Math 320 Lecture Notes, Chapter 1 and 2

Tony Armas

Spring 2020

1 Arithmetic in the Integers

1.1 The Division Algorithm

Recall that $\mathbb{Z}$ denotes the set of integers:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}.$$

We'll assume familiarity with the arithmetic (addition, subtraction, multiplication) of integers and the usual order relation $<$ on $\mathbb{Z}$.

Here, we're going to talk about *division*. Recall from grade-school that sometimes when you divide numbers, you get a *remainder*. For instance, when you divide 21 by 5, you get a *quotient* of 4 with remainder 1, and we can write

$$21 = 4 \cdot 5 + 1.$$

We can formalize this idea of division into a theorem, which we call the Division Algorithm:

Theorem 1.1 (The Division Algorithm): Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

Notice that a can be negative, but we're assuming that b is positive. Also notice that r must be nonnegative. If we let r be negative, then this will ruin the uniqueness of the theorem.

We won't prove this theorem, since the proof is difficult and the methods used in it are not relevant to this class.

Examples:

1. $a = 17, b = 4$:

$$17 = 4 \cdot 4 + 1,$$

so $q = 4, r = 1$.

2. $a = 0, b = 19$:

$$0 = 19 \cdot 0 + 0,$$

so $q = r = 0$.

3. $a = -51, b = 6$

$$-51 = -9 \cdot 6 + 3$$

When $a < 0$, this algorithm produces a different quotient than the "usual" division. Here, we require that the remainder r be *nonnegative*, so you have to "overshoot" with the quotient. In this example, we'd punch $-51/6$ into a calculator and get -8.5, but this gives us a remainder of -3. If we make the quotient $q = -9$, then our remainder will be 3, which satisfies the requirement that $0 \leq r < b = 6$.

The Division Algorithm can give us some more interesting results:

4. Let n be any integer. By the Division Algorithm, we know there exist $q, r \in \mathbb{Z}$ such that

$$n = 2q + r,$$

where $0 \leq r < 2$, i.e. $r = 0$ or 1. Since n is arbitrary, this tells us that every integer can be written as $2q$ or $2q + 1$, where q is some integer. This is the same as saying that every integer is either even or odd.

5. Let a be an odd integer, and $b = 4$. By the division algorithm, there exist q and $0 \leq r < 4$ such that

$$a = 4q + r.$$

What values can r be? If $r = 0$, then $a = 4q$, which implies that a is even, a contradiction.

If $r = 2$, then $a = 4q + 2$, which is again a contradiction, since this would imply that a is even.

This means that r can only be 1 or 3. So, every odd integer is either of the form $4q + 1$ or $4q + 3$ for some integer q.

6. Something more difficult: Show that the square of any integer a is either of the form $3m$ or $3m+1$ for some integer m.

By the Division Algorithm, we can write $a = 3q, 3q+1$, or $3q+2$. This gives us three cases to check:

1. $a = 3q$:

$$(3q)^2 = 9q^2 = 3(3q^2) = 3k,$$

where $k = 3q^2$ in this case.

2. $a = 3q + 1$:

$$(3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3p + 1,$$

where here, $p = 3q^2 + 2q$.

3. $a = 3q + 2$:

$$(3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1 = 3t + 1,$$

where $t = 3q^2 + 4q + 1$.

So, in any case, $a = 3m$ or $a = 3m + 1$ for some integer m.

1.2 Divisibility

Definition: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b **divides** a if $a = bc$ for some integer c.

We also say that b is a **divisor** or **factor** of a.

We denote "b divides a" using the symbols $b|a$, and "b doesn't divide a" is denoted by $b \nmid a$.

For example, 4 divides 20 since $20 = (4)(5)$, and -7 divides 35 since $35 = (-7)(-5)$ (negative divisors are allowed).

Also, every nonzero b divides 0 since $0 = b \cdot 0$, and for every integer a, 1 divides a since $a = 1 \cdot a$.

Remarks:

(i) If $b|a$, then $a = bc$ for some $c \in \mathbb{Z}$. This implies that

$$-a = b(-c),$$

so $b| - a$. Similarly, we can show that an integer that divides $-a$ also divides a, so $b|a$ if and only if $b| - a$. This implies that a and $-a$ have the same divisors.

(ii) If $a \neq 0$ and $b|a$, then $b = ac$, so $|a| = |bc| = |b||c|$, which implies that $|b|||a|$. Since a, b, c are all nonzero integers, this implies that $0 < |b| \leq |a|$, i.e. $-|a| \leq b \leq |a|$. This implies the following two facts:

(a) every divisor of a nonzero integer a is $\leq |a|$.

(b) a nonzero integer a has only finitely many divisors, since there are only finitely many integers between $-a$ and a.

Now, for two integers n and m, suppose that another integer b divides both n and m, that is $b|n$ and $b|m$. Then, we say that b is a **common divisor** of n and m.

For example, 7 is a common divisor of 42 and 56. Of course, for any two integers n and m, there is a largest integer d that divides both n and m, and we call this the greatest common divisor.

