Introduction to Number Theory

DEPARTMENT OF
MATHEMATICS

Neelam Akula

Spring 2021

Last Updated: March 31, 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 $k+1$

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

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 $a \mid (\alpha b + \beta c)$. $\square$

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 $a \mid c$. $\square$

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 $0 \leq r < b$.

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

$$a = bq_1 + r_1$$

$$a = bq_2 + r_2$$

for $0 \leq r_1 < b$ and $0 \leq r_2 < b$. 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) $\left\{\frac{a}{2} \mid a \in \mathbb{Z}, a \geq 10\right\}$

(d) $\left\{ \frac{2}{a} \,\middle|\, a \in \mathbb{Z}, a > 10 \right\}$

2. Suppose $a, b \in \mathbb{Z}^+$ are unknown. Let $S = \left\{ a - bk \,\middle|\, k \in \mathbb{Z}, a - bk > 0 \right\}$. 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) $\sum\limits_{k=2}^{10} \frac{1}{k^2-1}$

   (b) $\sum\limits_{k=2}^{n} \frac{1}{k^2-1}$

   (c) $\sum\limits_{k=1}^{n} \frac{1}{k^2+2k}$ Hint: $k^2 + 2k = (???)^2 - 1$

5. Find the value of each of the following:

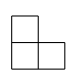
   (a) $\prod\limits_{j=2}^{7} \left(1 - \frac{1}{j}\right)$

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

   (c) $\prod\limits_{j=2}^{n} \left(1 - \frac{1}{j^2}\right)$ 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.

2 Primes and Greatest Common Divisors

2.1 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! $\square$

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 $p_i \mid p_1p_2\cdots p_n$ as well. So $p_i \mid 1$ because $1 = N - p_1p_2\cdots p_n$. This is a contradiction because p_i is a prime which means $p_i > 1$. $\square$

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 $p \mid n$. $\square$

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.

2.2 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.)

2.3 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 $0 \leq r < d$. So then $r = a - dq = a - (\alpha a + \beta b)q = (1 - \alpha q)a - \beta qb$ 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 $c\gcd(a, b) = \alpha ca + \beta cb$ = 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). □

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!

2.4 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 $\beta = -5$.

2.5 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 $a \mid c$. $\square$

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. $\square$

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! $\square$

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! $\square$

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. $\square$

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. $\square$

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). □

2.6 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 $\text{lcm}(a, b)$.

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) $100 \equiv 0 \mod m$

3 Congruences

3.1 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 $a \equiv b \mod m$ and $c \equiv \mod m$ then $a \pm c \equiv b \pm d \mod m$.

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

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

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

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

(b) **Division Issues.** First everything must be an integer, so does $2 \equiv 8 \mod 6 \implies \frac{2}{3} \equiv \frac{8}{3} \mod 6$ this is garbage because $\frac{2}{3}, \frac{8}{3} \notin \mathbb{Z}$. However, is $2 \equiv 8 \mod 6 \implies \frac{2}{2} \equiv \frac{8}{2} \mod 6$ true? No! because $1 \equiv 4 \mod 6$ 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 $ac \equiv bc \mod m$ then $a \equiv b \mod m/\gcd(m, c)$. 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 $ac \equiv bc \mod m$, $\exists k \in \mathbb{Z}$ 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 $\frac{m}{\gcd(\mathrm{c,m})} \Big| a - b$. Therefore, $a \equiv b \mod \frac{m}{\gcd(c,m)}$. □

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

4. **Residue Classes:**

(a) **Introduction:** Suppose we are working $\mod m = 5$. We know $0 \equiv 5 \equiv 10 \equiv -5 \equiv \cdots \mod 5$, we also know $1 \equiv 6 \equiv 11 \equiv -4 \equiv \cdots \mod 5$, 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. $\square$

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

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

3.2 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 $\mid$ 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:

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

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 $ax \equiv b \mod m$ 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. $20x \equiv 15 \mod 65$, gcd(20,65)=5 | 15 so ∃5 incongruent solutions mod 65. The Euclidean Algorithm gives us a solution $x_0 \equiv 56 \mod 65$. So all solutions are then

