NUMBER THEORY MIDTERM STUDY GUIDE

PHIL MAYER

1. Divisibility and Prime Numbers

Number theory has to do with the natural numbers and the integers: $\mathbb{N} = \{0, 1, 2, \cdots\}$ and $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \cdots\}$ respectively. We may also be interested in $\mathbb{Q}$, the set of ratios of integers. For the most part, the integers have the most interesting properties for our purposes. For example, $\mathbb{Z}$ is closed under addition, subtraction, and multiplication, but isn't closed under division in general. It has cancellation instead, which is almost as nice.

Definition 1.1. For $a, b, c \in \mathbb{Z}$, if $ab = ac$, then a can **cancel**. We are left with $b = c$.

Division does work at times. The notion of divisibility comes up frequently in our theorems and proofs.

Definition 1.2. Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$. Then a **divides** b if and only if $ac = b$ for some $c \in \mathbb{Z}$. We denote this $a \mid b$ and say a is a divisor or factor of b. If a does not divide b, it may be denoted $a \nmid b$.

By the axioms of arithmetic, 0 cannot be a factor for any number other than itself: $\forall x \in \mathbb{Z}, 0 \nmid x$. Also give by basic arithmetic, $\forall x \in \mathbb{Z}, 1 \mid x$ because $1 \cdot x = x$. We should also establish that if $a \mid c$ by $ab = c$, then $b \mid c$ as well. It is also true that if $a \mid c$, then $-a \mid c$. By convention, however, when we talk about a number's set of divisors, we only refer to the positive divisors. Let's now use what we know to prove some theorems:

Theorem 1.3. *"Divides" is a transitive relation. So $\forall a, b, c \in \mathbb{Z}$ with $ab \neq 0$, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.
Assume $a \mid b$ and $b \mid c$. So $\exists x, y \in \mathbb{Z}$ such that $ax = b$ and $by = c$.
So $(ax)y = c \implies a(xy) = c$.
Since $xy \in \mathbb{Z}, a \mid c$. □

Theorem 1.4. *Let $a, b, x, y, d \in \mathbb{Z}$ with $d \neq 0$. If $d \mid a$ and $d \mid b$ then $d \mid ax + by$.*

Proof. Let $a, b, x, y, d \in \mathbb{Z}$ with $d \neq 0$.
Assume $d \mid a$ and $d \mid b$. So $\exists p, q \in \mathbb{Z}$ such that $dp = a$ and $dq = b$.

Now $ax + by = (dp)x + (dq)y = d(px + qy)$.
So $d \mid ax + by$. □

Here $ax + by$ is called a linear combination of a and b. This fact is important: we now know that if d divides a and b, then d divides any linear combination of a and b. The most common uses of this fact are for the linear combinations $a - b$ and $a + b$. Finally, we introduce the set of primes, denoted $\mathbb{P}$.

Definition 1.5. Let $p \in \mathbb{N}$ with $p > 1$. Then p is **prime** if and only if its set of divisors is $\{1, p\}$. Otherwise p is called composite. Note that 0 and 1 are neither prime nor composite.

2. The Well-Ordering Principle

In the last section, we examined what makes $\mathbb{N}$ and $\mathbb{Z}$ special. One of the final properties that is useful on both systems is ordering: we can compare with the symbol $<$, for example.

Theorem 2.1. *(Well-Ordering) Every non-empty subset T of $\mathbb{N}$ has a least element. In other words, if $T \neq \varnothing$ and $T \subset \mathbb{N}$ then $\exists t \in T$ such that $\forall s \in T, t \leq s$.*

For example $T = \mathbb{N}$ has least element 0, $T = 2\mathbb{N} + 1$ (the odd natural numbers) has least element 1, and $T = \mathbb{P}$ has least element 2. Yet $T = \{n \in \mathbb{N} \nmid n^2 < n\}$ has no least element since $\forall n \in \mathbb{N}, n^2 \geq n$, so $T = \varnothing$. On the reals, a set like the unit interval $[0, 1] \subset \mathbb{R}$ does not have Well-Ordering. Even though 0 is its least element, we can choose a subset like $T_0 = (0, 1]$ that has no least element.

