SPRING 2025: MATH 540 DAILY UPDATE

Thursday, May 8. the class worked in groups on the practice problems for the final exam.

Tuesday, May 6. The class worked in groups on Quiz 12 and practice problems for the final exam.

Thursday, May 1. We continued with preliminary discussions intended to lead up to the proof of the theorem that for fixed $n \geq 1$, there are infinitely many primes in the arithmetic progression $\{nt+1\}_{t\geq 1}$. After recalling some basic facts about complex nth roots of unity, including the definition of the nth cyclotomic polynomial $\Phi_n(x)$, we calculated a few instances:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1.
\end{aligned}$$

We then recorded the facts

(i) $\Phi_p(x) = x^{p-1} + x^{p-1} + \cdots + x + 1$, if p is prime.
(ii) $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$, if p is prime and $n \geq 1$.
(iii) $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.
(iv) $\Phi_{105}(x)$ is the first cyclotomic polynomial with a coefficient different from -1, 0, or 1.

We then proceeded to establish

Three Facts.

(i) For $g(x) \in \mathbb{Z}[x]$, there are infinitely many primes appearing as factors of elements in the set $\{g(0), g(1), g(2), \ldots\}$.
(ii) For $n > 0$, $p \nmid n$ a prime, and $c \in \mathbb{Z}$, $p \mid \Phi_n(c)$ if and only if the order of c mod p is n.
(iii) For p prime and $p \nmid n$, $\mathbb{Z}_p$ has an element of order n if and only if $p \equiv 1 \bmod n$.

The proof of the first fact used a result established earlier in the semester (see the lecture of March 6): If p is prime, then $\mathbb{Z}_p$ has a primitive root of 1.

With the facts in hand, the proof of the theorem followed: By Fact (i), there are infinitely many primes p dividing the values $\Phi_n(c)$, for $c \in \{0, 1, 2, \ldots, \}$. Thus, by Fact (ii), there are infinitely many primes p not dividing n and elements $c \in \mathbb{Z}$ such that c has order n mod p. By Fact (iii), there are infinitely many primes p such that $p \equiv 1 \bmod n$. That is, there are infinitely many primes of the form $p = nt + 1$.

Tuesday, April 29. The first fifteen minutes of class were devoted to Quiz 11. Then after a brief discussion concerning the statement of Dirichlet's theorem concerning primes in an arithmetic progression, and a few examples using it, we began a discussion of material which will serve as background for our proof of the following theorem, which is a special case of Dirichlet's theorem.

Theorem. Fix $n \geq 1$. Then there exist infinitely many positive integers $t \geq 1$ such that $tn + 1$ is prime. Equivalently, are are infinitely many primes p such that $p \equiv 1 \bmod n$.

To set the stage for the proof of the theorem above, we first discussed polynomials with coefficients in $\mathbb{Z}_p$, p prime. We first noted that the division algorithm holds in $\mathbb{Z}_p[x]$, since non-zero elements of $\mathbb{Z}_p$ have multiplicative inverses. We then saw that $c \in \mathbb{Z}$ is a root of $f(x) \in \mathbb{Z}_p[x] \bmod p$ if and only if $f(x) \equiv (x-c)q(x)$ in $\mathbb{Z}_p[x]$, for some $q(x) \in \mathbb{Z}_p[x]$. Then, using the (algebraic) derivative of polynomials, we saw that if $p \nmid n$, then $x^n - 1$ does not have a repeated root mod p.

Fixing $n \geq 1$, we then discussed complex roots of unity, i.e., complex numbers $z \in \mathbb{C}$ satisfying $z^n = 1$. We saw that by taking $\epsilon := e^{\frac{2\pi i}{n}}$, $1, \epsilon, \epsilon^2, \ldots, \epsilon^{n-1}$ are the distinct nth roots of unity. We defined the order $o(z)$ of an nth root of unity to be the least d such that $z^d = 1$, and defined z to be a *primitive* nth root of unity if $o(z) = n$. Noting that if $o(z) = d$, for z an nth root of unity, $d \mid n$, we proved

Proposition. For ϵ as above, ϵ^r is a primitive nth root of unity if and only if $\gcd(r, n) = 1$. In particular, there are $\phi(n)$ primitive nth roots of unity, where ϕ is Euler's totient function.

The proposition then allowed us to observe that for $d \mid n$, if T_d denotes the set of primitive dth roots of unity, then $\{1, \epsilon \ldots, \epsilon^{n-1}\} = \bigcup_{d|n} T_d$. We ended class with the following definition and observation:

Definition-Observation. For $n \geq 1$ and $d \mid n$, let $u_1, \ldots, u_{\phi(d)}$ denote the primitive dth roots of unity. Set $\Phi_d(x) := (x - u_1) \cdots (x - u_{\phi(d)})$. Then $\Phi_d(x)$ is the dth *cyclotomic* polynomial. Moreover, $x^n - 1 = \Pi_{d|n} \Phi_d(x)$.

Thursday, April 24. We spent a good portion of class time giving a proof of Lagrange's four square theorem as stated in the previous lecture. The proof used Euler's square identity and the lemma proven at the end of the previous lecture. The idea of the proof (an infinite decent-style argument) was to note that it suffices to prove the theorem for an odd prime p. By the lemma, we can choose m least such that mp is a sum of four squares, with $m < p$. One then finds $0 < r < m$ such that rm is a sum of four squares, yielding a contradiction.