Here is the formal definition:

Definition: Let a and b both be integers, not both 0. The **greatest common divisor (gcd)** of a and b is the largest integer d that divides both a and b. So, the gcd d of a and b satisfies two conditions:

(1) $d|a$ and $d|b$,

(2) If $c|a$ and $c|b$, then $c \leq d$.

We usually denote the gcd of a and b by (a, b).

Earlier, we showed that every integer has only a finite number of divisors. So, for any $a, b \in \mathbb{Z}$, not both 0, then their gcd exists and is unique, since we can just look at the finite list of integers that divide both a and b and pick the unique largest one. Also, since 1 divides every integer, we know that for any $a, b \in \mathbb{Z}$,

$$(a, b) \geq 1.$$

Examples:

1. $(12, 8) = 4$,

2. $(66, -121) = 11$

3. $(49, 32) = 1$.

The last example is special: when the gcd of two integers is 1, we say that they are **relatively prime.**

4. $(a, 0) = a$.

If we consider the integers 12 and 30, we'll see that $6 = (12, 30)$. Notice that

$$6 = 12(-2) + 30(1) = 12(8) + 30(-3).$$

We can write 6 as a **linear combination** of 12 and 30, i.e. there exist integers u and v such that

$$6 = 12u + 30v.$$

This is possible for any gcd:

Theorem: Let $a, b \in \mathbb{Z}$, not both 0, and let $d = (a, b)$. Then, there exist (not necessarily unique) integers u and v such that $d = au + bv$.

Notice that this is *not* and "if and only if statement." The theorem says:

$$\text{If } d = (a, b), \text{ then there exist } u, v \in \mathbb{Z} \text{ s.t } d = au + bv.$$

It does **not** say that

$$\text{If there are } u, v \in \mathbb{Z} \text{ s.t. } d = au + bv, \text{ then } d = (a, b).$$

This direction is in fact **false**. For example, we know that the gcd of 8 and 7 is 1. **However**, we can write

$$3 = 3 \cdot 8 - 3 \cdot 7.$$

So we can write 3 as a linear combination using 8 and 7 even though $(8, 7) = 1$.

Here's a Corollary:

Corollary 1.3: Let $a, b \in \mathbb{Z}$, not both 0, and let $d \in \mathbb{Z}_{>0}$. Then, $d = (a, b)$ if and only if d satisfies:

(i) $d|a$ and $d|b$,

(ii) if $c|a$ and $c|b$, then $c|d$.

Proof:

This is an "if and only if" proof, so we have to prove both directions:

"$\Rightarrow$:" If $d = (a, b)$, then d satisfies (i) and (ii).

d satisfies (i) by definition of gcd. We proved the second condition in the proof of Theorem 1.2, but we'll show it again: by Theorem 1.2, there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. If c divides both a and b, then there are $k, s \in \mathbb{Z}$ with $a = ck, b = cs$, so that

$$d = au + bv = (ck)u + (cs)v = c(ku + sv).$$

So, $c|d$.

This proves the $\Rightarrow$ direction.

"$\Leftarrow$:" If d satisfies (i) and (ii), then $d = (a, b)$.

We just need to show that $c \leq d$. Well, by (ii), $c|d$, so $c \leq |d|$, but we're assuming that d is positive, so $c \leq d$. This shows that d satisfies the two conditions for being the gcd, so $d = (a, b)$.

This proves the $\Leftarrow$ direction, so we are now done. $\square$

There is actually one case in which this theorem is an "if and only if:"

Let $a, b \in \mathbb{Z}$, not both 0. Then, $(a, b) = 1$ if and only if there exist (not necessarily unique) integers u and v such that $au + bv = 1$.

Proof: The "$\Rightarrow$"direction is just the previous theorem. Now, we show the other direction:

"$\Leftarrow$" Suppose $au + bv = 1$, and let $d = (a, b)$. Then, $d|a$ and $d|b$, so $a = dp$ and $b = dq$ for some integers p and q. We substitue these into our equation:

$$1 = (dp)u + (dq)v = d(pu + qv).$$

This tells us that $d|1$, so $d \leq 1$. Since $d \leq 1$ and $1 \leq d$, this implies that $d = 1$. $\square$

Question: If $a|bc$ does $a|b$ or $a|c$? The answer is not always yes, since $6|24 = (8)(3)$ but $6 \not| 8$ and $6 \not| 3$.

Here is one case in which the answer to this question is "yes:"

Theorem 1.4: If $a|bc$ and $(a, b) = 1$, then $a|c$.

Proof: Since $(a, b) = 1$, there exist $u, v \in \mathbb{Z}$ such that $1 = au + bv$. This implies that

$$c = c(1) = c(au + bv) = a(uc) + (bc)v.$$

Since $a|bc$, there exists $q \in \mathbb{Z}$ such that $bc = aq$, so

$$c = a(uc) + (bc)v = a(uc) + aqv = a(uc + qv).$$

This shows that $a|c$. $\square$

1.2.1 The Euclidean Algorithm

The Euclidean Algorithm gives us a way to find the gcd of two integers a and b. To do this, we will prove a few facts (this is problem 1.2.13 in the book)

Let $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$.

