n+1$. Ο M είναι περιττός και δεν έχει πρώτους διαιρέτες της μορφής $4k+1$.

Άρα, έστω και ένας είναι της μορφής $4n+3=9$.
Τότε, $4(p_1 \dots p_n)^2 \equiv (-1) \pmod{4}$ και αντίστοιχα
με την $\tau\gamma$, άτοπο.

$\leadsto$ Τέτοιες αλυσές μέθοδοι μπορούν να βρεθούν
για κάποιες αριθμητικές προόδους (π.χ. $5n-1, 8n-1$)
αλλά όχι για όλες, και σίγουρα όχι για $kn+h$.

- Αναλυτικές μέθοδοι που ενέπνευσε τον Dirichlet, για την απόδειξη του γενικού Θεωρήματος για πρώτους σε αριθμητικές αλυσ.

• Θεώρημα: (Euler 1737)
Η σειρά $\sum_{n=1}^{\infty} \frac{1}{p_n} = \sum_{p \text{ πρώτος}} \frac{1}{p}$ αποκλίνει.

$\leadsto$ Υπενθύμιση:

Έστω μια ακολουθία αριθμών $(a_k)_{k \in \mathbb{N}}$. Έστω
η σειρά $\sum_{k=1}^{\infty} a_k$, με "μερικά αθροίσματα" $S_n = \sum_{r=1}^n a_r$.

Η σειρά συγχλίνει (αλυσά) και γράφω $S = \sum_{k=1}^{\infty} a_k$
όταν $S_n \xrightarrow{n \rightarrow \infty} S \iff \forall \varepsilon, \exists N(\varepsilon) \text{ τ.λ. } \forall n > m > N(\varepsilon),$
 $|S_n - S_m| = \left| \sum_{k=m+1}^n a_k \right| < \varepsilon.$

$\hookrightarrow$ Διασθετικά, η σειρά συγχλίνει αν η $(S_1, S_2, \dots)$
των μερικών αθροισμάτων της, πλησιάζει κάποιο
όριο, δηλαδή προσθέτοντας ένα a_k μετά το άλλο
παίρνουμε μερικά αθροίσματα που τείνουν σε έναν
αριθμό. Δηλαδή, το όριο S είναι τέτοιο που
για οποιονδήποτε μικρό θετικό ε , μπορεί να βρω
έναν N τ.λ. $|S_n - S| < \varepsilon.$

• Παραδείγματα:

$$\rightarrow \sum_{n=1}^{\infty} \frac{1}{n} = +\infty, \text{ αφού } 1 + \frac{1}{2} + \frac{1}{3} + \dots \rightarrow +\infty.$$

$$\rightarrow \sum_{n=1}^{\infty} \frac{1}{n^p} \text{ συγκλίνει} \Leftrightarrow p > 1 \quad (p\text{-αρμονική})$$

$$\text{π.χ.} \quad \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \dots = \frac{\pi^2}{6}$$

$$\rightarrow \sum_{n=0}^{\infty} 2^n \text{ συγκλίνει} \Leftrightarrow |2| < 1 \quad (\text{γεωμετρική})$$

$$\text{π.χ.} \quad \sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1 - \frac{1}{2}} = 2$$

$$\rightarrow \text{Αν } \sum_{n=1}^{\infty} a_n = S, \text{ τότε } \lim_{n \rightarrow \infty} a_n = 0 \quad (\text{όχι το αντίστροφο})$$

$$\cdot \text{Η σειρά συγκλίνει απόλυτα όταν } \sum_{n=0}^{+\infty} |a_n| = S.$$

• Κριτήριο σύγκρισης:

Αν $|b_n| \leq a_n$ και $\sum_{n=1}^{\infty} a_n$ συγκλίνει, τότε και $\sum_{n=1}^{\infty} b_n$ συγκλίνει.

Επίσης, αν $\sum_{n=1}^{\infty} |b_n|$ αποκλίνει, τότε και $\sum_{n=1}^{\infty} a_n$ αποκλίνει.

