Properties of the Integers

What can we know about integers when doing proofs? For this class, we are going to take the following as axiomatic truth (i.e. this is our basic starting point for facts about the integers):

Axioms. The following are our axioms for integers:

1. For all $a \in \mathbb{Z}$ both $a + 0 = a$ and $a \cdot 1 = a$. (Identity)
2. For all $a \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ so that $a + b = 0$. (Negatives)
3. For all $a, b \in \mathbb{Z}$ both $a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$. (Closure)
4. For all $a, b \in \mathbb{Z}$ both $a + b = b + a$ and $ab = ba$. (Commutativity)
5. For all $a, b, c \in \mathbb{Z}$ both $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$. (Associativity)
6. For all $a, b \in \mathbb{Z}$ if $ab = 0$, then either $a = 0$ or $b = 0$. (Zero Product)
7. For all $a, b, c \in \mathbb{Z}$ we have $a(b + c) = ab + ac$. (Distribution)
8. For all $a, b, c, d \in \mathbb{Z}$ if $a < c$ and $0 < b \leq d$, then $ab < cd$. (Comparison)
9. For all $a, b \in \mathbb{Z}$ if $a \leq b$ and $b \leq a$, then $a = b$. (Inequality Antisymmetry)
10. For all $a, b \in \mathbb{Z}$, exactly one of $a < b$ or $a = b$ or $b < a$ holds. (Total Ordering)

Fun fact: Most of these hold for natural numbers, and all of them hold for rational numbers and real numbers!

The following two definitions are critically important.

Definition. Let $m, n \in \mathbb{Z}$. We say m *divides* n (written $m \mid n$) when $n = mk$ for some $k \in \mathbb{Z}$.

Definition. An integer $p \geq 2$ is *prime* when for all $d \in \mathbb{N}_0$ we have $d \mid p$ implies either $d = 1$ or $d = p$. An integer $n \geq 2$ which is not prime is *composite*.

Divisibility

We can prove a number of elementary properties of divisibility quite easily. First we prove a simple lemma.

Lemma 1. *Let $d, n \in \mathbb{Z}_{>0}$. If $d \mid n$, then $d \leq n$.*

Proof. Exercise. □

Proposition 2 (Basic Properties of Divisibility)**.** *Let $a, b, c \in \mathbb{Z}$ be arbitrary.*

1. *We have $a \mid a$, $1 \mid a$, and $a \mid 0$.*
2. *If $a \mid b$ and $b \mid a$, then either $b = a$ or $b = -a$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
4. *If $a \mid b$ and $a \mid c$, then for all $s, t \in \mathbb{Z}$ we have $a \mid (bs + ct)$.*

Proof. Let $a, b, c \in \mathbb{Z}$ be arbitrary.

Part 1: Note that $a = a \cdot 1$, $a = 1 \cdot a$, and $0 = 0 \cdot a$ yield $a \mid a$, $1 \mid a$, and $a \mid 0$ respectively.

Part 2: Assume $a \mid b$ and $b \mid a$. Thus there exist integers $u, v \in \mathbb{Z}$ such that $b = au$ and $a = bv$ by definition of divisibility. Now either $a = 0$ or $a \neq 0$. If $a = 0$, then $b = 0 \cdot u = 0 = a$. Otherwise by substitution we have

$$a = bv = (au)v = a(uv),$$

which yields $1 = uv$ by the cancellation property of integers. Thus $1 = uv = \text{abs}(uv) = \text{abs}(u)\,\text{abs}(v)$ yields $\text{abs}(u) = 1$ by basic properties of the absolute value; hence $u = 1$ or $u = -1$, and so $b = a$ or $b = -a$.

Part 3: Assume $a \mid b$ and $b \mid c$. There are $u, v \in \mathbb{Z}$ with $b = au$ and $c = bv$. Now $c = bv = (au)v = a(uv)$ by substitution. Let $k := uv$ and note $k \in \mathbb{Z}$ by closure. Hence $c = ak$ and $a \mid c$ by definition of divisibility.

