Quick Review of Induction:

This is really prerequisite material, but we will review an example so we are all on the same page.

Example: Prove that $n! > n^3$ for every integer $n \geq 6$.

Proof: We proceed with induction on n. The base case is $n=6$. Observe that

$$6! = 720$$

and $6^3 = 216$, so indeed $n! > n^3$ for $n=6$.

Assume inductively that $K! > K^3$ for every integer $6 \leq K \leq N$ for some integer N. Now observe

$$\begin{aligned}(N+1)! &= (N+1)N! \\ &> (N+1)N^3.\end{aligned}$$

We would now like to say that $N^3 \geq (N+1)^2$. If this were true, then we would have

$$\begin{aligned}(N+1)! &> (N+1)N^3 \\ &\geq (N+1)^3\end{aligned}$$

and by induction we would be done. So we have reduced the problem to showing

$$N^3 \geq (N+1)^2 \quad \text{for } N \geq 6.$$

To see this, observe that this is equivalent to showing

$$N^3 \geq N^2 + 2N + 1.$$

Now since $N \geq 6$, $2N^2 \geq 2N$ and $N^2 > 1$., so we have

$$N^2 + 2N + 1 < N^2 + 2N^2 + N^2 = 4N^2.$$

Also since $N \geq 6$, $N^3 = N \cdot N^2 > 6 \cdot N^2 > 4N^2$, so we have

$$N^3 > 4N^2 > N^2 + 2N + 1 = (N+1)^2.$$

Thus, by induction we have the result. ∎

Not all inductions will be as easy or as difficult as this, depending on your perspective.

Divisibility Theory of the Integers:

Def: Let $a, b \in \mathbb{Z}$. We say a <u>divides</u> b, and write $a \mid b$ if $\exists\ c \in \mathbb{Z}$ s.t. $b = ac$.

This is also exactly the same notion you are used to from elementary school.

Thm 2.2: For $a, b, c \in \mathbb{Z}$, we have

① $a \mid 0$, and $1 \mid a$, $a \mid a$

② $a \mid 1$ iff $a = \pm 1$

③ If $a \mid b$ and $c \mid d$, then $ac \mid bd$

④ If $a \mid b$ and $b \mid c$, then $a \mid c$

⑤ $a \mid b$ and $b \mid a$ iff $a = \pm b$

⑥ If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$

⑦ If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

Example: If $a \mid b$ and $b \mid c$, prove $a \mid c$. (back of previous page)

Proof: Since $a \mid b$, there exists $n \in \mathbb{Z}$ s.t. $b = an$.

Similarly, since $b \mid c$ $\exists\, m \in \mathbb{Z}$ s.t. $c = bm$.

Combining these we have $c = bm = a \cdot nm$. Since $nm \in \mathbb{Z}$, we have $a \mid c$ as claimed. ∎

Of course, we can also divide integers that do not divide evenly into each other by considering division with remainder.

Thm 2.1 (The division alg): Let $a, b \in \mathbb{Z}$, $b > 0$. Then exists unique integers q, r w/

$$a = bq + r \qquad 0 \le r < b.$$

~~$b = aq + r$~~

q = quotient, r = remainder.

Proof: Consider the set

$$S = \{a - nb : n \in \mathbb{Z},\ a - nb \ge 0\}.$$

If we can show this set is nonempty, we will have a remainder at least. Then we will need to show we can choose n so that $a - nb$ is between 0 and b.

By assumption $b \geq 1$. We always have $|a| \geq a$, so

$a - (|a|)b = a + |a|b \geq 0$. Thus we have at

least one ~~positive~~ element in S. We can now

apply the well-ordering principle (this is a nonempty set

of nonnegative integers) to conclude there is a smallest

element $r \in S$. It remains to show that $r < b$.

Let q be such that

$$a - bq = r.$$

Suppose $r \geq b$. Then we have $a - bq \geq b$

$\Rightarrow$ $a - b(q+1) \geq 0$ and $a - b(q+1) < r$, which contradicts

the minimality of r. Thus $0 \leq r < b$.

To finish the proof, we only need to show r and q are

unique. Suppose $a = bq + r$, $0 \leq r < b$ and

$a = bq' + r'$, $0 \leq r' < b$. Subtracting the two we

obtain

$$b(q - q') = r - r'.$$

If $q \neq q'$, then taking absolute values we obtain

$$b|q - q'| = |r - r'|.$$

However, if $q \neq q'$, then $|q - q'| \geq 1$ and since $0 \leq r < b$ and

$0 \le r' < b$, we must have $|r - r'| < b \le b|q - q'|$. #.

Thus $q = q' \Rightarrow |r - r'| = 0 \Rightarrow r = r'$. Thus

q and r are unique. ∎

Let's look at an example of how the division algorithm can be used to help us prove general statements.

Example: Prove that the cube of any integer is of the form $9k$, $9k+1$ or $9k+8$ for some integer k.

