Math Circles - Elementary Number Theory - Fall 2023

Week 1 (Nov 15)

Welcome to this session of Math Circles! For the next three weeks, we'll be looking at elementary number theory. What is that? Well, as the name suggests, "number theory" is the study of numbers; in particular, it is the study of integers. The word "elementary" doesn't mean that it's "easy," but rather that we will not be using complex analysis (or anything else stemming from calculus) in order to do so. Today, we will go through some of the basic building blocks we need to study elementary number theory in more depth.

Greatest Common Divisors

We're going to start out by talking about division. This is something you've known about for many years at this point, but we're going to look at it from a different point of view from how it would have been taught to you in school.

Theorem. *(Division Theorem) Let a and b be integers such that $b \neq 0$. Then there exist unique integers q and r, where $r < |b|$, such that $a = bq + r$.*[1]

In the Division Theorem, we call a the *dividend*, b the *divisor*, q the *quotient*, and r the *remainder*.

This seems like a very simple result, but it's actually quite foundational in number theory. Based on this theorem, we can define what it means for an integer to divide another integer.

Definition. *Let a and b be integers such that $b \neq 0$. We say that b divides a (and write $b \mid a$) if there exists an integer q such that $a = bq$. In this case, we call b a divisor (or a factor) of a.*

In other words, a divides b if the remainder given by the division theorem is 0. It is worth noting that if $b \mid a$, then $|b| \leq |a|$.
Before getting into the next section, there are a few useful properties of divisors that we should know.

Theorem. *Let a and b be integers.*

1. *If $a \mid b$, then $a \mid xb$ for all integers x.*
2. *If $a \mid b$ and $a \mid c$, then $a \mid b \pm c$.*
3. *If $a \mid b$ and $a \mid c$, then $a \mid xb \pm yc$ for all integers x and y.*
4. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

The proofs of the above will be left as exercises.

In number theory, we are often interested in when numbers have common divisors.

Definition. *Let a and b be integers. We say that d is the greatest common divisor (GCD) of a and b if $d \mid a$, $d \mid b$, and $d \geq x$ for all x such that $x \mid a$ and $x \mid b$.*

[1] The proof is omitted here, as it is not terribly enlightening, but if you are interested, it can be found at https://en.wikipedia.org/wiki/Euclidean_division#Proof

Put simply, d is the largest positive integer that divides both a and b. From this definition, we get a few immediate results:

Theorem. *Let a and b be integers. Then a greatest common divisor of a and b exists, and is unique.*

Proof. First, let's prove existance. There are two cases when this statement could be false:

- If there are no common divisors of a and b.
- If there are is no upper bound on the common divisors of a and b (i.e, there are infinitely many common divisors, which keep increasing, and in this case, a maximum doesn't exist).

Since $1 \mid a$ and $1 \mid b$, then a and b have a common divisor (so, case 1 is not a problem). Now, without loss of generality[2], suppose $a \leq b$. Since every common divisor must divide a, that means that no common divisor can have absolute value greater than $|a|$. So, $|a|$ is an upper bound on $\gcd(a, b)$ (so, case 2 is not a problem). Therefore $\gcd(a, b)$ exists.
Now, we need to show uniqueness. Let d and d' both be greatest common divisors of a and b. Since d is a greatest common divisor, we have that $d \geq d'$, and since d' is a greatest common divisor, we have that $d' \geq d$. So, $d = d'$, and ■

Okay, so GCDs exist. That's great, but how do we compute them? Let's go through a few examples.

Example. *Compute the following:*

(a) $\gcd(6, 8)$

Solution. The factors of 6 are 1, 2, 3, and 6. The factors of 8 are 1, 2, 4, and 8. The largest number in both of these lists is 2. So, $\gcd(6, 8) = 2$. ■

(b) $\gcd(38, 76)$

Solution. The largest factor of 38 is 38, so $\gcd(38, 76) \leq 38$. Since $76 = 2 \cdot 38$, then 38 is also a factor of 76, and hence $\gcd(38, 76) \geq 36$. So, $\gcd(38, 76) = 38$. ■

(c) $\gcd(7112, 456)$

Solution. Listing all factors seems like a bad idea, and $456 \nmid 7112$, so we can't use the same trick as in part (b). Let's come back to this example later. ■

As we saw above, it is not always obvious at first glance what the GCD of two numbers is. However, there's an efficient way to compute GCDs! Before we get there, though, let's prove the following fact:

Theorem. *Let a and b be integers, and let q and r be such that $a = qb + r$ by the Division Theorem. Then* $\gcd(a, b) = \gcd(r, b)$.

