Chapter 3 Lecture Notes

Greg Knapp

January 31, 2022

1 Prime Numbers

1.1 Basic Facts

- **Def:** A *prime number* is a positive integer which has exactly two positive divisors. Every other integer greater than 1 is called *composite*
  - Note that 1 isn't prime because it only has one positive divisor
- Of course, numbers like 2, 3, and 5 are prime, where numbers like 4, 6, and 9 are composite
- Why do we care about primes?
  - They're another way to think about how to generate the integers (though we don't quite have the tools to see this yet)
  - Some cryptography relies on factoring numbers into primes
  - Often, when proving a question about natural numbers, you can reduce to a prime case
- What are some good things to know about primes?
- **Thm:** Every integer greater than 1 has a prime divisor
  - Suppose $n > 1$
  - Consider the set $S = \{d > 1 : d \mid n\}$
  - Since $n \in S$, the well-ordering principle tells us that S has a least element, say p
  - If p is not prime, p has at least three positive divisors: $1, p$, and something else, say d.
  - Then we know that $d \mid p$ and $p \mid n$, so $d \mid n$.
  - d is positive and not 1, so $d > 1$, so $d \in S$
  - Additionally, $d < p$ because d is a divisor of p and not equal to p.
  - This contradicts the minimality of p.
  - Therefore, p is prime
- **Thm:** There are infinitely many primes
  - Suppose not.
  - Let $P = \{p \in \mathbb{N} : p \text{ is prime}\}$
  - Since P is a finite set, let $k = \prod_{p \in P} p$
  - Note that the number $k + 1$ must have a prime divisor by our previous lemma.
  - But if $p \in P$, $p \nmid k$ because k is one more than a multiple of p
  - Hence, P is not the set of all primes, which is a contradiction
- Alternatively...Claim: for every $n > 1$, if p is a prime divisor of $n! + 1$, then $p > n$

  - By contradiction, suppose $p \leqslant n$.
  - Then $p \mid n!$
  - By assumption, $p \mid n! + 1$
  - Hence, $p \mid (n! + 1) - n! = 1$, which is a contradiction
- Note that we have shown that for any n, there exists a prime $p > n$, so there are infinitely many primes
- There are lots of proofs that there are infinitely many primes! We'll see if come across some more in this class
- **Thm:** If n is composite, then n has a prime factor $\leqslant \sqrt{n}$
  - Since n is composite, we can write $n = ab$ where $1 < a \leqslant b < n$
  - If $a > \sqrt{n}$, we would have $b > \sqrt{n}$ and hence, $n = ab > n$
  - Contradiction, so $a \leqslant \sqrt{n}$
- Sieve of Eratosthenes activity

1.2 Prime Distribution

- A major question in number theory is: where do the primes live?
  - Are they close together or far apart?
  - How many primes end in 1? 3? 5? 7?
  - How many primes are of the form $4k + 1$? $4k + 3$?
  - Are there infinitely many twin primes?
  - Erdös-Turán Conjecture: the set of primes contains arbitrarily long arithmetic progressions, i.e. for any n, there exists a prime p and a positive integer c for which $p, p + c, p + 2c, \ldots, p + nc$ are all prime
  - Are there infinitely many primes of the form $n^2 + 1$?
  - Given a number n, how far might you have to look to definitely find a prime?
- Some partial answers:
- **Def:** The prime counting function is $\pi(x)$ defined to be the number of prime numbers less than x.
- **Thm:** (Prime Number Theorem): The probability that a randomly selected positive integer less than x is prime is $\approx \frac{1}{\log(x)}$
- What does this say about $\pi(x)$?
  - We can use this probability statement to compute the expected number of primes less than x
  - The expected number of primes less than x is $\mathrm{Li}(x) := \int_2^x \frac{1}{\log(t)}\, dt$
  - Integrating by parts gives

$$\mathrm{Li}(x) = \frac{x}{\log(x)} - \frac{2}{\log(2)} + \int_2^x \frac{1}{\log^2(t)}\, dt$$