Part 4: Assume $a \mid b$ and $a \mid c$, and let $s, t \in \mathbb{Z}$ be arbitrary. Now $b = au$ and $c = av$ for some $u, v \in \mathbb{Z}$ by definition of divisibility. Thus we compute $bs + ct = (au)s + (av)t = a(us) + a(vt) = a(us + vt)$. Let $k := us + vt$ and note $k \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $bs + ct = ak$ and $a \mid (bs + ct)$ by definition.

We conclude that the original statement is true. □

Quotient-Remainder Theorem

The following theorem is of major importance in number theory (and mathematics as a whole).

Proposition 3 (Quotient-Remainder Theorem)**.** *Let $n, d \in \mathbb{Z}$ with $d \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that*

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d.$$

We say q is the *quotient* under division by d, and r is the *remainder* under division by d.

We will prove the special case of the above theorem when $n, d \in \mathbb{N}_0$; the general case is a **homework exercise**.

Proof. Let $n, d \in \mathbb{N}_0$ with $d \neq 0$. We must prove both existence and uniqueness.

Existence: We start by considering the set

$$S := \{m \in \mathbb{N}_0 : \text{there is a } q \in \mathbb{Z} \text{ with } n = dq + m\} \subseteq \mathbb{N}_0.$$

We have $n \in S \neq \emptyset$ because $n = d \cdot 0 + n$ and $n \in \mathbb{N}_0$. Thus S has a minimal element $r = \min(S)$ by the Well Ordering Principle; moreover, there is a $q \in \mathbb{Z}$ with $n = dq + r$ by definition of S. Now we must show $0 \leq r < d$; we have $0 \leq r$ by $r \in S \subseteq \mathbb{N}_0$. Assume to the contrary that $r \geq d$. Subtracting d from both sides of this inequality yields $0 \leq r - d$, so $r - d \in \mathbb{N}_0$. Moreover we compute

$$n = dq + r = dq + r + (d - d) = (dq + d) + (r - d) = d(q + 1) + (r - d),$$

and $q + 1 \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Relabelling $q' = q + 1$ and $r' = r - d$, we see $n = dq' + r'$; this yields $r' \in S$ under our assumptions. Now $r' < r$ yields $r \neq \min(S)$, which is a contradiction; thus our assumption $r \geq d$ cannot be true! Hence $r < d$ as desired. Thus we have shown that the existence claim holds.

Uniqueness: Assume there are pairs $q_1, r_1 \in \mathbb{Z}$ and $q_2, r_2 \in \mathbb{Z}$ such that

$$n = dq_1 + r_1 \qquad \text{and} \qquad 0 \leq r_1 < d \qquad \text{and} \qquad n = dq_2 + r_2 \qquad \text{and} \qquad 0 \leq r_2 < d.$$

Up to relabeling, we may assume $r_1 \leq r_2$. The equality $dq_1 + r_1 = n = dq_2 + r_2$; yields $r_2 - r_1 = dq_1 - dq_2 = d(q_1 - q_2)$. By the closure property of the integers we see $q_1 - q_2 \in \mathbb{Z}$, which yields $d \mid (r_2 - r_1)$ by definition of divisibility. On the other hand $0 \leq r_2 - r_1 \leq r_2 < d$ by $r_1 \leq r_2$; hence $r_2 - r_1 = 0$ by Lemma 1. Now we see $d(q_1 - q_2) = r_2 - r_1 = 0$, so either $d = 0$ or $q_1 - q_2 = 0$ by the Zero Product Property of $\mathbb{Z}$. However, we assumed that $d \neq 0$, so we must have $q_1 - q_2 = 0$. In particular $q_1 = q_2$ and $r_1 = r_2$. Hence the uniqueness claim holds. □

Modular Arithmetic

Now let's use the Quotient-Remainder Theorem to make a new system of arithmetic!