Proof. Let $d := \gcd(a, b)$, and let $d' := \gcd(r, b)$. By definition of GCD, we have that $d \mid a$ and $d \mid b$. Since $d \mid b$, we have that $d \mid qb$. Since $d \mid a$ as well, we get that $d \mid a - qb$. But $a - qb = r$, so $d \mid r$, so d is a common divisor of b and r, so $d \leq d'$. Similarly, we have that $d' \mid r$ and $d' \mid b$. Since $d' \mid b$, we have that $d' \mid qb$. Since $d' \mid r$ as well, we get that $d' \mid qb + r$, and hence $d' \mid a$. So d' is a common divisor of a and b, and hence $d' \leq d$. Since $d \leq d'$ and $d' \leq d$, we get that $d = d'$. ■

Now we have enough material to be able to compute GCDs efficiently.

[2] *Without loss of generality* means that even though we are picking a case to analyze, it doesn't matter which case we pick, because the proof is the same for each case.

Theorem. *(Euclidean Algorithm) Let a and b be integers, and consider the sequence of equations*

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{N-2} &= q_N r_{N-1} + r_N \end{aligned}$$

where N is the smallest integer such that $r_N = 0$. Then $\gcd(a, b) = r_{N-1}$.

Proof. To prove that this algorithm works, we actually have to prove two things. First, we need to prove that it terminates; that is, we need to prove that there always exists an integer N such that $r_N = 0$. Then, we need to prove that r_{N-1} is in fact the GCD of a and b.

First, we'll prove that there always exists an integer N such that $r_N = 0$. By the Division Theorem, we have that $|b| > r_0 > r_1 > \cdots$, and that each remainder r_i is an integer greater than or equal to 0. So, after finitely many steps, we must arrive at $r_N = 0$.

Now, we'll prove that $r_{N-1} = \gcd(a, b)$. By the previous theorem, we have that:

$$\begin{aligned} \gcd(a, b) &= \gcd(b, r_0) \\ \gcd(b, r_0) &= \gcd(r_0, r_1) \\ \gcd(r_0, r_1) &= \gcd(r_1, r_2) \\ &\vdots \\ \gcd(r_{N-2}, r_{N-1}) &= \gcd(r_{N-1}, r_N) \end{aligned}$$

But $r_N = 0$, so $\gcd(r_{N-1}, r_N) = \gcd(r_{N-1}, 0) = r_{N-1}$, so $\gcd(a, b) = r_{N-1}$. ■

Now, let's go back to the example we tried earlier.

Example. *Compute* $\gcd(7112, 456)$.

Solution. By following the Euclidean Algorithm, we get:

$$\begin{aligned} 7112 &= 15(456) + 272 \\ 456 &= 1(272) + 184 \\ 272 &= 1(184) + 88 \\ 184 &= 2(88) + 8 \\ 88 &= 11(8) + 0 \end{aligned}$$

So, $\gcd(7112, 456) = 8$. ■

One last important theorem, before we move into the next section, is Bézout's Lemma. It seems a little random right now, but in the next few weeks it will come in handy.

Theorem. *(Bézout's Lemma) Let a, b, and d be integers. Then there exist integers x and y such that $ax + by = \gcd(a, b)$.*

Proof. Let $S = \{ax + by : x \text{ and } y \text{ are integers, and } ax + by > 0\}$. That is, for all possible values of x and y, we put $ax + by$ in the set S if and only if $ax + by > 0$. First, note that S contains at least one element, since $|a| \in S$ (if we set $x = 1$ if $a > 0$ or $x = -1$ if $a < 0$, and set $y = 0$, then $ax + by = |a|$). So, since S has at least one element, and all elements of S are integers greater than

0, then S must have a minimum element, which we'll call d.

By the Division Theorem, we can write $a = dq + r$ for integers q and r, with $0 \leq r < d$. For some integers x and y, we have that

$$r = a - dq = a - (ax + by)q = a - aqx + bqy = a(1 - qx) + b(qy).$$

So, either $r \in S$, or $r = 0$. But since $0 \leq r < d$, and d is the smallest element in S, then it must be the case that $r = 0$. So, $d \mid a$. We can write an identical argument to show that $d \mid b$. So, d is a common divisor of a and b.

It remains to show that if c is common divisor of a and b, then $c \leq d$. Since $c \mid a$ and $c \mid b$, we can write $a = cu$ and $b = cv$ for some integers u and v. By definition of d, there also exist integers x and y such that $d = ax + by$. So,

$$d = ax + by = cux + cvy = c(ux + by).$$

So, $c \mid d$ and since $d > 0$, $c \leq d$. Hence $d = \gcd(a, b)$. ■

Prime Numbers

Definition. *An positive integer p is prime if it has exactly two distinct positive divisors.*

Since every positive integer n is divisible by 1 and n, this means that prime numbers are those which have no other divisors. This also means that 1 is not a prime number, since it is only divisible by one positive integer.

