Ελληνική Μαθηματική Εταιρεία
Παράρτημα Αχαΐας

Αλγεβρικές Ισοτιμίες

Συγγραφική Ομάδα:
Μπατέλης Γεώργιος
Κούλης Επαμεινώνδας
Νικολακόπουλος Δημήτριος

§ 1.1 Ορισμοί - Ιδιότητες

Ορισμός

Έστω α, β, ν ακέραιοι με ν>0. Αν οι ακέραιοι αριθμοί α, β διαιρούμενοι με τον ν αφήνουν το ίδιο υπόλοιπο, τότε οι αριθμοί αυτοί θα λέγονται ισοϋπόλοιποι με μέτρο ν θα γράφουμε:

α≡β(mod ν)

και θα διαβάζουμε "το α είναι **ισοϋπόλοιπο** με το β modulo ν" ή "το α είναι **ισότιμο** με το β ως προς modulo ν".

Παραδείγματα: 14≡5(mod 3), –11≡ 5(mod 4), 19≡ –3(mod 11).

Αν ο ακέραιος α δεν είναι ισοϋπόλοιπος με το β modulo ν θα γράφουμε: **α≢β(mod ν).**

Παράδειγμα: 7≢6(mod 2).

Θεώρημα 1.2

Έστω α, β, ν ακέραιοι με ν>0, τότε θα είναι: **α≡β(mod ν)⇔ν/(α–β).**

Απόδειξη

Έστω **α≡β(mod ν)** τότε, σύμφωνα με τον ορισμό, θα υπάρχουν ακέραιοι κ. λ τέτοιοι ώστε να ισχύει: $\left.\begin{matrix}\alpha=\kappa\cdot\nu+\upsilon\\ \beta=\lambda\cdot\nu+\upsilon\end{matrix}\right\}$ με $\mathbf{0\le\upsilon<\nu}$. Με αφαίρεση κατά μέλη θα έχουμε: $\alpha-\beta=(\kappa-\lambda)\nu\Leftrightarrow$ $\nu/(\alpha-\beta)$.

Έστω $\nu/(\alpha-\beta)\Leftrightarrow\ \alpha-\beta=\rho\cdot\nu$ (1).

Έστω $\beta=\mathbf{t}\cdot\nu+\upsilon$ με $\mathbf{0\le\upsilon<\nu}$, η ταυτότητα της διαίρεσης του β με το ν, οπότε η (1) γίνεται: $\alpha=\rho\cdot\nu+\beta=\rho\cdot\nu+\mathbf{t}\cdot\nu+\upsilon\Leftrightarrow\alpha=(\rho+\mathbf{t})\cdot\nu+\upsilon$, με $\mathbf{0\le\upsilon<\nu}$. Δηλαδή ο ακέραιος α διαιρούμενος με το ν δίνει υπόλοιπο υ, οπότε **α≡β(mod ν).**

Ιδιότητες

Με τη βοήθεια του ορισμού μπορούμε εύκολα να αποδείξουμε τις παρακάτω ιδιότητες:

- **α≡α(mod ν) ανακλαστική**
- **α≡β(mod ν) τότε και β≡α(mod ν) συμμετρική**
- **Αν α≡β(mod ν) και β≡γ(mod ν) τότε α≡γ(mod ν) μεταβατική.**

Παρατήρηση:

Οι παραπάνω ιδιότητες φανερώνουν ότι η ισοτιμία είναι μία **σχέση ισοδυναμίας στο Z**.

Πόρισμα 1.1

i. α≡0(mod ν)⇔ν/α

ii. Ο ακέραιος α είναι άρτιος, αν και μόνο αν, α≡0(mod 2)

iii. Ο ακέραιος α είναι περιττός, αν και μόνο αν, α≡1(mod 2)

iv. Αν α≡β(mod ν) και μ/ν τότε α≡β(mod μ)

v. Για κάθε ζεύγος ακεραίων α, β ισχύει α≡β(mod 1)

vi. Αν το υπόλοιπο της διαίρεσης του α με το ν είναι υ, τότε α≡υ(mod ν).

Απόδειξη

IV. Είναι α–β=λ·ν (1). Επειδή μ/ν θα είναι ν=ρ·μ, οπότε η (1) γίνεται α–β=λ·ρ·μ⇒μ/(α–β).

VI. Είναι α=λ·ν+υ⇒ α–υ=λ·ν⇒ν/ (α–β).

Θεώρημα 1.3

Έστω α, β, γ, δ, ν ακέραιοι με ν>0. Αν **α≡β(mod ν) και γ≡δ(mod ν)** τότε:

i. **α±γ≡β±δ(mod ν)**

ii. **α·γ≡β·δ(mod ν)**

iii. **α+μ≡β+μ(mod ν), με μ∈N***

iv. **α·μ≡β·μ(mod ν), με μ∈N***

v. **α·μ≡β·μ(mod μ·ν), με μ∈N*.**

vi. Αν **α≡β(mod ν)**, και **δ/ν**. **δ>**0, τότε **α≡β(mod δ)**.

Απόδειξη

I. Από την υπόθεση έχουμε:

$\Rightarrow \nu/(\alpha-\beta)+(\gamma-\delta) \Rightarrow \nu/(\alpha+\gamma)-(\beta+\delta) \Rightarrow$

α+γ≡β+δ(mod ν). Όμοια **α–γ≡β–δ(mod ν).**

II. Από την υπόθεση έχουμε: $\left.\begin{matrix}\nu/(\alpha-\beta)\\ \nu/(\gamma-\delta)\end{matrix}\right\} \Rightarrow \left.\begin{matrix}\nu/(\alpha-\beta)\gamma\\ \nu/(\gamma-\delta)\beta\end{matrix}\right\} \Rightarrow \left.\begin{matrix}\nu/(\alpha\gamma-\beta\gamma)\\ \nu/(\gamma\beta-\delta\beta)\end{matrix}\right\} \Rightarrow$

$\nu/(\alpha\gamma-\beta\gamma)+(\gamma\beta-\delta\beta) \Rightarrow \nu/(\alpha\gamma-\beta\delta) \Rightarrow$ **α·γ≡β·δ(mod ν).**

III. Είναι **μ≡μ(mod ν),** οπότε με τη βοήθεια από το I. έχουμε το ζητούμενο.

IV. Επειδή είναι **μ≡μ(mod ν)**, από το II θα έχουμε το ζητούμενο.

V. Είναι **α≡β(mod ν)**⇒ν/α–β⇒νμ/μ(α–β)⇒ νμ/μα–μβ⇒ **α·μ≡β·μ(mod μ·ν).**

VI. Είναι **α≡β(mod ν)**⇒ν/α–β και επειδή δ/ν θα έχουμε δ/(α–β)⇒**α≡β(mod δ).**

Παρατήρηση

Οι παραπάνω σχέσεις I, II, III, IV εκφράζουν ότι η ισοτιμία είναι συμβατή με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Οι σχέσεις V, VI αφορούν στη μεταβολή κλάσης mod.

ΠΡΟΣΟΧΗ: Όπως φαίνεται από την παραπάνω σχέση IV τα μέλη μιας ισοτιμίας πολλαπλασιάζονται με τον ίδιο ακέραιο. Δεν ισχύει γενικά για την διαίρεση!!!

Για παράδειγμα είναι 15≡9(mod 6), όμως δεν ισχύει 5≡3(mod 6).

Τα ουδέτερα στοιχεία της πρόσθεσης και του πολλαπλασιασμού (mod ν) είναι το 0 και το 1 αντίστοιχα.

Επίσης είναι $\alpha+(-\alpha)\equiv 0(\mathrm{mod}\ \nu)$, δηλαδή ο $(-\alpha)$ είναι ο αντίθετος του α ως προς (mod ν).

Ορισμός

Έστω $\alpha\in Z$. Αν υπάρχει ακέραιος β, τέτοιος ώστε $\boldsymbol{\alpha\cdot\beta\equiv 1(\mathrm{mod}\ \nu)}$, τότε ο β λέγεται **αντίστροφος του α** ως προς (mod ν).

Προφανώς δεν υπάρχει απαραίτητα ο αντίστροφος ενός ακεραίου ως προς (mod ν).

Για παράδειγμα οι 4 και 3 είναι αντίστροφοι (mod 11), διότι $3\cdot 4\equiv 1(\mathrm{mod}\ 11)$, ενώ οι αριθμοί 5, 10 δεν έχουν αντίστροφο (mod 15) διότι θα έπρεπε να υπάρχει $\alpha\in Z$ τέτοιος ώστε $\alpha\cdot 5\equiv 1(\mathrm{mod}\ 15)\Rightarrow 15/5\alpha-1\Rightarrow 5\alpha-1=15\rho\Rightarrow 5\alpha=15\rho+1\Rightarrow 5/1$ που είναι άτοπο. Όμοια και για το 10.

Ο νόμος της διαγραφής δεν ισχύει πάντοτε για τις ισοτιμίες, δηλαδή **δεν ισχύει η συνεπαγωγή:** Αν $\alpha\cdot\beta\equiv\gamma\cdot\beta(\mathrm{mod}\ \nu)$ τότε $\alpha\equiv\beta(\mathrm{mod}\ \nu)$, ισχύει όμως η παρακάτω ασθενέστερη μορφή του νόμου της διαγραφής.

Θεώρημα 1.4

Αν α, x, y ακέραιοι με $\kappa\neq 0$ και $\nu\in N^*$ τότε

- **i.** $\alpha\cdot x\equiv\alpha\cdot y(\mathrm{mod}\ \nu)$ αν και μόνο αν $x\equiv y\left(\mathbf{mod}\ \frac{\nu}{\delta}\right)$, όπου $\delta=(\alpha,\nu)$
- **ii.** Αν $\alpha\cdot x\equiv\alpha\cdot y(\mathrm{mod}\ \nu)$ και $(\alpha,\nu)=1$ τότε $x\equiv y\left(\mathbf{mod}\ \nu\right)$.

Απόδειξη

I. Έστω ότι $\alpha\cdot x\equiv\alpha\cdot y(\mathrm{mod}\ \nu)$, θα αποδείξουμε ότι $x\equiv y\left(\mathbf{mod}\ \frac{\nu}{\delta}\right)$ ή αρκεί $\boldsymbol{\frac{\nu}{\delta}/(x-y)}$ (1).

Είναι $\alpha\cdot x\equiv\alpha\cdot y(\mathrm{mod}\ \nu)\Rightarrow \alpha\cdot x-\alpha\cdot y=\kappa\nu$, για κάποιο $\kappa\in Z$, οπότε θα είναι $\alpha\cdot(x-y)=\kappa\nu\Rightarrow$ $\boldsymbol{\frac{\alpha}{\delta}\cdot(x-y)=\kappa\cdot\frac{\nu}{\delta}\Rightarrow\frac{\nu}{\delta}/\frac{\alpha}{\delta}\cdot(x-y)}$ (2). Είναι $\boldsymbol{\delta=(\alpha,\nu)\Rightarrow 1=(\frac{\alpha}{\delta},\frac{\nu}{\delta})}$, οπότε από τη σχέση (2) προκύπτει η (1).

Αντίστροφα.

Αν $x\equiv y\left(\mathbf{mod}\ \frac{\nu}{\delta}\right)\Rightarrow \boldsymbol{\frac{\nu}{\delta}/x-y}\Rightarrow\nu/\delta(x-y)$ (3).

Είναι $\delta=(\alpha,\nu)\Rightarrow\delta/\alpha\Rightarrow\alpha=\mu\delta$, $\mu\in Z$ (4).

Από τη σχέση (3) επειδή $\nu/\delta(x-y)\Rightarrow\nu/\mu\delta(x-y)$ και λόγω της (4) θα έχουμε $\nu/\alpha(x-y)\Rightarrow$ $\nu/\alpha x-\alpha y\Rightarrow\alpha\cdot x\equiv\alpha\cdot y(\mathrm{mod}\ \nu)$.

II. Προκύπτει από το I.

Θεώρημα 1.5

Ο αντίστροφος του θετικού ακεραίου α ως προς (mod ν) υπάρχει αν και μόνο αν $(\alpha,\nu)=1$.

Απόδειξη

Έστω ότι (α, ν)=1. Τότε θα υπάρχουν κ, λ∈Z τέτοιοι ώστε κα+λν=1⇒ κα−1=λν⇒ κα≡ 1(mod ν), δηλαδή ο ακέραιος κ είναι αντίστροφος του α (mod ν).

Αντίστροφα, έστω β∈Z τέτοιος ώστε αβ≡1(mod ν) και δ=(α, ν).

Από τη σχέση αβ≡1(mod ν) ⇒ ν/αβ−1(1).

Επειδή δ=(α, ν)⇒δ/ν, άρα λόγω της (1) θα έχουμε δ/(αβ−1) (2).

Επίσης δ=(α, ν)⇒δ/α⇒δ/αβ, οπότε από τη σχέση (2) θα έχουμε δ/−1, άρα δ=1⇒(α, ν)=1.

Θεώρημα 1.6

Ο αντίστροφος ενός ακεραίου α>0 ως προς mod ν, αν υπάρχει, είναι μοναδικός (mod ν).

Απόδειξη

Έστω ότι ο ακέραιος α>0, έχει δύο διαφορετικούς αντιστρόφους x, y, ως προς (mod ν). Τότε θα είναι αx≡1(mod ν) και αy≡1(mod ν).

Από τις παραπάνω σχέσεις θα έχουμε αx−αy≡1(mod ν)⇒ν/αx−αy⇒ν/α(x−y), και επειδή (α, ν)=1 (προϋπόθεση ύπαρξης αντιστρόφου) θα έχουμε ν/x−y⇒ x≡y(mod ν), δηλαδή ο αντίστροφος είναι μοναδικός (mod ν).

Θεώρημα 1.7

Αν $\alpha_1 \equiv \beta_1 \pmod{\nu}$, $\alpha_2 \equiv \beta_2 \pmod{\nu}$,..., $\alpha_\nu \equiv \beta_\nu \pmod{\nu}$, τότε:

i. $\alpha_1+\alpha_2+...+\alpha_\nu \equiv \beta_1+\beta_2+...+\beta_\nu \pmod{\nu}$
ii. $\alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_\nu \equiv \beta_1 \cdot \beta_2 \cdot ... \cdot \beta_\nu \pmod{\nu}$
iii. $\alpha^\nu \equiv \beta^\nu \pmod{\nu}$, με $\nu \in N^*$.

Πόρισμα 1.7.1

Έστω $f(x) = \alpha_\nu x^\nu + \alpha_{\nu-1} x^{\nu-1} + ... + \alpha_1 x + \alpha_o$ πολυώνυμο με ακέραιους συντελεστές, και κ≡λ (mod μ), με κ, λ ακέραιοι με μ∈N* . Τότε θα είναι f(κ)≡f(λ)(mod μ).

Απόδειξη

Από τη δοθείσα σχέση κ≡λ (mod μ) θα έχουμε:

$\kappa^\nu \equiv \lambda^\nu \pmod{\mu} \Rightarrow \alpha_\nu \kappa^\nu \equiv \alpha_\nu \lambda^\nu \pmod{\mu}$

$\kappa^{\nu-1} \equiv \lambda^{\nu-1} \pmod{\mu} \Rightarrow \alpha_{\nu-1} \kappa^\nu \equiv \alpha_{\nu-1} \lambda^\nu \pmod{\mu}$

.....

.....

κ≡λ (mod μ)⇒ $\alpha_1 \kappa \equiv \alpha_1 \lambda \pmod{\mu}$ και

$\alpha_o \equiv \alpha_o \pmod{\mu}$, οπότε με πρόσθε4ση κατά μέλη θα έχουμε f(κ)≡f(λ)(mod μ).

Θεώρημα 1.8 (Πρόταση χρήσιμη για ασκήσεις)

- **i.** Για κάθε πρώτο p>3 ισχύει ότι $p\equiv\pm1 \pmod 6$
- **ii.** Αν ο $p\neq3$ είναι πρώτος τότε $p^2\equiv 1 \pmod 3$
- **iii.** Αν ο $p\neq2$ είναι πρώτος τότε $p^2\equiv 1 \pmod 8$
- **iv.** Αν 0 p>3 είναι πρώτος τότε $p^2\equiv 1 \pmod{12}$.

Απόδειξη

Βασική Πρόταση: κάθε πρώτος αριθμός είναι της μορφής 6κ+1 ή της μορφής 6κ+5.

Πράγματι: Έστω p πρώτος, τότε θα είναι $p=6\mu+\upsilon$, με υ=0, 1, 2, 3, 4, 5.

Οι περιπτώσεις να είναι το υ=0 ή 2 ή 3 ή 4 απορρίπτονται διότι ο p θα είναι σύνθετος, άρα πρέπει υ=1, οπότε $p=6\mu+1$ ή υ=5, οπότε $p=6\mu+5$ ή $p=6\tau-1$, δηλαδή $p=6\nu\pm1$.

I. Επειδή ο p είναι πρώτος θα είναι $p=6\mu+1$, οπότε θα έχουμε ότι $p\equiv1\pmod 6$ ή $p=6\mu+5$, οπότε θα έχουμε ότι $p\equiv5 \pmod 6 \Rightarrow p\equiv-1 \pmod 6$. Άρα τελικά θα είναι $p\equiv\pm1 \pmod 6$.

II. Είναι $p=6\nu\pm1\Rightarrow p^2=36\nu^2\pm12\nu+1=3(12\nu^2\pm4\nu)+1$, οπότε $p^2\equiv 1 \pmod 3$.

III. Είναι $p=6\nu\pm1\Rightarrow p^2=36\nu^2\pm12\nu+1=32\nu^2+4\nu^2\pm8\nu\pm4\nu+1=8(4\nu^2\pm\nu)+4\nu(\nu\pm1)+1$ και επειδή ν, ν±1 είναι δύο διαδοχικοί ακέραιοι, θα είναι $\nu(\nu\pm1)=2t$, οπότε $p^2=8w+1$, άρα $p^2\equiv 1 \pmod 8$.

Θα μπορούσαμε να γράψουμε: $p=8\lambda+\upsilon$, με υ=0, 1, 2, 3, 4, 5, 6, 7 και επειδή ο p είναι πρώτος οι τιμές 0, 2, 4, 6 για το υ απορρίπτονται.

Αν υ=1 τότε $p^2=(8\lambda+1)^2=8\pi+1\Rightarrow$ άρα $p^2\equiv 1 \pmod 8$.

Αν υ=3 τότε $p^2=(8\lambda+3)^2=8\pi+9=8\alpha+1\Rightarrow$ άρα $p^2\equiv 1 \pmod 8$.

Αν υ=5 τότε $p^2=(8\lambda+5)^2=8\pi+25=8c+1\Rightarrow$ άρα $p^2\equiv 1 \pmod 8$.

Αν υ=7 τότε $p^2=(8\lambda+7)^2=8\pi+49=8m+1\Rightarrow$ άρα $p^2\equiv 1 \pmod 8$.

IV. Είναι $p=6\nu\pm1\Rightarrow p^2=36\nu^2\pm12\nu+1=12(3\nu^2\pm\nu)+1$, οπότε $p^2\equiv 1 \pmod{12}$.

Θεώρημα 1.9

Να αποδείξετε ότι κάθε ακέραιος α είναι ισότιμος με το άθροισμα των ψηφίων του modulo 9.

Απόδειξη

Έστω $\alpha\in Z$, τότε $\alpha=\alpha_\nu\cdot10^\nu+\alpha_{\nu-1}\cdot10^{\nu-1}+\ldots+\alpha_2\cdot10^2+\alpha_1\cdot10+\alpha_o$, γραμμένος με τη δεκαδική του παράσταση.

Αρκεί να αποδείξουμε ότι $\alpha\equiv(\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_2+\alpha_1+\alpha_o)(\mathrm{mod}\,9)$ αρκεί να αποδείξουμε ότι $9/\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_2+\alpha_1+\alpha_o$.

Είναι $\alpha=\alpha_\nu\cdot(9+1)^\nu+\alpha_{\nu-1}\cdot(9+1)^{\nu-1}+\ldots+\alpha_2\cdot(9+1)^2+\alpha_1\cdot(9+1)+\alpha_o\Leftrightarrow$

$\alpha=\alpha_\nu\cdot(\pi o\lambda 9+1)+\alpha_{\nu-1}\cdot(\pi o\lambda 9+1)+\ldots+\alpha_2\cdot(\pi o\lambda 9+1)+\alpha_1\cdot(9+1)+\alpha_o\Leftrightarrow$

$\alpha=\pi o\lambda 9(\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_2+\alpha_1)+\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_1+\alpha_o\Leftrightarrow$

$\alpha-(\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_1+\alpha_o)=9\rho\Leftrightarrow\alpha\equiv(\alpha_\nu+\alpha_{\nu-1}+\ldots+\alpha_2+\alpha_1+\alpha_o)(\mathrm{mod}\,9)$.

Θεώρημα 1.10

Αν $\alpha \equiv \beta \pmod{\mu}$, $\alpha \equiv \beta \pmod{\nu}$ και $(\mu, \nu)=1$, να αποδείξετε ότι $\alpha \equiv \beta \pmod{\mu\cdot\nu}$, $\alpha,\beta,\mu,\nu \in Z$.

Απόδειξη

Αρκεί να αποδείξουμε ότι $\mu\cdot\nu/(\alpha-\beta)$.

Είναι $\alpha \equiv \beta \pmod{\mu} \Rightarrow \mu/\alpha-\beta \Rightarrow \alpha-\beta=\kappa\cdot\mu$ (1).

Επίσης $\alpha \equiv \beta \pmod{\nu} \Rightarrow \nu/\alpha-\beta \Rightarrow \alpha-\beta=\lambda\cdot\nu$ (2).

Επειδή $(\mu, \nu)=1 \Rightarrow x\cdot\mu+y\cdot\nu=1$ (3).

Είναι $(\alpha-\beta)=(\alpha-\beta)\cdot 1 \overset{(3)}{=} (\alpha-\beta)\cdot(x\cdot\mu+y\cdot\nu)= (\alpha-\beta)x\cdot\mu+(\alpha-\beta)\cdot y\cdot\nu \overset{(2),(1)}{=} \lambda\cdot\nu\cdot x\cdot\mu+\kappa\cdot\mu\cdot\cdot y\cdot\nu=$
$\mu\cdot\nu\cdot(\lambda\cdot x+\kappa\cdot y) \Rightarrow \mu\cdot\nu/(\alpha-\beta)$.

Επίσης:

Αρκεί να αποδείξουμε ότι $\nu\cdot\mu/(\alpha-\beta)$.

Είναι $\alpha\equiv\beta \pmod{\mu} \Rightarrow \mu/\alpha-\beta \Rightarrow \alpha-\beta=\lambda\mu$, $\lambda\in Z$ (1).

Είναι $\alpha\equiv\beta \pmod{\nu} \Rightarrow \nu/\alpha-\beta$ και λόγω της (1) $\nu/\lambda\mu$ και επειδή $(\nu, \mu)=1$, $\nu/\lambda \Rightarrow \lambda=\pi\nu$, $\pi\in Z$ (2).

Η (1) λόγω της (2) γίνεται $\alpha-\beta=\pi\nu\cdot\mu \Rightarrow \mu\cdot\nu/(\alpha-\beta)$.

Παράδειγμα

Να δείξετε ότι $7^{13} \equiv 7 \pmod{1365}$.

Λύση

Αναλύουμε τον αριθμό 1365 σε γινόμενο παραγόντων, οπότε θα είναι $1365=3\cdot5\cdot7\cdot13$.

Εκμεταλλευόμενοι το προηγούμενο θεώρημα θα προσπαθήσουμε να δείξουμε ότι:

$7^{13} \equiv 7 \pmod{3}$, $7^{13} \equiv 7 \pmod{5}$, $7^{13} \equiv 7 \pmod{7}$, $7^{13} \equiv 7 \pmod{13}$, οπότε $7^{13} \equiv 7 \pmod{3\cdot5\cdot7\cdot13}$.

Είναι $7\equiv 1 \pmod{3}$, άρα $7^{12} \equiv 1 \pmod{3}$, επομένως $7^{13} \equiv 7 \pmod{3}$ (1).

Είναι $7\equiv 2 \pmod{5}$, $7^2 \equiv 4 \pmod{5}$, $7^3 \equiv 3 \pmod{5}$, $7^4 \equiv 1 \pmod{5}$, άρα $7^{12} \equiv 1 \pmod{5}$ επομένως θα είναι $7^{13} \equiv 7 \pmod{5}$ (2).

Προφανώς είναι $7^{13} \equiv 7 \pmod{7}$, διότι $7/7^{13}-7$ (3).

Είναι $7\equiv 7 \pmod{13}$, $7^2 \equiv 10 \pmod{13}$, $7^3 \equiv 5 \pmod{13}$, $7^4 \equiv 9 \pmod{13}$, $7^5 \equiv 11 \pmod{13}$, $7^6 \equiv 12 \pmod{13} \Rightarrow 7^6 \equiv -1 \pmod{13}$, άρα θα είναι $7^{12} \equiv 1 \pmod{13}$, επομένως θα είναι $7^{13} \equiv 7 \pmod{13}$ (4).

Από τις σχέσεις (1), (2), (3), (4) θα είναι $7^{13} \equiv 7 \pmod{3\cdot5\cdot7\cdot13}$.

Εφαρμογές

1) Έστω ένας φυσικός κ και ένας πρώτος ρ. Να αποδειχθεί ότι οι μόνες λύσεις της $x^2 \equiv x \pmod{\rho^\kappa}$ είναι οι $x \equiv 0$ ή $1 \pmod{\rho^\kappa}$, $x\in Z$.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Είναι $x^2 \equiv x \pmod{\rho^\kappa} \Rightarrow \rho^\kappa / x^2 - x \Rightarrow \rho^\kappa / x(x-1)$. Οι x, x−1 είναι διαδοχικοί ακέραιοι, οπότε ο ένας θα είναι άρτιος και ο άλλος περιττός.

Αν ρ=2 τότε ο ρ^κ θα είναι άρτιος, άρα θα διαιρεί έναν από τους x, x−1.

Αν ρ≠2, τότε ο ρ^κ θα είναι περιττός, άρα θα διαιρεί έναν από τους x, x−1,

Τελικά θα είναι $\rho^\kappa / x \Rightarrow x \equiv 0 \pmod{\rho^\kappa}$ ή $\rho^\kappa / x-1 \Rightarrow x \equiv 1 \pmod{\rho^\kappa}$.

2) Αν ν, μ είναι δύο φυσικοί αριθμοί, να αποδειχθεί ότι: $\mu^{2\nu} \equiv 1 \pmod{(\mu+1)}$.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Είναι $\mu \equiv (-1) \pmod{(\mu+1)} \Rightarrow \mu^{2\nu} \equiv (-1)^{2\nu} \pmod{(\mu+1)} \Rightarrow \mu^{2\nu} \equiv 1 \pmod{(\mu+1)}$.

3) Να βρείτε τι ώρα είναι

I. 100 ώρες μετά τα μεσάνυχτα

II. 1000 ώρες μετά τις 3 το μεσημέρι

III. 1000 ώρες πριν τις 5 το πρωί.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

I. Είναι $0+100 \pmod{24} \equiv 4 \pmod{24}$, οπότε θα είναι 4 το πρωί.

II. Είναι $15+1000 \pmod{24} \equiv 15+16 \pmod{24} \equiv 31 \pmod{24} \equiv 7 \pmod{24}$, οπότε θα είναι 7 το πρωί.

III. Είναι $5-1000 \pmod{24} \equiv 5-16 \pmod{24} \equiv -11 \pmod{24}$, οπότε θα είναι 11 το πρωί.

4) Να αποδείξετε ότι κάθε τέλειο τετράγωνο είναι 0, 1 ή 4(mod 8).

Απόδειξη

Για κάθε ακέραιο ν έχουμε ότι ν=8λ+υ, με υ=0,1,2,3,4,5,6,7, δηλαδή $\nu \equiv \upsilon \pmod 8$.

Για υ=0, έχουμε $\nu \equiv 0 \pmod 8 \Rightarrow \nu^2 \equiv 0 \pmod 8$

Για υ=1, έχουμε $\nu \equiv 1 \pmod 8 \Rightarrow \nu^2 \equiv 1 \pmod 8$

Για υ=2, έχουμε $\nu \equiv 2 \pmod 8 \Rightarrow \nu^2 \equiv 4 \pmod 8$

Για υ=3, έχουμε $\nu \equiv 3 \pmod 8 \Rightarrow \nu^2 \equiv 9 \pmod 8) \Rightarrow \nu^2 \equiv 1 \pmod 8$

Για υ=4, έχουμε $\nu \equiv 4 \pmod 8 \Rightarrow \nu^2 \equiv 16 \pmod 8) \Rightarrow \nu^2 \equiv 0 \pmod 8$

Για υ=5, έχουμε $\nu \equiv 5 \pmod 8 \Rightarrow \nu^2 \equiv 25 \pmod 8) \Rightarrow \nu^2 \equiv 1 \pmod 8$

Για υ=6, έχουμε $\nu \equiv 6 \pmod 8 \Rightarrow \nu^2 \equiv 36 \pmod 8) \Rightarrow \nu^2 \equiv 4 \pmod 8$

Για υ=7, έχουμε $\nu \equiv 7 \pmod 8 \Rightarrow \nu^2 \equiv 49 \pmod 8) \Rightarrow \nu^2 \equiv 1 \pmod 8$.

5)

I. Να αποδείξετε ότι αν οι αριθμοί ρ και 8ρ−1 είναι πρώτοι, τότε ο 8ρ+1 είναι σύνθετος.

II. Να αποδείξετε ότι αν οι αριθμοί ρ και $8\rho^2+1$ είναι πρώτοι, τότε ο $8\rho^2-1$ είναι πρώτος.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

I. Αν ρ=3 τότε 8ρ−1=25, που είναι σύνθετος.

Αν $\rho\neq 3$, τότε $\rho \equiv 1(\text{mod } 3)$ ή $\rho \equiv 2(\text{mod } 3)$.

Αν $\rho \equiv 1(\text{mod } 3) \Rightarrow 8\rho \equiv 8(\text{mod } 3) \Rightarrow 8\rho \equiv -1(\text{mod } 3) \Rightarrow 8\rho+1 \equiv 0(\text{mod } 3)$, δηλαδή $3/8\rho+1$, άρα $8\rho+1$ σύνθετος.

Αν $\rho \equiv 2(\text{mod } 3)) \Rightarrow 8\rho \equiv 16(\text{mod } 3) \Rightarrow 8\rho \equiv 1(\text{mod } 3)) \Rightarrow 8\rho-1 \equiv 0(\text{mod } 3)$, δηλαδή $3/8\rho-1$, άρα $8\rho-1$ σύνθετος που είναι άτοπο.

II. Αν $\rho\neq 3$ τότε $\rho \equiv 1(\text{mod } 3)$ ή $\rho \equiv 2(\text{mod } 3)$.

Αν $\rho \equiv 1(\text{mod } 3) \Rightarrow \rho^2 \equiv 1(\text{mod } 3) \Rightarrow 8\rho^2 \equiv 8(\text{mod } 3) \Rightarrow 8\rho^2 \equiv -1(\text{mod } 3) \Rightarrow$
$8\rho^2+1 \equiv 0(\text{mod } 3)$, δηλαδή ο $8\rho^2+1$ είναι σύνθετος, που είναι άτοπο.

Αν $\rho \equiv 2(\text{mod } 3) \Rightarrow \rho^2 \equiv 4(\text{mod } 3) \Rightarrow 8\rho^2 \equiv 32(\text{mod } 3) \Rightarrow 8\rho^2 \equiv -1(\text{mod } 3) \Rightarrow$
$8\rho^2+1 \equiv 0(\text{mod } 3)$, δηλαδή ο $8\rho^2+1$ είναι σύνθετος, που είναι άτοπο.

Αν $\rho=3$ τότε $8\rho^2+1=73$ που είναι πρώτος και $8\rho^2-1=71$ που είναι πρώτος. Άρα η μόνη περίπτωση είναι $\rho=3$.

Ασκήσεις

1) Με τη χρήση των ισοτιμιών να αποδειχθούν τα παρακάτω:

I. $13/(145^6+1)$

II. $431/(2^{43}-1)$

III. $233/(2^{29}-1)$

IV. $167/(2^{83}-1)$.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

I. Είναι $145\equiv 2(\text{mod } 13) \Rightarrow 145^6 \equiv 2^6 (\text{mod } 13) \Rightarrow 145^6 \equiv 64 (\text{mod } 13) \Rightarrow 145^6 \equiv (-1)$ $(\text{mod } 13) \Rightarrow 145^6+1 \equiv 0 (\text{mod } 13) \Rightarrow 13/(145^6+1)$.

II. Είναι $2^8 \equiv 256(\text{mod } 431) \Rightarrow 145^6 \equiv 2^6 (\text{mod } 13) \Rightarrow 145^6 \equiv 64 (\text{mod } 13) \Rightarrow$
$145^6 \equiv (-1) (\text{mod } 13) \Rightarrow 145^6+1 \equiv 0 (\text{mod } 13) \Rightarrow 13/(145^6+1)$.

III. Είναι $2^8 \equiv 256(\text{mod } 233) \Rightarrow 2^8 \equiv 23(\text{mod } 233) \Rightarrow 2^{24}=(2^8)^3 \equiv 23^3 (\text{mod } 233) \Rightarrow$
$2^{24} \equiv 12167 (\text{mod } 233) \Rightarrow 2^{24} \equiv 51 (\text{mod } 233) \Rightarrow 2^5 \cdot 2^{24} \equiv 32 \cdot 51 (\text{mod } 233) \Rightarrow$
$2^{29} \equiv 1632 (\text{mod } 233) \Rightarrow 2^{29} \equiv 1(\text{mod } 233) \Rightarrow 233/(2^{29}-1)$.