1. Suppose c is a common divisor of a and b. Then, $c|r$.

Proof: There exist $s, t \in \mathbb{Z}$ such that $a = cs$ and $b = ct$. Then,

$$r = a - bq = cs - (ct)q = c(s - tq) \Rightarrow c|r.$$

2. Every common divisor of b and r is also a common divisor of a and b.

This is clear, for if $c|b$ and $c|r$, then $c|(bq + r)$, i.e. $c|a$.

3. $(a, b) = (b, r)$

Let $d_1 = (a, b)$ and $d_2 = (b, r)$. Then, d_1 is a common divisor of a and b. By (1), d_1 is also a common divisor of b and r. By definition of gcd, this implies that $d_1|d_2$. Similarly, by (2), since d_2 is a common divisor of b and r, it is a common divisor of a and b, hence $d_2|d_1$. Since d_1 and d_2 divide each other and are positive, $d_1 = d_2$.

Now, we can establish the Euclidean Algorithm. For example, let's find $(330, 156)$. By the Division Algorithm,

$$330 = 156 \cdot 2 + 18.$$

Here the remainder is 18. By our work above, we get

$$(330, 156) = (156, 18).$$

We have simplified the problem because now we want to find the gcd of smaller numbers. We continue:

$$156 = 18 \cdot 8 + 12,$$

so

$$(330, 156) = (156, 18) = (18, 12),$$

$$18 = 12 \cdot 1 + 6$$

$$\Rightarrow (330, 156) = (156, 18) = (18, 12) = (12, 6)$$

$$12 = 6 \cdot 2 + 0,$$

$$\Rightarrow (330, 156) = (156, 18) = (18, 12) = (12, 6) = (6, 0) = 6.$$

After a certain number of steps, you'll end up with $(d, 0)$, then $d = (a, b)$.

We can perform this in reverse to write 6 as a linear combination of 330 and 156:

$$6 = 18 - 1 \cdot 12$$

Replace 12 with $156 - 8 \cdot 18$:

$$6 = 18 - 1 \cdot (156 - 8 \cdot 18) = 18 - 156 + 8 \cdot 18 = 9 \cdot 18 - 156.$$

Lastly, replace the 18 with $330 - 156 \cdot 2$:

$$6 = 9 \cdot (330 - 2 \cdot 156) - 156 = 9 \cdot 330 - 18 \cdot 156 - 156 = 9 \cdot 330 - 19 \cdot 156.$$

Another Example: Find $(1003, 456)$ and express this value as a linear combination of 1003 and 456.

$$1003 = 2 \cdot 456 + 91$$

$$456 = 5 \cdot 91 + 1$$

$$1 = 91 \cdot 1 + 0,$$

$$\Rightarrow (1003, 456) = 1.$$

$$1 = 456 - 5 \cdot 91$$

$$= 456 - 5 \cdot (1003 - 2 \cdot 456)$$

$$= 11 \cdot 456 - 5 \cdot 1003.$$

1.3 Primes and Unique Factorization

Note that every nonzero n except for ± 1 has at least four divisors: ± 1 and $\pm n$. Integers n that have only these four divisors are super important:

Definition: An integer p is called **prime** if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

Here are two easy facts:

(1) p is prime if and only if $-p$ is prime,

(2) if p, q are prime and $p|q$, then $p = \pm q$.

Theorem 1.5: Let p be an integer with $p \neq 0, \pm 1$. Then, p is prime if and only if p has the following property: whenever $p|bc$, then $p|b$ or $p|c$.

Proof: Another if and only if proof, so we need to prove both directions.

(1) "$\Rightarrow$:" If p is prime, then whenever $p|bc$, then $p|b$ or $p|c$.

Let's consider the gcd of p and b. (p, b) must be a positive divisor of p, so $(p, b) = 1$ or $\pm p$ (depending on whether p is positive or negative).

If $(p, b) = 1$, then by Theorem 1.4, $p|c$.

If $(p, b) = \pm p$, then by definition $p|b$. So, $p|c$ or $p|b$.

(2) "$\Leftarrow$:" If p has that property that whenever $p|bc$, then $p|b$ or $p|c$, then p is prime.

Let a be a divisor of p, so there's a $q \in \mathbb{Z}$ such that $p = aq$. Then, p divides aq so by assumption, p divides a or p divides q. If $p|a$, then $a = pk$, so $p = akp$, which means $ak = 1$, so $k = \pm 1$, so $a = \pm p$. If $p|q$, then $q = bp$, so $p = abp$, which implies that $ab = 1$, so $a = \pm 1$.

So, $a = \pm 1$ or $\pm p$. This implies that p is prime. $\square$

Corollary 1.6: If p is prime and $p|a_1 a_2 \cdots a_n$, then p divides at least one of the a_i.

Proof: Apply Theorem 1.5 to $b = a_1, c = a_2 a_3 \cdots a_n$. If $a|b$, then we're done. If $p|c$, then repeat this with $b = a_2, c = a_3 a_4 \cdots a_n$. Continue in this way until p divides an a_i. This process will terminate, since the final step is $b = a_{n-1}, c = a_n$.

Example: If p is prime and $p|a^n$, then $p^n|a^n$. Why?