Let $m \in \mathbb{Z}_{>0}$ be given. We can define *congruence modulo m* in the following way; for $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{m}$ when a and b have equal remainders under division by m.

Proposition 4. *For all $a, b \in \mathbb{Z}$ we have $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.*

Proof. Exercise! □

Problem 1. Let $m \in \mathbb{Z}$ with $m \neq 0$ be arbitrary. Show that congruence modulo m is an equivalence relation.

For all $a \in \mathbb{Z}$, let $[a] = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\}$ denote the *equivalence class of a modulo m*. We can define *addition modulo m* on the set $\mathbb{Z}_m := \{[n] : n \in \mathbb{Z}\}$ by $[a] + [b] = [a + b]$, and *multiplication modulo m* by $[a] \cdot [b] = [ab]$.

But is this well defined? In particular, we want to think of these operations as functions $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$; thus we need to see that given $a, b, c, d \in \mathbb{Z}$ we have $[a] = [c]$ and $[b] = [d]$ implies $[a] + [b] = [c] + [d]$. We will do that now.

Proposition 5. *Let $m \in \mathbb{Z}_{>0}$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$ and $ab \equiv cd \pmod{m}$.*

Proof. Let $m \in \mathbb{Z}_{>0}$ and $a, b, c, d \in \mathbb{Z}$ be arbitrary, and suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. By Proposition 4, we have $m \mid (a - c)$ and $m \mid (b - d)$. Thus there are integers $s, t \in \mathbb{Z}$ such that $a - c = ms$ and $b - d = mt$.

To see that the relevant sums are congruent, we compute

$$(a + b) - (c + d) = (a - c) + (b - d) = ms + mt = m(s + t).$$

Note $s + t \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$, so $m \mid ((a + b) - (c + d))$; hence $a + b \equiv c + d \pmod{m}$ by Proposition 4.

To see that the relevant products are congruent, we rewrite $a = ms + c$ and $b = mt + d$. Now we compute

$$ab = (ms + c)(mt + d) = msmt + msd + cmt + cd = m(mst + sd + ct) + cd.$$

Thus subtractiong cd from both sides we obtain $ab - cd = m(mst + sd + ct)$; but $mst + sd + ct \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $m \mid (ab - cd)$, yielding $ab \equiv cd \pmod{m}$ by Proposition 4. □

The proposition above yields immediately that our modular arithmetic above makes sense! What can we do with this? More to come on that, but for the time being let's try to get a feel for this new arithmetic. We will do so with a *Cayley table*, a sort of grid listing all of the possible operations. Here are Cayley tables for arithmetic modulo 2:[1]

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Here are Cayley tables for arithmetic modulo 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Just to have one, somewhat larger example, here are Cayley tables for arithmetic modulo 9:

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

It's quite therapeutic to draw Cayley tables; you might consider doing this the next time you are stressed...

Problem 2. Build Cayley tables for arithmetic modulo 4, 5, 6, 7, and 8.

Greatest Common Divisors

Oftentimes the following notion will be very useful.

Definition. Let $a, b \in \mathbb{Z}$ with either $a \neq 0$ or $b \neq 0$. The *greatest common divisor* of a and b is

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}.$$

Let's notice some elementary properties of $\gcd(a, b)$.

Proposition 6 (Properties of the Greatest Common Divisor)**.** *Let $a, b, c \in \mathbb{Z}$ with either $a \neq 0$ or $b \neq 0$. We have the following.*

1. *We have $\gcd(a, b) > 0$.*
2. *If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.*

Proof. Exercise. □

The following result is important in number theory.

Proposition 7 (Bézout's Identity)**.** *For all $a, b \in \mathbb{Z}_{>0}$ there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.*

[1] I've omitted the square brackets; it looks really messy if you include them... I had my computer generate these tables.