IV. Είναι $2^9 \equiv 512(\text{mod } 167) \Rightarrow 2^9 \equiv 11(\text{mod } 167) \Rightarrow (2^9)^9 \equiv 11^9 (\text{mod } 167)$ (1).

$11^2 \equiv 121 (\text{mod } 167) \Rightarrow 11^3 \equiv 1331 (\text{mod } 167) \Rightarrow 11^3 \equiv (-5) (\text{mod } 167) \Rightarrow$
$11^9 \equiv (-5)^3 (\text{mod } 167) \Rightarrow 11^9 \equiv (-125)(\text{mod } 167) \Rightarrow 11^9 \equiv (-1)(125)(\text{mod } 167) \Rightarrow$
$11^9 \equiv (-1)(-42)(\text{mod } 167) \Rightarrow 11^9 \equiv 42(\text{mod } 167)$, άρα η (1) γίνεται:
$(2^9)^9 \equiv 42(\text{mod } 167) \Rightarrow 2^2 \cdot 2^{81} \equiv 4 \cdot 42(\text{mod } 167) \Rightarrow 2^{83} \equiv 168(\text{mod } 167) \Rightarrow$
$2^{83} \equiv 1(\text{mod } 167) \Rightarrow 167/(2^{83}-1)$.

2) Να αποδείξετε ότι $100/11^{100}-1$.

Λύση

($1^{ος}$ τρόπος)

Είναι $11\equiv 11(\text{mod } 100)\Rightarrow 11^2\equiv 21(\text{mod } 100)\Rightarrow 11^3\equiv 31(\text{mod } 100)\Rightarrow$
$11^4\equiv 41(\text{mod } 100)\Rightarrow 11^5\equiv 51(\text{mod } 100)\Rightarrow 11^{10}\equiv 01(\text{mod } 100)\Rightarrow$
$(11^{10})^{10}\equiv 1(\text{mod } 100)\Rightarrow 100/11^{100}-1$.

($2^{ος}$ τρόπος)

Είναι $11^{100}-1=(11-1)(11^{99}+11^{98}+=...+11+1)=10)(11^{99}+11^{98}+=...+11+1)\cdot$

Η παράσταση $(11^{99}+11^{98}+=...+11+1)$ είναι άθροισμα 100 προσθετέων, στους οποίου το τελευταίο ψηφίο είναι η μονάδα. Άρα το τελευταίου ψηφίο του αθροίσματος αυτούς θα είναι το 0, δηλαδή θα είναι πολλαπλάσιο του 10. Άρα $(11^{99}+11^{98}+=...+11+1)=10\kappa$, οπότε $11^{100}-1=10\cdot 10100\lambda$, άρα $100/11^{100}-1$.

3) Αν ο φυσικός ν είναι σχετικά πρώτος με τον αριθμό 11, τότε να αποδείξετε ότι:

I. $5/(\nu^4-1)$

II. $5/(\nu^8-1)$.

Λύση

I. Διακρίνουμε περιπτώσεις:

- αν $\nu\equiv 1$ (mod 5), τότε $\nu^4\equiv 1$ (mod 5)
- αν $\nu\equiv 2$ (mod 5), τότε $\nu^4\equiv 2^4$ (mod 5)$\Rightarrow \nu^4\equiv 16(\text{mod } 5)\Rightarrow \nu^4\equiv 1$ (mod 5)
- αν $\nu\equiv 3$ (mod 5), τότε $\nu^4\equiv 3^4$ (mod 5)$\Rightarrow \nu^4\equiv 81(\text{mod } 5)\Rightarrow \nu^4\equiv 1$ (mod 5)
- αν $\nu\equiv 4$ (mod 5), τότε $\nu^4\equiv 4^4$ (mod 5)$\Rightarrow \nu^4\equiv 256(\text{mod } 5)\Rightarrow \nu^4\equiv 1$ (mod 5).

Άρα σε κάθε περίπτωση $5/(\nu^4-1)$.

II. Είναι $\nu^8-1=(\nu^4)^2-1=(\nu^4-1)\cdot(\nu^4+1)$ και επειδή $5/\nu^4-1)$ θα έχουμε ότι $5/(\nu^8-1)$.

4) Να αποδείξετε ότι αν οι συντελεστές της εξίσωσης $\alpha x^2+\beta x+\gamma=0$ είναι περιττοί ακέραιοι τότε η εξίσωση δεν έχει ρητές λύσεις.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Η εξίσωση έχει ρητές λύσεις, αν και μόνο αν, η διακρίνουσα είναι τέλειο τετράγωνο.

Η διακρίνουσα της εξίσωσης είναι $\Delta=\beta^2-4\alpha\gamma$, με α, β, γ περιττοί ακέραιοι.

Έστω $\alpha=2\kappa+1$, $\beta=2\lambda+1$ και $\gamma=2\mu+1$, τότε θα έχουμε:

$\Delta=(2\lambda+1)^2-4(2\kappa+1)(2\mu+1)=4\lambda^2+4\lambda+1-4(4\kappa\mu+2\kappa+2\mu+1)=4\lambda^2+4\lambda+1-16\kappa\mu-8\kappa-8\mu-4=4\lambda(\lambda+1)+1-16\kappa\mu-8\kappa-8\mu-4$ (1).

Επειδή $\lambda(\lambda+1)$ είναι διαδοχικοί ακέραιοι, οπότε $\lambda(\lambda+1)=2\rho$, η (1) γίνεται:

$\Delta=8\rho-16\kappa\mu-8\kappa-8\mu-3\Rightarrow\Delta=8(\rho-2\kappa\mu-\kappa-\mu)-3\Rightarrow\Delta=8\delta-3$, άρα $\Delta\equiv 3(\text{mod } 8)$, οπότε η Δ δεν μπορεί να είναι τέλειο τετράγωνο, επειδή κάθε τέλειο τετράγωνο είναι ισότιμο με 0, 1 ή 4(mod 8).

5)

I. Να βρείτε όλους τους φυσικούς ν για τους οποίους ο $2^\nu-1$ διαιρείται με το 7.

II. Να αποδείξετε ότι δεν υπάρχει ν για τον οποίο ο $2^\nu+1$ να διαιρείται με το 7.

(6η ΔΜΟ, 1964 Μόσχα).(ΕΜΕ. Θεωρία Αριθμών)

Λύση

I. Αναζητούμε τους φυσικούς για τους οποίους έχουμε $2^ν \equiv 1(\text{mod } 7)$.

Έχουμε $2^1 \equiv 2(\text{mod } 7) \Rightarrow 2^2 \equiv 4(\text{mod } 7) \Rightarrow 2^3 \equiv 8(\text{mod } 7) \Rightarrow 2^3 \equiv 1(\text{mod } 7)$.

Από την τελευταία σχέση μια προφανής λύση είναι η ν=3, αναζητώντας και άλλες λύσεις διακρίνουμε τις περιπτώσεις:

- Αν ν=3κ τότε θα είναι $2^ν=2^{3κ} \equiv 1(\text{mod } 7)$
- Αν ν=3κ+1 τότε θα είναι $2^ν=2^{3κ+1} \equiv 2(\text{mod } 7)$
- Αν ν=3κ+2 τότε θα είναι $2^ν=2^{3κ+2} \equiv 4(\text{mod } 7)$, άρα οι ζητούμενοι φυσικοί είναι όλα τα πολλαπλάσια του 3.

II. Διακρίνουμε περιπτώσεις

- Αν ν=3κ τότε θα είναι $2^ν=2^{3κ} \equiv 1(\text{mod } 7) \Rightarrow 2^ν+1 =2^{3κ}+1 \equiv 2(\text{mod } 7)$.
- Αν ν=3κ+1 τότε θα είναι $2^ν=2^{3κ+1} \equiv 2(\text{mod } 7) \Rightarrow 2^ν+1 =2^{3κ+1}+1 \equiv 3(\text{mod } 7)$.
- Αν ν=3κ+2 τότε θα είναι $2^ν=2^{3κ+2} \equiv 4(\text{mod } 7) \Rightarrow 2^ν+1 =2^{3κ+2}+1 \equiv 5(\text{mod } 7)$, άρα δεν υπάρχει ν για τον οποίον ο $2^ν+1$ να διαιρείται με το 7.

6) Έστω α ένας φυσικός αριθμός που διαιρείται από το 6. Να δείξετε ότι δεν υπάρχουν ακέραιες τιμές για τα x, y που να επαληθεύουν την εξίσωση $2016x^2-αy^2+15=0$ (1) .

Λύση

Επειδή $6/α \Rightarrow α=6λ$.

Έστω ότι η εξίσωση (1) έχει λύση ακέραια λύση (x,y)=(m, n).

Τότε η (1) γίνεται $2016m^2-αn^2+15=0 \Rightarrow 2016m^2+15=αn^2 \Rightarrow 2016m^2+15=6λn^2$ δηλαδή θα έχουμε $2016m^2+15 \equiv 0(\text{mod } 6)$ είναι άτοπο.

Παρατήρηση:

Μπορούμε να πούμε ότι το $6/6λn^2$, άρα $6/2016m^2+15$ και επειδή 6/2016 θα πρέπει 6/15 που είναι άτοπο.

7) Να βρεθούν οι λύσεις της εξίσωσης $\mathbf{x_1^4 + x_2^4 + ... + x_{14}^4 = 15999}$, όπου $\mathbf{x_1, x_2, ..., x_{14}}$ φυσικοί αριθμοί.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Παρατηρούμε ότι αν ο x είναι άρτιος τότε θα είναι

$x^4=(2κ)^4=16κ^4 \equiv 0(\text{mod } 16)$.

Αν ο x είναι περιττός τότε

$x^4=(2κ+1)^4=16κ^4+4(2κ)^3+6(2κ)^2+4(2κ)+1=16κ^4+32κ^3+24κ^2+8κ+1=$

$16(κ^4+2κ^3)+16κ^2+8κ^2+8κ+1=16(κ^4+2κ^3+κ^2)+8κ(κ+1)+1=16μ+1$, διότι $κ(κ+1)=2ρ$.

Άρα θα είναι $x^4=16μ+1 \equiv 1(\text{mod } 16)$.

Δηλαδή $x^4 \equiv 0(\text{mod } 16)$, αν ο x είναι άρτιος ή $x^4 \equiv 1(\text{mod } 16)$, αν ο x είναι περιττός.

Από τα παραπάνω, ανάλογο αν ο x είναι άρτιος ή περιττός θα έχουμε τις περιπτώσεις:

$\mathbf{x_1^4 + x_2^4 + ... + x_{14}^4 \equiv 0 \text{ ή } 1 \text{ ή } 2 \text{ ή} \cdots \text{ ή } 14 (\text{mod } 16)}$.

Επειδή $15999 \equiv 15(\text{mod } 16)$, η εξίσωση είναι αδύνατη.

8) Να δειχθεί ότι $\alpha^{3\nu} \equiv 1(\mathrm{mod}\,\alpha^2+\alpha+1)$ με $\alpha \in Z^*$, $\nu \in N^*$.

(Ε.Μ.Π.)

Λύση

Αρκεί να αποδείξουμε ότι $(\alpha^2+\alpha+1)/(\alpha^{3\nu}-1)$.

Είναι $\dfrac{\alpha^{3\nu}-1}{\alpha^2+\alpha+1} = \dfrac{\left(\alpha^3\right)^{\nu}-1}{\alpha^2+\alpha+1} = \dfrac{(\alpha^3-1)\left((\alpha^3)^{\nu-1}+(\alpha^3)^{\nu-2}+\cdots+\alpha^3+1\right)}{\alpha^2+\alpha+1} =$

$= \dfrac{(\alpha-1)(\alpha^2+\alpha+1)\left((\alpha^3)^{\nu-1}+(\alpha^3)^{\nu-2}+\cdots+\alpha^3+1\right)}{\alpha^2+\alpha+1} =$

$= (\alpha-1)\left((\alpha^3)^{\nu-1}+(\alpha^3)^{\nu-2}+\cdots+\alpha^3+1\right)$ δηλαδή $(\alpha^2+\alpha+1)/(\alpha^{3\nu}-1)$, οπότε θα είναι $\alpha^{3\nu}-1 \equiv 0(\mathrm{mod}\,\alpha^2+\alpha+1) \Rightarrow \alpha^{3\nu} \equiv 1(\mathrm{mod}\,\alpha^2+\alpha+1)$.

9) Να δείξετε ότ, αν ο 7 διαιρεί τον $\alpha^2+\beta^2$ (όπου α, β ακέραιοι), τότε θα διαιρεί και τους α, β.

(Waclaw Sierpinski 250 Προβλήματα της Στοιχειώδους Θεωρίας αριθμών)

Λύση

Έστω ένας ακέραιος x μη διαιρετός με το 7. Τότε θα είναι $x \equiv 1,2,3,4,5,6 \pmod 7$.

Υψώνοντας στο τετράγωνο θα έχουμε $x^2 \equiv 1,2,4 \pmod 7$.

Παίρνουμε όλους τους δυνατούς συνδυασμούς υπολοίπων modulo 7.

$\alpha^2 \equiv 1(\mathrm{mod}\,7)$	$\beta^2 \equiv 1(\mathrm{mod}\,7)$ $\beta^2 \equiv 2(\mathrm{mod}\,7)$ $\beta^2 \equiv 4(\mathrm{mod}\,7)$	$\alpha^2+\beta^2 \equiv 2(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 3(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 5(\mathrm{mod}\,7)$

$\alpha^2 \equiv 2(\mathrm{mod}\,7)$	$\beta^2 \equiv 1(\mathrm{mod}\,7)$ $\beta^2 \equiv 2(\mathrm{mod}\,7)$ $\beta^2 \equiv 4(\mathrm{mod}\,7)$	$\alpha^2+\beta^2 \equiv 3(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 4(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 6(\mathrm{mod}\,7)$

$\alpha^2 \equiv 4(\mathrm{mod}\,7)$	$\beta^2 \equiv 1(\mathrm{mod}\,7)$ $\beta^2 \equiv 2(\mathrm{mod}\,7)$ $\beta^2 \equiv 4(\mathrm{mod}\,7)$	$\alpha^2+\beta^2 \equiv 5(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 6(\mathrm{mod}\,7)$ $\alpha^2+\beta^2 \equiv 1(\mathrm{mod}\,7)$

Όπως φαίνεται από τα παραπάνω είναι $\alpha^2+\beta^2 \not\equiv 0(\mathrm{mod}\,7)$.

Συμπεραίνουμε ότι, αν $\alpha^2+\beta^2 \equiv 0(\mathrm{mod}\,7)$, τότε α, β ισότιμα με 0 modulo 7.

10) Δείξτε ότι υπάρχουν άπειροι φυσικοί αριθμοί n τέτοιοι ώστε ο $4n^2+1$ να διαιρείται ταυτόχρονα δια 5 και διά 13.

(Waclaw Sierpinski 250 Προβλήματα της Στοιχειώδους Θεωρίας αριθμών)

Λύση

Είναι $5\cdot13=65$, οπότε ο n, θα πρέπει να έχει μια μορφή $n=65\lambda+x$, με $\lambda\in N$ και κατάλληλο $x\in N$.

Τότε θα έχουμε $4n^2+1=4(65\lambda+x)^2+1=\pi o\lambda 65+4x^2+1$.

Για να διαιρείται ταυτόχρονα ο $4n^2+1$ δια 5 και διά 13, θα πρέπει $4x^2+1=65$, ή κάποιο πολλαπλάσιο του 65.

Αν $4x^2+1=65\Rightarrow 4x^2=64\Rightarrow x^2=16\Rightarrow x=4$, δηλαδή θα είναι $n=65\lambda+4$.

Θα είναι $n\equiv 4\ (\mathrm{mod}\ 5)\Rightarrow n^2\equiv 1\ (\mathrm{mod}\ 5)\Rightarrow 4n^2\equiv 4(\mathrm{mod}\ 5)\Rightarrow 4n^2+1\equiv 0(\mathrm{mod}\ 5)$.

Επίσης $n\equiv 4\ (\mathrm{mod}\ 13)\Rightarrow n^2\equiv 3\ (\mathrm{mod}\ 13)\Rightarrow 4n^2\equiv 12(\mathrm{mod}\ 13)\Rightarrow 4n^2+1\equiv 0(\mathrm{mod}\ 13)$.

Επειδή $(5,13)=1$, θα έχουμε ότι $4n^2+1\equiv 0(\mathrm{mod}\ 65)$, άρα υπάρχουν άπειροι φυσικοί αριθμοί n ώστε ο αριθμός $4n^2+1$ να διαιρείται ταυτόχρονα δια 5 και διά 13.

Παρατήρηση: Ο συγγραφέας θεωρεί τους ακεραίους $n=65k+56$.

§ 2.2 Το σύνολο των κλάσεων ισοδυναμίας

Γνωρίζουμε ότι η διαίρεση ενός ακεραίου αριθμού α με τον θετικό ακέραιο αριθμό ν δίνει πηλίκο π και υπόλοιπο υ, δηλαδή θα είναι α=ν·π+υ, με υ=0, 1, 2, ... , ν-1.
Για τις διάφορες τιμές του υ θα έχουμε:
Για υ=0 θα είναι α=ν·π, οπότε α≡ 0 (mod ν).
Για υ=1 θα είναι α=ν·π+1, οπότε α≡ 1 (mod ν).
Για υ=2 θα είναι α=ν·π+2, οπότε α≡ 2(mod ν).
.....
.....
Για υ=ν−1 θα είναι α=ν·π+ν−1, οπότε α≡ ν−1 (mod ν).

Δηλαδή κάθε ακέραιος α είναι ισότιμος με ένα και μοναδικό αριθμό από τους 0, 1, 2, ..., ν−1 ως προς (mod ν).

Σύμφωνα με τα παραπάνω μπορούμε να ορίσουμε τα σύνολα:
$\mathbf{Z_0 = \{x \in Z / x \equiv 0 (mod\ v)\}}$, δηλαδή οι ακέραιοι x που διαιρούμενοι με το ν δίνουν υπόλοιπο 0.
$\mathbf{Z_1 = \{x \in Z / x \equiv 1 (mod\ v)\}}$, δηλαδή οι ακέραιοι x που διαιρούμενοι με το ν δίνουν υπόλοιπο 1.
$\mathbf{Z_2 = \{x \in Z / x \equiv 2 (mod\ v)\}}$, δηλαδή οι ακέραιοι x που διαιρούμενοι με το ν δίνουν υπόλοιπο 2.

.....
.....

$\mathbf{Z_{v-1} = \{x \in Z / x \equiv (v-1) (mod\ v)\}}$, δηλαδή οι ακέραιοι x που διαιρούμενοι με το ν δίνουν υπόλοιπο ν−1.

Καθένα από τα σύνολα $\mathbf{Z_0, Z_1, Z_2, ..., Z_{v-1}}$ τα συμβολίζουμε με $\mathbf{\bar{0}, \bar{1}, \bar{2}, ..., \overline{v-1}}$ αντίστοιχα και ονομάζεται **κλάση ισοτιμίας ή κλάση υπολοίπων modulo ν**.

Για παράδειγμα για κάθε ακέραιο α ισχύει:
α≡ 0 (mod 5) ή α≡1 (mod 5) ή α≡ 2 (mod 5) ή α≡ 3(mod 5) ή α≡4(mod 5).
Ας θεωρήσουμε τα σύνολα:
$\mathbf{\bar{0} = Z_0 = \{x \in Z / x \equiv 0 (mod\ 5)\}}$, δηλαδή τους x∈Z που διαιρούμενοι με το 5 δίνουν υπόλοιπο 0,
$\mathbf{\bar{1} = Z_1 = \{x \in Z / x \equiv 1 (mod\ 5)\}}$, δηλαδή τους x∈Z που διαιρούμενοι με το 5 δίνουν υπόλοιπο 1,
$\mathbf{\bar{2} = Z_2 = \{x \in Z / x \equiv 2 (mod\ 5)\}}$, δηλαδή τους x∈Z που διαιρούμενοι με το 5 δίνουν υπόλοιπο 2,
$\mathbf{\bar{3} = Z_3 = \{x \in Z / x \equiv 3 (mod\ 5)\}}$, δηλαδή τους x∈Z που διαιρούμενοι με το 5 δίνουν υπόλοιπο 3,

$\bar{4} = Z_4 = \{x \in Z / x \equiv 4(\text{mod } 5)\}$, δηλαδή τους $x \in Z$ που διαιρούμενοι με το 5 δίνουν υπόλοιπο 4, οι οποίες είναι οι κλάσεις ισοτιμιών του 5.

Προφανώς οι κλάσεις αυτές ανά δύο είναι ξένες μεταξύ τους και η ένωσή τους δίνει το Z δηλαδή ισχύει $Z = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4}$.

Έστω $\bar{\alpha} = \{x \in Z / x \equiv \alpha(\text{mod } \nu)\}$ τότε $\nu / x - \alpha \Rightarrow x - \alpha = \lambda\nu$, $\lambda \in Z \Rightarrow x = \alpha + \lambda\nu$, $\lambda \in Z$, οπότε το σύνολο $\bar{\alpha} = \{\alpha + \lambda\nu, \lambda \in Z\}$ και οποιοδήποτε στοιχείο της κλάσης $\bar{\alpha}$ λέγεται αντιπρόσωπος της κλάσης $\bar{\alpha}$. Προφανώς ισχύει $\alpha \equiv \beta(\text{mod } \nu) \Leftrightarrow \bar{\alpha} = \bar{\beta}$.

Η κλάση υπολοίπων modulo 9 που περιέχει τους αριθμούς 3, 39 είναι το σύνολο

{...–24,–15,–6,3,12,21,30,39,48....}= $\bar{3}$ ή $\overline{12}$ ή $\overline{-24}$ κ.λ.π.

Κάθε ακέραιος α είναι ισότιμος μόνον με έναν από τους 0, 1, 2, ...,ν–1 modulo ν.

Το σύνολο των κλάσεων mod ν το συμβολίζουμε Z_ν **ή** $Z_{\text{mod } \nu}$.

Αν ισχύει $\alpha \not\equiv \beta(\text{mod } \nu)$, τότε επειδή οι διαιρέσεις των ακεραίων α, β με το ν δίνουν διαφορετικό υπόλοιπο θα έχουμε ότι $\bar{\alpha} \cap \bar{\beta} = \varnothing$.

Θεώρημα 2.1

Οι κλάσεις $\bar{0}, \bar{1}, \bar{2}, ..., \overline{\nu - 1}$ υπολοίπων mod ν είναι διαφορετικές ανά δύο.

Παρατήρηση: Σύμφωνα με τα παραπάνω, επειδή κάθε ακέραιος α, ανήκει μόνο σε μία από τις κλάσεις $\bar{0}, \bar{1}, \bar{2}, ..., \overline{\nu - 1}$ modulo ν και οι κλάσεις αυτές είναι ανά δύο ξένες μεταξύ, θα έχουμε:

$Z_\nu = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{\nu - 1}\}$ και για το σύνολο των ακεραίων $Z = \bar{0} \cup \bar{1} \cup \bar{2}. \cup .. \cup \overline{\nu - 1}$.

§ 2.3 Η συνάρτηση φ του Euler

Η συνάρτηση Euler, συμβολίζεται με το ελληνικό γράμμα φ, είναι μια αριθμοθεωρητική συνάρτηση και ορίζεται στο σύνολο των φυσικών αριθμών.
Για κάθε φυσικό αριθμό ν≥1, η φ(ν) μας δίνει το πλήθος των φυσικών αριθμών οι οποίοι είναι μικρότεροι ή ίσοι του ν και είναι πρώτοι προς το ν.
Δηλαδή: $\varphi:N^*\to N^*$ με φ(ν) να είναι το πλήθος των στοιχείων του συνόλου $\{\kappa\in N/1\le\kappa\le\nu$ και $(\kappa,\nu)=1\}$. Στην περίπτωση που ν=1 ορίζουμε φ(1)=1.
Ο παρακάτω πίνακας μας δείχνει μερικές τιμές της φ(ν).

ν	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
φ(ν)	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Γενικά ισχύει:

Αν $\nu=\rho_1^{\alpha_1}\cdot\rho_2^{\alpha_2}\cdot\ldots\cdot\rho_\kappa^{\alpha_\kappa}$, με $\rho_1,\rho_2,\ldots\rho_\kappa$ πρώτοι, τότε

$$\phi(\nu)=\nu\left(1-\frac{1}{\rho_1}\right)\cdot\left(1-\frac{1}{\rho_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{\rho_\kappa}\right).$$

Ιδιότητες της συνάρτησης φ

- **i.** φ(ν)≤ν, για κάθε $\nu\in N^*$
  (προκύπτει από τον ορισμό).
- **ii.** φ(ν)=ν−1 αν και μόνο αν ο ν είναι πρώτος.
  (Αν ο ν είναι πρώτος, τότε είναι σχετικά πρώτος με κάθε αριθμό κ<ν. Άρα φ(ν)=ν−1.
  Αν ο ν είναι σύνθετος τότε υπάρχει κ<ν με κ/ν, άρα (κ,ν)=κ, επομένως φ(ν)<ν−1).
- **iii.** Η συνάρτηση φ είναι πολλαπλασιαστική, δηλαδή αν (α, β)=1, τότε φ(α·β)=φ(α)·φ(β).
  Για παράδειγμα φ(3·5)=φ(3)·φ(5)=2·4=8.

Παραδείγματα

1) Είναι $\varphi(1200)=\varphi(2^2\cdot3^4\cdot5^2)=\phi(\nu)=1200\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)=$

$1200\left(\frac{1}{2}\right)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{4}{5}\right)=320$. (Α. Συγκελάκης)

2) Αν ν περιττός, τότε ισχύει φ(2ν)=φ(ν).
Απόδειξη
Επειδή ο ν είναι περιττός θα είναι (ν, 2)=1, οπότε θα έχουμε φ(2ν)=φ(ν)·φ(2) (1) (η συνάρτηση φ είναι πολλαπλασιαστική).
Επειδή φ(2)=2−1=1 η (1) γίνεται φ(2ν)=φ(ν).

3) Αν ν άρτιος, τότε ισχύει φ(2ν)=2φ(ν).

Απόδειξη

Επειδή ο ν είναι άρτιος θα είναι ν=$2^{\kappa}\cdot\lambda$, με κ∈N^{*} και λ περιττός φυσικός αριθμός.

Είναι (2^{κ}, λ)=1, (ο ένας άρτιος ο άλλος περιττός), οπότε θα έχουμε:

φ(ν)=φ($2^{\kappa}\cdot\lambda$)=·φ(2^{κ})·φ(λ)= $2^{\kappa}\left(1-\frac{1}{2}\right)=2^{\kappa-1}\cdot\phi(\lambda)$ (2).

Είναι φ(2ν)=φ(2·$2^{\kappa}\cdot\lambda$)=φ($2^{\kappa+1}\cdot\lambda$)= φ($2^{\kappa+1}$)·φ(λ)= $2^{\kappa+1}\left(1-\frac{1}{2}\right)\cdot\phi(\lambda)=2^{\kappa}\cdot\phi(\lambda)=$

$2\cdot 2^{\kappa-1}\cdot\phi(\lambda)=2\cdot\phi(\nu)$.

Θεώρημα Fermat

Αν ρ πρώτος και α ακέραιος με (α, ρ)=1, τότε $\alpha^{\rho-1}\equiv 1(\mathrm{mod}\ \rho)$.

- Επειδή το ρ είναι πρώτος αριθμός και ισχύει (α, ρ)=1 σημαίνει ότι ρ∤ α.

Σχόλιο: Πρώτος ο Fermat διατύπωσε το προηγούμενο θεώρημα. Ο Euler στη συνέχεια διατύπωσε και απόδειξε το παρακάτω θεώρημα, που είναι γενίκευση του θεωρήματος του Fermat, γι' αυτό αναφέρετε και ως **μικρό θεώρημα του Fermat**.

Πόρισμα 2.1. Αν ρ πρώτος και α ακέραιος με (α, ρ)=δ≥1, τότε $\alpha^{\rho}\equiv\alpha(\mathrm{mod}\ \rho)$.

Απόδειξη

Αν (α, ρ)=1, τότε από το θεώρημα Fermat θα είναι $\alpha^{\rho-1}\equiv 1(\mathrm{mod}\ \rho)\Rightarrow \alpha^{\rho}\equiv\alpha(\mathrm{mod}\ \rho)$.

Αν (α, ρ)>1 τότε, επειδή ο ρ είναι πρώτος θα έχουμε ρ/α, άρα θα διαιρεί και τον α^{ρ}, οπότε θα είναι $\alpha^{\rho}\equiv\alpha\equiv 0(\mathrm{mod}\ \rho)$.

Πόρισμα 2.2. Αν ρ πρώτος και α φυσικός αριθμός με (α, ρ)=δ≥1, και d είναι ο μικρότερος εκθέτης για τον οποίο ισχύει τότε $\alpha^{d}\equiv\alpha(\mathrm{mod}\ \rho)$, τότε d/ρ−1.

Απόδειξη

Είναι d≤ρ−1. Αν d=ρ−1 τότε d/ρ−1.

Αν d<ρ−1 τότε ρ−1=κd+υ, με 0≤υ<d.

Από το θεώρημα Fermat θα είναι $\alpha^{\rho-1}\equiv 1(\mathrm{mod}\ \rho)\Rightarrow \alpha^{\kappa d+\upsilon}\equiv 1(\mathrm{mod}\ \rho)\Rightarrow \alpha^{\kappa d}\cdot\alpha^{\upsilon}\equiv 1(\mathrm{mod}\ \rho)\Rightarrow (\alpha^{\kappa})^{d}\cdot\alpha^{\upsilon}\equiv 1(\mathrm{mod}\ \rho)$.

Αν υ≠0, τότε επειδή $\alpha^{d}\equiv\alpha(\mathrm{mod}\ \rho)\Rightarrow (\alpha^{\kappa})^{d}\equiv 1(\mathrm{mod}\ \rho)\Rightarrow (\alpha^{\kappa})^{d}\cdot\alpha^{\upsilon}\equiv\alpha^{\upsilon}\ (\mathrm{mod}\ \rho)$ (1).

Επειδή ο d είναι ο μικρότερος εκθέτης για τον οποίο ισχύει τότε $\alpha^{d}\equiv\alpha(\mathrm{mod}\ \rho)$, τότε λόγω της σχέσης (1) θα είναι $\alpha^{\upsilon}\ (\mathrm{mod}\ \rho)\not\equiv 1(\mathrm{mod}\ \rho)\Rightarrow \alpha^{\rho-1}\not\equiv 1(\mathrm{mod}\ \rho)$, που είναι άτοπο, άρα πρέπει υ=0, δηλαδή ρ−1=κd.

Παραδείγματα

1) Από το θεώρημα Fermat είναι $2^{7-1} \equiv 1(\text{mod } 7)$.

Είναι $\boldsymbol{\phi(7) = 7\left(1-\frac{1}{7}\right) = 6}$ και οι διαιρέτες τους 6 είναι Δ(6)=1,2,3,6.

Θα έχουμε $2 \equiv 2(\text{mod } 7)$, $2^2 \equiv 4(\text{mod } 7)$, $2^3 \equiv 1(\text{mod } 7)$, $2^4 \equiv 2(\text{mod } 7)$, $2^5 \equiv 4(\text{mod } 7)$, $2^6 \equiv 1(\text{mod } 7)$, δηλαδή το υπόλοιπο της διαίρεσης του 2^ν επαναλαμβάνεται κάθε τρία βήματα και το 3/6.

2) Να βρείτε το υπόλοιπο της διαίρεσης του 3^ν με το 11.

Λύση

Είναι (3,11)=1, οπότε από το θεώρημα Fermat θα έχουμε $2^{11-1} \equiv 1(\text{mod } 11)$.

Επειδή είναι $\boldsymbol{\phi(11) = 11\left(1-\frac{1}{11}\right) = 10}$ και οι διαιρέτες τους 10 είναι Δ(10)=1,2,5,10 το υπόλοιπο της διαίρεσης του 3^ν με το 11 θα επαναλαμβάνεται το πολύ κάθε 10 βήματα και το βήμα της επανάληψης θα είναι διαιρέτης του 10, δηλαδή 1,2,4,5,10.

Πράγματι είναι $3 \equiv 23\text{mod } 11)$, $3^2 \equiv 9(\text{mod } 11)$, $3^3 \equiv 5(\text{mod } 11)$, $3^4 \equiv 24\text{mod } 11)$,

$3^5 \equiv 1(\text{mod } 11)$, $3^6 \equiv 3(\text{mod } 11)$,...

Θεώρημα Euler

Αν α, m ακέραιοι με m>0 και (α, m)=1, τότε $\alpha^{\varphi(m)} \equiv 1(\text{mod } m)$, όπου φ(m) είναι η συνάρτηση του Euler.

Παρατηρήσεις:

- Αν m=ρ, τότε παίρνουμε το θεώρημα του Fermat.
- Από το παραπάνω θεώρημα του Euler θα έχουμε $\alpha^{\varphi(m)} \equiv 1(\text{mod } m) \Rightarrow$ $\alpha \cdot \alpha^{\varphi(m)-1} \equiv 1(\text{mod } m)$, δηλαδή ο αντίστροφος του α(mod m) είναι ο $\alpha^{\varphi(m)-1}$.

Εφαρμογές:

1) Είναι φ(11)=10 και (7,11)=1, τότε θα έχουμε $7^{10} \equiv 1(\text{mod } 11)$.

2) Οι αριθμοί 36 και 101 είναι πρώτοι μεταξύ τους και φ(36)=12 ($36=2^2 \cdot 3^2$, άρα $\boldsymbol{\phi(36) = 36\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right) = 12}$), άρα έχουμε $101^{36} \equiv 1(\text{mod } 36)$.

3) Ο αριθμός ρ=97 είναι πρώτος και (300, 97)=1, άρα $300^{96} \equiv 1(\text{mod } 97)$.

