Math 1365 (Intensive Mathematical Reasoning)

Lecture #13 of 35 $\sim$ October 5, 2023

The Euclidean Algorithm + Primes and Factorizations

- The Euclidean Algorithm (continued)
- Primes
- Unique Prime Factorization

This material represents §2.3.3-§2.4 from the course notes.

The Euclidean Algorithm, I

Recall the Euclidean algorithm from yesterday:

Theorem (Euclidean Algorithm)

Given integers $0 < b < a$, repeatedly apply the division algorithm as follows, until a remainder of zero is obtained:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ r_k &= q_{k+2} r_{k+1}. \end{aligned}$$

Then $\gcd(a, b)$ is equal to the last nonzero remainder, r_{k+1}. Furthermore, by successively solving for the remainders and plugging in the previous equations, r_{k+1} can be explicitly written as a linear combination of a and b.

The Euclidean Algorithm, II

Let's now show that the Euclidean algorithm works. There are a few pieces to this:

- First, we need to see that the algorithm will always terminate (i.e., it won't continue going forever without returning a result).

The Euclidean Algorithm, II

Let's now show that the Euclidean algorithm works. There are a few pieces to this:

- First, we need to see that the algorithm will always terminate (i.e., it won't continue going forever without returning a result).
- That's not too hard to see, because each remainder is strictly less than the previous one: $b > r_1 > r_2 > \cdots \geq 0$. Then the well-ordering axiom dictates that we cannot have an infinite decreasing sequence of nonnegative integers.
- So we must eventually get a remainder of zero, and then the algorithm terminates.

The Euclidean Algorithm, III

Second: We need to show that if $d|a$ and $d|b$, then $d|r_{k+1}$ (the last nonzero remainder).

- We will show more: that if $d|a$ and $d|b$ then in fact $d|r_n$ for all n. We use induction on n.

The Euclidean Algorithm, III

Second: We need to show that if $d|a$ and $d|b$, then $d|r_{k+1}$ (the last nonzero remainder).

- We will show more: that if $d|a$ and $d|b$ then in fact $d|r_n$ for all n. We use induction on n.
- A cheap way to avoid having to do too much work is to denote $r_0 = b$ and $r_{-1} = a$, and then start with these two remainders.
- So: we take base cases $k = -1$ and $k = 0$: then $d|r_{-1} = a$ and $d|r_0 = b$.
- For the inductive step suppose $d|r_k$ and $d|r_{k-1}$. Then $r_{k+1} = r_{k-1} - q_k r_k$. Since both terms r_{k-1} and $q_k r_k$ are divisible by d, so is their difference r_{k+1}.

The Euclidean Algorithm, IV

Third: We show that $r_{k+1} | a$ and $r_{k+1} | b$. Combined with the previous slide this will show r_{k+1} is the gcd, since it's a common divisor divisible by all the other common divisors.

- For this we induct "downwards" by showing $r_{k+1} | r_n$ for all n.

The Euclidean Algorithm, IV

Third: We show that $r_{k+1}|a$ and $r_{k+1}|b$. Combined with the previous slide this will show r_{k+1} is the gcd, since it's a common divisor divisible by all the other common divisors.

- For this we induct "downwards" by showing $r_{k+1}|r_n$ for all n.
- For base cases we observe $r_{k+1}|r_{k+1}$ and $r_{k+1}|r_k$ because $r_k = q_{k+1}r_{k+1}$.
- For the inductive step we observe $r_{n-1} = q_{n+1}r_n + r_{n+1}$, and by hypothesis the last nonzero remainder divides both r_n and r_{n+1}, so it also divides r_{n-1}.
- Moving all the way downward we see that r_{k+1} divides $r_0 = b$ and then $r_{-1} = a$, as desired.

The Euclidean Algorithm, V

Finally, we need to see that the last nonzero remainder can be written in terms of the original integers.

- It may surprise you, but this follows from another induction argument!

The Euclidean Algorithm, V

Finally, we need to see that the last nonzero remainder can be written in terms of the original integers.

- It may surprise you, but this follows from another induction argument!
- Explicitly, for base cases we take $r_{-1} = a = 1 \cdot a + 0 \cdot b$ and $r_0 = b = 0 \cdot a + 1 \cdot b$.
- For the inductive step, if we can write r_{n-1} and r_n in terms of a, b, then since $r_{n+1} = r_{n-1} - q_{n+1} r_n$, plugging in those expressions will yield r_{n+1} in terms of a, b as well.