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

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

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

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

3.3 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.

$$\begin{gathered} x_1 \equiv a_1 \mod m_1 \text{ and } x_2 \equiv a_1 \mod m_1 \\ \vdots \\ x_1 \equiv a_n \mod m_n \text{ and } x_2 \equiv a_n \mod m_n \end{gathered}$$

From here we get,

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

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

Since the m_i are all pairwise coprime, we get

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

Thus, $x_1 \equiv x_2 \mod M$. $\square$

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,

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

3.4 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:
$$\begin{aligned} 2x + 1 &\equiv 3 \mod 10 \\ x + 2 &\equiv 7 \mod 9 \\ 4x &\equiv 1 \mod 7 \end{aligned}$$

4 Special Congruences

4.1 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,

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

□

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. $\square$

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

4.2 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 $n = p_1 p_2 \cdots p_k$ 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 $b^{n-1} \equiv 1 \mod n$. $\square$

4.3 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 $ar_i \equiv ar_j \bmod n$, since $\gcd(a, n) = 1$ we can cancel. So $r_i \equiv r_j \bmod n$. 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,

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

$\square$

4. **Use For Calculation:** To reduce $9^{453} \bmod 16$, 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 $a \bmod n$.

4.4 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 $60 \mid a^4 + 59$.

5 Various Multiplicative Functions

5.1 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. $\square$

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 $1, 2, \cdots, 30$.

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

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 $\phi(mn) = \phi(m)\phi(n)$ □

(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.

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

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, $n = 2^0$.

5.2 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 $F(n) = \sum\limits_{d|n} f(d)$ (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,

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

□

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

5.3 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.

5.4 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}

6 Primitive Roots

6.1 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,

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

$\square$

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

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

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, $\text{ord}_{11} 2 = 10$.

$$2^1 \equiv 2 \not\equiv 1 \text{ mod } 11$$
$$2^2 \equiv 4 \not\equiv 1 \text{ mod } 11$$
$$2^5 \equiv 10 \not\equiv 1 \text{ mod } 11$$

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

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

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

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

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

3. **Primitive Roots**

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

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:

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

  So,

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

- Second observe:

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

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

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

□

(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.

6.2 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:

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

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 $\mathrm{ord}_{17} r = \phi(17) = 16$.
- 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
$\mathrm{ind}_3 a$	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.

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

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:

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

Use the table to "un-index":

$$x \equiv 15, 2 \bmod 17$$

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

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

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

$$\mathrm{ind}_3 x \equiv 6 \bmod 8 \implies \mathrm{ind}_3 x \equiv 6, 14 \bmod 16$$

Now we can "un-index"

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

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

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

$$x \equiv 2 \bmod 4$$

Note: Any of $x = \cdots, -6, -2, 2, 6, \cdots$ works.
Note: Could also give as $x \equiv 2, 6, 10, 14 \bmod 16$ ("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.

6.3 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.

A Practice Exams

A.1 Exam 1 Spring 2020

Note: I have ordered these in terms of what I think is increasing difficulty. You may have other opinions! Remember that this exam will be curved, I do not expect you to finish all the problems in 50 minutes.

1. Write down the prime factorization of 10!.

   Let 10! be written as,

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \times 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \times 5) \\ &= 1 \cdot 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \end{aligned}$$

   Therefore, the prime factorization of 10! is $2^8 3^4 5^2 7$.

2. Find the least non-negative residue of $11^{67} \mod 13$.

   Using Fermat's Little Theorem. Well $13 \nmid 11$ so $11^{12} \equiv 1 \mod 13$. Then $67 = 12(5) + 7$ so,

$$\begin{aligned} 11^{67} = 11^{12(5)+7} = 11^{12^5} 11^7 &\equiv (1)^{10} 11^7 \mod 13 \\ &\equiv 11^7 \mod 13 \\ &\equiv 11 \cdot 1771561 \mod 13 \\ &\equiv 11(-1) \mod 13 \\ &\equiv -11 \mod 13 \\ &\equiv 2 \mod 13 \end{aligned}$$

   So 2 is the least non-negative residue.