We'll use this corollary and set each $a_i = a$ for each i. Then, the corollary tells us that

$p|a$, so $a = pk$ for some integer k. This implies that

$$a^n = (pk)^n = p^n k^n = p^n q,$$

where $q = k^n \in \mathbb{Z}$. Thus, $p^n|a^n$.

The next theorem will show us that we can write any nonzero integer besides ± 1 can be written as a product of primes:

Theorem 1.7: Every integer n except $0, \pm 1$ is a product of primes.

Proof (not in class): We can assume that $n > 1$, because if $n = p_1 p_2 \cdots p_k$ is a product of primes, then $-n = (-p_1)p_2 \cdots p_k$ is also a product of primes.

Let S be the set of all integers greater than 1 that are *not* a product of primes. Our goal is to show that $S = \emptyset$.

We will prove this by contradiction. So, assume that S is nonempty. S is a subset of the positive integers, so we can use the Well-Ordering Axiom here: Let a be the smallest element of S.

If a is not a product of primes, then it cannot be prime, so it has a positive divisor b with $b \neq 1, a$. So, $a = bq$, with q positive. By the remark in section 1.2, $b, q < a$. The inequality is strict because we're assuming that $b \neq 1$ or p. Also, b and q cannot both be products of primes, because then a would be a product of primes. So, $b, q \in S$ and $b, q < S$, but this is a contradiction. $\square$

We showed that every integer can be written as a product of primes, but now we will show that every integer can be written *uniquely* as a product of primes, up to some negative signs:

Theorem 1.8 (The Fundamental Theorem of Arithmetic): Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: If

$$n = p_1 p_2 \cdots p_r, \quad \text{and} \quad n = q_1 q_2 \cdots q_s$$

with each p_i, q_j prime, then $r = s$ (that is, the number of factors are the same) and after possibly reordering and relabeling the q's,

$$p_1 = \pm q_1, p_2 = \pm q_2, p_3 = \pm q_3, \ldots, p_r = \pm q_r.$$

Proof: By Theorem 1.7, every integer (besides 0, ± 1) has at least one prime factorization. Now, suppose that n has two prime factorizations:

$$n = p_1 p_2 \cdots p_r, \quad \text{and} \quad n = q_1 q_2 \cdots q_s,$$

so

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

which implies that $p_1 | q_1 q_2 \cdots q_s$.

Since p_1 is prime, then by Corollary 1.6, p_1 divides some q_i. By relabelling if needed, we can just assume that p_1 divides q_1. Since p_1 and q_1 are prime and $p_1 | q_1$, then we know that $p_1 = \pm q_1$. This implies that

$$\pm q_1 p_2 \cdots p_r = q_1 \cdots q_s,$$

so

$$\pm p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

This implies that $p_2 | q_2 q_3 \cdots q_s$. Then, again by Corollary 1.6, p_2 divides a q_i, which we can assume is q_2, so $p_2 = \pm q_2$.

We can continue in this way. If $r = s$, then we'll get $p_i = \pm q_i$.

If $r < s$, then we'll have

$$1 = q_{r+1} \cdots q_s.$$

This implies that $q_s | 1$, so $q_s = \pm 1$, but q_s is prime, so $q_s \neq 1$. Thus, this is impossible.

A very similar argument works for the $r > s$ case. Therefore, $r = s$. $\square$

Corollary 1.9: Every integer $n > 1$ can be written in one and only one way in the form $n = p_1 p_2 p_3 \cdots p_r$, where the p_i are positive primes such that $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_r$. (Use this for Fundamental Theorem of Arithmetic)

Example: If $c^2 = ab$ and $(a, b) = 1$, prove that a and b are perfect squares.

Proof: By the Fundamental Theorem of arithmetic, $c = p_1 p_2 \cdots p_r$ for primes $p_1 \leq p_2 \leq \ldots p_2$. This tells us that

$$p_1^2 p_2^2 \cdots p_r^2 = ab.$$

By the fundamental theorem of arithmetic,

$$a = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_r^{\epsilon_r},$$

where each $\epsilon_i \in \{0, 1, 2\}$. We want to show that each $\epsilon_i \in \{0, 2\}$.

In particular, this tells us that $p_1 | ab$. Since p_1 is prime, $p_1 | a$ or $p_1 | b$. Let's assume without loss of generality that $p_1 | a$, so $a = p_1 k$ for some $k \in \mathbb{Z}$. We also have $p_1^2 | ab$, so

$$ab = (p_1 k) b = p_1^2 q.$$

Cancel p_1 on both sides to get

$$p_1 q = kb,$$

and now we have $p_1 | kb$. Again, since p_1 is prime, $p_1 |$

1.3.1 Primality Testing

Theorem 1.10: Let $n > 1$. If n has no positive prime factor less than or equal to $\sqrt{n}$, then n is prime.