Proof: Let n be an integer. Applying the division algorithm with $b = 9$, we have

$$n = 9q + r \qquad 0 \le r < 9.$$

Now we only need to calculate each of the possibilities:

$r = 0$: $n = 9q$: $n^3 = 9(9^2q^3) = 9k$.

$r = 1$: $n = 9q + 1$: $n^3 = 729q^3 + 243q^2 + 27q + 1$

$= 9(81q^3 + 27q^2 + 3q) + 1$

$r = 2$: $n = 9q + 2$: $n^3 = 9(81q^3 + 54q^2 + 12q) + 8$

$r = 3$: $n = 9q + 3$: $n^3 = 9(81q^3 + 81q^2 + 27q^3 + 3)$

etc..

2.2 The Greatest Common Divisor:

The greatest common divisor of two integers is another concept familiar from elementary school and is exactly what the name suggests, it is the largest integer that divides with no remainder into both integers. Formally,

Def: Let $a, b \in \mathbb{Z}$ with ~~at least one nonzero~~ $ab \neq 0$. The *greatest common divisor* of a and b, written $\gcd(a,b)$ is the positive integer d satisfying:

1. $d \mid a$ and $d \mid b$
2. if $e \mid a$ and $e \mid b$, then $e \leq d$.

Example: The gcd of 14 and 21 is 7.

The SAGE command for calculating the GCD is `GCD(a,b)`.

We will see in the next section how to calculate the GCD by an efficient algorithm, but it is good to be able to use the computer as well!

~~The following facts on divisibility will be useful:~~

One of the nice properties of the gcd is that if $d = \gcd(a,b)$,

$\exists\ m,n \in \mathbb{Z}$ so that

$$d = am + bn.$$

We say d is a <u>linear combination</u> of a and b.

<u>Thm 2.3:</u> Let $a,b \in \mathbb{Z}$ w/ $ab \neq 0$. There exists $m,n \in \mathbb{Z}$ s.t.

$$\gcd(a,b) = am + bn.$$

<u>Proof:</u> This proof has a similar flavor to the previous proof of the division algorithm. Let

$$S = \{ am + bn \mid am + bn > 0,\ m,n \in \mathbb{Z} \}.$$

It is clear that $S \neq \emptyset$, for example $a^2 \in S$ if $a \neq 0$ and $b^2 \in S$ if $b \neq 0$ since $a^2 = a \cdot a + b \cdot 0$. and similarly for b^2. Now S is a nonempty set of positive integers, so has a minimal element d by the well-ordering principle. By the definition of S we have $\exists\ m,n \in \mathbb{Z}$ s.t.

$$d = am + bn.$$

This does not prove d is the gcd though! We prove d is the gcd. The first step is to show $d \mid a$ and $d \mid b$. Use the division algorithm to write

$$a = dq + r \quad \text{with} \quad 0 \leq r < d.$$

$$r = a - dq$$
$$= a - (am+bn)q$$
$$= a(1-mq) + b(-nq).$$

Thus, either if $d \nmid c$, then $r > 0$ and $r < d$ and so $r \in S$. But this contradicts the minimality of d, so we must have $r = 0$ and $d \mid a$. Similarly for $d \mid b$. This gives ① of the definition.

Suppose $e \mid a$ and $e \mid b$ ($e > 0$). Then we have $e \mid (am+bn)$ $\forall m, n \in \mathbb{Z}$. In particular, $e \mid d$. Thus, $e \leq d$ and we are done. ∎

One should observe here that we have shown m and n exist, but not how to find them! This happens often in mathematics when we can show something must exist but the proof does not show us how to find it! Fortunately in this case there is an algorithm that allows us to find m and n.

The command in SAGE to find m and n is given by:

```
d, m, n = xgcd(a,b).
```

This will initially return nothing, but stores the values

of m and n. Then just type m or n to get the values. Alternately, type

$d,m,n = xgcd(a,b)\ ;\ m\ ;\ n$.

Def: Let $a,b \in \mathbb{Z}$, and $ab \neq 0$. We say a and b are <u>relatively prime</u> if $gcd(a,b)=1$.

<u>Example:</u> 15 and 28 are relatively prime.

We saw before that if $d=gcd(a,b)$, then $\exists\ m,n$ so that $d=am+bn$. One should be careful though, if there exist $m,n \in \mathbb{Z}$ s.t. $d=am+bn$ this does <u>NOT</u> mean that $d=gcd(a,b)$. For example, $gcd(3,2)=1$, but we can write

$$15 = 3(30) + 2(-15).$$

So having a linear combination is <u>NOT</u> enough to determine the gcd <u>unless</u> $gcd(a,b)=1$.

Thm 2.4: Let $a, b \in \mathbb{Z}$, not both 0. Then a and b are relatively prime iff $\exists\ m, n \in \mathbb{Z}$ s.t

$$1 = am + bn.$$

Proof: One direction is already done, namely if $\gcd(a,b) = 1$ then we know such an m and n exist. Suppose now that we have $m, n \in \mathbb{Z}$ s.t

$$1 = am + bn.$$

We wish to show $1 = \gcd(a,b)$. Suppose $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$, so $d \mid (am+bn)$, i.e., $d \mid 1$. Thus, $d = 1$ and we are done. ☒

Cor: If $\gcd(a,b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: Exercise.