Well-Ordering is useful in proofs by contradiction. For example, let's try to prove the following well-known fact. Our proof will use the following lemma, which can be proven by its contrapositive.

Lemma 2.2. If $x, y \in \mathbb{R}$ are positive and if $1 \leq y < x$ then $1 \leq \sqrt{y} < \sqrt{x}$.

Theorem 2.3. *$\sqrt{2}$ is irrational.*

Proof. Assume $\sqrt{(2)}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{N}$ with $a, b \neq 0$.
Let $T = \{k\sqrt{2} \in \mathbb{N} \mid k \in \mathbb{N} \setminus \{0\}\}$.
$T \subset \mathbb{N}$ because we required that $\forall k\sqrt{2} \in T, k\sqrt{2} \in \mathbb{N}$.
$T \neq \varnothing$ because if we take $k = b$, then $b\sqrt{2} = b \cdot \frac{a}{b} = a \in \mathbb{N}$, so $b\sqrt{2} \in T$.
By Well-Ordering, T has a least element $t \in T$. We will contradict this by proving $t(\sqrt{2} - 1) \in T$ is the least element.
Now since $1 < \sqrt{2}$, $0 < \sqrt{2} - 1$.
Additionally, $0 < t$ since $t = k\sqrt{2}$ for some $k \in \mathbb{N}$, $k \neq 0$.
So $0 < t(\sqrt{2} - 1)$, so the condition $t(\sqrt{2} - 1) = k\sqrt{2}$ for some $k \in \mathbb{N} \setminus \{0\}$ is satisfied.
Next, since $t \in T, \exists s \in \mathbb{N} \setminus \{0\}$ such that $t = s\sqrt{2}$ and $s\sqrt{2} \in \mathbb{N}$.
Then $t(\sqrt{2} - 1) = t\sqrt{2} - t = (s\sqrt{2})\sqrt{2} - t = 2s - t$.
But $s \in \mathbb{N}$ and $t \in \mathbb{N}$, so $2s - t \in \mathbb{Z}$. Yet $2s - t = t(\sqrt{2} - 1) > 0$, so $2s - t \in \mathbb{N} \setminus \{0\}$.
Now $t(\sqrt{2} - 1) = t\sqrt{2} - t = t\sqrt{2} - s\sqrt{2} = (t - s)\sqrt{2}$.
But $s, t \in \mathbb{N}$ so $t - s \in \mathbb{Z}$ and $(t - s)\sqrt{2} = t(\sqrt{2} - 1) > 0$.
So $(t - s)\sqrt{2} > 0$, so $t - s > 0 \implies t - s \in \mathbb{N} \setminus \{0\}$.
Overall, we know that $t(\sqrt{2} - 1) > 0$, $t(\sqrt{2} - 1) \in \mathbb{N} \setminus \{0\}$, and $t(\sqrt{2} - 1) = k\sqrt{2}$ for some $k \in \mathbb{N} \setminus \{0\}$.
Then $t(\sqrt{2} - 1) \in T$.
Since $\sqrt{2} < 2$ by our lemma, $\sqrt{2} - 1 < 1 \implies t(\sqrt{2} - 1) < t$.
So $t(\sqrt{2} - 1$ is a smaller element of T than t, so we have a contradiction.
$\therefore$ $\sqrt{2}$ is irrational. □

Overall, Well-Ordering can prove statements of the form $\forall n, p(n)$ by assuming $\exists n \in \mathbb{N}$ such that $\neg p(n)$ and showing that a contradiction arises. In general, we can think of T as a set of counterexamples to a statement. We use its least element to generate a contradiction. Let's do more proofs using Well-Ordering.

