Math 104A, Fall 2018

Number Theory, HW 9

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

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

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

  13(d) (← Problem B and/or Corollary 7.21 might be useful)

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

  1, 2[1]*, 9(a+b+c)*

Problem A. Which of the congruences below have solutions $x \in \mathbb{Z}$? Explain.

(a) $x^2 \equiv -1 \pmod{67}$

(b) $x^2 \equiv -1 \pmod{97}$

(c) $x^2 \equiv 2 \pmod{79}$

(d) $x^2 \equiv 2 \pmod{83}$

(e) $x^2 \equiv 3 \pmod{89}$

(f) $x^2 \equiv 3 \pmod{59}$

Problem B. Let $f(x)$ be a polynomial with integer coefficients. Suppose p is a prime and $a \in \mathbb{Z}$ satisfies the conditions

$$f(a) \equiv 0(\text{mod } p^n) \qquad f'(a) \not\equiv 0(\text{mod } p)$$

for some $n > 0$. Our goal is to modify a and get a root of f modulo p^{n+1}.

(a) Observe that there is a "Taylor expansion" for every $t \in \mathbb{Z}$:

$$f(a + p^n t) = f(a) + f'(a)(p^n t) + \frac{f''(a)}{2!}(p^n t)^2 + \cdots + \frac{f^{(N)}(a)}{N!}(p^n t)^N$$

where N is the degree of f.

[1] You may use the result of Problem B for $f(x) = x^2 - 41$.

(b) Explain why $\frac{f^{(k)}(a)}{k!} \in \mathbb{Z}$ for all k satisfying the inequalities $0 \le k \le N$.

(c) Deduce that

$$f(a + p^n t) \equiv f(a) + f'(a)(p^n t) \pmod{p^{n+1}}.$$

(d) Conclude that there is a $t \in \mathbb{Z}$ (which is uniquely determined modulo p) with the property that $a + p^n t$ is a root of f modulo p^{n+1}. That is,

$$f(a + p^n t) \equiv 0 \pmod{p^{n+1}}.$$

(This is where you need that assumption that $f'(a)$ is not divisible by p.)

Problem C. Compute the Legendre symbols below.

$$(\frac{-1}{53}) \quad (\frac{5}{101}) \quad (\frac{5}{103}) \quad (\frac{62}{41}) \quad (\frac{89}{97}).$$

Problem D. Let $p > 2$ be a prime not dividing a, and consider the first $\frac{p-1}{2}$ multiples of a:

$$1a, \ 2a, \ 3a, \ \cdots, \ \frac{p-1}{2}a.$$

For each i we let $0 \le r_i < p$ be the integer for which $r_i \equiv ia \pmod{p}$.

(a) Decompose the index set $\{1, 2, 3, \ldots, \frac{p-1}{2}\}$ as a disjoint union $I \cup J$ where

$$I = \{i : r_i > \frac{p}{2}\} \qquad J = \{i : r_i < \frac{p}{2}\}.$$

Observe that $|I| + |J| = \frac{p-1}{2}$.

(b) If $i \in I$ show that $p - r_i$ cannot be of the form r_j for an index $j \in J$.

(c) Noting that $p - r_i < \frac{p}{2}$ for $i \in I$ infer from (b) that

$$\{1, 2, 3, \ldots, \frac{p-1}{2}\} = \{p - r_i : i \in I\} \cup \{r_j : j \in J\}$$

by first showing the inclusion $\supseteq$ and then comparing cardinalities.

(d) By taking the product of the lists of numbers in (c) conclude that

$$\boxed{\left(\frac{a}{p}\right) = (-1)^{|I|}}$$

(This formula is known as the <u>Gauss</u> lemma.)

Problem E. We employ the notation introduced in Problem D. Thus

$$ia = [\frac{ia}{p}]p + r_i \qquad 0 \le r_i < p$$

for $i = 1, 2, 3, \dots, \frac{p-1}{2}$.

(a) Using part (c) of Problem D justify the following identities:

(1) $\sum_{i=1}^{\frac{p-1}{2}} r_i = \sum_{i \in I} r_i + \sum_{j \in J} r_j$

(2) $\sum_{i=1}^{\frac{p-1}{2}} i = p|I| - \sum_{i \in I} r_i + \sum_{j \in J} r_j$

(3) $\sum_{i=1}^{\frac{p-1}{2}} ia = p \cdot \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] + \sum_{i=1}^{\frac{p-1}{2}} r_i$

(b) Essentially by subtracting (2) from (3) deduce that

$$(a-1) \cdot \frac{p^2-1}{8} = p \cdot (\sigma - |I|) + 2 \sum_{i \in I} r_i$$

where we have used the notation $\sigma := \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right]$.

(c) Conclude that for <u>odd</u> a we have $\left(\frac{a}{p}\right) = (-1)^{\sigma}$.

(d) Furthermore, check that $\sigma = 0$ when $a = 2$ and deduce the formula

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}}$$

Problem F. Fill out your CAPE teaching evaluations **please**!