The purpose of this document is to introduce modular arithmetic along with some of the standard problems for which it provides elegant solutions.

1 $\mathbb{Z}$-Basics

Let's start at the very beginning, it is a good place to start.

Definition 1.1. *The integers $\mathbb{Z}$ are the set of natural numbers $\mathbb{N}$ together with 0 and the negatives of $\mathbb{N}$. It is possible to concretely construct (we will not) these from sets and set-operations.*

From the construction of $\mathbb{Z}$ it is clear (we assume these to be true)

1. the sum of integers is an integer
2. the product of integers is an integer
3. the usual rules of arithmetic hold for $\mathbb{Z}$

Much is hidden in (3.): let me elaborate, we assume for all $a, b, c \in \mathbb{Z}$,

$$\begin{aligned} a + b &= b + a \\ ab &= ba \\ a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \\ (a + b) + c &= a + (b + c) \\ (ab)c &= a(bc) \\ a + 0 &= 0 + a = a \\ 1a &= a1. \end{aligned}$$

Where we assume the **order of operations** is done multiplication then addition; so, for example, $ab + ac$ means to first multiply a with b and a with c then you add the result.

Let me comment briefly about our standard conventions for the presentation of numbers. If I write 123 then we understand this is the **base-ten** representation. In particular,

$$123 = 1 \times 10^2 + 2 \times 10 + 3.$$

On the other hand, $1 \cdot 2 \cdot 3$ denotes the product of $1, 2$ and 3 and $1 \cdot 2 \cdot 3 = 6$. By default, algebraic variables juxtaposed denote multiplication; xy denotes x multiplied by y. If we wish for symbolic variables to denote digits in a number then we must explain this explicitly. For example, to study all numbers between 990 and 999 I could analyze $99x$ where $x \in \{0, 1, \ldots, 9\}$. But, to be clear I ought to preface such analysis by a statement like: let $99x$ be the base-ten representation of a number where x represents the 1's digit.

2 division algorithm

Division is repeated subtraction. For example, consider 11/3. Notice repeated subtraction of the dividing number[1] 3 gives:

$$11-3=8 \qquad 8-3=5 \qquad 5-3=2$$

then we cannot subtract anymore. We were able to subtract 3 copies of 3 from 11. Then we stopped at 2 since $2<3$. To summarize,

$$\boxed{11=3(3)+2}$$

We say 2 is the **remainder**; the remainder is the part which is too small to subtract for the given *dividing number*. Divide the boxed equation by the divisor to see:

$$\frac{11}{3}=3+\frac{2}{3}.$$

The generalization of the boxed equation for an arbitrary pair of natural numbers is known as the **division algorithm**.

Theorem 2.1. positive division algorithm: *If $a,b\in\mathbb{Z}$ with $b>0$ then there is a unique quotient $q\in\mathbb{Z}$ and remainder $r\in\mathbb{Z}$ for which $a=qb+r$ and $0\leq r<b$.*

Proof (existence): suppose $a,b\in\mathbb{Z}$ and $b>0$. Construct $R=\{a-nb\,|\,q\in\mathbb{Z},\ \ a-nb\geq 0\}$. The set R comprises all non-negative integers which are reached from a by integer multiples of b. Explicitly,

$$R=\{a,a\pm b,a\pm 2b,\dots\}\cap\{0,1,2,\dots\}.$$

To prove R is non-empty we consider $n=-|a|\in\mathbb{Z}$ yields $a-nb=a+|a|b$. If $a\geq 0$ then clearly $a+|a|b\geq 0$. If $a<0$ then $|a|=-a$ hence $a+|a|b=-|a|+|a|b=|a|(b-1)$ but $b\in\mathbb{N}$ by assumption hence $b\geq 1$ and we find $a+|a|b\geq 0$. Therefore, as R is a non-empty subset of the non-negative integers. We apply the **Well-Ordering-Principle** to deduce there exists a smallest element $r\in R$.

