Recall from last time:

Euclid's Algorithm. (applied to 45 and 33)

$$\begin{aligned} 45 &= 1 \times 33 + 12 \\ 33 &= 2 \times 12 + 9 \\ 12 &= 1 \times 9 + 3 \\ 9 &= 3 \times 3 + 0 \end{aligned}$$

Algorithm returns last non-zero remainder, which is 3. We proved

Theorem 7.7. Euclid's algorithm, applied to two positive integers *a* and *b*, returns the highest common factor of *a* and *b*.

Along the way, we also proved
Lemma 7.6. If Euclid's algorithm applied to *a* and *b* returns the positive integer *d*, then for all divisors *e* of *a* and *b*, we have $e \mid d$ (and in particular $e \leq d$, because $d \in \mathbb{Z}_{\geq 1}$).

Lemma 7.6. If Euclid's algorithm applied to *a* and *b* returns the positive integer *d*, then for all divisors *e* of *a* and *b*, we have $e \mid d$ (and in particular $e \leq d$, because $d \in \mathbb{Z}_{\geq 1}$).

Theorem 7.7. Euclid's algorithm, applied to two positive integers *a* and *b*, returns the highest common factor of *a* and *b*.

Applying Theorem 7.7 to Lemma 7.6, we deduce

Theorem 7.8. If *a* and *b* are positive integers, and if $d = \text{hcf}(a, b)$, then any common divisor *e* of *a* and *b* divides *d*.

Lemma 7.6 and Theorem 7.7 are about an algorithm, but Theorem 7.8 is a "pure" theorem which does not mention Euclid's algorithm at all.

Here is another theorem whose statement does not mention Euclid's algorithm, but whose proof does.

Theorem 7.9. If a, b are positive integers, then there exists integers λ and μ such that $\lambda a + \mu b = \text{hcf}(a, b)$.

What do you think of the following "proof by example"?

Finding λ and μ such that hcf$(a, b) = \lambda a + \mu b$:

$$\begin{aligned} 45 &= 1 \times 33 + 12 \\ 33 &= 2 \times 12 + 9 \\ 12 &= 1 \times 9 + 3 \\ 9 &= 3 \times 3 + 0 \end{aligned}$$

We see from the first line that
$12 = 45 - 33 = 1 \times 45 + (-1) \times 33$.
From the second line we see $9 = 33 - 2 \times 12 =$
$33 - 2(45 - 33) = 3 \times 33 - 2 \times 45 = (-2) \times 45 + 3 \times 33$.
From the third line we see
$3 = 12 - 9 = (45 - 33) - (3 \times 33 - 2 \times 45) = 3 \times 45 - 4 \times 33$.
And from the fourth line we deduce that 3 is what Euclid's algorithm returns and hence 3 is the highest common factor of 45 and 33.
Will the same proof work for the general case?

Theorem 7.9. If a, b are positive integers, then there exists integers λ and μ such that $\lambda a + \mu b = \text{hcf}(a, b)$.

Boring formal proof of general case. Let the notation be as in Euclid's algorithm. We prove by strong induction on $i \geq 0$ that every remainder r_i can be written as $\lambda_i a + \mu_i b$. Case $i = 0$, need to solve $b = \lambda_0 a + \mu_0 b$ and so set $\lambda_0 = 0$ and $mu_0 = 1$. Case $i = 1$, recall that $r_1 = a - q_1 b$ so we can set $\lambda_0 = 1$ and $\mu_0 = -q_1$. General case $i \geq 2$, we know $r_i = r_{i-2} - q_i r_{i-1}$ and by the inductive hypothesis we know $r_{i-2} = \lambda_{i-2} a + \mu_{i-2} b$ and $r_{i-1} = \lambda_{i-1} a + \mu_{i-1} b$, so can deduce
$r_i = (\lambda_{i-2} - q_i \lambda_{i-1}) a + (\mu_{i-2} - q_i \mu_{i-1}) b$.

□

I hope you are all now enlightened.

We are now armed with the fundamental facts we need about greatest common divisors; let's now develop the basic theory of factorization into primes in the integers.

Factorization into primes.

Just before we start – some notation. Recall that we write $a \mid b$ for the true-false statement "a divides b". Its negation, "a does not divide b", is written $a \nmid b$ (`nmid` in LaTeX).

Recall that a positive integer p is called *prime* if $p > 1$ and the only factors of p are p and 1. Today we'll see why 1 is not a prime number, by the way.

Lemma 7.10 If p is prime and $a \in \mathbb{Z}_{\geq 1}$, and if $p \nmid a$, then $\text{hcf}(p, a) = 1$.

