

SOLUTIONS TO SELECTED PROBLEMS FROM FINAL EXAM
Math 104B - Dr. Evans
UCSD Spring 2004

Problems 7-9 on the final exam involved proving the following:

Theorem *Let p be a prime greater than 5. Then $p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$.*

Problem 7 proves one direction, namely that if $p = x^2 + 5y^2$, then $p \equiv 1, 9 \pmod{20}$. Problem 8 proves a lemma which allows us to prove the other direction in problem 9.

Solution to Problem 7 *For any prime $p > 5$, prove that if p has the form $p = x^2 + 5y^2$, then p is congruent to either 1 or 9 mod 20.*

Suppose there exist integers x and y such that $p = x^2 + 5y^2$. Reducing modulo 5, $p \equiv x^2 \pmod{5}$, so p is a square modulo 5. The squares modulo 5 are 0, 1, and 4. However, p is a prime greater than 5, so $p \not\equiv 0 \pmod{5}$. Hence, $p \equiv 1$ or $4 \pmod{5}$.

If x and y are both even or both odd, then p would be even, contradicting p being an odd prime greater than 5. So one of x and y is even, the other odd. Considering the equation $p = x^2 + 5y^2$ modulo 4, we have $p \equiv x^2 + y^2 \equiv 1 \pmod{4}$. By the Chinese Remainder Theorem, $p \equiv 1$ or $9 \pmod{20}$.

Solution to Problem 8 *Suppose that $-5 \equiv b^2 \pmod{p}$ for some prime $p > 5$. Prove that there are nonzero integers x and y , each with absolute value less than \sqrt{p} , such that p divides $x - b \cdot y$.*

Consider the set

$$S = \{x - b \cdot y \mid 0 \leq x \leq \sqrt{p}, 0 \leq y \leq \sqrt{p}\}$$

There are more than \sqrt{p} choices for x and more than \sqrt{p} choices for y , so there are more than p choices for $x - b \cdot y$. By the box principle (also called the pigeonhole principle), two different choices of x and y must be equivalent modulo p , i.e., $x_1 - b \cdot y_1 \equiv x_2 - b \cdot y_2 \pmod{p}$. Moving everything to one side, $(x_1 - x_2) - b(y_1 - y_2) \equiv 0 \pmod{p}$.

Let $x = x_1 - x_2$ and $y = y_1 - y_2$. Since $x - b \cdot y \equiv 0 \pmod{p}$, p divides $x - b \cdot y$. By the constraints of x_1 and x_2 , $-\sqrt{p} < x < \sqrt{p}$. Similarly, $-\sqrt{p} < y < \sqrt{p}$. Neither x nor y can be zero, otherwise the other is also zero and the two choices were the same to start with. Hence, $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$.

Solution to Problem 9 *Prove the converse of the statement in problem #7.*

Suppose p is congruent to either 1 or 9 modulo 20. By quadratic reciprocity,

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = +1 \cdot \left(\frac{p}{5}\right) = 1$$

Hence, -5 is a square modulo p . Let b be an integer such that $-5 \equiv b^2 \pmod{p}$. By problem 8, there exist integers x and y with absolute value less than \sqrt{p} such that $x - b \cdot y \equiv 0 \pmod{p}$. Multiplying by $x + b \cdot y$ gives $x^2 - b^2 y^2 \equiv x^2 + 5y^2 \equiv 0 \pmod{p}$, or equivalently, $kp = x^2 + 5y^2$ for some integer k . Since $0 < x^2 < p$ and $0 < y^2 < p$, we have $0 < x^2 + 5y^2 < p + 5p = 6p$. Thus, $x^2 + 5y^2$ equals p , $2p$, $3p$, $4p$, or $5p$.

To finish the proof, we must show that each case reduces to $p = x^2 + 5y^2$ or leads to a contradiction.

$p = x^2 + 5y^2$. This is what we want, so there is nothing to prove.

$2p = x^2 + 5y^2$. Reducing modulo 5, we have $2p \equiv x^2 \pmod{5}$. Note that x cannot be divisible by 5 (otherwise p is divisible by 5). The nonzero squares modulo 5 are 1 and 4, so $2p \equiv 1, 4 \pmod{5}$. Multiplying by the inverse of 2, $p \equiv 3, 2 \pmod{5}$. This contradicts the assumption that $p \equiv 1, 9 \pmod{20}$.

$3p = x^2 + 5y^2$. The same contradiction is reached by a similar argument as above.

$4p = x^2 + 5y^2$. If either x or y is odd, then $x^2 + 5y^2 \equiv 1$ or $2 \pmod{4}$. So x and y must both be even. Letting $x = 2k$ and $y = 2l$, $4p = (2k)^2 + 5(2l)^2 = 4(k^2 + 5l^2)$. Hence, $p = k^2 + 5l^2$.

$5p = x^2 + 5y^2$. Since $x^2 = 5(p - y^2)$, we have $5 \mid x^2$ which implies $5 \mid x$. Let $x = 5k$. Then $5p = (5k)^2 + 5y^2 = 5(y^2 + 5k^2)$. Hence, $p = y^2 + 5k^2$.

In every case, we either reach a contradiction or find two integers for which $p = x^2 + 5y^2$. This concludes the proof.