Suppose r is the smallest element in R and $r\geq b$. In particular, $r=a-nb$ for some $n\in\mathbb{Z}$. Thus $a-nb\geq b$ hence $r'=a-(n+1)b\geq 0$ hence $r'\in R$ and $r'<r$. But $r'<r$ contradicts r being the smallest element. Thus, using proof by contradiction, we find $r<b$.

Proof (uniqueness): assume $q,q'\in\mathbb{Z}$ and $r,r'\in\mathbb{Z}$ such that $a=qb+r$ and $a=q'b+r'$ where $0\leq r,r'<b$. We have $qb+r=q'b+r'$ hence $(q-q')b=r-r'$. Suppose towards a contradiction $q\neq q'$. Since $q,q'\in\mathbb{Z}$ the inequality of q and q' implies $|q-q'|\geq 1$ and thus $|r-r'|=|(q-q')b|\geq|b|=b$. However, $r,r'\in[0,b)$ thus the distance[2] between r and

[1] my resident Chinese scholar tells me in Chinese a/b has the "dividing" number b and the "divided" number a. I am tempted to call b the divisor, but the term "divisor" has a precise meaning, if b is a divisor of a then $a=mb$ for some $n\in\mathbb{Z}$. In our current discussion, to say b is a divisor assumes the remainder is zero.

[2] for a non-geometric argument here: note $0\leq r<b$ and $0\leq r'<b$ imply $-r'<r-r'<b-r'\leq b$. But, $r'<b$ gives $-b<-r'$ hence $-b<r-r'<b$. Thus $|r-r'|<b$. Indeed, the distance between r and r' is less than b.

r' cannot be larger than or equal to b. This is a contradiction, therefore, $q = q'$. Finally, $qb + r = q'b + r'$ yields $r = r'$. $\square$

We can say more about q and r in the case $b > 0$. We have

$$\frac{a}{b} = q + \frac{r}{b} \qquad \& \qquad q = \lfloor a/b \rfloor$$

That is q is the greatest integer which is below a/b. The function $x \mapsto \lfloor x \rfloor$ is the **floor function**. For example,

$$\lfloor -0.4 \rfloor = -1, \qquad \lfloor \pi \rfloor = 3, \qquad \lfloor n + \varepsilon \rfloor = n$$

for all $n \in \mathbb{Z}$ provided $0 \leq \varepsilon < 1$. It is easy to calculate the floor function of x when x is presented in decimal form. For example,

$$\frac{324}{11} = 29.4545... \quad \Rightarrow \quad \frac{324}{11} = 29 + 0.4545... \quad \Rightarrow \quad 324 = 29(11) + (0.4545...)(11)$$

We can calculate, $0.4545 \cdot 11 = 4.9995$. From this we find

$$324 = 29(11) + 5$$

In other words, $\frac{324}{11} = 29 + \frac{5}{11}$. The decimal form of numbers and the floor function provides a simple way to find quotients and remainders.

Consider $456/(-10) = -45.6 = -45 - 0.6$ suggests $456 = (-10)(-45) + 6$. In the case of a negative divisor ($b < 0$) the division algorithm needs a bit of modification:

Theorem 2.2. nonzero division algorithm: *If $a, b \in \mathbb{Z}$ with $b \neq 0$ then there is a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ for which*

$$a = qb + r \qquad \& \qquad 0 \leq r < |b|.$$

Proof: Theorem 2.1 covers case $b > 0$. Thus, assume $b < 0$ hence $b' = -b > 0$. Apply Theorem 2.1 to $a, b' \in \mathbb{Z}$ to find q', r' such that $a = q'b' + r'$ with $0 \leq r' < b'$. However, $b' = -b = |b|$ as $b < 0$. Thus,

$$a = -q'b + r'$$

with $0 \leq r' < |b|$. Identify $q = -q'$ and $r = r'$ in the case $b < 0$. Uniqueness is clear from the equations which define q and r from the uniquely given q' and r'. This concludes the proof as $b \neq 0$ means either $b < 0$ or $b > 0$. $\square$

The selection of the quotient in the negative divisor case is given by the **ceiling** function $x \mapsto \lceil x \rceil$. The notation $\lceil x \rceil$ indicates the next integer which is greater than or equal to x. For example,

$$\lceil 456/(-10) \rceil = -45, \quad \lceil 3.7 \rceil = 4, \quad \lceil n - \varepsilon \rceil = n$$

for all $n \in \mathbb{Z}$ given $0 \leq \varepsilon < 1$.

