

SOLUTIONS TO MIDTERM 2
Math 104 - Dr. Evans
UCSD Winter 2004

1. (A) Prove the following statement: There exist rational numbers x, y such that $5 = x^2 + 101y^2$.

(B) Is the statement still true if the number 5 on the left is replaced by the number 2? Justify.

Proof. (A) Suppose there is a solution in the rational numbers. Write $x = \frac{k}{l}$ and $y = \frac{m}{n}$. Then

$$5 = x^2 + 101y^2 = \left(\frac{k}{l}\right)^2 + 101\left(\frac{m}{n}\right)^2$$

Multiplying both sides by l^2n^2 results in the integer equation $5(ln)^2 = (kn)^2 + 101(ml)^2$. Hence, there is also a solution to $a^2 + 101b^2 = 5c^2$ in the integers. We may assume that a, b , and c are pairwise relatively prime.

By Legendre's Theorem, it suffices to check that the coefficient of a^2, b^2 , and c^2 satisfy the following conditions:

- i. 1, 101, and 5 are positive, squarefree, and pairwise relatively prime
- ii. $1 \cdot 5$ is a square modulo 101
- iii. $5 \cdot 101$ is a square modulo 1
- iv. $-1 \cdot 101$ is a square modulo 5

The first condition is obviously true, since 101 and 5 are prime. The third condition is trivial, since every number is a square modulo 1. To check the other two, we use the Legendre symbol:

$$\begin{aligned} \left(\frac{5}{101}\right) &= \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1 & 101 &\equiv 1 \pmod{5} \\ \left(\frac{-101}{5}\right) &= \left(\frac{4}{5}\right) = 1 & -101 &\equiv 4 \pmod{5} \end{aligned}$$

Since all four conditions are satisfied, by Legendre's theorem there exists a solution in the integers to $a^2 + 101b^2 = 5c^2$. Dividing through by c^2 gives a solution to $x^2 + 101y^2 = 5$ in the rational numbers, namely $x = \frac{a}{c}$ and $y = \frac{b}{c}$.

Alternatively, one could search for a solution over the integers to $a^2 + 101b^2 = 5c^2$. Two such solutions are $a = 12, b = 1, c = 7$, and $a = 1, b = 2, c = 9$. These result in the rational solutions $x = \frac{12}{7}, y = \frac{1}{7}$ and $x = \frac{1}{9}, y = \frac{2}{9}$.

(B) Assume there is a solution to $x^2 + 101y^2 = 2$. Once again, clear the denominators to get the integer equation $a^2 + 101b^2 = 2c^2$. Considering the equation modulo 101, we have $a^2 \equiv 2c^2 \pmod{101}$. Since we are assuming a and c are relatively prime, neither can be divisible by 101 (otherwise the other one would be as well). In particular, c has an inverse modulo 101. So $(ac^{-1})^2 \equiv 2 \pmod{101}$, which says that 2 must be a square modulo 101. By special case of Quadratic Reciprocity, 2 is a square modulo p if and only if $p \equiv \pm 1 \pmod{8}$. But $101 \equiv 5 \pmod{8}$, so 2 is a nonsquare modulo 101. This is a contradiction, so no solution in the rationals exists.

2. Find a prime $p > 50$ for which the congruence $x^2 + x + 1 \equiv 0 \pmod{p}$ has no solutions $x \pmod{p}$. Justify in detail.

By the quadratic formula, the solutions to $ax^2 + bx + c \equiv 0 \pmod{p}$ are $x \equiv \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \pmod{p}$, as long as everything makes sense. In this case, the solutions to $x^2 + x + 1 \equiv 0 \pmod{p}$ are

$$x \equiv \frac{-1 \pm \sqrt{1^2 - 4 \cdot 1 \cdot 1}}{2} \equiv 2^{-1}(-1 \pm \sqrt{-3}) \pmod{p}$$

Since p is odd, 2 has an inverse modulo p . So the question of whether $x^2 + x + 1 \equiv 0 \pmod{p}$ has a solution depends on whether -3 is a square modulo p , i.e., if $\left(\frac{-3}{p}\right)$ is 1 or -1 . By quadratic reciprocity,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{3} \\ -1, & \text{if } p \equiv 2 \pmod{3} \end{cases}$$

Therefore, the congruence $x^2 + x + 1 \equiv 0 \pmod{p}$ has no solutions modulo p if and only if $p \equiv 2 \pmod{3}$. There are several primes $p > 50$ which are congruent to 2 modulo 3; the first few are $p = 53$, $p = 59$, and $p = 71$.

3. Suppose that $m \equiv a^2 \pmod{3}$ and $m \equiv b^2 \pmod{5}$ for some integers a, b . Prove that $m \equiv c^2 \pmod{15}$ for some integer c .