3. Find all incongruent solutions $\mod 40$, as least non-negative residues, to the following lienar congruence:

$$12x \equiv 28 \mod 40$$

   Since $\gcd(12, 40) = 4 \mid 28$ there exists a solution. We use the Euclidean Algorithm to solve $12x' + 40y' = 4$. This gives us $12(-3) + 40(1) = 4$, we want a 28 on the right hand side so multiple by 7. We then get $12(-21) + 40(7) = 28$, so $12(-21) \equiv 28 \mod 40$. Therefore, $x_0 \equiv 19 \mod 40$, so all solutions are then

$$x \equiv 19 + 10k \mod 40k, k = 0, 1, 2, 3$$

   That is $x \equiv 19, 29, 39, 9 \mod 40$

4. Use the Euclidean Algorithm to find gcd(390, 72) and write this as a linear combination of the two.

   Using the Euclidean Algorithm we do the following:

$$\begin{aligned} 390 &= 5(72) + 30 \\ 72 &= 2(30) + 12 \\ 30 &= 2(12) + 6 \\ 12 &= 2(6) + 0 \end{aligned}$$

   So the gcd is 6. Now the find the linear combination.

$$\begin{aligned} 6 &= 1(30) - 2(12) \\ &= 1(30) - 2(72 - 2(30)) \\ &= 5(30) - 2(72) \\ &= 5(390 - 5(72)) - 2(72) \\ &= 5(390) - 27(72) \end{aligned}$$

   Where $\alpha = 5$ and $\beta = -27$.

5. Use the Chinese Remainder Theorem to find the smallest positive solution to the system:

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 1 \mod 6 \\ x &\equiv 4 \mod 7 \end{aligned}$$

   Test to see if all m_i are pairwise coprime, $\gcd(5, 6) = \gcd(5, 7) = \gcd(6, 7)$. This means that $M = 210$, $M_1 = 42$, $M_2 = 35$, and $M_3 = 30$.

   Solve for y_1:

$$\begin{aligned} 42y_1 &\equiv 1 \mod 5 \\ 2y_1 &\equiv 1 \mod 5 \\ y_1 &= 3 \end{aligned}$$

   Solve for y_2:

$$\begin{aligned} 35y_2 &\equiv 1 \mod 6 \\ 5y_2 &\equiv 1 \mod 6 \\ y_2 &= 5 \end{aligned}$$

   Solve for y_3:

$$\begin{aligned} 30y_3 &\equiv 1 \mod 7 \\ 2y_3 &\equiv 1 \mod 7 \\ y_3 &= 4 \end{aligned}$$

So we then get

$$x = (2)(42)(3) + (1)(35)(5) + (4)(30)(4) \equiv 907 \mod 210$$

$$x \equiv 67 \mod 210$$

So the least non-negative residue is 67.

6. Use mathematical induction to prove that:

$$n! \geq n^3 \text{ for } n \geq 6$$

Proof.

Base Case:

Let $n = 6$, $n! = 720$ and $6^3 = 216$, $720 \geq 216$ so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some $n \geq 6$. This implies that $n! \geq n^3$.

Inductive Step:

Then consider the equation to $n + 1$:

$$\begin{aligned} (n+1)! &\geq (n+1)^3 \\ (n+1)(n!) &\geq (n+1)^3 \\ (n+1)n^3 &> (n+1)^3 \quad \text{by IH} \\ n^3 &> (n+1)^2 \\ n^3 &> n^2 + 2n + 1 \end{aligned}$$

Which is true for any $n \geq 3$.

Thus for all $n \geq 6$,

$$n! \geq n^3$$

□

7. Determine if the following sets are well-ordered or not. You may assume only that $\mathbb{Z}^+$ is well-ordered.

$$S_1 = [0, 1] \cap \mathbb{Q}$$
$$S_2 = \{1 - 2^k \mid k \in \mathbb{Z}^+\}$$

The set S_1 is not well-ordered because the subset $(0, 0) \cap \mathbb{R}$ has no least element. Likewise, the set S_2 is also not well-ordered because the set itself has no least element.

