

# Ασκήσεις Θ. Αριθμών

6 Φυλλάδιο

Παράδοση Τετάρτη 11 Ιανουαρίου

1. Αν ισχύει

$$ab \equiv 1 \pmod{m},$$

να αποδειχτεί ότι ισχύει

$$\text{ord}_m a = \text{ord}_m b.$$

2. Αν ισχύει

$$\text{ord}_m a = r,$$

τότε θα ισχύει

$$\text{ord}_m a^n = \frac{r}{(n, r)}.$$

3. Αν για ένα πρώτο αριθμό  $p$  ισχύει

$$\text{ord}_p a = r \text{ και } \text{ord}_p b = s,$$

και επιπλέον ισχύει  $(r, s) = 1$ , να αποδειχτεί ότι θα ισχύει

$$\text{ord}_p ab = rs.$$

4. Αν  $a$  είναι μία αρχική ρίζα modulo  $m$ , τότε  $a^n$  είναι αρχική ρίζα modulo  $m$ , αν ισχύει  $(n, \phi(m)) = 1$ .

5. Αν  $w, u$  είναι δύο αρχικές ρίζες modulo  $p$ , όπου  $p$  πρώτος αριθμός, να αποδειχτεί ότι ισχύει

$$\text{ind}_u a \equiv \text{ind}_w a \cdot \text{ind}_u w \pmod{p-1}.$$

6. Να αποδειχτεί ότι το πλήθος των λύσεων της ισοδυναμίας

$$x^2 \equiv a \pmod{p},$$

όπου  $p$  περιττός πρώτος αριθμός είναι

$$N = \begin{cases} 1 + \left(\frac{a}{p}\right), & \text{αν } p \nmid a \\ 1, & \text{αν } p \mid a. \end{cases}$$