MATH406 Notes

Nyx

February 13, 2026

1 Intro

Number theory is mostly about the properties of integers

We will preemptively assume the entirety of set theory and the basics of lin alg.

Textbook: Divisibility

2 Lecture 1

2.1 2.1 - Divisibility

We can add/subtract/multiply integers to get integers (eg prop of field, closed).

Definition: Let a, b be integers, $b \neq 0$. We say that b divides a (denoted $b|a$) if there exists an integer k such that $a = bk$.

Additionally,

- If b does not divide a, we write $b \nmid a$.

- When $d|a$, we say that a is a multiple of d and that d is a divisor (or factor) of a.

- For any nonzero integer d we have $d|0$ since $0 = d \cdot 0$.

- We never consider division by zero, so $0|a$ is not defined.

<u>Convention:</u> When we talk about the set of divisors of a positive integer, we mean the set of positive divisors. For instance, the divisors of 6 are 1,2,3,6 (not -1,-2,-3,-6).

Proposition: Let a, b, c integers. Then $a|b$ and $b|c$ implies $a|c$.

Proof: Since $a|b$, there exists an integer k such that $b = ak$. Since $b|c$, there exists an integer l such that $c = bl$. Thus,

$$c = bl$$
$$= (ak)l$$
$$= a(kl)$$

Since kl is an integer under field closure, we have $a|c$. $\qquad\square$

Definition: A linear combination of integers is an expression of the form $ax + by$ where x, y are integers.

"A divisor of both a and b is a divisor of any linear combination of a and b."

Proposition: Bilinearity of division; that is, $d|ax + by$ if $d|a$ and $d|b$.

Proof: Since $d|a$, there exists an integer k such that $a = dk$. Since $d|b$, there exists an integer l such that $b = dl$. Thus,

$$ax + by = (dk)x + (dl)y$$
$$= d(kx) + d(ly)$$
$$= d(kx + ly)$$

Since $kx + ly$ is an integer under field closure, we have $d|ax + by$. $\qquad\square$

Corollary: Suppose a, b, d are integers. Then, if $d|a$ and $d|b$ then $d|(a - b)$ and $d|(a + b)$.

Proof: Let $x = 1$ and $y = -1$ in the previous proposition to get $d|(a - b)$. Let $x = 1$ and $y = 1$ to get $d|(a + b)$. $\qquad\square$

2.2   2.2 - Euclid's Theorem

Definition: A <u>prime number</u> is an integer $p \geq 2$ whose only positive divisors are 1 and p itself. An integer $n \geq 2$ that is not prime is called <u>composite</u>.

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

3   Lecture 2

Proof of Euclid's Theorem: Suppose there are finitely many primes $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 p_3 \cdots p_n + 1$$

Then Q is either prime or composite. If Q is prime, then Q is a prime not in our list. If Q is composite, then Q has a prime divisor p. Since p divides the product $p_1 p_2 \cdots p_n$, it follows that p does not divide $Q - p_1 p_2 \cdots p_n = 1$. Thus, p is not in our list of all primes. In either case, we have a contradiction. Therefore, there are infinitely many primes. $\qquad\square$

3.1   2.4 - The Sieve of Eratosthenes

Theorem (Sieve of Eratosthenes): To find all primes less than or equal to a given integer $n \geq 2$, we can use the following algorithm:

1. Write down all integers from 2 to n.

2. Start with the first number p in the list (which is 2). Circle p and cross out all multiples of p greater than p.

3. Find the next number in the list that is not crossed out. If there is no such number, stop. Otherwise, let p be this new number and repeat step 2.

4. When the algorithm stops, the circled numbers are all the primes less than or equal to n.

Proof: Let p be any prime less than or equal to n. When we reach step 2 with this value of p, we circle it since it has not been crossed out (as it is prime). Thus, all primes less than or equal to n are circled when the algorithm stops. $\qquad\square$

4 Lecture 3

4.0.1 2.5 - The Division Algorithm

Consider the grade school long division problem. We want to do, for instance, 95 divided by 7. We can write

$$95 = 7 \cdot 13 + 4$$

Theorem (The Division Algorithm): Let $a, b \in \mathbb{Z}$ and $b > 0$. Then $\exists ! q, r \in \mathbb{Z}$ st

$$a = bq + r \quad \text{with} \quad 0 \le r < b$$

Note that if $b > a$ then $r = a$ and $q = 0$.