Proof. Let $a, b \in \mathbb{Z}_{>0}$ be arbitrary, let $d := \gcd(a, b)$, and define

$$S := \{k \in \mathbb{Z}_{>0} : \text{there are } s, t \in \mathbb{Z} \text{ with } k = as + bt\}.$$

Notice that $a = a \cdot 1$ shows $S \neq \emptyset$, and thus S has a minimum element D by the Well Ordering Principle. There are $s, t \in \mathbb{Z}$ such that $D = as + bt$ because $D \in S$. We must show $D = d$; we do so by showing $d \mid D$, $D \mid d$, and $d, D > 0$.

We will first show $d \mid D$. Now $d \mid a$ and $d \mid b$, so $d \mid (as + bt)$ by Proposition 2. Hence $d \mid D$ as desired.

We next show $D \mid d$. By definition of S we have $D > 0$, so we may apply the Quotient-Remainder Theorem to obtain $a = Dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < D$. Now substituting $D = as + bt$ in this equation we obtain $a = (as + bt)q + r = asq + btq + r$; solving for r we obtain $r = a(1 - sq) + b(-tq)$. Letting $x = 1 - sq$ and $y = -tq$ we see that $r = ax + by$; but $x, y \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Thus either $r = 0$ or $r \in S$; noting that $r \notin S$ because $r < D = \min(S)$, we see $r = 0$. Hence $a = Dq + 0 = Dq$ yields $D \mid a$; a very similar argument shows that $D \mid b$ (**Exercise!**). Hence by basic properties of the greatest common divisor we have $D \mid d$.

Notice that $d > 0$ by properties of the greatest common divisor, and $D \in S \subseteq \mathbb{Z}_{>0}$ yields $D > 0$. Finally, by basic properties of divisibility we have $D = \pm d$, which yields (together with $d, D > 0$) that $d = D$. □

Euclid's Algorithm

Bézout's Identity is a really cool result; unfortunately, it doesn't give us a method to compute the greatest common divisor of two numbers. On the other hand, it does suggest an approach; if we can find the smallest $d \in \mathbb{N}_0$ which can be expressed as a linear combination of a and b, then we have computed $\gcd(a, b)$. Euclid's (Extended) Algorithm provides one way to do so. Before stating Euclid's Algorithm, we need a few more easy Lemmas.

Lemma 8. *Let $a, b \in \mathbb{Z}$.*

1. *We have $\gcd(a, b) = \gcd(b, a)$.*
2. *If $b = aq + r$ with $q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(a, r)$.*

Proof. Exercise! □

We can now state Euclid's Algorithm!

Algorithm (Euclid's (Extended) Algorithm). Let a and b be integers with $a \neq 0$.

1. Let $n_1 = b$ and $d_1 = a$.
2. Write $n_1 = d_1 q_1 + r_1$ where $q_1, r_1 \in \mathbb{Z}$ have $0 \leq r_1 < d_1$.
3. Having computed n_i, d_i, q_i, and r_i with $r_i \neq 0$:
   (a) Let $n_{i+1} = d_i$ and $d_{i+1} = r_i$.
   (b) Write $n_{i+1} = d_{i+1} q_{i+1} + r_{i+1}$ for $q_{i+1}, r_{i+1} \in \mathbb{Z}$ with $0 \leq r_{i+1} < d_{i+1}$.
   (c) Return to the beginning of this step and repeat until $r_{i+1} = 0$.
4. Now that $r_i = 0$, we have $d_i = \gcd(a, b)$.
5. (Extended) Perform back substitution to write $\gcd(a, b) = as + bt$ for some appropriate $s, t \in \mathbb{Z}$.

Problem 3. Why does Euclid's Algorithm have to stop? What prevents it from going *ad infinitum*?

Problem 4. Prove Euclid's Extended Algorithm computes $\gcd(a, b) = as + bt$ for some $s, t \in \mathbb{Z}$ (i.e. Bézout's Identity).

