The main purpose of this lesson is to introduce some important number theory which is frequently used in higher level math courses such as Abstract Algebra courses. Some of the more instructive proofs will be given.

Definition: The *greatest common divisor* (abbreviated GCD) of two integers a and b, one of which is nonzero, is the largest positive integer which divides both a and b. The GCD is often denoted by $\gcd(a, b)$.
Example:
$\gcd(4, 6) = 2$, $\gcd(24, 25) = 1$.

Definition: Two integers a and b are said to be *relatively prime* if $\gcd(a, b) = 1$.

How can we compute $\gcd(1245, 998)$? This seems quite difficult; it turns out that there is a useful algorithm for computing the GCD called the *Euclidean algorithm*. The Euclidean algorithm uses the division algorithm for integers repeatedly.

The Division Algorithm

The division algorithm for integers says the following: Given two positive integers a and b, with $b \neq 0$, there exists unique integers q and r such that

$$a = qb + r$$

where $0 \leq r < |b|$.

This may appear to be confusing at first, but it is literally just saying that you can divide an integer a by a nonzero integer b and get a remainder which is less than the number we are dividing by.

Example:

Given $a = 18$ and $b = 4$, we can write $18 = 4 \cdot 4 + 2$. This is just dividing 18 by 4 which we expect to have remainder 2.

The Euclidean Algorithm

Here is an example to illustrate how the Euclidean algorithm is performed on the two integers $a = 91$ and $b_1 = 17$.

Step 1: $91 = 5 \cdot 17 + 6$ (i.e. write $a = q_1 b_1 + r_1$ using the division algorithm)
Step 2: $17 = 2 \cdot 6 + 5$ (i.e. write $b_1 = q_2 r_1 + r_2$ using the division algorithm)
Step 3: $6 = 1 \cdot 5 + 1$ (i.e. write $r_1 = q_3 r_2 + r_3$ using the division algorithm)
Step 4: $5 = 5 \cdot 1 + 0$ (i.e. write $r_2 = q_4 r_3 + r_4$ using the division algoirhtm)

The general algorithm is as follows: Given two integers a and b
Step 1: Write $a = q_0 b + r_0$
Step 2: Write $b = q_1 r_0 + r_1$
Step i ($i \geq 2$): Write $r_{i-2} = q_i r_{i-1} + r_i$.

The algorithm terminates at the step j where we get $r_j = 0$. When the Euclidean algorithm is over, that is, when we get $r_j = 0$, then $r_{j-1} = \gcd(a, b)$. Said differently, $\gcd(a, b)$ is the last nonzero remainder in the Euclidean algorithm.

Bezout's Idenitity and the Extended Euclidean Algorithm

A very useful fact is *Bezout's identity.*

Bezout's Idenity:

Let a and b be nonzero integers and let d be their GCD. Then we can write d as a linear combination of a and b; that is, there exist integers s and t such that

$$d = sa + tb.$$

Furthermore,
i. d is the smallest positive integer that can be written in the form $sa + tb$,
ii. every other integer of the form $sa + tb$ is a multiple of d.

Example:

a. Above we computed that $\gcd(25, 24) = 1$. We can write $1 = 1 \cdot 25 - 1 \cdot 24$.

b. Consider $d = \gcd(1245, 998)$ from above. We can check using the Euclidean algorithm that $d = 1$. We can write $1 = 299 \cdot 1245 - 373 \cdot 998$.

Seeing the GCD from example (b) above written in the form of Bezout's identity can easily cause one to wonder how anyone would ever come up with that. This is fairly easy to do by using the *Extended Euclidean Algirhtm.* The proof of Bezout's identity also follows from the *extended Euclidean algorithm* but we will omit the proof and just assume Bezout's identity is true (the fact that you can always write d in the form $ax + by$ should be pretty clear from the example; proving it formally is just a matter of generalizing the example) . Here is an example illustrating how to use the Extended Euclidean Algorithm.

Example: Extended Euclidean Algorithm

Let's compute $\gcd(232, 108) = 4$ and then write the gcd in the form of Bezout's identity.

Step A: Use the Euclidean algorithm to compute $\gcd(232, 108)$

Step A1: $232 = 2 \cdot 108 + 16$
Step A2: $108 = 6 \cdot 16 + 12$
Step A3: $16 = 1 \cdot 12 + 4$
Step A4: $12 = 4 \cdot 3 + 0$

The last nonzero remainder in the Euclidean algorithm is 4 so $\gcd(232, 108) = 4$.

Step B: Use the Extended Euclidean Algorithm to write the GCD in the form of Bezout's identity

We want to find integers s and t such that $4 = s \cdot 232 + t \cdot 108$.