4) Να αποδείξετε ότι, για $\nu \in Z$

I. Το 3 διαιρεί τον $\nu^3 - \nu$

II. Το 13 διαιρεί τον $\nu^{13} - \nu$

III. Το 17 διαιρεί τον $\nu^{17}-\nu$

IV. Το 4 δεν διαιρεί τον $\nu^4-\nu$.

Λύση

Από το θεώρημα του Fermat θα έχουμε:

I. $\nu^3 \equiv \nu(\text{mod } 3) \Rightarrow 3/\ \nu^3-\nu$.

II. $\nu^{13} \equiv \nu(\text{mod } 13) \Rightarrow 13/\ \nu^{13}-\nu$.

III. $\nu^{17} \equiv \nu(\text{mod } 17) \Rightarrow 17/\ \nu^{17}-\nu$.

IV. Το 4 δεν είναι πρώτος, οπότε για ν=3 θα έχουμε $3^4-3=78$ που δεν διαιρείται με το 4.

5) Να δείξετε ότι ο αριθμός $A=0,7\cdot 1968^{1968}-0,3\cdot 68^{78}$ είναι ακέραιος.

(με μικρή αλλαγή ΕΜΕ. Εισαγωγή στη Θεωρία Αριθμών Α, Συγκελάκης)

Απόδειξη

Ο αριθμός Α γίνεται $\mathbf{A=\frac{7\cdot 1968^{1968}-3\cdot 68^{78}}{10}}$, αρκεί να αποδείξουμε ότι $\mathbf{10/7\cdot 1968^{1968}-3\cdot 68^{78}}$.

Ο Αριθμητής του κλάσματος Α είναι άρτιος αριθμός, άρα διαιρείται με το 2

Είναι $10=2\cdot 5$ και επειδή $(2, 5)=1$, αρκεί να αποδείξουμε ότι $5/7\cdot 1968^{1968}-3\cdot 68^{78}$.

Από το θεώρημα Fermat έχουμε $3^4 \equiv 1(\text{mod } 5)$.

Είναι $1968 \equiv 3(\text{mod } 5) \Rightarrow 1968^{1968} \equiv 3^{1968} (\text{mod } 13) \Rightarrow 1968^{1968} \equiv (3^4)^{495} (\text{mod } 5) \Rightarrow$

$1968^{1968} \equiv 1 (\text{mod } 5) \Rightarrow 7\cdot 1968^{1968} \equiv 7 (\text{mod } 5) \Rightarrow 7\cdot 1968^{1968} \equiv 2(\text{mod } 5)$.

$68 \equiv 3(\text{mod } 5) \Rightarrow 68^{78} \equiv 3^{78} (\text{mod } 5) \Rightarrow 68^{78} \equiv (3^4)^{19}\cdot 3^2 (\text{mod } 5) \Rightarrow 68^{78} \equiv 9 (\text{mod } 5) \Rightarrow$

$68^{78} \equiv 4 (\text{mod } 5) \Rightarrow 3\cdot 68^{78} \equiv 12 (\text{mod } 5) \Rightarrow 3\cdot 68^{78} \equiv 2 (\text{mod } 5)$, οπότε θα έχουμε:

$7\cdot 1968^{1968}-3\cdot 68^{78} \equiv 0(\text{mod } 5)$, δηλαδή το $5/7\cdot 1968^{1968}-3\cdot 68^{78}$.

Τελικά $10/7\cdot 1968^{1968}-3\cdot 68^{78}$.

6) Αν για το φυσικό αριθμό ν ισχύουν $7\nmid \nu-1$, $7\nmid \nu$, $7\nmid \nu+1$, να αποδείξετε ότι $7/(\nu^4+\nu^2+1)$.

Απόδειξη

Το 7 είναι πρώτος αριθμός και επειδή $7\nmid \nu$, από το θεώρημα Fermat, θα έχουμε:

$\nu^6 \equiv 1(\text{mod } 7) \Rightarrow \nu^6-1 \equiv 0(\text{mod } 7) \Rightarrow (\nu^2)^3-1 \equiv 0(\text{mod } 7) \Rightarrow$

$(\nu^2-1)(\nu^4+\nu^2+1) \equiv 0(\text{mod } 7) \Rightarrow (\nu-1)(\nu+1)(\nu^4+\nu^2+1) \equiv 0(\text{mod } 7)$.

Επειδή $7\nmid \nu-1$, $7\nmid \nu$, $7\nmid \nu+1$ θα έχουμε ότι $(\nu^4+\nu^2+1) \equiv 0(\text{mod } 7)$, δηλαδή $7/(\nu^4+\nu^2+1)$.

7) Αν ο ρ είναι πρώτος τότε για τους ακεραίους $\alpha_1, \alpha_2, ..., \alpha_\nu$ θα ισχύει:

$\mathbf{(\alpha_1+\alpha_2+...+\alpha_\nu)^\rho \equiv \alpha_1^\rho+\alpha_2^\rho+...+\alpha_\nu^\rho (\text{mod } p)}$.

Λύση

Επειδή το ρ είναι πρώτος, από το θεώρημα Fermat θα έχουμε:

$\mathbf{\alpha_i^\rho \equiv \alpha_i (\text{mod } p) \Rightarrow \alpha_i \equiv \alpha_i^\rho (\text{mod } p)}$, i=1,2,...,ν (1).

Από το ίδιο θεώρημα ισχύει επίσης

$\mathbf{(\alpha_1+\alpha_2+...+\alpha_\nu)^\rho \equiv (\alpha_1+\alpha_2+...+\alpha_\nu) (\text{mod } p)}$, i=1,2,...,ν (2).

Από τη σχέση (1) θα έχουμε:

$$\left.\begin{array}{l}\alpha_1 \equiv \alpha_1^{\rho}(\mathrm{mod}\, p)\\ \alpha_2 \equiv \alpha_2^{\rho}(\mathrm{mod}\, p)\\ \cdots\\ \cdots\\ \alpha_\nu \equiv \alpha_\nu^{\rho}(\mathrm{mod}\, p)\end{array}\right\} \Rightarrow \alpha_1+\alpha_2+\ldots+\alpha_\nu \equiv (\alpha_1^{\rho}+\alpha_2^{\rho}+\ldots+\alpha_\nu^{\rho})(\mathrm{mod}\, p) \text{ (3).}$$

Από τις σχέσεις (2), (3) θα έχουμε $(\alpha_1+\alpha_2+\ldots+\alpha_\nu)^{\rho} \equiv \alpha_1^{\rho}+\alpha_2^{\rho}+\ldots+\alpha_\nu^{\rho}(\mathrm{mod}\, p)$, μεταβατική ιδιότητα.

8) Έστω ρ≥7 ένας πρώτος αριθμός. Να αποδείξετε ότι ο αριθμός $\underbrace{111\cdots1}_{\rho-1\,\text{μονάδες}}$ διαιρείται από το ρ.

(ΕΜΕ. Ισοτιμίες Α. Συγκελάκης)

Απόδειξη

Είναι $\underbrace{111\cdots1}_{\rho-1\,\text{μονάδες}} = \frac{10^{\rho-1}-1}{9} \Rightarrow 9\cdot \underbrace{111\cdots1}_{\rho-1\,\text{μονάδες}} = 10^{\rho-1}-1$ (1).

Επειδή το ρ είναι πρώτος θα έχουμε (10,ρ)=1, οπότε από το μικρό θεώρημα του Fermat θα είναι $10^{\rho-1} \equiv 1(\mathrm{mod}\, \rho) \Rightarrow \rho / 10^{\rho-1}-1$ και επειδή (9, ρ)=1, θα έχουμε $\rho / \underbrace{111\cdots1}_{\rho-1\,\text{μονάδες}}$.

9) Να αποδείξετε ότι για κάθε πρώτο αριθμό ρ>2 ισχύει
$1^ρ+2^ρ+3^ρ+4^ρ+...+(ρ-1)^ρ \equiv 0(\mathrm{mod}\ ρ)$. (Θ. Ξένος)

Απόδειξη

Είναι $1^ρ\equiv 1(\mathrm{mod}\ ρ)$, $2^ρ\equiv 2(\mathrm{mod}\ ρ)$, $3^ρ\equiv 3(\mathrm{mod}\ ρ)$..., $(ρ-1)^ρ \equiv (ρ-1)(\mathrm{mod}\ ρ)$.

Με πρόσθεση θα έχουμε $1^ρ+2^ρ+3^ρ+4^ρ+...+(ρ-1)^ρ \equiv (1+2+3+...+(ρ-1))(\mathrm{mod}\ ρ)$ (1).

Είναι $1+2+\ldots+(\rho-1)=\frac{(\rho-1)\rho}{2}$ και επειδή ο ρ είναι περιττός (διότι είναι πρώτος >2), ο αριθμός ρ−1 θα είναι άρτιος, οπότε το άθροισμα $1+2+\ldots+(\rho-1)=\frac{(\rho-1)\rho}{2}$ θα είναι πολλαπλάσιο του ρ, άρα $1^ρ+2^ρ+3^ρ+4^ρ+...+(ρ-1)^ρ \equiv 0(\mathrm{mod}\ ρ)$.

10) Να δείξετε ότι εάν n φυσικός ≥1 τότε η παράσταση $2^{4n+1}-2^{2n}-1$ διαιρείται από το 9.

(ΕΜΕ. Ισοτιμίες. Α Συγκελάκης από το βιβλίου του Θ. Καζαντζή)

($1^{ος}$ τρόπος με επαγωγή)

Για n=1 έχουμε $2^{4n+1}-2^{2n}-1=2^5-2^2-1=27=$πολ9.

Έστω ότι η πρόταση ισχύει για n=κ, δηλαδή $2^{4κ+1}-2^{2κ}-1=9λ$ (1) θα αποδείξουμε ότι η πρόταση ισχύει και για n=κ+1, δηλαδή θα αποδείξουμε ότι $2^{4(κ+1)+1}-2^{2(κ+1)}-1=$πολ9 .

Η (1) $\Leftrightarrow 2^{4κ+1}=9λ+2^{2κ}+1$ (2).

Θα είναι $2^{4(κ+1)+1}-2^{2(κ+1)}-1=2^{4κ+1+4}-2^{2κ+2}-1=16\cdot 2^{4κ+1}-4\cdot 2^{2κ}-1 \overset{(2)}{=} 16\cdot(9λ+2^{2κ}+1)-4\cdot 2^{2κ}-1$
$=16\cdot 9λ+16\cdot 2^{2κ}+16-4\cdot 2^{2κ}-1=$ πολ9$+12\cdot 2^{2κ}+15$ (3).

Από τη σχέση (3) αρκεί να αποδείξουμε ότι η παράσταση $12\cdot 2^{2\kappa}+15$ είναι πολ9.
Για τη συγκεκριμένη παράσταση θα χρησιμοποιήσουμε ξανά μαθηματική επαγωγή.
Για κ=1 έχουμε $12\cdot 2^{2\kappa}+15=12\cdot 2^2+15=63=$πολ9.
Αν η πρόταση ισχύει για κ=λ, δηλαδή $12\cdot 2^{2\lambda}+15=9\mu \Rightarrow 12\cdot 2^{2\lambda}=9\mu-15$ (4),
θα αποδείξουμε ότι ισχύει και για κ=λ+1, δηλαδή θα αποδείξουμε ότι $12\cdot 2^{2(\lambda+1)}+15=9\rho$.
Είναι $12\cdot 2^{2(\lambda+1)}+15=4\cdot 12\cdot 2^{2\lambda}+15 \overset{(4)}{=} 4(9\mu-15)+15=$πολ9$-60+15=$πολ9, οπότε ισχύει η (3), άρα για κάθε $n\in N^*$, ισχύει $2^{4n+1}-2^{2n}-1=2^5-2^2-1=27=$πολ9.

($2^{ος}$ τρόπος με ισοτιμίες)
Είναι (9,2)=1, οπότε από το μικρό θεώρημα του Fermat, θα έχουμε:
$2^{9-1}\equiv 1 \pmod 9$.
Επειδή είναι φ(9)=6, το υπόλοιπο της διαίρεσης του 2^n με το 9 θα επαναλαμβάνεται το πολύ κάθε 6 βήματα και μάλιστα το βήμα της επανάληψης (πόρισμα 2.2), θα είναι διαιρέτης του 6 (Δ(6)=1,2,3,6).
Επειδή το υπόλοιπο της διαίρεσης του 2^n με το 9 θα επαναλαμβάνεται το πολύ κάθε 6 βήματα θα γράψουμε το n στη μορφή n=6κ+υ, με υ=0,1,2,3,4,5 και στη συνέχεια θα κατασκευάσουμε ένα πίνακα δυνάμεων για βρούμε για τις διάφορες τιμές του υ την παράσταση $2^{4n+1}-2^{2n}-1$.

υ=n (mod 6)	0	1	2	3	4	5	Επανάληψη ανά
4n+1 (mod 6)	1	5	3	1	5	3	.....
2^{4n+1} (mod 9)	2	5	8	2	5	8	3
-2^n(mod 9)	−1	−4	−7	−1	−4	−7	3
−1(mod 9)	−1	−1	−1	−1	−1	−1	1
$2^{4n+1}-2^{2n}-1$(mod 7)	0	0	0	0	0	0	....

Όπως λοιπόν φαίνεται από τον παραπάνω πίνακα ο αριθμός $2^{4n+1}-2^{2n}-1$ διαιρείται από το 9, για κάθε τιμή του $n\in N^*$.

11) Βρείτε όλους τους φυσικούς αριθμούς α για τους οποίους $10/\alpha^{10}+1$.
(Waclaw Sierpinski 250 προβλήματα της Στοιχειώδους Θεωρίας Αριθμών)

Λύση

Έστω $\alpha \equiv \upsilon \pmod{10}$, όπου $0\le\upsilon\le 9$.
Θα έχουμε $\alpha^{10}+1 \equiv \upsilon^{10}+1 \pmod{10}$, δηλαδή $10/\alpha^{10}+1 \Leftrightarrow \upsilon^{10}+1 \equiv 0 \pmod{10}$.
Κατασκευάζουμε για να υπολογίσουμε, για τις διάφορες τιμές του υ την παράσταση $\upsilon^{10}+1 \equiv 0 \pmod{10}$.

υ	0	1	2	3	4	5	6	7	8	9	
υ^{10}(mod 10)	0	1	4	9	6	5	6	9	4	1	(*)
$\upsilon^{10}+1$(mod 10)	1	2	5	0	7	6	7	0	5	2	

Όπως φαίνεται από τον παραπάνω πίνακα οι μοναδικές λύσεις είναι η υ=3 και υ=7. Επομένως, οι λύσεις του προβλήματος είναι οι αριθμοί α=10κ+3 και α=10κ+7, με $\kappa\in N$.
(*) Είναι $2\equiv 2 \pmod{10}$, $2^2\equiv 4 \pmod{10}$, $2^3\equiv 8 \pmod{10}$, $2^4\equiv 6 \pmod{10}$,

$2^5 \equiv 2(\text{mod } 10)$, δηλαδή έχουμε επανάληψη του υπολοίπου της διαίρεσης του 2^n με το 10 κάθε 4 βήματα, οπότε $2^{10} \equiv 4(\text{mod } 10)$.
Όμοια $3 \equiv 3(\text{mod } 10)$, $3^2 \equiv 9(\text{mod } 10)$, $3^3 \equiv 7(\text{mod } 10)$, $3^4 \equiv 1(\text{mod } 10)$, $3^5 \equiv 3(\text{mod } 10)$, δηλαδή έχουμε επανάληψη του υπολοίπου της διαίρεσης του 3^n με το 10 κάθε 4 βήματα, οπότε $3^{10} \equiv 9(\text{mod } 10)$.
Όμοια $4 \equiv 4(\text{mod } 10)$, $4^2 \equiv 6(\text{mod } 10)$, $4^3 \equiv 4(\text{mod } 10)$, $4^4 \equiv 6(\text{mod } 10)$, δηλαδή έχουμε επανάληψη του υπολοίπου της διαίρεσης του 4^n με το 10 κάθε 2 βήματα, οπότε θα είναι $4^{10} \equiv 6(\text{mod } 10)$.
Όμοια για τις υπόλοιπες δυνάμεις του υ.

Ασκήσεις

1) Ποιό είναι το τελευταίο ψηφίο του $\mathbf{2^{2018}}$.

Λύση

Πρέπει να βρούμε έναν αριθμό β τέτοιο ώστε $2^{2018} \equiv \beta(\text{mod } 10)$, με 0, 1,2,...,9.

Από το θεώρημα Fermat θα έχουμε $2^4 \equiv 1(\text{mod } 5) \Rightarrow 2^{2016} = (2^4)^{504} \equiv 1(\text{mod } 5) \Rightarrow$

$2^{2018} = (2^4)^{504} \cdot 2^2 \equiv 1(\text{mod } 5) \Rightarrow 2^{2018} \equiv 4(\text{mod } 5)$ (1).

Από τη σχέση (1) θα έχουμε $2^{2018} - 4 = 5\lambda$ (2).

Το πρώτο μέλος της (2) είναι άρτιος αριθμός, άρα θα πρέπει και το δεύτερο να είναι άρτιος αριθμός, οπότε θα πρέπει $\lambda = 2\mu$.

Τότε η (2) γίνεται $2^{2018} - 4 = 5 \cdot 2\mu \Rightarrow 2^{2018} - 4 = 10\mu \Rightarrow$

$2^{2018} \equiv 4(\text{mod } 10)$, άρα το τελευταίο ψηφίο του 2^{2018} είναι το 4.

2) Ποιό είναι το τελευταίο ψηφίο του $\mathbf{2^{2020}}$.

Λύση

Πρέπει να βρούμε έναν αριθμό β τέτοιο ώστε $2^{2020} \equiv \beta(\text{mod } 10)$, με β=0, 1,2,...,9.

Από το θεώρημα Fermat θα έχουμε $2^4 \equiv 1(\text{mod } 5) \Rightarrow 2^{2020} = (2^4)^{505} \equiv 1(\text{mod } 5)$(1).

Από τη σχέση (1) θα έχουμε $2^{2020} - 1 = 5\lambda$ (2).

Το πρώτο μέλος της (2) είναι περιττός αριθμός, άρα θα πρέπει και το δεύτερο να είναι περιττός αριθμός, οπότε θα πρέπει $\lambda = 2\mu + 1$. Τότε η (2) γίνεται $2^{2018} - 1 = 5 \cdot (2\mu + 1) \Rightarrow$

$2^{2018} - 1 = 10\mu + 5 \Rightarrow 2^{2018} - 6 \equiv 0(\text{mod } 10) \Rightarrow 2^{2018} \equiv 6(\text{mod } 10)$, άρα το τελευταίο ψηφίο του 2^{2020} είναι το 6.

Σχόλιο: Υπάρχουν και άλλοι τρόποι για να βρούμε το τελευταίο ψηφίο το 2^{2020}.

3) Να βρείτε το υπόλοιπο της διαίρεσης του $\mathbf{101^{82}}$ δια του 7.

Λύση

Είναι (101,7)=1, οπότε από το θεώρημα Fermat θα έχουμε:

$101^6 \equiv 1 (\text{mod } 7) \Rightarrow 101^{81} = (101^6)^{13} \cdot 101^2 \equiv 1 \cdot 101^2 (\text{mod } 7)$ (1).

Επειδή $101 \equiv 3 (\text{mod } 7) \Rightarrow 101^2 \equiv 3^2 (\text{mod } 7) \Rightarrow 101^2 \equiv 2 (\text{mod } 7)$ η (1) γίνεται:

$101^{81} \equiv 2(\text{mod } 7)$, άρα το υπόλοιπο της διαίρεσης.

4) Να βρεθεί το υπόλοιπο της διαίρεσης του $\mathbf{3^{100}}$ με το 101.

(Μαθηματικό Αθηνών)

Λύση

Ο αριθμός 101 είναι πρώτος, οπότε φ(101)=101−1=100 (*), άρα βολεύει να δουλέψουμε με το θεώρημα Euler.

Είναι (101,3)=1, άρα από το θεώρημα Euler θα είναι:

$3^{\varphi(\nu)} \equiv 1(\text{mod } 101) \Rightarrow 3^{100} \equiv 1(\text{mod } 101)$, άρα το υπόλοιπο είναι 1.

(*) Είναι $\sqrt{\mathbf{101}} < \mathbf{11}$, οπότε εύκολα διαπιστώνουμε ότι ο 101 είναι πρώτος, η φ(ν) είναι η συνάρτηση Euler για την οποία γνωρίζουμε ότι αν ν πρώτος τότε φ(ν)=ν−1.

5) **I.** Να βρεθεί το υπόλοιπο της διαίρεσης του $\mathbf{1!+2!+3!+...+1000!}$ με το 18.

II. Να βρεθεί το υπόλοιπο της διαίρεσης του $\mathbf{1^4+2^4+3^4+...+99^4+100^4}$ με το 5.

Λύση

I. Το 18=3·6, οπότε από τη στιγμή που θα εμφανιστεί το 3·6 στο πρώτο από το παραπάνω άθροισμα, όλοι οι επόμενοι προσθετέοι θα για παράγοντα το 3·6=18.

Είναι 1!+2!+3!+4!+5!=1+2+6+24+120=153,άρα $1!+2!+3!+4!+5!\equiv 153(\text{mod } 18) \Rightarrow 1!+2!+3!+4!+5!\equiv 9(\text{mod } 18)$ (1).

Είναι $6!=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6=40\cdot 18$, άρα $6!\equiv 0(\text{mod } 18)$, το ίδιο θα ισχύει και για τους προσθετέους 7!, 8!, ...1000!, διότι σε καθένα από αυτούς εμφανίζεται το 18.

Τελικά θα είναι $1!+2!+3!+...+1000! \equiv 9(\text{mod } 18)$, δηλαδή το υπόλοιπο θα είναι το 9.

II. Στο συγκεκριμένο άθροισμα ο εκθέτης είναι σταθερός, το 4, οι βάσεις αλλάζουν, από περιττό αριθμός σε άρτιο.

Ας πάρουμε περιπτώσεις:

- Αν $\nu=2\kappa$ τότε θα έχουμε $\nu^4=(2\kappa)^4=16\kappa^4$, άρα θα είναι $\nu^4\equiv 1(\text{mod } 5)$, με $\kappa=1,2,...,50$.

Άρα θα έχουμε $2^4+4^4+6^4+...+98^4+100^4 \equiv 50(\text{mod } 5) \Rightarrow 2^4+4^4+...+98^4+100^4 \equiv 0(\text{mod } 5)$.

- Αν ν περιττός τότε θα έχουμε:

$1 \equiv 1(\text{mod } 5) \Rightarrow 1^4 \equiv 1(\text{mod } 5)$

$3 \equiv 3(\text{mod } 5) \Rightarrow 3^4 \equiv 3^4 (\text{mod } 5) \Rightarrow 3^4 \equiv 1 (\text{mod } 5)$

$5 \equiv 0(\text{mod } 5) \Rightarrow 5^4 \equiv 0 (\text{mod } 5)$

$7 \equiv 2(\text{mod } 5) \Rightarrow 7^4 \equiv 2^4 (\text{mod } 5) \Rightarrow 7^4 \equiv 1 (\text{mod } 5)$

$9 \equiv 4(\text{mod } 5) \Rightarrow 9^4 \equiv 4^4 (\text{mod } 5) \Rightarrow 9^4 \equiv 256 (\text{mod } 5) \Rightarrow 9^4 \equiv 1 (\text{mod } 5)$, δηλαδή το αποτέλεσμα είναι 1 modulo 5, εκτός από το 5 και τα πολλαπλάσιά του που το αποτέλεσμα είναι modulo 0. Οι περιττοί είναι 50 και τα πολλαπλάσια του 5 είναι 10, άρα $1^4+3^4+5^4+...+97^4+99^4 \equiv 40(\text{mod } 5) \Rightarrow 1^4+3^4+5^4+...+97^4+99^4 \equiv 0(\text{mod } 5)$.

Τελικά $1^4+2^4+3^4+...+99^4+100^4 \equiv 0(\text{mod } 5)$.

6)

I. Να βρεθεί το υπόλοιπο της διαίρεσης του $\mathbf{5^{2016}}$ με το 7.

II. Να προσδιοριστεί ο x, ώστε να είναι $\mathbf{5^{2018}+\overline{6x47} \equiv 0(\text{mod } 7)}$, όπου $\mathbf{\overline{6x47}}$, αριθμός στο δεκαδικό σύστημα αρίθμησης.

Λύση

I. Είναι $5 \equiv 5(\text{mod } 7) \Rightarrow 5^2 \equiv 4(\text{mod } 7) \Rightarrow 5^3 \equiv (-1)(\text{mod } 7) \Rightarrow$

$\mathbf{5^{2018}=(5^3)^{627}\cdot 5^2 \equiv (-1)^{627}\cdot 25(\text{mod } 7) = -4(\text{mod } 7)}$.

II. Είναι $\mathbf{\overline{6x47}=6\cdot 10^3+x\cdot 10^2+4\cdot 10+7=6047+100x}$ (1).

Είναι $6047 \equiv 6 (\text{mod } 7)$ και $100 \equiv 2 (\text{mod } 7) \Rightarrow 100x \equiv 2x (\text{mod } 7)$, οπότε η (1) γίνεται:

$\mathbf{\overline{6x47}=(6+2x)(\text{mod } 7)}$.

Η αρχική εξίσωση γίνεται $-4+6+2x \equiv 0 (\text{mod } 7) \Rightarrow 2+2x \equiv 0 (\text{mod } 7) \Rightarrow 7/2+2x \Rightarrow 2+2x=7\lambda$ (2).

Το πρώτο μέλος της (2) είναι αριθμός άρτιος, άρα πρέπει και το λ να είναι άρτιος, Επίσης πρέπει $0\le x\le 9$, διότι ο x είναι ψηφίο.

Αν λ=2 τότε 2+2x=7λ⇒2+2x=14⇒2x=12⇒x=6.

Αν λ=4 τότε 2+2x=7λ⇒2+2x=28⇒2x=26⇒x=13, απορρίπτεται.

7) Να προσδιοριστούν οι ν∈Z, ώστε $\mathbf{\nu^2+\nu+5 \equiv 0 \pmod{11}}$.

Λύση

Είναι $\nu^2+\nu+5 \equiv 0 \pmod{11} \Rightarrow \nu^2+\nu+5-11+11 \equiv 0 \pmod{11} \Rightarrow \nu^2+\nu-6+11 \equiv 0 \pmod{11}$ $\Rightarrow (\nu-2)(\nu+3)+11 \equiv 0 \pmod{11} \Rightarrow (\nu-2)(\nu+3) \equiv 0 \pmod{11} \Rightarrow 11/(\nu-2)(\nu+3)$ και επειδή το 11 είναι πρώτος θα πρέπει $\left.\begin{matrix} 11/\nu-2 \\ \text{ή} \\ 11/\nu+3 \end{matrix}\right\} \Leftrightarrow \left.\begin{matrix} \nu-2=11\kappa \\ \text{ή} \\ \nu+3=11\lambda \end{matrix}\right\} \Leftrightarrow \left.\begin{matrix} \nu=11\kappa+2 \\ \text{ή} \\ \nu=11\lambda-3 \end{matrix}\right\}$.

8) Να δειχθεί ότι για κάθε τυχαίο φυσικό αριθμό ν ισχύει:

I. $\mathbf{30/(\nu^5-\nu)}$

II. $\mathbf{42/(\nu^7-\nu)}$.

(ΕΜΕ Θεωρία Αριθμών)

Λύση

I. Είναι $\nu^5-\nu=\nu(\nu^4-1)=\nu(\nu^2-1)(\nu^2+1)=\nu(\nu-1)(\nu+1)(\nu^2+1)$.

Το ν(ν−1)(ν+1) είναι γινόμενο τριών διαδοχικών ακεραίων, οπότε:

$6/\nu(\nu-1)(\nu+1) \Rightarrow 6/(\nu^5-\nu)$ (1).

Από το θεώρημα Fermat θα είναι $\nu^5 \equiv \nu \pmod 5 \Rightarrow 5/(\nu^5-\nu)$ (2).

Από τις σχέσεις (1), (2), επειδή (5,6)=1, από γνωστό θεώρημα, θα είναι και $5\cdot6=30/(\nu^5-\nu)$.

II. Είναι $\nu^7-\nu=\nu(\nu^6-1)=\nu(\nu^3-1)(\nu^3+1)=\nu(\nu-1)(\nu^2+\nu+1)(\nu+1)(\nu^2-\nu+1)$.

Το ν(ν−1)(ν+1) είναι γινόμενο τριών διαδοχικών ακεραίων, οπότε

$6/\nu(\nu-1)(\nu+1) \Rightarrow 6/(\nu^7-\nu)$ (3).

Από το θεώρημα Fermat θα είναι $\nu^7 \equiv \nu \pmod 7 \Rightarrow 7/(\nu^7-\nu)$ (4).

Από τις σχέσεις (3), (4), επειδή (6,7)=1, από γνωστό θεώρημα, θα είναι και $6\cdot7=42/(\nu^7-\nu)$.

9) Να αποδείξετε ότι για κάθε ζεύγος φυσικών αριθμών (μ, ν) ο αριθμός $\mathbf{\mu\nu(\mu^{60}-\nu^{60})}$ διαιρείται με το 56786730. (Υπόδειξη $56786730=2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot31\cdot61$).

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Αρκεί να αποδείξουμε ότι ο αριθμός αυτός διαιρείται με τους αριθμούς 2,3,5,7,11,13,31,61.

Για τη διαίρεση με το 2 παρατηρούμε ότι αν ένας από τους μ, ν είναι άρτιος τότε ο μν διαιρείται με το 2, ενώ αν οι μ, ν είναι περιττοί ο $\mu^{60}-\nu^{60}$ είναι άρτιος ως διαφορά δύο περιττών.

Για τη διαίρεση με τους υπόλοιπους αριθμούς χρησιμοποιούμε το θεώρημα Fermat.

Για την διαίρεση με το 3 έχουμε:

Αν ένας από τους μ, ν είναι πολλαπλάσιο του 3 τότε το γινόμενο μν διαιρείται με το 3.

Διαφορετικά θα είναι (μ, 3)=(ν, 3)=1, οπότε θα είναι
$\mu^{\rho-1} \equiv \nu^{\rho-1} \equiv 1 \pmod 3 \Rightarrow \mu^2 \equiv \nu^2 \equiv 1 \pmod 3 \Rightarrow \mu^{60} \equiv \nu^{60} \equiv 1 \pmod 3 \Rightarrow 3/\ \mu^{60}-\nu^{60}$.
Για την διαίρεση με το 5 έχουμε:
Αν ένας από τους μ, ν είναι πολλαπλάσιο του 5 τότε το γινόμενο μν διαιρείται με το 5.
Διαφορετικά θα είναι (μ, 5)=(ν, 5)=1, οπότε θα είναι
$\mu^{\rho-1} \equiv \nu^{\rho-1} \equiv 1 \pmod 5 \Rightarrow \mu^2 \equiv \nu^2 \equiv 1 \pmod 5 \Rightarrow \mu^{60} \equiv \nu^{60} \equiv 1 \pmod 5 \Rightarrow 5/\ \mu^{60}-\nu^{60}$.
Όμοια εργαζόμαστε και για τις άλλες περιπτώσεις.
Παρατήρηση: Το 60 είναι πολλαπλάσιο των αριθμών 2, 4, 6, 10, 12, 30, 60.

10) Να αποδείξετε ότι **$91/(\nu^{37}-\nu)$** για κάθε φυσικό ν.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Για ν=1 προφανώς ισχύει. Για ν≥2 έχουμε 91=7·13, οπότε αρκεί να δείξουμε ότι οι 7, 13 διαιρούν το $\nu^{37}-\nu$.
Ο 7 είναι 7 πρώτος και (ν, 7)=1, οπότε από το θεώρημα Fermat θα είναι
$\nu^6 \equiv 1 \pmod 7 \Rightarrow \nu^{36} \equiv 1 \pmod 7 \Rightarrow \nu^{37} \equiv \nu \pmod 7 \Rightarrow 7/\ (\nu^{37}-\nu)$.
Αν (ν, 7)>1, τότε επειδή ο 7 είναι πρώτος θα έχουμε 7/ν, άρα θα διαιρεί και το $\nu^{37}-\nu$.
Όμοια για το 13 και επειδή (7,13)=1 θα είναι $\nu^{37} \equiv \nu \pmod{7\cdot 13} \Rightarrow 91/(\nu^{37}-\nu)$.

11) Έστω ρ πρώτος με ρ>5. Να αποδείξετε ότι **$\rho^8 \equiv 1 \pmod{240}$.**

(ΕΜΕ. Διαιρετότητα και Ισοτιμίες Α, Συγγελάκης)

Απόδειξη

Είναι $240=2^4\cdot 3\cdot 5$.
Από το μικρό θεώρημα του Fermat, έχουμε ότι $\rho^2 \equiv 1 \pmod 3 \Rightarrow \rho^8 \equiv 1 \pmod 3$ (1).
Όμοια $\rho^4 \equiv 1 \pmod 5 \Rightarrow \rho^8 \equiv 1 \pmod 5$ (2).
Ο αριθμός ρ είναι πρώτος και ο 2^4 είναι άρτιος άρα θα είναι $(\rho, 2^4)=1$και επειδή $\varphi(2^4)=\varphi(16)=\mathbf{16\cdot\left(1-\frac{1}{2}\right)=8}$, από το θεώρημα Euler, θα είναι $\rho^8 \equiv 1$ (mo16) (3).
Από τις σχέσεις (1), (2) και (3) θα έχουμε $\rho^8 \equiv 1$ (mo$2^4\cdot 3\cdot 5$)$\Rightarrow \rho^8 \equiv 1$ (mo240).
Παρατήρηση: Μπορούμε να παρατηρήσουμε ότι $n^4 \equiv 1 \pmod{16}$ για $n=\pm 1,\pm 3,\pm 5,\pm 7 \pmod{16}$. Συνεπώς μπορούμε να βελτιώσουμε το αποτέλεσμα της άσκησης σε $\rho^4 \equiv 1$ (mo240) για όλους του πρώτος ρ>5.
Σχόλιο: Μπορούμε να δοκιμάσουμε και με το $540=2^2\cdot 3^3\cdot 5$ με $\rho^{36} \equiv 1 \pmod{540}$.

