Trey Manuszak
Christian Garcia

1 Introduction and Review

We have previously learned how to solve linear congruences such as $5x \equiv 7 \pmod{13}$, which is the same as $5x = 7 + 13y$. We are now moving on to Quadratic Congruences such as $5x^2 \equiv 7 \pmod{13}$, which is the same as $5x^2 = 7 + 13y$. The problem now is that the Euclidean algorithm will no longer help us with quadratic equations. To understand problems of the form $x^2 \equiv a \pmod{p}$, we must explore the squares $\pmod{p}$ (aka quadratic residues $\pmod{p}$).

Example 1 (Quadratic Residues (mod p)) What are the residues of $x^2 \equiv a \pmod{7}$? We find that $x^2 \equiv a \pmod{7}$ only has solutions when $a = 0, 1, 2, 4$. These were found by taking the square of all the numbers up to 7 with repsect to modulo 7, i.e,

x	0	1	2	3	4	5	6
$x^2 \pmod{7}$	0	1	4	2	2	4	1

2 Concept of Partnering

Say we wanted to find the sum of all the numbers up to 99, how would we go about this? Recall Gauß' idea of summing consecutive numbers. We would do this by partnering 1 and 99 to get 100, 2 and 98 to also get 100 and we would continue this process until we reached the middle which would give us 49 pairs that sum to 100. Also, there would be the lonely numbers 50 and 100. Add up all the partners along with the lonely numbers, we find that the sum is 5050. It's an efficient way to sum all the numbers, but it also has a multiplicative version which is the following theorem.

Theorem 8.2 (Wilson's Theorem) *If p is a prime number, then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. Partner numbers $\phi(p) = \{1, 2, 3, \ldots, p-1\}$ by pairing x with y when $xy \equiv 1 \pmod{p}$. Note that all partners are unique. The lonely numbers in this case would be the numbers for which $x^2 = x \times x \equiv 1 \pmod{p}$. By proposition 6.21, these lonely numbers are 1 and $p-1$. To multiply the numbers in $\Phi(p)$ we multiply partners, which results in 1 as the product. The lonely numbers are the only thing that contribute to the product. Thus,

$$1 \times 2 \times 3 \times ... \times (p-1) = 1 \times (p-1) \equiv -1 \pmod{p}.$$

□

"Wilson's theorem is my favorite concept from the lecture since it used the partnering concept we learned about early in the semester and applies to something more complex." -Christian Garcia

Wilson's theorem lets us analyze squares.

Proposition 8.3 *Let p be an odd prime number. Then among the set $\Phi(p)$ half the numbers are squares and half are not.*

Proof. Consider the squaring $\pmod p$ function on the set $\Phi(p)$. We find that the squaring $\pmod p$ function gives a two to one correspondence Indeed, if x and $p - x$ are input into this function, then the outputs are $x^2 \pmod p$ and $(p-x)^2 \pmod p$ But,

$$(p-x)^2 \equiv (-x)^2 = x^2.$$

So, both inputs give the same result. No more than two inputs yield the same output Because if $x^2 \equiv y^2 \pmod p$, then $(x+y)(x-y) \equiv 0 \pmod p$, so $x \equiv \pm y \pmod p$, which implies $y = p - x$ within the set $\Phi(p)$. Since there are two inputs for every output, there is half as many squares as inputs. Therefore, half of the elements of $\Phi(p)$ are squares. □

However, this proposition does not identify which half are squares. The following definition resolves the question.

Definition 8.4 Let p be a prime number. Let a, x, and y be elements of $\Phi(p)$. We declare x and y to be **a-partners** if $xy \equiv a \pmod p$.

Note, that every number in $\Phi(p)$ has an a-partner. So, if $x \in \Phi(p)$, then there exists a multiplicative inverse $y \in \Phi(p)$ such that ya is the a-partner of $x \pmod p$. So, $x(ya) = (xy)a = 1 \times a \equiv a \pmod p$. When a-partnering, the lonely numbers are the x for which $x^2 \equiv a \pmod p$.