• Απόδειξη: (Clarkson)

Έστω ότι η $\sum_{n=1}^{\infty} \frac{1}{p_n}$ συγκλίνει. Δηλαδή, ότι υπάρχει κάποιος k τέω. $\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$. ☆

Έστω το γινόμενο των πρώτων ως τον k , $Q = p_1 \cdot p_2 \cdot \dots \cdot p_k$. Φακνουμε την αριθμητική ακολουθία $nQ+1$. Όπως πριν, $p_1, \dots, p_k \nmid nQ+1$. Άρα οι πρώτοι παράγοντες στην ανάλυση των $nQ+1$ είναι

όλοι μεγαλύτεροι του P_k , άρα εκφράζονται μεζαζι των πρώτων αριθμών $P_{k+1}, P_{k+2}, \dots$. Άρα, για κάθε $k \geq 1$, έχουμε $\sum_{n=k+1}^{\infty} \frac{1}{nQ+1} \leq \sum_{m=1}^{\infty} \left(\sum_{n=k+1}^{\infty} \frac{1}{P_m} \right)^2$, αφού

το δεξί άθροισμα περιλαμβάνει όλους τους όρους του αριστερά.

Από: $\sum_{k=1}^{\infty} \left(\sum_{n=k+1}^{\infty} \frac{1}{P_n} \right)^2 \leq \sum_{k=1}^{\infty} \left(\frac{1}{2} \right)^k$ από την $\star$,

η οποία γεωμετρική σειρά συγκλίνει. Συνεπώς, αφού τα μερικά της άθροισματα φράσσονται, η $\sum_{n=1}^{\infty} \frac{1}{nQ+1}$ συγκλίνει. Όμως, $Q > 1 \Rightarrow \frac{1}{nQ+1} > \frac{1}{nQ+Q} = \frac{1}{Q} \cdot \frac{1}{n+1}$

που αποκλίνει αφού $\sum_{n=1}^{\infty} \frac{1}{n+1} = \infty$

Από κριτήριο σύγκρισης, η $\sum_{n=1}^{\infty} \frac{1}{nQ+1}$ συγκλίνει.

Άρα, άρα η $\sum_{\text{πρώτοι } p} \frac{1}{p}$ αποκλίνει.

Παρατήρηση:

Αφού $\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$ και $\sum_{\text{πρώτοι } p} \frac{1}{p} = +\infty$, αλλά $\sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$

Συμπεραίνουμε ότι οι πρώτοι αριθμοί είναι "πυκνοί" ανάμεσα στους θετικούς ακέραιους από ότι το τετράγωνο.

~ Συνδιαστιά με αυτή τις ιδέες, ο Euler απέδειξε πως $\prod_{\text{πρώτοι } p} \frac{1}{1 - \frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}$, οπότε αφού η αριστερή

αποκλίνει, συνεπάγεται ότι το γινόμενο αριστερά έχει άκρως άπειρο.

(Ιδιότητα): Ο Dirichlet έδειξε πως για $P = nk + h$

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log(p)}{p} = \frac{1}{\phi(k)} \log(x) + O(1) \text{ και αν } x \rightarrow \infty, \log(x) \rightarrow \infty$$

από το
↑
από το

Σειρές Dirichlet - Συνάρτηση Ζήτα του Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \mu\epsilon \quad s \in \mathbb{C}.$$

1737 → Ο Euler αποδεικνύοντας πως $\sum_p \frac{1}{p}$ αποκλίνει, συμπεραίνει επίσης πως και η $\zeta(s)$, $s \in \mathbb{R}$ είναι στο άπειρο όταν $s \rightarrow 1$.

1837 → Ο Dirichlet ανέπτυξε το Θεώρημα πρώτων στις αριθμητικές ακολουθίες μελετώντας τη σειρά $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, όπου $\chi(n)$ είναι ένας "Χαρακτήρας Dirichlet".

Ορισμοί:

Ονομάζουμε σειρά Dirichlet μια σειρά της μορφής $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, $s \in \mathbb{C}$, όπου $f(n)$ αριθμητική συνάρ-

τηση. Ονομάζουμε τους $f(n)$ συντελεστές της σειράς Dirichlet.

15/5/2025

$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, $s \in \mathbb{C}$ Σειρά Dirichlet $f(n)$
αριθμητική συνάρτηση

(Riemann) Συμβολίζουμε $s = \sigma + it \in \mathbb{C}$, με $\sigma, t \in \mathbb{R}$

$$\begin{aligned} \text{Έχουμε } n^s &= e^{\log(n^s)} = e^{s \cdot \log(n)} = e^{(\sigma + it) \log(n)} = e^{\sigma \log(n)} \cdot e^{it \log(n)} = \\ &= e^{\log(n)^\sigma} \cdot e^{it \log(n)} = n^\sigma \cdot e^{it \log(n)} \end{aligned}$$

$$\text{Από } |e^{i\theta}| = 1, \theta \in \mathbb{R}: |n^s| = n^\sigma = n^{\operatorname{Re}(s)}$$

Ονομάζουμε το σύνολο των σημείων $s = \sigma + it$, $\sigma > \alpha$
 $\alpha \in \mathbb{R}$, ένα ημιεπίπεδο.