12) Έστω ρ πρώτος. Να αποδείξετε ότι **$\rho / \alpha b^\rho - b\alpha^\rho$** για όλους τους ακεραίους α, b.

(ΕΜΕ. Διαιρετότητα και Ισοτιμίες Α, Συγγελάκης)

Απόδειξη

Είναι **$\alpha b^\rho - b\alpha^\rho = \alpha b(b^{\rho-1} - \alpha^{\rho-1})$**.

Διακρίνουμε περιπτώσεις:

- Αν ρ/αb τότε **$\rho / \alpha b^\rho - b\alpha^\rho$**.

- Αν ρ∤ αb τότε (ρ, α)=(ρ, b)=1, οπότε από το μικρό θεώρημα Fermat θα έχουμε:

$$b^{\rho-1} \equiv \alpha^{\rho-1} \equiv 1(\mathrm{mod}\,\rho) \Rightarrow \left.\begin{matrix} \rho / b^{\rho-1}-1 \\ \rho / \alpha^{\rho-1}-1 \end{matrix}\right\} \Rightarrow \rho/(b^{\rho-1}-1)-(\alpha^{\rho-1}-1) \Rightarrow$$

$\rho/(b^{\rho-1}-\alpha^{\rho-1}) \Rightarrow \rho/\alpha b(b^{\rho-1}-\alpha^{\rho-1}) \Rightarrow \rho/(\alpha b^{\rho}-b\alpha^{\rho})$, δηλαδή σε κάθε περίπτωση $\rho/\alpha b^{\rho}-b\alpha^{\rho}$.

13) Αν p≠q δύο περιττοί πρώτοι, να αποδείξετε ότι $p^{q-1}+q^{p-1} \equiv 1(\mathrm{mod}\,pq)$.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Επειδή οι p, q είναι πρώτοι έχουμε (p, q)=1, άρα από το θεώρημα Fermat θα είναι $p^{q-1} \equiv 1(\mathrm{mod}\,q)$ και $q^{p-1} \equiv 1(\mathrm{mod}\,p)$ δηλαδή θα έχουμε:

$q/(p^{q-1}-1)$ και $p/(q^{p-1}-1)$ άρα θα είναι $p \cdot q/(p^{q-1}-1)(q^{p-1}-1) \Rightarrow$

$p \cdot q/(p^{q-1} \cdot q^{p-1}-p^{q-1}-q^{p-1}+1) \Rightarrow p \cdot q/(-p^{q-1}-q^{p-1}+1) \Rightarrow$

$p^{q-1}+q^{p-1} \equiv 1(\mathrm{mod}\,pq)$.

14) Αν (α, 627)=1, (β, 627)=1 να δείξετε ότι $\alpha^{90} \equiv \beta^{90} \pmod{627}$.

Λύση

Θα γράψουμε το 627 σε γινόμενο παραγόντων.

Είναι 627=3·11·19 και επειδή (α,627)=1, θα είναι (α,3)=(α,11)=(α,19)=1.

Από το θεώρημα Fermat θα έχουμε:

$\alpha^2 \equiv 1(\mathrm{mod}\,3) \Rightarrow (\alpha^2)^{45} \equiv 1(\mathrm{mod}\,3) \Rightarrow \alpha^{90} \equiv 1(\mathrm{mod}\,3)$

$\alpha^{10} \equiv 1\ (\mathrm{mod}\,11) \Rightarrow (\alpha^{10})^9 \equiv 1(\mathrm{mod}\,11) \Rightarrow \alpha^{90} \equiv 1(\mathrm{mod}\,11)$

$\alpha^{18} \equiv 1\ (\mathrm{mod}\,19) \Rightarrow (\alpha^{18})^5 \equiv 1(\mathrm{mod}\,19) \Rightarrow \alpha^{90} \equiv 1(\mathrm{mod}\,19)$. Είναι ΕΚΠ(2,10,18)=90.

Επειδή οι αριθμοί 3, 11, 19 είναι πρώτοι θα έχουμε:

$\alpha^{90} \equiv 1(\mathrm{mod}\,3\cdot11\cdot19) \Rightarrow \alpha^{90} \equiv 1(\mathrm{mod}\,627)$ (1).

Όμοια θα είναι $\beta^{90} \equiv 1(\mathrm{mod}\,627)$ (2).

Από τις (1), (2) θα έχουμε $\alpha^{90}-\beta^{90} \equiv 0(\mathrm{mod}\,627) \Rightarrow \alpha^{90} \equiv \beta^{90}\ (\mathrm{mod}\,627)$.

15) Να δειχθεί ότι $\alpha^{13}-\alpha \equiv 0(\mathrm{mod}\,2730)$, για κάθε α∈Z.

(Μαθηματικό Αθηνών)

Λύση

Ο αριθμός 2730=2·3·5·7·13, και οι παράγοντες 2, 3, 5, 7, 13 είναι πρώτοι, άρα απο το θεώρημα Fermat θα έχουμε $\alpha^{\rho} \equiv \alpha(\mathrm{mod}\,\rho)$, με ρ πρώτο, για κάθε α∈Z.

Θα είναι $\alpha^2 \equiv \alpha(\mathrm{mod}\,2)$ (1).

Είναι $\alpha^{13} = (\alpha^2)^6\alpha \overset{(1)}{\equiv} \alpha^6\alpha(\mathrm{mod}\,2) \equiv (\alpha^2)^3\alpha(\mathrm{mod}\,2) \overset{(1)}{\equiv} \alpha^3\alpha(\mathrm{mod}\,2)$

$\equiv (\alpha^2)^2 \overset{(1)}{\equiv} \alpha^2(\mathrm{mod}\,2) \overset{(1)}{\equiv} \alpha(\mathrm{mod}\,2)$, δηλαδή $\alpha^{13} \equiv \alpha(\mathrm{mod}\,2)$ (2).

Επίσης θα είναι $\alpha^3 \equiv \alpha(\mathrm{mod}\,3)$ (3).

Είναι $\alpha^{13}=(\alpha^3)^4\alpha \overset{(3)}{\equiv} \alpha^4\alpha(\mathrm{mod}\,3)\equiv(\alpha^3)\alpha^2(\mathrm{mod}\,3)\overset{(3)}{\equiv}\alpha^3(\mathrm{mod}\,3)\overset{(3)}{\equiv}\alpha(\mathrm{mod}\,3)$,

δηλαδή $\alpha^{13}\equiv\alpha(\mathrm{mod}\,3)$ (4).

Όμοια θα είναι $\alpha^5\equiv\alpha(\mathrm{mod}\,5)$ (5).

Είναι $\alpha^{13}=(\alpha^5)^2\alpha^3\overset{(5)}{\equiv}\alpha^2\alpha^3(\mathrm{mod}\,5)\equiv(\alpha^5)(\mathrm{mod}\,5)\overset{(5)}{\equiv}\alpha(\mathrm{mod}\,5)\overset{(5)}{\equiv}\alpha(\mathrm{mod}\,2)$,

δηλαδή $\alpha^{13}\equiv\alpha(\mathrm{mod}\,5)$ (6).

Όμοια θα είναι $\alpha^7\equiv\alpha(\mathrm{mod}\,7)$ (7).

Είναι $\alpha^{13}=(\alpha^7)\alpha^6\overset{(7)}{\equiv}\alpha^7(\mathrm{mod}\,7)\overset{(7)}{\equiv}\alpha(\mathrm{mod}\,7)$, δηλαδή $\alpha^{13}\equiv\alpha(\mathrm{mod}\,7)$ (8).

Από τις σχέσεις (2), (4), (6), (8) και (6) θα είναι $\alpha^{13}\equiv\alpha(\mathrm{mod}\,2730)\Rightarrow$
$\alpha^{13}-\alpha\equiv0(\mathrm{mod}\,2730)$.

16) Να αποδείξετε ότι: $\mathbf{1^{101}+2^{101}+3^{101}+...+101^{101}=0(\mathrm{mod}\,101)}$.

Λύση

Ο αριθμός 101 είναι πρώτος, οπότε θα ισχύει:

$\mathbf{(1+2+...+101)^{101}\equiv 1^{101}+2^{101}+...+101^{101}(\mathrm{mod}\,101)}$ (1).

Ισχύει $\mathbf{1+2+...+101=\frac{100\cdot101}{2}=50\cdot101}$, άρα θα έχουμε

$\mathbf{(1+2+...+101)^{101}=(50\cdot101)^{101}\equiv0(\mathrm{mod}\,101)}$ (2).

Από τις σχέσεις (1) και (2) θα είναι:

$\mathbf{(1+2+...+101)^{101}-(1+2+...+101)^{101}\equiv1^{101}+2^{101}+...+101^{101}(\mathrm{mod}\,101)\Rightarrow}$

$\mathbf{0\equiv1^{101}+2^{101}+...+101^{101}(\mathrm{mod}\,101)\Rightarrow-(1^{101}+2^{101}+...+101^{101})\equiv0(\mathrm{mod}\,101)\Rightarrow}$

$\mathbf{(1^{101}+2^{101}+...+101^{101})\equiv0(\mathrm{mod}\,101)}$

17) Να δειχθεί ότι ο αριθμός $\mathbf{\nu^{22}-\nu^2}$, με $\nu\in N^*$ με $\nu>1$, έχει δύο μηδενικά στο τέλος.

(Μαθηματικό Αθήνας)

Λύση

Αρκεί να αποδείξουμε ότι $100/\ \nu^{22}-\nu^2$.

Είναι $100=2^2\cdot5^2$, οπότε αρκεί να αποδείξουμε ότι $2^2/\ \nu^{22}-\nu^2$ και $5^2/\ \nu^{22}-\nu^2$.

Διακρίνουμε περιπτώσεις για το ν.

- Αν ν άρτιος, τότε $\nu=2\lambda$, οπότε $\nu^{22}-\nu^2=\nu^2(\nu^{20}-1)=4\lambda^2[(2\lambda)^{20}-1]$, δηλαδή $2^2/\ \nu^{22}-\nu^2$.
- Αν ν περιττός, τότε $(\nu,4)=1$ (άρτιος-περιττός), οπότε από το θεώρημα του Euler θα είναι $\nu^{\varphi(4)}\equiv1(\mathrm{mod}\,4)\Leftrightarrow\nu^2\equiv1(\mathrm{mod}\,4)\Leftrightarrow4/\nu^2-1$ (1).

Είναι $\nu^{22}-\nu^2=\nu^2(\nu^{20}-1)=\nu^2[(\nu^4)^5-1]=\nu^2(\nu^4-1)[(\nu^4)^4+(\nu^4)^3+(\nu^4)^2+(\nu^4)+1]=$
$\nu^2(\nu^2-1)(\nu^2+1)[(\nu^4)^4+(\nu^4)^3+(\nu^4)^2+(\nu^4)+1]$ και λόγω της (1) θα έχουμε ότι $4/\ \nu^{22}-\nu^2$.

Τελικά για κάθε $\nu\in N^*$ με $\nu>1$ έχουμε $4/\ \nu^{22}-\nu^2$.

Αρκεί και το $5^2/\ \nu^{22}-\nu^2$.

Έστω ότι $(\nu,5)\neq1$, επειδή το 5 είναι πρώτος θα είναι $5/\nu\Rightarrow5^2/\nu^2\Rightarrow5^2/\nu^2(\nu^{20}-1)$.

Έστω ότι $(\nu,5)=1$, τότε από το θεώρημα του Euler θα έχουμε $\nu^{\varphi(25)}\equiv1(\mathrm{mod}\,25)\Leftrightarrow$

$\nu^{20} \equiv 1(\text{mod } 25) \Leftrightarrow 25/\nu^{20}-1 \Leftrightarrow 25/\nu^2(\nu^{20}-1) \Leftrightarrow 25/(\nu^{22}-\nu^2)$ (2).
Από τις (1), (2) έχουμε το ζητούμενο.

18) Να βρεθούν όλα τα δυνατά υπόλοιπα της διαίρεσης του αριθμού
$A=2\cdot 3^n+3\cdot 7^{n+1}+5^{3n+1}-7$ δια του 11.

(ΕΜΕ. Διαιρετότητα και Ισοτιμίες, Α Συγκελάκης)

Λύση

Είναι (11,3)=(11,7)=(11,5)=1, οπότε από το μικρό θεώρημα του Fermat, θα έχουμε:
$3^{11-1} \equiv 1(\text{mod } 11)$, $7^{11-1} \equiv 1(\text{mod } 11)$, $5^{11-1} \equiv 1(\text{mod } 11)$.
Επειδή είναι φ(11)=10, το υπόλοιπο της διαίρεσης του 3^n, 7^n, 5^n με το 11 θα επαναλαμβάνεται το πολύ κάθε 10 βήματα και μάλιστα το βήμα της επανάληψης (πόρισμα 2.2), θα είναι διαιρέτης του 10 (Δ(10)=1,2,5,10).
Επειδή το υπόλοιπο της διαίρεσης των 3^n, 7^n, 5^n με το 11 θα επαναλαμβάνεται το πολύ κάθε 10 βήματα θα γράψουμε το n στη μορφή n=10κ+υ, με υ=0,1,2,3,4,5,6,7,8,9 και στη συνέχεια θα κατασκευάσουμε ένα πίνακα δυνάμεων για βρούμε για τις διάφορες τιμές του υ την παράσταση A.

υ=n (mod 10) ή n (mod 10)	0	1	2	3	4	5	6	7	8	9	Επανάληψη ανά
n+1 (mod 10)	1	2	3	4	5	6	7	8	9	0	.....
3n+1 (mod 10)	1	2	3	4	5	6	7	8	9	0	.....
3^n (mod 11)	1	3	9	5	4	1	3	9	5	4	5
$2\cdot 3^n$ (mod 11)	**2**	**6**	**7**	**10**	**8**	**2**	**6**	**7**	**10**	**8**	**5**
7^n (mod 11)	1	7	5	2	3	10	4	6	9	8	10
$3\cdot 7^n$ (mod 11)	**10**	**4**	**6**	**9**	**8**	**1**	**7**	**5**	**2**	**3**	**10**
5^n (mod 11)	1	5	3	4	9	1	5	3	4	9	5
5^{3n+1} (mod 11)	**5**	**9**	**3**	**1**	**4**	**5**	**9**	**3**	**1**	**4**	**5**
A	**10**	**1**	**9**	**2**	**2**	**1**	**4**	**8**	**6**	**8**	**...**

Όπως λοιπόν φαίνεται από τον παραπάνω πίνακα ο αριθμός A δεν διαιρείται από το 11. , για κάθε τιμή του $n \in N^*$.

Παρατηρήσεις

1. Όπως φαίνεται από τον παραπάνω πίνακα μπορούμε να συμπεράνουμε ότι αν ο n είναι της μορφής n=2κ+2, τότε όταν ο A διαιρεθεί με το 11, αφήνει υπόλοιπο 9. Δηλαδή δημιουργούμε διάφορες ασκήσεις με τη βοήθεια του παραπάνω πίνακα.
2. Άσκηση. Να αποδειχθεί ότι αν το τελευταίο ψηφίο του αριθμού n είναι το 2 τότε ο αριθμός A αφήνει υπόλοιπο 9 όταν διαιρεθεί με το 11.

19) Να δείξετε ότι εάν $n \neq 0(\text{mod } 6)$ τότε **$1^n+2^n+3^n+4^n+5^n+6^n \equiv 0(\text{mod } 7)$.**

(ΕΜΕ. Διαιρετότητα και Ισοτιμίες, Α Συγκελάκης)

Λύση

Είναι (7,2)=(7,3)=(7,4)=(7,5)=(7,6)=1 και φ(7)=6 οπότε από το θεώρημα του Euler, θα έχουμε: $\alpha^{\varphi(7)1}\equiv 1(\text{mod } 7)$.

Άρα το υπόλοιπο της διαίρεσης του 1^n, 2^n, 3^n, 4^n, 5^n, 6^n με το 7 θα επαναλαμβάνεται το πολύ κάθε 6 βήματα και μάλιστα το βήμα της επανάληψης (πόρισμα 2.2), θα είναι διαιρέτης του 6 (Δ(6)=1,2,3,6).

Γράφουμε το n στη μορφή n=6κ+υ, με υ=1,2,3,4,5, διότι $n\neq 0(\text{mod } 6)$ και στη συνέχεια θα κατασκευάσουμε ένα πίνακα δυνάμεων για βρούμε για τις διάφορες τιμές του υ την παράσταση A.

n (mod 6)	1	2	3	4	5
1^n (mod 7)	1	1	1	1	1
2^n (mod 7)	2	4	1	2	4
3^n (mod 7)	3	2	6	4	5
4^n (mod 7)	4	2	1	4	2
5^n (mod 7)	5	4	6	2	3
6^n (mod 7)	6	1	6	1	2
A	**0**	**0**	**0**	**0**	**0**

Όπως λοιπόν φαίνεται από τον παραπάνω πίνακα ο αριθμός Α διαιρείται από το 7, για κάθε τιμή του $n\in N^*$.

§ 2.4 Το θεώρημα Wilson

Το παρακάτω θεώρημα αποτελεί ένα από τα λίγα καθολικά κριτήρια πρώτων αριθμών, το οποίο ωστόσο είναι ιδιαίτερα δύσχρηστο λόγω των μεγάλων αριθμών που προκύπτουν. (ΕΜΕ Θεωρία Αριθμών)

Θεώρημα Wilson
Ο φυσικός αριθμός ρ>2 είναι πρώτος αν και μόνο αν **$(\rho-1)! \equiv -1 \pmod{\rho}$.**

Πόρισμα
Για κάθε πρώτο φυσικό αριθμό ρ ισχύει **$(\rho-2)! \equiv 1 \pmod{\rho}$.**
Απόδειξη
Ισχύει $(\rho-1)! \equiv -1 \pmod{\rho} \Rightarrow (\rho-2)!(\rho-1) \equiv -1 \pmod{\rho} \Rightarrow \rho\,(\rho-2)! - (\rho-2)! \equiv -1 \pmod{\rho}$ (1).
Επειδή $\rho / \rho(\rho-2)!$ θα είναι $\rho\,(\rho-2)! \equiv -1 \pmod{\rho}$, οπότε από τη σχέση (1) θα έχουμε ότι $-(\rho-2)! \equiv -1 \pmod{\rho} \Rightarrow (\rho-2)! \equiv 1 \pmod{\rho}$.

Παραδείγματα

1) $(5-1)! = 4! = 24 \equiv -1 \pmod{5}$, άρα ο 5 είναι πρώτος.

2) $(8-1)! = 7! = 5040 \equiv 0 \pmod{8}$, άρα ο 8 δεν είναι πρώτος.

3) Αν ρ είναι ένας περιττός πρώτος, να αποδείξετε ότι $2(\rho-3)! \equiv -1 \pmod{\rho}$.
(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Από το θεώρημα Wilson θα έχουμε:
$(\rho-1)! \equiv -1 \pmod{\rho} \Rightarrow (\rho-3)!(\rho-2)(\rho-1) \equiv -1 \pmod{\rho}$ (1).
Είναι $(\rho-2) \equiv -2 \pmod{\rho}$ και $(\rho-1) \equiv -1 \pmod{\rho}$. οπότε η (1) γίνεται
$(\rho-3)!(-2)(-1) \equiv -1 \pmod{\rho} \Rightarrow (\rho-3)! \cdot 2 \equiv -1 \pmod{\rho} \Rightarrow 2(\rho-3)! \equiv -1 \pmod{\rho}$.

4) Να αποδείξετε ότι $\rho / (\alpha^{\rho} + (\rho-1)!\alpha)$ όπου ρ περιττός πρώτος και α ακέραιος με $(\alpha, \rho)=1$.
(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Από το θεώρημα του Fermat έχουμε $\alpha^{\rho-1} \equiv 1 \pmod{\rho} \Rightarrow \alpha^{\rho} \equiv \alpha \pmod{\rho}$ (1).
Από το θεώρημα Wilson έχουμε $(\rho-1)! \equiv -1 \pmod{\rho} \Rightarrow (\rho-1)!\alpha \equiv -\alpha \pmod{\rho}$ (2),
Από τις (1), (2) θα έχουμε $\alpha^{\rho} + (\rho-1)!\alpha \equiv 0 \pmod{\rho}$.

§ 2.5 Το τελευταίο ψηφίο Αριθμού

- Έστω $\mathbf{A=\alpha_\nu\cdot 10^\nu+\alpha_{\nu-1}\cdot 10^{\nu-1}+...+\alpha_2\cdot 10^2+\alpha_1\cdot 10+\alpha_o}$, ένα φυσικός αριθμός που είναι γραμμένος με τη δεκαδική του παράσταση. Προφανώς το τελευταίο ψηφίου του Α είναι το α_o, για το οποίο μπορούμε να παρατηρήσουμε ότι ισχύει:

$\mathbf{A-\alpha_o=\alpha_\nu\cdot 10^\nu+\alpha_{\nu-1}\cdot 10^{\nu-1}+...+\alpha_2\cdot 10^2+\alpha_1\cdot 10\Leftrightarrow A-\alpha_o=πολ10\Leftrightarrow}$

$\mathbf{A\equiv\alpha_o\ (mod\ 10)}$ (1).

Η σχέση (1) μας δείχνει έναν τρόπο για να υπολογίσουμε το τελευταίο ψηφίο ενός αριθμού Α, αρκεί να βρούμε ένα αριθμό $\beta\in\{0,1,2,3,4,5,6,7,8,9\}$, τέτοιο ώστε $A\equiv\beta(\text{mod }10)$.

Παραδείγματα

1) Να βρείτε το τελευταίο ψηφίο του αριθμού $\mathbf{2019^{101}}$.

Λύση

Είναι $2019=10\cdot 201+9$, οπότε θα έχουμε $2019\equiv 9(\text{mod }10)\Rightarrow 2019^{101}\equiv 9^{101}\ (\text{mod }10)$ (1).

Θα υπολογίσουμε το τελευταίο ψηφίο του αριθμού 9^{101}.

Θα είναι $9\equiv(-1)(\text{mod }10)\Rightarrow 9^{100}\equiv(-1)^{100}(\text{mod }10)\Rightarrow 9^{100}\equiv 1(\text{mod }10)\Rightarrow 9^{101}\equiv 9(\text{mod }10)$, και λόγω της (1) το τελευταίο ψηφίο του αριθμού 2019^{101} θα είναι το 9.

($2^{ος}$ τρόπος)

Είναι $(2010+9)^{101}=(πολ10+9)^{101}=πολ10+9^{101}=πολ10+(10-1)^{101}=πολ10+(-1)^{101}=πολ10-1=πολ10-10+9=πολ10+9$. Άρα το τελευταίο ψηφίο είναι το 9.

2) Να βρείτε το τελευταίο ψηφίο του αριθμού $\mathbf{19^{12}\cdot 9999^{21}}$.

Λύση

Είναι $199=10\cdot 19+9$, οπότε θα έχουμε $199\equiv 9(\text{mod }10)\Rightarrow 199^{12}\equiv 9^{12}\ (\text{mod }10)$ (1).

Θα υπολογίσουμε το τελευταίο ψηφίο του αριθμού 9^{12}.

Θα είναι $9\equiv(-1)(\text{mod }10)\Rightarrow 9^{12}\equiv(-1)^{12}(\text{mod }10)\Rightarrow 9^{12}\equiv 1(\text{mod }10)$ και λόγω της (1) θα έχουμε $199^{12}\equiv 1(\text{mod }10)$, άρα το τελευταίο ψηφίο του αριθμού 199^{12} θα είναι το 1.

Είναι $9999=10\cdot 999+9$, οπότε θα έχουμε $9999\equiv 9(\text{mod }10)\Rightarrow 9999^{21}\equiv 9^{21}\ (\text{mod }10)$ (2).

Θα υπολογίσουμε το τελευταίο ψηφίο του αριθμού 9^{21}.

Θα είναι $9\equiv(-1)(\text{mod }10)\Rightarrow 9^{20}\equiv(-1)^{20}(\text{mod }10)\Rightarrow 9^{20}\equiv 1(\text{mod }10)\Rightarrow 9^{21}\equiv 9(\text{mod }10)$ και λόγω της (2) θα έχουμε $9999^{21}\equiv 9(\text{mod }10)$, άρα το τελευταίο ψηφίο του αριθμού 9999^{21} θα είναι το 9. Άρα τελικά το τελευταίο ψηφίο του γινομένου $19^{12}\cdot 9999^{21}$, θα είναι το 9.

- Με την ίδια λογική μπορούμε να βρούμε τα δύο τελευταία ψηφία του φυσικού αριθμού **Α**.

Έστω ο φυσικός αριθμός $\mathbf{A=\alpha_\nu\cdot 10^\nu+\alpha_{\nu-1}\cdot 10^{\nu-1}+...+\alpha_2\cdot 10^2+\alpha_1\cdot 10+\alpha_o}$, γραμμένος στη δεκαδική του παράσταση. Προφανώς τα δύο τελευταία ψηφία του Α προκύπτουν από το άθροισμα $\alpha_1\cdot 10+\alpha_o$, για το οποίο ισχύει:

$\mathbf{A-(10\alpha_1+\alpha_o)=\alpha_\nu\cdot 10^\nu+\alpha_{\nu-1}\cdot 10^{\nu-1}+...+\alpha_2\cdot 10^2\Leftrightarrow A-(10\alpha_1+\alpha_o)=\pi o\lambda 10\Leftrightarrow}$

$\mathbf{A\equiv 10\alpha_1+\alpha_o\ (mod\ 10)}$ (2).

Η σχέση (2) μας δείχνει έναν τρόπο για να υπολογίσουμε τα δύο τελευταία ψηφία ενός αριθμού Α, αρκεί να βρούμε ένα αριθμό $\beta\in\{0,1,2,....,98,99\}$ τέτοιο ώστε $A\equiv\beta(mod\ 100)$.

Παραδείγματα

1) Τα δύο τελευταία ψηφία των φυσικών αριθμών α, β και γ είναι 79, 35 και 87 αντίστοιχα. Να βρεθούν τα δύο τελευταία ψηφία των αριθμών α+β+γ, α–7β+γ, α·β·γ.

Λύση

Είναι $\alpha\equiv 79(mod\ 100)$, $\beta\equiv 35(mod\ 100)$, $\gamma\equiv 87(mod\ 100)$.

Είναι $\alpha+\beta+\gamma\equiv(79+35+87)(mod\ 100)\Leftrightarrow\alpha+\beta+\gamma\equiv 201(mod\ 100)\Leftrightarrow\ \alpha+\beta+\gamma\equiv 1(mod\ 100)$, άρα τα δύο τελευταία ψηφία του α+β+γ είναι 01.

Είναι $\alpha-7\beta+\gamma\equiv(79-7\cdot 35+87)(mod\ 100)\Leftrightarrow\alpha-7\beta+\gamma\equiv -79(mod\ 100)\Leftrightarrow$

$\alpha-7\beta+\gamma\equiv 21(mod\ 100)$, άρα τα δύο τελευταία ψηφία του α–7β+γ είναι 21.

Είναι $\alpha\cdot\beta\cdot\gamma\equiv(79\cdot 35\cdot 87)(mod\ 100)\Leftrightarrow\ \alpha\cdot\beta\cdot\gamma\equiv 240555(mod\ 100)\Leftrightarrow\ \alpha\cdot\beta\cdot\gamma\equiv 55(mod\ 100)$, άρα τα δύο τελευταία ψηφία του α·β·γ είναι 55.

2) Μα βρείτε τα δύο τελευταία ψηφία του αριθμού $\mathbf{9999^{2019}}$.

Λύση

Αρκεί να βρούμε ένα αριθμό $\beta\in\{0,1,2,....,98,99\}$ τέτοιο ώστε $9999^{2019}\equiv\beta(mod\ 100)$.

Είναι $9999\equiv 99(mod\ 100)\Rightarrow\ 9999\equiv(-1)(mod\ 100)\Rightarrow\ 9999^{2018}\equiv(-1)^{2018}\ (mod\ 100)\Rightarrow$ $9999^{2018}\equiv 1(mod\ 100)\Rightarrow\ 9999^{2018}\cdot 9999\equiv 9999(mod\ 100)\Rightarrow\ 9999^{2019}\equiv 9999(mod\ 100)\Rightarrow\ 9999^{2019}\equiv 99(mod\ 100)$, επομένως τα δύο τελευταία ψηφία του αριθμού 9999^{2019} είναι το 99.

3) Ποιά είναι τα δύο τελευταία ψηφία του $\mathbf{11^{402}}$.

Λύση

Πρέπει να βρούμε έναν αριθμό β τέτοιο ώστε $11^{400}\equiv\beta(mod\ 100)$, με β=0,1,2,...,99.

Είναι 100=4·25, μπορούμε να δουλέψουμε με mod4 και mod25.

Είναι $25=5^2$, άρα $\mathbf{\phi(25)=25\left(1-\frac{1}{5}\right)=20}$, οπότε από το θεώρημα Euler θα έχουμε:

$11^{20}\equiv 1(mod\ 25)$ (1).

Όμοια φ(4)=2, οπότε από το θεώρημα Euler θα έχουμε:$11^2\equiv 1(mod\ 4)\Rightarrow\ 11^{20}\equiv 1(mod\ 4)$ (2).

Είναι (25,4)=1, άρα από θεώρημα θα έχουμε $11^{20} \equiv 1(\text{mod } 100) \Rightarrow 11^{400} \equiv 1(\text{mod } 100) \Rightarrow 11^{402} \equiv 11^2 (\text{mod } 100) \Rightarrow 11^{402} \equiv 121 (\text{mod } 100)$, δηλαδή τα δύο τελευταία ψηφία του 11^{401} είναι το 21.

4) Να βρείτε τα δύο τελευταία ψηφία του αριθμού $\mathbf{7^{2019}}$.

Λύση

Αρκεί να βρούμε ένα αριθμό $\beta \in \{0,1,2,....,98,99\}$ τέτοιο ώστε $7^{2019} \equiv \beta(\text{mod } 100)$.

Βρίσκουμε τα δύο τελευταία ψηφία των δυνάμεων του 7.

Είναι $7=\mathbf{07}$, $7^2=\mathbf{49}$, $7^3=3\mathbf{43}$, $7^4=24\mathbf{01}$, $7^5=168\mathbf{07}$, $7^6=11764\mathbf{9}$, $7^7=8235\mathbf{43}$, $7^8=57648\mathbf{01}$, δηλαδή τα δύο τελευταία ψηφία ξαναεμφανίζονται με περίοδο 4.

Είναι $7^4 \equiv 1(\text{mod } 10)$ και επειδή $2019=4\cdot 504+3$, θα έχουμε $7^{2019}=7^{4\cdot 504+3}=(7^4)^{504}\cdot 7^3$.

Άρα $7^4 \equiv 1(\text{mod } 10) \Rightarrow (7^4)^{504} \equiv 1(\text{mod } 10) \Rightarrow (7^4)^{504}\cdot 7^3 \equiv 7^3 (\text{mod } 10)$, επομένως τα δύο τελευταία ψηφία του 7^{2019} είναι ίδια με τα τελευταία ψηφία του $7^3=3\mathbf{43}$, δηλαδή θα είναι 43.

Γενικά: Αν $\alpha \equiv \upsilon(\text{mod } 10^{\nu})$ με $0 \le \upsilon < 10^{\nu}$, τότε τα τελευταία ν ψηφία του αριθμού α είναι το υ με τόσα μηδενικά στην αρχή, όσα χρειάζονται ώστε το μήκος του αριθμού υ να ίσο με ν.

§ 2.5 Κριτήρια διαιρετότητας

Στην παράγραφο αυτή θα δούμε πως μπορούμε να κατασκευάσουμε κριτήρια διαιρετότητας χρησιμοποιώντας τις ισοτιμίες.

Ας εξετάσουμε για παράδειγμα την περίπτωση τη διαίρεσης ενός ακεραίου Ν με το 11.

Είναι $\mathbf{N = \overline{\alpha_\nu \alpha_{\nu-1} ... \alpha_1 \alpha_o} = \alpha_\nu \cdot 10^\nu + \alpha_{\nu-1} \cdot 10^{\nu-1} + ... + \alpha_2 \cdot 10^2 + \alpha_1 \cdot 10 + \alpha_o}$, οπότε θέλουμε να διερευνήσουμε την περίπτωση για την οποία ισχύει $\mathbf{N \equiv 0(\text{mod } 11)}$.

Είναι $\mathbf{10^o \equiv 1(\text{mod } 11)}$,

$\mathbf{10^1 \equiv -1(\text{mod } 11)}$

$\mathbf{10^2 \equiv 1(\text{mod } 11)}$

$\mathbf{10^3 \equiv 10(\text{mod } 11) \Rightarrow 10^3 \equiv -1(\text{mod } 11)}$

$\mathbf{10^4 \equiv 1(\text{mod } 11)}$, δηλαδή οι άρτιες δυνάμεις του 10 είναι −1 (mod11) και οι περιττές 1 (mod11). Ας εξετάσουμε για παράδειγμα αν ο αριθμός 2345067 διαιρείται με το 11.