We then briefly mentioned the Jacobi formula for the the function $J(n)$ giving the number of ways to write an integer as a sum of four squares(allowing permutations and negatives)

$$J(n) = \begin{cases} 8 \sum_{m|n} m, & \text{if } n \text{ is odd} \\ 24 \sum_{m|n, m \text{ odd}} m, & \text{if } n \text{ is even} \end{cases}.$$

We also briefly mentioned the Waring problem, which asks for a given $k \geq 1$, what is the least positive integer s such that every positive integer is the sum of s kth powers, and also the asymptotic version of this studied by Hardy-Littlewood.

The rest of the class we devoted to a discussion of *Pythagorean triples*, ie., triples of positive integers x, y, z satisfying $x^2 + y^2 = z^2$. A Pythagorean triple is *primitive* if $\gcd(x, y, z) = 1$. After a few easy preliminary lemma, we stated and proved half of the following theorem.

Pythagorean triples theorem. Positive integers x, y, z form a primitive Pythagorean triple, with y even, if and only if, there exist relatively prime $m, n \in \mathbb{Z}$ with $m > n$ and $m \not\equiv n \bmod 2$ such that

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2. \end{aligned}$$

Tuesday, April 22. We began a discussion of the following sums of squares theorems.

Fermat's sums of two squares theorem. Let p be an odd prime. Then $p = a^2 + b^2$, for some $a, b \in \mathbb{N}$ if and only if $p \equiv 1 \bmod 4$.

Lagrange's sum of four squares theorem. Every positive integer is a sum of four squares.

We first noted that in Lagrange's theorem, 0 is allowed to be one of the squares, e.g., $2 = 1^2 + 1^2 + 0^2 + 0^2$. We then began a proof of Fermat's theorem above. We noted that if $p = a^2 + b^2$, then since p is odd, one of a, b is odd and the other is even. If a is even, then $a = 4n$ or $4n + 2$, for some n, while if b is odd, $b = 4n+1$ or $4n+3$, and it was straight forward to check that $p \equiv 1 \bmod p$ in each of the four resulting cases. The converse was more complicated and used the facts that if $p \equiv 1 \bmod p$, then -1 is a quadratic residue mod p.

We then made the following observation (with proof):

Observation. A products of sums of two squares is a sum of two squares.

The proof of the observation was straight forward when taking a product of tow sums of two squares, and the general case followed by induction. This then easily led to the more general statement.

General sum of two squares theorem. Take $n \in \mathbb{N}$ and write $n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$, for primes p_i, q_j, where each $p_i \equiv 1 \bmod 4$ and $q_j \equiv 3 \bmod 4$, and each $e_i, f_j \geq 0$. Then n is a sum of two squares if and only if each f_j is even.

The proof of the theorem made use of the previously established fact that if q is prime, $q \equiv 3 \bmod 4$, then if q divides $a^2 + b^2$, then $q \mid a$ and $q \mid b$.

We then began the proof of Lagrange's four square theorem by first recording

Euler's square identity. Given $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{N}$, $(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) =$

$(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 + ((a_1b_3 - a_2b_4 + a_3b_1 - a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a - 4b_1)^2$

and then establishing the the following

Lemma. Suppose p is an odd prime. Then there exist $u, v \in \mathbb{Z}$ such that $p \mid (v_2 + v^2 + 1)$.

We ended class by noting that for $, u, v$ as in the lemma, $u^2 + v^2 + 1 = tp$, for $t < p$.

Thursday, April 17. Exam 2.

Tuesday, April 15. The class worked in groups on Quiz 10, and then on practice problems for Exam 2.

Thursday, April 10. We continued our discussion of GCDs in G, the Gaussian integers, with the goal of proving a version of the Fundamental Theorem of Arithmetic for the Gaussian integers. We began by recalling that GCDs exist for any two non-zero elements in G. We then gave proofs of the following facts. Note we used the notation $g \sim h$, for $g, h \in G$ to indicate that h is a unit multiple of g, i.e., g and h are *associates*.

(i) $\gcd(x, y) \sim \gcd(y, x) \sim \gcd(ux, vy)$, for units $u, v \in G$.
(ii) $\gcd(x, y) \sim \gcd(x - gy, y)$, for all $g \in G$.
(iii) If $x \mid y$ for $x, y \in G$, then $x \sim \gcd(x, y)$.
(iv) $\gcd(zx, zy) \sim z \gcd(x, y)$, for $z, x, y \in G$.
(v) If z is a GCD of x, y, and h is a common divisor of x, y, then $h \mid z$ in G.
(vi) If d and d' are GCDs of $x, y \in G$, then $d \sim d'$.

We then gave the following important definition:

Definition. Given $q \in G$, we say that q is prime in G, or q *is a Gaussian prime* if and only if the only factors of q are: $\pm 1, \pm i, \pm q, \pm qi$.