Remark 2.3. The division algorithm proves an assertion of elementary school arithmetic. For example, consider the **improper fraction** $10/3$ we can write it as the sum of 3 and $1/3$. When you write $3\frac{1}{3}$ what is truly meant is $3+\frac{1}{3}$. In fact, the truth will set you free of a myriad of errors which arise from the poor notation $3\frac{1}{3}$. With this example in mind, let $a, b \in \mathbb{N}$. The division algorithm simply says for a/b there exists $q, r \in \mathbb{N} \cup \{0\}$ such that $a = qb + r$ hence $a/b = q + r/b$ where $0 \leq r < b$. This is merely the statement that any improper fraction can be reduced to the sum of a whole number and a proper fraction. In other words, you already knew the division algorithm. However, thinking of it without writing fractions is a bit of an adjustment for some of us.

3 divisibility

Consider $105 = 3 \cdot 5 \cdot 7$. We say 3 is a *factor* or *divisor* of 105. Also, we say 35 *divides* 105. Furthermore, 105 is a *multiple* of 3. Indeed, 105 is also a multiple of 5, 7 and even 21 or 35. Examples are nice, but, definitions are crucial:

Definition 3.1. *Let $a, b \in \mathbb{Z}$ then we say b* **divides** *a if there exists $c \in \mathbb{Z}$ such that $a = bc$. If b divides a then we also say b is a* **factor** *of a and a is a* **multiple** *of b.*

The notation $b \mid a$ means b divides a. If b is does not divide a then we write $b \nmid a$. The divisors of a given number are not unique. For example, $105 = 7(15) = (3)(35) = (-1)(-105)$. However, the prime divisors are unique up to reordering: $105 = (3)(5)(7)$. Much of number theory is centered around the study of primes. We ought to give a proper definition:

Definition 3.2. *If $p \in \mathbb{N}$ such that $n \mid p$ implies $n = p$ or $n = 1$ then we say p is* **prime***.*

In words: a prime is a positive integer whose only divisors are 1 and itself.

There are many interesting features of divisibility. Notice, every number $b \in \mathbb{Z}$ divides 0 as $0 = b \cdot 0$. Furthermore, $b \mid b$ for all $b \in \mathbb{Z}$ as $b = b \cdot 1$. In related news, 1 is a factor of every integer and every integer is a multiple of 1[3]

Proposition 3.3. *Let $a, b, c, d, m \in \mathbb{Z}$. Then,*

(i.) *if $a \mid b$ and $b \mid c$ then $a \mid c$,*

(ii.) *if $a \mid b$ and $c \mid d$ then $ac \mid bd$,*

(iii.) *if $m \neq 0$, then $ma \mid mb$ if and only if $a \mid b$*

(iv.) *if $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.*

[3]I should mention, I am partly following the excellent presentation of Jones and Jones *Elementary Number Theory* which I almost used as the text for Math 307 in Spring 2015. We're on page 4.

Proof (i.) : suppose $a \mid b$ and $b \mid c$. By the definition of divisibility there exist $m, n \in \mathbb{Z}$ such that $b = ma$ and $c = nb$. Hence $c = n(ma) = (nm)a$. Therefore, $c \mid a$ as $nm \in \mathbb{Z}$.