Proof: Suppose that n is not prime. Then, n has at least two prime factors p_1 and p_2, so that $n = p_1 p_2 k$ for some integer k. By hypothesis, n has no positive prime divisors $\leq \sqrt{n}$. So, $p_1 > \sqrt{n}$ and $p_2 > \sqrt{n}$. Therefore,

$$n = p_1 p_2 k \geq p_1 p_2 > \sqrt{n}\sqrt{n} = n,$$

so $n > n$, which is a contradiction.□

Before moving onto the next chapter, let's prove the Division Algorithm:

Proof of Division Algorithm: Let a, b be fixed integers with $b > 0$. Let S be the set

$$S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}.$$

x may be positive, negative, or 0, but $a - bx$ must be ≥ 0.

First, we're going to show that S is nonempty. Let $x = -|a|$. We want to show that $a + b|a| \in S$, that is $a + b|a| \geq 0$.

Indeed, since b is a positive integer, we have

$$b \geq 1.$$

Multiply both sides by $|a|$:

$$|a|b \geq |a| \geq -a.$$

The second inequality follows since $|a| \geq -a$ always. This implies that

$$|a|b + a \geq 0.$$

This implies that $a + b|a| \in S$, so S is nonempty.

Next step: find q and r such that $a = bq + r$ and $r \geq 0$.

We showed that S is nonempty, and by definition it consists of nonnegative integers. So, we can use the Well-Ordering Axiom to say that S has a smallest element. Let's call this element r.

So, $r \geq 0$ and $r = a - bx$ for some x, and let's rename this integer q, so $r = a - bq$, i.e. $a = bq + r$.

Next Step: Show that $r < b$.

On the contrary: suppose that $r \geq b$, i.e. $r - b \geq 0$. Then,

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

This shows us that $r - b = a - b(q + 1) \in S$.

However, $b \geq 1$, so $r - b < r$, but r is the minimal element of S. This is a contradiction, so it must be that $r < b$.

We have now show the *existence* part of the theorem, that is, we have shown that there exist q, r with $0 \leq r < b$ and $a = bq + r$.

Now, we want to show that these integers are *unique.*

So, suppose that there are other integers q_1, r_1 such that

$$a = bq_1 + r_1$$

and $r_1 < b$. We want to show that $r_1 = r$ and $b_1 = b$.

Since $a = bq + r$ and $a = bq_1 + r_1$, we have

$$bq + r = bq_1 + r_1,$$

so

$$b(q - q_1) = r_1 - r.$$

Since $0 \leq r < b$ and $0 \leq r_1 < b$, we have $-b < -r \leq 0$, so

$$-b < r_1 - r < b.$$

We can replace the middle term with

$$-b < b(q - q_1) < b,$$

which implies that

$$-1 < q - q_1 < 1.$$

Since $q - q_1 \in \mathbb{Z}$, this means that $q - q_1 = 0$, so $q = q_1$, which further implies that $r = r_1$.

We have proved existence and uniqueness, so we are done. $\square$.

2 Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

Definition: Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then a is **congruent to** b **modulo** n provided that n divides $a - b$.

We denote this by $a \equiv b(\mod n)$.

If n divides $a-b$, then there's some integer k such that $a-b = nk$, so if $a \equiv b \mod n$,then there's a $k \in \mathbb{Z}$ such that $a = b + nk$.

Examples:

(1) $5 \equiv 3(mod 2)$, since 2 divides $5 - 3 = 2$,

(2) $6 \equiv -2(\mod 4)$, since 4 divides $6 - (-2) = 8$.

Theorem 2.1: Let $n \in \mathbb{Z}_{>0}$. Congruence modulo n has the following properties:

(1) Reflexive: $a \equiv a(\mod n)$ for all $a \in \mathbb{Z}$,

(2) Symmetric: If $a \equiv b(\mod n)$, then $b \equiv a(\mod n)$ for all $a, b \in \mathbb{Z}$,

(3) Transitive: If $a \equiv b(\mod n)$ and $b \equiv c(\mod n)$, then $a \equiv c(mod n)$.

Proof:

(1) Clearly, n divides $0 = a - a$.

(2) If $a \equiv b(\mod n)$, then $n|a-b$, so $a - b = nk$ for some $k \in \mathbb{Z}$. Then,

$$b - a = -(a - b) = -nk = n(-k),$$

so $n|b-a$, which implies $b \equiv a(\mod n)$.

(3) $n|a-b$ and $n|b-c$, so there are k_1, k_2 such that $a - b = nk_1$ and $b - c = nk_2$. This implies that

$$a - c = (a - b) + (b - c) = nk_1 + nk_2 = n(k_1 + k_2).$$

Thus, $n|a-c$, so $a \equiv c(\mod n)$. $\square$

The following theorem shows us that some of the usual properties of regular addition and multiplication apply to congruence modulo n.

Theorem 2.2: If $a \equiv b(\mod n)$ and $c \equiv d(\mod n)$, then

(1) $a + c \equiv b + d(\mod n)$,

(2) $ac \equiv bd(\mod n)$.

Proof:

(a) There exists $k, t \in \mathbb{Z}$ such that $a - b = nk$ and $c - d = nt$, so

$$(a + c) - (b + d) = (a - b) + (c - d) = nk + nt = n(k + t),$$

so $n|[(a + c) - (b + d)]$, so $a + c \equiv b + d(\mod n)$.

