Introduction To Number Theory

Neelam Akula

Last Updated: April 26, 2021

Contents

1 The Integers

1.1 Numbers and Sequences

This section will set the stage for what's to come. It is primarily about numbers.

Mostly we will be working with the *integers* $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Additionally, we have the *natural numbers* $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ which are a subset of $\mathbb{Z}^+$.

Definition. We say a set of real numbers is *well-ordered* if every non-empty subset has a smallest element.
Ex. $S = \{1, 2, 3, \cdots\}$ is well-ordered because every subset of S has a least element.
Ex. $S = [0, \infty)$ is *not* well-ordered because every subset does *not* have a least element. Consider the subsets $(0, \infty)$, $(0, 2)$, or $(1, 5]$, none of them have least elements.

Well-Ordering Principle. $\mathbb{Z}^+$ is well-ordered. (This proof involves some serious set theory, far beyond the scope of this course. See this as the proof.)

Definition. A real number is *rational* if it can be expressed as a/b where $a, b \in \mathbb{Z}$ and $b \neq 0$. The set of all rational numbers is denoted as $\mathbb{Q}$.

Ex. Prove $\sqrt{2}$ is irrational (not rational).

Proof. We need to prove that we cannot write $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ and $b \neq 0$. By way of contradiction, suppose $\sqrt{2}$ is rational. That is, suppose

$$\sqrt{2} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}^+$ and $b \neq 0$. Then we have that $a = b\sqrt{2}$. Note that $b \in \mathbb{Z}^+$ and $b\sqrt{2} = a \in \mathbb{Z}^+$.

Let $S = \{k \mid k \in \mathbb{Z}^+ \text{ and } k\sqrt{2} \in \mathbb{Z}^+\}$. Then $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$ because $b \in S$. By the well-ordering principle, S has a least element, denote it m. Consider $m' = m\sqrt{2} - m$. Observe the following:

- $m' = m\sqrt{2} - m = m(\sqrt{2} - 1)$. Therefore $0 < m' < m$.
- Because $m \in S$ and $S \subset \mathbb{Z}^+$, $m, m\sqrt{2} \in \mathbb{Z}^+$. So $m' \in \mathbb{Z}^+$.
- Since $m \in \mathbb{Z}^+$ we have $2m \in \mathbb{Z}^+$, so now consider

$$m'\sqrt{2} = (m\sqrt{2} - m)\sqrt{2} = 2m - m\sqrt{2} \in \mathbb{Z}^+$$

Thus, $m' \in S$, which contradicts the fact that m is the least element in S. $\square$

Definition. A real number is *algebraic* if it is the root of a polynomial with integer coefficients.
Ex.

- Consider $x^3 + 3$. The roots are $x \pm \sqrt{3}$. So $\pm\sqrt{3}$ is algebraic.

- Is 7 algebraic? Yes, $x - 7$.
- Is $3/2$ algebraic? Yes, $3x - 2$.
- Is $\sqrt[3]{2-\sqrt{7}}$ algebraic? Yes (although a bit more complicated)

$$\begin{aligned} x = \sqrt[3]{2-\sqrt{7}} &\implies x^3 = 2 - \sqrt{7} \\ &\implies x^3 - 2 = \sqrt{7} \\ &\implies (x^3-2)^2 = 7 \\ &\implies x^6 - 4x^3 + 4 = 7 \\ &\implies x^6 - 4x^3 - 3 = 0 \end{aligned}$$

- Is π algebraic? No! So what is it?

Definition. A real number is not algebraic is *transcendental* (it transcends the ability to be expressed as a root of a polynomial). So π is transcendental.
It is not difficult to prove the existence of transcendental numbers, but it is difficult to prove that any given number is transcendental.

Definition. Define $\lfloor x \rfloor$ to be the largest integer $\leq x$. Similarly, define $\lceil x \rceil$ to be the smallest integer $\geq x$.
Ex.

- $\lfloor 5.2 \rfloor = 5$
- $\lfloor -3.8 \rfloor = -4$
- $\lceil 5.2 \rceil = 6$
- $\lceil -3.8 \rceil = -3$

Definition. A set of numbers is *countable* if it is either finite or it can be placed in one-to-one correspondance with the positive integers.
Ex. The positive, even integers are countable, as are the integers and the rationals.
Ex. The real numbers are not countable. This is proved by Cantor's Argument.

Consider all polynomials with integer coefficients. There are countably many of these, each having countably many roots. Thus there are countably many algebraic numbers (the countable union of countable sets is countable). So out of $\mathbb{R}$, which is uncountable, we must have uncountably transcendental numbers (because they are "everything else").

1.2 Sum and Products

Here is a quick review of sums and products.

1. Recall $\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$.

2. Additionally, some useful identities are:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(n+2)}{6}$$

$$\sum_{i=1}^{n} r^i = \frac{r^{n+1}-1}{r-1}$$

3. Telescoping sums (using partial fractions) $\sum_{i=2}^{n} \frac{1}{i(i+1)} = \sum_{i=2}^{n} \frac{1}{i} - \frac{1}{i+1}$.

4. Product notation $\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n$.

1.3 Mathematical Induction

Weak Mathematical Induction. Suppose we wish to prove some statement is true for all $n = 1, 2, 3, \cdots$. Induction works as follows. We prove two things

1. **Base Case:** We prove it for $n = 1$.
2. **Inductive Step:** We prove that *if* it is true for some $k \geq 1$, then it *must* be true for $k + 1$.

Then we can conclude that it is true for $n = 1, 2, 3, \cdots$
Ex. Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all $n = 1, 2, 3, \cdots$.

Proof.

Base Case:

Let $n = 1$, $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$ so the base case is valid.

Inductive Step:

Assume that it is true for some k. That is, assume

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Then consider the sum to $k+1$

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} +(k+1) \\ &= \left[\frac{k(k+1)}{2}\right] + (k+1) \quad \text{by IH} \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}\end{aligned}$$

Thus, by weak induction

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

□

Ex. Prove $2^n > n!$ for all $n \geq 4$.

Proof.

Base Case:

Let $n = 4$, $2^4 = 16$ and $4! = 24$ so the base case is valid.

Inductive Step:

Assume that it is true for some $k \geq 4$. That is, assume

$$2^k < k!$$

Then consider the equation to $k+1$

$$2^{k+1} = 2 \cdot 2^k < 2k! < (k+1)k! = (k+1)!$$

Thus, by weak induction

$$2^k < k!$$

□

Strong Mathematical Induction. Here, for the inductive step, instead of just assuming its true for k , we assume it is true for $1, 2, \cdots, k$. Then we show it is true for $k+1$. (The nice thing is we get to assume more for the inductive hypothesis.)
Why would we need to do this alternative form? Often, to prove it is true for $k+1$, it is insufficient to assume it is true for k. We may need earlier values. **Ex.** Suppose we only have 3 cent and 7 cent stamps. We claim that we can make any cent postage of 12 or more cents. Observe that, for example, knowing we can do 50 cents does not tell us we can do 51 cents! However, we know that if we can do 50 cents we can do 53 cents. Assume we can do $12, \cdots, k$. How can we do $k+1$? Well, since we can do 12 to k, we know can do $k-2$. So we just add a 3 cent stamp to $k-2$. But this only hold if $k-2 \geq 12$, which is only true if

$k \geq 14$. So the inductive step is only valid for $k = 14, 15, 16, \cdots$. So as our base case, we must do 12,13, and 14 as base cases! Thus, for strong induction, you actually would want to do the inductive step first to know how you should setup you base case! In this case we have,

$$\begin{aligned} 12 &= 4(\text{3-cent}) \\ 13 &= 2(\text{3-cent}) + 1(\text{7-cent}) \\ 14 &= 2(\text{7-cent}) \end{aligned}$$

Thus, by strong induction, we can form any cent postage greater than or equal to 12 with 3 and 7 cent stamps.

1.4 Divisibility

Divisibility underlies much of what is done in number theory.

Definition. Given $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there exists $c \in \mathbb{Z}$ such that $ac = b$. When this happens, we say $a \mid b$, otherwise we say $a \nmid b$.
Ex.

- $5 \mid 20$ because $5(4) = 20$.
- $7 \nmid 10$ because $7c \neq 10, \forall c \in \mathbb{Z}$.

Note, we may have $b = 0$. In fact $a \mid 0$ for all a because $a(0) = 0$ for all $a \in \mathbb{Z}$. We don't talk about either $0 \mid b$ nor $0 \nmid b$.

Theorem. If $a \mid b$ and $a \mid c$ then $a \mid (\alpha b + \beta c)$ for any $\alpha, \beta \in \mathbb{Z}$.

Proof. $a \mid b$ so $\exists x \in \mathbb{Z}$ such that $ax = b$. Additionally, $a \mid c$ so $\exists y \in \mathbb{Z}$ such that $ay = c$. Then $\alpha b + \beta c = \alpha(ax) + \beta(ay) = a(\alpha x + \beta y)$. So since $\alpha x + \beta y \in \mathbb{Z}$, we have $a \mid (\alpha b + \beta c)$. □

Theorem. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Since $a \mid b$, there $\exists x \in \mathbb{Z}$ such that $ax = b$. Additionally, $b \mid c$, there $\exists y \in \mathbb{Z}$ such that $by = c$. Then $c = by = axy = a(xy)$. So $a \mid c$. □

The Division Algorithm. If $a, b \in \mathbb{Z}$ and $b > 0$ then $!\exists q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = bq + r$.

Proof. First we'll prove that q, r exist. Define the set S as follows,

$$S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$$

Then $S \subset \mathbb{Z}^+$, therefore S has a least element. Let r be the least element and q be the k-value which yields it. So $r = a - bq$ is the smallest element in S. Therefore $a = bq + r$. We now need to show $0 \leq r < b$.

We know $r \geq 0$ because $r \in S$. Suppose $r \geq b$. Then note $r \geq b$ implies that $r - b \geq 0$. Separately, $r - b < r$ because $b > 0$. Therefore $0 \leq r - b = (a - bq) - b = a - b(q + 1)$.

Therefore $r - b \in S$, but this means that r is not the least element! This is a contradiction. Therefore $0 \le r < b$.

What remains to be shown is uniqueness. By way of contradiction, assume

$$a = bq_1 + r_1$$

$$a = bq_2 + r_2$$

for $0 \le r_1 < b$ and $0 \le r_2 < b$. Subtracting the equations, we get $0 = b(q_1 - q_2) + (r_1 - r_2)$ which implies $(r_2 - r_1) = b(q_1 - q_2)$. Therefore $b \mid (r_2 - r_1)$ but $-b < r_2 - r_1 < b$. So $r_2 - r_1 = 0$, which means $r_2 = r_1$. Therefore $0 = b(q_1 - q_2)$ which implies $q_1 - q_2 = 0$ because $b > 0$. So $q_1 = q_2$. $\square$

Definition. Suppose $a, b \in \mathbb{Z}$ with at least one nonzero. We define the *greatest common divisor* $\gcd(a, b)$, to be the largest integer dividing both.

Definition. For $a, b \in \mathbb{Z}$, with at least one nonzero. We say that a and b are *relatively prime* (or *coprime*) if $\gcd(a, b) = 1$.

1.5 Problems

---

1. Determine whether each of the following sets is well-ordered. If so, give a proof which relies on the fact that $\mathbb{Z}^+$ is well-ordered. If not, give an example of a subset with no least element.
   (a) $\{a \mid a \in \mathbb{Z}, a > 3\}$
   (b) $\{a \mid a \in \mathbb{Q}, a > 3\}$
   (c) $\{\frac{a}{2} \mid a \in \mathbb{Z}, a \ge 10\}$
   (d) $\{\frac{2}{a} \mid a \in \mathbb{Z}, a > 10\}$
2. Suppose $a, b \in \mathbb{Z}^+$ are unknown. Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk > 0\}$. Explain why S has a smallest element but no largest element.
3. Use the well-ordering property to show that $\sqrt{5}$ is irrational.
4. Use the identity
$$\frac{1}{k^2-1} = \frac{1}{2}\left(\frac{1}{k-1} - \frac{1}{k+1}\right)$$
   to evaluate the following:
   (a) $\sum_{k=2}^{10} \frac{1}{k^2-1}$
   (b) $\sum_{k=2}^{n} \frac{1}{k^2-1}$
   (c) $\sum_{k=1}^{n} \frac{1}{k^2+2k}$ Hint: $k^2 + 2k = (???)^2 - 1$

5. Find the value of each of the following:

   (a) $\prod_{j=2}^{7}\left(1-\frac{1}{j}\right)$

   (b) $\prod_{j=2}^{n}\left(1-\frac{1}{j}\right)$

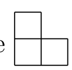
   (c) $\prod_{j=2}^{n}\left(1-\frac{1}{j^2}\right)$ Hint: Be sneaky!

6. Use weak mathematical induction to prove that

$$\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$$

   for every positive integer n.

7. Use Weak Mathematical Induction to show that $f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}$ for all $n \geq 1$.

8. Use weak mathematical induction to show that a $2^n \times 2^n$ chessboard with a corner missing can be tiled with pieces shaped like  for every integer $n \geq 0$.

9. Define:

$$H_{2^n} = \sum_{j=1}^{2^n} \frac{1}{j}$$

   Use weak mathematical induction to prove that for all $n \geq 1$ we have $H_{2^n} \leq 1 + n$.

10. Use strong mathematical induction to prove that every amount of postage over 53 cents can be formed using 7-cent and 10-cent stamps.

3 Primes and Greatest Common Divisors

3.1 Pime Numbers

Primes are important in number theory because they are the building blocks for the positive integers. Many things about $\mathbb{Z}^+$ have been proven by focusing on primes (this is done all the time in abstract algebra).

Definition. An integer greater than 1 is called *prime* if its only positive divisors are 1 and itself.

Definition. An integer greater than 1 is called *composite* if it is not prime.

Theorem. Every integer greater than 1 has at least one prime divisor.

Proof. By way of contradiction, suppose there's an integer greater than 1 with no prime divisors. Let $S = \{\text{all integers greater than 1 with no prime divisors}\}$. Then $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$. So S must have a least element. Call this n. So n is the smallest element with no prime divisors. Well, n divides n, so since n is a divisor of n, n is not prime, so it is composite. So $n = ab$ with $1 < a < n$ and $1 < b < n$.

Consider a. Since $a < n$, we know $a \notin S$. So a has at least one prime divisor, call it p. So $p \mid a$ and $a \mid n$, which means $p \mid n$. This is a contradiction! □

Theorem. There are infinetely many primes.

Proof. Assume there are fineitely many primes. Denote them by $p_1, p_2, \cdots, p_n$. Construct the number $N = p_1 \times p_2 \times \cdots \times p_n + 1$. By the previous theorem, there is a prime divisor of N. This must then equal p_i, for some $1 \leq i \leq n$. So $p_i \mid N$ but $p_i \mid p_1 p_2 \cdots p_n$ as well. So $p_i \mid 1$ because $1 = N - p_1 p_2 \cdots p_n$. This is a contradiction because p_i is a prime which means $p_i > 1$. □

Theorem If n is composite then n has a prime factor less than or equal to $\sqrt{n}$.

Proof. Suppose n is composite. So $n = ab$ where $1 < a < n$ and $1 < b < n$. We know one of a, b is $\leq \sqrt{n}$, otherwise $ab > \sqrt{n}\sqrt{n} = n$. Without loss of generality, suppose $a \leq \sqrt{n}$. We know a has a prime divisor p, so $p \mid a$. So $p \leq a \leq \sqrt{n}$. Since $p \mid a$ and $a \mid n$, we have that $p \mid n$. □

The last theorem is useful, because it theoretically reduces the amount of computation needed to check if a number is prime. That is, rather than dividing n by all numbers less than it, we only need to divide by numbers less than or equal to $\sqrt{n}$.

Suppose you started with the number 20 and added multiples of 7. In that resulting list of numbers, how many primes are there? It turns out that under certain conditions, there are infinitely many! This is stated in Dirichlet's Theorem on Arithmetic Progressions.
Theorem. Suppose $a, b \in \mathbb{Z}$ with gcd(a, b)=1. Then the sequence

$$a + b, a + 2b, a + 3b, \cdots$$

contains infinitely many primes. The proof for this is incredibly difficult and requires a deep understanding of algebra and analysis to prove it. (Well beyond the scope of this course. See this as the proof.)
Ex. Suppose $a = 20$ and $b = 7$. Then the sequence $27, 24, 41, 48, 55, 62, \cdots$ contains infinitely many primes.

3.2 The Distribution of Primes

We know there are infinitely many primes, but how are they distributed? Is there a formula for the n^{th} prime or do we have to go looking for it? Unfourtunately, there is no such formula. (If we knew a formula, then the idea of 'finding' the next largest prime would not be very interesting!)

Definition. Define $p_n = n^{th}$ prime. Let $\pi(x)$ be the number of primes $\leq x$ (note that x does not need to be an integer).
Ex. $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, etc...
Ex. $\pi(7) = \pi(8) = \pi(8.1) = 4$ because $2, 3, 5, 7$.

Prime Number Theorem. We have

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

Like Dirichlet's Theorem, the proof of this theorem is extremely difficult to understand and is even moreso beyond the scope of this course. In essence, the proof says that for *very* large x we have that $\pi(x) \approx \frac{x}{\ln(x)}$.
Corollary. If $p_n = n^{th}$ prime then

$$\lim_{n\to\infty} \frac{p_n}{n\ln(n)} = 1$$

The consequence is that for very large n, $p_n \approx n\ln(n)$. This tells us that the primes get more and more spread out as we move further down the number line.
Ex. The millionth prime is approximately $10^6 \cdot \ln(10^6) = 12,815,510.56$. In reality, the millionth prime is the number $15,485,863$. So we are not terribly far off from our approximation, relatively speaking.

So we have an idea of *how* the prime are distributed, but what about the gaps between them?
Gaps Between Primes. There are arbitrarily long sets of consecutive composite numbers. (That is, given any large enough gap desired, we can find a gap that big between consecutive primes.)

Proof. For any n, consider:

$$(n+1)! + 2, (n+1)! + 3, \cdots, (n+1)! + (n+1)$$

There are n numbers here. Observe that $(n+1)!+2$ is divisble by 2, so it is composite, $(n+1)!+3$ is divisble by 3, so it is composite... and so on, all the way up to $(n+1)!+(n+1)$ which is divisble by $(n+1)$ so it is composite! Therefore, we have a string of n consecutive composite numbers. □

Ex. If we need 6 consecutive composites, we have that

$$7! + 2, 7! + 3, \cdots, 7! + 7$$

is a string of 6 consecutive composites. Observe that this is nowhere near the most efficient way to find 6 consecutive composites (because factorials become large very quickly), but it works!

Conjectures Here are a few conjectures that are *believed* to be true but have not been proven yet.

- **Twin Prime Conjecture.** There are infinetely many twin primes (primes that differ by 2, think 3 and 5 or 5 and 7, etc...)
- **Goldbach Conjecture.** Every even integer greater than 2 can be written as the sum of two primes (not necessarily *distinct* primes). For example, $10 = 5+5$ or $12 = 5+7$, etc...
- **Legendre Conjecture.** There is a prime between the squares of any two consecutive integers. (This conjecture is relatively reasonable because the gaps between squares get larger as the numbers get larger.)

3.3 Greatest Common Divisors

Theorem. Suppose $d=\gcd(a,b)$. Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Theorem. $\gcd(a,b)=\gcd(a+\alpha b, b)$, with $\alpha \in \mathbb{Z}$ and $\gcd(a,b)=\gcd(a, b+\alpha a)$.
Ex. $\gcd(18,7)=\gcd(18, 7+42(18))$

Proof.