Step B1: From step A3 notice that you can write $4 = 16 - 1 \cdot 12$.

Step B2: From step A1 notice that $16 = 232 - 2 \cdot 108$ and $12 = 108 - 6 \cdot 16$. Substitute these in the equation from step B1 to get $4 = 232 - 2 \cdot 108 - (108 - 6 \cdot 16) \implies 4 = 232 - 2 \cdot 108 - 108 + 6 \cdot 16 \implies$

$4 = 232 - 3 \cdot 108 + 6 \cdot 16$. **Notice that we don't actually multiply out** $3 \cdot 108$ **because we want to write** 4 **in the form of Bezout's identity and we don't actually multiply out** $6 \cdot 16$ **because we wish to substitute 16 in terms of** 232 **and** 108 **in the next step**

Step B3: Notice from step A1 that $16 = 232 - 2 \cdot 108$. Substitute this in the final equation from step B2 to get $4 = 232 - 3 \cdot 108 + 6(232 - 2 \cdot 108) \implies 4 = 232 - 3 \cdot 108 + 6 \cdot 232 - 12 \cdot 108 \implies 4 = 7 \cdot 232 - 15 \cdot 108$.

Now we have written $4 = 7 \cdot 232 - 15 \cdot 108$ which is the desired form.

Remark: Your actual work in practice for the extended Euclidean algorithm should probably look something like this:

$4 = 16 - 1 \cdot 12$
$4 = 232 - 2 \cdot 108 - (108 - 6 \cdot 16) = 232 - 3 \cdot 108 + 6 \cdot 16$
$4 = 232 - 3 \cdot 108 + 6(232 - 2 \cdot 108) = 232 - 3 \cdot 108 + 6 \cdot 232 - 12 \cdot 108 = 7 \cdot 232 - 15 \cdot 108.$

A useful consequence of Bezout's identity is Euclid's Lemma:

Euclid's Lemma: Let p be a prime number; let a and b be integers. Then if $p|ab$ then $p|a$ or $p|b$.

Proof. Assume p is prime and that $p|ab$ so that there exists an integer n such that $ab = np$. Furthermore assume that $p \nmid a$. We show that that under this assumption it is necessary that $p|b$. Since p is prime, and $p \nmid a$, it follows that $\gcd(a, p) = 1$. Thus by Bezout's identity there exist integers s and t such that

$$1 = sp + ta. \tag{1}$$

Multiplying both sides of (1) by b yields

$$b = bsp + bta \tag{2}$$

Thus we have $b = bsp + npt = p(bs + nt)$; so $p|b$. □

Related to the GCD of two positive integers is the least common multiple of two positive integers.

Definition: The *least common multiple* of two positive integers a and b (abbreviated LCM) is the smallest positive integer which is a multiple of both a and b. The LCM is often denoted by $\text{lcm}(a, b)$.

Example:

$\text{lcm}(4, 2) = 4$,
$\text{lcm}(6, 9) = 18$,
$\text{lcm}(3, 7) = 21$

There is an important relationship between the GCD and LCM of two positive integers. It is given by the following theorem. The proof is tricky.

Theorem: The product of two positive integers a and b is equal to the product of the LCM and the GCD of a and b; that is,

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

Proof. Set $d = \gcd(a, b)$ and $\ell = \text{lcm}(a, b)$. Clearly d divides ab. Set

$$m = \frac{ab}{d}. \tag{3}$$

We show that $m = \ell$. Observe that since $d|a$ and $d|b$, we have that m is a multiple of both a and b; we show that in fact $m = \ell$. Suppose n is any positive common multiple of a and b. We show that $m|n$ so that $n \geq m$. Use Bezout's identity to write $d = sa + tb$ for integers s and t. Then we have

$$\frac{n}{m} = \frac{nd}{ab} = \frac{n(sa + tb)}{ab} = \frac{n}{b}s + \frac{n}{a}t.$$

Since $\frac{n}{b}, \frac{n}{a} \in \mathbb{Z}$, it follows that $\frac{n}{m} \in \mathbb{Z}$ so that $m|n$. Thus $m = \ell$ and $ab = d\ell$ by (3). □

Mathematical Induction

The principle of mathematical induction is a useful proof technique for establishing that a given statement P_n is true for all positive integers. There are two commonly used forms of induction.

The First Principle of Mathematical Induction: Suppose we have some statement P_n and suppose
(i) P_1 is true, that is, the statement is true for $n = 1$ and,
(ii) The assumption that P_n is true implies P_{n+1} is true.
Then the statement P_n is true for all $n \in \mathbb{N}$.