Definition. *An positive integer n is composite if there exists a positive integer p such that $p \mid n$, where $p \neq 1$ and $p \neq n$.*

Under this definition, 1 is also not a composite number. This means that the composite numbers are all positive integers, other than 1, which are not prime.

Prime numbers have been studied for thousands of years, and you probably already know a number of very significant results about them, which seem "obvious," but are actually extremely important in number theory. For instance:

Theorem. *(Fundamental Theorem of Arithmetic) Let n be a positive integer. Then n can be factored uniquely as a product of primes.*

This means that for any positive integer n, we can write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$, and positive integers $e_1, \ldots e_k$. There are many proofs of this theorem, but we're just going to take it as a fact.

Example. *The following are prime factorizations:*

- $12 = 2^2 \cdot 3$
- $70 = 3 \cdot 5 \cdot 7$
- $2023 = 7 \cdot 17$
- $934\,949\,400 = 2^3 \cdot 3 \cdot 5^2 \cdot 7^4 \cdot 11 \cdot 59$

As you can see by the last example, finding the prime factorization of an integer isn't always easy. In fact, there is no known way of doing this efficiently, without a quantum computer!

Definition. *Let a and b be integers. We say that a and b are relatively prime if they have no common factors (other than ± 1).*

Notice that if a and b are relatively prime, it must be the case that $\gcd(a, b) = 1$, since $\gcd(a, b)$ is a common factor of a and b. So, to check if two integers are relatively prime, we can simply compute their GCD using the Euclidean Algorithm.

Relatively prime integers are going to be very important to us in the next few weeks. In particular, given an integer n, we are going to want to know how many integers between 1 and n are relatively prime with n. This is such an important piece of information that there's an entire function dedicated to it.

Definition. *Euler's Totient Function, $\Phi(n)$, counts the number of integers less than or equal to n which are relatively prime with n.*

To get a feel for this, lets go through some examples.

Example. *Compute the following:*

(a) $\Phi(5)$

Solution. Since 5 is prime, it has no factors, so all smaller integers are relatively prime with 5. So, $\Phi(5) = 4 - 1$. ■

(b) $\Phi(8)$

Solution. All factors of 8 are even, so 8 is only relatively prime with odd integers less than 8. So, 8 is relatively prime with 1, 3, 5, and 7. Hence $\Phi(8) = 4$. ■

(c) $\Phi(24)$

Solution. The prime factorization of 24 is $24 = 2^3 \cdot 3$. So, 24 is relatively prime with all integers that do not have 2 or 3 as a factor. This would be: 5, 7, 11, 13, 17, 19, 23. So, $\Phi(24) = 7$. ■

Computing $\Phi(n)$ by checking whether each integer less than n is relatively prime with n is boring, time consuming, and prone to error. Luckily, there's a better way! First, let's consider $\Phi(p)$, where p is prime.

Theorem. *If p is prime then*

$$\Phi(p) = p - 1.$$

Proof. Since p is prime, it has no factors other than 1 and p. So, it cannot have any common factors with any integers less than p, so it is relatively prime with all integers less than p, other than 1. There are $p - 1$ such integers, so $\Phi(p) = p - 1$. ■

The next simplest case is when n is a prime power. That is, when $n = p^e$ for some prime p and exponent $e \geq 1$.

Theorem. *If $n = p^e$, where p is prime and $e \geq 1$, then*

$$\Phi(n) = p^{e-1}(p - 1).$$

Proof. The only integers m less than n such that $\gcd(n, m) \neq 1$ are $p, 2p, 3p, \ldots, p^{k-1}p$. There are p^{k-1} such multiples of p. So, there are $p^k - p^{k-1} = p^{k-1}(p-1)$ integers less than or equal to p which are relatively prime with p. So, $\Phi(n) = p^{k-1}(p - 1)$. ■

Before we move onto the general formula, a useful property to point out is that Φ is multiplicative. This will help us prove the general formula.

Theorem. *Let n and m be integers such that* $\gcd(n, m) = 1$. *Then $\Phi(nm) = \Phi(n)\Phi(m)$.*

We won't prove this, as it relies on a result called the Chinese Remainder Theorem, which we haven't seen yet. But we'll use the result here:

Theorem. *(Euler's Product Formula) Let* $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ *be the prime factorization of* n*. Then*

$$\Phi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).$$

Proof. Since Φ is multiplicative, we have that

$$\Phi(n) = \Phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \Phi(p_1^{e_1})\Phi(p_2^{e_2}) \cdots \Phi(p_k^{e_k}).$$

Bur for each i, we have that $\Phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$. So, we get that

$$\Phi(p_1^{e_1})\Phi(p_2^{e_2}) \cdots \Phi(p_k^{e_k}) = p_1^{e_1-1}(p_1 - 1) \ldots p_k^{e_k-1}(p_k - 1),$$

as desired. ■