Είναι $\mathbf{N = 2345067 = 2 \cdot 10^6 + 3 \cdot 10^5 + 4 \cdot 10^4 + 5 \cdot 10^3 + 0 \cdot 10^2 + 6 \cdot 10 + 7}$ τότε θα έχουμε:

$\mathbf{10^o \equiv 1(\text{mod } 11) \Rightarrow 7 \cdot 1 \equiv 7(\text{mod } 11)}$

$\mathbf{10^1 \equiv -1(\text{mod } 11) \Rightarrow 6 \cdot 10^1 \equiv -6(\text{mod } 11)}$

$\mathbf{10^2 \equiv 1(\text{mod } 11) \Rightarrow 0 \cdot 10^1 \equiv 0(\text{mod } 11)}$

$10^3 \equiv -1(\mathrm{mod}\,11) \Rightarrow 5\cdot 10^1 \equiv -5(\mathrm{mod}\,11)$

$10^4 \equiv 1(\mathrm{mod}\,11) \Rightarrow 4\cdot 10^4 \equiv 4(\mathrm{mod}\,11)$

$10^5 \equiv -1(\mathrm{mod}\,11) \Rightarrow 3\cdot 10^5 \equiv -3(\mathrm{mod}\,11)$

$10^6 \equiv 1(\mathrm{mod}\,11) \Rightarrow 2\cdot 10^6 \equiv 2(\mathrm{mod}\,11)$, άρα N ≡(7–6+0–5+4–3+2) (mod 11)⇒
N ≡(–1) (mod 11), οπότε ο αριθμός N δεν διαιρείται με το 11.
Όμοια για την περίπτωση της διαίρεσης ενός ακεραίου N με το 7 θα έχουμε:
$\mathbf{N = \overline{\alpha_\nu \alpha_{\nu-1} ... \alpha_1 \alpha_o} = \alpha_\nu \cdot 10^\nu + \alpha_{\nu-1} \cdot 10^{\nu-1} + ... + \alpha_2 \cdot 10^2 + \alpha_1 \cdot 10 + \alpha_o}$.

Είναι $10^o \equiv 1(\mathrm{mod}\,7)$,

$10^1 \equiv 3(\mathrm{mod}\,7)$

$10^2 \equiv 2(\mathrm{mod}\,7)$

$10^3 \equiv 6(\mathrm{mod}\,7) \Rightarrow 10^3 \equiv -1(\mathrm{mod}\,7)$

$10^4 \equiv 4(\mathrm{mod}\,7) \Rightarrow 10^4 \equiv -3(\mathrm{mod}\,7)$

$10^5 \equiv 5(\mathrm{mod}\,7) \Rightarrow 10^5 \equiv -2(\mathrm{mod}\,7)$

$10^6 \equiv 1(\mathrm{mod}\,7)$, δηλαδή όλα τα υπόλοιπα επαναλαμβάνονται περιοδικά με περίοδο 6.

Θα μπορούσαμε να διαπιστώσουμε και από το θεώρημα Fermat ότι $10^6 \equiv 1(\mathrm{mod}\,7)$, διότι το 7 είναι πρώτος.
Για παράδειγμα να εξετάσουμε αν ο αριθμός N=98778965401234 διαιρείται με το 7.

Ο $N=9\cdot 10^{13}+8\cdot 10^{12}+7\cdot 10^{11}+7\cdot 10^{10}+8\cdot 10^9+9\cdot 10^8+6\cdot 10^7+5\cdot 10^6+4\cdot 10^5+0+1\cdot 10^3+2\cdot 10^2+3\cdot 10+4$
οπότε θα είναι:
N≡(9·3+8·1+7·(–2)+7·(–3)+8·(–1)+9·2+6·3+5·1+4·(–2)+0+1·(–1)+2·2+3·3+4)(mod11)⇒.
N≡(27+8–14–21–8+18+18+5–8–1+4+9+4)(mod11)⇒ N≡41(mod11) N≡8(mod11).

Θα μπορούσαμε να χωρίσουμε τον αριθμό N σε εξάδες, από το τέλος προς την αρχή

9	8	7	7	8	9	6	5	4	0	1	2	3	4
3	1	–2	–3	–1	2	3	1	–2	–3	–1	2	3	1

Τα αθροίσματα των γινομένων είναι:
9·3+8·1+7·(–2)+7·(–3)+8·(–1)+9·2+6·3+5·1+4·(–2)+0+1·(–1)+2·2+3·3+4=41

Εφαρμογές

1) Να αποδειχθεί ότι για κάθε φυσικό ν το τελευταίο ψηφίο του $\mathbf{\nu^2}$ είναι ένα από τα ψηφία **0,1,4,5,6,9.**

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Το τελευταίο ψηφίο του ν^2 είναι ένα φυσικός υ για τον οποίον ισχύει: $\nu^2 \equiv \upsilon (\text{mod } 10)$ με $0 \leq \upsilon < 10$.

Διακρίνουμε περιπτώσεις για το ν:

- Αν $\nu \equiv 0 (\text{mod } 10)$, τότε $\nu^2 \equiv 0 (\text{mod } 10)$.
- Αν $\nu \equiv 1 (\text{mod } 10)$, τότε $\nu^2 \equiv 1 (\text{mod } 10)$.
- Αν $\nu \equiv 2 (\text{mod } 10)$, τότε $\nu^2 \equiv 4 (\text{mod } 10)$.
- Αν $\nu \equiv 3 (\text{mod } 10)$, τότε $\nu^2 \equiv 9 (\text{mod } 10)$.
- Αν $\nu \equiv 4 (\text{mod } 10)$, τότε $\nu^2 \equiv 16 (\text{mod } 10) \Rightarrow \nu^2 \equiv 6 (\text{mod } 10)$.
- Αν $\nu \equiv 5 (\text{mod } 10)$, τότε $\nu^2 \equiv 25 (\text{mod } 10)) \Rightarrow \nu^2 \equiv 5 (\text{mod } 10)$.
- Αν $\nu \equiv 6 (\text{mod } 10)$, τότε $\nu^2 \equiv 36 (\text{mod } 10)) \Rightarrow \nu^2 \equiv 6 (\text{mod } 10)$.
- Αν $\nu \equiv 7 (\text{mod } 10)$, τότε $\nu^2 \equiv 49 (\text{mod } 10)) \Rightarrow \nu^2 \equiv 9 (\text{mod } 10)$.
- Αν $\nu \equiv 8 (\text{mod } 10)$, τότε $\nu^2 \equiv 64 (\text{mod } 10)) \Rightarrow \nu^2 \equiv 4 (\text{mod } 10)$.
- Αν $\nu \equiv 9 (\text{mod } 10)$, τότε $\nu^2 \equiv 81 (\text{mod } 10)) \Rightarrow \nu^2 \equiv 1 (\text{mod } 10)$.

2) Να αποδείξετε ότι κάθε ακέραιος ικανοποιεί μία τουλάχιστον από τις παρακάτω ισοτιμίες:

$x \equiv 0 (\text{mod } 2)$, $x \equiv 0 (\text{mod } 3)$, $x \equiv 1 (\text{mod } 4)$, $x \equiv 1 (\text{mod } 6)$, $x \equiv 11 (\text{mod } 12)$.

(Θεωρία Αριθμών ΕΜΕ)

Απόδειξη

Κάθε ακέραιος αριθμός γράφεται σε μία από τις μορφές $x \equiv 0, 1, 2, ..., 11 (\text{mod } 12)$.

Αν $x \equiv 0, 2, 4, 6, 8, 10 (\text{mod } 12)$ τότε $x \equiv 0 (\text{mod } 2)$.

Αν $x \equiv 3, 9 (\text{mod } 12)$ τότε $x \equiv 0 (\text{mod } 3)$.

Αν $x \equiv 1, 5 (\text{mod } 12)$ τότε $x \equiv 1 (\text{mod } 4)$.

Αν $x \equiv 7 (\text{mod } 12)$ τότε $x \equiv 1 (\text{mod } 6)$.

Παρατηρούμε ότι οι αρχικές ισοτιμίες καλύπτουν όλους του ακεραίους.

3) Έστω α τυχαίος ακέραιος αριθμός. Τότε

i. $\mathbf{\alpha^2 \equiv 0, 1, 4 (\text{mod } 5)}$

ii. $\mathbf{\alpha^4 \equiv 0, 1 (\text{mod } 5)}$.

Απόδειξη

i. Κάθε ακέραιος αριθμός α γράφεται σε μία από τις μορφές $\alpha \equiv 0, 1, 2, 3, 4 (\text{mod } 5)$.

Άρα $\alpha^2 \equiv 0, 1, 4, 9, 16 (\text{mod } 5) \Rightarrow \alpha^2 \equiv 0, 1, 4, 9, 16 (\text{mod } 5)$.

Είναι $\alpha^2 \equiv 9 \pmod 5 \Rightarrow 5/\alpha^2-9 \Rightarrow \alpha^2-9=5\pi \Rightarrow \alpha^2=5\pi+9 \Rightarrow \alpha^2=5\pi+5+4 \Rightarrow \alpha^2=5\lambda+4 \Rightarrow \alpha^2 \equiv \pmod 5$. Όμοια θα είναι $\alpha^2 \equiv 16 \pmod 5 \Rightarrow 5/\alpha^2-16 \Rightarrow \alpha^2-16=5\mu \Rightarrow \alpha^2=5\mu+16 \Rightarrow \alpha^2=5\pi+15+1 \Rightarrow \alpha^2=5\psi+1 \Rightarrow \alpha^2 \equiv 1 \pmod 5$. Τελικά $\alpha^2 \equiv 0, 1, 4 \pmod 5$.

ii. Επειδή $\alpha^2 \equiv 0, 1, 4 \pmod 5 \Rightarrow \alpha^4 \equiv 0, 1, 16 \pmod 5 \Rightarrow \alpha^4 \equiv 0, 1 \pmod 5$.

4) Έστω α τυχαίου ακέραιος αριθμός. Τότε **$\alpha^2 \equiv 0, 1 \pmod 4$.**

Απόδειξη

Κάθε ακέραιος αριθμός α γράφεται σε μία από τις μορφές $\alpha \equiv 0, 1, 2, 3 \pmod 4$.

Άρα $\alpha^2 \equiv 0, 1, 4, 9 \pmod 4 \Rightarrow \alpha^2 \equiv 0, 1 \pmod 4$.

Διότι είναι $\alpha^2 \equiv 4 \pmod 4 \Rightarrow \alpha^2 \equiv 0 \pmod 4$ και $\alpha^2 \equiv 9 \pmod 4 \Rightarrow \alpha^2 \equiv 1 \pmod 4$.

5) Να βρεθεί το υπόλοιπο της διαίρεσης των αριθμών $\mathbf{5^\nu}$ και $\mathbf{4^\nu}$ με το 7.

Λύση

Στόχος είναι να βρούμε μια ισοτιμία $\alpha \equiv \beta \pmod 7$ με $\beta=1$ ή $\beta=-1$ και $\alpha=5^\nu$ ή 4^ν.

Πρώτα για το 5^ν.

Είναι $5 \equiv 5 \pmod 7$

$5^2 \equiv 25 \pmod 7 \Rightarrow 5^2 \equiv 4 \pmod 7$,

$5^3 \equiv 20 \pmod 7 \Rightarrow 5^3 \equiv (-1) \pmod 7 \Rightarrow (5^3)^2 \equiv (-1)^2 \pmod 7 \Rightarrow 5^6 \equiv 1 \pmod 7$.

Επειδή $5^6 \equiv 1 \pmod 7$ θα είναι $\nu=6\lambda+\upsilon$, με $\upsilon=0,1,2,3,4,5$, οπότε $5^\nu=5^{6\lambda+\upsilon}=5^{6\lambda} \cdot 5^\upsilon=(5^6)^\lambda \cdot 5^\upsilon$.

Επειδή $5^6 \equiv 1 \pmod 7 \Rightarrow (5^6)^\lambda \equiv 1 \pmod 7 \Rightarrow 5^{6\lambda+\upsilon} \equiv 5^\upsilon \pmod 7 \Rightarrow 5^\nu \equiv 5^\upsilon \pmod 7$.

Για $\upsilon=0$ θα είναι $5^\nu \equiv 1 \pmod 7$.

Για $\upsilon=1$ θα είναι $5^\nu \equiv 5 \pmod 7$.

Για $\upsilon=2$ θα είναι $5^\nu \equiv 25 \pmod 7 \Rightarrow 5^\nu \equiv 4 \pmod 7$.

Για $\upsilon=3$ θα είναι $5^\nu \equiv 125 \pmod 7 \Rightarrow 5^\nu \equiv 6 \pmod 7$.

Για $\upsilon=4$ θα είναι $5^\nu \equiv 625 \pmod 7 \Rightarrow 5^\nu \equiv 2 \pmod 7$.

Για $\upsilon=5$ θα είναι $5^\nu \equiv 3125 \pmod 7 \Rightarrow 5^\nu \equiv 3 \pmod 7$.

Από τα παραπάνω φαίνεται ότι το υπόλοιπο της διαίρεσης του αριθμού 5^ν με τον αριθμό 7 είναι 1 ή 2 ή 3 ή 4 ή 5 ή 6, ανάλογα με τη μορφή του ν.

Για το 4^ν.

Είναι $4 \equiv 4 \pmod 7$

$4^2 \equiv 16 \pmod 7 \Rightarrow 4^2 \equiv 2 \pmod 7$,

$4^3 \equiv 64 \pmod 7 \Rightarrow 4^3 \equiv 1 \pmod 7$.

Επειδή $4^3 \equiv 1 \pmod 7$ θα είναι $\nu=3\mu+\upsilon$, με $\upsilon=0,1,2$, οπότε $4^\nu=4^{3\mu+\upsilon}=4^{3\mu} \cdot 4^\upsilon=(4^3)^\mu \cdot 4^\upsilon$.

Επειδή $4^3 \equiv 1 \pmod 7 \Rightarrow (4^3)^\mu \equiv 1 \pmod 7 \Rightarrow 4^{3\mu+\upsilon} \equiv 4^\upsilon \pmod 7 \Rightarrow 4^\nu \equiv 4^\upsilon \pmod 7$.

Για $\upsilon=0$ θα είναι $4^\nu \equiv 1 \pmod 7$.

Για $\upsilon=1$ θα είναι $4^\nu \equiv 4 \pmod 7$.

Για $\upsilon=2$ θα είναι $4^\nu \equiv 16 \pmod 7 \Rightarrow 4^\nu \equiv 2 \pmod 7$.

Από τα παραπάνω φαίνεται ότι το υπόλοιπο της διαίρεσης του αριθμού $4^ν$ με τον αριθμό 7 είναι 1 ή 2 ή 4, ανάλογα με τη μορφή του ν.

Θα μπορούσαμε να κατασκευάσουμε δικές μας ασκήσεις.

Για παράδειγμα: Να βρείτε το υπόλοιπο της διαίρεσης του αριθμού $5^{2018}+3\cdot4^{2019}$ με το 7.

Είναι $2018=6\cdot336+2$, οπότε $5^{2018} \equiv 4(\text{mod } 7)$ (1).

Επίσης $2019=3\cdot673$, οπότε $4^{2019} \equiv 1(\text{mod } 7) \Rightarrow 3\cdot4^{2019} \equiv 3(\text{mod } 7)$ (2).

Λόγω των (1) και (2) θα έχουμε: $5^{2018}+3\cdot4^{2019} \equiv (4+3)(\text{mod } 7) \Rightarrow$

$5^{2018}+3\cdot4^{2019} \equiv 7(\text{mod } 7)$, δηλαδή το 7 διαιρεί τον αριθμό $5^{2018}+3\cdot4^{2019}$, οπότε το ζητούμενο υπόλοιπο είναι 0.

6) Δίνονται οι πρώτοι αριθμοί α, β, γ οι οποίοι είναι διάφοροι του 3. Να αποδειχθεί ότι ο αριθμός $\mathbf{3\alpha^2+2\beta^2+7\gamma^2}$ είναι σύνθετος.

Απόδειξη

Επειδή οι αριθμοί α, β, γ είναι πρώτοι και διαφορετικοί του 3, από το θεώρημα θα έχουμε:

$\alpha^2 \equiv 1 (\text{mod } 3) \Rightarrow 3\alpha^2 \equiv 3(\text{mod } 3)$,

$\beta^2 \equiv 1 (\text{mod } 3) \Rightarrow 2\beta^2 \equiv 2(\text{mod } 3)$,

$\gamma^2 \equiv 1 (\text{mod } 3) \Rightarrow 7\gamma^2 \equiv 7(\text{mod } 3)$, οπότε θα έχουμε:

$3\alpha^2+2\beta^2+7\gamma^2 \equiv (3+2+7)(\text{mod } 3) \Rightarrow 3\alpha^2+2\beta^2+7\gamma^2 \equiv 12(\text{mod } 3) \Rightarrow 3\alpha^2+2\beta^2+7\gamma^2 \equiv 0(\text{mod } 3) \Rightarrow 3/3\alpha^2+2\beta^2+7\gamma^2$ και επειδή ο αριθμός $3\alpha^2+2\beta^2+7\gamma^2>3$, θα είναι σύνθετος.

7) Αν α είναι ένας φυσικός αριθμός με (α, 6)=1, να αποδείξετε ότι $\mathbf{\alpha^2 \equiv 1 (\text{mod } 6)}$.

(Θεωρία Αριθμών ΕΜΕ)

Απόδειξη

Θα είναι $\alpha \equiv 0,1,2,3,4,5 (\text{mod } 6)$.

Επειδή (α, 6)=1, ο α θα είναι προφανώς πρώτος και όχι πολλαπλάσιο του 3, άρα θα έχουμε $\alpha \equiv 1,5 (\text{mod } 6) \Rightarrow \alpha \equiv \pm 1(\text{mod } 6)$.

8) Έστω ένας φυσικός x και ένας περιττός πρώτος p.

Να αποδειχθεί ότι οι λύσεις της $\mathbf{x^2 \equiv 1 (\text{mod } p^x)}$ είναι $\mathbf{x \equiv \pm 1 (\text{mod } p^x)}$.

(Θεωρία Αριθμών ΕΜΕ)

Απόδειξη

Είναι $x^2 \equiv x (\text{mod } p^x) \Rightarrow (x+1)(x-1) \equiv 0 (\text{mod } p^x) \Rightarrow p^x/(x+1)(x-1)$.

Ας υποθέσουμε ότι $\left.\begin{array}{c} \mathbf{p^x / x+1} \\ \mathbf{και} \\ \mathbf{p^x / x-1} \end{array}\right\} \Rightarrow \mathbf{p^x /(x+1)-(x-1)} \Rightarrow \mathbf{p^x / 2}$ και $\mathbf{p / p^x} \Rightarrow \mathbf{p / 2}$ που είναι άτοπο, επειδή p>2. Έτσι θα έχουμε: $p^x/(x+1) \Rightarrow x \equiv 1 \pmod{p^x}$ ή $p^x/(x-1) \Rightarrow x \equiv -1 \pmod{p^x}$.

9) Να βρείτε τους αντίστροφους modulo 5 των αριθμών 12, 29

Λύση

Για τον αντίστροφο του 12.

Αρκεί να βρούμε ακέραιο x τέτοιο ώστε $12 \cdot x \equiv 1 \pmod 5$.

Μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο του Ευκλείδη για (12, 5), οπότε θα έχουμε:

$$\left.\begin{array}{l} \mathbf{12 = 2 \cdot 5 + 2} \\ \mathbf{5 = 2 \cdot 2 + 1} \end{array}\right\} \Rightarrow \left.\begin{array}{l} \mathbf{2 = 12 - 2 \cdot 5} \\ \mathbf{1 = 5 - 2 \cdot 2} \end{array}\right\} \Rightarrow \mathbf{1 = 5 - 2(12 - 2 \cdot 5) \Rightarrow 1 = 12(-2) + 3 \cdot 5 \Rightarrow 12(-2) =}$$

$\mathbf{1 - 3 \cdot 5}$, άρα $12 \cdot (-2) \equiv 1 \pmod 5$, δηλαδή ο αντίστροφος του 12 είναι ο $-2 \pmod 5$ ή ο $3 \pmod 5$.

Για τον αντίστροφο του 29.

Αρκεί να βρούμε ακέραιο x τέτοιο ώστε $29 \cdot x \equiv 1 \pmod 5$.

Μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο του Ευκλείδη για (29, 5), οπότε θα έχουμε:

$$\left.\begin{array}{l} \mathbf{29 = 5 \cdot 5 + 4} \\ \mathbf{5 = 4 \cdot 1 + 1} \end{array}\right\} \Rightarrow \left.\begin{array}{l} \mathbf{4 = 29 - 5 \cdot 5} \\ \mathbf{1 = 5 - 4 \cdot 1} \end{array}\right\} \Rightarrow \mathbf{1 = 5 - 1(29 - 5 \cdot 5) \Rightarrow 1 = 29(-1) + 6 \cdot 5 \Rightarrow 29(-1) =}$$

$\mathbf{1 - 6 \cdot 5}$, άρα $29 \cdot (-1) \equiv 1 \pmod 5$, δηλαδή ο αντίστροφος του 12 είναι ο $-1 \pmod 5$ ή ο $4 \pmod 5$.

10) Αν $\nu \equiv 3 \pmod 4$ να αποδειχθεί ότι ο φυσικός ν είναι αδύνατο να γραφεί ως άθροισμα των τετραγώνων δύο ακεραίων.

(Θεωρία Αριθμών ΕΜΕ)

Λύση

Έστω ότι $\nu = x^2 + y^2$. Γνωρίζουμε, από προηγούμενη εφαρμογή, ότι $\alpha^2 \equiv 0, 1 \pmod 4$, άρα θα είναι $x^2 \equiv 0, 1 \pmod 4$ και $y^2 \equiv 0, 1 \pmod 4$.

Τότε θα έχουμε $\nu = x^2 + y^2 \equiv 0, 1, 2 \pmod 4 \not\equiv 3 \pmod 4$.

11) Αν $\lambda \in N$, να αποδείξετε ότι ο αριθμός $\mathbf{A = \sqrt[4]{5\lambda + 3}}$ είναι άρρητος.

(Θεωρία Αριθμών ΕΜΕ Α. Συγκελάκης)

Απόδειξη

Είναι $\mathbf{A^4 = 5\lambda + 3}$, οπότε αρκεί να αποδείξουμε ότι ο αριθμός 5λ+3 δεν έχει τη μορφή A^4. Ξέρουμε, από προηγούμενη εφαρμογή ότι $\alpha^2 \equiv 0, 1, 4 \pmod 5 \Rightarrow \alpha^4 \equiv 0, 1 \pmod 5$

και επειδή $5\lambda+3\equiv 3 \pmod 5$ συμπεραίνουμε ότι ο αριθμός $5\lambda+3$ δεν έχει τη μορφή A^4, άρα ο Α είναι άρρητος.

12) Αν $\mathbf{A=\nu^2-5\nu-5}$, $\nu\in Z$, να βρεθούν οι τιμές του ν, ώστε $\mathbf{11/A}$.

Λύση

Αρκεί να βρούμε τα $\nu\in Z$, έτσι ώστε $\nu^2-5\nu-5 \equiv 0 \pmod{11}$.

Αρκεί $\nu^2-5\nu-5 \equiv 0 \pmod{11}$, αρκεί $\nu^2-5\nu\equiv 5 \pmod{11}$, αρκεί $\nu^2-5\nu+6\equiv 11 \pmod{11}$, αρκεί $(\nu-3)(\nu-2)\equiv 0 \pmod{11}$, αρκεί $11/(\nu-3)(\nu-2)$ (1).

Επειδή όμως ο 11 είναι πρώτος, από τη σχέση (1) θα έχουμε:

$11/(\nu-3)\Rightarrow \nu-3=11\lambda,\ \lambda\in Z\Rightarrow \nu=11\lambda+3,\ \lambda\in Z$ ή $11/(\nu-2)\Rightarrow \nu-2=11\mu,\ \mu\in Z\Rightarrow \nu=11\mu+2,\ \lambda\in Z$.

Ασκήσεις

1) Να προσδιορίσετε τα υπόλοιπα των διαιρέσεων

I. $\mathbf{2017\cdot 2018\cdot 2019-2026^{2020}:9}$

II. $\mathbf{2^{2019}:3}$.

Λύση

Σχόλιο: Αν θέλουμε να βρούμε το υπόλοιπο του α^{μ} όταν διαιρεθεί με το **ν**, ένας καλός τρόπος είναι να βρούμε ακέραιο **κ** τέτοιο ώστε $\alpha^{\kappa}\equiv 1(\text{mod } \nu)$ ή $\alpha^{\kappa}\equiv -1(\text{mod } \nu)$ και να γράψουμε το **μ=κ·π+υ**.

Έτσι $\alpha^{\mu}\equiv\alpha^{\kappa\cdot\pi+\upsilon}(\text{mod } \nu)\Leftrightarrow \alpha^{\mu}\equiv\alpha^{\kappa\cdot\pi}\cdot\alpha^{\upsilon}(\text{mod } \nu)$ και επειδή $\alpha^{\kappa\cdot\pi}\equiv\left(\alpha^{\kappa}\right)^{\pi}(\text{mod } \nu)\Leftrightarrow \alpha^{\kappa\cdot\pi}\equiv 1^{\pi}(\text{mod } \nu)\Leftrightarrow \alpha^{\kappa\cdot\pi}\equiv 1(\text{mod } \nu)$ και $\alpha^{\upsilon}\equiv\alpha^{\upsilon}(\text{mod } \nu)$θα έχουμε:

$$\alpha^{\mu}=\alpha^{\kappa\cdot\pi+\upsilon}\equiv\alpha^{\kappa\cdot\pi}\cdot\alpha^{\upsilon}(\text{mod } \nu)=1\cdot\alpha^{\upsilon}(\text{mod } \nu)=\alpha^{\upsilon}(\text{mod } \nu).$$

($1^{ος}$ τρόπος)

I. Είναι 2017=9·224+1, άρα θα είναι 2017 ≡1 (mod 9),

2018=9·224+2, άρα θα είναι 2018 ≡2 (mod 9),

2019=9·224+3, άρα θα είναι 2019 ≡3 (mod 9), οπότε 2017·2018·2019≡6 (mod 9) (1).

Επίσης 2026=9·225+1, άρα θα είναι 2026^{2020} ≡1 (mod 9) (2).

Λόγω των σχέσεων (1) και (2) θα έχουμε $2017\cdot 2018\cdot 2019-2026^{2020}$ ≡5 (mod 9), δηλαδή το υπόλοιπο της διαίρεσης του $2017\cdot 2018\cdot 2019-2026^{2020}$ με το 9 είναι το 5.

($2^{ος}$ τρόπος)

Είναι 2017=9·224+1, 2018=9·224+2, 2019=9·224+3, 2026=9·225+1 οπότε θα έχουμε:

$(\pi\text{ολ}9+1)\cdot(\pi\text{ολ}9+2)\cdot(\pi\text{ολ}9+3)-(\pi\text{ολ}9+1)^{2020}=(\pi\text{ολ}9+6)-(\pi\text{ολ}9+1)=\pi\text{ολ}7+5$, οπότε το υπόλοιπο είναι 5.

II. Είναι $2^2=4\equiv 1(\text{mod } 3)$

Άρα $2^{2019}=2^{2\cdot 1009+1}=\left(2^2\right)^{1009}\cdot 2$, οπότε θα έχουμε:

$$2^{2019}=2^{2\cdot 1009+1}=\left(2^2\right)^{1009}\cdot 2\equiv 1\cdot 2(\text{mod } 3)\equiv 2(\text{mod } 3).$$

Άρα το ζητούμενο υπόλοιπο είναι 2.

2) Να βρεθεί το τελευταίο ψηφίο του αριθμού $\mathbf{2^{2019}+3^{2019}}$.

Λύση

Είναι $2\equiv -3(\text{mod } 5)\Rightarrow 2^{2019}\equiv(-3)^{2019}(\text{mod } 5)\Rightarrow 2^{2019}-(-3)^{2019}\equiv(\text{mod } 5)\Rightarrow 2^{2019}+3^{2019}\equiv(\text{mod } 5)$ άρα $5/2^{2019}+3^{2019}$, οπότε ο αριθμός αυτός θα λήγει σε 0 ή 5.

Ο αριθμός 2^{2019} είναι άρτιος και ο αριθμός 3^{2019} είναι περιττός, οπότε ο $2^{2019}+3^{2019}$ θα είναι περιττός, άρα θα λήγει σε 5.

Παρατήρηση

Θα μπορούσαμε να λύσουμε το πρόβλημα και με άλλο τρόπο.

Είναι $\mathbf{2^2=4=(3+1)=(\pi\circ\lambda 3+1)}$, οπότε $\mathbf{2^{2019}=2^{2\cdot 1009+1}=\left(2^2\right)^{1009}\cdot 2=(\pi\circ\lambda 3+1)^{1009}\cdot 2=(\pi\circ\lambda 3+1)\cdot 2=\pi\circ\lambda 3+2.}$ Άρα το ζητούμενο υπόλοιπο είναι 2.

3) Να βρεθεί το υπόλοιπο της διαίρεσης του $\mathbf{2^{2019}}$ με το **5**;

Λύση

Είναι $\mathbf{2^2=4\equiv -1(\text{mod } 5)}$

Άρα $\mathbf{2^{2019}=2^{2\cdot 1009+1}=\left(2^2\right)^{1009}\cdot 2}$, οπότε θα έχουμε:

$\mathbf{2^{2019}=2^{2\cdot 1009+1}=\left(2^2\right)^{1009}\cdot 2\equiv -1\cdot 2(\text{mod } 5)\equiv -2(\text{mod } 5)=3(\text{mod } 5).}$

Άρα το ζητούμενο υπόλοιπο είναι 3.

($2^{ος}$ τρόπος)

Είναι $\mathbf{2^4=16=(\pi\circ\lambda 5+1)}$, οπότε θα έχουμε:

$\mathbf{2^{2019}=2^{4\cdot 504+3}=\left(2^4\right)^{504}\cdot 2^3=(\pi\circ\lambda 5+1)^{504}\cdot 8=(\pi\circ\lambda 5+1)\cdot 8=\pi\circ\lambda 5+8=\pi\circ\lambda 5+3.}$

Άρα το ζητούμενο υπόλοιπο είναι 3.

4) Να αποδείξετε ότι ο αριθμός $\mathbf{2018^{200}\cdot 2019^{300}}$ διαιρείται με το 9.

Απόδειξη

Είναι $2018=9\cdot 224+2$, άρα θα έχουμε $2018^1\equiv 2(\text{mod } 9)\Rightarrow 2018^2\equiv 4(\text{mod } 9)\Rightarrow$ $2018^3\equiv 8(\text{mod } 9)\Rightarrow 2018^3\equiv -1(\text{mod } 9)$.

Είναι $200=3\cdot 63+2$, οπότε $\mathbf{2018^{200}=2018^{3\cdot 63+2}=\left(2018^3\right)^{63}\cdot 2018^2}$ και επειδή από τα προηγούμενα είναι $2018^3\equiv -1(\text{mod } 9)$ και $2018^2\equiv 4(\text{mod } 9)$ θα έχουμε:

$2018^{200}=(-1)^{63}\cdot 4(\text{mod } 9)=-4(\text{mod } 9)$ (1).

Όμοια $2019=9\cdot 224+3$, άρα θα έχουμε $2019^1\equiv 3(\text{mod } 9)\Rightarrow 2019^2\equiv 9(\text{mod } 9)\Rightarrow$ $2019^2\equiv 0(\text{mod } 9)$, δηλαδή 2019^2 διαιρείται ακριβώς με το 9.

Είναι $300=2\cdot 150$, οπότε $\mathbf{2019^{300}=2019^{2\cdot 150}=\left(2019^2\right)^{150}}$ και επειδή από τα προηγούμενα είναι $2019^2\equiv 0(\text{mod } 9)$ θα έχουμε: $2019^{300}=0^{63}(\text{mod } 9)=0(\text{mod } 9)$ (2).

Από τις σχέσεις (1) και (2) θα έχουμε: $\mathbf{2018^{200}\cdot 2019^{300}=-4\cdot 0(\text{mod } 9)=)=0(\text{mod } 9)}$, οπότε ο αριθμός $\mathbf{2018^{200}\cdot 2019^{300}}$ διαιρείται με το 9.

($2^{ος}$ τρόπος)

Είναι $2018=\text{πολ}9+2\Rightarrow 2018^{200}=(\text{πολ}9+2)^{200}=\text{πολ}9+2^{200}$ (3).
Επίσης $2019=\text{πολ}9+3\Rightarrow 2019^{300}=(\text{πολ}9+3)^{300}=\text{πολ}9+3^{300}$ (4).
Λόγω των (3) και (4) θα έχουμε:
$2018^{200}\cdot 2019^{300}=(\text{πολ}9+2^{200})(\text{πολ}9+3^{300})=\text{πολ}9+2^{200}\cdot 3^{300}=$
$\text{πολ}9+2^{200}\cdot 3^{200}\cdot 3^{100}=\text{πολ}9+6^{200}\cdot 3^{100}=\text{πολ}9+36^{100}\cdot 3^{100}=\text{πολ}9+(4\cdot 9)^{100}\cdot 3^{100}=\text{πολ}9.$

5) Να υπολογίσετε το υπόλοιπο της διαίρεσης του αριθμού $A=13^{23}\cdot 27^{41}$ με το 8.

