Recall the notation $\mathbb{Q} := \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$. It turns out that 100% of all real numbers are *not* in $\mathbb{Q}$! (To learn more about this, take Math 350.)

Recall that when we talk about simplifying fractions, there are a couple of different things we might mean:

Interpretation 1: $\frac{19}{4} = 4 + \frac{3}{4}$ Interpretation 2: $\frac{6}{9} = \frac{2}{3}$.

Interpretation 1: Given $a > b > 0$ with $a, b \in \mathbb{Z}$. We can write $\frac{a}{b} = q + \frac{r}{b}$ where $0 \leq r < b$ and q is the largest integer less than $\frac{a}{b}$. Notice that multiplying by b, we get $a = bq + r$, which is exactly what we proved before! This also explains where the proof came from (recall that we chose $q = \lfloor \frac{a}{b} \rfloor$ in that proof).

Interpretation 2: Given $\frac{a}{b} \in \mathbb{Q}$ we'd like to reduce it, i.e. rewrite $\frac{a}{b} = \frac{a/\gcd(a,b)}{b/\gcd(a,b)}$.
Example: $\frac{312}{453}$, is this reduced? No! Because Ben points out that both 312 and 453 are divisible by 3 because there is a 'rule' (to be proven later) that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Example: $\frac{203}{416}$ reduced? Oliver: yes! because $203 = 7 \times 29$ and $416 = 2^5 \times 13$ so these are relatively prime.

In general finding the prime factorization takes wayyy too long (imagine replacing our three digit numbers to 100-digit numbers!). Is there a way to check whether a fraction is reduced without finding the prime factorizations of numerator and denominator?

<u>Alternative Approach:</u> Suppose d is a common divisor of 203 and 416. So then d also divides $416 - 203 = 213$. So then d also divides $213 - 203 = 10$. Thus $d = 1, 2, 5$, or 10. Notice $2, 5, 10$ are not factors of 203, so $d = 1$. In other words, the only (and therefore greatest) common factor of 203 and 416 is 1. Thus we were able to prove $\gcd(203, 416) = 1$ without factoring either of the two numbers! (Note that we didn't avoid factoring entirely, since we factored 10. However, we succeeded in reducing a difficult factoring problem to a much simpler one.)

Let's explore a second example of this approach. Is $\frac{204}{527}$ reduced? Ben: No! They are both divisible by 17. To see this, suppose $d \mid 527$ and $d \mid 204$. Then

$$d \mid 527 - 2(204) = 119 \implies d \mid 204 - 119 = 85 \implies d \mid 119 - 85 = 34 \implies d \mid 85 - 2(34) = 17.$$

Now it's straightforward to check whether or not 204 and 527 are multiples of 17 ($204 = 170 + 34$ and $527 = 510 + 17$).

The formal version of this process has a fancy name: the *Euclidean Algorithm*.[1] Given

[1] Named for the mathematician Euclid, who lived in Alexandria, Egypt around 300 BC. The word *algo-*

integers $a > b > 0$, we'd like to find $\gcd(a,b)$ without factoring a and b. Using our division algorithm, we know there exists $q, r \in \mathbb{Z}$ such that

$$a - qb = r$$

with $0 \le r < b$. The idea is to iterate this. The notation is clumsy, so we're going to suppress writing the q; instead we'll simply write $a - \_\_b$ to indicate that we're subtracting as many copies of b as possible to leave the answer non-negative. Using this notation we find

$$\begin{aligned} a - \_\_b &= r_1 & \qquad 0 &\le r_1 < b \\ b - \_\_r_1 &= r_2 & 0 &\le r_2 < r_1 \\ r_1 - \_\_r_2 &= r_3 & 0 &\le r_3 < r_2 \\ &\vdots & &\vdots \end{aligned}$$

We thus generate a sequence of strictly decreasing non-negative integers:

$$a > b > r_1 > r_2 > \cdots \ge 0.$$

This sequence cannot go on forever (why?), so there must exist some k such that $r_k \ne 0$ but $r_{k+1} = 0$. We can thus complete our sequence of equalities from above:

$$\begin{aligned} a - \_\_b &= r_1 & \qquad 0 &\le r_1 < b \\ b - \_\_r_1 &= r_2 & 0 &\le r_2 < r_1 \\ r_1 - \_\_r_2 &= r_3 & 0 &\le r_3 < r_2 \\ &\vdots & &\vdots \\ r_{k-2} - \_\_r_{k-1} &= r_k & 0 &\le r_k < r_{k-1} \\ r_{k-1} - \_\_r_k &= 0 \end{aligned}$$

Theorem. The final nonzero remainder produced by this process is the gcd of the initial two numbers. Writing this using our symbols from above: $r_k = \gcd(a,b)$. (You will prove this on your problem set this week.)

Let's see an example of the Euclidean algorithm in action. What's $\gcd(7,3)$?

$$\begin{aligned} 7 - 2(3) &= 1 \\ 3 - 3(1) &= 0 \end{aligned}$$

Since the last nonzero remainder is 1, we have $\gcd(3,7) = 1$.

rithm is also named after someone, the Persian mathematician al-Khwarizmi, who spent most of his working life in Baghdad around 800 AD.