Proof: (Existence) Let q be the largest integer such

$$q \le \frac{a}{b} < q + 1$$

Then $bq \le a < bq + b$. and so $0 \le a - bq < b$. Let $r = a - bq$. Then $a = bq + r$ with $0 \le r < b$.

(Uniqueness) Suppose there exist q', r' such that

$$a = bq' + r' \quad \text{with} \quad 0 \le r' < b$$

Then

$$bq + r = bq' + r'$$
$$b(q - q') = r' - r$$

If $q \ne q'$, then $|b(q - q')| \ge b$ since $|q - q'| \ge 1$. But $|r' - r| < b$ since both r and r' are between 0 and b. This is a contradiction. Thus, $q = q'$, which implies $r = r'$. □

Example:

1. For $a = 100, b = 9$, we have $100 = 9 \cdot 11 + 1$.

2. For $a = -100, b = 9$, we have $-100 = 9 \cdot (-12) + 8$.

Corollary: $a|b$ iff the remainder when b is divided by a is 0.

Proof: Let $b = aq + r$ by the division algorithm. If $r = 0$, then $b = aq$ and so $a|b$. Conversely, if $a|b$, then $b = ak$ for some integer k. By the uniqueness part of the division algorithm, we must have $q = k$ and $r = 0$. □

4.0.2 2.6 - The GCD

Fact: If you have a nonzero integer a, then it has finite divisors by the well-ordering principle. (eg there are only finitely many positive integers less than or equal to $|a|$, and thus finite candidates for divisors).

Definition (GCD): Let a, b be integers, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.

Example:

- $\gcd(12, 15) = 3$

- $\gcd(0, 5) = 5$

- $\gcd(0, 0)$ is not defined.

Definition (Relatively Prime): Two integers are relatively prime if their gcd is 1.

Example:

- $\gcd(8, 15) = 1$ so 8 and 15 are relatively prime.

- $\gcd(9, 28) = 1$ so 9 and 28 are relatively prime.

- $\gcd(0, 1) = 1$ so 0 and 1 are relatively prime.

Corollary: $gcd(p, n) = 1 \iff p \nmid n$.

Proof: If $\gcd(p, n) = 1$, then the only positive divisor of both p and n is 1. Thus, p does not divide n. Conversely, if $p \nmid n$, then the only positive divisor of both p and n is 1, so $\gcd(p, n) = 1$. $\qquad\square$

5 Lecture 4

Last time, we defined the GCD.

Proposition (2.10): Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then,

$$\gcd(\frac{a}{d}, \frac{b}{d}) = 1$$

Proof: Recall that the gcd is defined to be at least 1, always. We will prove that

$$\gcd(\frac{a}{d}, \frac{b}{d}) \leq 1$$

To do this, we will show that any common divisor of $\frac{a}{d}$ and $\frac{b}{d}$ is ≤ 1.

Suppose that for some positive integer c, $c | \frac{a}{d}$ and $c | \frac{b}{d}$. By def of divisibility we thus have that $\frac{a}{d} = c \cdot k$, and that $\frac{b}{d} = c \cdot l$ for $k, l \in \mathbb{Z}$.

Then, $a = c \cdot d \cdot k$, and $b = c \cdot d \cdot l$. This shows that cd is a common divisor of a and b. However, d is the gcd of a, b, so it must be that $cd \leq d$. Under $\mathbb{Q}$ field properties there must $\exists!$ inverse to d, $\frac{1}{d}$ and by field closure we can multiply, so $c \leq 1$. $\qquad\square$

5.1 2.7 - The Euclidean Algorithm

How can we compute gcds?

One method is to factor each one into primes, take the overlapping subset, and find their product. This is dumb for large integers because factoring large integers is not computationally feasible (for traditional computers)

Lemma: Suppose $a = bq + r$. The set of common divisors of a and b is the same as the set of common divisors of b and r. It thus follows they have the same gcd.