Let's see a few examples applying Euclid's Algorithm.

Example 1. Compute $\gcd(8901, 210)$ via Euclid's Algorithm.

Solution. First we enact the divisions prescribed by steps 1 through 3 of the algorithm:

$$\begin{aligned} 210 &= 8901 \cdot 0 + 210 \\ 8901 &= 210 \cdot 42 + 81 \\ 210 &= 81 \cdot 2 + 48 \\ 81 &= 48 \cdot 1 + 33 \\ 48 &= 33 \cdot 1 + 15 \\ 33 &= 15 \cdot 2 + 3 \\ 15 &= 3 \cdot 5 + 0 \end{aligned}$$

Hence we have computed $\gcd(8901, 210) = 3$. □

Example 2. Compute $\gcd(34, 55)$ as a linear combination of 34 and 55 via Euclid's Extended Algorithm.

Solution. First we enact steps 1 through 3 of the algorithm below:

$$\begin{aligned} 55 &= 34 \cdot 1 + 21 \\ 34 &= 21 \cdot 1 + 13 \\ 21 &= 13 \cdot 1 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

In particular, this shows that $\gcd(34, 55) = 1$.

Now make back-substitutions to write $\gcd(34, 55)$ as a linear combination of 34 and 55. First, we solve each of the above equations for the remainder, working from the bottom up:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 5 - 3 \cdot 1 \\ 3 &= 8 - 5 \cdot 1 \\ 5 &= 13 - 8 \cdot 1 \\ 8 &= 21 - 13 \cdot 1 \\ 13 &= 34 - 21 \cdot 1 \\ 21 &= 55 - 34 \cdot 1 \end{aligned}$$

Now we substitute sequentially and simplify in the above:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 3 \cdot 2 - 5 \cdot 1 = (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1 \\ &= 8 \cdot 2 - 5 \cdot 3 = 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3 \\ &= 8 \cdot 5 - 13 \cdot 3 = (21 - 13 \cdot 1) \cdot 5 - 13 \cdot 3 \\ &= 21 \cdot 5 - 13 \cdot 8 = 21 \cdot 5 - (34 - 21 \cdot 1) \cdot 8 \\ &= 21 \cdot 13 - 34 \cdot 8 = 55 \cdot 13 - 34 \cdot 21 \end{aligned}$$

Hence the desired linear combination is $1 = 55 \cdot 13 + 34(-21)$. □

Problem 5. Let F_n denote the n^{th} Fibonacci number.

1. Show that $\gcd(F_n, F_{n+1}) = 1$ for all $n \in \mathbb{N}_0$.
2. Show that Euclid's Algorithm to compute $\gcd(F_n, F_{n+1})$ terminates after $n - 1$ computations for $n \geq 2$.
3. Can you find a general formula $1 = F_{n+1}s - F_n t$ for $s, t \in \mathbb{Z}$ for all $n \geq 3$?

Solving Linear Modular Equations

Proposition 9. *The equation* $ax \equiv b \pmod{m}$ *has a solution in* $\mathbb{Z}_m$ *if and only if* $\gcd(a, m) \mid b$.

Proof. Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$.

Suppose $ax \equiv b \pmod{m}$ has a solution $x = c$. Now $m \mid (ac - b)$ as $ac \equiv b \pmod{m}$ yields $ac - b = mk$ for some $k \in \mathbb{Z}$. Solving for b we obtain $b = ac + m(-k)$. Hence $\gcd(a, m) \mid b$ by basic properties of divisibility.

Suppose $\gcd(a, m) \mid b$ and let $d := \gcd(a, m)$. Thus $b = dk$ for some $k \in \mathbb{Z}$. Moreover $d = as + mt$ for some $s, t \in \mathbb{Z}$ by Bézout's Identity. Now $b = dk = (as + mt)k = a(sk) + m(tk)$ and closure properties of $\mathbb{Z}$ yield $sk, tk \in \mathbb{Z}$. Finally $b = a(sk) + m(tk) \equiv a(sk) + 0(tk) = a(sk) \pmod{m}$ yields that $x = sk$ is a solution to $ax \equiv b \pmod{m}$. □

Remark. If $ax \equiv b \pmod{m}$ has a solution and $m \nmid a$, then it has a unique solution with $0 \leq x < m$ (Why?).