(b) Again, there exists $k, t \in \mathbb{Z}$ such that $a - b = nk$ and $c - d = nt$, so

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = c(nk) + b(nt) = n(ck + bt).$$

So, $n|bd - ac$, so $ac \equiv bd(\mod n)$. $\square$

With congruence, we can create sets called congruence classes, that will allow us to perform arithmetic using congruence:

Definition: Let $a, n \in \mathbb{Z}$ with $n > 0$. The **congruence class of a modulo n**, denoted $[a]$, is the set of all integers that are congruent to a modulo n:

$$[a] = \{b : b \in \mathbb{Z}, b \equiv a(\mod n)\} = \{b : b = a + kn, k \in \mathbb{Z}\}.$$

Example:

In congruence modulo 5,

$$[7] = \{7 + 5k : k \in \mathbb{Z}\} = \{\ldots, -17, -12, -7, 0, 7, 12, 17 \ldots\}.$$

Note that this implies that $[7] = [12]$, so you can use different numbers to represent the same congruence class.

It's important to remember what modulus we're using, so sometimes we use $[\,]_n$ to denote that we're looking at a congruence class modulo n.

Theorem 2.3: $a \equiv c(\mod n)$ if and only if $[a] = [c]$.

Proof:

" $\Rightarrow$": If $a \equiv c(\mod n)$, then $[a] = [c]$.

Indeed, $a \equiv c(\mod n)$ implies that there's a $q \in \mathbb{Z}$ such that $a = c+qn$, which means

$$[a] = \{a + kn : k \in \mathbb{Z}\} = \{c + qn + kn : k \in \mathbb{Z}\} = \{c + n(q + k) : k \in \mathbb{Z}\}$$
$$= \{c + nm : m \in \mathbb{Z}\} = [c].$$

This proves one direction.

" $\Leftarrow$": If $[a] = [c]$, then $a \equiv c(\mod n)$.

If $[a] = [c]$, then $a \in [c]$, so $a = c + nk$ for some k, which means that n divides $a - c$, so $a \equiv c \mod n$.

One nice thing about congruence classes is that if there is any overlap between two classes, then the two classes must actually be the same:

Corollary: Two congruence classes modulo n are either disjoint or identical.

Proof: Suppose two classes $[a]$ and $[c]$ are not disjoint, so some integer $b \in [a] \cap [c]$. This implies that $b = a + nk = c + nq$ for some $k, q \in \mathbb{Z}$. This implies that $a = c + n(q - k)$, so $a \equiv c \mod n$, and by Theorem 2.3, this implies that $[a] = [c]$.

Corollary 2.5: Let $n > 1$ be an integer and consider congruence modulo n.

(1) If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.

(2) Ther are exactly n distinct congruence classes, namely $[0], [1], [2], \ldots, [n - 1]$.

Proof:

(1) If $a = nq+r$, then $a-r = nq$, so $a \equiv r \mod n$, and so by Theorem 2.3, $[a] = [r]$.

(2) Let a be any integer, and let r be its remainder when divided by n. By (1), $[a] = [r]$. By the division algorithm, $0 \leq r < n$, so $r \in \{0, 1, 2, \ldots, n - 1\}$. So, the only possible congruence classes are $[0], [1], \ldots, [n - 1]$, but we need to show that these classes are distinct.

Let s, t be distinct integers in the list $0, 1, 2, \ldots, n - 1$, and WLOG, assume that $s > t$. Then, $0 \leq s - t \leq n - 1$, so $n \not| s - t$, and by Theorem 2.3, $s \not\equiv t \mod n$. So, none of the classes $[0], [1], \ldots, [n - 1]$ are congruent modulo n, so they must all be distinct. $\square$

This set of congruence classes modulo n is denoted by $\mathbb{Z}_n$, which we read as "$\mathbb{Z}$ mod n." This corollary tells us that $\mathbb{Z}_n$ has exactly n elements.

And be careful: the elements of $\mathbb{Z}_n$ are *congruence classes*, not numbers.

2.2 Modular Arithmetic

Is there a way to define addition and multiplication on $\mathbb{Z}_n$?

Yes, but there's some nuance to this.

We're going to define addition $\oplus$ in $\mathbb{Z}_n$ by

$$[a] \oplus [c] = [a + c],$$

and we'll define multiplication $\odot$ in $\mathbb{Z}_n$ by

$$[a] \odot [c] = [ac].$$

For example, in $\mathbb{Z}_5$,

$$[2] \oplus [4] = [6] = [1].$$

However, note that $[2] = [7]$ and $[4] = [9]$. If we replace $[2]$ with $[7]$ and $[4]$ with $[9]$, will we get the same answer?

$$[7] \oplus [9] = [16] = [1].$$

The answer is "yes."

This brings up an important question? Are $\oplus$ and $\odot$ **well-defined?** What this means is: will we get the same answer for multiplication and addition if we use different representatives for our congruence classes?