Primes in G. The following gives the primes in G:

(ii) If $p \in \mathbb{Z}$ is prime and $p \equiv 3 \bmod 4$, then p remains prime in G.
(ii) If $q \in G$ satisfies $N(q)$ is prime in $\mathbb{Z}$, then q is prime in G.
(iii) If $a + bi \in G$ and a, b are both non-zero, then $a + bi$ is prime, if and only if $a^2 + b^2$ is prime, which only occurs when $p \equiv 1 \bmod 4$.
(iv) $2 = i(i - 1)^2$ is not prime in G.

While we saw each element on the list above is prime, we did not prove that any prime in G has one of the forms above. We did assume that primes in $\mathbb{Z}$ that are congruent to 1 mod 4 are sums of two squares, and used this to see that such primes are composite in G.

We next proved the following:

Crucial Proposition. Suppose $q \in G$ is prime and $q \mid xy$ in G. Then $q \mid x$ or $q \mid y$.

We were then able to prove

Fundamental Theorem of Arithmetic for Gaussian Integers. Suppose $g \in G$ is non-zero, and not a unit. Then $g = q_1 \cdots q_r$, for primes $q_i \in G$. Moreover, if $g = p_1 \cdots p_s$, for primes $p_j \in G$, then $r = s$ and after re-indexing the p_j, $p_j \sim q_j$, for all $1 \leq j \leq r$.

We noted that, just as in the case of integers, uniqueness followed from an extended version of the Crucial Proposition, and existence followed by applying the Well Ordering principal to an element of least degree that cannot be factored as a product of primes.

Tuesday, April 8. The first fifteen minutes of class were devoted to Quiz 9. We then continued our discussion of G, the Gaussian integers, by stating and proving the following items:

(a) Given $u, v \in G$, there exist $g, r \in G$ such that $u = vg + r$, with $r = 0$ or $N(r) < N(v)$. In other words, G has a division algorithm.
(b) Suppose $p \in \mathbb{Z}$ is a prime satisfying $p \equiv 3 \bmod 4$. If we can write $p = uv$ in G, then u or v is a unit in G.

(c) Suppose $p \in \mathbb{Z}$ is a prime satisfying $p \equiv 3 \bmod 4$. If, for $x, y \in G$, $p \mid xy$ in G, then $p \mid x$ or $p \mid y$ in G.
(d) Theorem: Suppose $p \in \mathbb{Z}$ is a prime satisfying $p \equiv 3 \bmod 4$. If $p \mid (a^2 + b^2)$ in $\mathbb{Z}$, then $p \mid a$ and $p \mid b$ in $\mathbb{Z}$.
(e) GCDs exist, and the Euclidean algorithm can be used to find the GCD of two elements in G, in the same way that it can be used to find the GCD of two integers.

Thursday, April 3. The first two thirds of the class was devoted to proving the main case of Quadratic Reciprocity, namely $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})$, for odd primes p, q. The proof relied heavily on Gauss's Lemma (and its proof) together with the following

Numerical Lemma. For odd primes p, q, $\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{i=1}^{\frac{p-1}{2}}[\frac{qi}{p}] + \sum_{j=1}^{\frac{q-1}{2}}[\frac{pj}{q}]$, where $[\frac{a}{b}]$ denotes the greatest integer less than or equal to $\frac{a}{b}$.

The proof of the Numerical Lemma was achieved by counting - in two ways - the lattice points strictly contained in the rectangle in $\mathbb{R}^2$ with vertices $(0,0), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2}), (0, \frac{q}{2})$.

The rest of the class was devoted to an introductory discussion involving various properties of the *Gaussian integers* $G := \{a + bi \mid a, b \in \mathbb{Z}\}$. Among other things we noted that:

(i) Addition and multiplication in G is just the usual addition and multiplication of complex numbers, so that G is closed under addition and multiplication.
(ii) It follows from (i) that addition and multiplication in G are associative and commutative, and multiplication distributes over addition.
(iii) Given $g, h \in G$, we say g *divides* h, denoted $g \mid h$, if $h = gk$, for some $k \in G$. If followed that if $n \in \mathbb{Z}$ and $h = a + bi \in G$, then $n \mid h$ in G if and only if $n \mid a$ and $n \mid b$ in $\mathbb{Z}$.
(iv) A *unit* in G is an element $u \in G$ having a multiplicative inverse. We noted that the only units in G are $\pm 1, \pm i$. This was accomplished by using the *norm* $N : \mathbb{C} \to \mathbb{R}$ given by $N(a + bi) = a^2 + b^2$, which satisfies $N(zz') = N(z)N(z')$, for $z, z' \in \mathbb{C}$. When restricted to G, $N(g)$ is a non-zero positive integer for any $0 \neq g \in G$.

Tuesday, April 1. The first fifteen minutes of class were devoted to Quiz 8. We then embarked on a proof of the Quadratic Reciprocity theorem. The first step was to establish

Gauss' Lemma. Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Consider the list of positive integers $L := \{a, 2a, 3a, \ldots, \frac{p-1}{2}\cdot a\}$. For each $1 \leq k \leq \frac{p-1}{2}$, take n_k in the open interval $(-\frac{p}{2}, \frac{p}{2})$ such that $n_k \equiv ka \bmod p$. If v is the number of negative n_k, then $(\frac{a}{p}) = (-1)^v$.