  - Check that $\frac{x}{\log(x)}$ is the main term by noting that $\mathrm{Li}(x) \to \infty$ (in comparison with $\int \frac{1}{x}\, dx$) and noting that $\frac{\mathrm{Li}(x)}{\int_2^x \frac{1}{\log^2(t)}\, dt} \to \infty$
  - Hence, $\pi(x) \approx \frac{x}{\log(x)}$
- What do we formally mean by $\approx$? Well, $\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log(x)}\right)} = 1$

- Note that this allows us to conclude that there are infinitely many primes, since $\frac{x}{\log(x)} \to \infty$
- **Thm:** Suppose that a and b are relatively prime positive integers. Then the arithmetic progression $x_n = an + b$ has infinitely many primes.
- On the question of "how far do you have to look to find a prime," we know that between n and $n! + 1$, there must be a prime.
- Better bounds exist:
- **Thm:** Bertrand-Chebyshev Theorem: For any $n \in \mathbb{N}$, there exists a prime p with $n < p < 2n$
- There are other related questions, like
- Legendre's conjecture: For each n, is there a prime p with $n^2 < p < (n+1)^2$?

2 Greatest Common Divisors and their Properties

2.1 Some Theory

- We previously defined the greatest common divisor of two integers a and b to be the maximal element of the set of their common divisors
- We'll explore some useful facts about them here
- **Thm:** Let $a, b, c \in \mathbb{Z}$. Then $(a, b) = (a + bc, b)$
  - Suppose $d \mid (a, b)$
  - Then $d \mid a$ and $d \mid b$, so $d \mid a + bc$.
  - Since $d \mid a + bc$ and $d \mid b$, $d \mid (a + bc, b)$
  - i.e. every divisor of (a, b) is a divisor of $(a + bc, b)$
  - Now suppose $f \mid (a + bc, b)$.
  - Since $f \mid a + bc$, there exists $d \in \mathbb{Z}$ with $fd = a + bc$, so $a = fd - bc$.
  - But since $f \mid b$, we find that $f \mid a$
  - Hence, $f \mid (a, b)$
  - i.e. every divisor of (a, b) is a divisor of $(a + bc, b)$
  - But if the divisors of (a, b) are the same as the divisors of $(a + bc, b)$, then they must be the same number up to sign
  - Since they are both positive, they are both equal
- We've seen before that if $d \mid a, b$, then $d \mid ma + nb$ for any m, n
- In particular, $(a, b) \mid ma + nb$
- **Ex:** $a = 9$, $b = 15$. We know that $(9, 15) = 3$ divides both 9 and 15 and hence, divides any $9m + 15n$.
- However, we can actually find an m and an n so that $9m + 15n \mid 3$, too: $9 \cdot (-3) + 15 \cdot 2 = 3$
- Can we always do this?
- **Thm:** If $a, b \in \mathbb{Z}$ with either $a \neq 0$ or $b \neq 0$, there exist $m, n \in \mathbb{Z}$ with $ma + nb = (a, b)$.
  - Consider the set $S = \{ma + nb > 0 : m, n \in \mathbb{Z}\}$
  - $S \neq \varnothing$, so S has a least element, say $d = ma + nb$
  - We claim that $d = (a, b)$

- To do this we need: $d \mid a$ and $d \mid b$
- We'll show that $d \mid a$ using Euclidean division:
- Write $a = dq + r$ for $q, r \in \mathbb{Z}$, $0 \leqslant r < d$
- We want to show that $r = 0$
- So we have $r = a - dq = a - (ma + nb)q = (1 - mq)a - nqb$, so r is a linear combination of a and b.
- Using $0 \leqslant r < d$ and the fact that d is the least positive linear combination of a and b, we find $r = 0$.
- Hence, $d \mid a$
- Similarly, $d \mid b$
- Additionally, $(a, b) \mid ma + nb = d$.
- So d is a positive divisor of a and b. Moreover, any other divisor of a and b divides d.
- So $d = (a, b)$

- This is nice, but how do we find m and n? It's not as simple as you might think...