- Suppose c is a common divisor of a, b. So $c \mid a$ and $c \mid b$ so $c \mid a+\alpha b$. So c is a common divisor of $a+\alpha b, b$.
- Suppose c is a common divisor of $a+\alpha b, b$. So $c \mid a+\alpha b$ and $c \mid b$ so $c \mid (a+\alpha b) - \alpha(b)$ So $c \mid a$ so c is a common divisor of a, b.

So the pairs a, b and $a+\alpha b, b$ have the same common divisors, so they have the same gcd. □

Theorem. Let $a, b \in \mathbb{Z}$ not both 0. Then $\gcd(a,b)$ = smallest positive linear combination of a and b.
Ex. Look at $a = 15$, $b = 35$. $\gcd(15,35) = 5$ (we know this). Some linear combinations would be; $1(15)+1(35) = 50$, $2(15)-3(35) = -75$, $-2(15)+1(35) = 5$. The theorem shows that $-2(15)+1(35) = 5$ is the smallest positive linear combination.

Proof. Let $d = \alpha a+\beta b$ be the smallest positive linear combination of a, b ($\exists$ by well-ordering of $\mathbb{Z}^+$). Claim $d=\gcd(a,b)$. First lets show $d \mid a$ and $d \mid b$ *then* show it is the greatest. By the division algorithm $a = dq + r$ with $0 \le r < d$. So then $r = a - dq = a - (\alpha a + \beta b)q = (1-\alpha q)a - \beta q b$ which is a linear combination of a, b. So $r = 0$ so $a = dq$ so $d \mid a$. Likewise, $d \mid b$ (same argument).

So $d \mid a$ and $d \mid b$, but why is it greatest?

Suppose some $c \mid a$ and $c \mid b$. Then $c \mid \alpha a + \beta b = d$ so $c \leq d$ therefore d is the greatest! $\square$

This is important because when working with gcd we can express it *as* a linear combination to work with it!
Ex. If we're working with $\gcd(a, b)$, we can write: aha, $\exists \alpha, \beta$ such that $\gcd(a, b) = \alpha a + \beta b$. Then we work with $\alpha a + \beta b$ instead.
Corollary. If a, b are coprime then $\exists \alpha, \beta$ such that $1 = \alpha a + \beta b$.

Theorem. If $a, b \in \mathbb{Z}^+$ not both 0, then the set of linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

$$\{\alpha a + \beta b\} = \{\text{multiples of } \gcd(a, b)\}$$

Ex. gcd(35,15)=5. All linear combinations of $35, 15$ are multiples of 5 and all multiples of 5 are linear combinations.

Proof. Suppose $x = \alpha a + \beta b =$ linear combination of a, b. Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ then $\gcd(a, b) \mid \alpha a + \beta b = x$. Thus, $\{\alpha a + \beta b\} = \{\text{mult. of } \gcd(a, b)\}$.

Then consider a multiple of $c\gcd(a, b)$. Well $\gcd(a, b) = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. So $c\gcd(a, b) = \alpha c a + \beta c b =$ linear combinations of a, b. Thus $\{\text{mult. of } \gcd(a, b)\} \subset \{\text{linear combinations of } a, b\}$. $\square$

Theorem. Suppose $a, b \in \mathbb{Z}$ not both 0, suppose $d \in \mathbb{Z}^+$. Then $d = \gcd(a, b)$ if d has these two properties:

- $d \mid a$ and $d \mid b$.
- $c \mid a$ and $c \mid b$ then $c \mid d$.

Proof.
$\rightarrow$ Suppose $d = \gcd(a, b)$. Obviously this meets the first property because d is a common divisor. To show the second property, suppose $c \mid a$ and $c \mid b$. Well $d = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$ so $c \mid a, c \mid b \implies c \mid d$.

$\leftarrow$ Suppose d satisfies the two properties, since $d \mid a$ and $d \mid b$, it is a common divisor. But why is it the greatest? Well if c is a common divisor (positive) then since $c \mid a$ and $c \mid b$ by property 2 $c \mid d$. So $c \leq d$. Thus $d = \gcd(a, b)$. $\square$

If we know $\gcd(a, b) = 20$, then not only are other positive common divisors smaller, but they are only $1, 2, 4, 5, 10$ that's it!

3.4 The Euclidean Algorithm

The goal of this section is to talk about the Euclidean Algorithm from a computational perspective and see what it can be used for. It is not theoretically significant, but it is a useful tool. Suppose $a, b \in \mathbb{Z}$, not both zero. Two things we would like to do are (1) calculate $\gcd(a, b)$ and (2) find α, β such that $\gcd(a, b) = \alpha a + \beta b$. Both of these can be accomplished using the Euclidean Algorithm!

Recall we saw that $\gcd(a, b) = gcd(a + \alpha b, b)$. That is, we can $\pm$ any multiple of one to the other and the gcd does not change. Suppose $a > b$. We know by the Division Algorithm that $a = qb + r$ where $0 \leq r < b$. Then $r = a - qb$, which means

$$\gcd(a, b) = \gcd(a - qb, b) = \gcd(r, b)$$

Thus, we can replace the larger of a and b by the remainder we get when we divide by the smaller. When we do this, wthe roles of the larger and smaller switch. We repeat this until we get the desired result.
Ex. Suppose we want gcd(252,198). Well,

$$252 = (1)198 + 54$$

So gcd(252,198)=gcd(54,198). Again,

$$198 = (3)54 + 36$$

So gcd(252,198)=gcd(54,198)=gcd(54,36). Again,

$$54 = (1)36 + 18$$

So gcd(252,198)=gcd(54,198)=gcd(54,36)=gcd(36,18). Again,

$$36 = (2)18 + 0$$

So gcd(252,198)=gcd(54,198)=gcd(54,36)=gcd(36,18)=gcd(18,0)=18.
Therefore, gcd(252,198)=18.

In practice, we can do this by repeated replacements of our division algorith,s (without writing the gcd's at each step). The last nonzero remainder is our gcd.
Ex. To find gcd(97,44), we do the following.

$$\begin{aligned} 97 &= (2)44 + 9 \\ 44 &= (4)9 + 8 \\ 9 &= (1)8 + 1 \\ 8 &= (1)8 + 0 \end{aligned}$$

So the gcd is 1.

Now, to find a linear combination, we use these successive divisions from the final gcd up to get the linear combination. We do this by replacing remainders. Keep track carefully!
Ex. For $a = 252$ and $b = 198$, we know that

$$\begin{aligned} 252 &= (1)198 + 54 \\ 198 &= (3)54 + 36 \\ 54 &= (1)36 + 18 \\ 36 &= (2)18 + 0 \end{aligned}$$

So we start with the last nonzero remainder, which in this case is 18. We know, from the second equation that

$$\begin{aligned} 18 &= 1(54) - 1(36) \\ &= 1(54) - (198 - (3)54) \\ &= 4(54) - (1)198 \\ &= 4(252 - (1)198) - (1)198 \\ &= 4(252) - 5(198) \\ &= \alpha a + \beta b \end{aligned}$$

where $\alpha = 4$ and $\beta = -5$.

3.5 Fundamental Theorem of Arithmetic

We want to work our way up to proving the Fundamental Theorem of Arithmetic. To prove this, we will need a few lemmas.

Lemma. Suppose $a, b, c \in \mathbb{Z}^+$ with $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

Proof. First write $1 = \alpha a + \beta b$ with $\alpha, \beta \in \mathbb{Z}$. Then $c = \alpha ac + \beta bc$. We know that $a \mid \alpha ac$ and $a \mid \beta bc$. So $a \mid \alpha ac + \beta bc$ so $a \mid c$. □

Note, in general, $a \mid bc$ does not imply $a \mid b$ or $a \mid c$!

Euclid's Lemma. Suppose p is prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$ (or both).

Proof. If $p \mid a$ we are done. If $p \nmid a$ then $\gcd(p, a) = 1$, so $p \mid b$ by the above lemma. □

In more abstract settings (in MATH 403, for example) this is the definition of what an abstract object means to be prime!

Euclid's Lemma (General). Suppose p is prime. If $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some i.

Proof. Induction! □

Fundamental Theorem of Arithmetic. For $n \in \mathbb{Z}$ where $n \geq 2$. We can write n uniquely as a product of primes where "uniquely" means up to the ordering. (That is, $45 = 3 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 3 = 5 \cdot 3 \cdot 3$ are considered identical.) The 'unique' part of this theorem is not to be taken for granted. In abstract algebra, many objects' objects can be factored into what are called 'irreducibles' but it will not always be the case that this factorization is unique!

Proof. First, we need to show that for any $n \in \mathbb{Z}^+$ where $n \geq 2$ that n can be written as a product of primes. By way of contradiction, suppose there exists integers ≥ 2 which cannot be written as the product of primes. Let n be the smallest of such numbers, which exists by well-ordering. Is n itself prime? If so, then

$$n = \text{itself} = \text{product of itself} = \text{product of prime(s)}$$

which is a contradiction! If n is not prime, then $n = ab$ where $1 < a < n$ and $1 < b < n$. But since $a, b < n$, they are products of primes. But then n can also be expressed as a product of primes, another contradiction.

What remains to be shown is that there is a *unique* prime factorization. Suppose not. That is, suppose

$$n = p_1 p_2 \cdot p_k = q_1 q_2 \cdots q_j$$

Let us assume we have cancelled all common primes between the p and q set. Thus $p_i \neq q_l$ for all i, l. Since $p_1, \cdots, p_k = q_1, \cdots q_j$, we know $p_1 \mid q_1 \cdots q_j$. Thus, by the lemma, $p_1 \mid q_i$ for some i. But $p_1 \neq q_i$ and $p_1 \neq 1$. This is a contradiction! ☐

We have several consequences of the Fundamental Theorem of Arithmetic.

Related to division:

We know $20 \mid 80$ in terms of primes $2^2 \cdot 5 \mid 2^4 \cdot 5$. In $\gcd(a, b)$, for any p^α appearing in a, there must be a p^β with $\beta \geq \alpha$ in b.
Theorem. For $a, b \in \mathbb{Z}$ with $a, b \geq 2$. Then $a \mid b$ if and only if, whenever p^α appears in the PF of a, p^β with $\beta \geq \alpha$ appears in the PF of b.

Proof.
$\leftarrow$ Suppose a, b have the property that whenever p^α appears in the prime factorization of a, then p^β, where $\beta \geq \alpha$ appears in the prime factorization of b. Then,

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} \cdots p_k^{\beta_k} p_{k+1} \cdots p_j$$

where $\beta_i \geq \alpha_i$ for all i. Then

$$b = \underbrace{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}_{=a} \underbrace{p_1^{\beta_1 - \alpha_1} \cdots p_k^{\beta_k - \alpha_k} p_{k+1} \cdots p_j}_{=m}$$

Therefore, $b = am$ for some $m \in \mathbb{Z}$. So $a \mid b$.

$\rightarrow$ By contradiction, assume $a \mid b$ and p^α appears in PF of a and p^β appears (or not) in PF of b with $0 \leq \beta < \alpha$. Since p^α appears in PF of a we can write

$$a = p^\alpha A \text{ where } A = \text{all the rest}$$

$$b = p^\beta B \text{ where } B = \text{all the rest}$$

Since $a \mid b, \exists c$ such that $ac = b$. It follows

$$p^\alpha Ac = p^\beta B$$

$$p^{\alpha-\beta} Ac = B, \qquad \alpha - \beta > 0$$

p appears on the left (in PF of left side) hence it must be in the PF of right side (because they're the same number). But $p \nmid B$ which is a contradiction. ☐

Related to Factors:

Theorem. The positive divisors of some $n \geq 2$ can all be constructed by taking the primes which appear in the PF of n to at most *those* powers.

Proof. Follows from the previous theorem. □

Ex. Find all factors of $2^3 5^2 7$. Factors all have the form $2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}$ with $0 \leq \alpha_1 \leq 3$, $0 \leq \alpha_2 \leq 2$, $0 \leq \alpha_3 \leq 1$. Thus there are $(4)(3)(2) = 24$ factors!

Related to GCD:

Theorem. The gcd of two numbers a, b can be found by taking the set of primes which appear in both a and b (intersection) to the power which is the minimum of the two powers.
Ex. $\gcd(2^3 \cdot 7^4 \cdot 11, 2^2 \cdot 7^5 \cdot 13) = 2^2 \cdot 7^4$

Related to LCM:

The *least common multiple* is the smallest integer which both a and b are factors of. $\text{lcm}(20, 30) = 60$.
Theorem. The lcm of two numbers a, b can be found by taking the set of primes which appear in either a and b (union) to the power which is the maximum of the two powers.
Ex. $\text{lcm}(2^3 \cdot 7^4 \cdot 11, 2^2 \cdot 7^5 \cdot 13) = 2^3 \cdot 7^5 \cdot 11 \cdot 13$

Together:

Theorem. We have $ab = \gcd(a, b)\text{lcm}(a, b)$.

Proof. Follows immediately. □

So $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$ and $\gcd(a, b) = \frac{ab}{\text{lcm}(a,b)}$.

Theorem. Suppose $n_1, n_2 \in \mathbb{Z}$ with $\gcd(n_1, n_2) = 1$. Suppose $d \mid n_1 n_2$, then $d = d_1 d_2$ where $\gcd(d_1, d_2) = 1$ and $d_1 \mid n_1$ and $d_2 \mid n_2$.

Proof. $d_1 =$ all primes in d which appear in n_1 (not n_2). Likewise, $d_2 =$ all primes in d which appear in n_2 (not n_1). □

3.6 Problems

---

1. Use the Euclidean Algorithm to calculate $d = \gcd(510, 140)$ and then use the result to find α and β so that $d = 510\alpha + 140\beta$.
2. Use the Euclidean Algorithm to show that if $k \in \mathbb{Z}^+$ that $3k + 2$ and $5k + 3$ are relatively prime.
3. How many zeros are there at the end of (1000!)? Do not do this by brute force. Explain your method.

4. Let $a = 1038180$ and $b = 92950$. First find the prime factorizations of a and b. Then use these to calculate $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

5. Which pairs of integers have gcd of 18 and lcm of 540? Explain.

6. Suppose that $a \in \mathbb{Z}$ is a perfect square divisible by at least two distinct primes. Show that a has at least seven distinct factors.

7. Show that if $a, b \in \mathbb{Z}^+$ with $a^3 \big| b^2$ then $a \big| b$.

8. For which positive integers m is each of the following statements true:

   (a) $34 \equiv 10 \mod m$

   (b) $1000 \equiv 1 \mod m$

   (c) $100 \equiv 0 \mod m$

4 Congruences

4.1 Introduction to Congruences

---

1. **Introduction:** Suppose you wished to find $x, y \in \mathbb{Z}$ satisfying $2x^2 - 8y = 11$. There is no solution because no matter what, $2x^2 - 8y$ is even and 11 is odd. What if even/odd does not work... what else might? $3x^2 - 15y = 8$, 3 divides the left side but not the right. If even/odd or divided by 3 works, there is no guarantee that it works $\underbrace{3x^2 - 15y = 9}_{\text{might work}}$.

   The idea of modular arithmetic formalizes all of this.

2. **Definition and Equivalencies:** For $a, b, m \in \mathbb{Z}$ with $m \geq 2$ we write $a \equiv b \bmod m$ which is read as "a and b are congruent modulo m." to mean that $m \mid (a - b)$. A few notes on this,

   - Equivalent to saying $m \mid (b - a)$.
   - Equivalent to saying $\exists c \in \mathbb{Z}$ such that $mc = a - b$ or $\exists x \in \mathbb{Z}$ such that $mc = b - a$ (definition of divisibility).
   - Equivalent to saying that if we divide a and b by m, the remainders are the same.

   Ex. $8 \equiv 18 \bmod 5$ in fact $8 \equiv 18 \equiv 3 \equiv -2 \equiv 23 \equiv \cdots \bmod 5$. Here with remainder 3. Also note $5 \mid (18 - 8)$ and $5 \mid (8 - 18)$.

   Even/odd is the same as $m = 2$.

   CS Note. In computer science we often define $\text{mod}(a, m) =$ remainder when $a/m = a\%m$. It is not uncommon to see $a = b \bmod m$ or $a \equiv_m b$ (strongly discouraged).

   Moving forward, please use $a \equiv b \bmod m$.

3. **Properties:**

   (a) **Theorem.** Congruence acts like an equals sign in the following sense:

   (i) $a \equiv a \bmod m$ (Reflexive).

   (ii) if $a \equiv b \bmod m$ then $b \equiv a \bmod m$ (Symmetric).

   (iii) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$ (Transitivity).

   Proof. $a \equiv b \bmod m \implies \exists x$ such that $a - b = mx$, $b \equiv c \bmod m \implies \exists y$ such that $b - c = my$. Then $a - c = (a - b) + (b - c) = mx + my = m(x + y)$ so $m \mid (a - c)$ so $a \equiv c \bmod m$. $\square$

   (iv) If $a \equiv b \bmod m$ and $c \equiv \bmod m$ then $a \pm c \equiv b \pm d \bmod m$.

   i.e. If we know $x \equiv y \bmod 5$ we can conclude $x + 7 \equiv y + 7 \bmod 5$ and also $x + 7 \equiv y + 12 \bmod 5$.

   (v) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$

   i.e. If we know $x \equiv y \bmod 5$ then we can conclude $17x \equiv 17y \bmod 5$ but we can also conclude $17x \equiv 12y \bmod 5$

(vi) If $a \equiv b \bmod m$ and $k \in \mathbb{Z}, k \geq 1$ then $a^k \equiv b^k \bmod m$. (Note: we can *not* use different powers!)

(b) **Division Issues.** First everything must be an integer, so does $2 \equiv 8 \bmod 6 \implies \frac{2}{3} \equiv \frac{8}{3} \bmod 6$ this is garbage because $\frac{2}{3}, \frac{8}{3} \notin \mathbb{Z}$. However, is $2 \equiv 8 \bmod 6 \implies \frac{2}{2} \equiv \frac{8}{2} \bmod 6$ true? No! because $1 \equiv 4 \bmod 6$ is not true. The point is even if division makes both sides integers there is no guarantee that the congruence is preserved!

Theorem. Suppose we have $ac \equiv bc \bmod m$ then $a \equiv b \bmod m/\gcd(m, c)$. In other words we may cancel an integer from both sides provided we divide the modulus by the gcd of the modulus and the integer we're canceling.

Proof. Suppose $ac \equiv bc \bmod m$, $\exists k \in \mathbb{Z}$ with $mk = ac - bc$. So $mk = c(b - a)$,

$$\frac{m}{\gcd(c, m)} k = \frac{c}{\gcd(c, m)} (a - b)$$

Note that from a previous theorem we know that:

$$\gcd\left(\frac{m}{\gcd(c, m)}, \frac{c}{\gcd(c, m)}\right) = 1$$

Then the above statement says that $\frac{m}{\gcd(c,m)} \Big| \frac{c}{\gcd(c,m)}(a-b)$ which implies $\frac{m}{\gcd(c,m)} \Big| a - b$. Therefore, $a \equiv b \bmod \frac{m}{\gcd(c,m)}$. $\square$

Note. Don't think division, think cancelation when dealing with modulo.
Ex. If we know that $4x \equiv 8y \bmod 50$ then we can conclude that $x \equiv 2y \bmod 50/\gcd(50, 4)$ and so $x \equiv 2y \bmod 25$ (think *cancel* the 4).
Corollary. If $ac \equiv bc \bmod m$ and $\gcd(c, m) = 1$ then $a \equiv b \bmod m$.
Ex. $15x \equiv 20y \bmod 27$, note that $\gcd(5, 27) = 1$ so we may cancel the 5. So $3x \equiv 4y \bmod 27$.