Proof (ii.) : suppose $a \mid b$ and $c \mid d$. By the definition of divisibility there exist $m, n \in \mathbb{Z}$ such that $b = ma$ and $d = nc$. Subsitution yields $bd = (ma)(nc) = mn(ac)$. But, $mn \in \mathbb{Z}$ hence we have shown $ac \mid bd$.

Proof (iii.) : left to the reader.

Proof (iv.) : if $d \mid a$ and $a \neq 0$ then $a = md$ for some $m \in \mathbb{Z}$. Suppose $m = 0$ then $a = (0)d = 0$ which contradicts $a \neq 0$. Therefore, $m \neq 0$. Recall that the absolute value function is multiplicative; $|md| = |m||d|$. As $m \neq 0$ we have $|m| \geq 1$ thus $|a| = |m||d| \geq |d|$. □

I hope you see these proofs are not too hard. You ought to be able to reproduce them without much effort.

Theorem 3.4. *Let $a_1, \ldots, a_k, c \in \mathbb{Z}$. Then,*

(i.) *if $c \mid a_i$ for $i = 1, \ldots, k$ then $c \mid (u_1a_1 + \cdots + u_ka_k)$ for all $u_1, \ldots, u_k \in \mathbb{Z}$,*

(ii.) *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof (i.): suppose $c \mid a_1, c \mid a_2, \ldots, c \mid a_k$. It follows there exist $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ such that $a_1 = cm_1$, $a_2 = cm_2$ and $a_k = cm_k$. Let $u_1, u_2, \ldots, u_k \in \mathbb{Z}$ and consider,

$$u_1a_1 + \cdots + u_ka_k = u_1(cm_1) + \cdots + u_k(cm_k) = c(u_1m_1 + \cdots + u_km_k).$$

Notice $u_1m_1 + \cdots + u_km_k \in \mathbb{Z}$ thus the equation above shows $c \mid (u_1a_1 + \cdots + u_ka_k)$.

Proof (ii.): suppose $a \mid b$ and $b \mid a$. If $a = 0$ then $a \mid b$ implies there exists $m \in \mathbb{Z}$ such that $b = m(0) = 0$ hence $b = 0$. Observe $a = \pm b = 0$. Continuing, we suppose $a \neq 0$ which implies $b \neq 0$ by the argument above. Notice $a \mid b$ and $b \mid a$ imply there exist $m, n \in \mathbb{Z} - \{0\}$ such that $a = mb$ and $b = na$. Multiply $a = mb$ by $n \neq 0$ to find $na = mnb$. But, $b = na$ hence $na = mn(na)$ which implies $1 = mn$. Thus, $m = n = 1$ or $m = n = -1$. These cases yield $a = b$ and $a = -b$ respective hence $a = \pm b$. □

The proof above is really not much more difficult than those we gave for Proposition 3.3. The most important case of the Theorem above is when $k = 2$ in part (i.).

Corollary 3.5. *If $c \mid x$ and $c \mid y$ then $c \mid (ax + by)$ for all $a, b \in \mathbb{Z}$.*

The result above is used repeatedly as we study the structure of common divisors.

Definition 3.6. *If $d \mid a$ and $d \mid b$ then d is a* **common divisor** *of a and b.*

Proposition 3.3 part (iv.) shows that a divisor cannot have a larger magnitude than its multiple. It follows that the largest a common divisor could be is $\max\{|a|, |b|\}$. Furthermore, 1 is a divisor of all nonzero integers. If both a and b are not zero then $\max\{|a|, |b|\} \geq 1$. Therefore, if both a and b are not zero then there must be a largest number between 1 and $\max\{|a|, |b|\}$ which divides both a and b. Thus, the definition to follow is reasonable:

Definition 3.7. *If $a, b \in \mathbb{Z}$, not both zero, then the* **greatest common divisor** *of a and b is denoted $gcd(a, b)$.*

The method to find the greatest common divisor which served me well as a child was simply to a and b in their prime factorization. Then to find the gcd I just selected all the primes which I could pair in both numbers.

