

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Έαρινό Έξάμηνο 2019

Καθηγητής Ν. Γ. Τζανάκης

Άσκησης τής 9ης εβδομάδας

1. Έστω περιττός αριθμός m και $(a, m) = 1$. Δείξτε ότι αν το σύμβολο Jacobi $\left(\frac{a}{m}\right) = -1$, τότε ή ισοτιμία $x^2 \equiv a \pmod{m}$ δεν έχει λύση. Αντιθέτως, αν $\left(\frac{a}{m}\right) = +1$ και ό m είναι σύνθετος (δηλαδή, όχι πρώτος), δεν σημαίνει όπωσδήποτε ότι ή ισοτιμία $x^2 \equiv a \pmod{m}$ έχει λύση! Δώστε παράδειγμα περιττού σύνθετου αριθμού m , τέτοιου ώστε $\left(\frac{a}{m}\right) = +1$ και ή ισοτιμία $x^2 \equiv a \pmod{m}$ να είναι αδύνατη.

2. Υπολογίστε τὰ παρακάτω σύμβολα Jacobi (οί “παρονομαστές” τών συμβόλων είναι πρώτοι):

$$\left(\frac{4321}{7919}\right), \left(\frac{10001}{48611}\right)$$

3. Δείξτε ότι κάθε μία από τις παρακάτω ισοτιμίες είναι επιλύσιμη και βρείτε τις λύσεις της.

$$x^2 \equiv 43 \pmod{3^7}, \quad x^2 \equiv 1492 \pmod{7^5}, \quad x^2 \equiv 3389 \pmod{11^4}.$$