Proof: Suppose $a = bq + r$. Then, a is a linear combination of b, r. Then, any common divisor of b, r must also divide a by a former proposition. Thus, any common divisor of b, r is by definition a divisor of b, but also a divisor of a. Thus, they are also common divisors of a, b.

Similarly, we can rewrite the equation to say that $r = a - bq$, and thus similarly all common divisors of a, b must be common divisors of r, b. So we are done. $\square$

Note: Here we can see the idea for the euclidean algorithm presented. We can reduce the gcd problem from a, b to be r, b, where r is strictly lesser than a. In fact, it's $\leq b$ by definition of division algorithm. Then, we can do this to b, then r again, etc until the numbers are very small.

Example: Let's use this idea to compute $\gcd(315, 220)$. Then,

$$315 = 1 \cdot 220 + 95 \quad 220 = 2 \cdot 95 + 30 \quad 95 = 3 \cdot 30 + 5 \quad 30 = 6 \cdot 5 + 0$$

and so applying the lemma, we get that $\gcd(315, 220) = \gcd(220, 95) = \gcd(95, 30) = \gcd(30, 5) = \gcd(5, 0) = 5$.

or the last nonzero remainder, is the gcd.

Theorem (The Euclidean Algorithm): Let $a, b \geq 0 \in \mathbb{Z}, b \neq 0$. Then, $a = bq_1 + r_1$ with $0 \leq r_1 \leq b$. Then, recursively apply the theorem with parameters b, r. The base case applies when the remainder is 0, in which case the divisor is the gcd.

In python,

```python
def gcd(a,b):
    if b==0:
        return a
    else:
        return gcd(b, a%b)
```

Proof: This is just repeated application of the lemma. $\square$

5.1.1 2.7.1 - The Extended Euclidean Algorithm

Theorem (2.12): $\exists x, y \in \mathbb{Z}$ st for $a, b \in \mathbb{Z}$ not both zero, $ax + by = \gcd(a, b)$.

Note: They are not unique.

6 Lecture 5

The idea is that we can solve for the remainder. For instance, take the example:

Ex: $\gcd(1239, 735)$ results in

$$1239 = 1 \cdot 735 + 504$$
$$735 = 1 \cdot 504 + 231$$
$$504 = 2 \cdot 231 + 42$$
$$231 = 5 \cdot 42 + 21$$
$$42 = 2 \cdot 21 + 0$$

But this also gives

$$504 = 1239 - 1 \cdot 735$$
$$231 = 735 - 1 \cdot 504$$
$$42 = 504 - 2 \cdot 231$$
$$21 = 231 - 5 \cdot 42$$

We can substitute these all the way up to get

$$\begin{aligned} 21 &= 231 - 5 \cdot 42 \\ &= 231 - 5 \cdot (504 - 2 \cdot 231) \\ &= 11 \cdot 231 - 5 \cdot 504 \\ &= 11 \cdot (735 - 1 \cdot 504) - 5 \cdot 504 \\ &= 11 \cdot 735 - 16 \cdot 504 \\ &= 11 \cdot 735 - 16 \cdot (1239 - 1 \cdot 735) \\ &= 27 \cdot 735 - 16 \cdot 1239 \end{aligned}$$

This gives us $x = -16$ and $y = 27$ such that $1239 \cdot (-16) + 735 \cdot 27 = 21$.

Theorem (The Extended Euclidean Algorithm): Let $a, b \in \mathbb{Z}$ not both zero. Then, we can find $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. Do so by:

- Apply the Euclidean algorithm to find the gcd and all the remainders.

- Rewrite each remainder as a linear combination of a and b by substituting the previous remainders.

- Continue substituting until you express the gcd as a linear combination of a and b.

In python,

```python
def extended_gcd(a,b):
    if b==0:
        return (a,1,0)
    else:
        d,x1,y1 = extended_gcd(b, a%b)
        x = y1
        y = x1 - (a//b)*y1
        return (d,x,y)
```

Proof: This is just the algorithm described above. The correctness follows from the Euclidean algorithm and properties of linear combinations. □

Example: Find x, y such that $19x + 7y = 1$.