We first illustrated Gauss' Lemma by working three examples, and having the class work one example and then gave a proof of the lemma. We then used Gauss' Lemma to prove the first and 3rd cases of

Quadratic Reciprocity for $(\frac{2}{p})$. If p is an odd prime, then $(\frac{2}{p}) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \mod p \\ -1 & \text{if } p \equiv 3, 5 \mod p \end{cases}$.

Thursday, March 27. The first fifteen minutes of class were devoted to Quiz 7. The remainder of class was devoted to group work on practice problems.

Tuesday, March 25. We began class by recalling the followings definitions and facts established in lectures prior to spring break. In the statements below, p is an odd prime.

(i) What it means for $a \in \mathbb{Z}$ to be a quadratic residue mod p or a quadratic non-residue mod p.
(ii) Euler's Quadratic residue Theorem.
(iii) The definition of the Legendre symbol $(\frac{a}{p})$.
(iv) The statement of the Quadratic Reciprocity Theorem, with an example illustrating the theorem.
(v) The result $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$.
(vi) The result $(\frac{ab}{p}) = (\frac{a}{p})\cdot(\frac{b}{p})$.

We then gave the following auxiliary statements to the quadratic reciprocity theorem: (2.) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ and (3.) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. After verifying (2.) and (3.) for $(\frac{-1}{5})$ and $(\frac{2}{7})$ respectively, we used the various properties listed above for the Legendre symbol to calculate $(\frac{5}{29})$. This was followed by presenting the following statements that are, respectively, equivalent formulations of Quadratic Reciprocity, and auxiliary statements (2.), and (3.)

Equivalent Formulations. (1'.) If $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$, then p is a quadratic residue mod q if and only if q is a quadratic residue mod p, while if $p \equiv 3 \equiv q \bmod 4$, then p is a quadratic residue mod q if and only if q is a quadratic non-residue mod p.

(2'.) -1 is a quadratic residue mod p if and only if $p \equiv 1 \bmod 4$.

(3'.) 2 is a quadratic residue mod p if and only if $p \equiv 1$ or 7 mod 8.

We then showed that Quadratic Reciprocity is equivalent to (1'.) above and left the remaining equivalence as a bonus problem. We then gave a proof of (2'). We ended class by having students determine if: (i) 41 is a square mod 103 and (ii) 79 is a square mod 101. Solutions were presented at the board.

Thursday, March 14. We began class by recalling that for an odd prime p, a is a quadratic residue mod p if $a \equiv b^2 \bmod p$, for some integer b, otherwise, a is a quadratic non-residue. We then proceeded to prove Euler's Quadratic Residue Theorem, as stated in the previous lecture. After noting that the theorem only tests whether or not a is a quadratic residue mod p, but does not give b with $a \equiv b^2 \bmod p$, we showed that if $p \equiv 3 \bmod 4$, and a is a quadratic residue mod p, then $b = a^{\frac{p+1}{4}}$ satisfies $b^2 \equiv a \bmod p$. We did not mention the case $p \equiv 1 \bmod 4$, but there is no simple answer in this case, and this must be solved using probabilistic means. We then illustrated how this works for the quadratic residues mod 7 and mod 11, after which we defined the

Legendre Symbol. Given and odd prime p and $a \in \mathbb{Z}$

$$(\frac{a}{p}) := \begin{cases} 1, \text{if } a \text{ is a quadratic residue mod } p \\ -1, \text{if } a \text{ is a quadratic non-residue mod } p \\ 0, \text{if } a \text{ is divisible by } p \end{cases}$$

We followed this by working a few examples calculating the value of $(\frac{a}{p})$ and made the following observation which was useful in calculating further examples.

Observation. $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$. We then proved the following proposition, verified it, and applied it to several examples.

Proposition. If p is an odd prime, then $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$.

We ended class by stating the celebrated quadratic reciprocity theorem of Gauss, and verified it for the case $p = 3$ and $q = 5$.

Quadratic Reciprocity Theorem. For odd primes $p \neq q$, $(\frac{p}{q}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\frac{q}{p})$.

Tuesday, March 11. The first fifteen minutes of class were devoted to Quiz 6. We then began a discussion of how to find roots to quadratic polynomials modulo a prime p. Starting with $f(x) = x^2 + bx + c$, with $p > 2$, we showed that $f(x)$ has roots modulo p if $b^2 - 4c$ has a square mod p. Upon choosing e and d satisfying $2e \equiv 1 \bmod p$ and $d^2 \equiv b^2 - 4c \bmod p$, it followed that $u := e(-b + d)$ and $v := e(-b - d)$ were roots of $f(x) \bmod p$. This was just a mod p version of the quadratic formula. We illustrated this with a few examples, including one for the class to try. We then gave the following definition.

Definition. Let $p > 2$ be prime. Suppose $p \nmid a$. Then a *is quadratic residue mod* p if $a \equiv b^2 \bmod p$, for some $b \in \mathbb{Z}$. Otherwise, s is a *quadratic non-reside* mod p.