Theorem 2.4. *$\forall n > 1$, n is divisible by a prime.*

Proof. Assume otherwise. So $\exists n > 1$ such that n is not divisible by a prime.
So let $T = \{n \in \mathbb{N} \mid n > 1$ and n not divisible by a prime $\}$.
By our hypothesis, $T \neq \varnothing$. Clearly $T \subset \mathbb{N}$.
By Well-Ordering, T has a least element t such that $t > 1$ and t is not divisible by a prime.
By minimality of t, $\forall n < t$ if $1 < n < t$, then $n \notin T$ so n is divisible by a prime.
Case: suppose t is prime. Then $t \mid t$ so t is divisible by a prime, namely itself.
So $t \notin T$: contradiction.
Case: suppose t is composite. Then $t = ab$ for some $a, b > 1$.
So $1 < a < t$ so $a \notin T$ by minimality of T.
So a is divisible by some prime p: $p \mid a$.
But $a \mid t$ so by transitivity, $p \mid t$. So contradiction: t is divisible by a prime.
In both cases, we have a contradiction. So $\forall n > 1, n$ is divisible by a prime. □

The following important corollary is a result of this theorem.

Corollary 2.5. (Euclid's Theorem) There are infinitely many prime numbers.

Proof. Assume not. Then we have a finite list $p_1, p_2, \cdots, p_k$ of primes.
Now consider $n = p_1 p_2 \cdots p_k + 1$.
We know $n > 1$, so by the previous theorem, n is divisible by a prime p.
Since we listed all the primes, $p = p_i$ for some $i \leq k$.
So $p_i \mid n$, but $p_i \mid p_1 p_2 \cdots p_k$ as well.
Since p_i divides both n and $p_1 p_2 \cdots p_k$, it also divides any linear combination of the two.
Then $p_i \mid n - p_1 p_2 \cdots p_k$.
But $n - p_1 p_2 \cdots p_k = 1$. So $p_i \mid 1 \implies p_i = 1$, but $p_i > 1$: contradiction.
$\therefore$ there are infinitely many primes. □

3. Recursion and Induction

We can also use Well-Ordering to prove statements about recursive functions.

Definition 3.1. Recursion is when we define something for each $n \in \mathbb{N}$ with respect to some initial values of n and a description of how to obtain the value at the next n using the previous one(s).

For example, suppose $f(0) = 1$ is chosen as an initial value and we say that $\forall n \geq 0$, $f(n+1) = 2 \cdot f(n)$. We can then prove $\forall n \geq 0, f(n) = 2^n$.

Proof. Suppose not. Then let $T = \{n \in \mathbb{N} \mid f(n) \neq 2^n\}$.
By our hypothesis, $T \neq \varnothing$ and clearly $T \subset \mathbb{N}$.
By Well-Ordering, T has a least element t such that $f(t) \neq 2^t$.
Now $t \neq 0$ since $f(0) = 1$ and $2^0 = 1$. So $t > 0$.
By our recursive formula, $f(t) = 2 \cdot f(t-1)$.
But since $t - 1 < t$ and t was our least element, $t - 1 \notin T$.
Now $f(t-1) = 2^{t-1} \implies f(t) = 2 \cdot 2^{t-1} = 2^t$.
But contradiction: $f(t) \neq 2^t$ and $f(t) = 2^t$. In other words, $t \in T$ and $t \notin T$.
$\therefore \forall n \geq 0, f(n) = 2^n$. □

Another proof, this time about factorials: that $\forall n \geq 4, n! > 2^n$. We first prove it by Well-Ordering, then by induction.

Proof. Assume not: suppose $T = \{n \in \mathbb{N} \mid n \geq 4 \text{ and } n! \leq 2^n\}$.
By our hypothesis, $T \neq \varnothing$. It is clear that $T \subset \mathbb{N}$.
By Well-Ordering, T has a least element t such that $t \geq 4$ and $t! < 2^t$.
Now $4! = 24$ and $2^4 = 16$ so $4 \notin T \implies t > 4$.
Recall $t! = t(t-1)!$ but since $t > 4$, $t - 1 \geq 4$ so it's still relevant to our claim.
Since $t - 1 < t$, $t - 1 \notin T$. So $(t-1)! > 2^{t-1}$.
But since $t! = t(t-1)! > t \cdot 2^{t-1} < 4 \cdot 2^{t-1}$ since $t > 4$ and $4 \cdot 2^{t-1} = 2^{t+1} > 2^t$.
So contradiction: $t! \leq 2^t$. □