3 Euler's Criterion for Squares (mod p)

The theorem uses the fact that the residue classes, which are a partition, modulo prime p create a field. A field is a ring, which is an algebraic structure that allows for two binary operations, that also allows for "division", or in better terms, a multiplicative inverse for every nonzero element of the field. Also, since the modulus is prime, then Lagrange's theorem applies.

Theorem 8.35 (Lagrange's theorem) *Any polynomial of degree k has at most k roots.*

As it applies to quadratic residue, Lagrange's theorem says that $x^2 \equiv a \pmod p$ has at most two solutions for a.

Theorem 8.5 (Euler's Criterion for Squares (mod p)) *Let p be an odd prime number, and let a be an integer coprime to p. Then,*

- *a is square $\pmod p$, if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.*
- *a is nonsquare $\pmod p$, if and only if $a^{(p-1)/2} \equiv -1 \pmod p$.*

Euler's criterion can also be expressed as a Legendre symbol which is defined as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

Example 2 Find residues given (mod 17).
Using the formula, we get the table

x	0	1	2	3	4	5	6	7	8
$x^{(17-1)/2} \pmod{17}$	0	1	1	-1	1	-1	-1	-1	1

Note, we dont need to try the values 9 through 16 since they are equivalent to the negative of 1 through 8, i.e, $16 \equiv -1 \pmod{17}$. So, we get that the quadratic residues modulo 17 are $\{1, 2, 4, 8, 9, 13, 15, 16\}$.

4 Applications of Reciprocity -1

We will first introduce Minkowski's theorem as the proof to Fermat's Christmas theorem, in the way that we currently know how to solve, involves the use of Minkowski's result.

"Minkowski's theorem in the plane is my favorite result from the lecture as it is not immediately intuitive that it would be true. Also, I felt that nearly every property of circles have been known for millenia, yet there is still more being discovered." -Trey Manuszak

Proposition 8.8 (Minkowski's theorem in the plane) *Consider a grid of parallelograms in the plane, with the origin at a grid point, and a circle centered at the origin. If the area of the circle is greater than 4 times the area of the parallelogram, then the circle contains a grid-point besides the origin.*

Theorem 8.7 (Fermat's Christmas Theorem) *Let p be a prime number with $p \equiv 1 \pmod{4}$. Then the Diophantine equation $x^2 + y^2 = p$ has a solution. In other words, p can be expressed as the sum of two squares.*

Proof. Let p be a prime number with p of the form $p \equiv 1 \pmod{4}$. Let $u \in \mathbb{Z}$ that satisfies $u^2 \equiv 1 \pmod{p}$. Consider the set $A = \{(x, y) : x \equiv uy \pmod{p}\}$. Note, this is the set of corners of a grid of parallelograms. Also, $(0, 0), (u, 1), (p, 0), (p + u, 1) \in A$. Note, each parallelogram has area p. Let B be a circle center at the origin with area $4p$. Then by Minkowski's theorem, we know that the circle contains some point (x, y) and $(x, y) \neq (0, 0)$. By construction, (x, y) satisfies

$$x^2 + y^2 \leq \frac{4}{\pi}p \quad \text{and} \quad x \equiv uy \pmod{p}.$$

Since $u^2 \equiv -1 \pmod{p}$, then $x^2 \equiv -y^2 \pmod{p}$, which implies $x^2 + y^2 \leq \frac{4}{\pi}p$ and $x^2 + y^2$ is a multiple of p. Note, $x^2 + y^2 > 0$ since $(x, y) \neq (0, 0)$. So, since $1 < \frac{4}{\pi} < 2$, then $0 < x^2 + y^2 < 2p$ and $x^2 + y^2$ is a multiple of p. Since the only multiple of p strictly between 0 and $2p$ is p, then we have

$$x^2 + y^2 = p.$$

$\square$

As a historical note on Fermat's Christmas theorem, it's name was coined as the idea of the theorem was first expressed in a letter to Merin Mersenne dated December 25, 1640.