Example 3.8.

$$gcd(105, 90) = gcd(\underline{3 \cdot 5} \cdot 7,\ 2 \cdot 3 \cdot \underline{3 \cdot 5}) = 3 \cdot 5 = 15.$$

The method above faces several difficulties as we attempt to solve non-elementary problems.

1. it is not an easy problem to find the prime factorization of a given integer. Indeed, this difficulty is one of the major motivations RSA cryptography.

2. it is not so easy to compare lists and select all the common pairs. Admittedly, this is not as serious a problem, but even with the simple example above I had to double-check.

Thankfully, there is a better method to find the gcd. It's old, but, popular. Euclid (yes, the same one with the parallel lines and all that) gave us the **Euclidean Algorithm**. We prove a Lemma towards developing Euclid's Algorithm.

Lemma 3.9. *Let $a, b, q, r \in \mathbb{Z}$. If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$.*

Proof: by Corollary 3.5 we see a divisor of both b and r is also a divisor of a. Likewise, as $r = a - qb$ we see any common divisor of a and b is also a divisor of r. It follows that a, b and b, r share the same divisors. Hence, $gcd(a, b) = gcd(b, r)$. □

We now work towards Euclid's Algorithm. Let $a, b \in \mathbb{Z}$, not both zero. Our goal is to calculate $gcd(a, b)$. If $a = 0$ and $b \neq 0$ then $gcd(a, b) = |b|$. Likewise, if $a \neq 0$ and $b = 0$ then $gcd(a, b) = |a|$. Note $gcd(a, a) = |a|$ hence we may asssume $a \neq b$ in what follows. Furthermore,

$$gcd(a, b) = gcd(-a, b) = gcd(a, -b) = gcd(-a, -b).$$

Therefore, suppose $a, b \in \mathbb{N}$ with $a > b$[4]. Apply the division algorithm (Theorem 2.1) to select q_1, r_1 such that

$$a = q_1 b + r_1 \qquad \text{such that} \qquad 0 \leq r_1 < b.$$

If $r_1 = 0$ then $a = q_1 b$ hence $b \mid a$ and as b is the largest divisor of b we find $gcd(a, b) = b$. If $r_1 \neq 0$ then we continue to apply the division algorithm once again to select q_2, r_2 such that

$$b = q_2 r_1 + r_2 \qquad \text{such that} \qquad 0 \leq r_2 < r_1.$$

If $r_2 = 0$ then $r_1 \mid b$ and clearly $gcd(b, r_1) = r_1$. However, as $a = q_1 b + r_1$ allows us to apply Lemma 3.9 to obtain $gcd(a, b) = gcd(b, r_1) = r_1$. Continuing, we suppose $r_2 \neq 0$ with $r_1 > r_2$ hence we may select q_3, r_3 for which:

$$r_1 = q_3 r_2 + r_3 \qquad \text{such that} \qquad 0 \leq r_3 < r_2.$$

[4]the equation above shows we can cover all other cases once we solve the problem for positive integers.

Once again, if $r_3 = 0$ then $r_2 \mid r_1$ hence it is clear $gcd(r_1, r_2) = r_2$. However, as $b = q_2 r_1 + r_2$ gives $gcd(b, r_1) = gcd(r_1, r_2)$ and $a = q_1 b + r_1$ gives $gcd(a, b) = gcd(b, r_1)$ we find that $gcd(a, b) = r_2$. This process continues. It cannot go on forever as we have the conditions:

$$0 < \cdots < r_3 < r_2 < r_1 < b.$$

There must exist some $n \in \mathbb{N}$ for which $r_{n+1} = 0$ yet $r_n \neq 0$. All together we have:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \ldots, \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

The last condition yields $r_n \mid r_{n-1}$ hence $gcd(r_{n-1}, r_n) = r_n$. Furthermore, we find, by repeated application of Lemma 3.9 the following string of equalities

$$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3) = \cdots = gcd(r_{n-1}, r_n) = r_{n-1}.$$

In summary, we have shown that repeated division of remainders into remainder gives a strictly decreasing sequence of positive integers whose last member is precisely $gcd(a, b)$.