And that establishes the correctness of the Euclidean algorithm! (Yay.)

The Euclidean Algorithm, VI

Example: Find $\gcd(565, 1241)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 565 and 1241.

The Euclidean Algorithm, VI

Example: Find $\gcd(565, 1241)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 565 and 1241.

- First, we use the Euclidean algorithm:

$$\begin{aligned} 1241 &= 2 \cdot 565 + 111 \\ 565 &= 5 \cdot 111 + 10 \\ 111 &= 11 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 \end{aligned}$$

and so the gcd is $\boxed{1}$.

The Euclidean Algorithm, VI

Example: Find $\gcd(565, 1241)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 565 and 1241.

- First, we use the Euclidean algorithm:

$$\begin{aligned} 1241 &= 2 \cdot 565 + 111 \\ 565 &= 5 \cdot 111 + 10 \\ 111 &= 11 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 \end{aligned}$$

  and so the gcd is $\boxed{1}$.

- For the linear combination, we solve for the remainders:

$$\begin{array}{ccccc} 111 & = & 1241 - 2 \cdot 565 & = & 1 \cdot 1241 - 2 \cdot 565 \\ 10 & = & 565 - 5 \cdot 111 & = & -5 \cdot 1241 + 11 \cdot 565 \\ 1 & = & 111 - 11 \cdot 10 & = & 56 \cdot 1241 - 123 \cdot 565 \end{array}$$

  so we obtain $\boxed{1 = 56 \cdot 1241 - 123 \cdot 565}$.

Primes

Now let's talk about the other fundamental property of the integers: the existence and uniqueness of prime factorizations. Here (again) is the official definition of a prime number:

Definition

If $p > 1$ is an integer, we say it is <u>prime</u> if there is no integer d with $1 < d < p$ such that $d|p$. An integer $n > 1$ that is not prime is called <u>composite</u>, because $n = ab$ for some $1 < a, b < n$.

- The primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.
- The prime numbers are often called the "building blocks under multiplication", because every positive integer can be written as the product of prime numbers in an essentially unique way. (Analogy: chemical elements.)

Prime Factorizations, I

Let's start by showing that every positive integer *has* a prime factorization:

Proposition (Existence of Prime Factorizations)

Every positive integer n can be written as a product of zero or more primes (where a "product" is allowed to have only one term, and the empty product has value 1).

- Some examples: $30 = 2 \cdot 3 \cdot 5$, $9 = 3 \cdot 3$, $17 = 17$, $12 = 2 \cdot 2 \cdot 3$.
- The representation of n as a product of primes is called the prime factorization of n. Our goal is to show it's unique, up to reordering the terms.

Prime Factorizations, II

Proof:

- We use strong induction on n. The result clearly holds if $n = 1$, since 1 is the empty product.
- Now suppose $n \geq 2$. If n is prime, we are done: simply take the product n with one term.
- So assume that n is not prime, hence composite since $n \geq 2$.
- By definition, there exists a d with $1 < d < n$ such that $d|n$: then n/d is an integer satisfying $1 < n/d < n$.
- By the strong induction hypothesis, both d and n/d can be written as a product of primes; multiplying these two products then yields n as a product of primes.

Prime Factorizations, III

To establish the uniqueness of prime factorizations, we require the following prime divisibility property:

Proposition (Prime Divisibility)

If a and b are integers and p is a prime number with $p|ab$, then $p|a$ or $p|b$.

Example: If $2|ab$, then $2|a$ or $2|b$. Or, equivalently, if a product of two integers is even, then at least one of the integers must have been even. (True!)

Prime Factorizations, IV

Proof:

- Let's instead prove the contrapositive: For a prime p, if $p \nmid a$ and $p \nmid b$ then $p \nmid ab$.
- So suppose $p \nmid a$ and $p \nmid b$.
- Consider $\gcd(a, p)$: it divides p, hence is either 1 or p since p is prime. But the gcd cannot be p because p doesn't divide a.
- So $\gcd(a, p) = 1$, meaning a and p are relatively prime.
- By the same logic, b and p are relatively prime.
- But now recall one of the properties from yesterday: if a and b are both relatively prime to an integer m, then so is ab. Applying that here shows immediately that ab is relatively prime to p.
- Finally, that tells us $p \nmid ab$, because otherwise we would have $\gcd(ab, p) = p$, but the gcd is 1.