Proof. Base case: consider $n = 4$. Since $4! = 24 > 2^4 = 16$, $4! > 2^4$.
Inductive hypothesis: assume for some $n \geq 4$ that $n! > 2^n$.
Inductive step: we want to show $(n+1)! > 2^{n+1}$.
Now $(n+1)! = (n+1) \cdot n! > (n+1) \cdot 2^n > 2 \cdot 2^n = 2^{n+1}$.
So $(n+1)! > 2^{n+1}$.
Therefore by induction, $\forall n \geq 4, n! > 2^n$. □

In our inductive proof, we used one base case and an inductive step to show that the hypothesis was true for all valid natural numbers. In some circumstances, multiple base cases are needed. The main reason is that the recursive formula relevant to the problem

uses multiple base cases. For example, we might have multiple base cases in proofs about the Fibonacci sequence. Let's do some examples to bound the Fibonacci sequence above and below.

Theorem 3.2. *$\forall n \geq 3$, we can bound the Fibonacci sequence above by $F_n \leq 2^{n-2}$.*

Proof. Base cases: consider $n = 3$ and $n = 4$.
Now $F_3 = 2 = 2^{3-2}$ and $F_4 = 3 < 2^{4-2} = 4$ so $F_4 \leq 2^{4-2}$.
Inductive hypothesis: assume for some $n \geq 3, F_n \leq 2^{n-2}$ and $F_{n+1} \leq 2^{(n+1)-2} = 2^{n-1}$.
Inductive step: we want to show that $F_{n+2} \leq 2^{n+2-2} = 2^n$.
Well $F_{n+2} = F_n + F_{n+1} \leq 2^{n-2} + 2^{n-1} < 2^{n-1} + 2^{n-1} = 2^n$.
Therefore by induction, $\forall n \geq 3, F_n \leq 2^{n-2}$. □

Theorem 3.3. *$\forall n \geq 3$, we can bound the Fibonacci sequence below by $F_n \geq 2^{\frac{n-1}{2}}$.*

Proof. Base cases: consider $n = 3$ and $n = 4$.
Now $F_3 = 2 \geq 2^{(3-1)/2} = 2$ and $F_4 = 3 \geq 2^{(4-1)/2} = 2 \cdot \sqrt{2} \approx 2.8$.
Inductive hypothesis: assume for some $n \geq 3, F_n \geq 2^{\frac{n-1}{2}}$ and $F_{n+1} \geq 2^{\frac{n}{2}}$.
Inductive step: we want to show that $F_{n+2} \geq 2^{\frac{n+1}{2}}$.
Well $F_{n+2} = F_n + F_{n+1} > 2^{(n-1)/2} + 2^{n/2} > 2^{(n-1)/2} + 2^{(n-1)/2} = 2 \cdot 2^{(n-1)/2} = 2^{\frac{n+1}{2}}$.
Therefore by induction, $\forall n \geq 3, F_n \geq 2^{\frac{n-1}{2}}$. □

4. The Division Algorithm

Theorem 4.1. *(Division Algorithm) Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$. We call q the quotient and r the remainder of the division.*

Proof. (Existence)
Consider $T = \{a - bq \mid q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$, the set of remainders.
By definition, $T \subset \mathbb{N}$. But why is $T \neq \varnothing$?
If $a \geq 0$, choose $q = -a$. Then $a - bq = a + ba \geq 0$. So in this case $a - bq \in T$.
If $a < 0$, choose $q = a$. Then $a - bq = a - ba = a(1 - b)$.
Since $b > 0$ and $b \in \mathbb{Z}$, $b \geq 1$. So $-b \geq -1$.
Then $1 - b \geq 1 - 1 = 0$, but $a < 0$ so $a(1 - b) \geq a \cdot 0 = 0$.
So in this case $a - bq = a(1 - b) \in T$.
Then by Well-Ordering, T has a least element r. We want to show $r - b \in T$ is smaller.
Since $r \in T$, we can choose $q \in \mathbb{Z}$ such that $r = a - bq$, and we have $r \geq 0$.
So $a = bq + r$ and we want to show $r < b$.
If $r \geq b$, then $r \geq b > 0$ and $0 \leq r - b = a - bq - b = a - b(q + 1)$.
But $r - b \geq 0$ and has form *dividend* $-$ *quotient* $\cdot$ *divisor*, so $r - b \in T$.
Yet $r - b < r$, the smallest element of T. So we have a contradiction.
Therefore $r < b$ and we found unique integers $q, r \in \mathbb{Z}$. □