We then calculated the quadratic residues mod 5, 7, 11 and noted that half the non-zero residues mod 5, 7, 11 were quadratic residues. We then proved this by observing that if a is a primitive root of 1 mod p, then the quadratic residues mod p were just $a^2, a^4, a^6, \cdots, a^{\frac{p-1}{2}}$, mod p. We ended class by checking the quadratic residues mod 5, 7, 11 against the following theorem.

Euler's Quadratic Residue Theorem. For p an odd prime and $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, a is a quadratic residue mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Thursday, March 6. We continued our discussion of roots to polynomial equations modulo n. In particular, we showed that if p is prime and $f(x) \in \mathbb{Z}[x]$ has degree d, then $f(x)$ has at most d distinct roots modulo p. This was followed by the important

Corollary. Suppose p is prime and $d \mid (p - 1)$. Then $f(x) = x^d - 1$ has d distinct roots mod p.

The corollary lead to the following

Definitions. (i) Given p and prime and $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, then the *order of* a mod p is the least r such that $a^r \equiv 1 \bmod p$. (ii) $a \in \mathbb{Z}$ is a *primitive root of 1* modulo n if the order of a mod n is $\phi(n)$.

We then calculated the order of integers not divisible by 5, mod 5, and noted that 2 and 3 are primitive roots of 1 mod 5. On the other hand, for any $a \in \mathbb{Z}$ such that $\gcd(a, 8) = 1$, the only orders of elements mod 8 are one and two. Thus, we saw that there are no primitive roots of 1 mod 8. This was followed by a side discussion of roots of unity over $\mathbb{C}$ and primitive roots of unity over $\mathbb{C}$. We ended class by proving the following theorem.

Theorem. Suppose p is prime. Then there exists at least one primitive root of 1 mod p.

The proof of the theorem was based upon two lemmas that allowed us to make the following statements: If we write $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ as a prime factorizations, then there are $q_i^{e_i}$ roots of $x^{q_i^{e_1}} - 1 \bmod p$, $q_i^{e_i-1}$ roots of $x^{q_i^{e_i-1}} - 1$, showing that there must be $q_i^{e_i} - q_i^{e_i-1}$ elements $1 < a_i \leq p$ such that $a^{q_i^{e_i}} \equiv 1 \bmod p$ and $a^{q_i^{e_i-1}} \not\equiv 1 \bmod p$, so that the order of $a_i \bmod p$ is $q_i^{e_i}$. Thus, the order of $a := a_1 \cdots a_r$ modulo p is $q_1^{e_1} \cdots q_r^{e_r} = p-1$, i.e., a is a primitive root of $1 \bmod p$.

Tuesday, March 4. Most of the class was devoted to discussing the Chinese Remainder Theorem (CRT):

Theorem. Suppose $n_1, \ldots, n_r \in \mathbb{Z}$ are positive integers such that for all $i \neq j$, $\gcd(n_i, n_j) = 1$. Then for all $a_1, \ldots, a_r \in \mathbb{Z}$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

has a solution in $\mathbb{Z}$. Moreover, if x, y are solutions to the system, then $x \equiv y \bmod N$, where $N = n_1 \cdot n_2 \cdots n_r$.

We first proved the case $n = 2$ and worked an example, and then had the class work the following example: Solve the system of congruences $x \equiv 5 \bmod 6$ and $x \equiv 2 \bmod 11$. We then noted that since 5 has a multiplicative inverse modulo 6 and 7 has a multiplicative inverse modulo 11, we can also solve the system: $5x \equiv 5 \bmod 6$ and $7x \equiv 2 \bmod 11$.

We then proved the general case of the CRT as follows. Set $N_i := \frac{N}{n_i}$. Let c_i be the multiplicative inverse of N_i modulo n_i. This is possible since $\gcd(n_i, N_i) = 1$ for all i. Then $x := a_1c_1N_1 + \cdots + a_rc_rN_r$ is a solution to the given system of congruences. This theorem was illustrated by an example in the lecture, and an example worked by the class.

The remainer of the class was devoted to an initial discussion of the following: Given $f(x) \in \mathbb{Z}[x]$, we say that $a \in \mathbb{Z}$ is a root of $f(x)$ modulo n if $f(a) \equiv 0 \bmod n$, or equivalently, $n \mid f(a)$. We also noted that this was equivalent to saying that in $\mathbb{Z}_n$, $\overline{f}(\overline{a}) = \overline{0}$, where $\overline{f}(x)$ is the polynomial in $\mathbb{Z}_n[x]$ obtained by reducing the coefficients of $f(x) \bmod n$. We then noted that if a is a root of $f(x) \bmod n$, then so is b, for any $b \in \mathbb{Z}$ satisfying $a \equiv b \bmod n$. Finally, we noted that if the degree of $f(x)$ is d it is possible for $f(x)$ to have more than d roots mod n, as illustrated by $f(x) = x^2 - 1$ which has four roots modulo 8. We also noted (but did not prove) that this cannot happen modulo a prime.

Thursday, February 27. Exam 1.

Tuesday, February 25. The first fifteen minutes of class was devoted to Quiz 5, and in the remaining time, the class worked in groups on practice problems for Exam 1.

Thursday, February 20. The first fifteen minutes of class were devoted to Quiz 4. This was followed by a review of the definition of an equivalence relation and the definition of equivalence class, given an equivalence relation. We then showed that if X is a set with an equivalence relation, then X is a disjoint union of its distinct equivalence classes.