2.2 Examples

- **Ex:** Show that if $k \in \mathbb{Z}_{>0}$, then $3k + 2$ and $5k + 3$ are relatively prime
  - $5(3k + 2) - 3(5k + 3) = 1$
- **Ex:** Show that if $n \in \mathbb{Z}_{>0}$, then $(n + 1, n^2 - n + 1) = 1$ or 3

$$\begin{aligned}(n+1, n^2 - n + 1) &= (n+1, n^2 - n + 1 - n(n+1)) \\ &= (n+1, -2n + 1) \\ &= (n+1, -2n + 1 + 2(n+1)) \\ &= (n+1, 3)\end{aligned}$$

  which is either 1 or 3. Note how we used polynomial long division here...

- **Def:** Integers $a_1, \ldots, a_n$ are *mutually relatively prime* if $(a_1, \ldots, a_n) = 1$. The integers are *pairwise relatively prime* if $(a_i, a_j) = 1$ when $i \neq j$.
- **Ex:** Find four integers which are mutually relatively prime so that any three of them are not mutually relatively prime
  - $2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 7, 2 \cdot 5 \cdot 7, 3 \cdot 5 \cdot 7$

3 The Euclidean Algorithm

3.1 The Basic Algorithm

- Last time, we saw an example of why the theorem $(a, b) = (a + nb, b)$ was useful:

$$(36, 122) = (36, 122 - 108 = 14) = (36 - 28 = 8, 14) = (8, 6) = (2, 6) = (2, 0) = 2$$

- Off hand, it might seem like this is slower for numbers like 36 and 122 which are only divisible by small primes (and you've probably memorized the prime factorization anyways).
- You're probably right, but for larger numbers, this algorithm runs much faster.
- But we want to formalize this process

- Note that we're using division with remainder every time: we're taking the gcd of the smaller thing with the remainder of the division of the bigger thing by the smaller thing.
- More precisely we have the following
- Let $a \geqslant b > 0$ and do the following divisions (we can let $r_0 = a$ and $r_1 = b$):

$$\begin{aligned} a &= bq_1 + r_2 \\ b &= r_2q_2 + r_3 \\ r_2 &= r_3q_3 + r_4 \\ &\vdots \\ r_{n-1} &= r_nq_n + 0 \end{aligned}$$

- Then $(a, b) = r_n$

3.2 Some Examples

- **Ex:** Compute $(60, 34)$:

$$\begin{aligned} 60 &= 34 \cdot 1 + 26 \\ 34 &= 26 \cdot 1 + 8 \\ 26 &= 8 \cdot 3 + 2 \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

- So $(60, 34) = 2$
- **Ex:** Compute $(105, 44)$:

$$\begin{aligned} 105 &= 44 \cdot 2 + 17 \\ 44 &= 17 \cdot 2 + 10 \\ 17 &= 10 \cdot 1 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

- So $(105, 44) = 1$
- **Ex:** Let F_{n+1} and F_{n+2} be successive terms in the Fibonacci sequence with $n > 1$. Show that the Euclidean algorithm takes exactly n divisions to compute $(F_{n+1}, F_{n+2}) = 1$

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ F_{n+1} &= F_n + F_{n-1} \\ &\vdots \\ F_4 + F_3 &+ F_2F_3 = F_2 \cdot 2 \end{aligned}$$

- So $F_2 = 1$ is the gcd and there are exactly $n + 2 - 3 + 1 = n$ divisions

3.3 Why does it work?

- Why does this work?
- Two questions: why does it finish and why is $r_n = (a, b)$?

- For the second question $(a,b) = (a - q_1 b, b) = (r_2, b) = (r_2, b - r_2 q_2) = (r_2, r_3) = (r_2 - q_3 r_3, r_3) = (r_4, r_3) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$

- How do we know we eventually get to some remainder of 0?
- Well, $b > r_2 > r_3 > \ldots \geqslant 0$, so some remainder had better be 0 eventually.

3.4 Using the Euclidean algorithm for linear combinations

- **Ex:** Write 1 as a linear combination of 105 and 44

$$\begin{aligned} 105 &= 44 \cdot 2 + 17 \\ 44 &= 17 \cdot 2 + 10 \\ 17 &= 10 \cdot 1 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Rewriting gives...