(Θεωρία Αριθμών ΕΜΕ Α. Συγκελάκης)

Λύση

Είναι $13=8\cdot 1+5$, άρα θα έχουμε $13^1\equiv 5(\text{mod } 8)\Rightarrow 13^2\equiv 25(\text{mod } 8)\Rightarrow 13^2\equiv 1(\text{mod } 8)$ (1).
Είναι $23=2\cdot 11+1$, οπότε θα έχουμε $13^{23}=13^{2\cdot 11+1}=(13^2)^{11}\cdot 13$ και λόγω της σχέσης (1) θα έχουμε:$(13^2)^{11}\equiv 1(\text{mod } 8)$ (2). Άρα θα είναι $13^{23}=(13^2)^{11}\cdot 13\equiv 1\cdot 5(\text{mod } 8)\equiv 5(\text{mod } 8)$ (2).
Επίσης $27=8\cdot 3+3$, άρα θα έχουμε $27^1\equiv 3(\text{mod } 8)\Rightarrow 27^2\equiv 9(\text{mod } 8)\Rightarrow 27^2\equiv 1(\text{mod } 8)$ (3).
Είναι $41=2\cdot 20+1$, οπότε θα έχουμε $27^{41}=27^{2\cdot 20+1}=(27^2)^{20}\cdot 27$ και λόγω της σχέσης (3) θα έχουμε:$(27^2)^{20}\equiv 1(\text{mod } 8)$. Άρα θα είναι $27^{41}=(27^2)^{20}\cdot 27\equiv 1\cdot 3(\text{mod } 8)\equiv 3(\text{mod } 8)$ (4).
Λόγω των (3) και (4) θα έχουμε: $A=13^{23}\cdot 27^{41}\equiv 5\cdot 3(\text{mod } 8)\equiv 15(\text{mod } 8)\equiv 7(\text{mod } 8)$.
Άρα θα υπάρχει $\alpha\in Z$ τέτοιος, ώστε $A=8\alpha+7$ και επειδή $7<8$ το ζητούμενο υπόλοιπο είναι ο αριθμός 7.
($2^{ος}$ τρόπος)
$13^2=169=168+1=21\cdot 8+1=\text{πολ}8+1\Rightarrow 13^{23}=13^{2\cdot 11+1}=(13^2)^{11}\cdot 13=(\text{πολ}8+1)^{11}\cdot 13=(\text{πολ}8+1)\cdot 13=\text{πολ}8+13$ (5).
$27^2=729=728+1=91\cdot 8+1=\text{πολ}8+1\Rightarrow 27^{41}=27^{2\cdot 20+1}=(27^2)^{20}\cdot 27=(\text{πολ}8+1)^{20}\cdot 27=(\text{πολ}8+1)\cdot 13=\text{πολ}8+27$ (6).
Λόγω των (5) και (6) θα έχουμε:
$A=13^{23}\cdot 27^{41}=(\text{πολ}8+13)(\text{πολ}8+27)=\text{πολ}8+13\cdot 27=\text{πολ}8+351=\text{πολ}8+344+7=$
$\text{πολ}8+8\cdot 43+7=\text{πολ}8+7.$

6) Να δείξετε ότι $\mathbf{2222^{5555}+5555^{2222}\equiv 0(\text{mod } 7).}$

(Θεωρία Αριθμών ΕΜΕ Α. Συγκελάκης)

Απόδειξη

Είναι $2222=7\cdot 317+3$, οπότε θα έχουμε $2222\equiv 3(\text{mod } 7)\Rightarrow 2222^{5555}\equiv 3^{5555}(\text{mod } 7)$ (1).
Επίσης $5555=7\cdot 793+4$, οπότε θα έχουμε $5555\equiv 4(\text{mod } 7)\Rightarrow 5555^{2222}\equiv 4^{2222}(\text{mod } 7)$ (2).
Λόγω των (2) και (3) θα έχουμε: $2222^{5555}+5555^{2222}\equiv 3^{5555}+4^{2222}(\text{mod } 7)$ (3).
Είναι $3\equiv 3(\text{mod } 7)\Rightarrow 3^2\equiv 9(\text{mod } 7)\Rightarrow 3^3\equiv 27(\text{mod } 7)\Rightarrow 3^3\equiv -1(\text{mod } 7)$, και επειδή είναι $5555=3\cdot 1851+2$, θα έχουμε ότι $3^{5555}=(3^3)^{1851}\cdot 3^2\equiv(-1)^{1851}\cdot 3^2(\text{mod } 7)\equiv -9(\text{mod } 7)\equiv -2(\text{mod } 7)$ (4).

Είναι $4 \equiv 4(\text{mod } 7) \Rightarrow 4^2 \equiv 16(\text{mod } 7) \Rightarrow 4^3 \equiv 64(\text{mod } 7) \Rightarrow 4^3 \equiv 1(\text{mod } 7)$, και επειδή είναι $2222=3\cdot 740+2$, θα έχουμε ότι $4^{2222}=(4^3)^{740}\cdot 4^2 \equiv 1^{740}\cdot 4^2(\text{mod } 7) \equiv 16(\text{mod } 7) \equiv 2(\text{mod } 7)$ (5).

Η (3) λόγω των (4) και (5) γίνεται $2222^{5555}+5555^{2222} \equiv -2+2(\text{mod } 7) \equiv 0(\text{mod } 7)$.

7) Όμοια **$7/333^{444}+444^{333}$**.

8) Να προσδιορίσετε τον αριθμό $\nu \in N^*$, για τον οποίον ισχύει $\mathbf{7/6^{\nu^{2018}}-15^{\nu^{2019}}}$.

Λύση

Είναι $6 \equiv (-1)(\text{mod } 7) \Rightarrow \mathbf{6^{\nu^{2018}} \equiv (-1)^{\nu^{2018}} \bmod 7}$.

Όμοια είναι $15 \equiv 1(\text{mod } 7) \Rightarrow \mathbf{15^{\nu^{2019}} \equiv 1 \bmod 7}$.

Τότε θα έχουμε: $\mathbf{6^{\nu^{2018}}-15^{\nu^{2019}} \equiv [(-1)^{\nu^{2018}}-1] \bmod 7}$ (1).

Διακρίνουμε περιπτώσεις.

Αν ν άρτιος τότε η (1) γίνεται $\mathbf{6^{\nu^{2018}}-15^{\nu^{2019}} \equiv (1-1) \bmod 7} \Rightarrow$ $\mathbf{6^{\nu^{2018}}-15^{\nu^{2019}} \equiv 0 \bmod 7}$, δηλαδή $\mathbf{7/6^{\nu^{2018}}-15^{\nu^{2019}}}$.

Αν ν περιττός τότε η (1) γίνεται $\mathbf{6^{\nu^{2018}}-15^{\nu^{2019}} \equiv [(-1)-1] \bmod 7} \Rightarrow$ $\mathbf{6^{\nu^{2018}}=15^{\nu^{2019}} \equiv (-2) \bmod 7}$, δηλαδή $7\nmid \mathbf{6^{\nu^{2018}}-13^{\nu^{2019}}}$.

Άρα θα πρέπει ο να είναι άρτιος.

9) Δείξτε ότι η παράσταση **$5^{2\nu}+3\cdot 2^{5\nu-2}$** διαιρείτε με το 7 για κάθε $\nu \in N$.

Απόδειξη

Δουλεύουμε με mod 7.

Είναι $5^2 \equiv 4(\text{mod } 7) \Rightarrow 5^{2\nu} \equiv 4^{\nu}(\text{mod } 7)$ (1).

Είναι $2^{5\nu-2}=2^{5(\nu-1)+3}=2^{5(\nu-1)}\cdot 2^3=32^{(\nu-1)}\cdot 8$.

Επειδή $8 \equiv 1(\text{mod } 7)$ και $32 \equiv 4(\text{mod } 7) \Rightarrow 32^{\nu-1} \equiv 4^{\nu-1}$ (mod 7) θα έχουμε:

$5^{2\nu}+3\cdot 2^{5\nu-2} \equiv 4^{\nu}+3\cdot 4^{\nu-1}$ (mod 7) $\equiv 4^{\nu-1}(4+3)$ (mod 7) $\equiv 0(\text{mod } 7)$.

10) Αν $\nu \in N^*$, να αποδειχθεί ότι ο 11 διαιρεί τον αριθμό **$A=3^{2\nu+2}+2^{6\nu+1}$**.

(Γαλλία 1991)

Απόδειξη

Δουλεύουμε με mod 11.

Είναι $3^{2\nu+2}=3^{2\nu}\cdot 3^2=9^{\nu}\cdot 9$ και $9 \equiv -2(\text{mod } 11) \Rightarrow 9^{\nu} \equiv (-2)^{\nu}(\text{mod } 11)$, οπότε θα έχουμε:

$3^{2\nu+2} \equiv (-2)^{\nu}\cdot 9$ (mod 11) (1).

Επίσης $2^{6\nu+1}=2^{6\nu}\cdot 2=64^{\nu}\cdot 2$ και $64 \equiv -2(\text{mod } 11) \Rightarrow 64^{\nu} \equiv (-2)^{\nu}$ (mod 11), οπότε θα έχουμε:

$2^{6\nu+1}=2^{6\nu}\cdot 2 \equiv (-2)^{\nu}\cdot 2$ (mod 11) (2).

Θα είναι $A=3^{2\nu+2}+2^{6\nu+1}\equiv(-2)^{\nu}\cdot 9+(-2)^{\nu}\cdot 2(\text{mod } 7)\equiv(-2)^{\nu}\cdot(9+2)(\text{mod } 11)\equiv(-2)^{\nu}\cdot 11(\text{mod } 11)\equiv 0(\text{mod } 7)$.

11) Να αποδειχθεί ότι για κάθε φυσικό ν ο αριθμός $A=5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}$ είναι πολλαπλάσιο του 33.

(Θεωρία Αριθμών ΕΜΕ)

Απόδειξη

Είναι $33=3\cdot 11$ και επειδή $(3,11)=1$, αρκεί να αποδείξουμε ότι 3/Α και 11/Α.

Είναι $5\equiv 2(\text{mod } 3)\Rightarrow 5^{2\nu+1}\equiv 2^{2\nu+1}(\text{mod } 3)$ (1),

$11\equiv 2(\text{mod } 3)\Rightarrow 11^{2\nu+1}\equiv 2^{2\nu+1}(\text{mod } 3)$ (2) και

$17\equiv 2(\text{mod } 3)\Rightarrow 17^{2\nu+1}\equiv 2^{2\nu+1}(\text{mod } 3)$ (3).

Από τις σχέσεις (1), (2), (3) θα έχουμε $5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}\equiv 2^{2\nu+1}+2^{2\nu+1}+2^{2\nu+1}(\text{mod } 3)\Rightarrow 5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}\equiv 3\cdot 2^{2\nu+1}(\text{mod } 3)\Rightarrow 5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}\equiv 0(\text{mod } 3)$, δηλαδή 3/Α.

Επίσης $5\equiv -6(\text{mod } 11)\Rightarrow 5^{2\nu+1}\equiv(-6)^{2\nu+1}(\text{mod } 11)$ (4),

$11\equiv 0(\text{mod } 11)\Rightarrow 11^{2\nu+1}\equiv 0(\text{mod } 11)$ (5) και

$17\equiv 6(\text{mod } 11)\Rightarrow 17^{2\nu+1}\equiv 6^{2\nu+1}(\text{mod } 11)$ (6).

Από τις σχέσεις (4), (5), (6) θα έχουμε $5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}\equiv(-6)^{2\nu+1}+6^{2\nu+1}(\text{mod } 11)\Rightarrow 5^{2\nu+1}+11^{2\nu+1}+17^{2\nu+1}\equiv 0(\text{mod } 11)$, δηλαδή 11/Α.

12) Να αποδείξετε ότι ο αριθμός $\nu^2+3\nu+5$ δεν διαιρείται με το 121 για κάθε τιμή του ν.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Είναι $121=11^2$, οπότε αν ο αριθμός $\nu^2+3\nu+5$ διαιρείται με το 121 θα πρέπει να διαιρείται και με το 11, που είναι πρώτος.

Το τριώνυμο $\nu^2+3\nu+5$ δεν έχει ρίζες, άρα θα πρέπει με κάποιο τρόπο να το μετατρέψουμε στη μορφή $\nu^2+3\nu+5=(\nu+\alpha)(\nu+\beta)+\gamma$, $\alpha, \beta, \gamma\in Z$ και το γ να είναι 11κ.

Σε μια τέτοια περίπτωση, αν το 11/ $\nu^2+3\nu+5$, επειδή θα διαιρεί και το $\gamma=11\kappa$, $\kappa\in Z$, θα διαιρεί και το γινόμενο $(\nu+\alpha)(\nu+\beta)$.

Επειδή ο 11 είναι πρώτος και $11/(\nu+\alpha)(\nu+\beta)\Rightarrow \nu+\alpha=11$ και $\nu+\beta=1$ ή $\nu+\alpha=1$ και $\nu+\beta=11$, οπότε μπορούμε να εκτιμήσουμε αν αυτό είναι σωστό ή λάθος.

Έστω λοιπόν $\nu^2+3\nu+5=(\nu+\alpha)(\nu+\beta)+\gamma\Rightarrow \nu^2+3\nu+5=\nu^2+(\alpha+\beta)\nu+\alpha\beta+\gamma$.

Για να ισχύει η ισότητα θα πρέπει $\alpha+\beta=3$ και $\alpha\beta+\gamma=5$, με $\gamma=11\kappa$.

Έστω $\kappa=1$, οπότε $\gamma=11$, τότε $\alpha+\beta=3$ και $\alpha\beta=-6$. Τα α, β θα είναι ρίζες της εξίσωσης $x^2-3x-6=0$, που έχει $\Delta=33$, άρα $\alpha,\beta\notin Z$.

Έστω $\kappa=2$, οπότε $\gamma=22$, τότε $\alpha+\beta=3$ και $\alpha\beta=-17$. Τα α, β θα είναι ρίζες της εξίσωσης $x^2-3x-17=0$, που έχει $\Delta=77$, άρα $\alpha,\beta\notin Z$.

Έστω $\kappa=3$, οπότε $\gamma=33$, τότε $\alpha+\beta=3$ και $\alpha\beta=-28$. Τα α, β θα είναι ρίζες της εξίσωσης $x^2-3x-28=0$, που έχει $\Delta=121$, άρα $\alpha=7$ και $\beta=-4$.

Θα έχουμε λοιπόν $\nu^2+3\nu+5=(\nu+7)(\nu-4)+33$.

Αν ο αριθμός $\nu^2+3\nu+5$ διαιρείται με το 11, θα πρέπει και ο $(\nu+7)(\nu-4)+33$ να διαιρείται με το 11 και επειδή 11/33, θα πρέπει $11/(\nu+7)(\nu-4)\Rightarrow\nu+7=11$ και $\nu-4=1$, διότι $\nu+7>\nu-4$, άρα $\nu=4$ και $\nu=5$, που είναι άτοπο.

Επίσης θα μπορούσαμε να παρατηρήσουμε: Οι αριθμοί $\nu+7$ και $\nu-4$ είναι ισοϋπόλοιποι modulo 11, είναι $\nu+7\equiv(\nu-4)(\text{ mol }11)$ και $\nu-4\equiv(\nu+7)\text{ mol }11$, οπότε $\nu+7=\nu-4+11\mu$ και $\nu-4=\nu+7+11\rho$.
Επειδή
$11/(\nu+7)(\nu-4)\Rightarrow11/[(\nu-4)+11\mu](\nu-4)\Rightarrow11/[(\nu-4)^2+11\mu(\nu-4)]\Rightarrow11/(\nu-4)^2\Rightarrow11/(\nu-4)$.
Όμοια $11/(\nu+7)$. Έτσι θα έχουμε $\nu^2+3\nu+5=(\nu+7)(\nu-4)+33\equiv33(\text{ mod }121)$, δηλαδή ο αριθμός $\nu^2+3\nu+5$ δεν είναι πολλαπλάσιο του 121.

13) Να λυθεί η εξίσωση $\mathbf{2^x-3^y=7}$, όπου x, y ακέραιοι με $x, y\geq1$.

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Έχουμε $2^x-3^y=7\Rightarrow2^x=7+3^y\equiv1(\text{ mod}3)$ (1).
Είναι $2^o\equiv1(\text{ mod }3)$, $2^1\equiv2(\text{ mod }3)$, $2^2\equiv1(\text{ mod }3)$, $2^3\equiv2(\text{ mod }3)$, δηλαδή οι άρτιες δυνάμεις του 2 είναι 1 modulo 3 και οι περιττές 2 modulo 3, οπότε από τη σχέση (1) θα πρέπει ο x να είναι άρτιος, άρα $x\geq2$, έστω $x=2\kappa$, $\kappa\in Z$.
Όμοια $2^x-3^y=7\Rightarrow3^y=2^x-7\equiv1(\text{ mod}4)$ (2).
Είναι $3^o\equiv1(\text{ mod }4)$, $3^1\equiv3(\text{ mod }4)$, $3^2\equiv1(\text{ mod }4)$, $3^3\equiv3(\text{ mod }4)$, δηλαδή οι άρτιες δυνάμεις του 3 είναι 1 modulo 4 και οι περιττές 3 modulo 4, οπότε από τη σχέση (2) θα πρέπει ο y να είναι άρτιος, έστω $y=2\lambda$, $\lambda\in Z$.
Η αρχική σχέση γίνεται $2^{2\mu}-3^{2\lambda}=7\Leftrightarrow(2^\mu-3^\lambda)(2^\mu+3^\lambda)=7$, με $2^\mu+3^\lambda>2^\mu-3^\lambda$.
Επειδή ο 7 είναι πρώτος θα πρέπει $2^\mu-3^\lambda=1$ και $2^\mu+3^\lambda=7$, άρα λύνοντας το σύστημα θα έχουμε $\kappa=2$ και $\lambda=1$, οπότε $x=4$ και $y=2$.

14) Να βρείτε τα δύο τελευταία ψηφία του αριθμού $\mathbf{9^{2015}}$.

Λύση

Αρκεί να βρούμε ένα αριθμό $\beta\in\{0,1,2,....,98,99\}$ τέτοιο ώστε $9^{2015}\equiv\beta(\text{mod }100)$.
Βρίσκουμε τα δύο τελευταία ψηφία των δυνάμεων του 9.
Είναι $9=\mathbf{09}$, $9^2=\mathbf{81}$, $9^3=7\mathbf{29}$, $9^4=65\mathbf{61}$, $9^5=590\mathbf{49}$, $9^6=5314\mathbf{41}$ και όπως φαίνεται δεν μας βολεύει να αναζητήσουμε κάποια περιοδικότητα.
Είναι $100=4\cdot25$ και $(4, 25)=1$ πράγμα που παραπέμπει σε προηγούμενη εφαρμογή.
Είναι $9^5\equiv-1(\text{mod }25)\Rightarrow(9^5)^2\equiv(-1)^2\text{ (mod }25)\Rightarrow9^{10}\equiv1(\text{mod }25)$.
Επίσης είναι $9^2\equiv1(\text{mod }4)\Rightarrow(9^2)^5\equiv1^5\text{ (mod }4)\Rightarrow9^{10}\equiv1(\text{mod }4)$ άρα θα έχουμε:

$$\left.\begin{matrix}\mathbf{9^{10}\equiv1(mod\ 4)}\\\mathbf{9^{10}\equiv1(mod\ 25)}\end{matrix}\right\}\Rightarrow9^{10}\equiv1(\text{mod }100)$$ διότι $(4, 25)=1$ (Εφαρμογή).

Είναι $9^{2015}=9^{2010}\cdot9^5=(9^{10})^{201}\cdot9^5$ και επειδή $9^{10}\equiv1(\text{mod }100)\Rightarrow(9^{10})^{201}\equiv1(\text{mod }100)$, οπότε θα έχουμε $9^{2015}\equiv9^5\text{ (mod }100)$, Επειδή $9^5=590\mathbf{49}\equiv49(\text{mod }100)$, άρα τα δύο τελευταία ψηφία του αριθμού 9^{2015} είναι το 49.

15) **I.** Να βρεθούν τα δύο τελευταία ψηφία του αριθμού $\mathbf{9^{9^9}}$.

II. Να βρεθούν τα δύο τελευταία ψηφία του αριθμού $\mathbf{9^{9^{9^9}}}$.

Λύση

I. Προφανώς πρέπει να δουλέψουμε με modulo 100.

Είναι $9 \equiv 9(\text{mod } 100) \Rightarrow 9^2 \equiv 81(\text{mod } 100) \Rightarrow 9^3 \equiv 29(\text{mod } 100) \Rightarrow 9^4 \equiv 61(\text{mod } 100) \Rightarrow 9^8 \equiv 21(\text{mod } 100) \Rightarrow 9^9 \equiv 89(\text{mod } 100)$ (*) $\Rightarrow 9^{10} \equiv 1(\text{mod } 100)$ (1).

Η σχέση (1) μας προτρέπει να γράψουμε τον εκθέτη 9^9 του $\mathbf{9^{9^9}}$ σε μια μορφή που να περιέχει το 10.

Χρησιμοποιώντας modulo 10 θα έχουμε:

$9 \equiv 9(\text{mod } 10) \Rightarrow 9^2 \equiv 1(\text{mod } 10) \Rightarrow 9^8 \equiv 1(\text{mod } 10) \Rightarrow 9^9 \equiv 9(\text{mod } 10) \Rightarrow 9^9 - 9 = 10\kappa \Rightarrow 9^9 = 10\kappa + 9$, $\kappa \in N^*$ (2).

Από τα παραπάνω θα έχουμε: $\mathbf{9^{9^9} \overset{(2)}{=} 9^{10\kappa+9} = 9^{10\kappa} \cdot 9^9}$ (3).

Η (1) $\Rightarrow 9^{10\kappa} \equiv 1(\text{mod } 100) \Rightarrow 9^{10\kappa} \cdot 9^9 \equiv 9^9 \ (\text{mod } 100)$ και λόγω της (3) θα είναι $\mathbf{9^{9^9} \equiv 9^9 (\text{mod } 100)}$ και επειδή $9^9 \equiv 89(\text{mod } 100)$, θα έχουμε $\mathbf{9^{9^9} \equiv 89 (\text{mod } 100)}$, δηλαδή τα δύο τελευταία ψηφία του $\mathbf{9^{9^9}}$ είναι τα 8,9.

II. Θα βρούμε πρώτα τον εκθέτη $\mathbf{9^{9^9}}$ του $\mathbf{9^{9^{9^9}}}$.

Είναι $\mathbf{9^{9^9} \overset{(2)}{=} 9^{10\kappa+9} = (9^{10})^{\kappa} \cdot 9^9 \overset{(1)}{\equiv} 9^9 (\text{mod } 10) \overset{(*)}{\equiv} 9 (\text{mod } 10) \Rightarrow 9^{9^9} = 10\lambda + 9}$ (4).

Λόγω της (4) θα έχουμε $\mathbf{9^{9^{9^9}} = 9^{10\lambda+9} = (9^{10})^{\lambda} \cdot 9^9 \overset{(1)}{\equiv} 9^9 (\text{mod } 100) \overset{(*)}{\equiv} 89 (\text{mod } 100)}$, δηλαδή τα δύο τελευταία ψηφία του $\mathbf{9^{9^{9^9}}}$ είναι τα 8,9.

16) Δείξτε ότι, για κάθε φυσικό αριθμό k, ο 19 διαιρεί τον αριθμό $\mathbf{2^{2^{6k+2}} + 3}$.

(Waclaw Sierpinski 250 προβλήματα της Στοιχειώδους Θεωρίας Αριθμών)

Λύση

Είναι $2 \equiv 2(\text{mod } 19)$, $2^2 \equiv 4(\text{mod } 19)$, $2^3 \equiv 8(\text{mod } 19)$, $2^4 \equiv 16(\text{mod } 19)$, $2^5 \equiv 13(\text{mod } 19)$, $2^6 \equiv 7(\text{mod } 19)$, $2^7 \equiv 14(\text{mod } 19)$, $2^8 \equiv 9(\text{mod } 19)$, $2^9 \equiv 1(\text{mod } 19)$ (1).

Η σχέση (1) μας προτρέπει να γράψουμε τον εκθέτη 2^{6k+2} του $\mathbf{2^{2^{6k+2}}}$ σε μια μορφή που να περιέχει το 9.

Χρησιμοποιώντας modulo 9 θα έχουμε:

$2^6 = 64 \equiv 1(\text{mod } 9) \Rightarrow 2^{6k} \equiv 1(\text{mod } 9) \Rightarrow 2^{6k+2} \equiv 4(\text{mod } 9) \Rightarrow 9 / 2^{6k+2} - 4 \Rightarrow 2^{6k+2} - 4 = 9\lambda \Rightarrow 2^{6k+2} = 9\lambda + 4$ (2).

Στη σχέση (2) το πρώτο μέλος είναι αριθμός άρτιος, οπότε πρέπει και το δεύτερο μέλος να είναι άρτιος αριθμός, οπότε πρέπει ο λ να είναι άρτιος, έστω $\lambda = 2\mu$, άρα η(2) γίνεται: $2^{6k+2} = 9 \cdot 2\mu\lambda + 4 \Rightarrow 2^{6k+2} = 18\rho + 4$ (3).

Θα είναι $\mathbf{2^{2^{6k+2}} \overset{(3)}{=} 2^{18\rho+4} = \left(2^9\right)^{2\rho} \cdot 2^4 \equiv 2^4 (\text{mod } 19)}$, άρα θα έχουμε:

$\mathbf{2^{2^{6k+2}} + 3 \equiv (2^4 + 3) (\text{mod } 19) \Rightarrow 2^{2^{6k+2}} + 3 \equiv 0 (\text{mod } 19)}$.

17) Να αποδείξετε ότι για κάθε σύνθετο φυσικό ν>4 ισχύει ότι **(ν–1)! ≡0(mod ν).**

(ΕΜΕ. Θεωρία Αριθμών)

Λύση

Επειδή ο φυσικός αριθμός ν είναι σύνθετος, θα υπάρχουν α, β φυσικοί τέτοιοι ώστε ν=α·β, με 0<α<ν , 0<β<ν και έστω α<β.

Είναι (ν–1)!=1·2·3·....·α·(α+1)·...·β(β+1)·...·(ν–1), δηλαδή ο αριθμός ν=α·β/(ν–1)!, άρα θα είναι (ν–1)! ≡0(mod ν).

Αν ο ν είναι τετράγωνο πρώτου, δηλαδή είναι $\nu=\pi^2$, με π πρώτο περιττό, γιατί ν>4, τότε θα είναι (ν–1)!=1·2·3·....·π·(π+1)·....2π(2π+1)·...·(ν–1), άρα ο ν/(ν–1)!.

18) Να εξεταστεί αν η εξίσωση $\mathbf{1+3^{x!}+5^{y!}+7^{z!}=w^2}$ έχει λύση στους ακέραιους για x, y, z>3.

Λύση (mathematica)

Οι αριθμοί 3, 5, 7 είναι πρώτοι, οπότε θα εκμεταλλευτούμε το θεώρημα Fermat.

Είναι (3,7)=1, οπότε θα έχουμε $3^6\equiv1(\text{mod }7)$.

Όμοια (5,7)=1, οπότε θα έχουμε $5^6\equiv1(\text{mod }7)$.

Επειδή x>3, θα είναι x!=1·2·3·4·...., οπότε x! ≡0(mod 6)⇒ x!=6κ, άρα θα είναι $\mathbf{3^{x!}=3^{6\kappa}=(3^6)^{\kappa}\equiv1(mod\,7)}$.

Όμοια, επειδή y>3, θα είναι y!=1·2·3·4·...., οπότε y! ≡0(mod 6)⇒ y!=6λ, άρα θα είναι $\mathbf{5^{y!}=5^{6\lambda}=(5^6)^{\kappa}\equiv1(mod\,7)}$.

Η αρχική εξίσωση, παίρνοντας modulo 7, θα έχουμε: $\mathbf{w^2\equiv1+1+1+0\equiv3(mod\,7)}$ (1).

Έστω ν=7π+υ, υ=0,1,2,3,4,5,6,7, τότε εύκολα μπορούμε να δείξουμε ότι:

$\mathbf{v^2\equiv0,1,2,4(mod\,7)}$, άρα η (1) είναι αδύνατη.

Θέματα Διαγωνισμών

1) Αν α, β, γ∈Z, να αποδείξετε ότι ο αριθμός $\mathbf{(5\alpha+3)^5+(5\beta+2)^4+(5\gamma+1)^3}$ διαιρείται με το 5.

(Τουρκία)

Απόδειξη

Είναι $5\alpha+3\equiv 3(\text{mod}5)\Rightarrow(5\alpha+3)^5\equiv 3^5(\text{mod}5)\Rightarrow(5\alpha+3)^5\equiv 243(\text{mod}5)\Rightarrow$
$(5\alpha+3)^5\equiv 3(\text{mod}5)$ (1).
Επίσης $5\beta+2\equiv 2(\text{mod}5)\Rightarrow(5\beta+2)^4\equiv 2^4(\text{mod}5)\Rightarrow(5\beta+2)^4\equiv 16(\text{mod}5)\Rightarrow$
$(5\beta+2)^4\equiv 1(\text{mod}5)$ (2).
Όμοια $5\gamma+1\equiv 1(\text{mod}5)\Rightarrow(5\gamma+1)^3\equiv 1^3(\text{mod}5)\Rightarrow(5\gamma+1)^3\equiv 1(\text{mod}5)$ (3).
Από τις (1), (2), (3) θα έχουμε:
$(5\alpha+3)^5+(5\beta+2)^4+(5\gamma+1)^3\equiv(3+1+1)(\text{mod}5)\Rightarrow(5\alpha+3)^5+(5\beta+2)^4+(5\gamma+1)^3\equiv 5(\text{mod}5)$,
οπότε ο αριθμός $(5\alpha+3)^5+(5\beta+2)^4+(5\gamma+1)^3$ διαιρείται με το 5.

2) Να αποδείξετε ότι το κλάσμα $\dfrac{\mathbf{3\cdot 10^{2001}+5\cdot 10^{1999}+1}}{\mathbf{4\cdot 10^{2003}+3\cdot 10^{2000}+2}}$, απλοποιείται με το 9.

(Ιταλία 1993)

Απόδειξη

($1^{ος}$ τρόπος)
Είναι $10\equiv 1(\text{mod}\,9)\Rightarrow 10^{2001}\equiv 1(\text{mod}\,9)\Rightarrow 3\cdot 10^{2001}\equiv 3(\text{mod}\,9)$.
Όμοια $5\cdot 10^{1999}\equiv 5(\text{mod}\,9)$, $4\cdot 10^{2003}\equiv 4(\text{mod}\,9)$, $3\cdot 10^{2000}\equiv 3(\text{mod}\,9)$, άρα θα έχουμε:
$\alpha=3\cdot 10^{2001}+5\cdot 10^{1999}+1\equiv(3+5+1)(\text{mod}9)\Rightarrow 3\cdot 10^{2001}+5\cdot 10^{1999}+1\equiv 9(\text{mod}9)\Rightarrow\alpha=9\lambda$.
Όμοια $\beta=4\cdot 10^{2003}+3\cdot 10^{2000}+2\equiv(4+3+2)(\text{mod}9)\Rightarrow 4\cdot 10^{2003}+3\cdot 10^{2000}+2\equiv 9(\text{mod}9)\Rightarrow\beta=9\lambda$,
οπότε το αρχικό κλάσμα απλοποιείται με το 9.
($2^{ος}$ τρόπος)
Το άθροισμα των ψηφίων του αριθμητή διαιρείται με το 9. Όμοια το άθροισμα των ψηφίων του παρονομαστή διαιρείται με το 9, επομένως το κλάσμα απλοποιείται με το 9.

3) Δίνονται οι ακέραιοι αριθμοί α, β, γ για τους οποίους ισχύει $\mathbf{\alpha+\beta+\gamma=0}$. Να αποδείξετε ότι: $\mathbf{\alpha^3+\beta^3+\gamma^3\equiv 0(\text{mod}\,3)}$.

(Τσεχία 2001)

Απόδειξη

Επειδή $\alpha+\beta+\gamma=0$, από την ταυτότητα Euler θα έχουμε $\alpha^3+\beta^3+\gamma^3 3\alpha\beta\gamma$, οπότε $3/(\alpha^3+\beta^3+\gamma^3)$, άρα θα έχουμε θα είναι $\alpha^3+\beta^3+\gamma^3\equiv 0(\text{mod}\,3)$.

4) Να αποδείξετε ότι ο αριθμός $\mathbf{\alpha=1999+1999^2+1999^3+...+1999^{1998}}$ διαιρείται με τον 1998.

(Βέλγιο 1998)

Απόδειξη

($1^{ος}$ τρόπος)
Είναι $1999\equiv 1(\text{mod}\,1998)$, οπότε θα είναι:

$\alpha \equiv(1+1+1+...+1)(\text{mod } 1998)\Rightarrow \alpha \equiv 1998(\text{mod } 1998)\Rightarrow \alpha \equiv 0(\text{mod } 1998)$.

($2^{ος}$ τρόπος)

Είναι $1999=1998+1$, οπότε $1999^{\nu} =(1998+1)^{\nu}=$πολ$1998+1$.

Άρα $\alpha=$πολ$1998+(1+1+....+1)=$πολ$1998+1998=$πολ1998.

5) Να αποδειχθεί ότι δεν υπάρχει φυσικός ν, τέτοιος ώστε οι αριθμοί:
$\alpha=\nu^3+3\nu^2+2\nu+1$ και $\beta=3\nu^2+3\nu-1$ να έχουν το ίδιο άθροισμα ψηφίων.

(Ρουμανία 1997)

Απόδειξη

Ξέρουμε ότι κάθε θετικός ακέραιος αριθμός ν είναι ισότιμος με το άθροισμα των ψηφίων του modulo 9.

Έστω ότι υπάρχει φυσικός αριθμός ν, τέτοιο ώστε το άθροισμα των ψηφίων του α να είναι ίδιο με το άθροισμα των ψηφίων του β. Έστω Α το άθροισμα των ψηφίων του α τότε θα ισχύει:

$\alpha\equiv A(\text{mod } 9)$ και $\beta\equiv A(\text{mod } 9)$, οπότε θα έχουμε $\alpha-\beta \equiv 0(\text{mod } 9)\Rightarrow 9/ \alpha-\beta$ (1).

Είναι $\alpha-\beta= \nu^3+3\nu^2+2\nu+1-3\nu^2-3\nu+1= \nu^3-\nu+2=\nu(\nu^2-1)+2= \nu(\nu-1)(\nu+1)+2$.

Ο αριθμός $\nu(\nu-1)(\nu+1)=3\lambda$, διότι οι $\nu-1$, ν, $\nu+1$ είναι τρείς διαδοχικοί ακέραιοι, άρα θα έχουμε $\alpha-\beta= 3\lambda+2$.

Από την (1) θα έχουμε $3/\alpha-\beta\Rightarrow 3/3\lambda+3\Rightarrow 3/2$ που είναι άτοπο.