Cor: If $a \mid c$ and $b \mid c$ w $\gcd(a,b) = 1$, then $ab \mid c$.

Observe that this cor is NOT true if $\gcd(a,b) \neq 1$. For example, $6 \mid 12$ and $4 \mid 12$, but $6 \cdot 4 = 24 \nmid 12$.

Proof: Since $a|b$ and $b|c$, $\exists$ integers m, n so that

$c = am$ and $c = bn$. We use that $\gcd(a,b) = 1$

to conclude $\exists$ integers r, s so that

$$1 = ar + bs. \qquad (*)$$

Multiplying both sides of $(*)$ by c we have

$$c = acr + bcs.$$

Now use our initial equations $c = am$ and $c = bn$ to

conclude:

$$c = a(bn)r + b(am)s$$

$$= ab(nr + ms).$$

Thus, $ab|c$. ∎

The following result, which is easy to prove, will be used heavily.

Thm 2.5 (Euclid's lemma): If $a|bc$ and $\gcd(a,b) = 1$, then $a|c$.

Proof: As before, $\exists$ $m, n \in \mathbb{Z}$ so that

$$1 = am + bn.$$

Multiplying by c:

$$c = acm + bcn.$$

Use now that $a|bc$ to get $r \in \mathbb{Z}$ s.t. $bc = ar$.

Then we have

$$c = acm + bcn$$
$$= acm + arn$$
$$= a(cm + rn),$$

Thus, $a \mid c$. ∎

Example: The sum of the squares of two odd integers cannot be a perfect square.

Proof: Let $m = 2k+1$ and $n = 2l+1$ be two odd integers. Then

$$m^2 + n^2 = (4k^2 + 4k + 1) + (4l^2 + 4l + 1)$$
$$= 4(k^2 + k + l^2 + l) + 2$$
$$= 2(\underbrace{2k^2 + k + l^2 + l}_{\text{odd integer}} + 1).$$

Thus, we get 2 times an odd integer. If this were a perfect square, we would need another 2! ∎

2.4 The Euclidean Algorithm:

We saw before that given integers a, b w/ $ab \neq 0$, ~~be coded~~ that there exists integers m, n so that

$$\gcd(a,b) = am + bn.$$

Unfortunately, our proof of this fact did not yield a method for determining m and n. The Euclidean algorithm is a method for determining m and n.

Assume w/o/s that $a \geq b > 0$. The division alg. allows us to write

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b.$$

If $r_1 = 0$, then $b \mid a$ and $\gcd(a,b) = b$ and $b = a \cdot 0 + b \cdot 1$ so we are done. Suppose $r_1 \neq 0$. Then divide r_1 into b:

$$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1.$$

If $r_2 = 0$ we stop, if not we divide r_2 into r_1:

$$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 < r_2.$$

Continuing in this pattern we obtain a decreasing sequence of positive integers $b > r_1 > r_2 > r_3 \ldots$

Thus, for some n we must have $r_n = 0$.

Lemma: If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$.

Proof: Let $d = \gcd(a,b)$, $e = \gcd(b,r)$. Since $e \mid b$ and $e \mid r$, $e \mid a = bq + r$. Thus $e \mid d$ because it is a common divisor of a and b. Similarly, $d \mid a$ and $d \mid b$, so $d \mid (a - bq) = r$. Thus $d \mid e$ and so $d = e$. ∎

We can apply this lemma to our process above to obtain

$$\begin{aligned}\gcd(a,b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &= \cdots = \gcd(r_{n-1}, 0) = r_{n-1}.\end{aligned}$$

Thus, the last nonzero remainder is the gcd! This gives an alternative to computing prime factorizations to compute gcd's! (Much more efficient!)

To obtain the linear combination, we can back substitute.

~~It may be easier to form a table:~~

Suppose our equations are

$$a = b q_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + 0.$$

We can back substitute to obtain the desired expression.

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$$

$$\Rightarrow \quad r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} \qquad (*1$$

Now use the previous equation

$$r_{n-4} = r_{n-3} q_{n-2} + r_{n-2}$$

to replace r_{n-2} in (*)

$$(*_2) \qquad r_{n-1} = r_{n-3} - q_{n-1} (r_{n-4} - r_{n-3} q_{n-2}).$$

Next we replace r_{n-3} and so on until we have only a and b left. This is best seen with an example:

Example: Compute $\gcd(348, 1532)$ and determine m and n so that

$$\gcd(348, 1532) = 348m + 1532n.$$

Solution:

$$1532 = 348(4) + 140$$

$$348 = 140(2) + 68$$

$$140 = 68(2) + 4$$

$$68 = 4(17) + 0$$

Thus, $\gcd(348, 1532) = 4$.