This was followed by a lengthy discussion of the realization of the rational numbers as the set of distinct equivalence classes on the set of ordered pairs (a, b) of integers with $b \neq 0$, under the relation $(a, b) \sim (c, d)$ if and only if $ad - bc$. We showed that if $[(a, b)]$ and $[(c, d)]$ are two such classes then the operation $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$ is well defined and left the corresponding well definedness of multiplication as an exercise.

The last part of the class was devoted to the consideration of solving linear congruence relations of the form $ax \equiv b \bmod n$. We noted we could ask for solutions to this equation in $\mathbb{Z}_n$ or $\mathbb{Z}$. We first observed that if $\gcd(a, n) = 1$, then the congruence equation has a unique solution, since a has a multiplicative inverse modulo n. However, if $\gcd(a, n) > 1$, we worked some examples where the congruence had not solution one the one hand, and multiplce solutions on the other.

Tuesday, February 18. Snow day.

Thursday, February 13. We began class by discussing Gauss's Theorem: $n = \sum_{d|n} \phi(d)$. We verified the theorem in a few cases, and then the class worked through how the proof goes for $n = 18$, by writing out the fractions $\frac{1}{18}, \frac{2}{18}, \ldots, \frac{18}{18}$, then reducing each fraction to lowest term, and counting how many times each denominator occurs - the denominators being the divisors of n. We noted each denominator d occurs $\phi(d)$ times, which lead to an understanding as to how the proof works in general.

We then introduced the function $\tau(n)$ and $\sigma(n)$, where $\tau(n)$ is the number of divisors of n and $\sigma(n)$ is the sum of the divisors of n. We then proved:

Theorem. For $n > 1$, with prime factorization $p_1^{e_1} \cdots p_r^{e_r}$, with each $e_i \geq 1$, we have"

(i) $\tau(n) = (e_1 + 1) \cdots (e_r + 1)$.

(ii) $\sigma(n) = \frac{p_1^{e_1+1}-1}{p_1-1} \cdots \frac{p_r^{e_r+1}-1}{p_r-1}$.

We then began a discussion of equivalence relations, by giving the standard definition and the flowing exams: (i) Equality on a set X is an equivalence relation; (ii) Fixing $n > 1$, then congruence modulo n is an equivalence relation on $\mathbb{Z}$. The details of this were given in the lecture of January 30; For the set $X := \{(a, b) \mid a, b \in \mathbb{Z}, \text{ with } b \neq 0\}$, and $(a, b) \sim (c, d)$ if and only if $ad - bc = 0$ is an equivalence relation.

Tuesday, February 11. The first fifteen minutes of class were devoted to Quiz 3. Then we began a discussion of the following theorems involving $\phi(n)$.

Euler's Theorem. For $n > 1$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, $a^{\phi(n)} \equiv 1 \bmod n$.

We first did some easy examples verifying the formula directly. Then we used Euler's theorem to: (a) Calculate the one's digit of 7^{222} and (b) Calculate the residue class of $1234^{7865435}$ modulo 11. We also noted that Fermat's theorem, which states that for any prime p and any $a \in \mathbb{Z}$, $a^p \equiv a \bmod p$. This was followed by giving a proof of Euler's theorem.

We then discussed:

Euler's Product formula. For $n \geq 1$, $\phi(n) = n \cdot \prod_{d|n}(1 - \frac{1}{p})$.

After verifying the formula for $n = 24, 42$, we asked the class to try to write a proof of the case $n = p_1^{e_1} p_2^{e_2}$. After discussing this case, we gave a proof of the formula that used the prime factorization of n.

We ended class with an initial discussion of Gauss's Theorem which states: For any $n \geq 1$, $n = \sum_{d|n} \phi(d)$.

Thursday, February 6. We began class by reviewing the definition of the Euler totient function $\phi(n)$and calculating some of its values. We then discussed and proved the following properties of $\phi(n)$:

Properties of the Euler totient function. Let $\phi(n)$ be the totient function. Then:

(i) If p is prime, $\phi(p) = p - 1$.

(ii) If $\gcd(a, b) = 1$, then $\phi(ab) = \phi 9a)\phi(b)$.

(iii) If p is prime, and $e \geq 1$, then $\phi(p^e) = p^e - p^{e-1}$.

(iv) If $n = p_1^{e_1} \cdots p_r^{e_r}$is a prime factorization of n, with $p_1, \ldots, p_r$ distinct primes, then

$$\phi(m) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1}).$$

The proof of (i) was clear, the proof of (iii) followed by counting the positive integers less than or equal to p^e that are not relatively prime to p^e, and the proof of (iv) was straightforward using an iteration of (ii) together with (iii). Most of the class was devoted to a proof of (ii).

To get an understanding of the proof of (ii), we defined a function $f : \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$ given by $f(\tilde{i}) = (\bar{i}, \hat{i})$, where $\tilde{i}$ is the residue class of i mod 12, $\bar{i}$ is the residue class of i mod 3 and $\hat{i}$ is the residue class of i mod 4. We noted that this function was one-one and set up a one-one, onto correspondence between the elements of $\mathbb{Z}_{12}$ that have a multiplicative inverse and the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$ that have a multiplicative inverse. Since there are $\phi(12)$ in the former set and $\phi(3)\phi(4)$ in the latter, this explains property (ii) in this special case.