Proof. $\text{hcf}(p, a)$ is a factor of p by definition of hcf, so it is 1 or p by definition of "prime".
Now of these two factors of p, we see that 1 is a factor of a, but p is by assumption not a factor of a. Hence the *only* common positive factor of p and a, and hence the highest common factor of p and a, is 1.

□

Now here is a question I already asked you a few days ago. Is it true that if a, b, c are positive integers, and $a \mid bc$, then $a \mid b$ or $a \mid c$? Let's vote on it!

It is *not true* that $a \mid bc$ implies $a \mid b$ or $a \mid c$.
Indeed, $6 \mid 4 \times 9$ but $6 \nmid 4$ and $6 \nmid 9$.
How can we fix it?

Lemma 7.11 If $a, b, c \in \mathbb{Z}_{\geq 1}$ with $a \mid bc$ and $\mathrm{hcf}(a, b) = 1$, then $a \mid c$.

Before we start on the proof, here's a question. Does $\mathrm{hcf}(a, b) = 1$ imply $a \nmid b$? Let's vote on it!

It's not true! Because a could be 1. But for $a > 1$ this is true, because $a \mid b$ implies that a is a common factor of a and b, so $\mathrm{hcf}(a, b) \geq a > 1$.

Lemma 7.11 If $a, b, c \in \mathbb{Z}_{\geq 1}$ with $a \mid bc$ and $\mathrm{hcf}(a, b) = 1$, then $a \mid c$.

Proof. By Theorem 7.9, we can find integers λ and μ with $\lambda a + \mu b = 1$.

Multiplying both sides of this equation by c we deduce

$$\lambda ac + \mu bc = c.$$

But certainly $a \mid \lambda ac$, and by assumption $a \mid bc$ so $a \mid \mu bc$. So a divides $\lambda ac + \mu bc$ which is the left hand side of the above equation. Hence $a \mid c$.

□

Lemma 7.10 If p is prime and $a \in \mathbb{Z}_{\geq 1}$, and if $p \nmid a$, then $\text{hcf}(p, a) = 1$.

Lemma 7.11 If $a, b, c \in \mathbb{Z}_{\geq 1}$ with $a \mid bc$ and $\text{hcf}(a, b) = 1$, then $a \mid c$.

Corollary 7.12 If $p, b, c \in \mathbb{Z}_{\geq 1}$ with p *prime*, and if $p \mid bc$, then $p \mid b$ or $p \mid c$.

Proof of 7.12. Let's assume $p \mid bc$, but that $p \nmid b$. Our goal is then to prove that $p \mid c$. But if $p \nmid b$ then $\text{hcf}(p, b) = 1$ by Lemma 7.10, and hence $p \mid c$ from Lemma 7.11.

□

Corollary 7.12 If $p, b, c \in \mathbb{Z}_{\geq 1}$ with p prime, and if $p \mid bc$, then $p \mid b$ or $p \mid c$.

Proposition 7.13 If $n \geq 1$ and $a_1, a_2, \ldots, a_n$ are all positive integers, with $p \mid \prod_{i=1}^{n} a_i$, then $p \mid a_j$ for some j with $1 \leq j \leq n$.

Proof. By induction on $n \geq 1$. Base case $n = 1$ says $p \mid a_1$ implies $p \mid a_1$, which is obvious.

Inductive step: let's assume it's true for $n = d$ and try and prove it for $n = d + 1$.

So let's assume $p \mid \prod_{i=1}^{d+1} a_i$. Now $\prod_{i=1}^{d+1} a_i = \left(\prod_{i=1}^{d} a_i\right) \times a_{d+1}$ (by *definition* of $\Pi_{i=1}^{n}$), so by Corollary 7.12 either $p \mid \prod_{i=1}^{d} a_i$ or $p \mid a_{d+1}$. In the first case, $p \mid a_j$ for some $j \leq d$ by the inductive hypothesis; in the second case set $j = d + 1$.

We just saw the "recursive step" in the definition of $\prod_{i=1}^{n} a_i$. What do you think the base case is? It's $\prod_{i=1}^{0} a_i = 1$. So $\prod_{i=1}^{1} a_i = \prod_{i=1}^{0} a_i \times a_1 = 1 \times a_1 = a_1$.

Theorem 7.14. Every positive integer is uniquely a product of prime numbers.

What does this even mean? For example $6 = 2 \times 3 = 3 \times 2$. That's two "different" ways of writing 6 as a product of primes!