Write

$$4 = 140 + 68(-2).$$

$$68 = 348 + 140(-2)$$

$$140 = 1532 + 348(-4).$$

Back substituting:

① $$4 = 140 + (348 + 140(-2))(-2)$$

$$= 140 + 140(4) + 348(-2)$$

$$= 140(5) + 348(-2)$$

② $$4 = 140(5) + 348(-2)$$

$$4 = (1532 + 348(-4))(5) + 348(-2)$$

$$4 = 1532(5) + 348(-22).$$

Thus, $m = -22$ and $n = 5$.

As was noted last time, the SAGE command for this is `d, m, n = xgcd(a,b)`.

The text also gives a short treatment of least common multiple. You should read this, but it is not real difficult and we won't discuss it in class, unless it becomes necessary. Essentially, one proves $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$, and so we can reduce anything about the lcm back to questions about the gcd.

2.5 The Diophantine Equation $ax+by=c$:

Now that we have seen that the gcd of a and b can be written as a linear combination of a and b, we are in a position to study ~~the solutions to~~ the equation

$$ax + by = c.$$

This is the first real "number theory" of the course, though it will be brief and not real difficult. In general, a diophantine equation is an equation in a finite # of variables that we wish to solve with integer values. In some cases there will be finitely many or no solutions, in other cases there many may be infinitely many solutions. The case with which we will deal with $ax+by=c$ should not lead you to believe diophantine equations are easy to study in general. Recall $x^n+y^n=z^n$ is a Diophantine equation and showing it has no nontrivial solutions for $n \geq 3$ was VERY difficult.

Let $d = \gcd(a,b)$. If the equation $ax+by=c$ has a solution w/ $x,y \in \mathbb{Z}$ then we must have $d \mid c$ since $d \mid a$ and $d \mid b$ so $d \mid (ax+by)$. So immediately we see that if $d \nmid c$, there are no integer solutions to $ax+by=c$.

Now suppose $d \mid c$. We know $\exists\ m,n \in \mathbb{Z}$ s.t

$$d = am + bn.$$

$d \mid c \Rightarrow \exists\ s \in \mathbb{Z}$ s.t $c = ds$. Thus,

$$c = ds = ams + bns.$$

So we have $x = ms$, $y = ns$ is a solution to the Diophantine equation.

We have easily determined when the equation $ax+by=c$ has integer solutions. The next question is if we can determine all the integer solutions when they exist. One way to accomplish such a goal is to give all solutions in terms of some known solution. Suppose x_0, y_0 is a solution to the equation

$$ax + by = c.$$

Let x_1 and y_1 be another solution. We have

$$ax_0 + by_0 = c = ax_1 + by_1.$$

We can write

$$a(x_0 - x_1) = b(y_1 - y_0).$$

Let $d = \gcd(a,b)$. There exists $r,s \in \mathbb{Z}$ s.t. $dr = a$, $ds = b$.

We claim that $\gcd(r,s) = 1$. Suppose $\gcd(r,s) = e > 1$. Then

$e \mid r$ and $e \mid s \Rightarrow de \mid a$ and $de \mid b$. # since $d = \gcd(a,b)$.

Thus, $\gcd(r,s) = 1$.

Write

$$rd(x_0 - x_1) = ds(y_1 - y_0).$$

$\Rightarrow$

$$r(x_0 - x_1) = s(y_1 - y_0).$$

Since $\gcd(r,s) = 1$ and $r \mid s(y_1 - y_0)$, we can apply Euclid's lemma to conclude $r \mid (y_1 - y_0)$. So $\exists\ t \in \mathbb{Z}$ s.t.

$$y_1 - y_0 = rt.$$

i.e.,

$$y_1 = y_0 + rt = y_0 + \left(\frac{a}{d}\right)t.$$

Substituting back in,

$$r(x_0 - x_1) = srt$$

i.e.,

$$x_0 - x_1 = st.$$

Thus

$$x_1 = x_0 - \left(\frac{b}{d}\right)t.$$

So we have shown that given a solution x_0, y_0, we can

write any other solution in the form

$$x_1 = x_0 - \left(\frac{b}{d}\right)t$$

$$y_1 = y_0 + \left(\frac{a}{d}\right)t \qquad t \in \mathbb{Z}.$$

It is easy to check by simple substitution that given any $t \in \mathbb{Z}$, (x_0, y_0) a solution of $ax+by=c$, then

$$x_1 = x_0 - \left(\frac{b}{d}\right)t$$

$$y_1 = y_0 + \left(\frac{a}{d}\right)t$$

is also a solution. Thus, we have found all solutions in terms of (x_0, y_0). We summarize with the following theorem.

<u>Thm 2.9:</u> The linear Diophantine equation $ax+by=c$ iff $d=\gcd(a,b) \mid c$. If (x_0, y_0) is a solution of the equation, then all other solutions are of the form

$$x = x_0 - \left(\frac{b}{d}\right)t$$

$$y = y_0 + \left(\frac{a}{d}\right)t$$

for $t \in \mathbb{Z}$.

