ΑΛΓΕΒΡΑ, ΑΣΚΗΣΕΙΣ # 5

Πρόβλημα 1. Υπολογίστε τούς αριθμούς Euler $\phi(35)$, $\phi(48)$, $\phi(1000)$.

Πρόβλημα 2. **α)** Βρείτε το υπόλοιπο τής διαίρεσης τού 3^{47} με το 23.
β) Βρείτε το υπόλοιπο τής διαίρεσης τού 94^{200} διά 13.
γ) Βρείτε το υπόλοιπο τής διαίρεσης τού 7^{1000} διά 24.
δ) Βρείτε τό υπόλοιπο τής διαίρεσης τού 641^{108002} διά 63.

Πρόβλημα 3. **α)** Βρείτε το τελευταίο δεκαδικό ψηφίο τού αριθμού 7^{123}.
β) Βρείτε το τελευταίο δεκαδικό ψηφίο τού αριθμού 4321^{4321}.
γ) Βρείτε τα τελευταία δύο δεκαδικά ψηφία τού αριθμού 4321^{4321}.

Πρόβλημα 4. Ποιά ένδειξη δείχνει ένα 24-ωρο ρολόι, 5^{19} ώρες μετά τίς 3:00;

Πρόβλημα 5. **α)** Δείξτε ότι $10 \mid 101^{2003} - 1$.
β) Δείξτε ότι αν $a \in \mathbb{N}$ με $(a, 23) = 1$ τότε $23 \mid a^{154} - 1$.

Πρόβλημα 6. Δείξτε ότι το αντίστροφο τού $\bar{5}$ στον δακτύλιο $\mathbb{Z}_{101}$ είναι τό $\overline{85}$. Ποιό είναι τό υπόλοιπο τής διαίρεσης τού 5^{99} δια τού 101;

Πρόβλημα 7. Έστω p πρώτος αριθμός και έστω $\bar{a} \neq \bar{0}$ ένα στοιχείο τού $\mathbb{Z}_p$. Δείξτε ότι δεν υπάρχει στοιχείο τού $\mathbb{Z}_p$ που να ικανοποιεί την εξίσωση $x^p - x + \bar{a} = \bar{0}$ (δηλ. η εξίσωση δεν έχει ρίζα στο $\mathbb{Z}_p$).

Πρόβλημα 8. **α)** Δείξτε ότι αν $a \in \mathbb{N}$ με $(a, 10) = 1$ τότε $a^2 \equiv 1 \mathrm{mod} 10$ ή $a^2 \equiv 9 \mathrm{mod} 10$.
β) Δείξτε ότι για κάθε $n \in \mathbb{N}$ έχουμε ότι $4^n \equiv 4 \mathrm{mod} 10$ ή $4^n \equiv 6 \mathrm{mod} 10$.
γ) Δείξτε ότι αν $a \in \mathbb{Z}$ το τελευταίο δεκαδικό ψηφίο τού a^2 δεν μπορεί να είναι 2.

Πρόβλημα 9. Αποδείξτε ότι, γιά κάθε ακέραιο n, ο αριθμός $n^{37} - n$ είναι πολλαπλάσιο τού 383838. (Υπόδειξη: $383838 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 37$.)

Πρόβλημα 10. Έστω p περιττός πρώτος. Αποδείξτε ότι τά μόνα στοιχεία τού $\mathbb{Z}_p$, τα οποία έχουν αντίστροφο τόν ευατό τους, είναι τα $\bar{1}$ και $\overline{p-1}$. Βάσει αυτού αποδείξτε ότι $1 \cdot 2 \cdots p - 1 \equiv (p-1) \mathrm{mod} p$ και αποδείξτε το *Θεώρημα τού Wilson*: $(p-1)! \equiv -1 \mathrm{mod} p$.