UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
NUMBER THEORY - MEM204 (SPRING SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

5th exercise set

Exercise 1. Let p be a prime and $m \in \mathbb{Z}_{>0}$. Prove that the congruence

$$x^m \equiv 0 \pmod{p^m}$$

has exactly p^{m-1} solutions.

In the Exercises 2–5, we will study, whether a is a quadratic residue modulo n, for arbitrary n, if $(a, n) = 1$. In particular, Exercise 5 can be used as a stated theorem.

Exercise 2. Let $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$, where $r \geq 0$ and $n_i \geq 0$, be the prime factorization of n. Further, let $(a, n) = 1$. Then

$$x^2 \equiv a \pmod{n}$$

is solvable if and only if $x^2 \equiv a \pmod{p_i^{n_i}}$ is solvable for $i = 1, \ldots, k$ and $x^2 \equiv a \pmod{2^r}$ is solvable (if $r \geq 2$).

Exercise 3. Let p be an odd prime, $r \geq 1$ and $p \nmid a$. Then $x^2 \equiv a \pmod{p^r}$ is solvable if and only if $x^2 \equiv a \pmod{p}$ is solvable.

Exercise 4. Let a be an odd number and $r \geq 3$. Then $x^2 \equiv a \pmod{2^r}$ is solvable if and only if $a \equiv 1 \pmod{8}$.

Exercise 5. Let $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$, where $r \geq 0$ and $n_i \geq 0$, be the prime factorization of n. Further, let $(a, n) = 1$. Then

$$x^2 \equiv a \pmod{n}$$

is solvable if and only if $\left(\frac{a}{p_i}\right) = 1$, for all $i = 1, \ldots, n$ and

$$a \equiv \begin{cases} 1 \pmod{8}, & \text{if } r \geq 3, \\ 1 \pmod{4}, & \text{if } r = 2. \end{cases}$$

Exercise 6. Solve the congruence $4x^4 + 4x^3 + 6x^2 + 21x + 7 \equiv 0 \pmod{252}$.

Exercise 7. Compute the following symbols:

$$\left(\frac{-14}{71}\right), \left(\frac{219}{383}\right), \left(\frac{100}{31}\right), \left(\frac{3}{23}\right).$$

Exercise 8. Check whether $x^2 - 6x - 13 \equiv 0 \pmod{127}$ is solvable.

Exercise 9. Check whether $x^2 \equiv 7 \pmod{19}$ is solvable.

Exercise 10. Find all the primes $10 < p < 100$, such that $p \mid n^2 + 1$, for some n.

Exercise 11. Let p be prime, such that $p \equiv 3 \pmod{4}$. If $a^2 + b^2 \equiv 0 \pmod{p}$, show that $a \equiv b \equiv 0 \pmod{p}$.

Exercise 12. Show that, if n is a positive odd number,

$$\left(\frac{6}{n}\right) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \text{ or } \pm 5 \pmod{24}, \\ -1, & \text{if } n \equiv \pm 7 \text{ or } \pm 11 \pmod{24}. \end{cases}$$

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ - ΜΕΜ204 (ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2019-20)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

5ο σετ ασκήσεων

Άσκηση 1. Έστω p πρώτος και $m \in \mathbb{Z}_{>0}$. Δείξτε ότι η ισοτιμία

$$x^m \equiv 0 \pmod{p^m}$$

έχει ακριβώς p^{m-1} λύσεις.

Στις Ασκήσεις 2–5, θα μελετήσουμε κατά πόσο ο a είναι τετραγωνικό υπόλοιπο n, για οποιονδήποτε n, με $(a, n) = 1$. Ειδικότερα, η Άσκηση 5 μπορεί να χρησιμοποιηθεί ως θεωρία.

Άσκηση 2. Έστω $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$, όπου $r \geq 0$ και $n_i \geq 0$, η παραγοντοποίηση σε πρώτους του n. Αν $(a, n) = 1$, τότε η

$$x^2 \equiv a \pmod{n}$$

είναι επιλύσιμη αν και μόνο αν η $x^2 \equiv a \pmod{p_i^{n_i}}$ είναι επιλύσιμη για $i = 1, \ldots, k$ και η $x^2 \equiv a \pmod{2^r}$ είναι επιλύσιμη (όταν $r \geq 2$).

Άσκηση 3. Έστω p περιττός πρώτος, $r \geq 1$ και $p \nmid a$. Τότε η $x^2 \equiv a \pmod{p^r}$ είναι επιλύσιμη αν και μόνο αν η $x^2 \equiv a \pmod{p}$ είναι επιλύσιμη.

Άσκηση 4. Έστω a περιττός και $r \geq 3$. Τότε η $x^2 \equiv a \pmod{2^r}$ είναι επιλύσιμη αν και μόνο αν $a \equiv 1 \pmod{8}$.

Άσκηση 5. Έστω $n = 2^r p_1^{n_1} \cdots p_k^{n_k}$, όπου $r \geq 0$ και $n_i \geq 0$, η παραγοντοποίηση σε πρώτους του n. Αν $(a, n) = 1$, τότε η

$$x^2 \equiv a \pmod{n}$$

είναι επιλύσιμη αν και μόνο αν $\left(\frac{a}{p_i}\right) = 1$, για κάθε $i = 1, \ldots, n$ και

$$a \equiv \begin{cases} 1 \pmod{8}, & \text{αν } r \geq 3, \\ 1 \pmod{4}, & \text{αν } r = 2. \end{cases}$$

Άσκηση 6. Λύστε την ισοτιμία $4x^4 + 4x^3 + 6x^2 + 21x + 7 \equiv 0 \pmod{252}$.

Άσκηση 7. Υπολογίστε τα παρακάτω σύμβολα:

$$\left(\frac{-14}{71}\right), \left(\frac{219}{383}\right), \left(\frac{100}{31}\right), \left(\frac{3}{23}\right).$$

Άσκηση 8. Εξετάστε κατά πόσο η ισοτιμία $x^2 - 6x - 13 \equiv 0 \pmod{127}$ είναι επιλύσιμη.

Άσκηση 9. Εξετάστε κατά πόσο η ισοτιμία $x^2 \equiv 7 \pmod{19}$ είναι επιλύσιμη.

Άσκηση 10. Βρείτε όλους τους πρώτους $10 < p < 100$, τέτοιους ώστε $p \mid n^2+1$, για κάποιο n.

Άσκηση 11. Έστω p πρώτος, τέτοιος ώστε $p \equiv 3 \pmod{4}$. Αν $a^2 + b^2 \equiv 0 \pmod{p}$, δείξτε ότι $a \equiv b \equiv 0 \pmod{p}$.

Άσκηση 12. Δείξτε ότι, αν n θετικός περιττός αριθμός, τότε

$$\left(\frac{6}{n}\right) = \begin{cases} 1, & \text{αν } n \equiv \pm 1 \text{ ή } \pm 5 \pmod{24}, \\ -1, & \text{αν } n \equiv \pm 7 \text{ ή } \pm 11 \pmod{24}. \end{cases}$$