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - (10 - 7) \cdot 2 \\ &= 7 \cdot 3 - 10 \cdot 2 \\ &= (17 - 10 \cdot 1) \cdot 3 - 10 \cdot 2 \\ &= 17 \cdot 3 - 10 \cdot 5 \\ &= 17 \cdot 3 - (44 - 17 \cdot 2) \cdot 5 \\ &= 17 \cdot 13 - 44 \cdot 5 \\ &= (105 - 44 \cdot 2) \cdot 13 - 44 \cdot 5 \\ &= 105 \cdot 13 - 44 \cdot 31 \end{aligned}$$

- Hm. Not something you'd expect. But not something unexpected either.
- This requires us to traverse the Euclidean algorithm twice though.
- Can we do better?
- Sure, by tracking some extra information

3.5 The Extended Euclidean Algorithm

- **Thm:** Let $a, b \in \mathbb{Z}$ with $a \geqslant b \geqslant 1$. Then $(a,b) = s_n a + t_n b$ where s_n and t_n are defined by $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$ and

$$s_j = s_{j-2} - q_{j-1} s_{j-1} \qquad t_j = t_{j-2} - q_{j-1} t_{j-1}$$

- What are s_j and t_j supposed to represent?
- They represent the coefficients in $r_j = s_j a + t_j b$
- This leads to the proof:
  - By strong induction on j: $r_0 = a = s_0 a + t_0 b$ and $r_1 = b = s_1 a + s_2 b$
  - Then suppose that $r_j = s_j a + t_j b$ for all $j < k$

– Then we have

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_{k-1} \\ &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1} \\ &= (s_{k-2} - s_{k-1}q_{k-1})a + (t_{k-2} - t_{k-1}q_{k-1})b \\ &= s_k a + t_k b \end{aligned}$$

– Ta da!

- **Ex:** Express $(102, 222)$ as a linear combination of 102 and 222.

$$\begin{aligned} 222 &= 102 \cdot 2 + 18 & s_2 &= 1 - 2 \cdot 0 & t_2 &= 0 - 2 \cdot 1 \\ 102 &= 18 \cdot 5 + 12 & s_3 &= 0 - 5 \cdot 1 & t_3 &= 1 - 5 \cdot (-2) \\ 18 &= 12 \cdot 1 + 6 & s_4 &= 1 - 1 \cdot (-5) & t_4 &= -2 - 1 \cdot 11 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

4 The Fundamental Theorem of Arithmetic

4.1 The Theorem

- Lemma: Suppose $(a, b) = 1$ and $a \mid bc$. Then $a \mid c$
- Proof:
  - Since $(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$
  - Multiply through by c to get $axc + byc = c$
  - The LHS is divisible by a because it is a linear combination of a and bc
  - Hence, the RHS is divisible by a, so $a \mid c$
- Lemma: Suppose $p \mid a_1 \cdots a_n$ for integers $a_1, \ldots, a_n$. Then $p \mid a_i$ for some $1 \leqslant i \leqslant n$.
- Proof:
  - By induction on n
  - $n = 1$ is trivial
  - Now we assume that if $p \mid b_1 \cdots b_{n-1}$, then $p \mid b_i$ for some $1 \leqslant i \leqslant n-1$
  - Suppose $p \mid a_1 \cdots a_n$
  - Either $(p, a_1 \cdots a_{n-1}) = 1$ or p.
  - If $(p, a_1 \cdots a_{n-1}) = 1$, then $p \mid a_n$ by the previous lemma
  - If $(p, a_1 \cdots a_{n-1}) = p$, then $p \mid a_1 \cdots a_{n-1}$ and by induction hypothesis, $p \mid a_i$ for some $1 \leqslant i \leqslant n-1$
- **Thm:** Every nonzero integer n can be written as a product $n = (-1)^b \prod_{i=1}^{g} p_i^{v_i}$ where $b = 0$ or 1, each p_i is prime, and each $v_i \in \mathbb{Z}_{>0}$. This expression is unique up to reordering the p_i.
- Proof:
  - We start by showing that every integer greater than 1 has a prime factorization.
  - By the well-ordering principle, there must be a least positive $n > 1$ without a prime factorization.
  - But we've shown (previously) that every integer greater than 1 has a prime factor, so n has a prime factor, p.
  - If $\frac{n}{p} = 1$ then $n = p$ is a prime factorization of n, contradiction.
  - If $\frac{n}{p} > 1$, then it has a prime factorization