Σκοπός: Ν.δ.ο. για κάθε σειρά Dirichlet υπάρχει
ημιεπίπεδο $\sigma > \sigma_c$ στο οποίο η σειρά
συγκλίνει και τα όσα και ένα ημιεπίπεδο
 $\sigma > \sigma_a$, στο οποίο η σειρά συγκλίνει
απόλυτα.

* Παρατηρούμε ότι $\sigma \geq \sigma_a$, $|n^s| = n^\sigma \geq n^a$, οπότε

$$\left| \frac{f(n)}{n^s} \right| = \frac{|f(n)|}{n^\sigma} \leq \frac{|f(n)|}{n^a}$$

Άρα, αν μια σειρά Dirichlet $\sum \frac{f(n)}{n^s}$ συγκλίνει
απόλυτα για $s = a + ib$, τότε από κριτήριο σύγκρισης,
θα συγκλίνει, επίσης απόλυτα, για κάθε s , $\sigma > a$.

Θεώρημα: (πρτ. απόλυτης σύγκλισης)

Έστω ότι η $\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right|$ δε συγκλίνει, ούτε απο-
κλίνει, για όλα τα $s \in \mathbb{C}$. Τότε, υπάρχει $\sigma_a \in \mathbb{R}$ τ.ω.
η $\sum \frac{f(n)}{n^s}$ συγκλίνει απόλυτα για $\sigma > \sigma_a$, ενώ δεν
συγκλίνει για $\sigma < \sigma_a$.

Απόδειξη:

Έστω ότι η $\sum \left| \frac{f(n)}{n^s} \right|$ δε συγκλίνει, ούτε αποκλίνει, για όλα τα s . Θεωρώ το $D = \{s \in \mathbb{R} \mid \sum \left| \frac{f(n)}{n^s} \right| = +\infty\}$ των πραγματικών για τους οποίους η σειρά αποκλίνει.

→ Το D είναι μη κενό, άρα υπάρχουν s για τα οποία η σειρά δεν συγκλίνει

→ Το D είναι άνω φραγμένο, αφού υπάρχουν s για τα οποία δε συγκλίνει.

Δηλαδή, έστω $s \in \mathbb{C}$ για το οποίο η $\sum \left| \frac{f(n)}{n^s} \right|$ συγκλίνει, άρα $s \notin D$. Αφού πραγματοποιήθηκε παρατήρηση, η $\sum \left| \frac{f(n)}{n^s} \right|$ συγκλίνει και για όλα τα s με μεγαλύτερο πραγματικό μέρος. Άρα, δεν υπάρχει s' με μεγαλύτερο πραγματικό μέρος που να ανήκει στο D , άρα $\text{Re}(s)$ είναι ένα άνω φράγμα του D .

Από Λήμμα Πληρότητας, το D έχει supremum, έστω σ_a .

→ Αν $\sigma > \sigma_a$, τότε $\sigma \notin D$, αφού το σ_a άνω φράγμα του D .

→ Αν $\sigma < \sigma_a$, τότε $\sigma \in D$ γιατί αλλιώς σ_a ήταν και αυτό άνω φράγμα - άτοπο, αφού σ_a το ελάχιστο άνω φράγμα.

Παράδειγμα:

Για τη συνάρτηση ζήτα του Riemann έχουμε ότι $\sum_{n=1}^{\infty} \frac{1}{n^s}$ συγκλίνει απόλυτα για $\sigma > 1$. ($\left| \frac{1}{n^s} \right| = \frac{1}{n^\sigma}$). Άρα για $s=1$, η σειρά αποκλίνει, οπότε $\sigma_a = 1$.

* Ορίζεται μια συνάρτηση από κάθε σειρά Dirichlet $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ στο ημιεπίπεδο απόλυτης σύγκλισης, δηλαδή $s \in \mathbb{C}$ με $\text{Re}(s) > \sigma_a$.

Θεώρημα: (του μονοσήμαντου)

Έστω ότι οι σειρές Dirichlet $\sum \frac{f(n)}{n^s}$ κ' $\sum \frac{g(n)}{n^s}$ συγκλίνουν και οι δύο απόλυτα για $\sigma > \sigma_a$. Αν $F(s) = G(s)$ για κάθε s που είναι όρος μιας άπειρης ακολουθίας (s_k) με $\lim_{k \rightarrow \infty} \sigma_k = +\infty$, τότε $f(n) = g(n)$, $\forall n \in \mathbb{N}$.

