Math 104A, Fall 2018

Number Theory, HW 8

Due Wednesday November 28th by 5PM in Shubham Sinha's box.

From Weissman's book `An illustrated theory of numbers`:

- Exercises (Section 7, pages 190–191):

  11, 15

- Exercises (Section 8, pages 220–221):

  6, 7, 8 (← feel free to use the result of Problem E for exc. 8 part (a))

Problem A. The Möbius function μ is defined on integers $n > 0$ as follows. If $n = p_1 p_2 \cdots p_r$ is a product of r distinct primes let $\mu(n) = (-1)^r$. Otherwise, if n is not square-free, let $\mu(n) = 0$. Note that by convention $\mu(1) = 1$.

(a) Check that μ is a multiplicative function. That is,

$$\mu(mn) = \mu(m)\mu(n) \qquad \textbf{provided} \qquad \mathrm{GCD}(m,n) = 1.$$

(b) Prove the identity below for all positive integers n.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1. \end{cases}$$

(Here the sum $\sum_{d|n}$ ranges over all positive divisors d of n.)

`Hint`: $\sum_{i=0}^{r} \binom{r}{i}(-1)^i = (1-1)^r = 0$ for $r > 0$ by the binomial formula.

Problem B.

(a) Let $n > 1$ be an integer for which Wilson's congruence holds. That is,

$$(n-1)! \equiv -1 \pmod{n}.$$

Prove that n is necessarily a prime number.

(b) (Based on a question asked in class.) For an integer $m > 1$ we let $\Phi(m)$ denote the set of integers $a \in \{1, 2, \ldots, m-1\}$ such that $\mathrm{GCD}(a, m) = 1$. Let $\Pi := \prod_{a \in \Phi(m)} a$ denote their product. Is it true $\forall m$ that

$$\Pi \equiv -1 \pmod{m}?$$

Give a proof or a counterexample.

Problem C.

(a) Find all solutions $x \in \mathbb{Z}$ to the quadratic congruence $x^2 \equiv -1(\mathrm{mod}\ 5)$.

(b) Which of the quadratic congruences below have[1] solutions? Explain.

(1) $x^2 \equiv -1(\mathrm{mod}\ 101)$

(2) $x^2 \equiv -1(\mathrm{mod}\ 103)$

(3) $x^2 + 2x + 2 \equiv 0(\mathrm{mod}\ 89)$

(c) Compute the Legendre symbol $\left(\frac{3}{p}\right)$ for $p = 5, 7, 11$.

Problem D.

(a) Express 89 as a sum of two squares: Find $a, b \in \mathbb{Z}$ such that $89 = a^2 + b^2$.

(b) Can the prime number 1999 be written as $a^2 + b^2$?

(c) Which of the numbers below are sums of two squares? Explain.

(1) $a = 2^9 \cdot 3^8 \cdot 5^7 \cdot 7^6$

(2) $b = 2^8 \cdot 3^7 \cdot 5^6 \cdot 7^5$

(3) $c = 2^7 \cdot 3^6 \cdot 5^6 \cdot 7^5$

(4) $d = 2^5 \cdot 3^8 \cdot 5^9 \cdot 7^4 \cdot 11^2 \cdot 13^6 \cdot 17^3 \cdot 19^8 \cdot 23^2$

Problem E. Let $a, b, c \in \mathbb{Z}$ be arbitrary integers, and let p be a prime. In this exercise we will show that the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has an integer solution $(x, y, z) \neq (0, 0, 0)$.

(a) Observe that we may assume $p \nmid abc$ and $p > 2$ – without loss of generality.

[1] You are **not** required to find a solution when it exists. Just prove or disprove existence.

(b) Introduce two finite sets of integers:

$$X = \{a + by^2 : y = 0, 1, \ldots, \frac{p-1}{2}\} \qquad Y = \{-cz^2 : z = 0, 1, \ldots, \frac{p-1}{2}\}.$$

Note that all elements of X are distinct modulo p. The same for Y.

(c) Use the pigeonhole principle to conclude that there must exist non-negative integers $y, z \leq \frac{p-1}{2}$ satisfying $a + by^2 \equiv -cz^2 \pmod{p}$. [In other words the triple $(1, y, z)$ is a solution to our problem.]