The general case proceeded in a similar fashion by first noting that an element in $\mathbb{Z}_a \times \mathbb{Z}_b$ has a multiplicative inverse if and only if each coordinate has a multiplicative inverse and the function $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ given by establishing the following facts about the function $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ by $f(\tilde{i}) = (\bar{i}, \hat{i})$: (1) F is multiplicative and (2) f is 1-1, and therefore onto. These properties implied that f gives a one-to-one, onto correspondence between the elements of $\mathbb{Z}_n$ that have a multiplicative inverse and the elements of $\mathbb{Z}_a \times \mathbb{Z}_b$ that have a multiplicative inverse. Since there are $\phi(n)$ in the former set and $\phi(a)\phi(b)$ in the latter, this established property (ii) in general.

Tuesday, February 4. The first fifteen minutes of class were devoted to Quiz 2. We then reviewed the definition of what it means for $a \in \mathbb{Z}$ to be congruent to b modulo n, i.e., $a \equiv b \bmod n$ if and only if n divides $a - b$. We wrote out the distinct congruence classes (remainder classes) modulo n and showed how to extend the modular arithmetic defined last time for remainders modulo n to all of $\mathbb{Z}$ by showing that if $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $(a + c) \equiv (b + d) \bmod n$ and $ac \equiv bd \bmod n$. We then defined $\mathbb{Z}_n$ to be the number system $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, where $\overline{i}$ can be taken to be any integer congruent to i modulo n. We then noted that all the usual rules for arithmetic over $\mathbb{Z}$ work for $\mathbb{Z}$ modulo n, namely: For all $a, b, c \in \mathbb{Z}$, we have

(i) $a + b \equiv b + a \bmod n$

(ii) $(a + b) + c \equiv a + (b + c) \bmod n$

(iii) $0 + a \equiv a \bmod n$

(iv) $a + (-a) \equiv 0 \bmod n$
(v) $ab \equiv ba \bmod n$
(vi) $a(bc) \equiv (ab)c \bmod n$
(vii) $a(b+c) \equiv ab + ac \bmod n$
(viii) $1 \cdot a \equiv a \bmod n$.

We then noted that, unlike the case for $\mathbb{Z}$, where the only numbers with multiplicative inverses are $1, -1$, over $\mathbb{Z}_n$, we can have several numbers who have multiplicative inverses modulo n. After the class worked several examples finding inverses modulo 7 and modulo 8, we proved the following:

Theorem. Fix $n > 1$. Then $a \in \mathbb{Z}$ has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.

We ended class by defining Euler's *totient* function $\phi(n)$, which gives the number of positive integers less than n and relatively prime to n, which by the theorem above gives the number of elements in $\mathbb{Z}_n$ that have a multiplicative inverse.

Thursday, January 30. We began by discussing and proving the following theorem:

Theorem. Given $a, b \in \mathbb{N}$, with $a, b > 1$, and $\gcd(a, b) \neq 1$. Write $a = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$ and $b = c_1^{d_1} \cdots c_t^{d_t} q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, then $\gcd(a, b) = q_1^{\min\{f_1, \alpha_1\}} \cdots q_s^{\min\{f_s, \alpha_s\}}$, where p_i, q_j, c_k are primes, $q_1, \ldots, q_s$ are the primes dividing both a and b and all exponents are greater than or equal to one.

We then defined the *least common multiple* - LCM - of two natural numbers a, b and presented the following:

Proposition. Given $a, b \in \mathbb{N}$:
(i) The LCM of a and b, exists.
(ii) If $e = \text{LCM}(a, b)$ and c is a common multiple of a and b, then $c \mid e$.
(iii) For $a, b \in \mathbb{N}$ as in the theorem above, $\text{LCM}(a, b) = p_1^{e_1} \cdots p_r^{e_r} c_1^{d_1} \cdots c_t^{d_t} q_1^{\max\{f_1, \alpha_1\}} \cdots q_s^{\max\{f_s, \alpha_s\}}$
(iv) $\text{LCM}(a, b) = \frac{ab}{\gcd(a,b)}$.

We then turned to a discussion of modular arithmetic. We began finding addition and multiplication tables for the integers modulo 4 and modulo 5. We noticed that a product of non-zero remainders can be zero, working modulo 4, but this does not happen modulo 5. We noted this latter fact followed from the fact that the non-zero remainders modulo 5 have multiplicative inverses.

For fixed $n > 1$, e then defined two integers a, b to be *congruent modulo* n, denoted $a \equiv b \bmod n$ if $a - b$ is divisible by n and then showed:
(i) $a \equiv a \bmod n$
(ii) If $a \equiv b \bmod n$, then $b \equiv a \bmod n$.
(iii) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.

We ended class by noting that: The integers congruent to 0 mod 4 are all integers of the form $4n$, with $n \in \mathbb{Z}$; The integers congruent to 1 mod 4 are all integers of the form $4n + 1$, with $n \in \mathbb{Z}$; The integers congruent to 2 mod 4 are all integers of the form $4n + 1$, with $n \in \mathbb{Z}$; The integers congruent to 3 mod four are all integers of the form $4n + 3$, with $n \in \mathbb{Z}$, finally noting that $\mathbb{Z}$ is the disjoint union of these four sets.