Απόδειξη:

Θέτουμε μια $h(n) = f(n) - g(n)$ και $H(s) = F(s) - G(s)$. Για να δείξω ότι $h(n) = 0$ $\forall n$, έστω ότι για κάποια φυσικούς δεν ισχύει. Θέτω N τον μικρότερο φυσικό για τον οποίο έχουμε $h(N) \neq 0$. Μετασχηματίζω την $H(s)$ συνάρτηση του N ως $H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} = \sum_{n \leq N} \frac{h(n)}{n^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}$.
 $h(n)=0$

Λύνοντας ως προς $h(N)$, έχουμε:

$$h(N) = N^s \cdot H(s) - N^s \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}$$

Συγκεκριμένα, για $s = s_k$ οποιονδήποτε όρο της ακολουθίας της υπόθεσης, έχουμε $H(s_k) = F(s_k) - G(s_k) = 0$.

$$\text{Άρα, } h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} \frac{h(n)}{n^{s_k}} *$$

Λήμμα: Για $N \geq 1$ και $\sigma \geq c > \sigma_a$, έχουμε:

$$\left| \sum_{n=N}^{\infty} \frac{f(n)}{n^s} \right| \leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} \frac{|f(n)|}{n^c}$$

Επιδειχνουμε ένα k τ.ω. $\sigma_k > c > \sigma_a$, και τότε έχω:

$$* : |h(N)| = \left| -N^{s_k} \sum_{n=N+1}^{\infty} \frac{h(n)}{n^{s_k}} \right| \leq N^{s_k} (N+1)^{-(\sigma_k-c)} \sum_{n=N+1}^{\infty} \frac{|h(n)|}{n^c} = \left(\frac{N}{N+1} \right)^{\sigma_k} (N+1)^c \cdot \sum_{n=N+1}^{\infty} \frac{|h(n)|}{n^c} \rightarrow \text{σταθ. ως προς } k$$

Όταν $k \rightarrow \infty$, $\delta_k \rightarrow \infty$ και αφού $N+1 > N$,
 $\left(\frac{N}{N+1}\right)^{\delta_k} \rightarrow 0$, άρα $h(N)=0$ άτομο

• Θεώρημα:

Έστω $F(s) = \sum \frac{f(n)}{n^s}$ για $\sigma > a$ κ' $G(s) = \sum \frac{g(n)}{n^s}$ για $\sigma > b$.
 Στο ημιεπίπεδο που και οι δύο συγκλίνουν απόλυτα,
 έχουμε:

$$F(s) \cdot G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s}$$

$$\left(\text{Συνέλιξη Dirichlet: } (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b) \right)$$

• Απόδειξη:

Για κάθε $s \in \mathbb{C}$ στο οποίο και οι δύο σειρές
 συγκλίνουν απόλυτα έχουμε:

$$F(s) \cdot G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \cdot \sum_{m=1}^{\infty} \frac{g(m)}{m^s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n) \cdot g(m)}{(n \cdot m)^s}$$

Λόγω της απόλυτης σύγκλισης, μπορούμε να πολλαπλασιάσουμε
 και αναδιατάξουμε με οποιονδήποτε τρόπο τους όρους
 χωρίς να μεταβληθεί το αποτέλεσμα.

Ομαδοποιούμε τους όρους για τους οποίους το $m \cdot n$
 είναι σταθερό, $m \cdot n = k$. Φυσικά, $k=1, 2, 3, \dots$ είναι οι
 δυνατές τιμές. Άρα:

$$F(s) \cdot G(s) = \sum_{k=1}^{\infty} \left(\sum_{m \cdot n = k} f(n) \cdot g(m) \right) \cdot k^{-s} = \sum_{k=1}^{\infty} \frac{(f * g)(k)}{k^s} \quad \square$$

• Παράδειγμα:

Ισχύει ότι $\zeta(s) = \sum \frac{1}{n^s}$ και $\sum \frac{\mu(n)}{n^s}$ συγκλίνουν
 απόλυτα για $\sigma > 1$. Παιρνοντας $f(n)=1$, $g(n)=\mu(n)$
 στο παραπάνω Θεώρημα, ισχύει πως:

$$(f * g)(n) = I(n) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$$

Άρα έχουμε:

$$\underbrace{f(s)}_{\zeta(s)} \cdot \underbrace{g(s)}_{\sum \frac{\mu(n)}{n^s}} = \sum_{n=1}^{\infty} \frac{I(n)}{n^s} = 1, \quad \sigma > 1$$

Ειδικότερα, παίρνουμε πως $\zeta(s) \neq 0$, $\sigma > 1$ και
 ότι $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$!