Checking that P_1 is true is often called the *base case* and (ii) is often called the *induction step* and the assumption that P_n is true is often called the *induction hypotheis*. You can also check that the base case holds for any natural number n_0 (say $n_0 = 0$ or $n_0 = 4$, etc.) and use induction to conclude that the statement is true for all $n \geq n_0$. Also, sometimes you need to establish your base case for $n = 2$ to succeed in your induction step (see Example 2 below). Intuitively the principle of mathematical induction makes sense; you can think of each of the statements P_n as being dominos. Then we have an infinite line of dominos and we establishing that P_1 is true can be thought of knocking over the first domino. Then, assuming that the n^{th} domino has been knocked over (i.e. statement P_n being true) implies that the next domino will be knocked over (i.e. statement P_{n+1} is true) then all dominos will be knocked over.

Example 1:
Prove by induction that the sum of the first n positive integers is equal to $\frac{n(n+1)}{2}$; that is,

$$1 + 2 + ... + n = \frac{n(n + 1)}{2}.$$

Proof. Proceed by induction on n.

Base Case: Check that the statement is true for $n = 1$. This is trivial, the sum of the first 1 integers is 1 and $1 = 1\frac{(2)}{2}$.

Induction Step: Assume that the statement is true for n and prove that it is true for $n + 1$; that

is, assume $1+2+...+n=\frac{n(n+1)}{2}$ and prove that $1+2+...+(n+1)=\frac{(n+1)(n+2)}{2}$. We have

$$\begin{aligned}1+2+...+(n+1) &= (1+2+...+n)+(n+1)\\ &= \frac{n(n+1)}{2}+n+1\\ &= \frac{n(n+1)+2(n+1)}{2}\\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

□

Exercise: Prove that $1^2+2^2+...+n^2=\frac{n(n+1)(2n+1)}{6}$. Clearly state what your base case, induction hypothesis, and desired conclusion are.

Example 2: Generalized Euclid's Lemma If p is a prime and p divides the product $a_1a_2...a_n$, then p must divide one of the factors a_i.

Proof. Proceed by induction on n.

Base Case: Here we need $n=2$ for our base case ($n=1$ is trivial). But this is just Euclid's lemma which was proved above.

Induction Step: Assume that it is true that if $p|a_1a_2...a_n$ then p divides one of the a_i and prove that if $p|a_1a_2...a_{n+1}$ then p divides one of the a_i..

Assume p divides $a_1a_2...a_{n+1}$. Then p divides $(a_1a_2...a_n)a_{n+1}$. But this is the product of two integers, namely the integers $a=a_1a_2...a_n$ and $b=a_{n+1}$. By the base case $p|a$ or $p|b$. If $p\nmid b$ then p divides a, so by the induction hypothesis p divides one of the a_i. □

The Second Principle of Mathematical Induction: Suppose we have some statement P_n and suppose
(i) P_1 is true, that is, the statement is true for $n=1$ and,
(ii) The assumption that P_k is true for all positive integers k with $1\leq k\leq n$ implies P_{n+1} is true.
Then the statement P_n is true for all $n\in\mathbb{Z}^+$.

The second principle of mathematical induction is also sometimes called *strong induction*. You can also use $n=n_0$ as your base case and then in (ii) you assume that P_k is true for all nonnegative integers k with $n_0\leq k\leq n$ and conclude that P_n is true for all integers $n\geq n_0$. You can think of the second principle of mathematical induction as assuming that all previous dominos have been knocked over implying that the next domino will still be knocked over as well. It turns out that the first and second principles of mathematical induction are logically equivalent, and you can always use the second principle of mathematical induction; however, it is generally advised to avoid using strong induction whenever you can use the first principle because if you can use the first principle, then assuming the induction hypothesis of the second principle is assuming more than one actually needs to assume, which is considered inelegant.

Example 3:
We prove using the second principle of mathematical induction that every positive integer n with $n\geq 2$ has a prime divisor.

Proof. Base Case: Here we use the base case $n = 2$. This is trivial.

Induction Step: We assume that n is an integer and that all integers k with $2 \leq k \leq n$ have a prime divisor and prove that the integer $n+1$ has a prime divisor. If $n+1$ is prime then $n+1$ trivially has a prime divisor, so assume $n+1$ is not prime. Then there exist an integer a different from 1 and $n+1$ which divides $n+1$; that is,

$$n + 1 = ab$$

for integers a and b, where $a \neq 1$ and $b \neq 1$. Thus $a \leq n$ so by the induction hypothesis a has a prime divisor p; it follows that p divides $n+1$ as well. □

Example 4: The Fundamental Theorem of Arithmetic

Theorem: Ever integer greater than $n > 1$ there exists a factorization of n into a product of prime numbers. Furthermore, this product is unique up to order of the factors.

