1 Primes and GCDs

1.1 Pime Numbers

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

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

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

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

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

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

Theorem. There are infinetely many primes.

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

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

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

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

Suppose you started with the number 20 and added multiples of 7. In that resulting list of numbers, how many primes are there? It turns out that under

certain conditions, there are infinitely many! This is stated in Dirichlet's Theorem on Arithmetic Progressions.
Theorem. Suppose $a, b \in \mathbb{Z}$ with gcd(a, b)=1. Then the sequence

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

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

1.2 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.)

1.3 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 $r = a - dq = a - (\alpha a + \beta b)q = (1 - \alpha q)a - \beta q b$ which is a linear combination of a, b. So $r = 0$ so $a = dq$ so $d \mid a$. Likewise, $d \mid b$ (same argument).

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

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

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 $\{\text{mult. of } \gcd(a, b)\} \subset \{\text{linear combinations of } a, b\}$. □

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

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

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

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

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

1.4 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 $\beta = -5$.

1.5 Fundamental Theorem of Arithmetic

We want to work our way up to proving the Fundamental Theorem of Arithmetic. To prove this, we will need a few lemmas.
Lemma. Suppose $a, b, c \in \mathbb{Z}^+$ with $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

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

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

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

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

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

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

Proof. Induction! □

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

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

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

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

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

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

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

We have several consequences of the Fundamental Theorem of Arithmetic.

Related to division:

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

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

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

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

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

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

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

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

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

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

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

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

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

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). □

1.6 Homework