Remark. If p is prime, then $ax \equiv b \pmod{p}$ has a solution as long as $p \nmid a$.

The above proposition gives us a criterion for solvability of modular linear equations, but its proof gives us a method. To solve a modular linear equation $ax \equiv b \pmod{m}$, we can first compute $\gcd(a, m)$ via Euclid's Algorithm. If $\gcd(a, m) \nmid b$, then we know $ax \equiv b \pmod{m}$ has no solution. Otherwise let $d := \gcd(a, m)$ and write $b = mk$ for some $k \in \mathbb{Z}$; apply back substitutions to finish Euclid's Extended Algorithm to write $d = as + mt$. Finally $b = dk = a(sk) + m(tk) \equiv a(sk) \pmod{m}$ yields $x = sk$ as the solution.

Example 3. If possible, solve $77x \equiv 204 \pmod{213}$ for an integer $0 \leq x < 13$.

Solution. First we apply Euclid's Algorithm to compute $\gcd(77, 213)$.

$$\begin{aligned} 213 &= 77 \cdot 2 + 59 \\ 77 &= 59 \cdot 1 + 18 \\ 59 &= 18 \cdot 3 + 5 \\ 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Now we know $\gcd(77, 213) = 1 \mid 204$; we apply back substitutions to obtain the following.

$$\begin{aligned} 1 &= 3 + 2(-1) \\ &= 3 + (5 - 3(1))(-1) = 3(2) + 5(-1) \\ &= (18 + 5(-3))(2) + 5(-1) = 18(2) + 5(-7) \\ &= 18(2) + (59 + 18(-3))(-7) = 18(23) + 59(-7) \\ &= (77 + 59(-1))(23) + 59(-7) = 77(23) + 59(-30) \\ &= 77(23) + (213 + 77(-2))(-30) = 77(83) + 213(-30) \end{aligned}$$

Thus $77 * 83 \equiv 1 \pmod{213}$. Finally we multiply through the original equation to obtain $x \equiv 83 \cdot 204 \pmod{213}$. Thus to finish the computation we need only compute $83 \cdot 213$ and reduce modulo 213.

$$x \equiv 83 \cdot 204 = 16932 = 79 * 213 + 105 \equiv 105 \pmod{213}$$

Hence we have computed the desired $x = 105$. □

Example 4. If possible, solve $15x \equiv 4 \pmod{3}$ for an integer $0 \leq x < 3$.

Solution. This is not possible; we will show this in two different ways.

First Solution: We can rewrite the modular equation $15x \equiv 4 \pmod{3}$ as $3 \cdot 5x \equiv 3 + 1 \pmod{3}$; rewriting again yields $0 \equiv 1 \pmod{3}$ which is false! Thus no solution can exist.

Second Solution: Observe $\gcd(15, 3) = 3 \nmid 4$; thus the proposition yields $15x \equiv 4 \pmod{3}$ has no solution.

Hence $15x \not\equiv 4 \pmod{3}$ for all $x \in \mathbb{Z}$. □

Note that there is a theory for solving quadratic equations, but it turns out to be a bit more complicated (in a similar way to how solving quadratic equations is more complicated than solving linear equations over $\mathbb{R}$).

Prime Numbers and the Fundamental Theorem of Arithmetic

Example 5. The integer 2 is prime. The integer 1 is not divisible by any prime. The integer 15 is not prime.