4. **Residue Classes:**

(a) **Introduction:** Suppose we are working $\bmod m = 5$. We know $0 \equiv 5 \equiv 10 \equiv -5 \equiv \cdots \bmod 5$, we also know $1 \equiv 6 \equiv 11 \equiv -4 \equiv \cdots \bmod 5$, all of $\mathbb{Z}$ fall into one out of $m = 5$ classes.

$$\{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$$
$$\{\cdots, -16, -9, -4, 1, 6, 11, 16, \cdots\}$$
$$\{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$$
$$\{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$$
$$\{\cdots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

(b) **Definition.** For a given $m \geq 2$ there are m congruence classes.

(c) **Definition.** From each we may pick a representative of the class so those would be m representatives.
Ex. $m = 5 : \{0, 1, 2, 3, 4\}$ (the obvious one) or you could use $m = 5 : \{0, 2, 4, 6, 8\}$ (all even) or $m = 5 : \{0, 2, 4, 8, 16\}$ (all powers of 2, except 0).
Ex. $m = 5 : \{0, 1, 2, 3, 4\}$ (the obvious one) or you could use $m = 5 : \{0, 2, 4, 6, 8\}$ (all even) or $m = 5 : \{0, 2, 4, 8, 16\}$ (all powers of 2, except 0).

(d) **Definition.** The set of representatives $\{0, \cdots, m-1\}$ = the complete set of least non-negative residues.

In $\mathbb{R}$, $17^x = 48246319 \implies x = \log_1 7(48246319)$. Now consider $\mathbb{Z}$ mod 100, $6^x \equiv 88 \bmod 100$ is *significantly* harder to solve (the discrete logarithm problem).

(e) **Definition.** A complete set of residues (CSOR) mod m is a set of m integers, no two of which are congruent mod m.
Ex. $m = 5$: here are 3 CSORs: $\{0, 1, 2, 3, 4\}$, $\{0, 2, 4, 6, 8\}$, $\{0, 2, 4, 8, 16\}$, and more!

(f) **Theorem.** A subset S of $\mathbb{Z}$ is a CSOR mod m if and only if every integer is congruent to exactly one element in S.
Ex. $m = 4$: $S = \{0, 9, 14, 3\}$ some observations:

- $m = 4$ of them.
- No two are congruent to each other.
- Any $a \in \mathbb{Z}$ is congruent to exactly one of these.

(g) **Theorem.** If $\{r_1, r_2, \cdots, r_m\}$ is a CSOR mod m and if $a, b \in \mathbb{Z}$ with $\gcd(a, m) = 1$ then $\{ar_1 + b, ar_2 + b, \cdots, ar_m + b\}$ if also a CSOR mod m.

Proof. We will show that no two are congruent mod m. Suppose $ar_i + b \equiv ar_j + b \bmod m$ with $i \neq j$. Then $ar_i \equiv ar_j \bmod m \implies r_i \equiv r_j \bmod m$ because $\gcd(a, m) = 1$. Contradiction because the r_i, r_j came from a CSOR mod m. ☐

Ex. $\{0, 1, 2, 3, 4\}$ CSOR mod 5. Pick $a = 9, b = 42$, $\{0 \cdot 9 + 42, 1 \cdot 9 + 42, 2 \cdot 9 + 42, 3 \cdot 9 + 42, 4 \cdot 9 + 42\}$ is also a CSOR mod 5.

5. **Fast Arithmetic - Fast Exponentiation.** Suppose we wished to calculate $2^{503} \equiv a \bmod 5$, $a = 0, 1, 2, 3, 4$ but which one? Warning: Do not reduce exponent mod 5! $2^{503} \equiv 2^x \bmod 5$.

(a) Look for patterns: $2^1 \equiv 2 \bmod 5$, $2^2 \equiv 4 \bmod 5$, $2^3 \equiv 3 \bmod 5$, $2^4 \equiv 1 \bmod 5$, $2^5 \equiv 2 \bmod 5$. This last one is a repeat, so it repeats every 4. Note $503 = 4(125) + 3$ so

$$\begin{aligned} 2^{503} &\equiv 2^{4(503)} 2^3 \\ &\equiv (1)^{125} 2^3 \bmod 5 \\ &\equiv (1)8 \bmod 5 \\ &\equiv 3 \bmod 5 \end{aligned}$$

(b) Use binary expansions. Suppose we want $3^{81} \equiv a \bmod 5$. $3^1 \equiv 3$, $3^2 \equiv 4$, $3^4 \equiv 1$, $3^8 \equiv 1$, $3^{16} \equiv 1$, $3^{32} \equiv 1$, $3^{64} \equiv 1$. Then $81 = 64 + 16 + 1$ so

$$\begin{aligned} 3^{81} &= 3^{64} 3^{16} 3^1 \\ &\equiv 1 \cdot 1 \cdot 3 \\ &\equiv 3 \bmod 5 \end{aligned}$$

4.2 Solving Linear Congruences

---

1. **Introduction:** The idea is that we would ideally like to solve "equations" like $3x^2 + x \equiv 5 \bmod 72$, $8^x \equiv 12 \bmod 5$, etc... So let's go back to basics.
   Definition: A linear congruence has the form $ax \equiv b \bmod m$. We would like to find all possible solutions, whatever that means.
   Process:
   (a) Do solutions exist?
   (b) If so, can we find just one?
   (c) Can we find more?
   (d) When are they "different"

2. **Do Solutions Exist:** To say that $ax \equiv b \bmod m$ has a solution means, $\exists x$ such that $ax \equiv b \bmod m$ which in turn means $\exists x, \exists y$ such that $ax + my = b$ ($ax \equiv b \bmod m \implies m \mid (ax - b) \implies my = ax - b \implies ax - my = b$). This means that b is a linear combination of a, m.
   Recall: $\{$Linear combination of $a, m\} = \{$ multiples of $\gcd(a, m)\}$.
   Thus, b is a linear combination of a, m when b =multiple of $\gcd(a, m)$, so $ax \equiv b \bmod m$ has solution(s) if and only if $\gcd(a, m) \mid b$.
   Ex. $2x \equiv 8 \bmod 18$ has solutions, because gcd(2,18)=2 | 8.
   $6x \equiv 8 \bmod 36$ does not, because gcd(6,36)=6 $\nmid$ 8.

3. **Finding One Solution:** We would like to solve $ax + my = b$, with b as a multiple of $\gcd(a, m)$. Well, we can solve $ax' + my' = \gcd(a, m)$! But how? With the Euclidean Algorithm. Use the Euclidean Algorithm to solve $ax' + my' = \gcd(a, m)$ then multiple both sides to get b on the right.
   Ex. Consider $4x \equiv 6 \bmod 50$. We have gcd(4,50)=2 | 6 so solutions exist. First we use the Euclidean Algorithm to solve:

$$4x' + 50y' = 2$$

   This gives us $4\underbrace{(-12)}_{x'}+50\underbrace{(1)}_{y'} = 2$, we want to get a 6 on the right hand side so multiple by 3. So then we get $4\underbrace{(-36)}_{x}+50\underbrace{(3)}_{y} = 6$, so $4(-36) \equiv 6 \bmod 50$. Typically, we will use the least non-negative residue (add until you get a non-negative). So here the solution is $x_0 = (-36) + 50 = 14$.

4. **Finding All Solutions:** Suppose we have our one solution, $x_0 \implies ax_0 \equiv b \bmod m$. Suppose now x is another, this implies $ax \equiv b \bmod m$. So we subtract the second from the first

$$\begin{aligned} a(x) - a(x_0) &\equiv b - b \bmod m \\ a(x - x_0) &\equiv 0 \bmod m \\ x - x_0 &\equiv 0 \bmod \frac{m}{\gcd(a, m)} \end{aligned}$$

So,

$$x = x_0 + k\left(\frac{m}{\gcd(a,m)}\right)$$

Warning! Solutions must look like this but are all things which look like this actually solutions?

We would like $ax \equiv b \bmod m$.

$$\begin{aligned}
ax &\equiv a\left(x_0 + k\left(\frac{m}{\gcd(a,m)}\right)\right) \bmod m \\
ax &\equiv \underbrace{ax_0}_{b} + \underbrace{k\left(\frac{m}{\gcd(a,m)}\right)}_{\text{lcm}} \bmod m \\
ax &\equiv b + k\text{lcm}(a,m) \bmod m \\
ax &\equiv b \bmod m
\end{aligned}$$

Therefore all solutons can be gained by doing, $x = x_0 + k\left(\frac{m}{\gcd(a,m)}\right), \forall k \in \mathbb{Z}$.

Lastly, when are they unique mod m?
Consider that two of them with k_1 and k_2 are identical mod m when:

$$\begin{aligned}
x_0 + k_1\left(\frac{m}{\gcd(a,m)}\right) &\equiv x_0 + k_2\left(\frac{m}{\gcd(a,m)}\right) \bmod m \\
k_1\left(\frac{m}{\gcd(a,m)}\right) &\equiv k_2\left(\frac{m}{\gcd(a,m)}\right) \bmod m \\
k_1 &\equiv k_2 \bmod \frac{m}{m/\gcd(a,m)} \\
k_1 &\equiv k_2 \bmod \gcd(a,m)
\end{aligned}$$

Therefore, it follows that solutions will be congruent mod m when k-values are congruent mod $\gcd(a,m)$. So solutions are not congruent mod m by ensuring that the k-values are not congruent mod $\gcd(a,m)$. This can be done using $k = 0, 1, 2, \cdots, \gcd(a,m) - 1$.

5. **Summary Theorem:** The linear congruence $ax \equiv b \bmod m$ has solutions if and only if $\gcd(a,m) \mid b$. If it has solutions then it has $\gcd(a,m)$ unique solutions mod m. If x_0 is one of those then all are

$$x = x_0 + k \cdot \frac{m}{\gcd(a,m)}, \text{ for } k = 0, 1, 2, \cdots, \gcd(a,m) - 1$$

Ex. $20x \equiv 15 \bmod 65$, gcd(20,65)=5 $\mid$ 15 so $\exists 5$ incongruent solutions mod 65. The Euclidean Algorithm gives us a solution $x_0 \equiv 56 \bmod 65$. So all solutions are then

$$x \equiv 56 + k \cdot \frac{65}{\gcd(20,65)} \bmod m, \text{ for } k = 0, 1, 2, 3, 4$$

$$x \equiv 56 + 13k \bmod 65, k = 0, 1, 2, 3, 4$$

That is $x \equiv 56, 4, 17, 30, 43 \bmod 65$.

Note: If $\gcd(a,m) = 1$ there exists only one solution mod m.

4.3 The Chinese Remainder Theorem

---

1. **Introduction:** How can we solve systems of linear congruences? For example, suppose we wished to find x satisfying all of these:

$$\begin{aligned} x &\equiv 2 \mod 6 \\ x &\equiv 4 \mod 7 \\ x &\equiv 3 \mod 25 \end{aligned}$$

Is it always possible to find a solution to something like this? No! However, under certain circumstances, yes!

2. **Chinese Remainder Theorem:** Suppose we have a system of the form

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}$$

If all the m_i are pairwise coprime (so $\gcd(m_i, m_j) = 1, \forall i, j$), then $\exists!$ solution mod $M = m_1 m_2 \cdots m_n$. So for our example, since $6, 7, 25$ are all pairwise coprime, $\exists!$ solution mod $(6)(7)(25) = 1050$.

Proof. For each i define $M_i = M/m_i$, then consider the equation:

$$M_i y_i \equiv 1 \mod m_i$$

Note that $\gcd(M_i, m_i) = 1$ [1]. because the m_i are all coprime. Since $\gcd(M_i, m_i) = 1 \mid 1, \exists!$ solution mod m_i. Let y_i be that solution. Take all y_i and construct the integer:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

Claim that this is a solution to the system. Pick some i and observe that

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \mod m_i \\ &\equiv 0 + 0 + \cdots + a_i M_i y_i + \cdots + 0 \mod m_i \\ &(\text{because } M_i \equiv 0 \mod m_i \text{ when } j \neq i) \\ x &\equiv a_i(1) \mod m_i \\ x &\equiv a_i \mod m_i \end{aligned}$$

Claim x is unique mod M. Suppose x_1, x_2 are both solutions to the original system.

$$x_1 \equiv a_1 \mod m_1 \text{ and } x_2 \equiv a_1 \mod m_1$$

$$\vdots$$

[1] Recall: $ax \equiv b \mod m$ solutions if and only if $\gcd(a, m) | b \; \exists \gcd(a, m)$ solutions.

$$x_1 \equiv a_n \mod m_n \text{ and } x_2 \equiv a_n \mod m_n$$

From here we get,

$$\begin{aligned}
x_1 \equiv x_2 \mod m_1 &\implies m_1 \mid (x_1 - x_2) \\
x_1 \equiv x_2 \mod m_2 &\implies m_2 \mid (x_1 - x_2) \\
&\vdots \\
x_1 \equiv x_2 \mod m_n &\implies m_n \mid (x_1 - x_2)
\end{aligned}$$

Since the m_i are all pairwise coprime, we get

$$m_1 m_2 \cdots m_n \mid (x_1 - x_2)$$

Thus, $x_1 \equiv x_2 \mod M$. □

3. **Example:** Take a look at

$$\begin{aligned}
x &\equiv 2 \mod 6 \\
x &\equiv 4 \mod 7 \\
x &\equiv 3 \mod 25
\end{aligned}$$

This means that $M = (6)(7)(25) = 1050$ and that $M_1 = \frac{1050}{6} = 175$, $M_2 = \frac{1050}{7} = 150$, $M_3 = \frac{1050}{25} = 42$.

Solve for y_1:

$$\begin{aligned}
M_1 y_1 &\equiv 1 \mod m_1 \\
175 y_1 &\equiv 1 \mod 6 \\
1 y_1 &\equiv 1 \mod 6 \\
y_1 &= 1
\end{aligned}$$

Solve y_2:

$$\begin{aligned}
M_2 y_2 &\equiv 1 \mod m_2 \\
150 y_2 &\equiv 1 \mod 7 \\
3 y_2 &\equiv 1 \mod 7 \\
y_2 &\equiv 5 \mod 7 \\
y_2 &= 5
\end{aligned}$$

Solve y_3:

$$\begin{aligned}
M_3 y_3 &\equiv 1 \mod m_3 \\
42 y_3 &\equiv 1 \mod 25 \\
17 y_3 &\equiv 1 \mod 25 \\
y_3 &\equiv 3 \mod 25 \\
y_3 &= 3
\end{aligned}$$

Now for the solution,

$$\begin{aligned}
&x \equiv (2)(175)(1) + (4)(150)(5) + (3)(42)(3) \mod 1050 \\
&x \equiv 3728 \equiv 578 \mod 1050
\end{aligned}$$

4.4 Factoring Using Pollard's Rho Method

---

1. **Introduction:** John Pollard invented the Rho factorization algorithm in 1975. It does a fairly fast job for numbers with small prime factors, even if those numbers themsevles are large, it also has a small memory footprint. So it is a useful tool for inital probing.

2. **Idea:** We have some n and wish to find a factor. Suppose p is a prime factor of n. The Goal is to look at a sequence of integers $x_0, x_1, x_2, \ldots$ until we find two x_i and x_j with the properties that: $x_i \not\equiv x_j \bmod n$ and $x_i \equiv x_j \bmod p$. Suppose then, that somehow we obtain such x_i and x_j. Then observe $p \mid (x_j - x_i)$ and $p \mid n$, so then $\gcd(x_j - x_i, n) \geq p$. Note: we can calculate the gcd easily via the Euclidean Algorithm.

   So the idea will be to generate a sequence $x_0, x_1, x_2, \ldots$ and then check $\gcd(x_j - x_i, n)$ but to do this in a way which is systematic and guarantees that eventually we will get $\gcd(x_j - x_i, n) \neq 1$ which will then give us a factor. Suppose we are given $x_0, x_1, x_2, \ldots$ if we consider these mod p, eventually they repeat since there are only p distinct values mod p. Once they repeat, they keep repeating. In other words, if $\alpha, \beta \geq i$ then $x_\alpha \equiv x_\beta \bmod p$ if and only if $(i-j) \mid (\alpha - \beta)$.

   Suppose s is the smallest multiple of $(j-i)$ which is larger than i. Observe that since $s, 2s \geq i$ and $(j-i) \mid s$, we have $(j-i) \mid (2s - s)$ and so $x_{2s} \equiv x_s \bmod p$. So instead of checking all combinations of x_i and x_j, we will just check x_{2s} and x_s when possible.

3. **Pollard's Rho Method:** Generate our $x_0, x_1, x_2, \ldots$ as follows: Let x_0 be some starting value, say $x_0 = 2$. Define $f(x) = x^2 + 1$ and put $x_1 = f(x_0) \bmod n$ (so $x_1 \equiv x_0^2 + 1 \bmod n$). This function creates a pseudorandom sequence of integers mod n. Everytime we calculate x_{2s} (even subscript) check $\gcd(x_{2s} - x_s, n)$. Eventually, we will get the gcd to be not equal to 1.

   Thus: The assumption that n has a "small" factor p, $p \mid n$, suggests that $x_i \equiv x_j \bmod p$ fairly quickly which then suggests that $\gcd(x_{2s} - x_s, n) \neq 1$ also fairly quickly.

   Ex. Let $n = 1111$, then set $x_0 = 2$ and $f(x) = x^2 + 1$. Then we have,

   $$x_1 \equiv 2^2 + 1 \equiv 5 \bmod 1111$$
   $$x_2 \equiv 5^2 + 1 \equiv 26 \bmod 1111 \implies \gcd(x_2 - x_1, n) = \gcd(21, 1111) = 1$$
   $$x_3 \equiv 26^2 + 1 \equiv 677 \bmod 1111$$
   $$x_4 \equiv 677^2 + 1 \equiv 598 \bmod 1111 \implies \gcd(x_4 - x_2, n) = \gcd(572, 1111) = 11$$

   So we get 11 as a factor of 1111 (no surprise there).

Ex. Let $n = 1189$, then set $x_0 = 2$ and $f(x) = x^2 + 1$. Then we have,

$$\begin{aligned}
x_1 &\equiv 5 \\
x_2 &\equiv 26 \implies \gcd(26-5, 1189) = 1 \\
x_3 &\equiv 677 \\
x_4 &\equiv 565 \implies \gcd(565-26, 1189) = 1 \\
x_5 &\equiv 574 \\
x_6 &\equiv 124 \implies \gcd(124-677, 1189) = 1 \\
x_7 &\equiv 1109 \\
x_8 &\equiv 456 \implies \gcd(456-565, 1189) = 1 \\
x_9 &\equiv 1051 \\
x_{10} &\equiv 21 \implies \gcd(21-574, 1189) = 1 \\
x_{11} &\equiv 442 \\
x_{12} &\equiv 369 \implies \gcd(369-124, 1189) = 1 \\
x_{13} &\equiv 616 \\
x_{14} &\equiv 166 \implies \gcd(166-1109, 1189) = 41
\end{aligned}$$

So we get 41 as a factor of 1189.