- But then n has a prime factorization: $n = p \cdot \text{prime-factorization-of-}\frac{n}{p}$
- This contradicts the fact that n has no prime factorization
- Therefore, every integer greater than 1 has a prime factorization
- To see that this factorization is unique, suppose that we can write $n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$
- Then $p_1 \mid q_1 q_2 \cdots q_m$, so $p_1 \mid q_i$ for some i.
- WLOG, $i = 1$. Then $p_1 = q_1$
- So $p_2 \cdots p_n = q_2 \cdots q_m$ and apply the same process to find that $p_2 = q_2, \ldots, p_n = q_n$.
- If $m > n$, we'd have $1 = q_{n+1} \cdots q_m$ and that doesn't work, so $m = n$
- Hence, our two prime factorizations were the same!
- This gives uniqueness
- The only integers left are $1 = (-1)^0$, $1 = (-1)^1$, and any negative integer, which you get of course by factoring $|n|$ and then multiplying by $(-1)^1$.

4.2 Factorization in Other Contexts

- In what other number systems can we factor things?
- Let $\mathbb{Q}[x]$ be the set of polynomials with coefficients in $\mathbb{Q}$.
- We can factor polynomials there, but notice that we lose some uniqueness: $x = 2 \cdot \frac{x}{2}$
- What about $\mathbb{Q}$?
- Note that first, we can write any element of $\mathbb{Q}$ as $\frac{r}{s}$ where $r, s \in \mathbb{Z}$, $s > 0$, and $(r, s) = 1$
- Then if $r \neq 0$, we can factor r and s into primes and write $\frac{r}{s} = \prod_{i=1}^{g} p_i^{v_i}$ where the v_i are either positive or negative
- This factorization is somehow a special feature of $\mathbb{Q}$ however
- It comes from the fact that $\mathbb{Q}$ is the set of fractions of $\mathbb{Z}$
- A set like $\mathbb{R}$ has no meaningful way to factor its elements
- There's nothing like "primes" that show up in the context of $\mathbb{R}$
- This is because you can always take a real number x and do something silly with it like write $x = \pi \cdot \frac{x}{\pi}$, so there aren't any numbers that "don't factor"
- $\mathbb{C}$ is pretty similar: there's no good analogue of factoring
- But maybe we end up with a good question based on our experiences so far: in any context in which factoring makes sense, will we have unique factorization?

4.3 Unique Factorization in Other Contexts

- Let's look at the set $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$
- Note that this set has all of the usual integers, $-10, 2, 3, 5$, etc. and also some extra numbers $1 + \sqrt{-5}$, $1 - \sqrt{-5}$, etc
- Just like in the integers, we can add, subtract, and multiply elements of $\mathbb{Z}[\sqrt{-5}]$ and stay in $\mathbb{Z}[\sqrt{-5}]$
- Note that $(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-5}$
- Also, $(a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5}) = a_1a_2 - 5b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{-5}$

- Given these two operations, we call $\mathbb{Z}[\sqrt{-5}]$ a ring and it's a special type of ring with the following property: if $xy = 0$, then $x = 0$ or $y = 0$
- Not every ring has this property: think about matrices
- Are there any numbers that play the role of primes in $\mathbb{Z}[\sqrt{-5}]$?
- Sure: we say that a number $x \in \mathbb{Z}[\sqrt{-5}]$ is <u>irreducible</u> if any time you write $x = yz$ for $y, z \in \mathbb{Z}[\sqrt{-5}]$, $y = \pm 1$ or $z = \pm 1$.
- Here are a few numbers that you can check are irreducible: $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$
- But note that there's something weird that happens $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$
- So $\mathbb{Z}[\sqrt{-5}]$ has factorization and the equivalent of primes, but it doesn't have unique factorization. Weird!!!
- What about $\mathbb{Z}[\sqrt{d}]$ for other d?
- $\mathbb{Z}[i]$ has unique factorization!
- Some of the "traditional" primes lose their primality though: $5 = (1 + 2i)(1 - 2i)$.
- Note that this has something to do with $5 = 1^2 + 2^2$.
- Question: which numbers can be written as the sum of two squares? Three squares? Four squares? More squares?