Αυτό το παράδειγμα, γενικεύεται σε οποιαδήποτε ζεύγη αντιστρόφων αριθμητικών συναρτήσεων.

• Παράδειγμα:

Έστω $f(n)=1$ και $g(n)=\varphi(n)$ η συνάρτηση του Euler.
 Επειδή $\varphi(n) \leq n \quad \forall n \Rightarrow \sum \frac{\varphi(n)}{n^s}$ συγκλίνει απόλυτα
 για $\sigma > 2$. Επίσης, παρατηρώ ότι $(f * \varphi)(n) = \sum_{d|n} \varphi(d) = n$
 Άρα το Θεώρημα δίνει:

$$\underbrace{f(s)}_{\zeta(s)} \cdot \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} = \zeta(s-1), \quad \forall s \in \mathbb{C} \quad \sigma > 2.$$

• Παρατήρηση:

Ισχύει και το "αντίστροφο" του Θεωρήματος, δηλαδή αν
 $F(s) \cdot G(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \quad \forall s$ όρο μιας ακολουθίας $(a(n))$

με $\lim_{k \rightarrow \infty} a_k = \tau \neq 0$ τότε $a = f * g$.

Αυτό προκύπτει από Θεώρημα Μανασιγιάτου.

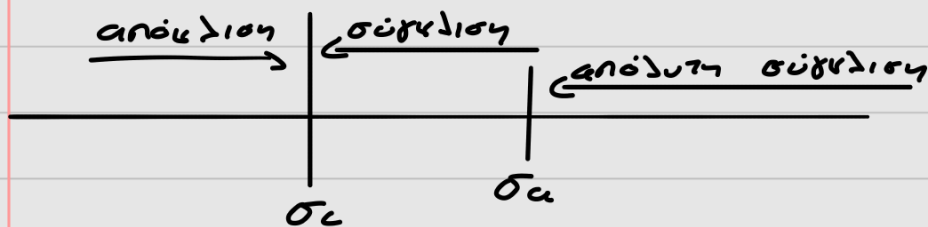
21/05/2025

Θεώρημα:

Για κάθε σειρά Dirichlet, υπάρχει $\sigma_c \in \mathbb{R}$ τ.λ. η σειρά να συγκλίνει (απόλυτα) $\forall \sigma > \sigma_c$ και να αποκλίνει $\forall \sigma < \sigma_c$. Επιπλέον, το $\sigma_c \leq \sigma_a \leq \sigma_c + 1$

Παρατήρηση:

Αφού η απόλυτη σύγκλιση συνεπάγεται την απλή, σίγουρα ισχύει πάντα πως $\sigma_c \leq \sigma_a$. Αν $\sigma_a \neq \sigma_c$, τότε συγκλίνει (όχι απόλυτα) για άπειρο τμήμα σ μήκους 1.



Παράδειγμα:

Μιας και η $\zeta(s) = \sum \frac{1}{n^s}$ συγκλίνει απόλυτα για $\sigma > 1$ και αποκλίνει για $\sigma = 1$, για αυτήν την περίπτωση ισχύει $\sigma_c = \sigma_a = 1$.

Από την αλλαγή, η σειρά $\sum \frac{(-1)^n}{n^s}$ συγκλίνει (...) για $\sigma > 0$, όμως η σύγκλιση είναι απόλυτη μόνο για $\sigma > 1$ (αφού γίνεται $\zeta(s)$). Άρα, εδώ έχουμε $\sigma_c = 0$, $\sigma_a = 1$.

Σeries Bell Αριθμητικών Συναρτήσεων

Ορισμός:

Αν f αριθμητική συνάρτηση και p πρώτος, συμβολίζουμε με $f_p(x) = \sum_{n=0}^{\infty} f(p^n) \cdot x^n$ την ζυγική δυναμοσειρά και την ονομάζουμε σειρά Bell της f modulo p .

Θεώρημα: (μοναδικότητα)

Έστω ότι f, g πολλαίς αριθμητικές συναρτήσεις. Τότε $f = g \Leftrightarrow f_p(x) = g_p(x) \quad \forall p$ πρώτο

Απόδειξη:

" $\Rightarrow$ " Προφανώς, αν $f(n) = g(n) \quad \forall n \in \mathbb{N}$, τότε $f(p^n) = g(p^n) \quad \forall p$ πρώτο, $n \geq 0$, άρα $f_p(x) = g_p(x)$.