The biggest mistake is to assume that m is a *nonzero* square modulo 3 or 5. There is no such condition on a or b . The first condition states that $m \equiv 0, 1 \pmod{3}$, while the second condition implies that $m \equiv 0, 1, 4 \pmod{5}$. By the Chinese Remainder Theorem,

$$\begin{array}{lll} m \equiv 0 \pmod{3}, m \equiv 0 \pmod{5} & \implies & m \equiv 0 \pmod{15} \\ m \equiv 0 \pmod{3}, m \equiv 1 \pmod{5} & \implies & m \equiv 6 \pmod{15} \\ m \equiv 0 \pmod{3}, m \equiv 4 \pmod{5} & \implies & m \equiv 9 \pmod{15} \\ m \equiv 1 \pmod{3}, m \equiv 0 \pmod{5} & \implies & m \equiv 10 \pmod{15} \\ m \equiv 1 \pmod{3}, m \equiv 1 \pmod{5} & \implies & m \equiv 1 \pmod{15} \\ m \equiv 1 \pmod{3}, m \equiv 4 \pmod{5} & \implies & m \equiv 4 \pmod{15} \end{array}$$

Now the squares modulo 15 are

$$\begin{array}{ll} 0^2 \equiv 0 \pmod{15} & 4^2 \equiv 1 \pmod{15} \\ 1^2 \equiv 1 \pmod{15} & 5^2 \equiv 10 \pmod{15} \\ 2^2 \equiv 4 \pmod{15} & 6^2 \equiv 6 \pmod{15} \\ 3^2 \equiv 9 \pmod{15} & 7^2 \equiv 4 \pmod{15} \end{array}$$

In all six cases of m , m is a square modulo 15. Therefore, there exists an integer c such that $m \equiv c^2 \pmod{15}$.

4. Let $h = \frac{p-1}{2}$, where p is an odd prime. Prove that $h!^2 \equiv -\left(\frac{-1}{p}\right) \pmod{p}$, where $\left(\frac{-1}{p}\right)$ is the Legendre symbol.

Note that for any integer j , $j \equiv -(p-j) \pmod{p}$. So

$$\begin{aligned} h! &= (1)(2) \cdots \left(\frac{p-1}{2}\right) \\ &\equiv (-(p-1))(-(p-2)) \cdots \left(-\left(p - \left(\frac{p-1}{2}\right)\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}} (p-1)(p-2) \cdots \left(\frac{p+1}{2}\right) \pmod{p} \end{aligned}$$

Multiplying this congruence by $h!$,

$$\begin{aligned} h!^2 &\equiv (-1)^{\frac{p-1}{2}} (p-1)(p-2) \cdots \left(\frac{p+1}{2}\right) \left(\frac{p-1}{2}\right) \cdots (2)(1) \\ &\equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod{p} \end{aligned}$$

By Euler's Criterion, $(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p}$. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Hence,

$$h!^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv -\left(\frac{-1}{p}\right) \pmod{p}.$$

5. Given distinct odd primes p and q , let M be the set of all positive integers k less than or equal to $\frac{pq-1}{2}$ for which $\gcd(k, pq) = 1$. How many elements are in the set M ? Justify.

Since p and q are primes, $\gcd(k, pq) = 1 \iff p \nmid k$ and $q \nmid k$. Let

$$M = \left\{ k \in \mathbb{Z} \mid 1 \leq k \leq \frac{pq-1}{2}, p \nmid k \text{ and } q \nmid k \right\}$$

One way to count the number of elements in M is to take all the integers between 1 and $\frac{pq-1}{2}$, subtract the number of integers divisible by p and by q , then add back in the integers divisible by pq (since those numbers were counted twice). This is called the "inclusion-exclusion principle."

The biggest multiple of p less than $\frac{pq-1}{2}$ is $\frac{q-1}{2}p$, since $\frac{q-1}{2}p = \frac{pq-p}{2} < \frac{pq-1}{2}$ and $\frac{q+1}{2}p = \frac{pq+p}{2} > \frac{pq-1}{2}$. Hence, there are $\frac{q-1}{2}$ integers less than $\frac{pq-1}{2}$ and divisible by p . Similarly, there are $\frac{p-1}{2}$ integers less than $\frac{pq-1}{2}$ and divisible by q . Since $\frac{pq-1}{2} < pq$, there are no integers divisible by pq in M . Therefore,

$$\#M = \frac{pq-1}{2} - \frac{q-1}{2} - \frac{p-1}{2} = \frac{(p-1)(q-1)}{2}$$

6. We define the set M as in problem 5. Show in detail that when $q = 5$, the product of all the elements of M is congruent to the Legendre symbol $\left(\frac{5}{p}\right) \pmod{p}$.

In this case, $q = 5$ implies k runs from 1 to $\frac{5p-1}{2}$. Hence,

$$M = \left\{1, 2, \dots, p-1, p+1, \dots, 2p-1, 2p+1, \dots, 2p + \frac{p-1}{2}\right\}$$

where every number divisible by 5 is skipped. Taking the product over all these numbers, we have

$$\begin{aligned} \prod M &= \frac{(1)(2) \cdots (p-1)(p+1) \cdots (2p-1)(2p+1) \cdots \left(2p + \frac{p-1}{2}\right)}{(5)(10) \cdots \left(\frac{p-1}{2}5\right)} \\ &\equiv \frac{((p-1)!)^2 \cdot \left(\frac{p-1}{2}\right)!}{5^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!} \equiv \frac{((p-1)!)^2}{5^{\frac{p-1}{2}}} \pmod{p} \end{aligned}$$

The fractions are valid since p does not divide 5 or any integer between 1 and $\frac{p-1}{2}$.

By Euler's Criterion, $5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) \pmod{p}$. Also, $\left(\frac{5}{p}\right)^{-1} = \left(\frac{5}{p}\right)$ since the Legendre symbol is either 1 or -1. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Therefore,

$$\prod M \equiv \frac{((p-1)!)^2}{5^{\frac{p-1}{2}}} \equiv (-1)^2 \left(\frac{5}{p}\right) \equiv \left(\frac{5}{p}\right) \pmod{p}.$$