4.5 Problems

---

1. Calculate the least positive residues modulo 47 of each of the following with justification:
   (a) 2^{543}
   (b) 32^{932}
   (c) $46^{327349287323}$
2. Exhibit a complete set of residues mod 17 composed entirely of multiples of 3.
3. Show that if $a, b, m \in \mathbb{Z}$ with $m > 0$ and if $a \equiv b \mod m$ then $\gcd(a, m) = \gcd(b, m)$.
4. Suppose p is prime and $x \in \mathbb{Z}$ satisfies $x^2 \equiv x \mod p$. Prove that $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$. Show with a counterexample that this fails if p is not prime.
5. Show that if n is an odd positive integer or if n is a positive integer divisible by 4 that:
   $$1^3 + 2^3 + ... + (n-1)^3 \equiv 0 \mod n$$
6. Find all solutions (mod the given value) to each of the following.
   (a) $10x \equiv 25 \mod 75$
   (b) $9x \equiv 8 \mod 12$
7. Solve each of the following linear congruences using inverses.

(a) $3x \equiv 5 \mod 17$

(b) $10x \equiv 3 \mod 11$

8. What could the prime factorization of m look like so that $6x \equiv 10 \mod m$ has at least one solution? Explain.

9. Use the Chinese Remainder Theorem to solve:
A troop of monkeys has a store of bananas. When they arrange them into 7 piles, none remain. When they arrange them into 10 piles there are 3 left over. When they arrange them into 11 piles there are 2 left over. What is the smallest positive number of bananas they can have? What is the second smallest positive number?

10. Solve the system of linear congruences:

$$\begin{aligned} 2x+1 &\equiv 3 \mod 10 \\ x+2 &\equiv 7 \mod 9 \\ 4x &\equiv 1 \mod 7 \end{aligned}$$

6 Special Congruences

6.1 Wilson's Theorem & Fermat's Little Theorem

---

1. **Wilson's Theorem:** If p is prime then

$$(p-1)! \equiv -1 \mod p$$

Proof. The case where $p = 2$ is trivial to show, so let's look at primes $p \geq 3$. Consider the set of numbers $\underbrace{\{1, 2, 3, 4, 5, \cdots, p-1\}}_{\text{even number of integers}}$. Suppose a is one of these, then $\exists b \in \mathbb{Z}$ such that $ab \equiv 1 \mod p$ (a multiplicative inverse). Because the equation $ax \equiv 1 \mod p$ has one solution because $\gcd(a, p) = 1 \mid 1$. Note that $\gcd(a, p) = 1$ because a is one of $\{1, 2, 3, \cdots, p-1\}$.
Could we have, for some $a \in \{1, 2, 3, \cdots, p-1\}$ that $a^2 \equiv 1 \mod p$?
Suppose $a^2 \equiv 1 \mod p$, then $p \mid a^2 - 1$ so $p \mid (a+1)(a-1)$, either $p \mid (a+1)$ or $p \mid (a-1)$. If $p \mid (a+1)$ then $a \equiv -1 \mod p$ or $a \equiv p-1 \mod p$. If $p \mid (a-1)$ then $a \equiv 1 \mod p$.

Ex. Suppose $p = 11$, the set is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Then the respective pairs would be $2 \cdot 6$, $3 \cdot 4$, $5 \cdot 9$, and $7 \cdot 8$. Notice that 1 and 10 do not have a pair that results in congruence $\mod 11$.

In general in $\{1, 2, 3, \cdots, p-1\}$ the integers all pair up such that their products are congruent $1 \mod p$, except for 1 and $p-1$. Thus,

$$(p-1)! = (1)(2)(3)\cdots(p-1) \equiv p-1 \equiv -1 \mod p$$

$\square$

Ex. Find the least non-negative residue of $20! \mod 23$.
Note: We see $20!$ and think $20! \equiv -1 \mod 21$, but 21 is not prime so there is no guarantee and it does not apply anyways because we have $\mod 23$.
However, $22! \equiv -1 \mod 23$

$$\begin{aligned} 22! &\equiv -1 \mod 23 \\ (22)(21)(20!) &\equiv -1 \mod 23 \\ (-1)(-2)(20!) &\equiv -1 \mod 23 \\ (2)(20!) &\equiv -1 \mod 23 \\ (2)(20!) &\equiv 22 \mod 23 \\ 20! &\equiv 11 \mod 23 \end{aligned}$$

In this case, 11 is the least non-negative residue.

2. **Fermat's Little Theorem:** Suppose p is prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then,

$$a^{p-1} \equiv 1 \mod p$$

Ex. $p = 97$ and $a = 10$, so $10^{96} \equiv 1 \mod 97$.

Proof. Consider the set of integers $S = \{a, 2a, 3a, \cdots, (p-1)a\}$ (there are $p-1$ integers in this set).

- First observe that none are congruent $0 \mod p$ because if $p \mid ka$ for some $1 \leq k \leq (p-1)$. Then $p \mid k$ or $p \mid a$ but $p \nmid a$ so $p \mid k$ but $1 \leq k \leq p-1$.
- Second, no two are congruent one another $\mod p$ because if $k_1 a \equiv k_2 a \mod p$ for some $1 \leq k_1 \leq p-1$ and $1 \leq k_2 \leq p-1$. Then $p \mid (k_1 a - k_2 a) = p \mid a(k_1 - k_2)$, since $p \nmid a$ then $p \mid (k_1 - k_2)$. But this is impossible because $1-(p-1) \leq k_1 - k_2 \leq (p-1)-1$.

Thus the set S, is we take all $\mod p$, is equivalent to the set $T = \{1, 2, 3, \cdots, p-1\}$ in some order. Since, mod p, all the numbers in S is congruent to all the numbers in T, we have

$$\begin{aligned}(a)(2a)(3a)\cdots((p-1)a) &\equiv (1)(2)(3)\cdots(p-1) \mod p\\ a^{p-1}(p-1)! &\equiv (p-1)! \mod p\\ a^{p-1}(-1) &\equiv (-1) \mod p\\ a^{p-1} &\equiv 1 \mod p\end{aligned}$$

Notice that we can canel all of the $1, 2, 3, \cdots, p-1$ without affecting the modulus because they are coprime to p. ☐

Ex. Find the least non-negative residue of $5^{123} \mod 13$.
Well $13 \nmid 5$ so $5^{12} \equiv 1 \mod 13$. Then $123 = 12(10) + 3$ so

$$\begin{aligned}5^{123} = 5^{12(10)+3} = 5^{12^{10}} 5^3 &\equiv (1)^{10} 5^3 \mod 13\\ &\equiv 5^3 \mod 13\\ &\equiv 5 \cdot 25 \mod 13\\ &\equiv 5(-1) \mod 13\\ &\equiv -5 \mod 13\\ &\equiv 8 \mod 13\end{aligned}$$

So 8 is the least non-negative residue.

Corollary: From $a^{p-1} \equiv 1 \mod p$ we get $a^p \equiv a \mod p$. Note that $a^p \equiv a \mod p$ even when $p \mid a$ because if $p \mid a$ then $a \equiv 0 \mod p$ and $a^p \equiv a \mod p$ is saying $0 \equiv 0$ mod p.

3. **Closing Notes:** This is relevant to cryptography for one of two reasons.
    - Encryption (which involved big exponents) is both practical and theoretically possible based on Fermat's Little Theorem and Euler's Theorem.
    - Pseudoprime is a non-prime which "behaves like a prime". e.g. in FLiT maybe p is not prime but still when $p \nmid a$ we get $a^{p-1} \equiv 1 \mod p$.

6.2 Fermat Pseudoprimes & Carmichael Numbers

1. **Introduction:** Primes are useful. Given $n \in \mathbb{Z}^+$ how can we check if n is prime? We could divide by everything (computationally intensive). Or we could use some tests which give insight.

2. **Fermat Pseudoprimes:**

   (a) **Reminder:** FLiT: If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$. Suppose we have some $n \in \mathbb{Z}$ with $n \geq 2$. Suppose we find some a with $n \nmid a$ and $a^{n-1} \not\equiv 1 \mod n$. We can conclude that n is not prime.
   Ex: Let $n = 63$, observe that if $a = 2$ then $n \nmid a$ clearly and $2^{62} \equiv 4 \not\equiv 1 \mod 63$. Thus, 63 is not prime.
   Definition: $a = 2$ is a *Fermat Witness* to the fact that 63 is composite.

   However, we might have some n and a with $n \nmid a$ and $a^{n-1} \equiv 1 \mod n$ but still have n composite.
   Ex. Let $n = 341$ and $a = 2$, then $341 \nmid 2$ and observe

   $$2^{340} \equiv 1 \mod 341$$

   Even though $n = 341 = 11 \cdot 31$ is not prime it still "passes Fermat's Little Theorem with $a = 2$."
   Definition: $a = 2$ is a *Fermat Liar* for $n = 341$.

   (b) **Definition:** Suppose n is composite and $b \in \mathbb{Z}$ satisfies $\gcd(n, n) = 1$ and $b^{n-1} \equiv 1 \mod n$. Then we say n is a *Fermat Pseudoprime to the base b*.
   Ex: So 341 is a *Fermat Pseudoprime with the base* $b = 2$.
   Ex: Likewise, 645 is a *Fermat Pseudoprime with the base* $b = 2$.

3. **Carmichael Numbers:**

   (a) **Introduction:** Given some n we wish to test if it is prime.

   - Pick some b with $\gcd(b, n) = 1$. Suppose we find $b^{n-1} \equiv 1 \mod n$. Either n is prime or b is a liar and n is a Fermat Pseudoprime with base b.
   - Try another b with $\gcd(b, n) = 1 \cdots$

   So, is it possible that we could try all b with $\gcd(b, n) = 1$ and always get $b^{n-1} \equiv 1 \mod n$ and still have a composite n? The answer, yes!

   (b) **Definition:** A number n is a *Carmichael Number* if it is a Fermat Pseudoprime for every base b with $\gcd(b, n) = 1$. These are sometimes called Absolute Pseudoprimes.
   Ex: $n = 561$ is a Carmichael Number. Note that $561 = 3 \cdot 11 \cdot 17$. Suppose b satisfies $\gcd(b, 561) = 1$. Then

   - $\gcd(b, 3) = 1$ so by FLiT $b^2 \equiv 1 \mod 3$. So $b^{560} = (b^2)^{280} \equiv 1 \mod 3$ so $3 \mid b^{560} - 1$.
   - $\gcd(b, 11) = 1$ so by FLiT $b^{10} \equiv 1 \mod 11$. So $b^{560} = (b^{10})^{56} = (1)^{56} \equiv 1 \mod 11$ so $11 \mid b^{560} - 1$.

- $\gcd(b,17)=1$ so by FLiT $b^{16}\equiv 1 \mod 17$. So $b^{560}=(b^{16})^{35}\equiv(1)^{35}\equiv 1 \mod 17$ so $17 \mid b^{560}-1$.

So $3\cdot 11\cdot 17 \mid b^{560}-1 \implies 561 \mid b^{560}-1$. Therefore $b^{560}\equiv 1 \mod 561$.

(c) **Theorem:** Suppose $n=p_1p_2\cdots p_k$ such that $\forall i$ we have $p_i-1 \mid n-1$. Then n is a Carmichael Number.

Proof. Suppose $\gcd(b,n)=1$. Claim that $b^{n-1}\equiv 1 \mod n$ well, for each i we have $\gcd(b,p_i)=1$. By FLiT we have $b^{p_i-1}\equiv 1 \mod p_i$ then $b^{n-1}=b^{\alpha(p_i-1)}\equiv(1)^{\alpha}\equiv 1 \mod p_i$. Thus, $p_i \mid b^{n-1}-1$ for all i. Therefore, $n \mid b^{n-1}-1$ so $b^{n-1}\equiv 1 \mod n$. $\square$

6.3 Euler's Theorem

---

1. **Introduction:** Fermat's Little Theorem tells us that is p is a prime and if $p\nmid a$ then $a^{p-1}\equiv 1 \mod p$. This is relevant for both calculation and cryptography. Since this is useful for reducing large powers of $a \mod p$ it might be helpful if we had a version for when the modulus is not prime.

2. **Preliminaries:**

(a) **Definition:** Define the *Euler Phi-Function* $\phi:\mathbb{Z}^+\to\mathbb{Z}$. For $n\in\mathbb{Z}^+$ we define $\phi(1)=1$ and $\phi(n)=$ the number of positive integers less than n which are coprime to n.
Ex. $\phi(10)=4$ because the set $\{1,3,7,9\}$ is all coprime to 10.
Ex. $\phi(97)=96$ because $\{1,2,\cdots,96\}$ are all coprime to 96.
Definition: If n is prime then $\phi(n)=n-1$.

(b) **Recall:** A complete residue system mod n is a set of n integers, none of them congruent to each other mod n. CRS mod 8 is $\{0,1,2,\cdots,7\}$.

(c) **Definition:** A *reduced residue system* mod n is a set of $\phi(n)$ integers all of which are coprime to n and no two of which are congruent to each other mod n.
Ex. RRS mod 10 is $\{1,3,7,9\}$ or $\{11,-7,7,29\}$.

(d) **Theorem:** Suppose $\{r_1,r_2,\cdots r_{\phi(n)}\}$ is a RRS mod n. Then suppose $a\in\mathbb{Z}$ with $\gcd(a,n)=1$. Then $\{ar_1,ar_2,\cdots ar_{\phi(n)}\}$ is also a RRS mod n.

Proof. We see there are $\phi(n)$ of them. Claim that each is coprime to n.

- By means of contradiction, suppose we have some ar_i not coprime to n, that is $\gcd(ar_i,n)\neq 1$. Then $\exists$ a prime p with $p\mid ar_i$ and $p\mid n$. Since $p\mid ar_i$ so $p\mid a$ or $p\mid r_i$. If $p\mid a$ then, along with $p\mid n$, we have a contradiction because $\gcd(a,n)=1$. If $p\mid r_i$ then, along with $p\mid n$, we have a contradiction because $\gcd(r_i,n)=1$. So the ar_i are coprime to n.
- Suppose we have $ar_i\equiv ar_j \mod n$, since $\gcd(a,n)=1$ we can cancel. So $r_i\equiv r_j \mod n$. So no two new elements are congruent mod n.

$\square$

3. **Euler's Theorem:** Suppose n is a modulus and $\gcd(a,n) = 1$. Then $a^{\phi(n)} \equiv 1 \bmod n$. **Note.** If $n = p =$ prime we have $\phi(n) = n-1$ and we get Fermat's Little Theorem.

   Proof. Given a modulus n, let $S = \{r_1, \cdots, r_{\phi(n)}\}$ be any RRS. Then by the theorem above, $S' = \{ar_1, \cdots ar_{\phi(n)}\}$ is also a RRS. It follows that S and S' consist of the same integers mod n. Thus,

   $$(ar_1)(ar_2)\cdots(ar_{\phi(n)}) \equiv r_1 r_2 \cdots r_{\phi(n)} \bmod n$$
   $$a^{\phi(n)} \equiv 1 \bmod n$$

   □

4. **Use For Calculation:** To reduce 9^{453} mod 16, we note that $\gcd(9,16) = 1$ so Euler's Theorem tells us that $9^{\phi(16)} \equiv 1 \bmod 16$. Since $\phi(16) = 8$ we ahve $9^8 \equiv 1 \bmod 9$ and so:

   $$9^{453} = 9^{8(56)+5} \equiv 9^5 \equiv 9(81)^2 \equiv 9 \bmod 16$$

5. **Note:** If $\gcd(a,n) = 1$ then $a^{\phi(n)-1}$ is a multiplicative inverse of a mod n.

6.4 Problems

---

1. Use Fermat's Little Theorem to find the least nonnegative residue of $2^{1000003} \mod 17$.
2. Use Fermat's Little Theorem to solve the following, giving the result as the least nonnegative residue.
   (a) $7x \equiv 12 \mod 17$
   (b) $10x \equiv 13 \mod 19$
3. Use Fermat's Little Theorem to show that $30 \big| (n^9 - n)$ for all positive integers n.
4. The definition of n being a Fermat pseudoprime to base b does not actually require that $\gcd(b,n) = 1$ because it's not possible to have $b^{n-1} \equiv 1 \mod n$ with $\gcd(b,n) \neq 1$. Prove this.
5. We didn't exclude even integers from the definition of a Fermat Pseudoprime. Some books do. Show that with our definition 4 is a Fermat Pseudoprime to a certain base.
6. Prove that if n is an odd Fermat Pseudoprime to some base then it must be so to an even number of bases.
7. Prove that 1105 is a Carmichael number.
8. Use Euler's Theorem to find the units digit of 7^{999999}.
9. Solve each of the following using Euler's Theorem. Solutions should be least nonnegative residues.
   (a) $5x \equiv 3 \mod 14$

(b) $4x \equiv 7 \mod 15$

(c) $3x \equiv 5 \mod 16$

10. Prove that if $\gcd(a, 30) = 1$ then $60 \mid a^4 + 59$.

7 Various Multiplicative Functions

7.1 Multiplicative Functions and The Euler Phi Function

---

1. **Introduction:** In 4.3 (Chapter 6 of the text), we looked at ϕ in Euler's Theorem. If calculating ϕ is useful, we would like to do it easily. Perhaps find some properties. The goal in this section is to introduce related concepts.

2. **Function Definitions:**

   (a) **Definition:** A function is *arithmetic* if it is defined on all positive integers.
   Ex. $f(n) = n^2$
   Ex. $f(n) = \sqrt{10 - n^2}$ is not, because it fails for $n \geq 4$.

   (b) **Definition:** An arithmetic function is *multiplicative* if, whenever $\gcd(m, n) = 1$, we have $f(mn) = f(m)f(n)$.

   (c) **Definition:** An arithmetic function is *completely multiplicative* if $f(mn) = f(m)f(n)$ always.
   Ex. $f(n) = n$ because $f(mn) = mn = f(m)f(n)$.
   Ex. $f(n) = n^3$ because $f(mn) = (mn)^3 = m^3n^3 = f(m)f(n)$.
   Ex. $f(n) = n + 1$ because $f(3 \cdot 3) = f(9) = 10$ but $f(3)f(3) = 4 \cdot 4 = 16$.
   Clearly, all completely multiplicative functions are multiplicative. Are there any functions which are multiplicative but not *completely* multiplicative.

   Note: ϕ is not completely multiplicative because

   $$\phi(10)\phi(10) = 4 \cdot 4 = 16 \neq 25 = \phi(100) = \phi(10)\phi(10)$$

   Is ϕ, perhaps, multiplicative?

3. **Theorem** If f is multiplicative and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ then

   $$f(n) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_n^{\alpha_n})$$

   Proof. This follows from being multiplicative. □

4. **Back to ϕ:**

   (a) **Theorem:** If p is prime then $\phi(p) = p - 1$

   Proof. All of $1, 2, 3 \cdots, p - 1$ are coprime to p. □

   (b) **Theorem:** If p is prime then $\phi(p^k) = p^k - p^{k-1}$.

   Proof. Of all the numbers $1, 2, 3 \cdots, p - 1$, the only ones which are not coprime to p^k are the multiples of p itself. Those are $p, 2p, 3p, \cdots, p^{k-1}p$ and so there are p^{k-1} of these. The remaining ones are coprime and there are $p^k - p^{k-1}$ of these. □

Ex. $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$.
Ex. $\phi(7^3) = 7^3 - 7^2 - 243 - 49 = 194$.

It is often good to note: $\phi(p^k) = p^{k-1}(p-1)$, $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.