Proof. Existence: The existence of the factorization uses the second principle of mathematical induction. The base case $n = 2$ is clearly true since 2 is prime. So we assume that all integers k with $2 \leq k \leq n$ have a prime factorization and prove that $n+1$ has a prime factorization. If $n+1$ is prime it is its own factorization so the theorem holds. If $n+1$ is not prime, then by the previous example $n+1$ has a prime divisor p_1 so that we have $n + 1 = p_1 m$ for some $m \in \mathbb{Z}^+$. But then m is an integer with $2 \leq m \leq n$. Thus $m = p_2...p_r$ for primes $p_2, ..., p_r$ by the induction hypothesis. Hence $n + 1 = p_1 p_2...p_r$ is a prime factorization of $n + 1$. Thus by induction all integers have a prime factorization.

Uniqueness: Now we prove that the prime factorization of an integer n is unique up to reordering of the factors. That is, if

$$n = p_1...p_s$$
$$n = q_1...q_t$$

are both prime factorizations of n, then $s = t$ and that the q_i are a rearrangement of the p_i. To obtain a contradiction, assume that $s < t$. We have that q_1 divides $p_1...p_s$, so by generalized Euclid's lemma p_1 divides one of the q_i. By relabeling the q_i if necessary (which is okay since multiplication is commutative), assume that p_1 divides q_1. But p_1 and q_1 are prime so in particular $p_1 \neq 1$ and the only divisors of q_1 are 1 and itself, we must have $p_1 = q_1$. Using the exact same argument we can show that $p_i = q_i$ for all i with $1 \leq i \leq s$. Then

$$1 = \frac{n}{n} = \frac{q_1..q_t}{p_1...p_s} = \frac{q_1...q_s q_{s+1}...q_t}{p_1...p_s} = \left(\frac{q_1...q_s}{p_1...p_s}\right) q_{s+1}...q_t.$$

Since $\frac{q_1...q_s}{p_1...p_s} = 1$ we must also have $q_{s+1}...q_t = 1$, but these are integers so $q_{s+1}, ..., q_t$ must also all be equal to 1, contradicting the assumption that q_t is prime. □

Exercises

1. Use the division algorithm to find q and r such that $a = qb + r$ with $0 \leq r < |b|$.
a. $a = 300$, $b = -17$,
b. $a = 389$, $b = 4$.

2. Use the Euclidean algorithm to
a. Compute $\gcd(323, 437)$ and write $\gcd(323, 437) = 323s + 437t$ for some $s, t \in \mathbb{Z}$.
b. Compute $\gcd(1437, 345)$ and write $\gcd(1437, 345) = 1437s + 345t$ for some $s, t \in \mathbb{Z}$.

3. Let $a, b, c, n \in \mathbb{Z}$. Prove
a. if $a|n$ and $b|n$ and $\gcd(a, b) = 1$, then $ab|n$,
b. if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

4. Let a, b, c, d and $m \in \mathbb{Z}$. Prove
a. if $a|b$ and $b|c$, then $a|c$,
b. if $a|b$ and $c|d$, then $ac|bd$,
c. if $m \neq 0$, then $a|b$ if and only if $ma|mb$.

5.
a. Let $k \in \mathbb{Z}$. Show that 3 divides one of k, $k + 2$, or $k + 4$.
b. Find all prime numbers p for which $p + 2$ and $p + 4$ are also prime.

6. Prove the following for every $n \in \mathbb{Z}^+$.
a. $2n^3 - 3n^2 + n$ is divisible by 6,
b. $5^n - 1$ is divisible by 4,
c. (If you're feeling motivated) $1^4 + 2^4 + ... + n^4 = \frac{1}{30}n(n + 1)(2n + 1)(3n^2 + 3n - 1)$.

7 Let $x_1, ..., x_n \in \mathbb{R}^+$. Prove that for $\ln(x_1x_2...x_n) = \ln(x_1) + \ln(x_2) + ... + \ln(x_n)$ for every $n \in \mathbb{Z}^+$. *(You may assume* $\ln(ab) = \ln(a) + \ln(b)$ *for all* $a, b \in \mathbb{R}^+$*).*

8. Recall that the Fibonacci sequence is defined recursively as follows: $f_0 = 0$, $f_1 = f_2 = 1$ and $f_n = f_{n-2} + f_{n-1}$ for $n \geq 3$.
a. Use induction to prove that $f_1 + f_3 + f_5 + ... + f_{2n-1} = f_{2n}$ for all $n \geq 1$.
b. Prove that the GCD of two consecutive numbers in the Fibonacci sequence is equal to 1.

9. Use induction to prove that the power set of a set with n elements has 2^n elements.