Math 104A, Fall 2018

Number Theory, HW 5

Due Wednesday November 7th by 5PM in Shubham Sinha's box.

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

- Exercises (Section 5, pages 150–151):
  1, 2, 3, 4, 5, 6, 7, 9[1]

Problem A.

(a) Show that squares are congruent to either 0 or 1 modulo 4.

(b) Deduce from (a) that $a^2 + b^2 \equiv 3 \pmod 4$ has no solutions $a, b \in \mathbb{Z}$.

(c) By a case-by-case analysis similar to (a) and (b) show that the congruence

$$a^2 + b^2 + c^2 \equiv 7 \pmod 8$$

has no solutions $a, b, c \in \mathbb{Z}$.

(d) In continuation of (c) also verify that

$$a^2 + b^2 + c^2 \equiv 0 \pmod 8 \implies a, b, c \text{ are even}.$$

(e) Use (c) and (d) to prove that an integer of the form $4^m(8n+7)$ cannot be written as a sum of three squares[2]. (`Hint`: Use induction on m.)

Problem B. Fix an odd integer $m > 0$ and any two $a, b \in \mathbb{Z}$.

(a) In analogy to Problem A on HW1, show that the quadratic congruence

$$x^2 + ax + b \equiv 0 \pmod m \tag{1}$$

has integer solutions if and only if $x^2 \equiv a^2 - 4b \pmod m$ does.

– Continued on the next page.

[1] Primes > 3 are $\equiv \pm 1 \pmod 6$; show that $6(p_1 \cdots p_n) - 1$ must have a prime factor $\equiv -1$.
[2] Legendre's three-square theorem says that all other numbers *can* be written as $a^2+b^2+c^2$.

(b) Assuming m is prime, explain why (1) can have at most <u>two</u> solutions modulo m. (`Hint`: Reduce to the case $a = 0$ and try to show that

$$y^2 \equiv x^2 \pmod{m} \implies y \equiv \pm x \pmod{m}$$

by applying Euclid's lemma to the factorization $y^2 - x^2 = (y-x)(y+x)$.)

(c) List all solutions modulo 8 to the congruence $x^2 \equiv 1 \pmod{8}$.