We need to show that these operations in $\mathbb{Z}_n$ do not depend on our choice of representatives for the congruence classes we're using. This is exactly what it means to show that the operations are **well-defined.** The following theorem shows this:

Theorem 2.6: If $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$, then

$$[a + c] = [b + d], \quad [ac] = [bd].$$

Proof: $[a] = [b]$ means that $a \equiv b \mod n$ and $[c] = [d]$ means that $c \equiv d \mod n$. This implies that

$$a + c \equiv b + d \mod n, \quad ac = \equiv bd \mod n.$$

So,

$$[a + c] = [b + d], \quad [ac] = [bd],$$

by Theorem 2.3. □

Here are the addition and multiplication tables for $\mathbb{Z}_5$:

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

2.2.1 Properties of Modular Arithmetic

We are now going to prove properties about modular arithmetic that are analogues of basic properties of arithmetic in $\mathbb{Z}$:

Theorem 2.7: For any classes $[a], [b], [c] \in \mathbb{Z}_n$,

1. If $[a], [b] \in \mathbb{Z}_n$, then $[a] \oplus [b] \in \mathbb{Z}_n$ (closure under addition),

2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$ (addition is associative),

3. $[a] \oplus [b] = [b] \oplus [a]$ (addition is commutative)

4. $[a] \oplus [0] = [a] = [0] \oplus [a]$ ([0] is the additive identity)

5. For each $[a] \in \mathbb{Z}_n$, then equation $[a] \oplus X = [0]$ has a solution in $\mathbb{Z}_n$, (Additive Inverse)

6. If $[a], [b] \in \mathbb{Z}_n$, then $[a] \odot [b] \in \mathbb{Z}_n$ (closure under multiplication),

7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$ (multiplication is associative),

8. $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$, and

$([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ (distributive laws),

9.$[a] \odot [b] = [b] \odot [a]$ (multiplication is commutative),

10. $[a] \odot [1] = [a] = [1] \odot [a]$ (multiplicative identity)

Proof:

(1) and (6) are immediate by definition.

(2)

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b+c] = [a+(b+c)] = [(a+b)+c] = [a+b] \oplus [c] = ([a] \oplus [b]) \oplus [c].$$

Here, we used the fact that addition in $\mathbb{Z}$ is associative.

(3)

$$[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$$

(4)

$$[a] \oplus [0] = [a+0] = [a] = [0+a] = [0] \oplus [a].$$

(5) $X = [a]$ is a solution:

$$[a] \oplus [-a] = [a+(-a)] = [0].$$

(7)

$$[a] \odot ([b] \odot [c]) = [a] \odot [bc] = [a(bc)] = [(ab)c] = ([a] \odot [b]) \odot [c].$$

(8)

$$[a] \odot ([b] \oplus [c]) = [a] \odot [b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] = [a] \odot [b] \oplus [a] \odot [b].$$

(9)

$$[a] \odot [b] = [ab] = [ba] = [b] \odot [a].$$

(10)

$$[a] \odot [1] = [a(1)] = [a] = [(1)a] = [1] \odot [a].$$

2.2.2 Exponents and Equations

If $[a] \in \mathbb{Z}_n$, then

$$[a]^k = [a] \odot [a] \odot \cdots \odot [a], \quad (k \text{ factors}).$$

We can solve equations in $\mathbb{Z}_n$. For small n, you can just plug in values since there are only a small number to check.

For instance ,the zeros of $x^2 \oplus [5] \odot x = [0]$ in $\mathbb{Z}_6$ are $x = [0], [1], [3], [4]$. Notice that this is a quadratic polynomial with 4 zeros. In $\mathbb{Z}$, this is not possible, but in $\mathbb{Z}_n$, it sometimes is.

2.3 The Structure of $\mathbb{Z}_p$ (p prime) and $\mathbb{Z}_n$

Now, we're going to drop the circles and brackets in our notation for modular arithmetic in $\mathbb{Z}_n$, so instead of writing $[5]+[1]=[6]=[0]$ in $\mathbb{Z}_6$, we're just going to write $5+1=6=0$.

We'll go back to the old notation if they're needed.

Note: Exponents are still just regular-old integers, so do not reduce them as well. In $\mathbb{Z}_5$,$2^5=32=2$, and $2^0=1$, so $2^5\neq 2^0$ even the $5=0$ in $\mathbb{Z}_5$.

2.3.1 The Structure of $\mathbb{Z}_p$ When p Is Prime

When n is not prime, $\mathbb{Z}_n$ has some interesting properties that it doesn't share with $\mathbb{Z}$.

For example, in $\mathbb{Z}_6$, $3\cdot 2=0$. In $\mathbb{Z}$, you can't multiply two nonzero integers together and get a product of 0.

However, when p is prime, $\mathbb{Z}_p$ has some nice special properties:

Theorem 2.8: If $p>1$ is an integer, then the following conditions are equivalent:

(1) p is prime,

(2) For any $a\neq 0$ in $\mathbb{Z}_p$, the equation $ax=1$ has a solution in $\mathbb{Z}_p$,

(3) Whatever $bc=0$ in $\mathbb{Z}_p$, then $b=0$ or $c=0$.

Proof:

(1) $\Rightarrow$ (2): Suppose p is prime and $[a]\neq[0]$ in $\mathbb{Z}_p$. This means that $a\not\equiv 0 \mod p$ in $\mathbb{Z}$. So, $p\not| a$. Is this is the case, then the gcd of p and a is $(a,p)=1$, since the only divisors of p are 1 and p, and p is not a divisor of a.