(c) **Theorem:** The Euler Phi function is multiplicative.
Ex. To model the proof after $\phi(6 \cdot 5)$, where $m = 6$ and $n = 5$. List $1, 2, \cdots, 30$.

$$\begin{array}{llllll}
\boxed{1} & \boxed{7} & \boxed{13} & \boxed{19} & 25 & \\
2 & 8 & 14 & 20 & 26 & \text{-}\textit{ignore} \\
3 & 9 & 15 & 21 & 27 & \text{-}\textit{ignore} \\
4 & 10 & 16 & 22 & 28 & \text{-}\textit{ignore} \\
5 & \boxed{11} & \boxed{17} & \boxed{23} & \boxed{29} & \\
6 & 12 & 18 & 24 & 30 & \text{-}\textit{ignore}
\end{array}$$

We see that there are two rows to consider and $\phi(6) = 2$ within each of those rows there are 4 good values and $\phi(5) = 4$. So we see that two rows with four values each $= 2 \cdot 4$ values which is $\phi(6)\phi(5)$. Thus $\phi(6 \cdot 5) = \phi(6)\phi(5) = 8$.

Proof. Look at $\phi(mn)$ with $\gcd(m, n) = 1$. List them all,

$$\begin{array}{llll}
1 & m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & \cdots & (n-1)m+2 \\
\vdots & \vdots & \ddots & \vdots \\
m & m+m & \cdots & (n-1)m+m = mn
\end{array}$$

Consider row r with $1 \leq r \leq m$. This row is $r, m+r, 2m+r, \cdots, (n-1)m+r$. All have the form $km + r$ with $0 \leq k \leq n-1$. Note that $\gcd(km+r, m) = \gcd(r, m)$. So the entire of row r is coprime to m if and only if r is coprime to m. So throw out those entire rows which are not coprime to m because the values are not coprime to m, hence not coprime to mn. Note that $\phi(m)$ rows remains, look at each row which remains. Each is a row r with $\gcd(r, m) = 1$. Observe that $\{0, 1, 2, \cdots, n-1\}$ is a CSOR mod n and since $\gcd(m, n) = 1$, so is the set $\{0 \cdot m + r, 1 \cdot m + r, \cdots, m(n-1) + r\}$. Note this is one of our rows, row r. Out of that CSOR, $\phi(n)$ will be coprime to n those are also coprime to m because they are in a row which survived. Thus they are coprime to mn.

Finally: $\phi(m)$ rows survive, in each $\phi(n)$ entries. Thus $\phi(m)\phi(n)$ entires coprime to mn. So $\phi(mn) = \phi(m)\phi(n)$ $\square$

(d) **Corollary:** For $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ we have:

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

Ex. $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 100(\frac{1}{2})(\frac{4}{5}) = 40$.
Ex. To find $\phi(432)$ we find $432 = 2^4 \cdot 3^3$ and so:

$$\phi(432) = 432\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 144$$

Observation For Analysis:

- If some prime $p \mid n$ then $p - 1 \mid \phi(n)$.
- If some $p^\alpha \mid n$ then $p^{\alpha - 1} \mid \phi(n)$.

This can help us with a calculation like the following.

Ex. Find all n with $\phi(n) = 6$.
First note if $p \mid n$ then $p - 1 \mid \phi(n) = 6$, thus we can only have $p - 1 = 1, 2, 3, 6 \implies p = 2, 3, 4, 7 \implies p = 2, 3, 7$ (4 is not prime). Thus the only primes are $p = 2, 3, 7$. So we now know n is of the form $n = 2^\alpha 3^\beta 7^\gamma$ with $\alpha, \beta, \gamma \geq 0$.

- If $\alpha \geq 1$ then $2^\alpha \mid n \implies 2^{\alpha - 1} \mid \phi(n) = 6$ and so $\alpha = 0, 1, 2$.
- If $\beta \geq 1$ then $3^\beta \mid n \implies 3^{\beta - 1} \mid \phi(n) = 6$ and so $\beta = 0, 1, 2$.
- If $\gamma \geq 1$ then $7^\gamma \mid n \implies 7^{\gamma - 1} \mid \phi(n) = 6$ and so $\gamma = 0, 1$.

So then $\phi(n) = 6$ then $n = 2^\alpha 3^\beta 7^\gamma$ with $\alpha = 0, 1, 2$, $\beta = 0, 1, 2$, and $\gamma = 0, 1$. These are all neccessary but *not* sufficient, we have to check each combination.

$$\begin{aligned}
&\phi(2^0 3^0 7^0) = 1 \\
&\phi(2^0 3^0 7^1) = 6 \\
&\qquad \vdots \\
&\phi(2^0 3^2 7^0) = 6 \\
&\qquad \vdots \\
&\phi(2^1 3^2 7^0) = 6 \\
&\qquad \vdots \\
&\phi(2^1 3^0 7^1) = 6 \\
&\qquad \vdots
\end{aligned}$$

Thus $n = 7, 9, 14, 18$.

Ex. $\phi(n) = 97$ if $p \mid n$ then $p-1 \mid \phi(n) = 97$, $p - 1 = 1 \implies p = 2$. Then $n = 2^\alpha$ with $\alpha \geq 0$. If $\alpha \geq 1$, then $2^\alpha \mid n \implies 2^{\alpha-1} \mid 97$ so no $\alpha \geq 1$ works, $n = 2^0$.

7.2 The Sum and Number of Divisors

---

1. **Introduction:** We can define two more related functions besides Euler's Phi function.
   Definition: $\tau(n)$ is the number of positive divisors of n.
   Definition: $\sigma(n)$ is the sum of all positive divisors of n.
   Ex. $\tau(6) = 4$ because $1, 2, 3, 6 \mid 6$.
   Ex. $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

   It turns out that these are also multiplicative functions, this will allow nice formulas.

2. **Formulas:**

   (a) First note that $\tau(p^\alpha) = \alpha + 1$ because the divisors are $1, p^1, \cdots, p^\alpha$. So now for $n = p^{\alpha_1} \cdots p^{\alpha_k}$ we have

   $$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

   because τ is multiplicative.

   (b) Then note that $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \sum_{i=0}^{n} p^i = \frac{p^{\alpha+1}-1}{p-1}$. So now for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ we have

   $$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

   because σ is multiplicative.

   Ex. If $n = 3^2 \cdot 5^5 \cdot 11$ then $\tau(n) = (2 + 1)(5 + 1)(1 + 1) = 36$ and then $\sigma(n) = \left(\frac{3^3-1}{3-1}\right)\left(\frac{5^6-1}{5-1}\right)\left(\frac{11^2-1}{11-1}\right)$

3. **Proving τ and σ are Multiplicative**
   Theorem: Suppose $f(n)$ is multiplicative. Define $F(n) = \sum_{d \mid n} f(d)$ (Summatory Function) i.e. $F(6) = f(1) + f(2) + f(3) + f(6)$. If the base function is multiplicative, then the summatory function is also multiplicative.

Proof. Claim $F(mn) = F(m)F(n)$ with $\gcd(m, n) = 1$. The proof then follows,

$$\begin{aligned}
F(mn) &= \sum_{d|mn} f(d) \\
&= \sum_{d_1|m, d_2|n} f(d_1 \cdot d_2) \\
&= \sum_{d_1|m, d_2|n} f(d_1)f(d_2) \\
&= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\
&= F(m)F(n)
\end{aligned}$$

$\square$

Corollary: Let $f(n) = 1$. This is clearly multiplicative (completely multiplicative), so $F(n) = \sum_{d|n} 1$ is multiplicative. But $F(n) = \tau(n)$ so τ is multiplicative.

Corollary: Let $f(n) = n$. This is also completely multiplicative, so $F(n) = \sum_{d|n} f(d)$ is multiplicative. But $F(n) = \sigma(n)$ so σ is multiplicative.

7.3 Perfect Numbers and Mersenne Primes

---

1. **Introduction:** The definition of the sum of the divisors of a positive integer leads to the concept of a perfect number which is intrinsically connected to a Mersenne prime.

2. **Definition:** A positive integer is *perfect* if the sum of the positive divisors equals twice the integer, that is, $\sigma(n) = 2n$.
   Ex. The integer $n = 6$ is a perfect number since $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2(6)$.

3. **Finding Perfect Numbers:** It is unknown whether there are infinitely many perfect numbers and it is unknown whether there are any odd perfect numbers - all perfect numbers which have been found have been even. Currently there are only 51 known perfect numbers, the largest of which has 49724095 digits.

4. **Theorem:** If $n \in \mathbb{Z}^+$ is perfect and even if and only if $n = 2^{m-1}(2^m - 1)$ for some $m \in \mathbb{Z}$ with $m \geq 2$ and $2^m - 1$ being prime. To find perfection look at $2^m - 1$'s until we get primes!

   - $2^2 - 1 = 3$ prime! So $2^{2-1}(2^2 - 1) = 2(3) = 6$ perfect!
   - $2^3 - 1 = 7$ prime! So $2^{3-1}(2^3 - 1) = 4(7) = 28$ perfect!
   - $2^4 - 1 = 15$ nope!
   - $2^5 - 1 = 31$ prime! So $2^{5-1}(2^5 - 1) = (16)(31) = 496$ perfect!
   - $2^6 - 1 = 63$ nope!

- $2^7 - 1 = 127$ prime! So $2^{7-1}(2^7 - 1) = 8128$ perfect!
- $2^8 - 1 = 255$ nope!
- $2^9 - 1 = 511 = (7)(73)$ nope!
- $2^{10} - 1 = 1023 = (3)(11)(31)$ nope!
- $2^{11} - 1 = 2047 = (23)(89)$ nope!

Up until here it seemed that $2^p - 1$ is prime but not so.

Proof.
$\Leftarrow$: Suppose $2^m - 1$ is prime with $m \geq 2$. Define $n = 2^{m-1}(2^m - 1)$ and claim that n is perfect. Claim $\sigma(n) = 2n$, look at $\sigma(n) = \sigma(2^{m-1}(2^m - 1))$ well, $2^m - 1 \geq 3$ and is odd, 2^{m-1} is a power of 2, so $\gcd(2^{m-1}, 2^m - 1) = 1$. So, $\sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1)$. Then observe from 5.2.2a,

$$\sigma(2^{m-1}) = \frac{2^m - 1}{2 - 1} = 2^m - 1$$

and

$$\sigma(2^m - 1) = 1 + (2^m - 1)$$

because $2^m - 1$ is prime. So $\sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)(2^m) = 2 \cdot 2^{m-1}(2^m - 1) = 2n$. Thus, $\sigma(n) = 2n$.

$\Rightarrow$: This direction is fairly lengthy and will be omitted. It is in the text if you're interested. $\square$

5. **Theorem:** If $2^m - 1$ is prime then m is prime. I.e. if m is composite then $2^m - 1$ is composite.

   Proof. If m is composite then $m = ab$ with $a, b > 1$, then observe

   $$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^{a(1)} + 1)$$

   So 2^m is composite. $\square$

   All together we see,

   $$[m \text{ prime }] \Leftarrow [2^m - 1 \text{ prime }] \iff \left[2^{m-1}(2^m - 1) \text{ perfect }\right]$$

   Definition: The m^{th} Mersenne number is $M_m = 2^m - 1$.

   Definition: If p is prime and if $2^p - 1$ is also prime then $M_p = 2^p - 1$ is a Mersenne prime.

   Ex. $2^5 - 1 = 31$ is a Mersenne prime.

   Ex. 29 is a prime but not a Mersenne prime because it is not of the form $2^p - 1$.

   Suppose p is prime. We know $2^p - 1$ might be prime. Is there a way of checking besides trying all divisors?

6. **Theorem:** If p is prime, then all factors of 2^p-1 must have the form $2pk+1$ for $k \in \mathbb{Z}^+$.

   Theorem: We only need to check factors of this form.

   Proof. Omitted, the proof is not long but depends on an obscure lemma related to the Eulcidean Algorithm. $\square$

   Ex. Consider $p = 11$ is prime. Look at $2^{11} - 1 = 2047$, by the theorem check $2(11)k+1 = 22k+1$ for $k = 1, 2, 3, \cdots$. Also only check up to $\sqrt{2047} \approx 45.24$, so only check 23 and 45. We find $2047 = (23)(89)$. Not Prime!

   Ex. Consider $p = 13$ is prime. Look at $2^{13} - 1 = 8191$, by the theorem check $2(13)k = 26k + 1$ for $k = 1, 2, 3, \cdots$. Also only check up to $\sqrt{8191} \approx 90.5$, so only check 27, 53, 79. None of the factors check so 8191 is prime.

7.4 Problems

---

1. Find all n satisfying $\phi(n) = 18$.
2. Show there are no n with $\phi(n) = 14$.
3. For what values of n is $\phi(n)$ odd? Justify.
4. Prove that $f(n) = \gcd(n, 3)$ is multiplicative. (This is actually true if 3 is replaced by any positive integer.)
5. Find $\tau(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$
6. Find $\sigma(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$
7. Find $\tau(20!)$.
8. Classify all n with $\tau(n) = 30$. Explain!
9. Prove that $\sigma(n) = k$ has at most a finite number of solutions when k is a positive integer.
10. Show that if a and b are positive integers and p and q are distinct odd primes then $n = p^a q^b$ is deficient.
11. Prove that a perfect square cannot be a perfect number.
12. Use Theorem 7.12 to determine whether each of the following Mersenne numbers is a Mersenne prime:
    (a) M_{11}
    (b) M_{21}
    (c) M_{31}

9 Primitive Roots

9.1 The Order of an Integer & Primitive Roots

---

1. **Introduction:** The process of exponentiation and its inverse (logarithms) is as essential in modular arithmetic as it is in regular math and forms the basis for various encryption techniques. We begin by taking a base a which is coprime to a modulus m and looking at the powers of a mod m.

2. **Order:** Given a modulus m and an integer a with $\gcd(a, m) = 1$ Euler's Theorem tells us that $a^{\phi(m)} \equiv 1 \bmod m$. It does not however tell us that $\phi(m)$ is the lowest power which yields 1. This leads to the following.

   (a) **Definition:** Suppose $\gcd(a, m) = 1$ we define the *order* of a mod m as the smallest power x such that $a^x \equiv 1 \bmod m$. This is denoted $\text{ord}_m a$.
   Note: $\text{ord}_m a \leq \phi(m)$
   Note: We can say "order of a" when m is contextually obvious.
   Ex. Let's find $\text{ord}_{11} 3$. Well,

   $$\begin{aligned} 3^1 &\equiv 3 \bmod 11 \\ 3^2 &\equiv 9 \bmod 11 \\ 3^3 &\equiv 5 \bmod 11 \\ 3^4 &\equiv 4 \bmod 11 \\ 3^5 &\equiv 1 \bmod 11 \end{aligned}$$

   Thus, $\text{ord}_{11} 3 = 5$.
   Note: We can now start to see that the order gives us a pattern under which 3^x will repat!

   (b) **Theorem:** For $x \in \mathbb{Z}^+$ we have $a^x \equiv 1 \bmod m$ if and only if $x \equiv 0 \bmod \text{ord}_m a$ if and only if $\text{ord}_m a \mid x$.
   Ex. We saw $\text{ord}_{11} 3 = 5$ so $3^x \equiv 1 \bmod 11$ if and only if $x \equiv 0 \bmod 5$ if and only if $5 \mid x$.

   Proof.
   $\rightarrow$ Assume $a^x \equiv 1 \bmod m$, use the Divison Algorithm to write $x = q(\text{ord}_m a) + r$. Observe,

   $$1 \equiv a^x \equiv \left(a^{\text{ord}_m a}\right)^q a^r \equiv a^r \bmod m$$

   Since $\text{ord}_m a$ is the smallest positve power, we must have $r = 0$. Thus, $x = q\text{ord}_m a$ so $\text{ord}_m a \mid x$.

   $\leftarrow$ Assume $\text{ord}_m a \mid x$. Then,

   $$a^x \equiv a^{k\text{ord}_m a} \equiv \left(a^{\text{ord}_m a}\right)^k \equiv 1^k \equiv 1 \bmod m$$

   $\square$

(c) **Corollary:** We have $\text{ord}_m a \mid \phi(m)$.

Proof. The proof here is obvious because $a^{\phi(m)} \equiv 1 \bmod m$. Apply the theorem. □

So to find $\text{ord}_m a$ try divisors of $\phi(m)$ only.
Ex. To find $\text{ord}_{11} 2$ we note that $\phi(11) = 10$. So we need to check $1, 2, 5$ because if it fails for those, $\text{ord}_{11} 2 = 10$.

$$2^1 \equiv 2 \not\equiv 1 \bmod 11$$
$$2^2 \equiv 4 \not\equiv 1 \bmod 11$$
$$2^5 \equiv 10 \not\equiv 1 \bmod 11$$

Aha, from this we can see that $2^{10} \equiv 1 \bmod 11$ by Euler's Theorem. So $\text{ord}_{11} 2 = 10$.

(d) **Theorem:** We have $a^x \equiv a^y \bmod m$ if and only if $\text{ord}_m a \mid (x - y)$ if and only if $x \equiv y \bmod \text{ord}_m a$. i.e. Exponents work mod $\text{ord}_m a$.
Ex. $\text{ord}_{11} 3 = 5$ so $3^x \equiv 3^y \bmod 11$ if and only if $x \equiv y \bmod \text{ord}_{11} 3$ ($x \equiv y \bmod 5$).

Proof.
$\rightarrow$ Suppose $a^x \equiv a^y \bmod m$ without loss of generality, assume $x > y$. Since $\gcd(a, m) = 1$ we can cancel a^y from each side to get $a^{x-y} \equiv 1 \bmod m$. By (b) above then $x - y \equiv 0 \bmod \text{ord}_m a$.

$\leftarrow$ Suppose $x \equiv y \bmod \text{ord}_m a$, then $x = y + k\text{ord}_m a$ for some k. Then $a^x \equiv a^y a^{k\text{ord}_m a} \equiv a^y \left(a^{\text{ord}_m a}\right)^k \equiv a^y \cdot 1 \equiv a^y \bmod m$. □

Summary Ex. We saw $\text{ord}_{11} 3 = 5$. So 3^x repeats every 5^{th} power mod 11 and $3^5 \equiv 1 \bmod 11$.

3. **Primitive Roots**

(a) **Introduction:** If $\gcd(a, m) = 1$ we know that $a^{\phi(m)} \equiv 1 \bmod m$ by Euler's Theorem, but this may not be the smallest power.
Ex. $\gcd(3, 11) = 1$ and so $3^{\phi(11)} \equiv 1 \bmod 11$ so $3^{10} \equiv 1 \bmod 11$, but in fact $3^5 \equiv 1 \bmod 11$ and $\text{ord}_{11} 3 = 5$ (smallet than 10).
Ex. $\gcd(6, 11) = 1$ and so $6^{\phi(11)} \equiv 1 \bmod 11$ so $6^{10} \equiv 1 \bmod 11$ and in fact this is the smallest. $\text{ord}_{11} 6 = 10 = \phi(11)$.

(b) **Definition:** Suppose $\gcd(a, m) = 1$, we say a is a *primitive root* modulus m if $\text{ord}_m a = \phi(m)$. $a = 3$ is not a primitive root mod 11, but $r = 6$ is a primitive root mod 11.
Intuition: Having a primitive root as a base results in more results when we raise it to powers.

(c) **Theorem:** Suppose r is a primitive root mod m. Then $\left\{r, r^2, \cdots, r^{\phi(m)}\right\}$ is a reduced residue set mod m, meaning there are $\phi(m)$ distinct items and all are coprime to m.

