ΑΛΓΕΒΡΑ, ΑΣΚΗΣΕΙΣ #4

Πρόβλημα 1. Έστω $a, n \in \mathbb{N}$ και έστω d=μ.κ.δ.(a, n). Δείξτε ότι ο $\frac{n}{d}$ είναι ο ελάχιστος φυσικός k με την ιδιότητα $n \mid ka$.

Πρόβλημα 2. **α)** Εστω a ακέραιος αριθμός. Δείξτε ότι το 4 δεν διαιρεί το $a^2 - 2$ ούτε το $a^2 - 3$.
β) Αν γιά τον ακέραιο a ισχύει ότι $4|a - 3$ δείξτε ότι δεν υπάρχουν ακέραιοι x, y γιά τούς οποίους έχουμε $x^2 + y^2 = a$.

Πρόβλημα 3. Έστω ότι $a^s \equiv 1 \mathrm{mod} m$ και $a^t \equiv 1 \mathrm{mod} m$. Αν $d =$ μ.κ.δ.(s, t) να δειχθεί ότι $a^d \equiv 1 \mathrm{mod} m$.

Πρόβλημα 4. Δείξτε ότι για κάθε φυσικό n έχουμε ότι $n^5 = n \mathrm{mod} 30$ (Υπόδειξη: αρχίστε με το $n^5 - n$).

Πρόβλημα 5. **α)** Γράψτε όλα τα μή μηδενικά στοιχεία τού δακτυλίου $\mathbb{Z}_{13}$ και δίπλα στο καθένα το αντίστροφό του.
β) Βρείτε τα αντιστρέψιμα στοιχεία τού δακτυλίου $\mathbb{Z}_{24}$. Για κάθε ένα από αυτά βρείτε το αντιστροφό του.

Πρόβλημα 6. Ποιό είναι το αντίστροφο $\bar{7}^{-1}$ τού στοιχείου $\bar{7}$ στο σώμα $\mathbb{Z}_{17}$;

Πρόβλημα 7. Αν $p \neq 2$ είναι πρώτος αριθμός γνωρίζουμε ότι τά μή-μηδενικά στοιχεία τού $\mathbb{Z}_p$ είναι αντιστρέψιμα. Βρείτε το αντίστροφο τού στοιχείου $\bar{2}$ (Υπόδειξη: κάνετε πρώτα μερικά παραδείγματα για συγκεκριμμένες τιμές τού p).

Πρόβλημα 8. Εστω R αντιμεταθετικός δακτύλιος.
α) Δείξτε, με επαγωγή, ότι αν $a, b \in R$, τότε για κάθε φυσικό n έχουμε $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$, όπου $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.
β) Από την συνδυαστική είναι γνωστό ότι το $\binom{n}{i}$ απαριθμεί το πλήθος των υποσυνόλων με i το πλήθος στοιχεία ενός συνόλου που έχει n το πλήθος στοιχεία. Επομένως είναι ένας φυσικός αριθμός. Δείξτε οτι αν p πρώτος αριθμός και $1 \leq i \leq p - 1$ τότε $p \mid \binom{p}{i}$.
Υπόδειξη: Έστω $\binom{p}{i} = n \in \mathbb{N}$. Τότε, $p! = i!(p - i)!n$. Το p διαιρεί το αριστερό μέλος άρα θα πρέπει να διαιρεί και το δεξί. Δείξτε ότι δεν διαιρεί το $i!$ και το $(p - i)!$ άρα θα πρέπει να διαιρεί το n.
γ) Δείξτε ότι αν $\bar{a}$, $\bar{b} \in \mathbb{Z}_p$, όπου p πρώτος αριθμός, τότε $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$ (Υπόδειξη: δείξτε πρώτα ότι $p\,\bar{a} = \overline{pa} = \bar{0}$).