The Euclidean algorithm is really nifty, but is surprisingly hard to remember. I therefore urge you to remember it in the simplified form given before the formal statement, with the examples of $\frac{203}{416}$ and $\frac{204}{527}$.

We next briefly touched on a few open questions in number theory.

1. Consider the decimal expansion $\pi = 3.1415926\cdots$. Are there infinitely many 1's in the decimal expansion? It seems like there should be about 10%, but we don't even know whether there are infinitely many 1's (or any other digit, for that matter). This happens not just for π, but for any naturally occurring irrational number like $\sqrt{2}$ and e.
2. How are the primes distributed? What is the 1000000th prime, for example? Brute force would tell us the answer, but takes a very long time. Is there a shortcut? Even though a precise formula for the n-th prime is unknown (and likely doesn't exist), there are some really good estimates available. We'll prove some of these in the next couple of weeks.
3. Studying solutions of equations in settings other than $\mathbb{R}$ or $\mathbb{C}$ is an important part of number theory. One major theorem we'll prove, related to solving quadratics in so-called *finite fields*, is the famous Quadratic Reciprocity law.
4. We'll discuss applications of number theory to cryptography.
5. We'll discuss continued fractions, a remarkably structured and beautiful way to represent real numbers that, in some ways, is much better than the decimal system.

Perhaps the main take-away from all this: number theory, being many millennia old, is a vast field. Our course will sample some of the biggest and most important parts, but it will (of necessity) be a bit of a hodge-podge.

And with this caveat, we dove into our next topic:

Irrationality:
On the homework due this Thursday, you prove that given $n \geq 1$, either $\sqrt{n} \in \mathbb{Z}$ or $\sqrt{n} \notin \mathbb{Q}$. This implies that $\sqrt{2} \notin \mathbb{Q}$ because $1 < \sqrt{2} < 2$. Here are some other proofs of the latter assertion.

Theorem: $\sqrt{2} \notin \mathbb{Q}$.
Proof 1: Suppose $\sqrt{2} \in \mathbb{Q}$, i.e. $\sqrt{2} = \frac{a}{b}$ where we may assume that $\frac{a}{b}$ is reduced. Then

$$2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a \Rightarrow a = 2c \text{ for } c \in \mathbb{Z} \Rightarrow 2b^2 = a^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$$

but now we have that a and b are both even, so $\frac{a}{b}$ is not reduced, a contradiction. $\square$

Proof 1 (v 2.0): Let $S = \{n \geq 1 : n \in \mathbb{Z}, n\sqrt{2} \in \mathbb{Z}\}$. (Note that S is the set of all denominators of fractions representing $\sqrt{2}$.) We want to prove that $S = \varnothing$, i.e. that S is empty. If S is nonempty, let b be the smallest element of S. Then $\exists a \in \mathbb{Z}$ such that $b\sqrt{2} = a$. From above, the first version of this proof, we know that a and b are both even. Then $\sqrt{2} = \frac{a}{b} = \frac{a/2}{b/2}$ so then $b/2 \in S$, which tells us that b is not the minimal element of S, a contradiction. $\square$

Proof 2: Let $S = \{n \geq 1 : n \in \mathbb{Z}, n\sqrt{2} \in \mathbb{Z}\}$. Claim: If $n \in S$ then $n(\sqrt{2} - 1) \in S$. Note that this claim immediately proves the theorem! Indeed, assuming the claim as true for the moment, we see that given any element of S there must be a strictly smaller element of S (since $n(\sqrt{2} - 1) < n$). This creates an infinite sequence of strictly decreasing positive integers, which is impossible, whence we deduce $S = \varnothing$. The proof of the claim itself is on the homework, to be proved by viewers like you! $\square$

Proof 3: Suppose that $\sqrt{2} = \frac{a}{b}$. Then $a^2/b^2 = 2$, whence $\frac{a}{b} = \frac{2b}{a}$. We now take the fractional part of both sides, using the notation $\{x\}$ to denote the fractional part of a given number x. (For example, $\{\pi\} = 0.14159\cdots$ and $\{\frac{5}{3}\} = \frac{2}{3}$.)

Since $\frac{a}{b} = \frac{2b}{a}$, we deduce that $\{\frac{a}{b}\} = \{\frac{2b}{a}\}$. Now $\{\frac{a}{b}\} = \frac{b'}{b}$ where $0 < b' < b$ and $\{\frac{2a}{b}\} = \frac{a'}{a}$ where $0 < a' < a$. We've therefore proved

$$\frac{b'}{b} = \{\frac{a}{b}\} = \{\frac{2b}{a}\} = \frac{a'}{b}$$

whence $\sqrt{2} = \frac{a}{b} = \frac{a'}{b'}$. But $b' < b$, so as before we can obtain a contradiction by assuming from the outset that b is the minimal denominator one can choose when writing $\sqrt{2}$ as a fraction. $\square$