" $\Leftarrow$ " Αν $f_p(x) = g_p(x) \quad \forall$ πρώτο p , τότε αναγκαστικά $f(p^n) = g(p^n)$ για τους συντελεστές της δυναμοσειράς. Αφού οι f, g είναι πολλαπλασιαστικές και έχουν τις ίδιες τιμές για όλες τις δυνάμεις πρώτων, από Θεμελιώδες Θεώρημα Αριθμητικής, $f(n) = f(\prod_{p_i \text{ πρώτος}} p_i^{a_i}) = \prod f(p_i^{a_i}) = \prod g(p_i^{a_i}) = g(n) \Rightarrow f = g \quad \square$

Παραδείγματα:

$\rightarrow$ (Möbius): Αφού $\mu(1) = 1, \mu(p) = -1, \mu(p^n) = 0 \quad \forall n \geq 2$. Έχουμε $\mu_p(x) = \sum_{n=0}^{\infty} \mu(p^n) x^n = \mu(1) \cdot 1 + (-1)x^1 + 0 = 1 - x$

$\rightarrow$ (Euler): Αφού $\varphi(1) = 1, \varphi(p^n) = p^n - p^{n-1} \quad \forall n \geq 1$. Έχουμε $\varphi_p(x) = \sum_{n=0}^{\infty} \varphi(p^n) x^n = 1 + \sum_{n=1}^{\infty} \varphi(p^n) x^n = 1 + (p-1)x + (p^2-p)x^2 + (p^3-p^2)x^3 + \dots = 1 + \underline{px} - \underline{x} + \underline{p^2x^2} - \underline{px^2} + \underline{p^3x^3} - \underline{p^2x^3} + \dots = \sum_{n=0}^{\infty} p^n x^n - x \sum_{n=0}^{\infty} p^n x^n = (1-x) \sum_{n=0}^{\infty} p^n x^n = \frac{1-x}{1-px}$

ΓΙΝΟΜΕΝΑ EULER

• Θεώρημα: (Αναλυτική παραλλαγή του ΘΘΑ)

Έστω f μια πολλαπλασιαστική αριθμητική συνάρτηση, τ.ώ. η $\sum_{n=0}^{\infty} f(n)$ να συγκλίνει απόλυτα, δηλαδή $\sum_{n=0}^{\infty} |f(n)| < +\infty$. Τότε, το άθροισμα της σειράς εκφράζεται ως απόλυτως συγκλίνον άηερο γινόμενο, δηλαδή $\sum_{n=0}^{\infty} f(n) = \prod_{p \text{ πρ}} (1 + f(p) + f(p^2) + \dots)$ για όλους τους πρώτους, το οποίο γινόμενο συγκλίνει απόλυτα. Ειδικότερα, αν f πλησιάζει πολλαπλή, τότε $\sum_{n=1}^{\infty} f(n) = \prod_{p \text{ πρ}} \frac{1}{1 - f(p)}$. Και τα δύο, ονομάζονται γινόμενα Euler της σειράς.

• Απόδειξη:

Έστω το πεπερασμένο γινόμενο $P(x) = \prod_{p \leq x} (1 + f(p) + f(p^2) + \dots)$ για όλους τους πρώτους μικρότερους του x . Αφού το γινόμενο περιλαμβάνει πεπερασμένου πλήθους σειράς που συγκλίνουν απόλυτα, μπορούμε να τις πολλαπλασιάσουμε και να αναδιατάξουμε τους όρους. Αφού η f είναι πολλαπλή, ένας τυχαίος όρος του γινομένου είναι $f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot \dots \cdot f(p_r^{a_r}) = f(p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r})$ με p_i διαφορετικούς πρώτους. Από Θ.Θ.Α, έχουμε $P(x) = \sum_{\substack{p_i \leq x \\ a_i \in \mathbb{N}}} f(\prod p_i^{a_i}) = \sum_{n \in A} f(n)$, όπου A είναι το σύνολο των φυσικών με πρώτους παράγοντες $\leq x$.

Συνεπώς, έχουμε και ότι $\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n)$, όπου B είναι το σύνολο των φυσικών που έστω και ένας πρώτος τους παράγοντας είναι μεγαλύτερος του x . Αρα, $|\sum_{n=1}^{\infty} f(n) - P(x)| = |\sum_{n \in B} f(n)| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|$

αφού στους φυσικούς μεγαλύτερους του x , συμπεριλαμβάνονται σίγουρα, όλοι αυτοί που έχουν έναν πρώτο παράγοντα, μεγαλύτερο του x .