Besides being of interest because we like to find integer solutions to the Diophantine equations in general, linear Diophantine equations

We can apply the Euclidean alg. (or just inspection in this case) to obtain

$$5(1) + 3(0) = 1.$$

Thus, $100 = 5(-100) + 3(200)$. $\therefore$ $x = -100$, $y = 200$ is a solution. However, we can't have a negative # of men, so we need to find a positive solution. We need

$$x = -100 - 3t > 0$$

$$y = 200 + 5t > 0$$

i.e., $-3t > 100$

i.e. $t < \frac{-100}{3}$

and

$$200 > -5t$$

ie. $$-\frac{200}{5} < t$$

So $$-40 < t < -33.\overline{3}$$

Thus, t can be $-39, -38, -37, \ldots, -34$.

This gives x as $17, 14, \ldots, 2$

y as $5, 10, \ldots, 30$

and z as $78, 76, \ldots, 68$.

also often show up in word problems.

Example: One hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 bushels, and each child $\frac{1}{2}$ bushel. How many men, women, and children are there in the village?

Solution: Let x = # of men, y = # of women, z = # of children.

Then we have 3 unknowns and 2 equations:

$$x + y + z = 100 \qquad (1)$$

and

$$3x + 2y + \tfrac{1}{2}z = 100. \qquad (2)$$

We can remove z from equation (2):

$$z = 100 - x - y$$

So

$$3x + 2y + \tfrac{1}{2}(100 - x - y) = 100$$

i.e.

$$2.5x + 1.5y = 50 \qquad \left(\tfrac{5}{2}x + \tfrac{3}{2}y = 50\right)$$

clear the denominators:

$$5x + 3y = 100$$

Since $\gcd(5, 3) = 1$ and $1 \mid 100$, we have a solution to this equation.

3.1 The Fundamental Theorem of Arithmetic:

Def: An integer $p > 1$ is called a **prime number** if the only divisors of p are 1 and p. An integer $n > 1$ that is not prime is said to be **composite**.

The important thing about prime numbers, as we will see in a minute, is they are the building blocks of all the numbers! So by understanding primes we can often understand general properties.

Examples: 2, 3, 5, 7, 11, 13, ..., 17449, ..., 132241, ...

Aside: To compute the n^{th} prime number using SAGE one uses the command with `nth_prime(n)`.

As for example `nth_prime(31) = 5`.

One can also compute the next prime after any given number with the command `next_prime(n)`.

For example, `next_prime(12345) = 12347`.

The following theorem is an important property of prime numbers.

In fact, this theorem could be used as the definition of prime and often is in a more abstract setting.

Thm 3.1: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose $p \mid ab$. Then $p \mid a$ or $p \nmid a$. If $p \mid a$ we are done so assume $p \nmid a$. We need to show that $p \mid b$. However, since p is prime and $p \nmid a$, we must have $\gcd(a, p) = 1$. Euclid's lemma then gives that $p \mid b$. ∎

To see this can actually be used as the definition, we must show that if $p > 1$ and whenever $p \mid ab$ then $p \mid a$ or $p \mid b$, then there are no positive divisors of p other than 1 and p. Let $1 \le n \le p$ be a divisor of p. Then $\exists\, m \in \mathbb{Z}$ s.t. $mn = p$. Necessarily we have $1 \le m \le p$ as well. Then $p \mid mn$ since $p \mid p$, and so by assumption $p \mid m$ or $p \mid n$. However, since $1 \le m, n \le p$, we must have $p = m$ or $p = n$. Thus the only divisors of p are 1 and p. This shows Thm 3.1 could be taken as the definition of prime and then we would have a theorem that stated the only divisors of a prime are 1 and p. This is how one defines prime ideal in abstract algebra.

The following 2 results are easily corollaries.

Cor 3.1.1: If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $1 \le i \le n$.

Cor 3.1.2: If $p, q_1, \ldots, q_n$ are all primes and $p \mid q_1 \cdots q_n$, then $p = q_i$ for some $1 \le i \le n$.

We now show that primes are in fact the building blocks of all integers.

Thm 3.2 (The Fundamental Theorem of Arithmetic): Every positive integer $n > 1$ can be written as a product of primes. This factorization is unique up to reordering the primes.

Proof: ~~Let n be an integer. If n is prime we are done, so suppose n is not prime.~~

Observe that 2 is prime so is clearly the product of primes. We proceed by induction. Suppose that all integers $2 \le n \le N$ are the product of primes. Consider $N+1$. If $N+1$ is prime we are done. Suppose $N+1$ is not prime. Then $\exists\ a, b \in \mathbb{Z}$ with $2 \le a, b \le N$

so that $N+1 = ab$. We can apply our induction hypothesis to obtain a prime factorization of a and of b. But this in turn gives a prime factorization of $N+1$. Thus, by induction we see all integers >1 have a prime factorization. It remains to show uniqueness.

Let $n = p_1 \cdots p_r = q_1 \cdots q_s$ be two prime factorizations of n. We wish to show $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$.

