1. 2/6

1.1. Syllabus. Do introductions.

1.2. What is number theory about?

(1) Integer solutions to polynomial equations ("Diophantine equations")
(2) Prime numbers

1.3. Some notation:

$$\begin{aligned} \mathbf{N} &= \{1, 2, 3, \ldots\}, \\ \mathbf{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}, \\ \mathbf{Q} &= \{\tfrac{a}{b} \mid a, b \in \mathbf{Z} \text{ with } b \text{ nonzero}\}. \end{aligned}$$

1.4. *Well-ordering principle* Any nonempty subset of $\mathbf{N}$ contains a smallest element. (Not true if we replace $\mathbf{N}$ with $\mathbf{Z}$ or $\mathbf{Q}$ or $\mathbf{Q}_{>0}$!)

1.5. *Eratosthenes's sieve* When we say "prime number", we will always mean a positive number. We exclude 1 from being prime.

		$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9
10	$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$
20	21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$

Primes are simple to define yet hard to classify.

1.6. *Euclid's proof of the infinitude of primes* Suppose that $p_1, \ldots, p_k$ is a finite list of prime numbers. It suffices to show that we can always find another prime not on our list. Let

$$m = p_1 \cdots p_k + 1.$$

How to conclude the proof?

Informal. Since $m > 1$, it must be divisible by some prime number, but this number can't be any of the p_i. □

The problem is: How do we know that any integer > 1 must be divisible by some prime?

Rigorous. Let S be the set of integers greater than 1 that divide m. Note that S does not contain any of the p_i. Yet it is a nonempty subset of $\mathbf{N}$, because it contains m. Thus, by well-ordering, S has a smallest element q.

We claim that q is prime. For if it has a divisor q' such that $1 < q' < q$, then q' would also divide m, contradicting the minimality of q. □

1.7. Warning: The above proof does not imply that m itself is prime.

$$2 + 1 = 3, \quad 2(3) + 1 = 7, \quad \ldots, \quad 2(3)(5)(7)(11) + 1 = 59(509).$$

2. 2/8

2.1. Which of the following sets has an analogue of the well-ordering principle for **N**?

(1) $\mathbf{N}_0 = \{0\} \cup \mathbf{N}$.
(2) $2\mathbf{Z}$, the set of even integers.
(3) $\{\frac{a}{b} \mid a, b \in \mathbf{N} \text{ and } b < 100\}$.
(4) $\{\frac{1}{2^n} \mid n \in \mathbf{N}\}$.

2.2. *Prime factorization* Another application of well-ordering:

Theorem 2.1. *Any positive integer can be written as a product of prime numbers.*

(Is 1 a product of primes? Yes: The so-called empty product.)

Proof. Suppose for the sake of contradiction that the set of counterexamples $C \subseteq \mathbf{N}$ is nonempty. By well-ordering, C contains a smallest element m.

Note that m can't be prime itself. So there is some integer d such that d divides m and $1 < d < m$. But now, $e = m/d$ is also an integer such that e divides m and $1 < e < m$. By the minimality of m in C, we know d and e are both products of primes. But then, $m = de$ is also a product of primes, a contradiction. □

An expression for $a \in \mathbf{N}$ as a product of primes is called a *prime factorization* of n. There may be repeated primes, so in general, it will look like

$$a = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_i are pairwise distinct primes and the e_i are positive integers.

If the p_i are ordered from smallest to largest, then this expression is unique. That is: If we have another prime factorization

$$a = q_1^{f_1} \cdots q_\ell^{f_k},$$

where the q_i are also ordered from smallest to largest, then $k = \ell$, and $p_i = q_i$ for all i, and $e_i = f_i$ for all i.

2.3. *Digression on uniqueness* We often meet situations like this, where there are separate claims of *existence* and *uniqueness*. To show that X exists, you use sets and elements to build a mathematical object that satisfies the definition of X. To show that X is unique, you must show that if Y is any other object that also satisfies the definition, then $X = Y$.

Example 2.2. Let's imagine that we are mathematicians in ancient India, trying to invent the concept of zero. We define a *zero* to be a number z such that the addition law on **N** extends to the rule $n + z = n$ for any $n \in \mathbf{N}$.

We claim that such a number must be unique. Suppose z and z' are both zeroes. Then we have both $z + z' = z$ and $z' + z = z'$. Therefore, $z = z'$.

2.4. If a is very large, then computing its (unique) prime factorization can be very hard, because finding divisors of n can be very hard. This is an important principle behind much cryptography.