(συνεχίζεται)

Αφού η σειρά $\sum f(n)$ συγκλίνει απόλυτως, για $x \rightarrow +\infty$, τα αθροίσματα $\sum_{n \geq x} |f(n)|$ τείνουν στο 0. Συνεπώς, $\rho(x) \xrightarrow{x \rightarrow \infty} \sum_{n \geq x} f(n)$, και άρα
$$\prod_{p \in P} (1 + f(p) + f(p^2) + \dots) = \sum_{n=0}^{\infty} f(n).$$

Τώρα Θ.δ.ο. το άπειρο γινόμενο συγκλίνει απόλυτα, δηλαδή $\prod_{n=1}^{\infty} (1 + a_n)$ συγκλίνει απόλυτα $\Leftrightarrow \sum_{n=1}^{\infty} a_n$ συγκλίνει απόλυτα.

Στη συγκεκριμένη περίπτωση, έχουμε $(\sum_p |f(p) + f(p^2) + \dots| < \infty)$:
$$\sum_{p \leq x} |f(p) + f(p^2) + \dots| \leq \sum_{p \leq x} |f(p)| + |f(p^2)| + \dots \leq \sum_{n=2}^{\infty} |f(n)| < \infty.$$

Άρα, αφού τα μερικά αθροίσματα είναι πραγματικά, τότε η $\sum_p |f(p) + f(p^2) + \dots|$ συγκλίνει, και άρα το άπειρο γινόμενο είναι απόλυτως συγκλίνον. Τέλος, αν η f είναι πλήρως πολλαί, ισχύει $f(p^n) = f(p)^n$ και κάθε σειρά $1 + f(p) + f(p^2) + \dots$ είναι μια γεωμετρική σειρά (η οποία συγκλίνει απόλυτα) με όριο σύγκλισης $\frac{1}{1 - f(p)}$.

$$\text{Άρα, } \sum f(n) = \prod_p \left(\sum_{n=0}^{\infty} (f(p))^n \right) = \prod_p \frac{1}{1 - f(p)}$$

□

~> Μπορούμε τώρα, να εφαρμόσουμε το παραπάνω Θεώρημα με απόλυτα συγκλίνουσες σειρές Dirichlet.

• Θεώρημα:

Έστω μια σειρά Dirichlet $\sum_{n=0}^{\infty} \frac{f(n)}{n^s}$ η οποία συγκλίνει απόλυτα στο $\sigma > \sigma_a$.

→ Αν f πολλαί:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots \right) \quad \text{αν } \sigma > \sigma_a$$

(1)

→ Αν f ηλίκως πολλα

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - \frac{f(p)}{p^s}}, \quad \sigma > \sigma_a. \quad (2)$$

↳ Όντως, αν $f(n)$ (ηλίκως) πολλα αριθμητική συνάρτηση, τότε $g(n) = \frac{f(n)}{n^s}$ ($g: \mathbb{N} \rightarrow \mathbb{C}$) είναι ηλίκως πολλα αριθμητική συνάρτηση, αφού $g(m \cdot n) = \frac{f(m)}{m^s} \cdot \frac{f(n)}{n^s} = \frac{f(m \cdot n)}{(m \cdot n)^s}$, για $(m, n) = 1$.

Οπότε, εφαρμόζω το προηγούμενο Θεώρημα.

* Ο γενικός όρος του (2) είναι :

$$\frac{f(p^n)}{p^{ns}} = f(p^n) \cdot (p^{-s})^n, \text{ δηλαδή εμφανίζεται η σειρά Bell της } f \text{ για } x = p^{-s}.$$

$$f_p(p^{-s})$$

• Παραδείγματα:

→ $f(n) = 1$: $\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s)$
 ↳ ηλίκως πολλα

→ Möbius : $f(n) = \mu(n) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \stackrel{\text{Bell}}{=} \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}$

→ Euler : $f(n) = \varphi(n) : \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_p \frac{1 - p^{-s}}{1 - p^{1-s}} = \frac{\zeta(s-1)}{\zeta(s)}$