Proof. (Uniqueness)
Suppose $a = bq + r$ and $a = bq' + r'$ where $0 \leq r < b$ and $0 \leq r' < b$.
So $bq + r = bq' + r' \implies bq - bq' = r' - r \implies b(q - q') = r' - r$.
Then $b \mid (r' - r)$. Do we have bounds on $r' - r$ knowing $0 \leq r < b$ and $0 \leq r' < b$?
Now $0 \leq r < b \implies 0 \geq -r > -b$. So $-b < -r \leq 0$ and $-b < r' - r < b$.
Since $(r' - r) \mid b$, $r' - r$ is a multiple of b between $-b$ and b, namely 0. So $r' = r$.
Then since we had $b(q - q') = r' - r = 0$ and $b > 0$, $q - q' = 0 \implies q' = q$.
$\therefore$ r, q are unique. □

So when we run the division algorithm, we are looking for q such that bq is below a. Our value of r then makes up for the difference. For example, for $a = 100, b = 12$, our quotient and remainder would be $q = 8$ and $r = 4$.

5. The Greatest Common Divisor

Definition 5.1. Let $a, b \in \mathbb{Z}$ not both 0. Then the **greatest common divisor** of a and b, denoted $\gcd(a, b)$ is the largest divisor of both a and b. If $d = \gcd(a, b)$ then $d \mid a, d \mid b$, and $\forall c \in \mathbb{N}$ if $c \mid a$ and $c \mid b$ then $c \leq d$.

We know that the greatest common divisor of two numbers (both nonzero) exists because $1 \in \{$ divisors of $a\} \cap \{$ divisors of $b\}$. Additionally, since $d \mid a$ and $d \mid b$, $d \leq |a|$ and $d \leq |b|$, so there are only finitely many common divisors. The following ideas are crucial in studying the greatest common divisor.

Definition 5.2. a and b are relatively prime if and only if $\gcd(a, b) = 1$.

Theorem 5.3. *Let $a, b \in \mathbb{Z}$ not both 0. Then $\exists x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. Furthermore, $\gcd(a, b)$ is the least positive linear combination of a and b.*

First we will show that the least positive linear combination of a and b, called d, has the property that $d \leq \gcd(a, b)$.

Proof. Let $T = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$.
We previously showed that $T \neq \varnothing$ because $a^2 + b^2 \in T$.
By Well-Ordering, T has a least element d. So choose $x, y \in \mathbb{Z}$ such that $d = ax + by$.
We know $d > 0$, so we just want to show $d = \gcd(a, b)$.
By the division algorithm, $a = dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$.
So $r = a - dq = a - (ax + by)q = a - axq - byq = a(1 - xq) + b(-yq)$.
Then r is a linear combination of a and b and $0 \leq r < d$.
If $r > 0$, then $r \in T$, the set of positive linear combinations of a and b.
But $r < d$, the smallest element of T, which is a contradiction.
So $r = 0$ and $a = dq$, so $d \mid a$. A similar argument shows $d \mid b$.
Then d is a common divisor of a and b, so $d \leq \gcd(a, b)$. □

Now we show $d = \gcd(a, b)$.

Proof. Suppose $d = ax + by$ as before.
Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, the greatest common divisor divides any linear combination of a and b.
In particular, $\gcd(a, b) \mid d$.
Since $d > 0$, we must have $\gcd(a, b) \leq d$.
$\therefore \gcd(a, b) = d$. □

Corollary 5.4. Let $a, b \in \mathbb{Z}$ not both 0. If c is a divisor of a and b, then $c \mid \gcd(a, b)$.

Proof. We know $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.
Since $c \mid a$ and $c \mid b$, c divides any linear combination of a and b.
So $c \mid ax + by \implies c \mid \gcd(a, b)$. □

Note that our definition of the greatest common divisor only said that the g.c.d. was the biggest divisor under $\leq$. This corollary tells us that the g.c.d. is the biggest divisor under the relation $|$ as well. Some additional important theorems follow.