6) Να αποδείξετε ότι ο αριθμός **$\alpha=3\lambda+2$, $\lambda\in\mathbf{N}$**, δεν είναι ποτέ τετράγωνο ακεραίου αριθμού.

(Λουξεμβούργο)

Απόδειξη

Θα είναι $\alpha\equiv 0(\text{mod } 3)$ ή $\alpha\equiv 1(\text{mod } 3)$ ή $\alpha\equiv 2(\text{mod } 3)$.

Θα έχουμε $\alpha^2 \equiv 0(\text{mod } 3)$ ή $\alpha^2 \equiv 1(\text{mod } 3)$ ή $\alpha^2 \equiv 4(\text{mod } 3)\Leftrightarrow \alpha^2 \equiv 1(\text{mod } 3)$.

Επειδή $\alpha=3\lambda+2\Rightarrow \alpha\equiv 2(\text{mod } 3)$ που είναι διαφορετικό $1(\text{mod } 3)$ και του $0(\text{mod } 3)$. Άρα ο α δεν είναι ποτέ τετράγωνο ακεραίου.

7) Να αποδείξετε ότι ο αριθμός $\boldsymbol{\alpha = \sqrt{5\nu^2+10}}$ είναι άρρητος για κάθε $\nu\in Z$.

(Μολδαβία 1997)

Απόδειξη

Αρκεί να αποδείξουμε ότι ο αριθμός $5\nu^2+10$ δεν είναι τέλειο τετράγωνο.

Έστω ότι ο αριθμός $5\nu^2+10$ είναι τέλειο τετράγωνο. Τότε επειδή $5\nu^2+10=5(\nu^2+2)$ και ο 5 είναι πρώτος, θα πρέπει τουλάχιστον $5/(\nu^2+2)$.

Για κάθε $\nu\in Z$ ισχύει: $\nu \equiv 0,1,2,3,4(\text{mod } 5)$, επομένως θα είναι:

$\nu^2 \equiv 0,1,4(\text{mod } 5)\Rightarrow \nu^2+2 \equiv 2,3,1(\text{mod } 5)$, δηλαδή το 5 δεν διαιρεί τον αριθμό ν^2+2, άρα ο αριθμός δεν μπορεί να είναι τέλειο τετράγωνο, επομένως ο α είναι άρρητος.

8) Να αποδείξετε ότι ο 121 δεν διαιρεί τον αριθμό $\boldsymbol{\nu^2+3\nu+5}$ για κάθε τιμή του $\nu\in Z$.

(Βουλγαρία)

Απόδειξη

Έστω ότι $\mathbf{121/v^2+3v+5}$, οπότε $\nu^2+3\nu+5\equiv 0(\text{mod } 121)$ (1).

Ο στόχος είναι να κάνουμε γινόμενο παραγόντων το πρώτο μέλος της (1) με ρητές ρίζες.

Το $\nu^2+3\nu+5$, δεν αναλύεται σε γινόμενο παραγόντων, γι΄ αυτό δοκιμάζουμε με το 11, διότι 11/121, οπότε $11/\nu^2+3\nu+5$.

Θα είναι $\nu^2+3\nu+5\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu+5\equiv 11(\text{mod } 11)\Rightarrow \nu^2+3\nu+5-11\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu-6\equiv 0(\text{mod } 11)$. Το τριώνυμο $\nu^2+3\nu-6$ έχει ρίζες άρρητες.

Δοκιμάζουμε με ένα πολλαπλάσιο του 11, έστω το 22, οπότε θα έχουμε:

Θα είναι $\nu^2+3\nu+5\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu+5\equiv 22(\text{mod } 11)\Rightarrow \nu^2+3\nu+5-22\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu-17\equiv 0(\text{mod } 11)$. Το τριώνυμο $\nu^2+3\nu-17$ έχει επίσης ρίζες άρρητες.

Δοκιμάζουμε με το 33, οπότε θα έχουμε:

Θα είναι $\nu^2+3\nu+5\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu+5\equiv 33(\text{mod } 11)\Rightarrow \nu^2+3\nu+5-33\equiv 0(\text{mod } 11)\Rightarrow \nu^2+3\nu-28\equiv 0(\text{mod } 11)$. Το τριώνυμο $\nu^2+3\nu-28$, έχει διακρίνουσα $\Delta=121$ και ρίζες 4 και -7, όποτε θα έχουμε $\nu^2+3\nu-28\equiv 0(\text{mod } 11)\Rightarrow (\nu-4)(\nu+7)\equiv 0(\text{mod } 11)\Leftrightarrow 11/(\nu-4)(\nu+7)$.

Επειδή το 11 είναι πρώτος θα έχουμε $11/\nu-4$ ή $11/\nu+7\Leftrightarrow \nu=11\kappa+4$ ή $\nu=11\mu-7$.

Έστω ότι $\nu=11\kappa+4$ τότε η παράσταση $A=\nu^2+3\nu+5$ θα γίνεται

$A=121\kappa^2+88\kappa+16+33\kappa+12+5\Leftrightarrow$

$A=121\kappa^2+121\kappa+17$, άρα το 121 δεν διαιρεί τον Α.

Έστω ότι $\nu=11\mu-7$ τότε η παράσταση $A=\nu^2+3\nu+5$ θα γίνεται $A=121\mu^2-154\mu+49+33\mu-21+49\Leftrightarrow A=121\mu^2-121\mu+28$, άρα το 121 δεν διαιρεί τον Α.

9) Να βρείτε τα δύο τελευταία ψηφία του αριθμού $\mathbf{9^{64}}$**.**

(Ουγγαρία 1991)

Λύση

($1^{ος}$ τρόπος)

Από προηγούμενη άσκηση έχουμε ότι:

Είναι $9^5\equiv -1(\text{mod } 25)\Rightarrow (9^5)^2\equiv(-1)^2\ (\text{mod } 25)\Rightarrow 9^{10}\equiv 1(\text{mod } 25)$.

Επίσης είναι $9^2\equiv 1(\text{mod } 4)\Rightarrow (9^2)^5\equiv 1^5\ (\text{mod } 4)\Rightarrow 9^{10}\equiv 1(\text{mod } 4)$ άρα θα έχουμε:

$$\left.\begin{matrix}\mathbf{9^{10}\equiv 1(mod\ 4)}\\ \mathbf{9^{10}\equiv 1(mod\ 25)}\end{matrix}\right\}\Rightarrow 9^{10}\equiv 1(\text{mod } 100)$$ διότι (4, 25)=1 (Εφαρμογή).

Θα είναι $9^{64}=9^{60}\cdot 9^4=(9^{10})^6\cdot 9^4$ και επειδή $9^{10}\equiv 1(\text{mod } 100)\Rightarrow (9^{10})^6\equiv 1(\text{mod } 100)$, οπότε θα έχουμε $9^{64}\equiv 9^4\ (\text{mod } 100)$, Επειδή $9^4=6561\equiv 61(\text{mod } 100)$, άρα τα δύο τελευταία ψηφία του αριθμού 9^{64} είναι το 61.

($1^{ος}$ τρόπος)

Είναι:

$9\equiv 9(\text{mod } 100)$.

$9^2\equiv 81(\text{mod } 100)\Rightarrow 9^2\equiv -19(\text{mod } 100)$.

$9^4 \equiv (-19)(-19) (\text{mod } 100) \Rightarrow 9^4 \equiv 361 (\text{mod } 100) \Rightarrow 9^4 \equiv 61 (\text{mod } 100)$.

$9^8 \equiv 61 \cdot 61 (\text{mod } 100) \Rightarrow 9^4 \equiv 3721 (\text{mod } 100) \Rightarrow 9^8 \equiv 21 (\text{mod } 100)$.

$9^{16} \equiv 21 \cdot 21 (\text{mod } 100) \Rightarrow 9^{16} \equiv 441 (\text{mod } 100) \Rightarrow 9^{16} \equiv 41 (\text{mod } 100)$.

$9^{32} \equiv 41 \cdot 41 (\text{mod } 100) \Rightarrow 9^{32} \equiv 1681 (\text{mod } 100)) \Rightarrow 9^{32} \equiv 81 (\text{mod } 100)$.

$9^{64} \equiv 81 \cdot 81 (\text{mod } 100) \Rightarrow 9^{64} \equiv 6561 (\text{mod } 100) \Rightarrow 9^{64} \equiv 61 (\text{mod } 100)$, οπότε τα δύο τελευταία ψηφία του αριθμού 9^{64} είναι 61.

10) Αν ο αριθμός p είναι πρώτος και p>3, να αποδείξετε ότι ο αριθμός $\boldsymbol{\alpha = 2^{4p} - 2^{2p} + 1}$ είναι σύνθετος.

(Σουηδία 1999)

Απόδειξη

Επειδή p>3 πρώτος, δοκιμάζουμε για p=5 να βρούμε τον αριθμό που διαιρεί τον α.

Θα είναι λοιπόν $\alpha = 2^{20} - 2^{10} + 1 = 1048576 - 1024 + 1 = 1047553$. Ο αριθμός αυτός δεν διαιρείται με το 2, ούτε με το 3, ούτε με 5. Δοκιμάζουμε με το 7, 11, 13 και διαπιστώνουμε ότι διαιρείται με το 13. Αυτό μας οδηγεί στο να αποδείξουμε ότι ο α διαιρείται με το 13.

Βρίσκουμε τις δυνάμεις του 2 που είναι:

$2, 2^2=4, 2^3=8, 2^4=16, 2^5=32, 2^6=64, 2^7=128, 2^8=256, 2^9=512$ και $2^{10}=1024$.

Μπορούμε εύκολα να διαπιστώσουμε ότι

$2^6 \equiv 64 (\text{mod } 13) \Rightarrow 2^6 \equiv (-1) (\text{mod } 13) \Rightarrow (2^6)^2 \equiv 1 (\text{mod } 13)$, δηλαδή θα πρέπει τον πρώτο αριθμό p να τον γράψουμε στη μορφή $p = 6\kappa + \upsilon$, με $0 \le \upsilon < 6$, για να εμφανιστεί το 2^{12}.

Ξέρουμε από προηγούμενη πρόταση, ότι ένας πρώτος αριθμός β μεγαλύτερος του 3 είναι της μορφής $6\kappa+1$ ή $6\kappa+5$, $\kappa \in N^*$.

Έστω ότι $p = 6\kappa + 1$ τότε θα είναι:

$2^{4p} = 2^{24\kappa+4} = (2^{12})^{2\kappa} \cdot 2^4 \equiv 2^4 (\text{mod } 13) \Rightarrow 2^{4p} \equiv 3 (\text{mod } 13)$ (1).

$2^{2p} = 2^{12\kappa+2} = (2^{12})^{\kappa} \cdot 2^2 \equiv 2^2 (\text{mod } 13) \Rightarrow 2^{4p} \equiv 4 (\text{mod } 13)$ (2).

Λόγω των (1) και (2) θα είναι $\alpha = 2^{4p} - 2^{2p} + 1 \equiv (3 - 4 + 1) (\text{mod } 13) \Rightarrow \alpha \equiv 0 (\text{mod } 13)$ και επειδή $\alpha \neq 13$, θα είναι $\alpha = 13\lambda$, οπότε σύνθετος.

Έστω ότι $p = 6\kappa + 5$ τότε θα είναι:

$2^{4p} = 2^{24\kappa+20} = (2^{12})^{2\kappa} \cdot 2^{20} \equiv 2^{20} (\text{mod } 13) \Rightarrow 2^{4p} \equiv (2^6)^3 \cdot 2^2 (\text{mod } 13) \Rightarrow 2^{4p} \equiv -4 (\text{mod } 13)$ (3).

$2^{2p} = 2^{12\kappa+5} = (2^{12})^{\kappa} \cdot 2^5 \equiv 2^5 (\text{mod } 13) \Rightarrow 2^{4p} \equiv 2^4 \cdot 2 (\text{mod } 13) \Rightarrow 2^{4p} \equiv 6 (\text{mod } 13)$ (4).

Λόγω των (3) και (4) θα είναι $\alpha = 2^{4p} - 2^{2p} + 1 \equiv (-4 - 6 + 1) (\text{mod } 13) \Rightarrow \alpha \equiv 0 (\text{mod } 13)$ και επειδή $\alpha \neq 13$, θα είναι $\alpha = 13\lambda$, οπότε σύνθετος.

11) Να βρεθεί το τελευταίο ψηφίο του αριθμού $\boldsymbol{\alpha = \underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot 7}}}}}}_{\textbf{1001 7-άρια}}}$.

(Ολυμπιάδα Καναδά) (ΕΜΕ Διαιρετότητα και Ισοτιμίες Α, Συγκελάκης)

Λύση

Αρκεί να εκφράσουμε τον αριθμό α στη μορφή $\alpha \equiv \beta \pmod{10}$, $\alpha, \beta \in N$, με $0 \le \beta \le 9$.
Ας δούμε πρώτα τις δυνάμεις του 7 modulo 10.
Είναι $7 \equiv 7 \pmod{10} \Rightarrow 7^2 \equiv 9 \pmod{10} \Rightarrow 7^3 \equiv 3 \pmod{10} \Rightarrow 7^4 \equiv 1 \pmod{10}$.
Επειδή $7^4 \equiv 1 \pmod{10} \Rightarrow 7^{4\kappa} \equiv 1 \pmod{10} \Rightarrow 7^{4\kappa+\upsilon} = 7^{4\kappa} \cdot 7^{\upsilon} \equiv 7^{\upsilon} \pmod{10}$ με $\upsilon = 0,1,2,3$.
Από τα παραπάνω φαίνεται ότι πρέπει να εκφράσουμε τον εκθέτη του 7, δηλαδή τον αριθμό $\beta = \underbrace{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}_{\mathbf{1000\ 7\text{-άρια}}}$ που αποτελείται από 1000 επτάρια με τη μορφή 4κ+υ. Δηλαδή αρκεί να δούμε τις δυνάμεις του 7 με το modulo 4.
Είναι $7 \equiv 3 \pmod{4} \Rightarrow 7^2 \equiv 1 \pmod{4} \Rightarrow 7^3 \equiv 3 \pmod{4} \Rightarrow 7^4 \equiv 1 \pmod{4}$, δηλαδή για τις άρτιες δυνάμεις του 7 έχουμε 1 (mod4) και για τις περιττές έχουμε 3(mod4).
Είναι λοιπόν $7^2 \equiv 1 \pmod{4} \Rightarrow 7^{2\kappa} \equiv 1 \pmod{4}$ και $7^{2\kappa+1} = 7^{2\kappa} \cdot 7 \equiv 7 \pmod{4} \Rightarrow$
$7^{2\kappa+1} \equiv 3 \pmod{4}$.

Άρα για τον αριθμό β θα έχουμε $\beta = \underbrace{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}_{\mathbf{1000\ 7\text{-άρια}}} \mathbf{= 3 (mod\, 4) \Rightarrow \beta - 3 = 4\kappa \Rightarrow \beta = 4\kappa + 3,\ \kappa \in Z.}$

Επομένως θα είναι $\alpha = \underbrace{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}_{\mathbf{1001\ 7\text{-άρια}}} \mathbf{= 7^{\beta} = 7^{4\kappa+3} = 7^{4\kappa} \cdot 7^3 \equiv 7^3 (mod\, 10) \equiv 3 (mod\ 10)}$,
άρα το τελευταίο ψηφίο του αριθμού α είναι το 3.

Διαγωνισμοί ΕΜΕ

1) Να βρεθούν τα δύο τελευταία ψηφία του αριθμού $\mathbf{2^{70}}$

(Γ Γυμν.12/11/88 ΠΜΔ)

Λύση

Είναι $2^{10}=1024\equiv 24(\text{mod}100)\Rightarrow 2^{70}\equiv 24^7\ (\text{mod}100)$ (1).

Αρκεί να υπολογίσουμε το $24^7\ (\text{mod}100)$.

Είναι $24\equiv 24\ (\text{mod}100)$,

$24^2\equiv 24^2\ (\text{mod}100)\Rightarrow 24^2\equiv 576\ (\text{mod}100)\Rightarrow 24^2\equiv 76\ (\text{mod}100)\Rightarrow$

$24^2\equiv -24(\text{mod}100)$,

$24^3\equiv -24^2\ (\text{mod}100)\Rightarrow 24^3\equiv 24\ (\text{mod}100)$,

$24^4\equiv 24^2\ (\text{mod}100)\Rightarrow 24^4\equiv -24\ (\text{mod}100)$,

$24^5\equiv -24^2\ (\text{mod}100)\Rightarrow 24^5\equiv 24\ (\text{mod}100)$,

$24^6\equiv 24^2\ (\text{mod}100)\Rightarrow 24^6\equiv -24\ (\text{mod}100)$ και

$24^7\equiv -24^2\ (\text{mod}100)\Rightarrow 24^7\equiv 24\ (\text{mod}100)$ (2).

Από τις σχέσεις (1), (2) τα δύο τελευταία ψηφία του 2^{70}, θα είναι το 24.

($2^{ος}$ τρόπος) (mathematica)

Είναι $2^{10}=1024=1025-1=25\kappa-1$, οπότε $2^{70}=(25\kappa-1)^7=25\lambda-1$, $\lambda\in Z$.

Για το λ έχουμε ότι $\lambda=4\mu+\upsilon$, με $\upsilon=0,1,2,3$, οπότε θα έχουμε περιπτώσεις:

Αν $\upsilon=0$ τότε $\lambda=4\mu$, άρα $2^{70}=25\cdot 4\mu-1=100\mu-1$, απορρίπτεται διότι το 2^{70} είναι πολλαπλάσιο του 4.

Αν $\upsilon=1$ τότε $\lambda=4\mu+1$, άρα $2^{70}=25\cdot(4\mu+1)-1=100\mu+24$, το οποίο είναι δεκτό διότι είναι πολλαπλάσιο του 4.

Αν $\upsilon=2$ τότε $\lambda=4\mu+2$, άρα $2^{70}=25\cdot(4\mu+2)-1=100\mu+49$, απορρίπτεται διότι το 2^{70} είναι πολλαπλάσιο του 4.

Αν $\upsilon=3$ τότε $\lambda=4\mu+3$, άρα $2^{70}=25\cdot(4\mu+3)-1=100\mu+74$, απορρίπτεται διότι το 2^{70} είναι πολλαπλάσιο του 4.

Άρα η μοναδική περίπτωση είναι η $\upsilon=1$, άρα τα δύο τελευταία ψηφία του 2^{70} είναι 24.

2) Επειδή είναι η 6η ΕΜΟ (Ελληνικά Μαθηματική Ολυμπιάδα) και το έτος είναι 1989, μπορείτε να βρείτε τα δυο τελευταία ψηφία του αριθμού $\mathbf{6^{1989}}$**;**

(ΕΜΟ 15/12/1989 Α Λυκείου)

Λύση (mathematica)

$$\mathbf{6^4=1296\equiv -4(\text{mod}100)}$$

$$\mathbf{6^{1989}=(6^4)^{497}\cdot 6\equiv(-4)^{497}\cdot 6(\text{mod}100)=-4^{497}\cdot 6(\text{mod}100).}$$

$$\mathbf{4^6=4096\equiv -4(\text{mod}100)}$$

$$\mathbf{4^{497}=(4^6)^{82}\cdot 4^5\equiv(-4)^{82}\cdot 4^5\ \text{mod}(100)=4^{87}(\text{mod}100)=(4^6)^{14}\cdot 4^3(\text{mod}100)=}$$

$$\mathbf{=(-4)^{14}\cdot 4^3(\text{mod}100)=4^{17}(\text{mod}100)=(4^6)^2\cdot 4^5(\text{mod}100)=(-4)^2\cdot 4^5(\text{mod}100)=}$$

$$\mathbf{4^7(\text{mod}100)=-16(\text{mod}100)}.$$

Άρα $\mathbf{6^{1989} \equiv 16 \cdot 6 (\mathrm{mod}\, 100) = 96 (\mathrm{mod}\, 100)}$.

3) Για ποιες τιμές του $\nu \in N$ ο αριθμός $\mathbf{A=1^{\nu}+2^{\nu}+3^{\nu}}$ διαιρείται με το 7;

(15/12/1989 Β Λυκείου)

1η Λύση (Ε. Μήτσιου)

Για n=1 η δοθείσα παράσταση δεν διαιρείται με το 7, για n=2 διαιρείται με το 7 και για n=3 δεν διαιρείται με το 7.

- Για $n=2\kappa$ έχουμε
  $A=1^n+2^n+3^n=1+4^{\kappa}+9^{\kappa}=1+4^{\kappa}+\pi o\lambda 7+2^{\kappa}=\pi o\lambda 7+1+2^{\kappa}+4^{\kappa}$ (1).
  - ✓ Εάν $\kappa=3\lambda$ τότε η (1) γίνεται (το
    $\pi o\lambda 7+1+2^{3\lambda}+4^{3\lambda}=\pi o\lambda 7+1+8^{\lambda}+64^{\lambda}=\pi o\lambda 7+1+\pi o\lambda 7+1+\pi o\lambda 7+1=\pi o\lambda 7+3$.
  - ✓ Εάν $\kappa=3\lambda+1$ τότε η (1) γίνεται
    $\pi o\lambda 7+1+2^{3\lambda+1}+4^{3\lambda+1}=\pi o\lambda 7+1+2\cdot 8^{\lambda}+1\cdot 64^{\lambda}$
    $=\pi o\lambda 7+1+2(\pi o\lambda 7+1)+4(\pi o\lambda 7+1)=\pi o\lambda 7+1+2+3=\pi o\lambda 7$.
  - ✓ Εάν $\kappa=3\lambda+2$ τότε η (1) γίνεται
    $\pi o\lambda 7+1+2^{3\lambda+2}+4^{3\lambda+2}=\pi o\lambda 7+1+4\cdot 8^{\lambda}+16\cdot 64^{\lambda}$
    $=\pi o\lambda 7+1+\pi o\lambda 7+4\cdot 1+\pi o\lambda 7+16\cdot 1=\pi o\lambda 7+1+4+16=\pi o\lambda 7$.

  Άρα εάν $n=2\kappa$, τότε πρέπει $\kappa=3\lambda+1$ ή $\kappa=3\lambda+2$, οπότε $n=6\lambda+2$ ή $n=6\lambda+4$, για να διαιρείται ο αριθμός Α με το 7.
- Για $n=2\kappa+1$ έχουμε
  $A=1^{2\kappa+1}+2^{2\kappa+1}+3^{2\kappa+1}=1+2\cdot 4^{\kappa}+3\cdot 9^{\kappa}=1+2\cdot 4^{\kappa}+\pi o\lambda 7+3\cdot 2^{\kappa}=\pi o\lambda 7+2(1+2^{\kappa}+4^{\kappa})+2^{\kappa}-1$.
  Βρήκαμε ότι αν $\kappa=3\lambda+1$ ή $\kappa=3\lambda+2$, τότε $1+2^{\kappa}+4^{\kappa}=\pi o\lambda 7$. Θα εξετάσουμε το $2^{\kappa}-1$ για $\kappa=3\lambda+1$ ή $\kappa=3\lambda+2$.
  - ✓ Εάν $\kappa=3\lambda+1$ τότε $2^{\kappa}-1=2^{3\lambda+1}-1=2\cdot 8^{\lambda}-1=\pi o\lambda 7+2\cdot 1-1=\pi o\lambda 7+1\neq\pi o\lambda 7$.
  - ✓ Εάν $\kappa=3\lambda+2$ τότε $2^{\kappa}-1=2^{3\lambda+2}-1=4\cdot 8^{\lambda}-1=\pi o\lambda 7+4\cdot 1-1=\pi o\lambda 7+3\neq\pi o\lambda 7$.
  - ✓ Εάν $\kappa=3\lambda$ τότε $2^{\kappa}-1=2^{3\lambda}-1=8^{\lambda}-1=\pi o\lambda 7+1-1=\pi o\lambda 7$, όμως τότε το Α δεν είναι πολ7.

  Άρα τελικά πρέπει ο n να είναι πολ2 και όχι πολ3 , δηλαδή πρέπει $n=6\kappa+2$ ή n6κ+4 ή διαφορετικά $n=6\kappa\pm 2$.

2η Λύση (Αλεξ. Συγκελάκης)

Το 7 είναι πρώτος αριθμός και (7,2)=1=(7,3), οπότε από το μικρό θεώρημα του Fermat θα έχουμε:

$\mathbf{2^{7-1} \equiv 1 (\mathrm{mod}\, 7) \Rightarrow 2^6 \equiv 1 (\mathrm{mod}\, 7)}$ και $\mathbf{3^{7-1} \equiv 1 (\mathrm{mod}\, 7) \Rightarrow 3^6 \equiv 1 (\mathrm{mod}\, 7)}$.

Άρα, το υπόλοιπο του 2^{ν} με το 7, θα επαναλαμβάνεται το πολύ κάθε 6 βήματα και μάλιστα το βήμα της επανάληψης (πόρισμα 2.2) θα είναι διαιρέτης του 6 (δηλαδή 1,2,3,6).

Όμοια και για το υπόλοιπο της διαίρεσης του 3^{ν} με το 7.

Αυτό που μένει λοιπόν να κάνουμε για να δούμε εποπτικά τα παραπάνω, είναι ένας απλός πίνακας δυνάμεων για να βρούμε το $1^{\nu}+2^{\nu}+3^{\nu}$ για τις διάφορες τιμές του υ, όπου

ν=6κ+υ, υ=0,1,2,3,4,5, θα χρειαστούν το πολύ 6 βήματα για να δούμε τα δυνατά υπόλοιπα των $2^ν$και $3^ν$ με το 7.

υ=ν(mod 6)	0 1 2 3 4 5	επανάληψη ανά
$1^ν$(mod 7)	1 1 1 1 1 1	1
$2^ν$(mod 7)	1 2 4 1 2 4	3
$3^ν$(mod 7)	1 3 2 6 4 5	6
$1^ν+2^ν+3^ν$(mod 7)	3 6 0 1 0 3	....

Τώρα φαίνεται καθαρά από τον παραπάνω πίνακα ότι ο αριθμός $1^ν+2^ν+3^ν$ είναι πολλαπλάσιο του 7, όταν έχει τη μορφή ν=6κ+2 ή 6κ+4. (Ή ακόμη, ότι ο αριθμός $1^ν+2^ν+3^ν$, διαιρούμενος με το 7 δεν αφήνει υπόλοιπο 2, 4, 5).

4) Εάν ο ρ είναι αριθμός πρώτος με ρ>3. να αποδείξετε ότι **$42ρ/3^ρ–2^ρ–1$.**
($2^{ος}$ Εσωτερικός Διαγωνισμός ΕΜΕ 1989) Διαιρετότητα και Ισοτιμίες Α. Συγκελάκης.
Απόδειξη
Αν ρ=5 τότε θα έχουμε 42ρ=42·5=210 και $3^ρ–2^ρ–1=3^5–2^5–1=243–32–1=210$ που διαιρείται με το 210.
Έστω ρ≥7.
Είναι 42ρ=2·3·7·ρ, οπότε θα αποδείξουμε ότι η παράσταση $3^ρ–2^ρ–1$ διαιρείτε με καθένα από τους παράγοντες 2, 3, 7 και ρ.
Είναι $3^ρ–2^ρ–1≡0–(–1)^ρ–1$(mod 3) και επειδή ρ περιττός θα είναι $3^ρ–2^ρ–1 ≡1–1$(mod 3) $⇒ 3^ρ–2^ρ–1 ≡ 0$(mod 3).
Όμοια είναι $3^ρ–2^ρ–1 ≡ 1^ρ–0–1$ (mod 2)$⇒ 3^ρ–2^ρ–1 ≡ 0$(mod 2).
Θα αποδείξουμε ότι $3^ρ–2^ρ–1 ≡ 0$(mod 7).
Ξέρουμε ότι κάθε πρώτος αριθμός ρ είναι της μορφής 6κ+1 ή 6κ+5.
Αν ρ=6κ+1 τότε $3^ρ–2^ρ–1=3^{6κ+1}–2^{6κ+1}–1$.
Είναι $3 ≡ 3$(mod 7)$⇒ 3^2 ≡ 2$(mod 7)$⇒ 3^3 ≡ –1$(mod 7)$⇒(3^3)^2 ≡ 1$(mod 7)$⇒$
$3^6 ≡ 1$(mod 7), οπότε $3^{6κ+1}=(3^6)^κ·3 ≡ 3$(mod 7) (1).
Επίσης $2 ≡ 2$(mod 7)$⇒ 2^2 ≡ 4$(mod 7)$⇒ 2^3 ≡ 1$(mod 7), οπότε
$2^{6κ+1}=(2^3)^{2κ}·2 ≡ 2$(mod 7) (2)
Τελικά από τις (1), (2) θα έχουμε $3^ρ–2^ρ–12^3 ≡ 3–2–1$(mod 7)=0(mod 7).
Από το πόρισμα του θεωρήματος του Fermat θα έχουμε:
$3^ρ ≡ 3$(mod ρ) και $2^ρ ≡ 2$(mod ρ), άρα $3^ρ–2^ρ–1 ≡ 3–2–1=0$ (mod ρ).
Επειδή (2, 3, 7, ρ)=1 θα έχουμε ότι $42ρ/3^ρ–2^ρ–1$.

Αν ρ=6κ+5 τότε $3^ρ–2^ρ–1=3^{6κ+5}–2^{6κ+5}–1$.
Είναι $3 ≡ 3$(mod 7)$⇒ 3^2 ≡ 2$(mod 7)$⇒ 3^3 ≡ –1$(mod 7)$⇒(3^3)^2 ≡ 1$(mod 7)$⇒$
$3^6 ≡ 1$(mod 7), οπότε $3^{6κ+5}=(3^6)^κ·3^5 ≡ 3^5$ (mod 7) $≡3^3·3^2$(mod 7) $≡ –2$(mod 7) (3).
Επίσης $2 ≡ 2$(mod 7)$⇒ 2^2 ≡ 4$(mod 7)$⇒ 2^3 ≡ 1$(mod 7), οπότε
$2^{6κ+5}=(2^3)^{2κ}·2^5 ≡ 2^5$ (mod 7) $≡ 2^3·2^2$ (mod 7) $≡ 2^2$ (mod 7) $≡ 4$ (mod 7) (4).
Από τις (3), (4) θα έχουμε $3^ρ–2^ρ–12^3 ≡ –2–4–1$(mod 7)=–7(mod 7)=0(mod 7).

Από το πόρισμα του θεωρήματος του Fermat θα έχουμε:

$3^\rho \equiv 3(\text{mod } \rho)$ και $2^\rho \equiv 2(\text{mod } \rho)$, άρα $3^\rho-2^\rho-1 \equiv 3-2-1=0 \text{ (mod } \rho)$.

Επειδή $(2, 3, 7, \rho)=1$ θα έχουμε ότι $42\rho/3^\rho-2^\rho-1$.

Άρα για κάθε ρ πρώτο με $\rho>3$. ισχύει $42\rho/3^\rho-2^\rho-1$.

5) Να αποδείξετε ότι υπάρχουν φυσικοί αριθμοί που τα τέσσερα τελευταία ψηφία τους είναι 1994 και διαιρούνται με το 1993.

(ΕΜΕ 1994)

Απόδειξη (Α. Συγκελάκης)

Ο αριθμός αυτός είναι της μορφής $\underbrace{\overline{\alpha_\nu\alpha_{\nu-1}\alpha_{\nu-2}\cdots\alpha_4}}_{\mathbf{A}}\mathbf{1994}=\mathbf{10000A+1994}$

$=A(5\cdot1993+35)+1993+1 \equiv 35A+1(\text{mod}1993)$.

Για να είναι $35A+1 \equiv 0 \text{ (mod}1993)$ θα πρέπει $35A+1=1993\kappa$, $\kappa\in Z$.

Δηλαδή $\mathbf{A=57\kappa-\frac{2\kappa+1}{35}}$ (1). Άρα θα πρέπει $2\kappa+1$ να είναι πολλαπλάσιο του 35.

Για $\kappa=17$ έχουμε $A=968$. Ο αριθμός λοιπόν 6681994 είναι πολλαπλάσιο του 1993.

Υπάρχουν άπειροι τέτοιοι αριθμοί αφού η (1) έχει άπειρες λύσεις.

6) Να προσδιορίσετε τους πρώτους αριθμούς $\mathbf{x,y}$ για τους οποίους ο αριθμός $\boldsymbol{x^{x+1}+y^{y+1}}$ είναι πρώτος.

(Ευκλείδης Β Λυκείου 94-95)

Λύση (mathematica)

Αν οι $\mathbf{x,y}$ ήταν και οι δύο περιττοί ή και οι δύο άρτιοι τότε ο αριθμός $\mathbf{x^{x+1}+y^{y+1}}$ θα ήταν άρτιος πρώτος και μεγαλύτερος του 2, άτοπο.

Άρα ένας από τους $\mathbf{x,y}$ είναι άρτιος πρώτος δηλαδή είναι το 2.

Έστω $\mathbf{x=2}$ (και $\mathbf{y}$ περιττός). Τότε ο αριθμός $\mathbf{2^{2+1}+y^{y+1}}$ θα ήταν πρώτος.

Αν ήταν $y\equiv\pm1(\text{mod } 3)$ τότε επειδή ο $y+1$ είναι άρτιος, άρα $y^{y+1} \equiv 1(\text{mod } 3)$ κι έτσι $8+y^{y+1} \equiv 9 \equiv 0(\text{mod } 3)$, άτοπο διότι αφενός ο αριθμός $8+y^{y+1}$ είναι πρώτος και είναι μεγαλύτερος του 3 άρα δε μπορεί να διαιρείται από το 3.

Άρα $y\equiv0(\text{mod } 3)$ κι επειδή ο y είναι πρώτος είναι $y=3$.

Πράγματι ο αριθμός $2^3+3^4=89$ είναι πρώτος.