8. Use the Fundamental Theorem of Arithmetic (uniqueness of prime factorization) to prove that $\sqrt{2}$ is irrational. Hint: Use contradiction.

   Suppose that $\sqrt{2}$ is rational, this means that $\sqrt{2}$ is of the form $\frac{a}{b}$, $a, b \in \mathbb{Z}^+$. Then $2 = \frac{a^2}{b^2}$ so $a^2 = 2b^2$. Because a^2 and b^2 are both squared the prime factorizations of both are even, but $a^2 = 2b^2$ implies there is an odd number of prime factorizations for 2. This contradicts uniqueness of prime factors.

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 $ab \mid c$.

   Given that $a \mid c$, $b \mid c$, and $d^2 \mid c$ given that $d = \gcd(a, b)$ we can *not* conclude that $ab \mid c$. We will show this with a simple contradiction, let $a = 2$, $b = 4$, $c = 4$. We know that $2 \mid 4$ and $4 \mid 4$, it follows that $\gcd(2, 4) = 2^2 \mid 4$ but $ab \nmid c$ because $2 \cdot 4 \nmid 4$ because $8 > 4$. So the statement is false.

A.2 Exam 1 Summer 2016

Note: I've ordered these by difficulty as I perceive it. Your opinion on difficulty might vary, but knowing how I ordered them might help you decide which to do first and which to do last!

1. (a) Find $\pi(18)$.

   We first list the primes up to 18, $\{2, 3, 5, 7, 11, 13, 17\}$. We see that there are 7 primes, therefore $\pi(18) = 7$.

   (b) Show that the set $\{\frac{a}{b} \mid a, b \in \mathbb{Z}^+, a > b\}$ is not well-ordered.

   Since $a > b$ we know a subset $\{\frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \cdots\}$ exists, and it does not have a least element. Since the subset does not have a least element, the set is not well-ordered.

   (c) Find how many primes there are, approximately, between one billion and two billion.

   From section 2.2 we know that for very large x, $\pi(x) = \frac{x}{\ln x}$. So there are, approximately,

$$\frac{2000000000}{\ln(2000000000)} - \frac{1000000000}{\ln(1000000000)}$$

   primes between one and two billion.

2. Find the number of zeros at the end of 1000! with justification.

   Zeros at the end of numbers are from multiples of 10 which are pairs of 2 and 5, so we find the number of pairs of 2's and 5's to find the number of zeros. Let $d_n(x)$ represent the sum of the numbers divisible by all powers of n less than x.

$$d_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$$

$$d_5(1000!) = 200 + 40 + 8 + 1 = 249$$

Thus, there can only be 249 pairs of 2's and 5's, so there are only 249 10's, so there are 249 zeros at the end of (1000!).

3. The following are all false. Provide explicit numerical counterexamples.

   (a) $a \mid bc$ implies $a \mid b$ or $a \mid c$.

   $6 \mid 3 \cdot 4$ but $6 \nmid 3$ and $6 \nmid 4$.

   (b) $a \mid b$ and $a \mid c$ implies $b \mid c$.

   $2 \mid 4$ and $2 \mid 6$ but $4 \nmid 6$.

   (c) $3 \mid a$ and $3 \mid b$ implies $\gcd(a, b) = 3$.

   $3 \mid 6$ and $3 \mid 12$ but $\gcd(6, 12) = 6 \neq 3$.

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.

$$\prod_{j=1}^{n} \left(1 + \frac{2}{j}\right) = \prod_{j=1}^{n} \left(\frac{j+2}{j}\right) = \frac{3}{1} \times \frac{4}{2} \times \cdots \times \frac{n+2}{n} = \frac{(n+2)(n+1)}{2}$$

5. Use Mathematical Induction to prove $2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$ for all integers $n \geq 1$.

Proof.