The fastest way to test whether b divides a is to use long division.

Even if b does not divide a, they will still have divisors in common: for instance, because 1 divides both a and b. In particular, they have a *greatest common divisor*, or *gcd*. The fastest way to compute $\gcd(a, b)$ is by using repeated long division in a form called the Euclidean algorithm, or Euclid's ladder.

2.5. *Long division* Recall that the well-ordering principle applies just as well with $\mathbf{N}_0$ in place of $\mathbf{N}$.

Theorem 2.3. *For all $a \in \mathbf{N}_0$ and $b \in \mathbf{N}$, there exist $q, r \in \mathbf{N}_0$ such that*

$$a = qb + r \quad \text{and} \quad r < b.$$

(In particular, b divides a if and only if $r = 0$.)

Proof. Intuition: When you do long division, you're using a greedy algorithm ("What's the largest q such that $qb \leq a$?"). So let

$$S = \{n \in \mathbf{N}_0 \mid n = a - kb \text{ for some } k \in \mathbf{N}_0\}.$$

Since $a \in \mathbf{N}_0$ and $a = a - 0b$, we know that $a \in S$. Thus, S is nonempty. By well-ordering, it contains a smallest element: say, $r = a - qb$ for some $q \in \mathbf{N}_0$. It remains to show $r < b$.

Indeed, if $r \geq b$, then $r - b \in \mathbf{N}_0$ and $r - b = a - (q + 1)b$, so we have $r - b \in S$. This contradicts the minimality of r. □

2.6. *Euclid's ladder* The reason long division can help us compute $\gcd(a, b)$ is the following fact, whose proof I'll skip today:

$$\text{If } a = qb + r, \text{ then } \gcd(a, b) = \gcd(b, r).$$

It shows that if we want to compute $\gcd(a, b)$, where $a > b$, then we can switch to computing $\gcd(b, r)$, where $b > r$.

Let's illustrate by computing $\gcd(462, 1071)$. Since $1071 > 462$, we start with $a = 1071$ and $b = 462$.

a	b	q	qb	r
1071	462	2	924	147
462	147	3	441	21
147	21	7	147	0

The last line has a remainder $r = 0$, so it shows that 21 divides 147. Altogether, $\gcd(462, 1071) = \gcd(147, 462) = \gcd(21, 147) = \boxed{21}$.

Why must the ladder eventually stop? Again, the reason is well-ordering. The sequence of remainders r gives us a nonempty subset of $\mathbf{N}_0$, so it must contain a smallest element (which is, in fact, always 0).

2.7. *Digression on induction* Just as the well-ordering principle lets us "descend" to the smallest case of something, the principle of induction lets us "ascend" from a base case to infinitely many cases.

Example 2.4. We prove that for any $k \in \mathbf{N}$, the sum of the first k positive integers is equal to $\frac{1}{2}k(k+1)$.

Base case. If $k = 1$, then the sum is just 1. We know $1 = \frac{1}{2}(1)(2)$.

Inductive step. Suppose the claim is true when $k = n$. We will show it is true for $k = n + 1$. To do this, we expand:

$$\begin{aligned}\left[\tfrac{1}{2}k(k+1)\right]\Big|_{k=n+1} &= \tfrac{1}{2}(n+1)(n+2)\\ &= \tfrac{1}{2}n(n+1) + (n+1)\\ &= \left[\tfrac{1}{2}k(k+1)\right]\Big|_{k=n} + (n+1).\end{aligned}$$

By the inductive hypothesis, the red term equals the sum of the first n positive integers. Therefore, the whole last expression equals the sum of the first $n+1$ positive integers.

3. 2/10

3.1. Recall that a Diophantine equation is a polynomial equation with integer (or rational) coefficients, which we are typically solving for integer (or rational) solutions.

Which of the following linear equations can be solved for integer x and y? For those, how many solutions are there?

(1) $6x + 7y = 1$.
(2) $6x + 7y = 2$.
(3) $6x - 15y = 2$.
(4) $6x - 15y = -99$.
(5) $1071x + 462y = 42$.

3.2. Last time, we began to discuss gcd's in a loose way. Today, we do it more systematically.

Firstly: When should $\gcd(a, b)$ exist? For instance, $\gcd(0, 0)$ does not exist.

For any $a, b \in \mathbf{Z}$, the set of common divisors of a and b is nonempty, since it contains 1. If at least one of a, b is nonzero, say a, then any common divisor can be at most $|a|$. So by a flipped version of well-ordering, there is a greatest such divisor.