Theorem 5.5. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $\gcd(a, b) = 1$. If $a \mid bc$ then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, pick $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
So $acx + bcy = c$.
Then we have $a \mid acx$ and by our hypothesis $a \mid bc$, so $a \mid bcy$.
Then $a \mid acx + bcy \implies a \mid c$. □

But what if $\gcd(a, b) \neq 1$? We can attempt to modify our proof, multiplying through by $\frac{c}{\gcd(a,b)}$. We would get the equation:

$$\frac{cx}{\gcd(a, b)}a + \frac{cy}{\gcd(a, b)}b = c$$

But $a \mid \frac{cx}{\gcd(a,b)}a$ is not guaranteed: $\frac{cx}{\gcd(a,b)} \notin \mathbb{Z}$ in general.

We can also extend the notion of the greatest common divisor to that of more than two natural numbers. One potential extended definition of the g.c.d. might look like:

Definition 5.6. Let $a_1, a_2, \cdots, a_k \in \mathbb{Z}$ not all 0. The greatest common divisor of the sequence, denoted $\gcd(\{a_1, a_2, \cdots, a_k\})$ is the greatest positive d that is a common divisor of all the a_i. Equivalently, $d > 0, \forall i, d \mid a_i$, and if $c \mid a_i$, then $c \leq d$.

Our previous proofs can be adapted to show that d is the least positive linear combination of the $a_1, a_2, \cdots, a_k$, and that if c divides $a_1, a_2, \cdots, a_k$, then c divides $\gcd(\{a_1, a_2, \cdots, a_k\})$. Back to considering the less general case of $\gcd(a, b)$, the following theorem often proves useful.

Theorem 5.7. *Let $a, b \in \mathbb{Z}$ not both 0. Set $d = \gcd(a, b)$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

So for example, $\gcd(12, 66) = 6$ and $\gcd(\frac{12}{6}, \frac{66}{6}) = \gcd(2, 11) = 1$. Since the g.c.d. is the greatest common divisor of a and b, then $\frac{a}{d}$ and $\frac{b}{d}$ share no common factors except 1.

Proof. We know $d = ax + by$, so $1 = \frac{a}{d}x + \frac{b}{d}y \implies 1$ is a linear combination of the two fractions, which reduce to integers since $d \mid a$ and $d \mid b$.
By one of our previous theorems, the g.c.d. is the least positive linear combination of the two numbers, and we found an x, y that made our linear combination equal to the least positive natural number: 1.
$\therefore \gcd(\frac{a}{d}, \frac{b}{d}) = 1$. □

6. Linear Diophantine Equations

Definition 6.1. Let $a, b, c \in \mathbb{Z}$ with a, b not both 0. Then $ax + by = c$ is called a **linear Diophantine equation**. In general, **Diophantine equations** only allow their variables to take on integer values. Sometimes we allow for rational values, but for the most part we are interested in finding integer solutions.

Solutions (x, y) to linear Diophantine equations exist if and only if $\gcd(a, b) \mid c$. If we are able to find one solution (x_0, y_0), then we can use it to generate infinite equations. The trick is the following:

$$c = ax_0 + by_0 = ax_0 + (ab - ab) + by_0$$

We can also add and subtract infinitely many multiples of ab:

$$c = ax_0 + by_0 = ax_0 + tab - tab + by_0 = a(x_0 + tb) + b(y_0 - tb)$$

Putting this all together and rearranging this final equation, we have the following useful theorem.

Theorem 6.2. *Let $a, b, c \in \mathbb{Z}$ with a, b not both 0. Then the equation $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$. Furthermore, given an initial solution (x_0, y_0), there are infinitely many solutions given by $x = x_0 + \frac{b}{\gcd(a,b)}t, y = y_0 - \frac{a}{\gcd(a,b)}t$ for parameter $t \in \mathbb{Z}$.*