Prime Factorizations, V

Now we can show the uniqueness of prime factorizations:

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be factored into a product of primes, and this factorization is unique up to reordering of the factors.

Note that we already showed that every positive integer has a prime factorization, so we only need to show that factorizations are unique up to reordering.

Prime Factorizations, VI

Proof:

- Strong induction on the integer n. The base case $n = 1$ is immediate, since any nonempty product will be larger than 1.

Prime Factorizations, VI

Proof:

- Strong induction on the integer n. The base case $n = 1$ is immediate, since any nonempty product will be larger than 1.
- Now suppose every positive integer less than n has a unique prime factorization, and suppose we have two prime factorizations $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$.
- Since p_1 is prime and divides the product $q_1 q_2 \cdots q_l$, by the prime divisibility property applied repeatedly, we see that p_1 divides some prime q_i. By rearranging, we can assume $p_1 | q_1$.
- But q_1 is prime, so its only positive divisors are 1 and itself. Since $p_1 | q_1$ and $p_1 \neq 1$ (1 is not prime), $p_1 = q_1$.

Prime Factorizations, VI

Proof:

- Strong induction on the integer n. The base case $n = 1$ is immediate, since any nonempty product will be larger than 1.
- Now suppose every positive integer less than n has a unique prime factorization, and suppose we have two prime factorizations $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$.
- Since p_1 is prime and divides the product $q_1 q_2 \cdots q_l$, by the prime divisibility property applied repeatedly, we see that p_1 divides some prime q_i. By rearranging, we can assume $p_1 | q_1$.
- But q_1 is prime, so its only positive divisors are 1 and itself. Since $p_1 | q_1$ and $p_1 \neq 1$ (1 is not prime), $p_1 = q_1$.
- Now, by the induction hypothesis, the prime factorization of $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_l$ is unique, so the primes $q_2, \dots, q_l$ are some rearrangement of $p_2, \dots, p_k$.
- Since $p_1 = q_1$ also, that means the two factorizations of n are just rearrangements! Victory.

Applications of Factorizations, I

Let's mention a few applications of prime factorizations.

Proposition (Divisibility and Factorizations)

Suppose that a and b have prime factorizations given by $a = \prod_{i=1}^{j} p_i^{a_i}$ and $b = \prod_{i=1}^{j} p_i^{b_i}$ for distinct primes p_i. Then

1. *We have $a|b$ if and only if $a_i \leq b_i$ for each i.*
2. *We have $\gcd(a, b) = \prod_{i=1}^{j} p_i^{\min(a_i, b_i)}$ and $\operatorname{lcm}(a, b) = \prod_{i=1}^{j} p_i^{\max(a_i, b_i)}$.*

What this proposition tells us is how to understand divisibility in terms of prime factorizations: it says a divides b when the power of each prime in the factorization of a is $\leq$ the corresponding power of each prime in b.

Applications of Factorizations, II

Before doing the proof let's look at a few examples:

- Does $a = 2^3 3^2 5^1$ divide $b = 2^4 3^3 5^1$?

Applications of Factorizations, II

Before doing the proof let's look at a few examples:

- Does $a = 2^3 3^2 5^1$ divide $b = 2^4 3^3 5^1$? Yes: just divide to see $(2^4 3^3 5^1)/(2^3 3^2 5^1) = 2^{4-3} 3^{3-2} 5^{1-1} = 2^1 3^1 5^0 = 6$, which is an integer.
- Does $a = 2^3 3^2 5^1$ divide $b = 2^2 3^4 5^2$?

Applications of Factorizations, II

Before doing the proof let's look at a few examples:

- Does $a = 2^3 3^2 5^1$ divide $b = 2^4 3^3 5^1$? Yes: just divide to see $(2^4 3^3 5^1)/(2^3 3^2 5^1) = 2^{4-3} 3^{3-2} 5^{1-1} = 2^1 3^1 5^0 = 6$, which is an integer.
- Does $a = 2^3 3^2 5^1$ divide $b = 2^2 3^4 5^2$? No: if we divide we get $(2^2 3^4 5^2)/(2^3 3^2 5^1) = 2^{2-3} 3^{4-2} 5^{2-1} = 2^{-1} 3^2 5^1 = 45/2$ which isn't an integer. The problem is that a has a higher power of 2 than b does.
- The idea is that for a to divide b, each prime must appear in at least as high a power in b as in a.