Proposition 10. *Every natural number $n \geq 2$ is divisible by some prime.*

Our proof below will use Strong Mathematical Induction; the formal statement of Strong Induction is

$$(P(0) \wedge \forall n \in \mathbb{N}_0[\forall k \in \mathbb{N}_0[k \leq n \implies P(k)] \implies P(n+1)]) \implies \forall n \in \mathbb{N}_0[P(n)].$$

Recall that Strong Mathematical Induction, Weak Mathematical Induction, and the Well Ordering Principle all express the same idea in slightly different ways.

Proof. We proceed by induction on n.

Base Case: If n is any prime number, then $n \mid n$ yields the result for n; in particular, the result holds for $n = 2$.

Inductive Step: Assume that for some $n \geq 2$ and all $2 \leq k \leq n$ we have that k is divisible by some prime number. We must now show that $n+1$ is also divisible by a prime. Either $n+1$ is prime or not; we proceed by cases. If $n+1$ is prime, then $(n+1) \mid (n+1)$ yields that $n+1$ is divisible by a prime. If $n+1$ is not prime, then by definition, there is a d such that $1 < d < n+1$ and $d \mid (n+1)$. Now $2 \leq d \leq n$, so by the inductive hypothesis there is a prime p such that $p \mid d$; hence $p \mid (n+1)$ by transitivity of divisibility. In either case $n+1$ is divisible by a prime number.

We conclude that the original statement is true by Strong Mathematical Induction. □

Problem 6. Give a proof of the proposition above using the Well Ordering Principle.

The proposition above has the following cool consequence.

Proposition 11. *There are infinitely many prime numbers.*

Proof. Assume to the contrary that there are finitely many prime numbers $p_1, p_2, \cdots, p_n$. Let $P := p_1 p_2 \cdots p_n$; we know $p_1 = 2$, so by elementary arithmetic $P \geq 2$, and thus $P + 1 \geq 2$. Thus P is divisible by a prime number q by the previous proposition. Now $q = p_k$ for some $1 \leq k \leq n$; by definition of divisibility, there is an $m \in \mathbb{Z}$ with $P+1 = qm$. Now write $Q = p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n$ for the product of all the primes other than $q = p_k$; thus $P = qQ$ and so $qm = P + 1 = qQ + 1$. Subtract qQ from both sides to see $1 = qm - qQ = q(m - Q)$. This yields $q \mid 1$, and thus $q = 1$ by properties of divisibility. But this implies $q = 1$ is not prime, a contradiction!

We conclude that our initial assumption was false; in particular, there are infinitely many primes. □

Proposition 12 (Euclid's Lemma)**.** *Let $p, m, n \in \mathbb{N}_0$. If p is prime and $p \mid mn$, then either $p \mid m$ or $p \mid n$.*

Proof. Let $p \in \mathbb{N}_0$ be an arbitrary prime number and $m, n \in \mathbb{N}_0$ such that $p \mid mn$. If $p \mid m$ we are done. Otherwise $p \nmid m$, so we can conclude $\gcd(p, m) = 1$ because p is prime. By Bézout's Identity, we can write $1 = ps + mt$ for some $s, t \in \mathbb{Z}$. Now multiply both sides of this equation by n to obtain $n = psn + mnt$. As $p \mid mn$ there is a $k \in \mathbb{Z}$ such that $mn = pk$; thus $n = psn + mnt = psn + pkt = p(sn + kt)$ and $sn + kt \in \mathbb{Z}$ by basic properties of integers. Hence $p \mid n$. As the result holds in either case, we conclude that the original statement is true. □

Problem 7. Find three numbers $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.

The following is a consequence of Euclid's Lemma and the fact that every natural number is divisible by a prime.

Proposition 13. *Every natural number can be written as a product of primes, unique up to the order of the primes.*

Proof. Exercise.[2] □

Searching for Primes

How do we test whether or not a given number is prime? The following algorithm is an obvious approach.

Algorithm (Attempt 1). Let $n \geq 2$ be an integer and let $p = 2$.