We apply the extended euclidean algorithm:

$$\begin{aligned} 19 &= 2 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Then, in reverse,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 19 - 8 \cdot 7 \end{aligned}$$

6

Some applications:

Proposition (2.16): Let $a, b, c \in \mathbb{Z}$ st $a \neq 0, \gcd(a, b) = 1$. Then if $a|bc$, then $a|c$.

The idea is that if a, b are coprime, then a has no common factors with b. Thus, if a divides bc, it must be that a divides c.

Proof: Since $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying both sides by c gives $acx + bcy = c$. Since $a|acx$ and $a|bcy$ (since $a|bc$), it follows that $a|c$. $\qquad\square$

Corollary: Let $p \in \mathbb{Z}$ prime, and $a, b \in \mathbb{Z}$. Then if $p|ab$, then $p|a$ or $p|b$.

Proof: If $p|a$, we are done. Otherwise, $\gcd(p, a) = 1$ since p is prime and does not divide a. Thus, by the previous proposition, $p|b$. $\qquad\square$

Corollary (2.14): Let $a, b, d \in \mathbb{Z}$ st $d = \gcd(a, b)$. For $e \in \mathbb{Z}$ if $e|a, e|b$, then $e|d$.

Proof: Since d is a linear combination of a and b, we have that $d = ax + by$ for some integers x, y. Since $e|a$ and $e|b$, it follows that $e|ax$ and $e|by$. Thus, $e|d$. $\qquad\square$

6.1   2.9 - Fermat and Mersenne Primes

We know that there are infinitely many primes by Euclid's theorem. However, are there infinitely many primes of certain forms? And can we use this to generate primes? Useful for cryptography, etc.

Definition (Mersenne Number): The nth Mersenne number is defined as $M_n = 2^n - 1$ for $n \geq 1$.

Proposition: If $a|n$, then $M_a|M_n$. If n is composite, then M_n is composite.

Proof: Suppose $n = ab$ for integers $a, b > 1$. Then,

$$
\begin{aligned}
M_n &= 2^{ab} - 1 \\
&= (2^a)^b - 1^b \\
&= (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\right)
\end{aligned}
$$

Since $a, b > 1$, it follows that $2^a - 1 > 1$ and the second factor is also greater than 1. Thus, M_n is composite. $\square$

Example: $M_10 = 2^{10} - 1 = 1023$ is composite. We know that $2|10$ so $M_2|M_{10}$. In fact, $M_2 = 3$ and $1023 = 3 \cdot 341$. Also, $5|10$ so $M_5|M_{10}$. In fact, $M_5 = 31$ and $1023 = 31 \cdot 33$.

Note: If p is prime, is M_p prime? For some, yes, i.e. 13, 17, 19. However M_{11} isn't prime for instance.

Definition (Fermat Number): The nth Fermat number is defined as $F_n = 2^{2^n} + 1$ for $n \geq 0$.

Note: He initially looked at $2^m + 1$ but found that unless m is a power of 2, $2^m + 1$ is composite. For instance, $2^6 + 1 = 65$ is composite.

Proposition: For $2^m + 1$, if m is not a power of 2, then $2^m + 1$ is composite. If $m = 2^n$, then $2^m + 1$ is prime for $n = 0, 1, 2, 3$ but composite for $n = 4$.

Proof: Suppose m is not a power of 2. Recall that if k is odd, then $x^k + 1$ is divisible by $x + 1$. Since m is

not a power of 2, then we can write $m = 2^n \cdot k$ for some odd integer $k > 1$. Then,

$$
\begin{aligned}
2^m + 1 = 2^{2^n \cdot k} + 1 \\
= (2^{2^n})^k + 1^k \\
= (2^{2^n} + 1)\left((2^{2^n})^{k-1} - (2^{2^n})^{k-2} + \cdots - 1\right)
\end{aligned}
$$

Since $k > 1$, it follows that $2^{2^n} + 1 > 1$ and the second factor is also greater than 1. Thus, $2^m + 1$ is composite. $\qquad\square$

7   Lecture 6

Proposition: If $M_p = 2^p - 1$ is prime, then p is prime. Such an M_p is called a Mersenne prime.