Applications of Factorizations, III

1. For $a = \prod_{i=1}^{j} p_i^{a_i}$ and $b = \prod_{i=1}^{j} p_i^{b_i}$, $a|b$ if and only if $a_i \leq b_i$ for each i.

Proof:

- Suppose $a|b$ so that $b = ak$ for some integer k.
- If k has prime factorization $k = \prod_{i=1}^{j} p_i^{k_i}$, then $a_i + k_i = b_i$ by uniqueness of prime factorizations.
- Since all exponents are nonnegative, this means $a_i \leq b_i$ for each i.
- Conversely, if $a_i \leq b_i$ for each i, then taking $k_i = b_i - a_i$ and $k = \prod_{i=1}^{j} p_i^{k_i}$ yields an integer such that $b = ak$ (as follows by comparing the factorizations.

Applications of Factorizations, IV

2. For $a = \prod_{i=1}^{j} p_i^{a_i}$ and $b = \prod_{i=1}^{j} p_i^{b_i}$, we have $\gcd(a, b) = \prod_{i=1}^{j} p_i^{\min(a_i, b_i)}$ and $\mathrm{lcm}(a, b) = \prod_{i=1}^{j} p_i^{\max(a_i, b_i)}$.

Proof:

- Consider the prime factorization of a common divisor $d = \prod_{i=1}^{j} p_i^{d_i}$.
- By the result we just proved, since $d|a$ and $d|b$, we must have $d_i \leq a_i$ and $d_i \leq b_i$ for each i.
- This means $d_i \leq \min(a_i, b_i)$. But if we take $d_i = \min(a_i, b_i)$ then the resulting value of d is a common divisor, and so $\gcd(a, b) = \prod_{i=1}^{j} p_i^{\min(a_i, b_i)}$.
- A similar argument with $a|l$ and $b|l$ with the lcm yields the formula for the lcm.

Applications of Factorizations, V

Example: Find the gcd and lcm of $2^2 3^3 5^2 7^1$ and $2^3 3^3 5^1 7^2$.

Applications of Factorizations, V

Example: Find the gcd and lcm of $2^2 3^3 5^2 7^1$ and $2^3 3^3 5^1 7^2$.

- The gcd has each prime to the smaller power that appears, which yields $\gcd = 2^2 3^3 5^1 7^1$.
- The lcm has each prime to the larger power that appears, which yields $\text{lcm} = 2^3 3^3 5^2 7^2$.
- Intuitively, the idea is that for the gcd, we want to take as many factors for each prime as possible, while still making sure that $d|a$ and $d|b$. For the lcm, we want to use as few factors as possible, while still making sure that $a|l$ and $b|l$.

Applications of Factorizations, VI

One question we might have is: how many primes are there? The most basic answer to this question is that there are infinitely many primes:

Theorem (Euclid's Theorem)

There are infinitely many prime numbers.

In fact, you already saw this proof on the first day of the course, but now we have enough tools to understand how it works.

Applications of Factorizations, VII

Proof:

- Suppose there are only finitely many primes $p_1, p_2, \ldots, p_k$ and consider $n = p_1 p_2 \cdots p_k + 1$.
- Since n is greater than each p_i, n cannot be prime (since it would necessarily have to be on the list).
- Therefore n is composite. Consider the prime factorization of n: since $n > 1$, the factorization has at least one prime, which must appear on the list. Suppose that p_i divides n.
- Since p_i also divides $p_1 p_2 \cdots p_k$, we see that p_i therefore divides $n - p_1 p_2 \cdots p_k = 1$.
- But this is a contradiction because 1 has no prime divisors. Hence there are infinitely many primes.

Applications of Factorizations, VIII

Another particularly famous use of prime factorizations is in proving that $\sqrt{2}$ is irrational:

Proposition (Irrationality of $\sqrt{2}$)

The number $\sqrt{2}$ is irrational, which is to say, there do not exist integers m and n such that $\sqrt{2} = m/n$.

Naturally, because we are trying to prove that there do not exist integers with this claimed property, we need to do a proof by contradiction.

Applications of Factorizations, IX

Proof:

- Suppose by way of contradiction that $\sqrt{2}$ were rational so that $\sqrt{2} = m/n$ for some integers m and n, which (by negating if needed) we may assume are positive.
- Squaring both sides and clearing denominators yields the equivalent equation $2n^2 = m^2$.