Proof. All are distinct because powers all distinct mod $\phi(m) = \text{ord}_m a$. All are coprime to m because all are powers of r and r is coprime to m. $\square$

Intuition: Given an m, finding a primitive root r is nice because there will be $\phi(m)$ distinct powers of r and that is the most we could have.
Given an m, can we always find a primitive root? No. $m = 8$ has no primitive roots, but if m is prime then we can. If m has a primitive root, might it have several? It might ...

(d) **Theorem:** Given a modulus m and an integer a with $\gcd(a, m) = 1$ we have:

$$\text{ord}_m\left(a^k\right) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

Note: In MATH403 this is the same result as the result from cyclic groups which states that if $|g| = n$ then $\left|g^k\right| = \frac{n}{\gcd(n,k)}$.
Ex. $\text{ord}_{11}6 = 10$. Look at $\text{ord}_{11}(6^2)$, intuitively it should be 5.

$$\text{ord}_{11}(6^2) = \frac{\text{ord}_{11}6}{\gcd(\text{ord}_{11}6, 2)} = \frac{10}{\gcd(10, 2)} = \frac{10}{2} = 5$$

Proof. We'll first proof it is $\leq$ and $\geq$, thereby proving it is equal.

- First observe:

$$\begin{aligned}\left(a^k\right)^{\text{ord}_m a/\gcd(\text{ord}_m a,k)} &= \left(a^{\text{ord}_m a}\right)^{k/\gcd(\text{ord}_m a,k)} \\ &\equiv 1^{k/\gcd(\text{ord}_m a,k)} \\ &\equiv 1 \bmod m\end{aligned}$$

  So,

$$\text{ord}_m(a^k) \leq \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

- Second observe:

$$\begin{aligned}a^{k\text{ord}_m(a^k)} &= \left(a^k\right)^{\text{ord}_m(a^k)} \\ &\equiv 1 \bmod m\end{aligned}$$

  So then, $\text{ord}_m a \Big| k\text{ord}_m\left(a^k\right) \implies \frac{\text{ord}_m a}{\gcd(\text{ord}_m a,k)} \Big| \frac{k\cdot\text{ord}_m(a^k)}{\gcd(\text{ord}_m a,k)}$. Then, because gcd of two fractions is 1 we get, $\frac{\text{ord}_m a}{\gcd(\text{ord}_m a,k)} \Big| \text{ord}_m\left(a^k\right)$, and so $\frac{\text{ord}_m a}{\gcd(\text{ord}_m a,k)} \leq \text{ord}_m\left(a^k\right)$

Thus, the two results together give us that

$$\text{ord}_m\left(a^k\right) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, k)}$$

$\square$

(e) **Theorem:** Suppose r is a primitive root of m. Then r^k is a primitive root of m if and only if $\gcd(k, \phi(m)) = 1$.

Proof. Well, r^k is a primitive root mod m if and only if $\text{ord}_m\left(r^k\right) = \phi(m) = \text{ord}_m a$, by the theorem this is true if and only if and only if $\gcd(\text{ord}_m r, k) = 1$ if and only if $\gcd(\phi(m), k) = 1$. ☐

(f) **Corollary:** If there is a primitive root mod m then there are $\phi(\phi(m))$ of them.

Proof. Let r be a primitive root. Since powers of r form a reduced residue set mod m we know that all other integers coprime to m may be written as r^k for some k, then by the previous theorem we know that r^k is also a primitive root if and only if $\gcd(k, \phi(m)) = 1$ and there are $\phi(\phi(m))$ such k. ☐

Ex. $r = 6$ is a primitive root mod 11. Then is has $\phi(\phi(11)) = \phi(10) = 4$ primitive roots. What are they? Take k with $\gcd(k, \phi(11)) = 1$ i.e. k with $\gcd(k, 10) = 1$. So $k = 1, 3, 7, 9$, therefore $6^1, 6^3, 6^7, 6^9 \implies 6, 7, 8, 2$ are the primitive roots.

9.2 Discrete Logarithms

---

1. **Introduction:** Just for reference, sections 9.2 and 9.3 concern themselves with the existence of primitive roots. They are quite technical so we will omit them and go on to section 9.4 which addresses what we can do with them. How can we solve (or even know if solutions exist) something like $3^x \equiv 5 \bmod 22$ or -how many solutions there might be, or -if the solutions are mod 22 or something else. In pre-calculus with $3^x \equiv 5$ we can do $x = \log_3 5$, but we cannot do that here (yet).

2. **Back to Primitive Roots:** Recall that if $\gcd(r, m) = 1$ and r is a primitive root mod m then the set $\{r^1, r^2, \cdots, r^{\phi(m)}\}$ gets us all integers coprime to m.
Ex. $r = 3$ is a primitive root of $m = 14$, because $3^1 \equiv 1, 3^2 \equiv 9, 3^3 \equiv 13, 3^4 \equiv 11, 3^5 \equiv 5, 3^6 \equiv 1 \bmod 14$. Note: $\text{ord}_{14} 3 = 6 = \phi(14)$ so it is a primitive root. Note: we obtain $3, 9, 13, 1, 5, 1$ are all coprime to 14. Thus, we see that we can solve $3^x \equiv a \bmod 14$ if and only if $\gcd(a, 14) = 1$.

   In general, when r is a primitive root mod m then

   $$r^x \equiv a \bmod m \iff \gcd(a, m) = 1$$

   has solutions.

3. **Indices:**

   (a) **Definition:** Suppose r is a primitive root mod m and $\gcd(a, m) = 1$. The exponent x with $1 \leq x \leq \phi(m)$ satisfying $r^x \equiv a \bmod m$ is the *index* of a mod m with primitive root r. This is denoted $\text{ind}_r a$. Note: m is missing from the notation but it matters, generally it is known in the problem. We could also write $\log_r a$ too but be careful to not think it be a 'normal' log.

Ex. $r = 3$ is a primitive root mod 14 and:

$$\begin{aligned}
3^1 &\equiv 3 \bmod 14 \leftrightarrow \text{ind}_3 3 = 1\\
3^2 &\equiv 9 \bmod 14 \leftrightarrow \text{ind}_3 9 = 2\\
3^3 &\equiv 13 \bmod 14 \leftrightarrow \text{ind}_3 13 = 3\\
3^4 &\equiv 11 \bmod 14 \leftrightarrow \text{ind}_3 11 = 4\\
3^5 &\equiv 5 \bmod 14 \leftrightarrow \text{ind}_3 5 = 5\\
3^6 &\equiv 1 \bmod 14 \leftrightarrow \text{ind}_3 1 = 6
\end{aligned}$$

Two Immediate Notes: If a, b coprime to m and r is a primitive root then:

i. $r^{\text{ind}_r a} = a$

ii. $a \equiv b \bmod m \iff \text{ind}_r a = \text{ind}_r b$. Side note, since indices are always between 1 and $\phi(m)$ we can actually write $a \equiv b \bmod m \iff \text{ind}_r a \equiv \text{ind}_r b \bmod \phi(m)$

Idea - in pre-calculus we do things like:

$$\begin{aligned}
3^x &= 4^{x-1}\\
\ln 3^x &= \ln 4^{x-1}\\
x \ln 3 &= (x-1)\ln 4
\end{aligned}$$

So now we can do things like:

$$\begin{aligned}
11^x &\equiv 5^{x-1} \bmod 14\\
\text{ind}_3 11^x &\equiv \text{ind}_3 5^{x-1} \bmod \phi(14)
\end{aligned}$$

Can we know do "log-like" rules?

(b) **Index Rules:** Indices behave like logarithms (think logarithm laws) but there is a quirk that arises from the order of r, that being $\phi(m)$. To see why this is, consider the logarithm rule $\log(ab) = \log a + \log b$. It would be tempting to write: $\text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b$. However, this is not quite right. Consider that with $m = 14$ and $r = 3$ if we have $a = 13$ and $b = 5$ then $ab \equiv 9 \bmod 14$, the tempting statement would say:

$$\begin{aligned}
\text{ind}_3 9 &= \text{ind}_3 13 + \text{ind}_3 5\\
2 &= 3 + 5\\
2 &= 8
\end{aligned}$$

Which is clearly false. However, we see that $2 \equiv 8 \bmod \phi(14)$.

Theorem: Let m be a modulus, r be a primitive root, and a, b coprime to m. Then we have:

i. $\text{ind}_r 1 \equiv 0 \bmod \phi(m)$

Proof. By Euler's Theorem we know that $r^{\phi(m)} \equiv 1 \bmod m$. So,

$$\text{ind}_r 1 = \phi(m) \equiv 0 \bmod \phi(m)$$

□

ii. $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$

Proof. Observe that from the definition of index:

$$r^{\text{ind}_r(ab)} \equiv ab \bmod m$$
$$r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a} r^{\text{ind}_r b} \equiv ab \bmod m$$

Then by a theorem from section 9.1 (which states that $a^x \equiv a^y \bmod m$ if and only if $x \equiv y \bmod \text{ord}_m a$) we get:

$$\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$$

□

iii. $\text{ind}_r a^k \equiv k\text{ind}_r a \bmod \phi(m)$

4. **The Discrete Logarithm Problem:** Given a modulus m and a primitive root r we know how to calculate $r^x \bmod m$ (given x) to reduce it. How hard is it to solve $r^x \equiv y \bmod m$ if y is given and we need x i.e. solving $\text{ind}_r y$. The answer, it is extremely hard. There is no meaningfully better way than trying all $1 \leq x \leq \phi(m)$. In simple cases we can try them all.

5. **Index Arithmetic:** We can use indices to solve modular problems involving exponets. Suppose we work frequently with the modulus $m = 17$. We first find a primitive root mod 17.

   Note: Assuming you know one exists

   - Find one by finding r with $\text{ord}_{17} r = \phi(17) = 16$.
   - There will be $\phi(\phi(17)) = \phi(16) = 8$ of them.

   Turns out $r = 3$ is a primitive root. So let's solve some problems.

   First, to find necessary discrete logs (aka indices) we will build a table:

a mod 17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

   (a) **Ex.** Solve $3x^{10} \equiv 12 \bmod 17$. Take the ind_3 of both sides.

$$\text{ind}_3(3x^{10}) \equiv \text{ind}_3(12) \bmod 16$$
$$\text{ind}_3 3 + \text{ind}_3 x^1 0 \equiv \text{ind}_3 12 \bmod 16$$
$$\text{ind}_3 3 + 10(\text{ind}_3 x) \equiv \text{ind}_3 12 \bmod 16$$
$$1 + 10(\text{ind}_3 x) \equiv 13 \bmod 16$$
$$10(\boxed{\text{ind}_3 x}) \equiv 12 \bmod 16{*} \qquad \text{treat this as } \textit{one} \text{ variable}$$

   Recall: $ax \equiv b \bmod m$ has solutions if and only if $\gcd(a, m) \mid b$ and if so, $\exists \gcd(a, m)$ incongruent solutions mod m. Obtain x_0 via guessing or the Euclidean Algorithm, then all solutions have the form $x = x_0 + k\frac{m}{\gcd(a,m)}$.
   Since $\gcd(10, 16) = 2 \mid 12$, $\exists 2$ solutions mod 16. The solutions we get are:

$$\text{ind}_3 x \equiv 6, 14 \bmod 16$$

Use the table to "un-index":

$$x \equiv 15, 2 \text{ mod } 17$$

***Note:** We could, at this point, do

$$\begin{aligned} 5\text{ind}_3 x &\equiv 6 \text{ mod } \frac{16}{\gcd(16,2)} \\ 5\text{ind}_3 x &\equiv 6 \text{ mod } 8 \\ \text{ind}_3 x &\equiv 6 \text{ mod } 8 \end{aligned}$$

This is unique mod 8 because $\gcd(5,8) = 1$. To "un-index" we need mod 16.

$$\text{ind}_3 x \equiv 6 \text{ mod } 8 \implies \text{ind}_3 x \equiv 6, 14 \text{ mod } 16$$

Now we can "un-index"

(b) **Ex.** Solve $4^x \equiv 16$ mod 17. We will take the ind_3 of both sides.

$$\begin{aligned} \text{ind}_3(4^x) &\equiv \text{ind}_3(16) \text{ mod } 16 \\ x\text{ind}_3 4 &\equiv \text{ind}_3(16) \text{ mod } 16 \\ x(12) &\equiv 8 \text{ mod } 16 \\ 12x &\equiv 8 \text{ mod } 16 \\ 3x &\equiv 2 \text{ mod } \frac{16}{\gcd(4,16)} \\ 3x &\equiv 2 \text{ mod } 4 \end{aligned}$$

Since $\gcd(3,4) = 1 \mid 2$, $\exists$ a solution mod 4.

$$x \equiv 2 \text{ mod } 4$$

Note: Any of $x = \cdots, -6, -2, 2, 6, \cdots$ works.
Note: Could also give as $x \equiv 2, 6, 10, 14$ mod 16 ("un-index" back to original mod)

Note: We can do either of these problems again with a completely different primitive root mod 17. As an exercise in understanding, we could do the two examples above with a different primitive root.

9.3 Problems

---

1. Determine the following orders and justify each.
   (a) $\text{ord}_{21} 8$
   (b) $\text{ord}_{25} 8$
2. Find all primitive roots (reduced mod 50) for $n = 50$ as follows: First find (with justification) the smallest primitive root. Then use the Theorem from class which yields all the remaining ones.

3. Prove that if p is an odd prime and a has $\text{ord}_p a = 2k$ then $a^k \equiv -1 \mod p$

4. Show that if a is relatively prime to m and $\text{ord}_m a = m - 1$ then m is prime.

5. Suppose r is a primitive root of an odd prime p. Prove that:

$$\text{ind}_r(p-a) \equiv \text{ind}_r a + \left(\frac{p-1}{2}\right) \mod p - 1$$

6. Show that if n is an integer and a and b are integers which are relatively prime to n with $\gcd(\text{ord}_n a, \text{ord}_n b) = 1$ then $\text{ord}_n(ab) = (\text{ord}_n a)(\text{ord}_n b)$.

7. Let r be a primitive root of the prime p with $p \equiv 1 \mod 4$. Prove that $-r$ is also a primitive root.

8. It's a fact that $r = 7$ is a primitive root mod 13.

   (a) Use this to construct a table of indices for this primitive root.

   (b) Use the table of indices to solve the equation: $x^2 \equiv 12 \mod 13$. Your answer(s) should be mod 13.

   (c) Use the table of indices to solve the equation: $4^x \equiv 12 \mod 13$. Your answer(s) should be mod 12.

9. With logarithms we have $\log_r a - \log_r b = \log_r \left(\frac{a}{b}\right)$

   (a) Why is it not reasonable to write $\equiv \text{ind}_r a - \text{ind}_r b \mod \phi(n) \equiv \text{ind}_r \left(\frac{a}{b}\right)$ when a, b are coprime to n and r is a primitive root?

   (b) What would be a reasonable index substitute for this logarithm rule?

   (c) Prove this substitute.

10. Suppose p is an odd prime and both r_1 and r_2 are primitive roots for p. Prove that $r_1 r_2$ is not a primitive root for p.

11 Quadratic Residues

Introduction: The concept of Quadratic Residues is a fundamental tool which has ramifications in lots of other number theory places: Cryptography, Factoring, etc...

11.1 Quadratice Residues & Nonresidues

---

1. **Introduction:** Suppose we asked the following, given a modulus m: Which numbers are perfect squares mod m?

   Ex. Let $m = 7$. What are the perfect squares? We could of course work backwards, squaring each value:

$$\begin{aligned}
0^2 &\equiv 0 \bmod 7\\
1^2 &\equiv 1 \bmod 7\\
2^2 &\equiv 4 \bmod 7\\
3^2 &\equiv 2 \bmod 7\\
4^2 &\equiv 2 \bmod 7\\
5^2 &\equiv 4 \bmod 7\\
6^2 &\equiv 1 \bmod 7
\end{aligned}$$

   Then the perfect squares are $0, 1, 2, 4$ and $3, 5, 6$ are not.

2. **Quadratice Residues & Nonresidues - Counting**

   (a) **Definition:** Let m be a modulus and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. We say a is a *quadratic residue mod m* if $\exists x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod m$. Otherwise, we say a is a *quadratic nonresidue mod m* if $\nexists x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod m$.

   Ex. If $m = 7$ then QR:$1, 2, 4$, QNR:$3, 5, 6$, and Neither:0.

   (b) **Theorem:** If p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a \implies \gcd(p, a) = 1$, then $x^2 \equiv a \bmod p$ has either no solutions or exactly two solutions mod p.

   Proof. If there are none, we are done. Suppose x is one solution to $x^2 \equiv a \bmod p$. Claim $-x$ is also a solution. Then $2x \equiv 0 \bmod p$. Since p is odd we can do $x \equiv 0 \bmod p$ which implies $p \mid x \implies p \mid x^2$. Then, $x^2 \equiv 0 \bmod p \implies a \equiv 0 \bmod p$ which contradicts $p \nmid a$.

   Let's show that for any two solutions, they are negative of one another. Suppose $x_1^2 \equiv a \bmod p$ and $x_2^2 \equiv a \bmod p$. Then $x_1^2 - x_2^2 \equiv 0 \bmod p$ so $p \mid (x_1^2 - x_2^2)$ so $p \mid (x_1 - x_2)(x_1 + x_2)$ so $p \mid (x_1 - x_2)$ or $p \mid (x_1 + x_2)$.
   If $p \mid (x_1 - x_2)$ then $x_1 \equiv x_2 \bmod p$. If $p \mid (x_1 + x_2)$ then $x_1 \equiv -x_2 \bmod p$. Thus, there can only be the two which are negatives of one another ☐

   (c) **Theorem:** Suppose p is an odd prime. Then $\exists \frac{p-1}{2}$ QR and $\exists \frac{p-1}{2}$ QNR.

Proof. If we square all of $1, 2, 3, \cdots, p-1$ the results will be in pairs (two of every result) the $\frac{p-1}{2}$ we do get are the QR. We miss $\frac{p-1}{2}$ results, those are the QNR. $\square$

(d) **Theorem:** Let p be an odd prime and r a primitive root mod p. Suppose $p \nmid a$, then a is a QR mod p if and only if $\text{ind}_r a$ is even.

Proof.
$\rightarrow$ Suppose a is a quadratice residue mod p, $\exists x$ such that $x^2 \equiv a \bmod p$. Then take the index of both sides to get $\text{ind}_r x^2 \equiv \text{ind}_r a \bmod p-1$ and so $2\text{ind}_r x \equiv \text{ind}_r a \bmod p-1$. From here we see $\text{ind}_r a = 2\text{ind}_r x + k(p-1)$ for some $k \in \mathbb{Z}$ and so since $p-1$ is even we know $\text{ind}_r a$ is even.

$\leftarrow$ Suppose $\text{ind}_r a$ is even. Say $\text{ind}_r a = 2k$ for $k \in \mathbb{Z}$ so $r^{2k} \equiv a \bmod p$ so $(r^k)^2 \equiv a \bmod p$. Then, a is a quadratice residue mod p. $\square$

To illustrate: $r = 3$ is a primitive root mod 17.

a mod 17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	$\underline{16}$	$\underline{14}$	1	$\underline{12}$	5	15	11	$\underline{10}$	$\underline{2}$	3	7	13	$\underline{4}$	9	$\underline{6}$	$\underline{8}$

So what this theorem tells us is that $a = 1, 2, 4, 8, 9, 13, 15, 16$ are the quadratic residues

3. **The Legendre Symbol and Properties**

(a) **Definition:** Given an odd prime p and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$, define the Legendre Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratice residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

Ex. If $p = 7$ we have:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Since $1, 2, 4$ are QR mod 7 and $3, 5, 6$ are QNR mod 7.