Theorem 7.14, formally stated:
(a) If $s \in \mathbb{Z}_{\geq 1}$ then there exists $n \in \mathbb{Z}_{\geq 0}$ and $p_1, p_2, \ldots, p_n$ prime numbers, such that $s = \prod_{i=1}^{n} p_i$. (note that we already did this – it's Theorem 4.1.)
(b) If also $m \in \mathbb{Z}_{\geq 0}$ and $q_1, q_2, \ldots, q_m$ are prime numbers, and $s = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$, then $m = n$, and after possibly re-arranging the order of the q_j (which of course doesn't change the product), we have $p_i = q_i$ for all $1 \leq i \leq n$.

(a) says existence, and (b) says uniqueness, of prime factorization.

Theorem 7.14, formally stated:
(a) If $s \in \mathbb{Z}_{\geq 1}$ then there exists $n \in \mathbb{Z}_{\geq 0}$ and $p_1, p_2, \ldots, p_n$ prime numbers, such that $s = \prod_{i=1}^{n} p_i$.
(b) If also $m \in \mathbb{Z}_{\geq 0}$ and $q_1, q_2, \ldots, q_m$ are prime numbers, and $s = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$, then $m = n$, and after possibly re-arranging the order of the q_j (which of course doesn't change the product), we have $p_i = q_i$ for all $1 \leq i \leq n$.

Proof. (a) is Theorem 4.1.

As for (b), for $n \in \mathbb{Z}_{\geq 0}$ we let $P(n)$ be the statement "If $m \in \mathbb{Z}_{\geq 0}$ and $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$ are primes, and if $\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$, then $n = m$ and after possibly re-arranging the order of the q_j we have $p_i = q_i$ for all $1 \leq i \leq n$."

We prove this by induction on n. What do we need to do to prove the base case $P(0)$? Well, if $n = 0$ then the assumption in $P(0)$ is that $1 = \prod_{j=1}^{m} q_j$, and if $m \geq 1$ then we have a contradiction because then $q_1 \leq \prod_{j=1}^{m} q_j = 1 < q_1$. So we can conclude $m = 0$ and hence that $P(0)$ is a true statement.

$P(n) :=$ "If $m \in \mathbb{Z}_{\geq 0}$ and $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$ are primes, and if $\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$, then $n = m$ and after possibly re-arranging the order of the q_j we have $p_i = q_i$ for all $1 \leq i \leq n$."

The inductive step: say $n = d + 1$ and $\prod_{i=1}^{d+1} p_i = \prod_{j=1}^{m} q_j$. Setting $p = p_{d+1}$ we deduce $p \mid \prod_{j=1}^{m} q_j$. By Proposition 7.13 we deduce that $p \mid q_k$ for some k with $1 \leq k \leq m$ (and in particular that $m \geq 1$). But q_k is prime, so only has factors 1 and q_k, and $p > 1$, so $p = q_k$. Now swap q_k and q_m, so now $p = q_m$, and cancel p from $\prod_{i=1}^{d+1} p_i = \prod_{j=1}^{m} q_j$, and we deduce that $\prod_{i=1}^{d} p_i = \prod_{j=1}^{m-1} q_j$. By the inductive hypothesis, we can assume $P(d)$, so we can conclude that $d = m - 1$ and after re-arranging the q_j we have $p_i = q_i$ for all $i \leq d$. Also $p_{d+1} = p = q_m = q_{d+1}$, so we are done.

□

One consequence of this theorem is that we can now talk unambiguously about “the” prime factors of a positive integer.

Here’s another consequence. Because we don’t care about the order of the prime factors of a positve integer, we may as well put them into increasing order. Once we’ve done that, we can start collecting up primes that occur with multiplicity greater than one and and writing them as prime powers. For example $24 = 2 \times 2 \times 2 \times 3$ becomes $24 = 2^3 \times 3$.
So now let’s break with the convention that $p_1, p_2, p_3, \ldots$ are just any old primes, and let’s instead use the convention that $2 = p_1 < 3 = p_2 < 5 = p_3 < 7 = p_4 < \cdots$ are all the prime numbers arranged in increasing order. For example one can check $p_{100} = 541$.

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$.
Now if s is a positive integer, and we choose $N \in \mathbb{Z}_{\geq 1}$ large enough all primes occurring in its factorization are at most p_N, then we have a new way of writing s as a product of primes: we can write

$$s = \prod_{i=1}^{N} p_i^{e_i}$$

with $e_i \in \mathbb{Z}_{\geq 0}$, but $e_i = 0$ is allowed.

For example, $45 = 2^0 \times 3^2 \times 5^1$. The uniqueness part of the theorem above says that if $\prod_{i=1}^{N} p_i^{e_i} = \prod_{i=1}^{N} p_i^{f_i}$ then $e_i = f_i$ for all i.

