

SPRING 2025: MATH 540 DAILY UPDATE

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 $2e \equiv 1 \pmod{p}$ and $d^2 \equiv b^2 - 4c \pmod{p}$, it followed that $u := e(-b + d)$ and $v := e(-b - d)$ were roots of $f(x)$ mod 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 a *quadratic residue mod p* if $a \equiv b^2 \pmod{p}$, for some $b \in \mathbb{Z}$. Otherwise, a is a *quadratic non-residue 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 $a^2, a^4, a^6, \dots, a^{\frac{p-1}{2}}$, 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 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

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 $p \mid (d - 1)$. 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 $a^r \equiv 1 \pmod{p}$. (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 $x^{q_i^{e_i}} - 1 \pmod{p}$, $q_i^{e_i-1}$ 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 $a_i^{q_i^{e_i}} \equiv 1 \pmod{p}$ and $a_i^{q_i^{e_i-1}} \not\equiv 1 \pmod{p}$, so that the order of a_i mod 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 mod p .

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

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

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

has a solution in \mathbb{Z} . Moreover, if x, y are solutions to the system, then $x \equiv y \pmod{N}$, 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 $x \equiv 5 \pmod{6}$ and $x \equiv 2 \pmod{11}$. 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: $5x \equiv 5 \pmod{6}$ and $7x \equiv 2 \pmod{11}$.

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 $x := a_1 c_1 N_1 + \dots + a_r c_r N_r$ 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 remainder 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 $f(a) \equiv 0 \pmod{n}$, or equivalently, $n \mid f(a)$. We also noted that this was equivalent to saying that in \mathbb{Z}_n , $\bar{f}(\bar{a}) = \bar{0}$, where $\bar{f}(x)$ is the polynomial in $\mathbb{Z}_n[x]$ obtained by reducing the coefficients of $f(x) \pmod{n}$. We then noted that if a is a root of $f(x) \pmod{n}$, then so is b , for any $b \in \mathbb{Z}$ satisfying $a \equiv b \pmod{n}$. 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 $ad - bc = 0$. 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 $ax \equiv b \pmod{n}$. 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 no solution on the one hand, and multiple 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 $\frac{1}{18}, \frac{2}{18}, \dots, \frac{18}{18}$, 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 $p_1^{e_1} \dots p_r^{e_r}$, with each $e_i \geq 1$, we have"

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

We then began a discussion of equivalence relations, by giving the standard definition and the following examples: (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 $\gcd(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$.

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 $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$. This was followed by giving a proof of Euler's theorem.

We then discussed:

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

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 $\phi(ab) = \phi(a)\phi(b)$.
- (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, \dots, p_r distinct primes, then

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

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 $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_4$ given by $f(\tilde{i}) = (\tilde{i}, \hat{i})$, where \tilde{i} is the residue class of $i \pmod{12}$, \bar{i} is the residue class of $i \pmod{3}$ and \hat{i} is the residue class of $i \pmod{4}$. 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 $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ given by establishing the following facts about the function $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ by $f(\tilde{i}) = (\tilde{i}, \hat{i})$: (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., $a \equiv b \pmod{n}$ 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 $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$ and $ac \equiv bd \pmod{n}$. We then defined \mathbb{Z}_n to be the number system $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, where \bar{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) $a + b \equiv b + a \pmod{n}$
- (ii) $(a + b) + c \equiv a + (b + c) \pmod{n}$
- (iii) $0 + a \equiv a \pmod{n}$
- (iv) $a + (-a) \equiv 0 \pmod{n}$
- (v) $ab \equiv ba \pmod{n}$

- (vi) $a(bc) \equiv (ab)c \pmod n$
- (vii) $a(b+c) \equiv ab+ac \pmod n$
- (viii) $1 \cdot a \equiv a \pmod n$.

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, \dots, 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 $n > 1$, we then defined two integers a, b to be *congruent modulo n* , denoted $a \equiv b \pmod n$ if $a - b$ is divisible by n and then showed:

- (i) $a \equiv a \pmod n$
- (ii) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
- (iii) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

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 $4n + 2$, 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 $d \nmid n$.

We followed this by discussing several properties of divisibility, the most crucial being that if d divides n_1, \dots, n_k , then d divides $a_1n_1 + \dots + a_kn_k$, for all choices of $a_1, \dots, a_k \in \mathbb{Z}$. 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 $b > 0$, 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 of 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 overview 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 uniqueness statement is not easy to prove, namely, if $p_1 \cdots p_r = q_1 \cdots q_s$, 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: $(n + 1)! + 2, (n + 1)! + 3, \dots, (n + 1)! + (n + 1)$, 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 technique. 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 $1 \leq k \leq n - 1$.