MATH 311, FALL 2020 MIDTERM 1 SOLUTIONS

SEPTEMBER 23

Each problem is worth 10 points.

Problem 1.

a. State the law of quadratic reciprocity.

b. Calculate the Legendre symbols $\left(\frac{143}{7}\right)$, $\left(\frac{19}{101}\right)$, $\left(\frac{21}{103}\right)$.

Solution.

a. Let p and q be distinct odd primes. The Legendre symbols satisfy

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

b. By periodicity

$$\left(\frac{143}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Since $101 \equiv 1 \bmod 4$,

$$\left(\frac{19}{101}\right) = \left(\frac{101}{19}\right) = \left(\frac{6}{19}\right) = \left(\frac{25}{19}\right) = 1.$$

We have

$$\left(\frac{21}{103}\right) = \left(\frac{3}{103}\right)\left(\frac{7}{103}\right) = \left(\frac{103}{3}\right)\left(\frac{103}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = -1.$$

Problem 2. Find all solutions of the congruence $x^2 \equiv 5 \bmod 836$.

Solution. Factor $836 = 4 \times 11 \times 19$. By the Chinese remainder theorem, it suffices to solve the equation $x^2 \equiv 5$ modulo $4, 11, 19$. The two solutions modulo 4 are 1 and 3. There are two solutions modulo 11 and 19 since each is prime. The two solutions modulo 11 are 4 and 7, and the two solutions modulo 19 are 9 and 10. Thus the 8 solutions are given by

$$\{1,3\}209 \cdot \overline{209} + \{4,7\}76 \cdot \overline{76} + \{9,10\}44 \cdot \overline{44}$$

where $\overline{209}$ is the multiplicative inverse of 209 modulo 4, $\overline{76}$ is the multiplicative inverse of 76 modulo 11, and $\overline{44}$ is the multiplicative inverse of 44 modulo 19. Thus

$$\overline{209} \equiv 1 \bmod 4, \qquad \overline{76} \equiv -1 \bmod 11, \qquad \overline{44} \equiv -3 \bmod 19.$$

This produces the solutions

$$29, 161, 257, 389, 447, 579, 675, 807 \bmod 836.$$

Problem 3.

a. State Fermat's theorem classifying the numbers which are the sum of two squares.
b. Write $2465 = 5 \times 17 \times 29$ as the sum of two squares.

Solution.

a. A number $n > 0$ is the sum of two squares if and only if each prime $q \equiv 3 \bmod 4$ which divides n appears with even multiplicity.
b. Recall $a^2 + b^2 = (a + bi)(a - bi)$. We have $5 = 1^2 + 2^2$, $17 = 1^2 + 4^2$, $29 = (2^2 + 5^2)$. Thus if

$$(A + Bi) = (1 + 2i)(1 + 4i)(2 + 5i)$$

then $A^2 + B^2 = 2465$. This produces $44^2 + 23^2 = 2465$.

Problem 4. Find a primitive root modulo $1331 = 11^3$.

Solution. We'll show that 2 is a primitive root modulo 1331. Since the order of 2 modulo 11 divides 10, and $2^2 \equiv 4 \bmod 11, 2^5 \equiv -1 \bmod 11$, the order of 2 modulo 11 is 10. The order of 2 mod 121 divides $10 \cdot 11 = 110$ and is divisible by 10. Since $2^{10} = 1024 \equiv 56 \bmod 121$, the order of 2 modulo 121 is 110, and 2 is a primitive root modulo 121. Since 2 is a primitive root modulo 11^2, it is a primitive root modulo 11^α for all $\alpha > 2$.