Theorem 3.10. Euclidean Algorithm: *suppose $a, b \in \mathbb{N}$ with $a > b$ and form the finite sequence $\{b, r_1, r_2, \ldots, r_n\}$ for which $r_{n+1} = 0$ and $b, r_1, \ldots, r_n$ are defined as discussed above. Then $gcd(a, b) = r_n$.*

Example 3.11. *Let me show you how the euclidean algorithm works for a simple example. Consider $a = 100$ and $b = 44$. Euclid's algorithm will allow us to find $gcd(100, 44)$.*

1. $100 = 44(2) + 12$ *divided 100 by 44 got remainder of 12*
2. $44 = 12(3) + 8$ *divided 44 by 12 got remainder of 8*
3. $12 = 8(1) + \boxed{4}$ *divided 12 by 8 got remainder of 4*
4. $4 = 4(1) + 0$ *divided 4 by 1 got remainder of zero*

The last nonzero remainder will always be the gcd when you play the game we just played. Here we find $\boxed{gcd(100, 44) = 4}$. *Moreover, we can write 4 as a $\mathbb{Z}$-linear combination of 100 and 44. This can be gleaned from the calculations already presented by working backwards from the gcd:*

3. $4 = 12 - 8$
2. $8 = 44 - 12(3)$ *implies* $4 = 12 - (44 - 12(3)) = 4(12) - 44$
1. $12 = 100 - 44(2)$ *implies* $4 = 4(100 - 44(2)) - 44 = 4(100) - 9(44)$

I call this a "$\mathbb{Z}$-linear combination of 100 and 44 since $4, -9 \in \mathbb{Z}$. We find $\boxed{4(100) - 9(44) = 4}$.

The fact that we can always work euclid's algorithm backwards to find how the $gcd(a, b)$ is written as $ax + by = gcd(a, b)$ for some $x, y \in \mathbb{Z}$ is remarkable. I continue to showcase this side-benefit of the Euclidean Algorithm as we continue. We will give a general argument after the examples. I now shift to a less verbose presentation:

Example 3.12. *Find* $gcd(62, 626)$

$$626 = 10(62) + 6$$

$$62 = 10(6) + 2$$

$$6 = 3(2) + 0$$

From the E.A. I deduce $gcd(62, 626) = 2$. *Moreover,*

$$2 = 62 - 10(6) = 62 - 10[626 - 10(62)] = 101(62) - 10(626)$$

Example 3.13. *Find* $gcd(240, 11)$.

$$240 = 11(21) + 9$$

$$11 = 9(1) + 2$$

$$9 = 2(4) + 1$$

$$2 = 1(2)$$

Thus, by E.A., $gcd(240, 11) = 1$. *Moreover,*

$$1 = 9 - 2(4) = 9 - 4(11 - 9) = -4(11) + 5(9) = -4(11) + 5(240 - 11(21))$$

That is,

$$\boxed{1 = -109(11) + 5(240)}$$

Example 3.14. *Find* $gcd(4, 20)$. *This example is a bit silly, but I include it since it is an exceptional case in the algorithm. The algorithm works, you just need to interpret the instructions correctly.*

$$20 = 4(5) + 0$$

Since there is only one row to go from we identify 4 *as playing the same role as the last non-zero remainder in most examples. Clearly,* $gcd(4, 20) = 4$. *Now, what about working backwards? Since we do not have the gcd appearing by itself in the next to last equation (as we did in the last example) we are forced to solve the given equation for the gcd,*

$$20 = 4(4 + 1) = 4(4) + 4 \implies \boxed{20 - 4(4) = 4}$$

The following result also follows from the discussion before Theorem 3.10. I continue to use the notational set-up given there.

Theorem 3.15. Bezout's Identity: *if* $a, b \in \mathbb{Z}$, *not both zero, then there exist* $x, y \in \mathbb{Z}$ *such that* $ax + by = gcd(a, b)$.