1. If $p = n$, stop; conclude n is prime.
2. Otherwise:
   (a) If $p \mid n$, stop; conclude n is composite.
   (b) If $p \nmid n$, replace p by $p + 1$ and return to step 1.

This algorithm is obviously very inefficient; it has us testing all integers up to n for a prime n.

Remark. Let $n = 8675309$. There are $60 * 60 * 24 = 86400$ seconds in a day; if we were to run these computations nonstop, checking one number by hand every second, we could expect to be done applying this algorithm after $8675309/86400 \approx 100$ days...

A slightly more efficient algorithm is informed by the following proposition.

Proposition 14. *If $n \geq 2$ is composite, then n has a prime factor p with $p \leq \sqrt{n}$.*

Proof. Let $n \geq 2$ be composite. We show $n = ab$ for some $a, b \in \mathbb{N}_0$ implies either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Assume to the contrary $a > \sqrt{n}$ and $b > \sqrt{n}$; so $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, which is absurd. Hence either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. □

[2] HINT: Use Strong Induction or the Well Ordering Principle, together with the two facts mentioned before the proposition.

Using this proposition we can modify our algorithm above into the following (the maroon part has changed):

Algorithm (Attempt 2). Let $n \geq 2$ be an integer and let $p = 2$.

1. If $p > \sqrt{n}$, stop; conclude n is prime.
2. Otherwise:
   (a) If $p \mid n$, stop; conclude n is composite.
   (b) If $p \nmid n$, replace p by $p + 1$ and return to step 1.

This algorithm has us checking far fewer divisibility conditions; that's good!

Remark. We have $\sqrt{8675309} \approx 2945$, so we only need to check about 3000 divisibility conditions with this algorithm.

We still check more than we need–we only need to check prime p. Let's modify the algorithm! This time, we also increase the power of the algorithm by asking for the full set of primes smaller than a given n.

Algorithm (Sieve of Eratosthenes). Let $n \geq 2$.

1. Create a list of integers $1 \leq k \leq n$ and cross off 1.
2. Let p be the smallest number in the list which is neither circled nor crossed off.
   (a) If $p > \sqrt{n}$, go to step 3.
   (b) Otherwise, circle p and cross off all multiples of p greater than p on the list.
   (c) Return to the beginning of step 2.
3. Circle all numbers on the list which have not yet been crossed off.
4. Output the list of circled numbers.

Example 6. We will compute the set of prime numbers which are at most $n = 30$ via the Sieve of Eratosthenes; note $5 < \sqrt{30} < 6$. First we write out the list of integers less than or equal to 30 and strike out the number 1.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Next find the first uncrossed number $p = 2$ and circle it; as $2 < \sqrt{30}$, also cross out all multiples of 2.

~~1~~	[2]	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~

Now find the first uncrossed number $p = 3$ and circle it; as $3 < \sqrt{30}$, also cross out all multiples of 3.

~~1~~	[2]	[3]	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~

Now find the first uncrossed number $p = 5$; as $5 < \sqrt{30}$ circle it and cross out all multiples of 5.

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

Now find the first uncrossed number $p = 7$; as $7 > \sqrt{30}$, we can proceed to circle all uncrossed numbers:

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	[7]	~~8~~	~~9~~	~~10~~
[11]	~~12~~	[13]	~~14~~	~~15~~	~~16~~	[17]	~~18~~	[19]	~~20~~
~~21~~	~~22~~	[23]	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	[29]	~~30~~

Finally, we output the set of circled numbers $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$. □

This algorithm is a lot quicker than the previous one for large n, but requires us to store more information.

Problem 8. Prove that the output set from the Sieve of Eratosthenes is the set of all prime numbers at most n.

Remark. This algorithm is quite good, but we could improve it a little bit more if we tried. Most improvements are very small in the big picture (more on this "big picture" later in the course).

Problem 9. Write a program in your favorite programming language to implement the Sieve of Eratosthenes.