<u>Note:</u> There are only 52 known Mersenne primes! And it's not known if there are infinitely many.

It turns out that F_5, F_6, F_7 are all composite. In fact, only F_0 to F_4 are known to be prime. It is not known if there are infinitely many Fermat primes.

8   Lecture 7

Chapter 3 now, Linear Diophantine Equations.

8.1   3.1 - Linear Diophantine Equations

Take $ax + by = c$ for $a, b, c \in \mathbb{Z}$. We are interested in integer pairs (x, y) that satisfy this linear diophantine equation.

The goal will be to describe <u>all</u> such solutions (x, y)

<u>Example:</u> Find integers x, y such that $19x + 7y = 1$.

By the extended euclidean algorithm,

$$
\begin{aligned}
19 &= 2 \cdot 7 + 5 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}
$$

Then, in reverse,

$$
\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 \\
&= 3 \cdot 19 - 8 \cdot 7
\end{aligned}
$$

Then, one solution is $3, -8$. There are infinitely many solutions, since we can add $7k$ to x and subtract $19k$ from y for any integer k to get another solution. So, the set of all solutions is $\{(3 + 7k, -8 - 19k) : k \in \mathbb{Z}\}$.

<u>Example:</u> Find integers x, y such that $19x + 7y = 6$.

We do know that

$$1 = 3 \cdot 19 - 8 \cdot 7$$
$$6 = 18 \cdot 19 - 48 \cdot 7$$

Then, we can similarly add $7k$ to x and subtract $19k$ from y for any integer k to get another solution. So, the set of all solutions is $\{(18 + 7k, -48 - 19k) : k \in \mathbb{Z}\}$.

Example: Find integers x, y such that $6x + 15y = 10$.

There are no integer solutions since $\gcd(6, 15) = 3$ does not divide 10. Generally if $\gcd(a, b)$ does not divide c, then there are no integer solutions to $ax + by = c$.

Proof: Let $d = \gcd(a, b)$. Then $d|a, d|b$ and $d|ax + by$ by bilinearity of divisibility. However, $d \nmid c$ by assumption, so there are no integer solutions to $ax + by = c$. $\qquad\square$

Theorem (3.1): Assume $a, b, c \in \mathbb{Z}$, and at least one of $a, b \neq 0$, and let $d = \gcd(a, b)$. Then,

(1) The equation $ax + by = c$ has integer solutions iff $d|c$.

(2) Additionally, if it has an integer solution, it has infinitely many integer solutions. In particular, if (x_0, y_0) is one integer solution, then the set of all integer solutions is given by

$$\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) : k \in \mathbb{Z}\}$$

Proof:

(1) $\Rightarrow$: Let $ax + by = c$ have integer solutions. Then, since $d|a, d|b$, we have that $d|ax + by$ by bilinearity of divisibility. Thus, $d|c$.

$\Leftarrow$ Suppose $d|c$. THen, $c = d \cdot e$ for some integer e. Since d is a linear combination of a and b, we have that $d = ax_0 + by_0$ for some integers x_0, y_0. Thus,

$$c = d \cdot e$$
$$= (ax_0 + by_0)e$$
$$= a(ex_0) + b(ey_0)$$

So, (ex_0, ey_0) is an integer solution to $ax + by = c$.

(2) (This is my own proof) First, $\frac{b}{d}, \frac{a}{d} \in \mathbb{Z}$ by proposition 2.10. Now, let (x_0, y_0) be one integer solution to $ax + by = c$. Then, for any integer k, we have

$$a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + by_0 + ab\frac{k}{d} - ab\frac{k}{d}$$
$$= c$$

Thus, $(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k)$ is an integer solution for any integer k.

$\qquad\square$

Definition (Homogeneous LDE): A linear diophantine equation of the form $ax + by = 0$ is called a homogeneous linear diophantine equation.

Lemma: Suppose a, b are not both 0. Then

(1) If $\gcd(a, b) = 1$, every solution to $ax + by = 0$ is of the form $(bk, -ak)$ for some integer k.

(2) In general, if $d = \gcd(a, b)$, every solution to $ax + by = 0$ is of the form $(\frac{b}{d}k, -\frac{a}{d}k)$ for some integer k.