Applications of Factorizations, IX

Proof:

- Suppose by way of contradiction that $\sqrt{2}$ were rational so that $\sqrt{2} = m/n$ for some integers m and n, which (by negating if needed) we may assume are positive.
- Squaring both sides and clearing denominators yields the equivalent equation $2n^2 = m^2$.
- Now consider the prime factorizations of both sides: say $m = 2^{m_2}3^{m_3}\cdots$ and $n = 2^{n_2}3^{n_3}\cdots$.
- We obtain the equality $2^{2m_2+1}3^{m_3}\cdots = 2^{2n_2}3^{2n_3}\cdots$, and so by the uniqueness of prime factorizations, all of the corresponding exponents must be equal.
- In particular, $2m_2 + 1 = 2n_2$, so that $2(n_2 - m_2) = 1$. But this is impossible, because 2 does not divide 1.
- Therefore, it could not have been true that $\sqrt{2} = m/n$, so $\sqrt{2}$ must be irrational as claimed.

Other Things About Primes, I

Even though the prime numbers appear quite simple, in fact there are very many difficult problems, and very many more unsolved problems, in number theory involving primes. Here are a few:

Other Things About Primes, II

Q: How common are primes?

- Euclid's proof shows that there are infinitely many primes, but that doesn't say much about how common they are.
- Are they as common as even numbers? Or are they more like squares, which are rarer? Or somewhere in between?
- More precisely, consider the function $\pi(n)$ counting the number of primes $\leq n$: how does $\pi(n)$ behave as $n \to \infty$?

Other Things About Primes, II

Q: How common are primes?

- Euclid's proof shows that there are infinitely many primes, but that doesn't say much about how common they are.
- Are they as common as even numbers? Or are they more like squares, which are rarer? Or somewhere in between?
- More precisely, consider the function $\pi(n)$ counting the number of primes $\leq n$: how does $\pi(n)$ behave as $n \to \infty$?
- For example, $\pi(100) = 25$ since there are 25 primes less than 100, while $\pi(1000) = 168$, $\pi(10^4) = 1229$, $\pi(10^5) = 9592$, $\pi(10^6) = 78498$, and $\pi(10^7) = 664579$.
- It seems like $\pi(n)$ is growing a lot faster than $\sqrt{n}$ but slower than n itself. Any ideas what the growth rate might be?

Other Things About Primes, II

Q: How common are primes?

- Euclid's proof shows that there are infinitely many primes, but that doesn't say much about how common they are.
- Are they as common as even numbers? Or are they more like squares, which are rarer? Or somewhere in between?
- More precisely, consider the function $\pi(n)$ counting the number of primes $\leq n$: how does $\pi(n)$ behave as $n \to \infty$?
- For example, $\pi(100) = 25$ since there are 25 primes less than 100, while $\pi(1000) = 168$, $\pi(10^4) = 1229$, $\pi(10^5) = 9592$, $\pi(10^6) = 78498$, and $\pi(10^7) = 664579$.
- It seems like $\pi(n)$ is growing a lot faster than $\sqrt{n}$ but slower than n itself. Any ideas what the growth rate might be?
- In fact, the answer is given by the Prime Number Theorem: $\pi(n) \sim \dfrac{n}{\ln n}$ as $n \to \infty$. (Yes, that's the natural logarithm.)

Other Things About Primes, III

Q: How close do primes get?

- Obviously, 2 and 3 differ by 1, but since 2 is the only even prime, any other pair of primes must differ by at least 2.
- Primes that differ by 2 (like 5 and 7, or 17 and 19) are called "twin primes". One can write down many pairs of twin primes, even very large ones.

Other Things About Primes, III

Q: How close do primes get?

- Obviously, 2 and 3 differ by 1, but since 2 is the only even prime, any other pair of primes must differ by at least 2.
- Primes that differ by 2 (like 5 and 7, or 17 and 19) are called "twin primes". One can write down many pairs of twin primes, even very large ones.
- For example, 99989 and 99991 are both prime, as are 643301 and 643303, and 1866633479 and 1866633481, just to give three fairly small random examples.
- But are there infinitely many pairs of twin primes?
- In fact, we don't know! There are heuristics suggesting there should be infinitely many pairs of twin primes (indeed, the arguments used for the Prime Number Theorem suggest there should be about $n/(\ln n)^2$ of them that are $\leq n$), but this problem is still unsolved.

Summary

We discussed the Euclidean algorithm and how to use it to calculate greatest common divisors.

We discussed prime numbers and unique prime factorization.

We discussed some applications of prime factorization, and some other questions about primes.

Next lecture: Modular congruences and residue classes.