Here's some consequences of uniqueness of prime factorization which can be useful.

Proposition 7.15. If $a, b, c, n \in \mathbb{Z}_{\geq 1}$ with $\mathrm{hcf}(a, b) = 1$, and if $ab = c^n$, then both a and b are nth powers of positive integers.

Proof. Assume a, b, c, n are chosen to satisfy the equation. Choose N so large that all prime factors of a, b and c are at most p_N, the Nth prime. Write $a = \prod_{i=1}^N p_i^{r_i}$, $b = \prod_{i=1}^N p_i^{s_i}$ and $c = \prod_{i=1}^N p_i^{t_i}$, with $r_i, s_i, t_i \in \mathbb{Z}_{\geq 0}$.

The assertion that $\mathrm{hcf}(a, b) = 1$ means that no p_i divides both a and b, and so for each $i \leq N$ we must have either $r_i = 0$ or $s_i = 0$. And the assertion that $ab = c^n$ implies that $\prod_{i=1}^N p_i^{r_i+s_i} = \prod_{i=1}^N p_i^{nt_i}$. By Theorem 7.14, $r_i + s_i = nt_i$ for all i.

There is only quite a restricted set of solutions to these equations. We could have $r_i = s_i = t_i = 0$. But if one of r_i or s_i is non-zero, then the other one must be zero by the above, and so from $r_i + s_i = nt_i$ we deduce that the non-zero one is nt_i. In all possible cases, we see that n must divide both r_i and s_i.

We just saw that if $a = \prod_{i=1}^{N} p_i^{r_i}$ and $b = \prod_{i=1}^{N} p_i^{s_i}$ then $n \mid r_i$ and $n \mid s_i$ for all i.

Hence $r_i/n \in \mathbb{Z}_{\geq 0}$, so $\prod_{i=1}^{N} p_i^{r_i/n}$ is a positive integer whose nth power is a, and similarly $\prod_{i=1}^{N} p_i^{s_i/n}$ has nth power equal to b.

□

Proposition 7.16. If $a, n \in \mathbb{Z}_{\geq 1}$ and if there exists $b \in \mathbb{Q}_{>0}$ with $b^n = a$, then $b \in \mathbb{Z}$.

Here's an application of 7.16. There is clearly no *integer s* such that $s^5 = 44$, because $2^5 = 32$ is too small and $3^5 = 243$ is too big. So by Proposition 7.16, there can be no rational number whose 5th power is 44. So if you believe in existence of real *n*th roots, you can deduce that $44^{1/5}$ is irrational.

Proof. Write $b = \frac{c}{d}$ in lowest terms; then $\mathrm{hcf}(c, d) = 1$. We multiply up and deduce $c^n = ad^n$. We are trying to prove that $d = 1$. If however $d > 1$, then we can choose a prime $p \mid d$, and then $p \mid c^n$. By Proposition 7.13, $p \mid c$. This contradicts $\mathrm{hcf}(c, d) = 1$.

□

Now consider this. We deduced this amazing theorem, that every positive integer was uniquely a product of prime numbers, just from basic reasoning about division with remainder.

But polynomials over the rationals, reals, complexes, or any field at all (if you know what a field is – and if you don't then don't worry) also have the division with remainder property.

If f, g are polynomials with real coefficients, and if g is non-zero, then we can write $f = qg + r$ with $\deg(r) < \deg(g)$.

Proof by example: too hard for me to LaTeX.

If you go through this lecture and the last lecture, you can see that the theory of the highest common factor (which in this case is the monic polynomial of highest degree which divides a and b) works, all the lemmas are true in this case, and we conclude that polynomials factor uniquely into "irreducible polynomials", modulo scalars.

Applications to Diophantine equations.

A Diophantine equation is just a polynomial equation which you have to find one, or all, solutions of, in integers or rational numbers.
Here's an example: $x^3 - x = y^5 - y$.
Obvious solutions in integers: if $x = 0$ or ± 1, and if $y = 0$ or ± 1, then both the left hand side and the right hand side are zero, which gives nine solutions.

An application of a deep theorem of Faltings from 1984 (which applies to a large class of Diophantine equations including this one) shows that the number of rational solutions to this equation (i.e., solutions to the equation with $x, y \in \mathbb{Q}$) is *finite*.
But Faltings' theorem is *ineffective* – it is an abstract proof by contradiction. No algorithm is known which is guaranteed to spit out all the solutions to this equation and then stop.

Finding, with proof, all rational solutions to $x^3 - x = y^5 - y$, is *beyond current human capabilities*.