Note that our reasoning showed $\gcd(a, b) \geq 1$. Moreover, $\gcd(a, 0) = |a|$ for all nonzero a.

3.3. It turns out that our study of linear Diophantine equations above leads to a very natural characterization of gcd's.

Theorem 3.1. *For fixed $a, b \in \mathbf{Z}$, not both zero(!), let*

$$S = \{ax + by \mid x, y \in \mathbf{Z}\} \subseteq \mathbf{Z}.$$

Then there exists $d \in \mathbf{N}$ such that $S = d\mathbf{Z}$, the set of integer multiples of d.

Proof. We can't apply well-ordering directly to S. But consider $S \cap \mathbf{N}$: This is a subset of $\mathbf{N}$ by construction, and nonempty, since it contains $|a|$ and $|b|$. We take d to be the smallest element of $S \cap \mathbf{N}$.

To show that $S = d\mathbf{Z}$, we must show that each set is contained in the other. It will be convenient to write $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbf{Z}$, which we can do because $d \in S$.

Any element of $d\mathbf{Z}$ takes the form md for some $m \in \mathbf{Z}$ We see that $md = a(mx_0) + b(my_0) \in S$. This proves $d\mathbf{Z} \subseteq S$.

Conversely, suppose $n \in S$. If $-n$ is a multiple of d, then so is n, so it suffices to assume $n \geq 0$. We must show that d divides n. By long division, $n = qd + r$ for some $q, r \in \mathbf{N}_0$ with $r < d$. But $n = ax_1 + by_1$ for some $x, y \in \mathbf{Z}$, so

$$r = n - qd = a(x_1 - qx_0) + b(y_1 - qy_0) \in S.$$

Since d is the smallest positive element of S, this forces $r = 0$, whence d divides n. This proves $S \subseteq d\mathbf{Z}$. $\square$

Theorem 3.2. *The d resulting from the previous theorem is precisely* $\gcd(a, b)$.

Proof. We must prove two things: (1) That d divides both a and b. (2) That if $d' \in \mathbf{N}$ is any other common divisor of a and b, then $d' \leq d$.

(1) We know that d divides every element of S. But we certainly have $a = a(1) + b(0) \in S$, and similarly, $b \in S$.

(2) It suffices to show that d' divides d. (Here it would be tempting to try long division, but ultimately, we only need the defining properties of d' and d.) We know that $a = d'a'$ and $b = d'b'$ and $d = ax_0 + by_0$ for some integers a', b', x_0, y_0, from which

$$d = (d'a')x_0 + (d'b')y_0 = d'(a'x_0 + b'y_0),$$

as needed. □

3.4. We return to linear Diophantine equations.

Corollary 3.3 (Bézout). *For fixed $a, b, c \in \mathbf{Z}$, where a and b are not both zero,*

$$ax + by = c$$

admits a solution with $x, y \in \mathbf{Z}$ if and only if c is a multiple of $\gcd(a, b)$.

Proof. Let S be as in Theorem 3.1. By definition, we can solve the equation for $x, y \in \mathbf{Z}$ if and only if $c \in S$, and the two previous theorems show $S = \gcd(a, b)\mathbf{Z}$. □

3.5. We can also prove a claim left unproved on Wednesday, which we needed to run the Euclidean algorithm.

Corollary 3.4. *If $a = bq + r$ for some $a, b, q, r \in \mathbf{Z}$ with b nonzero, then* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $S = \{ax + by \mid x, y \in \mathbf{Z}\}$ and $T = \{bx + ry \mid x, y \in \mathbf{Z}\}$. Then $a \in T$ and $r = a - bq \in S$, so we get

$$\gcd(a, b)\mathbf{Z} = S = T = \gcd(b, r)\mathbf{Z}$$

How to finish? Intersect both sides with $\mathbf{N}$; compare smallest elements. □

3.6. There is a generalization of everything above to the case of three or more integers. One can define $\gcd(a_1, \dots, a_k)$ as long as some a_i is nonzero. Then

$$a_1x_1 + \cdots + a_kx_k = c$$

has a solution with $x_1, \dots, x_k \in \mathbf{Z}$ if and only if $c \in \gcd(a_1, \dots, a_k)\mathbf{Z}$.

3.7. All of this differs, however, from the Chicken McN*gget problem, because there, we are seeking solutions in *nonnegative* integers—not arbitrary integers.

3.8. We've now covered some version of §1.1–1.4, 2.1–2.6 in Stillwell.