

MEM 204 ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Φυλλάδιο Ασκήσεων 7

Άσκηση 7.1 Έστω $p > 3$ πρώτος αριθμός. Δείξτε ότι το άθροισμα των τετραγωνικών υπολοίπων modulo p διαιρείται από το p .

Άσκηση 7.2 Έστω $p > 2$ πρώτος και $S_n(p) = \sum_{k=1}^{p-1} k^n$, όπου $n > 1$ φυσικός αριθμός. Δείξτε ότι

$$S_n(p) \equiv \begin{cases} 0 \pmod{p} & , \text{αν } n \not\equiv 0 \pmod{p-1}, \\ -1 \pmod{p} & , \text{αν } n \equiv 0 \pmod{p-1}. \end{cases}$$

Άσκηση 7.3 Έστω $p > 2$ πρώτος αριθμός. Δείξτε ότι $(p-1)! \equiv -1 \pmod{p}$.

Άσκηση 7.4 Έστω $p > 3$ πρώτος αριθμός. Δείξτε ότι το γινόμενο των πρωταρχικών ριζών modulo p είναι ισότιμο με 1 modulo p .

Άσκηση 7.5 Έστω $p > 2$ πρώτος αριθμός και $d \mid p-1$. Ένας αριθμός $a \in \mathbb{Z}$, με $(a, p) = 1$ θα λέγεται d -δύναμη modulo p αν υπάρχει $b \in \mathbb{Z}$ τέτοιος ώστε $a \equiv b^d \pmod{p}$. Αποδείξτε ότι το πλήθος των d -δυνάμεων modulo p σε κάθε περιορισμένο σύνολο υπολοίπων modulo p είναι $\frac{p-1}{d}$.

Άσκηση 7.6 Έστω $p > 2$ πρώτος αριθμός και $d \mid p-1$. Δείξτε ότι το άθροισμα των (ανά δύο ανισότιμων) d -δυνάμεων modulo p διαιρείται από το p .