Proof:

(1) Let a, b not both 0. Suppose $\gcd(a, b) = 1$. Let (x, y) be a solution to $ax + by = 0$. Then, $ax = -by$ and so $a|by$. Since $\gcd(a, b) = 1$, it follows that $a|y$. Thus, $y = ak$ for some integer k. Substituting back gives $ax = -bak$, so $x = -bk$. Thus, every solution is of the form $(bk, -ak)$ for some integer k.

(2) Let a, b not both 0. Let $d = \gcd(a, b)$. Let (x, y) be a solution to $ax + by = 0$. Then, $ax = -by$ and so $a|by$. Since $\gcd(a, b) = d$, it follows that $\frac{a}{d}|\frac{b}{d}y$. Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ by proposition 2.10, it follows that $\frac{a}{d}|y$. Thus, $y = \frac{a}{d}k$ for some integer k. Substituting back gives $ax = -b\frac{a}{d}k$, so $x = -\frac{b}{d}k$. Thus, every solution is of the form $(\frac{b}{d}k, -\frac{a}{d}k)$ for some integer k.

9 Lecture 8

Theorem (3.1): Let $d = \gcd(a, b)$. Then

1. $ax + by = c$ has solutions iff $d|c$.

2. If (x_0, y_0) is one solution to $ax + by = c$, then the solution set is given by

$$x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$$

where t is an integer

We proved this last time, along with a related lemma. I will now write Prof's proof of part 2.

Proof: (of part 2) Suppose (x_0, y_0) is some solution for $ax + by = c$. Then, we should show that the above format gives solutions, and additionally that they are all of the solutions. So

- Verify it is a solution:

$$a(x_0 + \frac{b}{d}t) + b(y_0 + \frac{a}{d}t) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t$$
$$= ax_0 + by_0$$

which is a solution by assumption.

- Verify it is all the solutions: Let (x, y) be any solution to $ax + by = c$. Then,

$$a(x - x_0) + b(y - y_0) = ax + by - (ax_0 + by_0)$$
$$= c - c$$
$$= 0$$

Thus, $(x - x_0, y - y_0)$ is a solution to the homogeneous linear diophantine equation $ax + by = 0$. By the previous lemma, there exists an integer t such that

$$(x - x_0, y - y_0) = (\frac{b}{d}t, -\frac{a}{d}t)$$

Thus,

$$(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$$

which is of the desired form.

Note: Thus, to solve a linear diophantine equation

$$ax + by = c$$

, first ensure that $d = \gcd(a, b)$ divides c. If not, there are no solutions. If it does, then find one solution (x_0, y_0) using the extended euclidean algorithm. Then, the set of all solutions is given by

$$\left\{\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right) : t \in \mathbb{Z}\right\}$$

Example: Solve $12x + 45y = 30$. Then, $\gcd(12, 45) = 3, 3|30$ so there are solutions

$$45 = 12(3) + 9$$
$$12 = 9(1) + 3$$
$$9 = 3(3) + 0$$

going back up we have

$$3 = 12 - 9(1)$$
$$= 12 - (45 - 12(3))$$
$$= 4 \cdot 12 - 45$$

we can multiply by 10 to get $30 = 40 \cdot 12 - 10 \cdot 45$. Thus, one solution is $(40, -10)$. The set of all solutions is given by

$$\{(40 + 15t, -10 - 4t) : t \in \mathbb{Z}\}$$

9.1   3.2 - Postage Stamp Problem

Problem: You have an unlimited supply of 3 cent and 5 cent stamps. What amounts of postage can you make? Generalize this to a cent and b cent stamps, frequently where a, b are coprime.

The answer is obviously intuitively

$$ax + by = c$$

for some nonnegative integers x, y. We want to find the largest c such that there are no nonnegative integer solutions to this equation. Also, what are all of the values of c such that there are no nonnegative integer solutions to this equation?