Proof. If $ax + by = c$ has a solution then it is easy to show that $\gcd(a, b) \mid c$ because $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b \implies \gcd(a, b) \mid ax + by$, a linear combination of a and b.
Conversely, if $\gcd(a, b) \mid c$ then $c = k \gcd(a, b)$ for some $k \in \mathbb{Z}$.
So $\exists u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$.
Then $c = k \gcd(a, b) = a(ku) + b(ky)$, so a solution exists, namely $(x_0, y_0) = (ku, ky)$.
We claim that all other solutions are given by the formula in the above theorem.
So $ax + by = a(x_0 + \frac{b}{\gcd(a,b)}t) + b(y_0 - \frac{a}{\gcd(a,b)}t)$.
Expanded out, $ax + by = ax_0 + \frac{ab}{\gcd(a,b)}t - \frac{ab}{\gcd(a,b)}t + by_0 = ax_0 + by_0 = c$.
We claim that these are the only solutions.
Let (x_0, y_0) denote our original solution and suppose we have a second solution (x^*, y^*).
Case: suppose $a = 0$ or $b = 0$.
Assume without loss of generality that $a = 0$.
Then $by_0 = c$ and $by^* = c$, so $y^* = y_0$.
But how can we relate x_0 and x^*? There appears to be no immediate relation, but we know some information about t.
We want to find what values of $t \in \mathbb{Z}$ satisfy $y^* = y_0 - \frac{a}{\gcd(a,b)}t$.
Since $a = 0$, any value of t gives $y^* = y_0$. We want to find what values of t then satisfy $x^* = x_0 + \frac{b}{\gcd(a,b)}t$.
We can simplify this to $x^* = x_0 + t$ since $\gcd(a, b) = b$ and then take $t = x - x_0$.
So we have a value of t that satisfies both equations: $x = x_0 + (x - x_0)$.

Case: suppose $a \neq 0$ or $b \neq 0$.
Then since $ax_0 + by_0 = c$ and $ax^* + by^* = c$, we have $ax_0 + by_0 = ax^* + by^*$.
Rearranging, $a(x^* - x_0) = b(y_0 - y^*)$.
Now a and b have a common factor, namely $\gcd(a, b)$. Dividing out both sides, we have:

$$\frac{a}{\gcd(a,b)}(x^* - x_0) = \frac{b}{\gcd(a,b)}(y_0 - y^*)$$

But $\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)} \in \mathbb{Z}$ and $\frac{a}{\gcd(a,b)} \mid (\frac{b}{\gcd(a,b)})(y_0 - y^*)$.
By one of our previous theorems, $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.
So $(\frac{a}{\gcd(a,b)}) \mid (y_0 - y^*)$.
Choose $t \in \mathbb{Z}$ such that $\frac{a}{\gcd(a,b)}t = y_0 - y^* \implies y^* = y_0 - \frac{a}{\gcd(a,b)}t$.
We want to see if this value of t satisfies the other equation relating x^* and x_0.
Since $\frac{a}{\gcd(a,b)}(x^* - x_0) = \frac{b}{\gcd(a,b)}(y_0 - y^*)$, we have:

$$\frac{a}{\gcd(a,b)}(x^* - x_0) = \frac{b}{\gcd(a,b)}\Big(\frac{a}{\gcd(a,b)}t\Big)$$

Canceling, we see that $x^* - x_0 = \frac{b}{\gcd(a,b)}t \implies x^* = x_0 + \frac{b}{\gcd(a,b)}t$.
So we have a valid value for t in this case as well. □

7. The Euclidean Algorithm

Expressing the solutions to a linear Diophantine equation is clearly dependent on finding an initial solution (x_0, y_0). We want to find a systematic approach to finding such an ordered pair, if it exists. The process is relatively simple: given a solvable linear Diophantine equation of the form $ax + by = c$, we want to find values of $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$. We can then multiply both sides of the equation by some value of $k \in \mathbb{Z}$ such that $a(ku) + b(kv) = k \gcd(a, b) = c$.

This process is not necessary efficient by itself. We need efficient ways to find both $\gcd(a, b)$ and the necessary values of u, v. Fortunately, we can use the Euclidean algorithm and the Extended Euclidean algorithm to solve each problems, respectively.