Tuesday, January 28. We began class with our first Quiz. We then reviewed the fact that the GCD of two integers can be found using the Euclidian, where the last non-zero remainder is the GCD, and recalling that backwards substitution yields $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. We then discussed Blankinship's Method for finding $\gcd(a, b)$, and the s, t used to express $\gcd(a, b)$ in terms of a, b and did a few examples using this method.

Blankinship's Method. For $b > a > 0$, starting with $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$, perform a sequence of the row operation of adding a multiple of one row to another, to end up with either $\begin{pmatrix} 0 & * & * \\ d & s & t \end{pmatrix}$ or $\begin{pmatrix} d & s & t \\ 0 & * & * \end{pmatrix}$, then $d = sa + tb$ is the GCD of a and b.

From here, we then proved the following

Fundamental Property of primes. Suppose $p \in \mathbb{N}$ is prime and $p \mid ab$, for $a, b \in \mathbb{Z}$. Then, $p \mid a$ or $p \mid b$.

Using the fundamental property of primes we then gave an inductive argument proving the uniqueness part of the Fundamental Theorem of Arithmetic, as stated in the lecture of January 21. We ended class by discussing how to use prime factorization to find the GCD of two positive integers.

Thursday, January 23. We began class with the following definition.

Definition. Given integers d, n with $0 \neq d$, we say d *divides* n if $n = dm$, for some integer m. In this case we write $d \mid n$. If d does not divide n, we write $d \nmid m$.

We followed this by discussing several properties of divisibility, the most most crucial being that if d divides $n_1, \ldots, n_k$, then d divides $a_1 n_1 + \cdots + a_k n_k$, for all choices of $a_1, \ldots, a_k \in \mathbb{Z}$. We then asked the class to take a couple of minutes at their desk to prove that if $d > 0$ and d divides both a and $a + 1$, then $d = 1$.

We then had a lengthy discussion, including a proof of the:

Division Algorithm. Given integers a, b with > 0, there exist *unique* integers q, r such that: (i) $b = aq + r$ and (ii) $0 \leq r < a$.

After giving a proof of the Division Algorithm, we used iterations of the algorithm (called the Euclidean algorithm) to calculate the greatest common divisor of a few pairs of integers. We noticed that in each case, the GCD f the original pair of integers was the last non-zero remainder in the Euclidean Algorithm. We then formally verified that this process works to yield the GCD by induction. The critical point was the following: Given integers a, b, with $a > 0$, if $b = aq + r$, as in the division algorithm, $\gcd(a, b) = \gcd(r, a)$. This was followed by establishing the two properties of GCD: (i) $\gcd(na, nb) = n \gcd(a, b)$, for any $n > 0$ and (ii) If $e \mid a$ and $e \mid b$, then $e \mid \gcd(a, b)$.

We ended class by mentioning Bezout's Principle: For non-zero $a, b \in \mathbb{Z}$, there exist $n, m \in \mathbb{Z}$ such that $\gcd(a, b) = na + mb$.

Tuesday, January 21. We began class by giving an over view of some of the topics to be covered this semester. Then, we began an informal discussion of the following fact: Every natural number has a prime factor. Here we argued heuristically, noting that this fact is a consequence of the following property of natural numbers: There does not exist an infinite decreasing sequence of natural numbers. We then stated the following principle, which we take as an axiom:

Well Ordering Principle. Every non empty subset of the natural numbers has a least element.

Using the Well Ordering Principle, we gave a formal proof of the existence statement in the following theorem:

Fundamental Theorem of Arithmetic. Every natural number greater than or equal to 2 can be written *uniquely*, up to order, as a product of prime numbers.

We noted that the uniqeness statement is not easy to prove, namely, if $p_1 \cdots p_2 = q_1 \cdots q_s$, with each p_i, q_j prime, then $r = s$ and, after re-indexing, $p_i = q_i$, for all $1 \leq i \leq r$. The proof of this will require more tools than we currently have available.

We then had a general discussion about the family of primes, first proving that there are infinitely many primes, and noting that the proof gives a crude estimate for how far from a given prime one has to go to encounter the next prime. We noted that in general, there are difficult theorems that say *as a rule*, primes are more scarce as one goes further out among the natural numbers, but that a famous conjecture, the Twin Prime Conjecture, hypothesizes that there are infinitely many prime pairs $p, p + 2$. We also showed that one can create arbitrarily large gaps between consecutive primes by considering the sequence: $(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + (n + 1)$, which consists of n consecutive composite numbers.

We ended class by presenting three forms of mathematical induction and working a couple of examples to illustrate this proof technque. Here is the most general form we presented:

Mathematical Induction. Given a sequence of statements $P(n)$, with $n \geq n_0$. The statements $P(n)$ are valid for all $n \geq n_0$ if the following two statements hold:

(i) $P(n_0)$ is valid.
(ii) $P(n)$ is valid if each $P(k)$ is valid, for $1 \leq k \leq n - 1$.