WLOG we can assume $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq \cdots \leq q_s$.

Observe that $p_1 \mid q_1 \cdots q_s$ and so $p_1 = q_j$ for some $1 \leq j \leq s$. This implies $p_1 \geq q_1$. However, we can play the same game to get $q_i \mid p_i$ for some $1 \leq i \leq r$, i.e., $q_1 \geq p_1$. Thus, $p_1 = q_1$. Now we can cancel to arrive at $p_2 \cdots p_r = q_2 \cdots q_s$. We can continue this way. If $r < s$, then we eventually obtain $1 = q_{k+1} \cdots q_s$, #. Thus $r \geq s$. Same argument gives $s \geq r$ and so $r = s$. Thus we are done. ∎

($\mathbb{Z}[\sqrt{-5}]$) example when this fails!

We can write our prime factorizations in a canonical form as $n = p_1^{e_1} \cdots p_r^{e_r}$ with $p_1 < p_2 < \cdots < p_r$ and

$e_1, \ldots, e_r \geq 1$.

Thm: Let p be a prime #. Then $\sqrt{p}$ is irrational, i.e., $\sqrt{p} \notin \mathbb{Q}$.

Proof: Suppose $\exists\ a, b \in \mathbb{Q}$ with $\sqrt{p} = \frac{a}{b}$. WLOG we can assume $\gcd(a,b) = 1$. Then $a^2 = pb^2$. Thus $p \mid a^2$ and hence $p \mid a$. Thus $\exists\ a_1$ s.t. $a = pa_1$. Rewriting our equation we obtain $p^2 a_1^2 = pb^2$, i.e. $pa_1^2 = b^2$. But then $p \mid b^2$ and so $p \mid b$. Thus, $p \mid a$ and $p \mid b \Rightarrow p \mid \gcd(a,b) = 1$. #. Thus $\sqrt{p} \notin \mathbb{Q}$. ☐

The next natural question is now that we know what primes are, how many are there?

Let x be a real number. The function $\pi(x)$ counts how many primes there are less than x, i.e.,

$$\pi(x) = \#\{p : p \leq x,\ p \text{ prime}\}.$$

You will see what this function behaves like for large values of x in the homework. A couple sample values are

$\pi(10) = 4$

$\pi(50) = 15$

$\pi(2000) = 46$

One can check whether an integer is prime on SAGE with the command `is_prime(n)`. If n is prime this will return true, it will return false otherwise.

As is probably already known to all of you, there are infinitely many primes. We give a few proofs of this fact.

Thm: There are infinitely many primes.

Proof (1): Suppose there are only finitely many primes, $p_1, \ldots, p_n$. Consider the integer $N = p_1 \cdots p_n + 1$. The fundamental theorem of arithmetic implies there must be a prime that divides N. Thus, $p_j \mid N$ for some $1 \leq j \leq n$. But we also have that $p_j \mid p_1 \cdots p_n$, and so $p_j \mid 1$. #. Thus there must be infinitely many primes. ∎

Proof (2): Suppose there are only finitely many primes $p_1, \dots, p_n$. Consider the integer

$$N = p_2 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 \cdots p_{n-1}.$$

The fundamental theorem of arithmetic implies there is a prime $p \mid N$. Thus, $\exists\ j \in \{1, \dots, n\}$ s.t. $p_j \mid N$.

But

Wlog assume $j = 1$. Then $p_1 \mid (p_1 p_3 \cdots p_n + \cdots + p_1 \cdots p_{n-1})$ and $p_1 \mid N \Rightarrow p_1 \mid p_2 \cdots p_n$. #. Thus there are infinitely many primes. ∎

The last proof we will give has a different flavor, though it relies on the fundamental theorem of arithmetic as well. The Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It turns out this function has analytic continuation so that $s \in \mathbb{C}$ with a pole at $s = 1$. If you are unfamiliar with complex analysis, just recall from calculus that

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n}$$

diverges but $\zeta(s)$ converges for $s > 1$, $s \in \mathbb{R}$.

We have

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

We can use the fundamental theorem to write

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

To get an idea why this is true, we start writing out the first few terms:

$$\left(1 - \frac{1}{2^s}\right)^{-1}\left(1 - \frac{1}{3^s}\right)^{-1}\left(1 - \frac{1}{5^s}\right)^{-1} \cdots$$

We observe, the geometric series: $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$, so

$$\left(1 - \frac{1}{2^s}\right)^{-1} = \frac{1}{1 - \frac{1}{2^s}} = \sum_{n=0}^{\infty} \frac{1}{2^{sn}} = \left(\frac{1}{2^{s0}} + \frac{1}{2^s} + \frac{1}{2^{s2}} + \cdots\right)$$

So we have

$$\left(1 - \frac{1}{2^s}\right)^{-1}\left(1 - \frac{1}{3^s}\right)^{-1} \cdots$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right) \cdots$$

$$= 1 + \frac{1}{2^s} + \frac{1}{4^s} + \cdots$$
$$+ \frac{1}{3^s} + \frac{1}{9^s} + \cdots$$
$$+ \frac{1}{6^s} + \frac{1}{18^s} + \cdots$$