Theorem 7.1. *(Euclidean Algorithm) For $a, b \in \mathbb{Z}$ not both 0, we can find $\gcd(a, b)$ by the following process: first, divide a by b to get $a = bq_0 + r_0$ where $q_0, r_0 \in \mathbb{Z}$, $0 \leq r_0 < b$ by the division algorithm. Then divide b by r_0 to get $b = r_0q_1 + r_1$ given similarly by the division algorithm. Continue dividing the divisor r_{i-1} by the remainder r_i of each division until the remainder is 0. The previous remainder is equal to $\gcd(a, b)$.*

In order to solve the second problem of finding values of u, v such that $au + bv = \gcd(a, b)$, we can use the following theorem:

Theorem 7.2. *(Extended Euclidean Algorithm) For two integers a, b not both 0, we can find values of $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$ where possible by running the Euclidean algorithm many times and solving each intermediate equation (given by the division algorithm) for the remainder. We can then combine the equations, solving for $\gcd(a, b)$ in terms of a and b.*

We should now prove the correctness of the Euclidean algorithm. To do so, we will need the following lemmas:

Lemma 7.3. Let $a, b \in \mathbb{Z}$ with $b > 0$. Let r be the remainder from dividing a by b. Then for some $c \in \mathbb{Z}$, $c \mid a$ and $c \mid b$ if and only if $c \mid b$ and $c \mid r$.

Proof. By the division algorithm, we have $a = bq + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < b$.
If $c \mid a$ and $c \mid b$ then we know $cx = a$ and $cy = b$, so $a - bq = c(x - yq)$.
Then $c \mid a - bq = r$, so $c \mid b$ and $c \mid r$.
If $c \mid b$ and $c \mid r$, then c divides any linear combination of the two, namely $bq - r = a$.
Then $c \mid a$ and $c \mid b$. □

Lemma 7.4. (Special case of the first lemma) If $a = bq + r$ with $0 \leq r < b$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. The first lemma says that the set of common divisors of a equals the set of common divisors of b.

Since the two sets are equal, their largest values (the greatest common divisors) are equal. So $\gcd(a, b) = \gcd(b, r)$. □

Theorem 7.5. *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. Then the Euclidean algorithm on (a, b) terminates after at most b divisions, returning* $\gcd(a, b)$.

Proof. Assume otherwise. Then $\exists a, b \in \mathbb{Z}$ such that $a \geq b > 0$ yet Euclid(a, b) either doesn't terminate, terminates after more than b divisions, or terminates but does not return $\gcd(a, b)$.
Consider $T = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}$ with $0 < n \leq m$ and any one of the failure conditions is satisfied $\}$.
So T is the set of all second coordinates of a counterexample pair.
Since counterexamples exist by our assumption, $T \neq \varnothing$.
Since $T \subset \mathbb{N}$, we can pick a least element $b \in T$ by Well-Ordering. In this case, b is the least second coordinate of any counterexample pair.
Since $b \in T$, choose a corresponding a with $0 < b \leq a$ and any one of the three failure conditions satisfied for Euclid(a, b).
Run Euclid(a, b) once: so we have $a = bq + r$ for $0 \leq r < b$.
Case: suppose $r = 0$. Then we stop and return b.
Since we terminate in this case, the first possibility is false.
Since $1 \leq b$, the second is false.
We returned b, and since $r = 0$, $a = bq$. So $b \mid a \implies \gcd(a, b) = b$.
So we have a contradiction in this case.
Case: suppose $r > 0$. Then run Euclid(b, r).
Since $r < b$ and b was the least second coordinate of a counterexample pair, r is not the second coordinate of any counterexample.
So Euclid(b, r) runs as anticipated: it terminates in at most r divisions with $\gcd(b, r)$.
Overall, our call to Euclid(a, b) did one division then ran Euclid(b, r) which terminated.
So Euclid(a, b) terminated.
Since Euclid(a, b) did one division and Euclid(b, r) ran k divisions for $k \leq r$, we ran $1 + k \leq 1 + r \leq 1 + (b - 1) = b$ divisions at most.
Finally, Euclid(a, b) returned the result of Euclid(b, r), namely $\gcd(b, r)$.
By our second lemma, $\gcd(a, b) = \gcd(b, r)$.
So we have a contradiction in both cases. □