4.4 An Example or Two

- Recall Dirichlet's theorem on primes in arithmetic progressions: fixing $a, d \in \mathbb{Z}$ with $(a, d) = 1$, there are infinitely many primes of the form $a + kd$
- **Ex:** Show that there are infinitely many primes of the form $3 + 4k$
- Proof:
  - Suppose there are only finitely many primes of this form: $q_0 = 3, q_1, \ldots, q_r$.
  - Define $Q = 4q_1 \cdots q_r + 3$
  - Since Q is of the form $4k+3$, it must have some prime p of the form $p = 4k+3$ in its factorization (if all of the primes are of the form $4k + 1$, then Q would be of the form $4k + 1$)
  - Let's check to see if $p = q_i$ for some $0 \leqslant i \leqslant r$
  - Could $p = q_0$?
  - No: if $p = 3 \mid Q$, then $3 \mid Q - 3 = 4q_1 \cdots q_r$, which can't happen because none of the primes are divisible by 3.
  - Could $p = q_i$ for some $i \geqslant 1$?
  - No: if $p = q_i$, then $p \mid Q - 4q_1 \cdots q_r = 3$, but $p \nmid 3$
  - Hence, p is of the form $4k + 3$ but is not in the list $q_0, \ldots, q_r$.
  - Contradiction. Therefore, infinitely many primes of the form $4k + 3$.
- **Ex:** Factor the Riemann zeta function (only if time...)

5 Linear Diophantine Equations

5.1 Intro

- Mathematicians often use the phrase "Diophantine Equations" to refer to
  - polynomial equations
  - any number of variables
  - with integer coefficients
  - where a "solution" means a solution in integers
- For instance, one might want to fix an integer n and find the solutions to $x^2 - ny^2 = 1$ (this is called Pell's equation because Euler mistakenly thought that a person named John Pell found the general method to find solutions to this equation)

5.2 Linear Diophantine Equations

- We're going to focus on solving linear Diophantine equations to start because these are the easiest.
- Diophantine equations can get pretty tough at the quadratic level, too...

5.2.1 In One Variable

- These are pretty easy (but worth starting at): They look like $ax = b$ for integers a and b.
- Q: When does this have solutions in the integers?
- A: When $a \mid b$
- In that case, it has a unique solution, namely $\frac{b}{a}$.
- So this equation has either 0 or 1 solution

5.2.2 In Two Variables

- This is where things get a little trickier.
- Consider an equation of the form $ax + by = n$ for integers a, b, n
- Where does an equation like this show up?
- **Ex:** Can you make 83 cents of change out of 6 cent coins and 15 cent coins?
- How can we examine this question?
- Option 1: geometrically
  - $6x + 15y = 83$ forms a line in the xy-plane. Does it pass through any lattice points?
  - Drawing it out shows that there aren't any solutions in the first quadrant
- Option 2: algebraically
  - Observe that the LHS is a linear combination of the numbers 6 and 15.
  - In particular, the LHS is divisible by $(6, 15) = 3$
  - But the RHS isn't divisible by 3, so there can't be any integer solutions!
- The algebraic approach (in this case) gives us a bit more insight into how we can change the problem to yield a solution