So these two terms give all the $\frac{1}{n^s}$ with $n = 2^m 3^r$

for $u, v \in \mathbb{Z}$. Continuing in this way we get the result that

$$\zeta(s) = \prod_p (1 - \tfrac{1}{p^s})^{-1}.$$

Proof (3): Suppose there are only finitely many primes $p_1, \ldots, p_n$. Then we have that

$$\zeta(s) = (1 - \tfrac{1}{p_1^s})^{-1} \cdots (1 - \tfrac{1}{p_n^s})^{-1}.$$

In particular, $\zeta(s)$ is a finite product. But then $\zeta(1)$ must be a #. This contradicts that $\zeta(1)$ is a divergent series. Thus there must be ∞'ly many primes. ∎

So we now have several ways to show there are infinitely many primes. What about the summation

$$\sum_{p \text{ prime}} \frac{1}{p} \quad ?$$

We know this is smaller than the divergent harmonic series, but does it converge or diverge? It turns out it diverges!

On your homework you will prove this using $\zeta(s)$. Here we will actually get a bound on the series

$$\sum_{p \le y} \frac{1}{p}$$

for $y \in \mathbb{R}$.

Thm: For every $y \in \mathbb{R}$, $y \ge 2$,

$$\sum_{p \le y} \frac{1}{p} > \log\log y - 1.$$

Observe that once we have shown this, letting $y \to \infty$ gives that the series $\sum_p \frac{1}{p}$ diverges. This is a much stronger result though because it tells how fast the series is growing. (very slowly!)

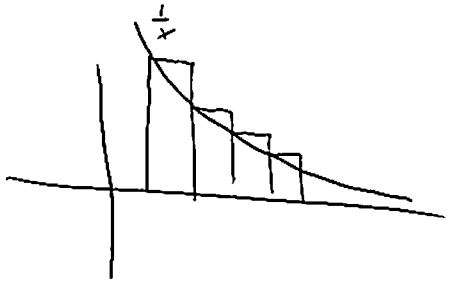
Note that this series diverging gives yet another proof that there are ∞'ly many primes.

Proof: Let $y \in \mathbb{R}$, $y \ge 2$. Let N be the set of $\overset{p \le y.}{\text{integers}}$ whose prime factorizations contain only primes $\le y$.

There are only finitely many primes $p \le y$, so we may rearrange the summation $\sum_{n \in N} \frac{1}{n}$ to see

$$\sum_{n \in N} \frac{1}{n} = \prod_{p \le y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \qquad (*)$$

(just like above!) If $n \le y$, then clearly $n \in N$ and so $\sum_{n \in N} \frac{1}{n}$ includes the sum $\sum_{n \le y} \frac{1}{n}$. We now apply the integral test from calculus



to conclude

$$\sum_{n=1}^{N} \frac{1}{n} \ge \int_1^{N+1} \frac{1}{x}\, dx = \log(N+1) > \log y$$

where N is the largest integer $\le y$, i.e., $N \le y < N+1$.

Thus, $\sum_{n \in N} \frac{1}{n} > \log y$. Thus, we have

$$\prod_{p \le y} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \le y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

$$= \sum_{n \in N} \frac{1}{n} > \log y.$$

<u>Claim:</u> $e^{v+v^2} \ge (1-v)^{-1}$ for all $0 \le v \le 1/2$.

Pf: We show that if $f(v) = e^{v+v^2}(1-v)$, then $f(v) \geq 1$ for all $0 \leq v \leq 1/2$. $f(0) = 1$, so we are done if we show f is an increasing function. Then

$$f'(v) = -e^{v+v^2} + (1-v)(1+2v)e^{v+v^2}$$

$$= v(1-2v)e^{v+v^2} \geq 0$$

for $0 \leq v \leq 1/2$. □

Set $v = \frac{1}{p}$. Then $e^{\frac{1}{p}+\frac{1}{p^2}} \geq (1-\frac{1}{p})^{-1}$.

$$\Rightarrow \prod_{p \leq y} e^{\frac{1}{p}+\frac{1}{p^2}} \geq \prod_{p \leq y} (1-\tfrac{1}{p})^{-1} > \log y. \quad (**)$$

But

$$\prod_{p \leq y} e^{\frac{1}{p}+\frac{1}{p^2}} = e^{\sum_{p \leq y}(\frac{1}{p}+\frac{1}{p^2})},$$

so taking logs of both sides of $(**)$ we have

$$\sum_{p \leq y} \left(\frac{1}{p} + \frac{1}{p^2}\right) > \log\log y \log\log y$$

i.e.,

$$\sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p^2} > \log\log y.$$

However, we have

$$\sum_{p \leq y} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2} < \int_1^{\infty} \frac{dx}{x^2} = 1.$$

Thus,

$$\sum_{p \leq y} \frac{1}{p} > \log\log y - 1.$$

□

Thm: The n^{th} prime p_n satisfies $p_n < 2^{2^{n-1}}$ for $n \geq 2$.