(b) **Euler's Criterion:** If p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$ then:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$$

Proof. Suppose $\left(\frac{a}{p}\right) = 1$ then $\exists x$ such that $x^2 \equiv a \bmod p$. Then observe, $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \bmod p$ by Euler's Theorem/Fermat's Little Theorem they are equal.

Suppose $\left(\frac{a}{p}\right) = -1$. Consider the list $\{1, 2, \cdots, p-1\}$, each is coprime to p and there are an even number of them because p is odd. Suppose $b \in \{1, 2, \cdots, p-1\}$, then consider the equation $bx \equiv a \bmod p$. Since $\gcd(b, p) = 1 \mid a$, $\exists!$ solution. Could $x \equiv b \bmod p$? No because if $b \cdot b \equiv a \bmod p \implies b^2 \equiv a \bmod p$ but then a would be a

QR mod p. Since the solution is not b it is another element in the set $\{1, 2, \cdots, p-1\}$. Thus all of $\{1, 2, \cdots, p-1\}$ pair up to give pairs whose products are a. Thus,

$$\underbrace{(1)(2)\cdots(p-1)}_{\text{Wilson's Theorem}} \equiv a^{(p-1)/2} \bmod p$$

$$a^{(p-1)/2} \equiv -1 \bmod p$$

□

Ex. $\left(\frac{6}{11}\right) = 6^{(11-1)/2} = 6^5 \equiv 10 \equiv -1 \bmod 11$. So 6 is a QNR mod 11. i.e. $x^2 \equiv 6 \bmod 11$ has no solution.

(c) **Theorem:** If p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = \gcd(b,p) = 1$ then:

i. If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. This statements that we can reduce the numerator mod the denominator.

Proof. Clear because $x^2 \equiv a \bmod p$ if and only if $x^2 \equiv b \bmod p$ because $a \equiv b \bmod p$. □

ii. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof. Well,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$$

So $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$ so $p \mid \left[\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right]$ but $p \geq 3$ Since $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ is between -2 and 2 and p divides it, we know that it must be 0. Therefore, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

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

Proof. Obvious. □

(d) **Gauss' Lemma:** Suppose p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Let s be the number of least nonnegative residues in the set

$$\{a, 2a, \cdots, ((p-1)/2)\, a\}$$

which are $> p/2$. Then $\left(\frac{a}{p}\right) = (-1)^s$.

Ex. Consider $\left(\frac{8}{13}\right)$. Note that $\left(\frac{p-1}{2}\right) = \frac{12}{2} = 6$ so look at

$$\{8, 2 \cdot 8, 3 \cdot 8, \cdots, 6 \cdot 8\} \equiv \{8, 3, 11, 6, 1, 9\} \bmod 13$$

Since only three of these are greater than $p/2 = 6.5$ we have $\left(\frac{8}{13}\right) = (-1)^3 = -1$. Thus, 8 is a quadratic nonresidue mod 13.

4. **Two Special Cases**
These will turn out to be really useful after 11.2 and 11.3 .

(a) **Theorem:** Suppose p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Proof. By Euler's Criterion we have,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p$$

If $p \equiv 1 \bmod 4$ then $p = 4k + 1$ for some $k \in \mathbb{Z}$ so:

$$(-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1$$

If $p \equiv 3 \bmod 4$ then $p = 4k + 3$ for some $k \in \mathbb{Z}$ so:

$$(-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1$$

□

(b) **Theorem:** Suppose p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases}$$

Proof. Not obvious as it uses Gauss' Lemma and is lengthy. □

Note: This is equivalent to

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

11.2 Quadratic Reciprocity and Calculation Examples

---

1. **Introduction:** The Law of Quadratic reciprocity establishes that for odd primes p and q there is a connection between when p is a quadratic residue mod q when q is a quadratic residue mod p.

2. **Theorem:** If p, q are odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Proof. Omitted due to length. □

Use for Calculation: Under what circumstances will $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ be identical? We would need $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ to be even. This happens if and only if one of the two is even, say $\frac{p-1}{2}$ is even. That is, $\frac{p-1}{2} = 2k$ for some $k \in \mathbb{Z}$, so $p-1 = 4k$ so $p \equiv 1 \bmod 4$. Thus, for calculation, we get:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if either } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \text{ (or both).} \\ -\left(\frac{q}{p}\right) & \text{if both } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4. \end{cases}$$

3. **Theorem:**
   (a) If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Call this "reducing".
   (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Call this "splitting".
   (c) $\left(\frac{a^2}{p}\right) = 1$. Call this the "square rule".
   (d) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$. Call this the "-1 rule".
   (e) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \bmod 8 \\ -1 & \text{if } n \equiv 3, 5 \bmod 8 \end{cases}$. Call this the "2 rule".

4. **Examples:**
   Ex. Calculate $\left(\frac{48}{29}\right)$:

$$\left(\frac{48}{29}\right) = \left(\frac{19}{29}\right) \text{ by reducing}$$
$$\left(\frac{19}{29}\right) = \left(\frac{29}{19}\right) \text{ by LoQR since } 19 \equiv 1 \bmod 4.$$
$$\left(\frac{29}{19}\right) = \left(\frac{10}{19}\right) \text{ by reducing.}$$
$$\left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right) \text{ by splitting.}$$

Then, we calculate these separately. First $\left(\frac{2}{19}\right) = -1$ by the "2 rule" because $19 \equiv 2 \bmod 8$. Then second,

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) \text{ by LoQR since } 5 \equiv 1 \bmod 4.$$
$$\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) \text{ by reducing.}$$
$$\left(\frac{4}{5}\right) = 1 \text{by square rule.}$$

Thus $\left(\frac{48}{29}\right) = (-1)(1) = -1$.

Ex. Calculate $\left(\frac{105}{1009}\right)$. Note that 105 is not prime so we cannot use the LoQR immediately.

$$\left(\frac{105}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{7}{1009}\right) \text{ by splitting.}$$

Then we calculate these separately. First,

$$\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right) \text{ by LoQR since } 1009 \equiv 1 \bmod 4.$$
$$\left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right) \text{ by reducing}$$
$$\left(\frac{1}{3}\right) = 1$$

Second,

$$\left(\frac{5}{1009}\right) = \left(\frac{1009}{5}\right) \text{ by LoQR since } 1009 \equiv 1 \bmod 4.$$
$$\left(\frac{1009}{5}\right) = \left(\frac{4}{5}\right) \text{ by reducing}$$
$$\left(\frac{4}{5}\right) = 1 \text{ by the square rule}$$

Third,

$$\left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right) \text{ by LoQR since } 1009 \equiv 1 \bmod 4.$$
$$\left(\frac{1009}{7}\right) = \left(\frac{1}{7}\right) \text{ by reducing}$$
$$\left(\frac{1}{7}\right) = 1$$

Thus, $\left(\frac{105}{1009}\right) = (1)(1)(1) = 1$.

11.3 The Jacobi Symbol

---

1. **Introduction:** The Jacobi symbol is a generalization of the Legendre symbol for when the denominator is odd but not necessarily prime. It preserves many of the same useful properties and almost the same meaning.

2. **Definition:** Let n be an odd positive integer with prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and let $\alpha \in \mathbb{Z}$ be coprime to n. Define:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

   Thus the Jacobi symbol is defined in terms of the Legendre symbol.

3. **Theorem:** Assume $\gcd(a, n) = \gcd(b, n) = 1$.

   (a) If $a \equiv b \bmod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

   (b) $\left(\frac{a^2}{n}\right) = 1$

   (c) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

   (d) $\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$

   (e) $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \bmod 8 \\ -1 & \text{if } n \equiv 3, 5 \bmod 8 \end{cases}$

   (f) $\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{m}{n}\right) & \text{if either } m \equiv 1 \bmod 4,\ n \equiv 1 \bmod 4 \\ -\left(\frac{n}{m}\right) & \text{if both } m \equiv 3 \bmod 4 \text{ and } n \equiv 3 \bmod 4 \end{cases}$

Proof. Lots of calculation. $\square$

4. **Question:** We know $\left(\frac{a}{p}\right)$ tells us if a is a QR or QNR mod p. Does $\left(\frac{a}{n}\right)$ tell us if a is a QR or QNR mod n? Well, half-yes.

   Theorem: Suppose $\gcd(a, n) = 1$ and n is an odd prime.

   (a) If a is a QR mod n then $\left(\frac{a}{n}\right) = 1$.

   (b) If $\left(\frac{a}{n}\right) = 1$ then we cannot conclude a is a QR mod n.

   Proof. Suppose a is a QR mod n, then $\exists x$ such that $x^2 \equiv a \bmod n$ has solutions then $n \mid (x^2 - a)$ and so for every p in the prime factorization of n we have $p \mid (x^2 - a)$ and so $x^2 \equiv a \bmod p$ which then tells us that $\left(\frac{a}{p}\right) = 1$. It follows that $\left(\frac{a}{n}\right) = 1$ because $\left(\frac{a}{n}\right)$ is simply a product of 1s. The reverse cannot be guaranteed, for example $x^2 \equiv 2 \bmod 15$ has no solution (can be verified by trial and error). However $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{2}{5}\right) = -1$ and so $\left(\frac{2}{15}\right) = (-1)(-1) = 1$. $\square$

5. **Calculations:** We can then calculate Jacobi symbols essentially as we did with Legendre symbols. The biggest thing to watch out for is making sure that we obey the rules at each step of the calculation.

   Ex. Let's calculate $\left(\frac{1009}{2307}\right)$. We have:

$$\begin{aligned}
\left(\frac{1009}{2307}\right) &= \left(\frac{2307}{1009}\right) && \text{by LoQR since } 1009 \equiv 1 \bmod 4.\\
&= \left(\frac{289}{1009}\right) && \text{by reducing.}\\
&= \left(\frac{1009}{289}\right) && \text{by LoQR since } 1009 \equiv 1 \bmod 4.\\
&= \left(\frac{142}{289}\right) && \text{by reducing.}\\
&= \left(\frac{2}{289}\right)\left(\frac{71}{289}\right) && \text{by splitting.}
\end{aligned}$$

   Then we calculate the first, $\left(\frac{2}{289}\right) = 1$ by the 2 rule, since $289 \equiv 1 \bmod 8$. For the second part,

$$\begin{aligned}
\left(\frac{71}{289}\right) &= \left(\frac{289}{71}\right) && \text{by LoQR since } 289 \equiv 1 \bmod 4.\\
&= \left(\frac{5}{71}\right) && \text{by reducing.}\\
&= \left(\frac{71}{5}\right) && \text{by LoQR since } 5 \equiv 1 \bmod 4.\\
&= \left(\frac{1}{5}\right) && \text{by reducing.}
\end{aligned}$$

Thus, $\left(\frac{1009}{2307}\right) = 1$. We cannot conclude if 1009 is a QR or a QNR mod 2307.

Ex. Let's calculate $\left(\frac{1999}{2315}\right)$. We have:

$$\begin{aligned}
\left(\frac{1999}{2315}\right) &= -\left(\frac{2315}{1999}\right) \text{ by LoQR since } 1999 \equiv 3 \bmod 4 \text{ and } 2315 \equiv 1 \bmod 4. \\
&= -\left(\frac{316}{1999}\right) \text{ by reducing.} \\
&= -\left(\frac{2^2}{1999}\right)\left(\frac{79}{1999}\right) \text{ by splitting.} \\
&= -(1)\left(\frac{79}{1999}\right) \\
&= -\left(-\left(\frac{1999}{79}\right)\right) \text{ by LoQR since } 1999, 79 \equiv 3 \bmod 4. \\
&= \left(\frac{24}{79}\right) \text{ by reducing.} \\
&= \left(\frac{2}{79}\right)^3 \left(\frac{3}{79}\right)
\end{aligned}$$

Then, $\left(\frac{2}{79}\right) = 1$ since $79 = 7 \bmod 8$. Then, $\left(\frac{3}{79}\right) = -\left(\frac{79}{3}\right)$ since $79, 3 \equiv 3 \bmod 4$. Which then becomes $-\left(\frac{1}{3}\right) = -1$ from reducing. Therefore, $\left(\frac{1999}{2315}\right) = -1$ and 1999 is a QNR mod 2315.

11.4 Problems

---

1. Determine, by squaring, which of $1, ..., 16$ are quadratic residues of $p = 17$.
2. Calculate $\left(\frac{3}{17}\right)$ by
   (a) Euler's Criterion
   (b) Gauss's Lemma
3. Prove that if p and $q = 2p + 1$ are both odd primes then -4 is a primitive root of q.
4. Prove that if $p \equiv 1 \mod 4$ is a prime then -4 and $(p-1)/4$ are both quadratic residues of p.
5. Calculate each of the following:
   (a) $\left(\frac{21}{59}\right)$
   (b) $\left(\frac{1463}{89}\right)$
   (c) $\left(\frac{1547}{1913}\right)$
6. Using the Law of Quadratic Reciprocity, show that if p is an odd prime that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 12 \\ -1 & \text{if } p \equiv \pm 5 \mod 12 \end{cases}$$

7. Classify all primes p with $\left(\frac{5}{p}\right) = 1$

8. Calculate each of the following using properties of the Jacobi Symbol, not by raw calculation.

   (a) $\left(\frac{5}{21}\right)$

   (b) $\left(\frac{1009}{2307}\right)$

   (c) $\left(\frac{27}{101}\right)$

9. Categorize all positive integers n which are relatively prime to 15 and for which $\left(\frac{15}{n}\right) = 1$.

10. Show that if $a > 0$ is not a perfect square then there exists a positive integer n such that $\left(\frac{a}{n}\right) = -1$.

8 Cryptography

8.1 Character Ciphers

---

1. **Introduction:** The goal of this entire chapter (and the rest of the course) is to talk about encryption and cryptography.

2. **Terminology:** We have the following:

   (a) *Cryptology*: The study of encryption/decryption.

   (b) *Cryptography*: The study of methods of encryption/decryption.

   (c) *Cipher*: A particular method of encryption.

   (d) *Cryptanalysis*: Breaking of systems of encryption.

   (e) *Plaintext*: The human-readable text we wish to encryp.

   (f) *Encryption*: The process of applying a cipher to plaintext.

   (g) *Ciphertext*: The human-non-readable result.

   (h) *Decryption*: The process of getting the plaintext back.

   (i) *Some Names*:

      i. Alice: encrypts and sends
      ii. Bob: receives and decrypts
      iii. Eve: eavesdropper

3. **Basic Methods:**

   (a) **Character Assignment:** To begin, we will assign a number to each letter of the alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

   Note: For now we will exclude lower-case, punctuation and spaces, but we could include those and use a different modulus.
   Note: This can be confusing since `A` is the first leter of the alphabet and so we would naturally want to assign it to 1. We use this for purposes of making our modular arithmetic easier.

   (b) **Shift Cipher:** For each plaintext letter P we assign ciphertext

$$C \equiv P + b \bmod 26$$

Ex. Encrypt `LEIBNIZ` with $b = 3$.

$$\begin{aligned} L: &\quad P = 11, 11+3 \equiv 14 = C : O \\ E: &\quad P = 4, 4+3 \equiv 7 = C : H \\ I: &\quad P = 8, 8+3 \equiv 11 = C : L \\ B: &\quad P = 1, 1+3 \equiv 4 = C : E \\ N: &\quad P = 13, 13+3 \equiv 16 = C : Q \\ I: &\quad P = 8, 8+3 \equiv 11 = C : L \\ Z: &\quad P = 25, 25+3 \equiv 2 = C : C \end{aligned}$$

Which then results in `OHLEQLC`. To decrypt we simply reverse: $C \equiv P + b \bmod 26$, $P \equiv C - b \bmod 26$.

(c) **Affine Cipher:** Choose a and b and encrypt via $C = aP + b \bmod 26$. How will decryption work? $C \equiv aP + b \bmod 26$, $aP \equiv C - b \bmod 26$ there needs to be a unique P. To have this we need $\gcd(a, 26) = 1$ so that a has a multiplicative inverse. Then $P \equiv a^{-1}(C - b) \bmod 26$. How many choices? $\phi(26) = 12$ for a and 26 choices for b.

Ex. If we choose $a = 5$ and $b = 7$ then encryption is $C \equiv 5P + 7 \bmod 26$ and decryption is $5P \equiv C - 7 \bmod 26 \implies P \equiv 21(C - 7) \bmod 26$ (calculated from 21 being the multiplicative inverse of 5).

4. **Breaking Shift Ciphers:** To break a shift cipher, we only need b. For example, if we manage to find a specific C_0 for a specifice P_0, then we know that $C_0 \equiv P_0 + b \bmod 26$ so $b \equiv C_0 - P_0 \bmod 26$. How might we do this? With frequency analysis.

   Frequency Analysis: In english, the most frequent letter is `E`, note this is $P_0 = 4$. Find the most frequent ciphertext letter. If that is C_0 we guess at that.

5. **Breaking Aphine Ciphers:** One C_0 and P_0 pair is not sufficient! Since knowing $C_0 \equiv aP_0 + b \bmod 26$ is not enough to find a and b. However, having another pair is good enough because:

$$\begin{aligned} C_0 &\equiv aP_0 + b \bmod 26 \\ C_1 &\equiv aP_1 + b \bmod 26 \\ \hline C_0 - C_1 &\equiv a(P_0 - P_1) \bmod 26 \end{aligned}$$

   This will have solutions if and only if $\gcd(P_0 - P_1, 26) \mid C_0 - C_1$, and if so there will be $\gcd(P_0 - P_1, 26)$ solutions.

   Note: Keep in mind this is valid cipher text. There is an a (which Alice chose). So there will be solutions. There may be more than 1. If multiple possible a, for each, find b, simply try all of those a, b combinations until we get proper plaintext.

8.2 Exponentiation Ciphers

---

1. **Introduction:** Can we find a process which is harder to invert?
First we will modify the table of letters slightly: Now, we can put letters together

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

unambigiously. For example `JU` can be assigned to 0920 or just 920. Without the leading 0 it is unclear what something like 111 means. It could be 111 $\implies$ 0111 or 111 $\implies$ 1101.

Fermat's Little Theorem: Recall, if p is prime and $a \in \mathbb{Z}$ with $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

2. **Exponentiation Cipher**

   (a) **Encryption:** Let p be an odd prime (typically very large) and let e be a positive integer with $\gcd(e, p-1) = 1$ (use Euclidean Algorithm for this). We then take the plaintext and group the letters into blocks so no block is larger than p.
   For example,

   - If $p = 29$ then blocksize is 1 since `z` $\leftrightarrow 25 < p$.
   - If $p = 3001$ then blocksize is 2 since `zz` $\leftrightarrow 2525 < p$.
   - If $p = 377173$ then blocksize is 3 since `zzz` $\leftrightarrow 252525 < p$.

   We then pad the plaintext with junk letters at the end if needed so that the plaintext length is a multiple of the blocksize. Traditionally `X` is used but any letter can be used. To encrypt, Alice needs to divide full plaintext into blocks. For each block P we do
   $$C \equiv P^e \bmod p$$

   Ex. Alice wants to encrypt `LOVENOTE` with $(e, p) = (479, 3001)$ and $\gcd(479, 3000) = 1$. So we get `0169 0317 0017 1697` as the ciphertext that Alice would send to

   $$\begin{array}{ccccc} & \texttt{LO} & \texttt{VE} & \texttt{NO} & \texttt{TE} \\ & 1114 & 2104 & 1314 & 1904 \\ & 1114^{479} & 2104^{479} & 1314^{479} & 1904^{479} \\ \hline \equiv & 0169 & 0317 & 0017 & 1697 \end{array}$$

   Bob.