22/5/2025

ΕΠΙΛΟΓΗ ΠΡΟΒΛΗΜΑΤΩΝ

• Διαμετρώσιμα Πρώτα Αριθμοί

- Ιδιότητες Διαμετρώσιμων

- Θ. Bézout - ΜΚΔ

- Σωστή κλάση

- Διωνευτικές (γραμμικές) εξισώσεις

- Ανεξάρτητα πρώτων αριθμών (Θ. Ευκλείδη) και μέσω $\sum \frac{1}{p}$ αναδίδει

- Θεμελιώδες Θεώρημα Αριθμητικής

- Διαίρεση: $n = \prod p_i^{r_i}$, διαίρεση $d = \prod p_i^{e_i}$ με $0 \leq e_i \leq r_i$

Πλῆθος? $\Rightarrow \prod_p (\nu_p(n) + 1)$

ΜΚΔ? $\Rightarrow \nu_p(w, n) = \min \{ \nu_p(n), \nu_p(w) \}$

- Αλγόριθμος Ευκλείδη

~ Εύρεση a, b zw $ax + by = (w, n)$

~ Εύρεση ΜΚΔ ~ Σωστή κλάση ~ Εύρεση αντίστροφου modulo

• Αριθμητικές Συναρτήσεις

- Möbius μ ($\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$ τύπος Gauss) $\rightarrow \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

- Euler φ

- Γινόμενο/συνέλιξη Dirichlet

- Η σύνολο αριθμητικών συναρτήσεων, $f(1) \neq 0$ είναι αβελιανή ομάδα με $*$. Πολλαπλές αριθμητικές συναρτήσεις είναι υποομάδα

• Ισοδυναμίες modulo

- $a \equiv b \pmod{m} \Leftrightarrow m | a - b \Leftrightarrow a, b$ ισοδυναμικοί modulo

- $\equiv$ Έχει 16 ιδιότητες

- $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{c}$ για $c|m$

- $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

- $a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}$

- $a \equiv b \pmod{m} \xrightarrow{c>0} ac \equiv bc \pmod{mc}$

- Νόμος Διαγραφής: $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$

- $a \equiv b \pmod{m} \xrightarrow{\chi(m,n)=1} a \equiv b \pmod{mn}$

$a \equiv b \pmod{n} \xleftarrow{\text{κάθε } m \text{ που } (m,n)=1}$

Γενικότερα, $a \equiv b \pmod{m_i} \forall i \xLeftrightarrow{(m_i, m_j)=1} a \equiv b \pmod{\prod m_i}$

- Κριτήρια Διαπερατότητας

- Πλήρη $\{0, 1, \dots, n-1\}$ και όλα τα ισοδύναμα $\pmod{m}$

- Αντικείμενα $\{a_1, a_2, \dots, a_{\phi(m)}\}$ συστήματα $\pmod{m}$

Ισοδυναμίες $\pmod{m}$

- Γραμμικές Ισοδυναμίες $ax \equiv b \pmod{m}$

$\leadsto (a, m) = 1 \rightarrow$ μοναδική λύση της $x \equiv a^{-1}b \pmod{m}$

$\updownarrow$
 a αντιστρέφεται $\pmod{m}$

$\leadsto (a, m) = d, d \nmid b \rightarrow$ καμία λύση

$\leadsto (a, m) = d, d \mid b \rightarrow d$ λύσεις, z ς $z, z + \frac{m}{d}, \dots, z + (d-1)\frac{m}{d} \pmod{m}$

όπου z η μοναδική λύση της $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

- Euler - Fermat

$(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$

$\downarrow$
 $a^{p-1} \equiv 1 \pmod{p}, p \nmid a$

$\downarrow$
 $a^p \equiv a \pmod{p}, \forall p$ (Μικρό EF)

- Lagrange: $a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$ με $a_n \not\equiv 0 \pmod{p}$

έχει το πολύ n λύσεις

- Wilson: $(p-1)! \equiv (-1) \pmod{p}$, p πρώτος

- Χινέτσκο Θεώρημα

- Λήμμα Hensel

• Τετραγωνικά Υπόλοιπα - Τετραγωνική Αναεξαρτησία

$x^2 \equiv n \pmod{p}$ έχει λύση?

- $\# \mathbb{Z}^* \pmod{p} = (p-1)/2$

- Κριτήριο Euler: $(n|p) \equiv n^{\frac{p-1}{2}} \pmod{p}$

- Λήμμα Gauss $(n|p) \equiv (-1)^u$

- Ιδιότητες σύμβολου Legendre

- Τετραγωνική Αναεξαρτησία $(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}$, για p, q

πρώτους πρώτους

- Jacobi για σύνθετους πρώτους

• Πρώτοι σε αριθμητικές προόδους

- Απειρία πρώτων της μορφής $4n-1, 4n+1$

• Σειρές Dirichlet - Συναρτήσεις f