Base Case:

Let $n = 1$, $2^1 = 2^{1+1} - 2$ is true, so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some $n \geq 1$. This implies that $2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$.

Inductive Step:

Then consider the equation to $n + 1$:

$$\begin{aligned} 2^1 + 2^2 + \cdots + 2^{n+1} &= 2^1 + 2^2 + \cdots 2^n + 2^{n+1} \\ &= 2^{n+1} - 2 + 2^{n+1} \qquad \text{by IH} \\ &= 2^{(n+1)+1} - 2 \end{aligned}$$

Thus for all $n \geq 1$,

$$2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$$

$\square$

6. Find all $n \in \mathbb{Z}$ with $n^2 - 5n + 6$ prime.

   Factor $n^2 - 5n + 6$ out to be of the form $(n-2)(n-3)$. For this polynomial to be prime we need one factor to be ± 1 and the other to be a prime. We have four cases:

   - If $n - 2 = 1 \implies n = 3$ then $n^2 - 5n + 6 = 0$ which is not prime.
   - If $n - 2 = -1 \implies n = 1$ then $n^2 - 5n + 6 = 2$ which is prime.
   - If $n - 3 = 1 \implies n = 4$ then $n^2 - 5n + 6 = 2$ which is prime.
   - If $n - 3 = -1 \implies n = 2$ then $n^2 - 5n + 6 = 0$ which is not prime.

   So the only values of n such that $n^2 - 5n + 6$ is prime is $n = 1, 4$.

7. Suppose p is a prime and a is a positive integers less than p. Find all possibilities for $\gcd(a, 7a + p)$.

   We know that $\gcd(a, 7a + p) = \gcd(a, p)$, but since $a < p$ and the only divisors of p are 1 and p we know that $a \nmid p$, therefore $\gcd(a, p) = 1$.

8. Use the Fundamental Theorem of Arithmetic to prove that $\sqrt{6}$ is irrational.

   Suppose that $\sqrt{6}$ is rational, this means that $\sqrt{6}$ is of the form $\frac{a}{b}$, $a, b \in \mathbb{Z}^+$. Then $6 = \frac{a^2}{b^2}$ so $a^2 = 6b^2$. Because a^2 and b^2 are both squared the prime factorizations of both are even, but $a^2 = 6b^2$ implies there is an odd number of prime factorizations for 2 and 3. This contradicts uniqueness of prime factors.

9. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$.

   Suppose that $a^n \mid b^n$, this implies that $b^n = ka^n$ for some $k \in \mathbb{Z}$. We know that any prime in the prime factorization of k must be to the power of αn. This implies that $k = p_1^{\alpha_1 n} p_2^{\alpha_2 n} \cdots p_i^{\alpha_i n}$ which in turn implies that $k = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i})^n$. From this we know that k is a perfect square, meaning that $\sqrt{k} \in \mathbb{Z}^+$, thus $a\sqrt{k} = b$ and $a \mid b$.

B Symbols and Notation

Logic Notation

- $\exists$ - There exists at least one.
- $\exists!$ - There exists one and one only.
- $\nexists$ - There is no.
- $\forall$ - For all.
- $\neg$ - Logical not.
- $\vee$ - Logical or.
- $\wedge$ - Logical and.
- $\implies$ - Implies.
- $\iff$ - If and only if.
- $\leftrightarrow$ - Equivalence.

Set Notation

- $\mathbb{N}$ - Set of natural numbers.
- $\mathbb{Z}$ - Set of integers.
- $\mathbb{Q}$ - Set of rational numbers.
- $\mathbb{A}$ - Set of algebraic numbers.
- $\mathbb{R}$ - Set of real numbers.
- $\mathbb{C}$ - Set of complex numbers.
- $\in$ - Is member of.
- $\notin$ - Is not member of.
- $\ni$ - Owns.
- $\subset$ - Is proper subset of.
- $\subseteq$ - Is subset of.
- $\supset$ - Is proper superset of.
- $\supseteq$ - Is superset of.
- $\cup$ - Set union.
- $\cap$ - Set intersection.
- $\setminus$ - Set difference.