> Professor gives an example for postage stamps with values of 3 and 5 here, which is a trivially solved problem. The idea is that if you can find 3 consecutive values of c that can be achieved, then all values of c greater than the largest of those 3 must also be achievable. This is because you can add 3 to any of those 3 values to get the next value, and so on. Thus, you just need to find the largest c such that there are no 3 consecutive values of c that can be achieved.
>
> In general, we can intuit from this that for the smallest of a, b, if we can find a consecutive values of c that can be achieved, then all values of c greater than the largest of those a must also be achievable. Thus, you just need to find the largest c such that there are no a consecutive values of c that can be achieved.

Example: Suppose in some fucked up version of football the only ways to score are with 3 or 7 points. What scores can be achieved?

Remember you just need 3 in a row that can be achieved and everything after is doable.

Score	Achievable?
0	Yes
1	No
2	No
3	Yes
4	No
5	No
6	Yes
7	Yes
8	No
9	Yes
10	Yes
11	No
12	Yes
13	Yes
14	Yes

and so on. We can see that the largest score that cannot be achieved is 11, and all scores greater than 11 can be achieved.

Proposition (3.3): Suppose $a > 1, b > 1$ are coprime. Then there are no nonnegative integers x, y such that $ax + by = ab - a - b$.

Proof: (This is my proof) Let $d = \gcd(a, b)$. Since a, b are coprime, $d = 1$. Thus, by the extended euclidean algorithm, there exist integers x_0, y_0 such that $ax_0 + by_0 = 1$. Multiplying both sides by $ab - a - b$ gives

$$(ab - a - b)ax_0 + (ab - a - b)by_0 = ab - a - b$$
$$a(x_0(ab - a - b)) + b(y_0(ab - a - b)) = ab - a - b$$

Thus, $(x_0(ab - a - b), y_0(ab - a - b))$ is an integer solution to $ax + by = ab - a - b$. Here, we will establish a contradiction.

Suppose on the contrary both are positive. Note that if $x_0(ab - a - b) \geq 0$, then $x_0 \geq 0$ since $ab - a - b > 0$ for $a, b > 1$. Similarly, if $y_0(ab - a - b) \geq 0$, then $y_0 \geq 0$. We thus have that $ax_0 + by_0 \geq 0$.

Note here that x_0, y_0 are forced to sum to at most 1 since if $x_0 + y_0 > 1 \implies x_0 + y_0 \geq 2$, then $ax_0 + by_0 \geq 2a + 2b > 1$. Thus, $0 \leq x_0 + y_0 \leq 1$. By integer properties, this means that either $x_0 = 0, y_0 = 0$ or one of them is 1 and the other is 0.

Then, if $x_0 = 0, y_0 = 0$, then $ax_0 + by_0 = 0 \neq 1$. If $x_0 = 1, y_0 = 0$, then $ax_0 + by_0 = a > 1$. If $x_0 = 0, y_0 = 1$, then $ax_0 + by_0 = b > 1$. But we need it to be identically 1, a contradiction.

Thus, there are no integer solutions to $ax + by = ab - a - b$ where both are positive. $\qquad\square$

The general idea behind this proof is that when you plug in any arbitrary integer solution to $ax + by = ab - a - b$, you get that $ax_0 + by_0 = 1$. Since $a, b > 1$, this forces x_0, y_0 to be nonnegative and sum to at most 1, none of which can satisfy the equation.

> The professor gives a proof that requires memorizing some answer for x_0, y_0, which is why I don't like it and derived my own.
>
> **Proof:** (by the professor) Consider the Diophantine Equation
>
> $$ax + by = ab - a - b$$

Notice that $x_0 = -1, y_0 = a - 1$ is a solution, as

$$a(-1) + b(a - 1) = -a + ab - b$$
$$= ab - a - b$$

Thus, the general solution of the Diophantine Equation is $x = -1 + bt, y = a - 1 - at$ for some integer t.

WLOG (this must be briefly justified in reality), suppose (x, y) is a solution such that $x \geq 0$. Since $x \geq 0$, we have that $-1 + bt \geq 0$. This implies that $t > 0$, an integer, so $t \geq 1$. Then, since $y = a - 1 - at$, we have that $y \leq a - 1 - a = -1 < 0$. Thus, if $x \geq 0$, then $y < 0$. Similarly, if $y \geq 0$, then $x < 0$. Thus, there are no nonnegative integer solutions to the equation. $\qquad\square$