- **Ex:** Find an integer solution to $6x + 15y = 3$
  - We know the Euclidean algorithm will let us do this, but we can also do it by inspection
  - $6 \cdot 2 + 15 \cdot (-1) = 3$ for instance.
- **Ex:** Find an integer solution to $6x + 15y = 21$
  - Note that now that we've found $6 \cdot 2 + 15 \cdot (-1) = 3$, we can multiply by 7 to get $6 \cdot 14 + 15 \cdot (-7) = 3$
  - But there's another obvious solution: $6 \cdot 1 + 15 \cdot 1 = 21$
- **Ex:** How many integer solutions are there to $6x + 15y = 3$?
  - We know $6 \cdot (-2) + 15 \cdot 1 = 3$
  - Note that if I add $5k$ to the -2 and subtract $2k$ from the 1, the $6 \cdot 5k$ and the $15 \cdot 2k$ cancel out: i.e. $6 \cdot (-2 + 5k) + 15 \cdot (1 - 2k) = 3$ is true for every integer k
  - This gives infinitely many solutions!
  - Maybe there's a question of "where did the 5 and 2 come from?"
  - Let's start there.
  - Any solution to $6x + 15y = 3$ can be re-written as $6 \cdot (-2 + a) + 15 \cdot (1 - b) = 3$.
  - Simplifying gives $6a - 15b = 0$
  - One more step gives $2a = 5b$ and since 2 and 5 are relatively prime, we must have that a is a multiple of 5 and b is a multiple of 2
  - Moreover, if $a = 5k$, then we have $10k = 5b$ so $b = 2k$.
  - Hence, we find that every solution can be rewritten as $6 \cdot (-2 + 5k) + 15 \cdot (1 - 2k) = 3$ for some integer k
  - We still haven't answered the question, so let's go a bit more abstract
- **Ex:** Classify the integer solutions to $ax + by = (a, b)$
  - You know that there exists some solution x_0, y_0
  - Any other solution can be written as $a(x_0 + n) + b(y_0 + m) = (a, b)$ for some integers m and n
  - Rewriting gives $an + bm = 0$, i.e. $an = -bm$
  - When we got to this step previously, we had $6n = 15m$, which wasn't useful because n didn't have to be a multiple of 15 for this to work. Instead, we divided by the gcd to get further
  - So now $\frac{a}{(a,b)} \cdot n = -\frac{b}{(a,b)} \cdot m$
  - Since $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$ are relatively prime, we can conclude that n must be a multiple of $\frac{b}{(a,b)}$, say $n = \frac{b}{(a,b)}k$.
  - But then $\frac{a}{(a,b)}k = -m$
  - So we have $a(x_0 + \frac{b}{(a,b)}k) + b(y_0 - \frac{a}{(a,b)}k) = (a, b)$ classifies all the solutions
- **Ex:** Classify the integer solutions to $ax + by = c$
  - If $(a, b) \nmid c$, there are no solutions and we are done.
  - If $(a, b) \mid c$, then by the same reasoning as above, find one solution (x_0, y_0) and every other solution will look like $x_0 + \frac{b}{(a,b)}k$ and $y_0 - \frac{a}{(a,b)}k$
- **Ex:** Find all solutions to $6x + 15y = 21$
- Using $x_0 = -14$ and $y_0 = 7$, we can write all solutions as $x = -14 + 5k$ and $y = 7 - 2k$
- Note that the solution $x = 1$ and $y = 1$ has $k = 3$

5.2.3 More than two variables

- Now consider the linear diophantine equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$
- If $(a_1, a_2, \ldots, a_n) \nmid c$, then there are no solutions
- If $(a_1, a_2, \cdots, a_n) \mid c$, then we claim that there are infinitely many solutions
- We do this by induction on n
- If $n = 2$, we have already found that there are infinitely many solutions.
- Now suppose that any linear Diophantine equation of less than n variables has infinitely many solutions
- Let's focus on the first two variables briefly.
- We know that the set of linear combinations of a_1 and a_2 is the same as the set of multiples of (a_1, a_2)
- This implies that for any $y \in \mathbb{Z}$, there exists $x_1, x_2 \in \mathbb{Z}$ with $a_1x_1 + a_2x_2 = (a_1, a_2)y$
- So every solution to $(a_1, a_2)y + a_3x_3 + \cdots a_nx_n = c$ gives a solution to $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$
- But $((a_1, a_2), a_3, \ldots, a_n) = (a_1, \ldots, a_n) \mid c$, so by the induction hypothesis $(a_1, a_2)y + a_3x_3 + \cdots a_nx_n = c$ has infinitely many solutions
- Hence, $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ has infinitely many solutions
- How do you find them?
- Generalize the previous algorithm.
- Not really worth it to spend lecture time on that.