   (b) **Decryption:** This process is invertible since the fact that $\gcd(e, p-1)$ guarantees that there exists some d with $de \equiv 1 \bmod p$. Then for a ciphertext block raised to d:

   $$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k(p-1)} \equiv P(P^{p-1})^k \equiv P(1)^k \equiv P \bmod p$$

   Here the fact that $P^{p-1} \equiv 1 \bmod p$ is guaranteed by FLiT. Note that $p \nmid P$ since $P < p$.

   Thus, to decrypt ciphertext, Bob simply takes C and raises it to d, $C^d \bmod p$.

   Ex. Alice sends cipher text to `2672 0317 1665 2110 0246 1749 0017 2112`

	2672	0317	1665	2110	0246	1749	0017	2112
	2672^{119}	0317^{119}	1665^{119}	2110^{119}	0246^{119}	1749^{119}	0017^{119}	2112^{119}
$\equiv$	1800	2104	2414	2017	1804	1105	1314	2223
	`SA`	`VE`	`YO`	`UR`	`SE`	`LF`	`NO`	`WX`

Bob. She encrypted using Bob's choice of $(e, p) = (479, 3001)$. To decrypt Bob would have to use $e^{-1} = d = 119$. Then, Bob can obviously see the message `SAVE YOURSELF NOW` which is padded with an `X` to make the length a multiple of two characters.

Note: Bob chose $p = 3001$ and $e = 479$ and provided them to Alice so she can send him messages. Two things

- If the two of them keep the p and e secret this is fairly secure.
- Since Alice knows e, she can calculate d. So Alice can decrypt anything else sent to Bob if that specific p and e are used. So Bob would have to use a different p, e with each person.

This is symmetric: knowing $p, e \equiv$ knowing p, d. Is there a way to provide an encryption method so that even if you know how to encrypt you cannot figure out how to decrypt?

8.4 Public Key Encryption and RSA

---

1. **Introduction:** The primary problem with a technique like an exponentiation cipher is that given (p, e) it is easy to find (p, d).

2. **RSA:**

   (a) **Encryption:** Bob picks two distinct large primes p and q and calculated $n = pq$. This will be his modulus. He then chooses e with $\gcd(\phi(n), e) = 1$. Note that $\phi(n) = \phi(pq) = (p-1)(q-1)$ so he can choose an e pretty easily via the Euclidean Algorithm. Bob makes the pair (n, e) publicly avaliable.

   Alice takes her message and breaks it up just like the exponentiation cipher, breaking it into blocks with numerical value not possible more than n. For each plaintext block P, she calculates the ciphertext block as the least nonnegative residue:

   $$C = P^e \bmod n$$

   She then sends all the ciphertext blocks to Bob.

   Ex. Suppose Bob chooses $p = 59$ and $q = 73$. Then $n = (59)(73) = 4307$ and $\phi(n) = (58)(72) = 4176$. He then chooses $e = 7$ with $\gcd(e, \phi(n)) = 1$. Alice wishes to encrypt and send `WORD`. She divides it into blocks of length 2 and does:

   (b) **Decryption:** Since Bob knows $\phi(n) = (p-1)(q-1)$ he can easily find d with $ed \equiv 1 \bmod \phi(n)$. Then for each ciphertext block$C$ he can decrypt by calculating the least nonnegative residue $C^d \bmod n$.

	WO	RD	
	2214	1703	
	2214^7	1703^7	
$\equiv$	3918	1655	mod 4307

Proof. Claim that $C^d \equiv P \bmod n$ because p, q are coprime it suffices to show that $C^d \equiv P \bmod p$ and $C^d \equiv P \bmod q$. Let's show $C^d \equiv P \bmod p$. $C^d \equiv (P^e)^d \equiv P^{ed}$ and $ed = 1 + k\phi(n)$, then

$$P^{ed} \equiv P^1 P^{k\phi(n)} = P(P^{\phi(n)})^k \equiv P(P^{(p-1)(q-1)})^k \equiv P(P^{(p-1)})^{(q-1)k}$$

$$\equiv P(1)^{(q-1)k} \bmod p$$

But we can't guarantee $\gcd(P, p) = 1$ then certainly we get $C^d \equiv P \bmod p$. However, if $\gcd(P, p) \neq 1$ then $p \mid P$ and then, $C^d \equiv (P^e)^d \equiv 0 \equiv P \bmod p$. Together, we see that $C^d \equiv P \bmod p$ always and a similar argument for q gives us $C^d \equiv P \bmod q$ always. Thus,

$$C^d \equiv P \bmod n$$

$\square$

Ex. If Bob receives `1611` from Alice, he has computed $d = 2983$ so $ed = 1 \bmod \phi(n)$. He then does $1611^{2983} \equiv 0704 \bmod 4307$ to receieve `HE` from Alice.

(c) **Security:** If Alice (or Eve) knows (n, e) only, how hard is it to find d? The short answer, no, it's extremely hard. Eve wants d with $ed \equiv 1 \bmod \phi(n)$, to do this she needs to know $\phi(n)$, which means she has to factor n to get $n = pq$ to get $\phi(n) = (p-1)(q-1)$. The issue with this is that factoring seems to be hard. Is it possible that Eve can find $\phi(n)$ without factoring n? Well, if she can factor, then she knows $\phi(n)$. Suppose she knows $\phi(n)$. She also knows n. Observe:

$$p + q = pq - (p-1)(q-1) + 1 = n - \phi(n) + 1$$

$$p - q = \sqrt{(p-q)^2} = \sqrt{(p+q)^2 - 4pq} = \sqrt{(n - \phi(n) + 1)^2 - 4n}$$

Then notice,

$$p = \frac{1}{2}((p+q) + (p-q)) \text{ and } q = \frac{1}{2}((p+q) - (p-q))$$

What all this shows is if we have $n, \phi(n)$ we can get p, q. So, factoring n is equivalently difficult to finding $\phi(n)$.

(d) **Digital Signatures:** Suppose Alice has public key (n_A, e_A) and private key (n_A, d_A) while Bob has public key (n_B, e_B) and private key (n_B, d_B). If Alice wants to send a message to Bob, is there a way to "sign" her message such that Bob knows that she sent it and no one else could have.

Alice takes the plaintext block P and she signs it by doing $S \equiv P^{d_A} \bmod n_A$ (only Alice can do this!). So S is the signed plaintext. Note: Since (n_A, e_A) is public, anyone can do S^{e_A} and get $(P^{d_A})^{e_A} \equiv P \bmod n_A$ so anyone/everyone can verify that it is "signed" by Alice and only Alice. Then she does S^{e_B} to get $C \equiv S^{e_B} \bmod n_B$ this is the encrypted signed plaintext. So in summary,

$$C = \left(P^{d_A} \bmod n_A\right)^{e_B} \bmod n_B$$

To decrypt and unsign it, Bob does

$$P = \left(C^{d_B} \bmod n_B\right)^{e_A} \bmod n_A$$

Note: Alice may need to re-block the text here. This is beause the result of signing a block might result in a signed block with a numerical value larger than Bob's encryption modulus.

8.5 RSA Attacks

---

1. **Introduction:** RSA is (currently) incredibly hard to break. Most methods for breaking the encrpytion are well beyond the scope of this course (technical and physical attacks alike). So for this section the "attacks" we cover are less attacks and more so warnings for users of RSA encryptions to be wary of.

2. **Common Modulus Attack:** Suppose Bob1 and Bob2 use the same n. Suppose for security they use coprime e. Bob1 has (n, e_1) and Bob2 has (n, e_2). Suppose then that Alice wants to send P to both of them (scandalous). Then suppose that Eve intercepts both ciphertexts C_1 and C_2. Remeber that (n, e) are public. Eve knows C_1 and C_2 as well as $C_1 = P^{e_1} \bmod n$ and $C_2 = P^{e_2} \bmod n$. However, she does not know P. Since she can discover that $\gcd(e_1, e_2) = 1$ so $\exists \alpha, \beta$ such that $\alpha e_1 + \beta e_2 = 1$. Then she does:

$$C_1^{\alpha} C_2^{\beta} = (P^{e_1})^{\alpha} (P^{e_2})^{\beta} = P^{\alpha e_1 + \beta e_2} = P^1 \equiv P \bmod n$$

3. **Hastad Broadcast Attack:** This generalizes but the simple version is with three Bobs. Suppose we have Bob1, Bob2, and Bob3 each use $e = 3$ for their encryption exponent, but they all choose pairwise coprime moduli n_1, n_2, and n_3. Suppose then that Alice sends P to all of them;

$$\begin{aligned} C_1 &\equiv P^3 \bmod n_1 \\ C_2 &\equiv P^3 \bmod n_2 \\ C_3 &\equiv P^3 \bmod n_3 \end{aligned}$$

Suppose then that Eve intercepts all of them, and then creates the following system of linear congruences.

$$\begin{aligned} x \equiv C_1 &\equiv P^3 \bmod n_1 \\ x \equiv C_2 &\equiv P^3 \bmod n_2 \\ x \equiv C_3 &\equiv P^3 \bmod n_3 \end{aligned}$$

Then by the Chinese Remainder Theorem she can find a unique solution mod $n_1n_2n_3$. So she has $x \equiv P^3 \bmod n_1n_2n_3$. However, $P < n_1$, $P < n_2$, and $P < n_3$ so in fact $P^3 < n_1n_2n_3$ so we then have $P^3 = x \implies P = \sqrt[3]{x}$. (We know that $P^3 = x$ since x is congruent to P^3 and they have the same bounds of $0 \leq x < n_1n_2n_3$.)

4. **Interception/Resend Attack:** (Burn Your Trash!) Suppose Bob uses public key (n, e) and private key (n, d). Alice wants to send P to Bob so of course she does $C \equiv P^e \bmod n$. Suppose then that Eve intercepts this C, she will then choose r such that $\gcd(r, n) = 1$ and then sends Bob $\bar{C} \equiv Cr^e \bmod n$. Bob then (not knowing that his message has been tampered with) receieves $\bar{C}$ and attempts to decrypt it, finding:

$$(\bar{C})^d \equiv (Cr^e)^d \equiv (P^e r^e)^d \equiv P^{ed} r^{ed} \equiv Pr \bmod n$$

Which is incomprehensible to him so he bins the message, at which point Eve retrieves it and multiplies by r^{-1} to get P.

8.6 Problems

---

1. Given the plaintext `LISTENTOITTWICE`. Encrypt using an affine cipher with $a = 11$ and $b = 8$.

2. Suppose Eve intercepts the message `USWNRSCHISPWRCVSHGKCNSBINMRCNPSDN` sent from Alice to Bob using an affine cipher.

   (a) Use frequency analysis to find the values of a and b. Make your steps clear with explanations.

   (b) Decrypt the message.

3. Use the exponentiation cipher with $p = 3637$ and $e = 71$ to encrypt the message:

   `NEEDBACKUPNOWX`

4. Suppose Bob receives the following ciphertext:

   `1333 0513 0452 0767 2130 1395 1097 3597`

   which he knows Alice encrypted using an exponentiation cipher with $p = 3637$ and $e = 71$.

   (a) Find the least nonnegative residue of the decryption exponent d and make sure it's clear what the modulus is.

   (b) Decode the message.

5. Eve intercepts the following ciphertext from Alice to Bob

   `11,17,00,12,10,24,14,00,13,10,11`

which she knows Alice encrypted using an exponentiation cipher with $p = 29$ and (obviously) using single-character chunks. Eve does not know e or d but she discovered that the first character of the plaintext is `S`.

(a) Write down the discrete logarithm problem that corresponds to the encrypti on of the first character.

(b) It is a fact that the integer $r = 2$ is a primitive root modulo $p = 29$. Use this fact along with index arithmetic to solve for e.
Note: You don't need to write down the entire table of indices for $r = 2$ since you only need two specific values. You can find these by trial-and-error on Wolfram Alpha if you like.

(c) Use e to solve for d.

(d) Use d to decrypt the message.

6. Given:

- Alice: Public key $(e_a, n_a) = (103, 3551)$ and private key $d_a = 2599$.
- Bob: Public key $(e_b, n_b) = (27, 4189)$ and private key $d_b = 1203$.

(a) Suppose Alice wishes to send the following message to Bob, signed and encrypted:

`EVEISLISTENING`

i. Break the plaintext up into two-character strings, padded with an `X` if necessary and assign numerical values.

ii. Sign the text.

iii. Encrypt the signed text.

(b) Suppose Bob receives the following from Alice:

`0502 0684 2713 1962 3755 1695`

i. First decrypt the message. The result is signed and hence still unreadable.

ii. Un-sign the message to reveal the message.

7. Suppose you intercept the following ciphertext from Alice to Bob:

```
160574 069934 062359 171345 116991 061338 246034 232780 197240 238665
264414
062793 213172 090175 151722 269709 259093 194899 145138 280675 059999
147437
```

You know that Bob's public key is $(e, n) = (5201, 288319)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor n, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take.

8. Suppose you intercept the two ciphertext blocks $C_1 = 4280$ and $C_2 = 0330$ sent to Bob1 and Bob2. You know that the Bobs' public keys are $(e_1, n) = (100, 4757)$ and $(e_2, n) = (49, 4757)$. Use a common modulus attack to find P.

9. Suppose you intercept the three ciphertext blocks $C_1 = 1533$, $C_2 = 3561$, and $C_3 = 0835$ sent to Bob1, Bob2, and Bob3. You know that the Bobs' public keys are $(e_1, n) = (3, 5353)$, $(e_2, n) = (3, 5251)$, and $(e_3, n) = (3, 5893)$. Use a Hastad Broadcast Attack to find P.

10. Suppose you intercept the ciphertext block $C = 0156$ sent to Bob. You know that Bob's public key is $(e_B, n_B) = (27, 4189)$ so you choose $r = 888$ with $\gcd(888, 4189) = 1$ and perform an intercept and resend attack as follows:

    (a) Find the $\overline{C}$ you would resend to Bob.

    (b) Bob attempts to decrypt it and gets trash. You retrieve the trash and find it to be 0662. Find the multiplicative inverse of r and use it to find P.

Practice Exams

Exam 1 Sample A

---

1. Write down the prime factorization of 10!.
2. Find the least non-negative residue of $11^{67} \mod 13$.
3. Find all incongruent solutions $\mod 40$, as least non-negative residues, to the following lienar congruence:
$$12x \equiv 28 \mod 40$$
4. Use the Euclidean Algorithm to find $\gcd(390, 72)$ and write this as a linear combination of the two.
5. Use the Chinese Remainder Theorem to find the smallest positive solution to the system:
$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 1 \mod 6 \\ x &\equiv 4 \mod 7 \end{aligned}$$
6. Use mathematical induction to prove that:
$$n! \geq n^3 \text{ for } n \geq 6$$
7. Determine if the following sets are well-ordered or not. You may assume only that $\mathbb{Z}^+$ is well-ordered.
$$\begin{aligned} S_1 &= [0,1] \cap \mathbb{Q} \\ S_2 &= \{1 - 2^k \mid k \in \mathbb{Z}^+\} \end{aligned}$$
8. Use the Fundamental Theorem of Arithmetic (uniqueness of prime factorization) to prove that $\sqrt{2}$ is irrational. Hint: Use contradiction.
9. Suppose $a, b, c, d \in \mathbb{Z}$ with $a \mid c$, $b \mid c$, $d = \gcd(a, b)$, and $d^2 \mid c$. Prove that $ab \mid c$.

Exam 1 Sample B

---

1. (a) Find $\pi(18)$.
   (b) Show that the set $\{\frac{a}{b} \mid a, b \in \mathbb{Z}^+, a > b\}$ is not well-ordered.
   (c) Find how many primes there are, approximately, between one billion and two billion.
2. Find the number of zeros at the end of 1000! with justification.

3. The following are all false. Provide explicit numerical counterexamples.
   (a) $a \mid bc$ implies $a \mid b$ or $a \mid c$.
   (b) $a \mid b$ and $a \mid c$ implies $b \mid c$.
   (c) $3 \mid a$ and $3 \mid b$ implies $\gcd(a, b) = 3$.
4. Simplify $\prod_{j=1}^{n} \left(1 + \frac{2}{j}\right)$. Your result should not have a $\prod$ in it, or any sort of long product.
5. Use Mathematical Induction to prove $2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$ for all integers $n \geq 1$.
6. Find all $n \in \mathbb{Z}$ with $n^2 - 5n + 6$ prime.
7. Suppose p is a prime and a is a positive integers less than p. Find all possibilities for $\gcd(a, 7a + p)$.
8. Use the Fundamental Theorem of Arithmetic to prove that $\sqrt{6}$ is irrational.
9. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$.

Exam 2 Sample A

---

1. Show that 91 is a Fermat Pseudoprime to the base 3. Note that 91 is not prime!
2. Prove that if $n \geq 2$ and $\gcd(6, n) = 1$ then $\phi(3n) = 2\phi(2n)$.
3. Classify all numbers n for which $\tau(n) = 12$.
4. Suppose n is a perfect number and p is a prime such that pn is also perfect. Prove $\gcd(p, n) \neq 1$.
5. Prove that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \bmod ab$ if $\gcd(a, b) = 1$.
6. Suppose that p is prime and $n \in \mathbb{Z}^+$. Prove that $p \nmid n$ iff $\phi(pn) = (p-1)\phi(n)$.
7. (a) Show that 3 is a primitive root modulo 17.
   (b) Find all primitive roots modulo 17.
8. A partial table of indices for 7, a primitive root of 13 is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_7 a$	12	b	8	10	3	7	a	9	4	2	5	6

   (a) Find a and b.
   (b) Use the table to solve the congruence $3^{x-1} \equiv 5 \bmod 13$.
   (c) Use the table to solve the congruence $4x^5 \equiv 11 \bmod 13$.
9. Suppose $\text{ord}_p a = 3$, where p is an odd prime. Show $\text{ord}_p(a + 1) = 6$.
10. Suppose r is a primitive root modulo m, and k is a positive integers with $\gcd(k, \phi(m)) = 1$ Prove r^k is also a primitive root.

Exam 2 Sample B

1. Calculate:
   (a) $\phi(2^3 \cdot 5 \cdot 11^2)$
   (b) $\sigma(200)$
   (c) $\tau(2000)$
2. Use Wilson's Theorem to find the remainder when 16! is divided by 19.
3. Find all n with $\phi(n) = 16$.
4. Show that 25 is a Fermat Pseudoprime to the base 7.
5. An abundant number is a number n with $sigma(n) > 2n$. Prove that there are infinitely many even abundant numbers by finding on eabundant number and by showing that if n is abundant and a prime p satisfies $p \nmid n$ then pn is also abundant.
6. A partial table of indices for 2, a primitive root of 13, is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	a	b	7	6

   (a) Find a and b with justification.
   (b) Use the table to solve the congruence $3^{2x+1} \equiv 9 \bmod 13$.
   (c) Use the table to solve the congruence $7x^5 \equiv 3 \bmod 13$.
7. Prove that if $\text{ord}_n a = hk$ then $\text{ord}_n(a^h) = k$.
8. Let r be a primitive root for an odd prime p. Prove that $\text{ind}_r(p-1) = \frac{1}{2}(p-1)$.
9. Find all positive integers n such that $\phi(n)$ is prime. Explain!
10. Show that if a is relatively prime to m and $\text{ord}_m a = m - 1$ then m is prime.