So, there exist integers u and v such that

$$1=au+pv,$$

so

$$au=1-pv,$$

so $au\equiv 1 \mod p$, hence $[au]=[a][u]=[1]$ in $\mathbb{Z}_p$, so $x=[u]$ is a solution to $[a]x=[1]$.

(2) $\Rightarrow$ (3)

Suppose $bc=0$ in $\mathbb{Z}_p$. If $b=0$, then we're done. So, suppose that $b\neq 0$. Then, by (2), there exists $u\in\mathbb{Z}_p$ such that $bu=1$. Then,

$$0=u\cdot 0=u(bc)=(ub)c=1\cdot c=c,$$

so c must be 0. So, either $b = 0$ or $c = 0$.

(3) $\Rightarrow$ (1) Suppose that $a|p$. Then $p = ab$ for some $b \in \mathbb{Z}$. Then, $[p] = [ab] = [a][b] = [0]$ in $\mathbb{Z}_p$. By (3) $[a] = [0]$ or $[b] = [0]$. This implies that $a \equiv 0 \mod p$ or $b \equiv 0 \mod p$. This means that $p|a$ or $p|b$, which means that p is prime by Theorem 1.5.

2.3.2 The Structure of $\mathbb{Z}_n$

Theorem 2.9: Let $a, n \in \mathbb{Z}$ with $n > 1$. Then, the equation $[a]x = [1]$ has a solution in $\mathbb{Z}_p$ if and only if $(a, n) = 1$ in $\mathbb{Z}$.

Proof: Another "if and only if" statement:

(1) " $\Rightarrow$" if $[a]x = [1]$ has a solution in $\mathbb{Z}_n$, then $(a, n) = 1$ in $\mathbb{Z}$.

If $[a]x = [1]$ has a solution in $\mathbb{Z}_n$, then there's some $[m] \in \mathbb{Z}$ such that $[a][m] = [1]$, which means that

$$[am] = [1].$$

Recall that this implies

$$am \equiv 1 \mod n,$$

so there's some $k \in \mathbb{Z}$ with $am = 1 + kn$, i.e. $am + (-k)n = 1$.

Let $d = (a, n)$. d is a common divisor of a and n, so there are $r, s \in \mathbb{Z}$ such that $a = dr$ and $n = ds$, so

$$am + (-k)n = 1$$

$$(dr)m + (-k)(ds) = 1$$

$$d(rm - ks) = 1.$$

So, $d|1$. Since d is positive by definition, we have $d = 1$, so $(a, n) = 1$. This proves the first direction of the proof.

(2) " $\Leftarrow$" If $(a, n) = 1$ in $\mathbb{Z}$, then $[a]x = [1]$ has a solution in $\mathbb{Z}_n$.

This direction is easier. If $(a, n) = 1$, then there exist $u, v \in \mathbb{Z}$ such that $au + nv = 1$, and after rearranging we have

$$au = 1 - nv,$$

so $au \equiv 1 mod n$, that is $[au] = [a][u] = [1]$ in $\mathbb{Z}_n$, so $x = [u]$ is a solution. $\square$

2.3.3 Units and Zero Divisors

An element $a \in \mathbb{Z}_n$ is called a **unit** if the equation $ax = 1$ has a solution. That is, a is a unit if there's some $u \in \mathbb{Z}_n$ such that $au = 1$. Here, we call u the **inverse** of a. We sometimes denote the inverse of a by a^{-1}.

In $\mathbb{Z}_{13}$, 2 and 7 are units, since $2 \cdot 7 = 14 = 1$ in $\mathbb{Z}_{13}$. So, we say that 7 is the inverse of 2 (and vice-versa).

Notice that part (b) in Theorem 2.8 implies that every nonzero element of $\mathbb{Z}_p$ is a unit when p is prime.

We can restate the previous theorem using the terminology of units:

Theorem 2.10: Let $a, n \in \mathbb{Z}$ with $n > 1$. Then $[a]$ is a unit in $\mathbb{Z}_n$ if and only if $(a, n) = 1$ in $\mathbb{Z}$.

A nonzero element $a \in \mathbb{Z}_n$ is called a **zero divisor** if the equation $ax = 0$ has a *nonzero* solution, i.e. there's a $c \in \mathbb{Z}_n$ with $ac = 0$.

For example, 2 and 3 are zero divisors in $\mathbb{Z}_6$ since $2 \cdot 3 = 6 = 0$.

Note that part 3 of Theorem 2.8 says that $\mathbb{Z}_p$ has no zero divisors when p is prime. Why is that? Let's write the proposition "$\mathbb{Z}_n$ has zero divisors" as a quantified proposition: "there exist nonzero $a, c \in \mathbb{Z}_n$ such that $ac = 0$," or

$$\exists 0 \neq a, c \in \mathbb{Z}_n, ac = 0,$$

If we negate this, i.e. saying $\mathbb{Z}_n$ has no zero divisors, then we get

$$\forall 0 \neq a, c \in \mathbb{Z}_n, ac \neq 0.$$

So, if we have $ac = 0$, then we must have either $a = 0$ or $c = 0$.