Άρα έχουμε τη λύση $(x,y)=(2,3)$ και λόγω συμμετρίας έχουμε και την $(x,y)=(3,2)$.

7) Εάν ο ρ είναι αριθμός πρώτος με $\rho>3$. να αποδείξετε ότι $\mathbf{20\rho/5^\rho-4^\rho-1.}$

(Εσωτερικός Διαγωνισμός ΕΜΕ 1995) Διαιρετότητα και Ισοτιμίες Α, Συγκελάκης.

Απόδειξη

Αν $\rho=5$ τότε θα έχουμε $20\rho=20\cdot5=100$ και $5^\rho-4^\rho-1=5^5-4^5-1=3125-1024-1=2100$ που διαιρείται με το 100.

Έστω $\rho\geq7$.

Τότε θα είναι $5^\rho-4^\rho-1 \equiv 0-(-1)^\rho-1 \pmod 5$ και επειδή ρ περιττός θα είναι $5^\rho-4^\rho-1 \equiv 1-1 \pmod 5 \Rightarrow 5^\rho-4^\rho-1 \equiv 0 \pmod 5$.

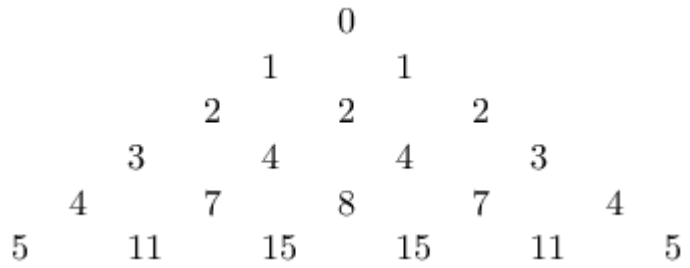
Όμοια είναι $5^\rho-4^\rho-1 \equiv 1^\rho-0-1 \pmod 4 \Rightarrow 5^\rho-4^\rho-1 \equiv 0 \pmod 4$.

Από το πόρισμα του θεωρήματος του Fermat θα έχουμε:

$5^\rho \equiv 5 \pmod \rho$ και $4^\rho \equiv 4 \pmod \rho$, άρα $5^\rho-4^\rho-1 \equiv 5-4-1=0 \pmod \rho$.

Επειδή $(4,5,\rho)=1$ θα έχουμε ότι $20\rho / 5^\rho-4^\rho-1$.

8) Θεωρούμε μία τριγωνική τοποθέτηση των αριθμών 0, 1, 2, 3,.... . Οι αριθμοί που βρίσκονται στο εσωτερικό του τριγώνου είναι ίσοι με το άθροισμα των δύο γειτονικών αριθμών της προηγούμενης σειράς. Για παράδειγμα οι έξι πρώτες σειρές είναι:



Έστω S(n) το άθροισμα των αριθμών της n σειράς. Να προσδιορίσετε τα δύο τελευταία ψηφία του S(100).

(Θέμα 4ο 3η προκριματική φάση 1995 Γυμνάσιο)

Λύση

Είναι S(1)=0, S(2)=2, S(3)=6, S(4)=14, S(5)=30....

Θα προσπαθήσουμε να βρούμε ένα τρόπο που να υπολογίζει το S(n) συναρτήσει του n.

Ας δούμε πως δημιουργείται το άθροισμα κάθε γραμμής.

Η 3^η γραμμή έχει άθροισμα $S(3)=2+2+2=(1+1)+(1+1)+(1+1)=2S(2)+2$.

Αυτό μπορεί να δικαιολογηθεί ως εξής:

Στο S(3) για τη κατασκευή του μεσαίου $2=(1+1)$ χρησιμοποιήσαμε τις δύο μονάδες της $2^{\eta\varsigma}$ γραμμής. Για τα δύο άλλα δυάρια, ένα αριστερά και ένα δεξιά χρησιμοποιήσαμε, από μία μονάδα, δηλαδή συνολικά χρησιμοποιήσαμε 2S(2), και προσθέσαμε από μία μονάδα επιπλέον.

Όμοια η 4^η γραμμή έχει άθροισμα:

$S(4)=3+4+4+3=(1+2)+(2+2)+(2+2)+(2+1)=2S(3)+2$.

Όμοια η 5^η γραμμή έχει άθροισμα:

$S(5)=4+7+8+7+4=(1+3)+(3+4)+(4+4)+(4+3)+(3+1)=2S(4)+2$.

Γενικά η $S(n)=2S(n-1)+2$ (1).

Αυτή η σημαντική παρατήρηση δεν μας βοηθάει να βρούμε τα δύο τελευταία ψηφία του S(100), διότι η σχέση (1) είναι ένας αναδρομικός τύπος για το S(n). Δηλαδή αν θέσουμε n=100 τότε η (1) γίνεται $S(100)=2S(99)+2$, πράγμα που δεν μας βοηθά να βρούμε το S(100).

Θα προσπαθήσουμε να βρούμε κάποια άλλη σχέση που να συνδέει το S(n) με το n.

Είναι $S(3)=6=2^3-2$, το $S(4)=14=2^4-2$, το $S(5)=30=2^5-2$, το $S(2)=2=2^2-2$ και το $S(1)=0=2^1-2$, οπότε φαίνεται ότι το $S(n)=2^n-2$.

Αυτό βέβαια θέλει απόδειξη, δηλαδή θα αποδείξουμε ότι $S(n)=2^n-2$ (2).
Θα το λύσουμε με τη βοήθεια της μαθηματικής επαγωγής.
Η πρόταση (1) προφανώς ισχύει για n=1.
Πράγματι για n=1 η (2) γίνεται $S(1)=2^1-2=0$, που ισχύει.
Υποθέτουμε ότι η πρόταση ισχύει για n=k, $S(k)=2^k-2$ (3)
και θα αποδείξουμε ότι η πρόταση ισχύει και για n=k+1, δηλαδή θα αποδείξουμε ότι ισχύει $S(k+1)=2^{k+1}-2$ (4).
Η (3)$\Rightarrow 2S(k)=2^{k+1}-4\Rightarrow 2S(k)+2=2^{k+1}-2$ (5).
Από τις σχέσεις (4) , (5) αρκεί να αποδείξουμε $S(k+1)=2S(k)+2$, το οποίο ισχύει λόγω της (1).
Πράγματι η (1) για n=k+1 γίνεται $S(k+1)=2S(K+1-1)+2\Rightarrow S(k+1)=2S(k)+2$.
Η (1) για n=100 γίνεται $S(100)=2^{100}-2$, οπότε πρέπει να βρούμε τα τελευταία δύο ψηφία του $S(100)=2^{100}-2$, δηλαδή αρκεί να υπολογίσουμε το $2^{100}-2\equiv\beta(\text{mod } 100)$, με $0\le\beta\le 99$.
($1^{ος}$ τρόπος)
Είναι $\boldsymbol{\phi(100)=100\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)=40}$, άρα το υπόλοιπο του 2^v με το 100, θα επαναλαμβάνεται το πολύ κάθε 40 βήματα.
Είναι $2^{10}\equiv 24(\text{mod } 100)\Rightarrow 2^{20}\equiv 76(\text{mod } 100)\Rightarrow 2^{40}\equiv 76(\text{mod } 100)\Rightarrow 2^{80}\equiv 76(\text{mod } 100)$ άρα $2^{100}\equiv 76^2 (\text{mod } 100)\Rightarrow 2^{100}\equiv 76 (\text{mod } 100)$, οπότε $2^{100}-2\equiv 74(\text{mod } 100)$.
Επομένως τα δύο τελευταία ψηφία του S(100) είναι 74.
($2^{ος}$ τρόπος)
Είναι $2^{10}=1024=1025-1=25\kappa-1$, οπότε $2^{100}=(25\kappa-1)^{10}=25\lambda+1$, $\lambda\in Z$.
Για το λ έχουμε ότι $\lambda=4\mu+\upsilon$, με $\upsilon=0,1,2,3$, οπότε θα έχουμε περιπτώσεις:
Αν $\upsilon=0$ τότε $\lambda=4\mu$, άρα $2^{100}=25\cdot 4\mu+1=100\mu+1$, απορρίπτεται διότι το 2^{100} είναι πολλαπλάσιο του 4.
Αν $\upsilon=1$ τότε $\lambda=4\mu+1$, άρα $2^{100}=25\cdot(4\mu+1)+1=100\mu+26$, απορρίπτεται διότι το 2^{100} είναι πολλαπλάσιο του 4.
Αν $\upsilon=2$ τότε $\lambda=4\mu+2$, άρα $2^{100}=25\cdot(4\mu+2)+1=100\mu+51$, απορρίπτεται διότι το 2^{100} είναι πολλαπλάσιο του 4.
Αν $\upsilon=3$ τότε $\lambda=4\mu+3$, άρα $2^{100}=25\cdot(4\mu+3)+1=100\mu+76$, το οποίο είναι δεκτό διότι είναι πολλαπλάσιο του 4.
Άρα η μοναδική περίπτωση είναι η $\upsilon=3$, άρα τα δύο τελευταία ψηφία του 2^{100} είναι 76.
Επομένως τα δύο τελευταία ψηφία του S(100) είναι 74.
($3^{ος}$ τρόπος) (mathematica)
Είναι $100=4\cdot 25$, με (25,4)=1, οπότε θα δουλέψουμε με modulo 4 και modulo 25, εκμεταλλευόμενοι το θεώρημα 1.10.
Είναι $25=5^2$, άρα $\boldsymbol{\phi(25)=25\left(1-\frac{1}{5}\right)=20}$, οπότε από το θεώρημα Euler θα έχουμε:
$2^{20}\equiv 1(\text{mod } 25)\Rightarrow 2^{100}\equiv 1(\text{mod } 25)$ (6).
Επίσης είναι: $2^2\equiv 0(\text{mod } 4)\Rightarrow 2^{100}\equiv 0(\text{mod } 4)$ (7).

Για να εφαρμόσουμε το θεώρημα 1.10 πρέπει να έχουμε τη μορφή $2^{100} \equiv \alpha \pmod{25}$ για το modulo 25 και τη μορφή $2^{100} \equiv \alpha \pmod 4$ για το modulo 4.
Θα πρέπει το α να το αντικαταστήσουμε με κάποιον ακέραιο μικρότερο του 100 τέτοιο ώστε $2^{100} \equiv \alpha \pmod{25} \Rightarrow 2^{100} \equiv 1 \pmod{25}$ και $2^{100} \equiv \alpha \pmod 4 \Rightarrow 2^{100} \equiv 0 \pmod 4$.
Ξεκινάμε από το 25 και βάζουμε στη θέση του α το 26.
Τότε $2^{100} \equiv 26 \pmod{25} \Rightarrow 2^{100} \equiv 1 \pmod{25}$, όμως $2^{100} \equiv 26 \pmod 4 \Rightarrow 2^{100} \equiv 2 \pmod 4$, άρα απορρίπτεται η τιμή α=26.
Διπλασιάζουμε το 25 και προσθέτουμε το 1, δηλαδή στη θέση του α βάζουμε το 51.
Τότε $2^{100} \equiv 51 \pmod{25} \Rightarrow 2^{100} \equiv 1 \pmod{25}$, όμως $2^{100} \equiv 51 \pmod 4 \Rightarrow 2^{100} \equiv 3 \pmod 4$, άρα απορρίπτεται η τιμή α=26.
Παίρνουμε για α=76.
Τότε $2^{100} \equiv 76 \pmod{25} \Rightarrow 2^{100} \equiv 1 \pmod{25}$, και $2^{100} \equiv 76 \pmod 4 \Rightarrow 2^{100} \equiv 0 \pmod 4$, άρα η τιμή α=26 είναι δεκτή.
Είναι $2^{100} \equiv 76 \pmod{25}$ και $2^{100} \equiv 76 \pmod 4$ με (25,4)=1, οπότε θα έχουμε:
$2^{100} \equiv 76 \pmod{100}$, επομένως τα δύο τελευταία ψηφία του S(100) είναι 74.

9)

I. Να αποδείξετε ότι δεν υπάρχει ακέραιος αριθμός ν τέτοιος ώστε ο $\mathbf{v^3 + 3v}$ να είναι περιττός.

II. Να αποδείξετε ότι δεν υπάρχουν ακέραιοι αριθμοί x και y τέτοιοι ώστε να ισχύει: $\mathbf{5x^3 - 4y^2 - 6xy + 15x + 6y - 5 = 0}$ (1).

(Α Λυκείου. Διαγωνισμός Θαλής 19/10/1996)

Λύση

I. Είναι $\mathbf{v^3 + 3v = v(v^2 + 3)}$.

Διακρίνουμε περιπτώσεις

- Αν ν άρτιος τότε ο ακέραιος $\mathbf{v^3 + 3v}$ θα είναι άρτιος.
- Αν ν περιττός τότε και ο $\mathbf{v^2}$ θα είναι περιττός, οπότε ο $\mathbf{(v^2 + 3)}$ θα είναι άρτιος, άρα το γινόμενο $\mathbf{v(v^2 + 3)}$ θα είναι αριθμός άρτιος.

II. Έστω ότι υπάρχουν ακέραιοι αριθμοί x και y τέτοιοι ώστε να ισχύει να ισχύει η (1).

Η (1) γράφεται $\mathbf{4x^3 + x^3 - 4y^2 - 6xy + 14x + x + 6y - 4 - 1 = 0 \Leftrightarrow x^3 + x - 1 + 2m = 0}$ (2), όπου $\mathbf{2m = 2(2x^3 - 2y^2 - 3xy + 7x + 3y - 2)}$.

Από τη σχέση (2) παίρνοντας mod 2 θα έχουμε: $\mathbf{x^3 + x - 1 \equiv 0 \bmod 2 \Leftrightarrow x^3 + x \equiv 1 \bmod 2}$ (3).

Επίσης είναι $\mathbf{2x \equiv 0 \bmod 2}$ και λόγω της (2) θα είναι $\mathbf{x^3 + 3x \equiv 1 \bmod 2}$, δηλαδή ο ακέραιος αριθμός $\mathbf{x^3 + 3x}$ είναι περιττός, που είναι άτοπο από το πρώτο ερώτημα.
Άρα δεν υπάρχουν x, y ακέραιοι που να ικανοποιούν την (1).

10) Να δείξετε ότι η εξίσωση $\mathbf{x^2 - 4x - 19^{96} - 96^{19} - 1992 = 0}$ (1), δεν έχει ακέραια λύση.

(Α Λυκείου. Διαγωνισμός Ευκλείδης 14/12/1996)

Λύση

Η (1)$\Leftrightarrow$ $\mathbf{x^2-4x+4-4-19^{96}-96^{19}-1992=0\Leftrightarrow(x-2)^2=19^{96}+96^{19}+1996}$ (2).

Ένας ακέραιος αριθμός α γράφεται α=3κ+υ, με υ=0, 1, 2.

Αν υ=0 τότε α=3κ$\Rightarrow$α$\equiv$0(mod 3)$\Rightarrow$ $\alpha^2\equiv$0(mod 3).

Αν υ=1 τότε α=3κ+1$\Rightarrow$α$\equiv$1(mod 3)$\Rightarrow$ $\alpha^2\equiv$1(mod 3).

Αν υ=2 τότε α=3κ+2$\Rightarrow$α$\equiv$2(mod 3)$\Rightarrow$ $\alpha^2\equiv$4(mod 3)$\Rightarrow$ $\alpha^2\equiv$1(mod 3), δηλαδή το τετράγωνο ενός ακεραίου είναι της μορφής $\alpha^2\equiv$0(mod 3) ή $\alpha^2\equiv$1(mod 3).

Είναι 19 $\equiv$1(mod 3)$\Rightarrow$ $19^{96}\equiv$1(mod 3)

96 $\equiv$0(mod 3)$\Rightarrow$ $96^{19}\equiv$0(mod 3)

1996 $\equiv$1(mod 3), οπότε θα έχουμε $19^{96}+96^{19}+1996\equiv$2(mod 3), δηλαδή ο αριθμός $19^{96}+96^{19}+1996$ δεν μπορεί να είναι τέλειο τετράγωνο, άρα η εξίσωση (1) είναι αδύνατη.

11) Έστω ότι για τους ακεραίους αριθμούς α, β, γ ισχύει η σχέση **(α–β)(β–γ)(γ–α)=α+β+γ** (1).

Να αποδείξετε ότι ο αριθμός **α+β+γ**, διαιρείται με το **27.**

(Β. Λυκείου. Διαγωνισμός Θαλής 18/10/1997)

Λύση

Θα χρησιμοποιήσουμε mod 3.

Για κάθε αριθμό α έχουμε α$\equiv$0(mod 3) ή α$\equiv$1(mod 3) ή α$\equiv$2(mod 3).

Έστω ότι οι α, β, γ διαιρούμενοι με το 3 αφήνουν διαφορετικό υπόλοιπο και ας είναι:
α$\equiv$0(mod 3), β$\equiv$1(mod 3) και γ$\equiv$ 2(mod 3), τότε α+β+γ$\equiv$3(mod 3)$\Rightarrow$ α+β+γ$\equiv$ 0(mod 3), δηλαδή 3/α+β+γ.

Θα είναι α–β $\equiv$–1(mod 3), β–γ $\equiv$–1(mod 3) και γ–α $\equiv$2(mod 3), οπότε θα είναι:

(α–β)(β–γ)(γ–α) $\equiv$2(mod 3) , δηλαδή το 3$\nmid$ (α–β)(β–γ)(γ–α).

Άρα δύο τουλάχιστον από τους α, β, γ θα είναι ισοϋπόλοιποι modulo 3.

Έστω ότι οι αριθμοί α, β είναι ισοϋπόλοιποι modulo 3, άρα θα είναι α–β $\equiv$0(mod 3), δηλαδή το 3 διαιρεί το πρώτο μέλος της (1), άρα θα πρέπει να διαιρεί και το δεύτερο.

Σε αυτή την περίπτωση θα πρέπει α+β+γ $\equiv$ 0(mod 3)$\Rightarrow$2α+β $\equiv$0(mod 3). Αυτό όμως γίνεται μόνο άν και οι τρείς αριθμοί είναι ισοϋπόλοιποι. Τότε όμως η κάθε παρένθεση θα διαιρείται με το 3, οπότε όλες μαζί θα διαιρούνται με το 27.

12) Αν ο p είναι πρώτος, να εξετάσετε αν ο αριθμός $\mathbf{N=p^{1997}+1997^p+1998^{1997+p}}$ είναι πρώτος.

(Γ Λυκείου. Διαγωνισμός Θαλής 18/10/1997)

Λύση

Διακρίνουμε δύο περιπτώσεις:

- Έστω ότι p=2, τότε θα είναι $\mathbf{N=2^{1997}+1997^2+1998^{1999}}$.

Είναι 2 $\equiv$–1(mod 3)$\Rightarrow$ $2^{1997}\equiv$–1(mod 3),

$1997 \equiv 2(\text{mod } 3) \Rightarrow 1997^2 \equiv 4(\text{mod } 3) \Rightarrow 1997^2 \equiv 1(\text{mod } 3)$ και

$1998 \equiv 0(\text{mod } 3) \Rightarrow 1998^{1999} \equiv 0(\text{mod } 3)$, οπότε $\mathbf{2^{1997} + 1997^2 + 1998^{1999} \equiv 0(\text{mod } 3)}$, δηλαδή ο αριθμός 3/N και επειδή N>3, ο N θα είναι σύνθετος.

- Έστω ότι p>2, τότε ο p είναι περιττός.

Τότε οι αριθμοί $\mathbf{p^{1997}}$, $\mathbf{1997^p}$ θα είναι περιττοί , ως γινόμενοι περιττών, οπότε το άθροισμά τους θα είναι αριθμός άρτιος, ενώ ο αριθμός $\mathbf{1998^{1997+p}}$ θα είναι άρτιος.

Άρα ό αριθμός $\mathbf{N = p^{1997} + 1997^p + 1998^{1997+p}}$ θα είναι άρτιος , οπότε ο N θα είναι σύνθετος για κάθε τιμή του πρώτου αριθμού p.

13) Έστω $\nu \in N^*$. Να αποδείξετε ότι οι αριθμοί $\boldsymbol{\alpha=\nu(\nu-1)}$ **και** $\boldsymbol{\beta=(\nu+1)^2}$ έχουν διαφορετικό άθροισμα ψηφίων.

(Α Λυκείου. Διαγωνισμός Ευκλείδης 1997)

Λύση

($1^{ος}$ τρόπος)

Από το θεώρημα 1.9, ξέρουμε ότι κάθε ακέραιος είναι ισότιμος με το άθροισμα των ψηφίων του modulo 9, άρα θα είναι και modulo 3.

Αν οι αριθμοί α, β έχουν το ίδιο άθροισμα ψηφίων τότε θα έχουμε:

$\alpha \equiv \sigma(\text{mod } 3)$, $\beta \equiv \sigma(\text{mod } 3)$, όπου σ το άθροισμα των ψηφίων του.

Τότε θα είναι $\alpha - \beta \equiv 0(\text{mod } 3)$, δηλαδή $3/\alpha-\beta$.

Είναι $\beta-\alpha=(\nu+1)^2-\nu(\nu-1)=\nu^2+2\nu+1-\nu^2+\nu=3\nu+1$, και επειδή $3\nmid(\alpha-\beta)$ οι αριθμοί α, β δεν έχουν το ίδιο άθροισμα ψηφίων.

($2^{ος}$ τρόπος)

Οι αριθμοί ν−1, ν, ν+1 είναι διαδοχικοί ακέραιοι, οπότε ένας μόνο θα είναι πολλαπλάσιο του 3.

- Έστω ότι ο ν+1 είναι πολλαπλάσιο του 3, τότε και $(\nu+1)^2$ θα είναι πολλαπλάσιο του3.

Επειδή οι αριθμοί ν, ν−1 δεν είναι πολλαπλάσια του 3, ο ένα θα είναι 3λ+1 και ο άλλος 3λ+2, οπότε $\nu(\nu-1)=(3\lambda+1)(3\lambda+2)=\text{πολ}3+2$, που δεν είναι πολλαπλάσιο του 3.

- Έστω ότι ο ν+1 δεν είναι πολλαπλάσιο του 3, τότε $(\nu+1)^2=3\pi+1$, δηλαδή ο αριθμός $(\nu+1)^2$ διαιρούμενος με το 3 δίνει υπόλοιπο 1.

Από τους άλλους δύο διαδοχικούς αριθμού ν, ν−1 ο ένα θα έχει τη μορφή 3δ και ο άλλος 3δ+2, οπότε το γινόμενο ν(ν−1) θα είναι πολλαπλάσιο του 3.

Από τα παραπάνω φαίνεται ότι μόνο ένας από τους αριθμούς $(\nu+1)^2$, ν(ν−1) είναι πολλαπλάσιο του 3 και επειδή ξέρουμε ότι ένας αριθμός είναι πολλαπλάσιο του 3, αν και μόνο αν, το άθροισμα των ψηφίων του διαιρείται με το 3, άρα τα δυο αθροίσματα δεν μπορούν να είναι ίσα.

14) Να δειχτεί ότι ο αριθμός $\alpha=\underbrace{111...1}_{\nu\ \psi\eta\phi\acute{\iota}\alpha}2\underbrace{111...1}_{\nu\ \psi\eta\phi\acute{\iota}\alpha}$ είναι σύνθετος, για κάθε ν∈N*.

(Β Λυκείου. Διαγωνισμός Ευκλείδης 1997)

Λύση

(1ος τρόπος)

Ο αριθμός α γραμμένος στη δεκαδική του παράσταση θα είναι:

$\alpha=10^{2\nu}+10^{2\nu-1}+...+2\cdot10^{\nu}+10^{\nu-1}+...+10+1=$

$(10^{2\nu}+10^{2\nu-1}+...+10^{\nu}+10^{\nu-1}+...+10+1)+10^{\nu}$ (1).

Είναι $\beta^{\mu}-1=(\beta-1)(\beta^{\mu-1}+\beta^{\mu-2}+...+\beta+1)\Leftrightarrow\beta^{\mu-1}+\beta^{\mu-2}+...+\beta+1=\frac{\beta^{\mu}-1}{\beta-1}$,

οπότε θέτοντας όπου β=10 και μ=2ν+1θα έχουμε:

$10^{2\nu}+10^{2\nu-1}+...+10+1=\frac{10^{2\nu+1}-1}{10-1}=\frac{10^{2\nu+1}-1}{9}$, οπότε η (1) γίνεται

$\alpha=\frac{10^{2\nu+1}-1}{9}+10^{\nu}=\frac{10^{2\nu+1}+9\cdot10^{\nu}-1}{9}=\frac{10^{2\nu+1}+10\cdot10^{\nu}-10^{\nu}-1}{9}=$

$\frac{10^{2\nu+1}+10^{\nu+1}-(10^{\nu}+1)}{9}=\frac{10^{\nu+1}(10^{\nu}+1)-(10^{\nu}+1)}{9}=\frac{(10^{\nu}+1)(10^{\nu+1}-1)}{9}$ (2).

Είναι $10\equiv1(\text{mod }9)\Rightarrow10^{\nu+1}\equiv1(\text{mod }9)\Rightarrow10^{\nu+1}-1\equiv0(\text{mod }9)\Rightarrow10^{\nu+1}-1=9\kappa$ (3).

Η (2) λόγω της (3) γίνεται: $\alpha=\frac{(10^{\nu}+1)9\kappa}{9}=(10^{\nu}+1)\kappa$, με κ∈N, άρα ο α είναι σύνθετος.

(2ος τρόπος)

Ας δούμε πρώτα, μια περίπτωση γραφής του α αν για παράδειγμα ν=5.

Θα είναι $\alpha=11111211111=\begin{array}{r}11111100000\\+\quad\ 111111\\\hline 11111211111\end{array}$, άρα τον αριθμό α μπορούμε να τον γράψουμε και με τη μορφή: $\alpha=11111211111=11111\cdot10^5+111111=11111\cdot(10^5+1)$ που είναι σύνθετος. Με ανάλογο τρόπο γενικεύοντας θα έχουμε:

$\alpha=\underbrace{111...1}_{\nu\ \psi\eta\phi\acute{\iota}\alpha}2\underbrace{111...1}_{\nu\ \psi\eta\phi\acute{\iota}\alpha}=\underbrace{111...1}_{\nu+1\ \psi\eta\varphi}\underbrace{00...0}_{\nu\ \psi\eta\phi\acute{\iota}\alpha}\underbrace{111...1}_{\nu+1\ \psi\eta\varphi}=\underbrace{111...1}_{\nu+1\ \psi\eta\varphi}\cdot10^{\nu}+\underbrace{111...1}_{\nu+1\ \psi\eta\varphi}=$

$\underbrace{111...1}_{\nu+1\ \psi\eta\varphi}\cdot(10^{\nu}+1)$, οπότε ο αριθμός α είναι σύνθετος.

15) Για ποιους θετικούς ακεραίους m και n μεγαλύτερους του 1 ισχύει: $2^{1999}+3^{1999}=m^n$;

(Γ Λυκείου. Διαγωνισμός Θαλής 24/10/1998)

Λύση (ΕΜΕ)

Έστω ότι $2^{1999}+3^{1999}=m^n$ με n>1.

Είναι $2^{1999}+3^{1999}=(2+3)(2^{1998}-2^{1997}\cdot 3+2^{1996}\cdot 3^2-...-2\cdot 3^{1997}+3^{1998})$.

Η παράσταση $(2^{1998}-2^{1997}\cdot 3+2^{1996}\cdot 3^2-...-2\cdot 3^{1997}+3^{1998})$ είναι ισοϋπόλοιπη ως προς τη διαίρεση με το 5 με τη παράσταση

$2^{1998}-2^{1997}\cdot(-2)+2^{1996}\cdot(-2)^2-...-2\cdot(-2)^{1997}+(-2)^{1998}=1998\cdot 2^{1998}$ όμως το 5 δε διαιρεί τέλεια το $1998\cdot 2^{1998}$.

Έτσι ο εκθέτης του 5 στα α΄ μέλος της $2^{1999}+3^{1999}=m^n$ είναι 1, άρα n=1 (άτοπο).

16) Να προσδιορίσετε τους φυσικούς αριθμούς **ν** για τους οποίους ο αριθμός $2007+4^{\nu}$ είναι τέλειο τετράγωνο.

(Αρχιμήδης θέματα μεγάλων 24/2/2007)

Λύση

(1ος τρόπος) (mathematica)

Αν ν=0 τότε $2007+4^{\nu}=2008$ που δεν είναι τέλειο τετράγωνο.

Αν ν≥1 τότε $2007+4^{\nu}\equiv 2007\equiv 3(\mathrm{mod}\,4)$ που είναι αδύνατο, διότι το τετράγωνο ακεραίου modulo 4 είναι 0 ή 1.

(2ος τρόπος) (ΕΜΕ)

Έστω ότι ισχύει $2007+4^{\nu}=\kappa^2$, κ∈Ν. Τότε θα έχουμε $\kappa^2-4^{\nu}=2007\Leftrightarrow \kappa^2-2^{2\nu}=2007\Leftrightarrow(\kappa-2^{\nu})(\kappa+2^{\nu})=1\cdot 3\cdot 3\cdot 223$. Επειδή $\kappa-2^{\nu}<\kappa+2^{\nu}$, από την τελευταία ισότητα προκύπτουν τα συστήματα: $\left.\begin{matrix}\kappa-2^{\nu}&=&1\\ \kappa+2^{\nu}&=&2007\end{matrix}\right\}(\Sigma_1)$ ή $\left.\begin{matrix}\kappa-2^{\nu}&=&3\\ \kappa+2^{\nu}&=&669\end{matrix}\right\}(\Sigma_2)$ $\left.\begin{matrix}\kappa-2^{\nu}&=&9\\ \kappa+2^{\nu}&=&223\end{matrix}\right\}(\Sigma_3)$.

Όμως $(\Sigma_1)\Leftrightarrow\left.\begin{matrix}2\kappa&=&2008\\ 2\cdot 2^{\nu}&=&2006\end{matrix}\right\}\Rightarrow 2^{\nu}=1003$ που είναι άτοπο.

Επίσης $(\Sigma_2)\Leftrightarrow\left.\begin{matrix}2\kappa&=&672\\ 2\cdot 2^{\nu}&=&666\end{matrix}\right\}\Rightarrow 2^{\nu}=333$ που είναι άτοπο.

Επίσης $(\Sigma_3)\Leftrightarrow\left.\begin{matrix}2\kappa&=&232\\ 2\cdot 2^{\nu}&=&214\end{matrix}\right\}\Rightarrow 2^{\nu}=107$ που είναι άτοπο.

Άρα δεν υπάρχουν φυσικοί αριθμοί ν με την ιδιότητα ο αριθμός $2007+4^{\nu}$ να είναι τέλειο τετράγωνο.

17) Να αποδείξετε ότι δεν υπάρχουν ακέραιοι x,y,z τέτοιοι ώστε να ικανοποιούν την ισότητα $x^2+y^2-8z=6$.

(Θαλής 4/11/2000 Γ Λυκείου)

Λύση

(1ος τρόπος) (mathematica)

Πρέπει $\mathbf{x^2+y^2\equiv 6(mod\ 8)}$ που είναι προφανώς άτοπο, διότι κάθε τέλειο τετράγωνο είναι 0 ή 1 ή 4 modulo 8.

($2^{ος}$ τρόπος) (ΕΜΕ)

Έστω ότι υπάρχουν x, y, z∈Z τέτοιοι ώστε: $\mathbf{x^2+y^2-8z=6}$ ή $\mathbf{x^2+y^2=2(4z+3)}$ (1).

Κατ΄ αρχήν παρατηρούμε ότι το τετράγωνο ενός άρτιου αριθμού είναι άρτιος, ενώ το τετράγωνο ενός περιττού αριθμού είναι περιττός. Έτσι, αν οι ακέραιοι x και y στην ισότητα (1) είναι ένας άρτιος και ένας περιττός, τότε το πρώτο μέλος της (1) θα είναι περιττός αριθμός, ενώ το δεύτερο μέλος αυτής είναι άρτιος (άτοπο).

Άρα θα έχουμε μόνο τις περιπτώσεις:

I) x, y άρτιοι, δηλαδή x=2μ, y=2ω, μ, ν∈Z.

Τότε η (1) γίνεται $4\mu^2+4\nu^2=2(4z+3)$ ή $4\mu^2+2\nu^2=4z+3$, που είναι αδύνατη γιατί $2\mu^2+2\nu^2$ είναι άρτιος, ενώ ο 4z+3 είναι περιττός.

II) x,y περιττοί, δηλαδή x=2μ+1, y2ν+1, μ,ν∈Z. Τότε η (1) γίνεται $(2\mu+1)^2+(2\nu+1)^2=2(4z+3)$ ή $\mu(\mu+1)+\nu(\nu+1)=2z+1$ που είναι αδύνατη, γιατί οι αριθμοί μ(μ+1) και ν(ν+1) είναι άρτιοι, ενώ ο αριθμός 2z+1 είναι περιττός.

Βιβλιογραφία

1. Θεωρία Αριθμών ΕΜΕ
2. Εισαγωγή στη θεωρία Αριθμών για το Λύκειο Αλέξανδρος Συγκελάκης
3. Θεωρία Αριθμών Θανάση Ξένου
4. Ολυμπιάδες Μαθηματικών. Μαθητικοί διαγωνισμοί Α Λυκείου. Μπάμπης Στεργίου
5. Θεωρία Αριθμών Ι. Μαντά
6. Μαθηματικοί Διαγωνισμοί Χαράλαμπος Στεργίου Σιλουανός Μπραζιτίκος
7. Περιοδικά Ευκλείδης Α και Ευκλείδης Β.
8. Ασκήσεις Θεωρίας Αριθμών Βαγγέλη Σπανδάγου.
9. Μαθηματικές Ολυμπιάδες Δ. Γ. Κοντογιάννη
10. Waclaw Sierpinski 250 προβλήματα της στοιχειώδους Θεωρίας Αριθμών