Proof: We proceed by induction on n. The case $n=2$ is clear as $n=2$ gives $p_2 = 3$ and $2^{2^{2-1}} = 2^2 = 4$. Assume the statement is true for $2 \leq n \leq N$ for some integer N. Recall when we showed there are infinitely many primes that there is a prime p with $p > p_j$ for $1 \leq j \leq N$ as that $p \mid p_1 \cdots p_N + 1$. Since p_{N+1} is the next prime after p_N, we must have $p_{N+1} \leq p$. Thus, $p_{N+1} \leq p_1 \cdots p_N + 1$. Now apply the inductive hypothesis:

$$\begin{aligned} p_{N+1} &\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{N-1}} + 1 \\ &= 2^{1+2+2^2+\cdots+2^{N-1}} + 1 \\ &= 2^{2^N - 1} + 1 \\ &\leq 2^{2^N - 1} + 2^{2^N - 1} \\ &= 2^{2^N}. \end{aligned}$$

Thus, by induction we have

$$p_n \leq 2^{2^{n-1}}$$

for all $n \geq 2$. However, we know for $n \geq 2$ that p_n is odd, so cannot be a power of 2. Thus $p_n < 2^{2^{n-1}}$. ∎

Cor: We have $\pi(x) > \log\log x + 1$ for $x \geq 2$.

Proof: Let $x \in \mathbb{R}$ with $x \geq 2$. Choose $k \in \mathbb{Z}$ so that $2^{2^k} \leq x < 2^{2^{k+1}}$. This is clearly possible.

Our previous result shows that there are at least $k+1$ primes smaller than 2^{2^k}, thus $\pi(x) \geq k+1$. The logarithm is an increasing function, so $\log x < \log 2^{2^{k+1}}$

$$= 2^{k+1} \log 2$$

$$= 2^k \, 2 \log 2$$

$$< 2^k.$$

i.e., $\log x < 2^k$. Thus,

$$\log \log x < k \log 2$$

$$< k.$$

Thus, $\log \log x + 1 < k+1 < \pi(x)$,

which gives the result. ∎

Thm: There are arbitrarily large gaps between consecutive prime numbers.

Proof: Let n be any (pos) integer. Consider the sequence of consecutive integers given by:

$n!+2$, $n!+3$, ..., $n!+n$.

Each of these is composite, so we have a sequence of $n-1$ consecutive composite numbers. As $n \to \infty$, the gaps between primes in such a sequence get arbitrarily large. ∎

So we have two opposite ends of the spectrum. The twin prime Conjecture said there are infinitely many primes p so that $p+2$ is prime as well. These primes have as small a gap as possible. On the other hand, we have just shown there are gaps as large as we would like between consecutive primes! This should convince you that prime numbers and how they appear among the integers is a pretty difficult thing to understand!

We conclude our study of primes with a few more Conjectures and results.

Goldbach's Conjecture: Every even integer greater than 4 is the sum of two odd primes.

This is still unknown! Your text has a good summary of where the conjecture stands right now!

Dirichlet's Theorem: Let $a, b \in \mathbb{Z}_{>0}$ with $\gcd(a,b)=1$. The sequence

$$a,\ a+b,\ a+2b,\ a+3b,\ \ldots$$

contains infinitely many primes.

This is a known result, but requires much more background than we have for this class. As a special case we have:

Thm: There are ∞'ly many primes of the form $4k+3$.

This is a specific example of Dirichlet's theorem with $a=3$, $b=4$. However, we can prove this theorem without resorting to Dirichlet's theorem.

Proof: Suppose there are only finitely many such primes, say $p_1, \ldots, p_n$. Let $N = 4p_1 \cdots p_n - 1$

$$= 4(p_1 \cdots p_n - 1) + 3.$$

As in the case of the proof of ∞'ly many primes, there must be a prime other than $p_1, \ldots, p_n$ that divides N for otherwise we get $p_j \mid 1$. We also have N is odd, so $2 \nmid N$. So there is an odd prime other

that is not of the form $4k+3$ that divides N. Odd primes are of the form $4k+1$ or $4k+3$. Since N cannot be divisible by any primes of the form $4k+3$, it must be divisible by primes of the form $4k+1$. However, this contradicts that N is of the form $4m+3$ since $(4k+1)(4l+1) = 4x+1$. ∎

Thus far, everything we have discussed has had to do with divisibility in one form or another. We have basically worked from the definition to gain insights. We will now introduce a new tool, the theory of congruences. This was first established by Gauss. You should read the section in the text for some relevant historical background.

Def: Let $n \in \mathbb{Z}_{>0}$. We say integers a and b are congruent modulo n, written

$$a \equiv b \pmod{n}$$

if $n \mid (a-b)$.

Examples: ① $2 \equiv 9 \pmod{7}$

$6 \equiv -1 \pmod{7}$