Proof: we have illustrated the proof in the examples. Basically we just back-substitute the division algorithms. For brevity of exposition, I assume $r_3 = gcd(a,b)$. It follows that:

$$\begin{aligned} a = q_1 b + r_1 \quad &\Rightarrow \quad r_1 = a - q_1 b \\ b = q_2 r_1 + r_2 \quad &\Rightarrow \quad r_2 = b - q_2 r_1 \\ r_1 = q_3 r_2 + r_3 \quad &\Rightarrow \quad r_3 = r_1 - q_3 r_2 \end{aligned}$$

where $gcd(a,b) = r_3$. Moreover, $r_2 = b - q_2(a - q_1 b)$ implies $r_3 = r_1 - q_3[b - q_2(a - q_1 b)]$. Therefore,

$$gcd(a,b) = a - q_1 b - q_3[b - q_2(a - q_1 b)] = a - (q_1 - q_3[1 - q_2(a - q_1)]b.$$

Identify $x = 1$ and $y = q_1 - q_3[1 - q_2(a - q_1)]$. □

We should appreciate that x, y in the above result are far from unique. However, as we have shown, the method at least suffices to find a solution of the equation $ax + by = gcd(a,b)$. We have much more to say about this as the course unfolds. In fact, there are additional calculational ideas in Chapter 2 of Stillwell which **improve** on these notes. The main purpose of this note is to expand Stillwell's comments on modular arithmetic a bit. That work begins in the section which follows.

4 modular arithmetic

In this section we assume $n \in \mathbb{N}$ throughout.

Definition 4.1. *Let $a, b \in \mathbb{Z}$ then we say a is* **congruent** *to b mod(n) and write $a \equiv b$ mod(n) if a and b have the same remainder when divided by n.*

The definition above is made convenient by the simple equivalent criteria below:

Theorem 4.2. *$a \equiv b$ mod(n) if and only if $n \mid (b - a)$.*

Proof: Suppose $a \equiv b$ mod(n) then a and b share the same remainder after division by n. By the Division Algorithm, there exist $q_1, q_2 \in \mathbb{Z}$ for which $a = q_1 n + r$ and $b = q_2 n + r$. Observe, $b - a = (q_2 n + r) - (q_1 n + r) = (q_2 - q_1)n$. Therefore, $n \mid (b - a)$.

Conversely, suppose $n \mid (b - a)$ then there exists $q \in \mathbb{Z}$ for which $b - a = qn$. Apply the Division Algorithm to find q_1, q_2 and r_1, r_2 such that: $a = q_1 n + r_1$ and $b = q_2 n + r_2$ with $0 \leq r_1 < n$ and $0 \leq r_2 < n$. We should pause to note $|r_2 - r_1| < n$. Observe,

$$b - a = qn = (q_2 n + r_2) - (q_1 n + r_1) = (q_2 - q_1)n + r_2 - r_1.$$

Therefore, solving for the difference of the remainders and taking the absolute value,

$$|q - q_2 + q_1|n = |r_2 - r_1|$$

Notice $|q - q_2 + q_1| \in \mathbb{N} \cup \{0\}$ and $|r_2 - r_1| < n$. It follows $|q - q_2 + q_1| = 0$ hence $|r_2 - r_1| = 0$ and we conclude $r_1 = r_2$. □

Congruence has properties you might have failed to notice as a child.

Proposition 4.3. *Let n be a positive integer, for all $x, y, z \in \mathbb{Z}$,*

(i.) *$x \equiv x \ mod(n)$,*

(ii.) *$x \equiv y \ mod(n)$ implies $y \equiv x \ mod(n)$,*

(iii.) *if $x \equiv y \ mod(n)$ and $y \equiv z \ mod(n)$ then $x \equiv z \ mod(n)$.*

Proof: we use Theorem 4.2 throughout what follows.
(i.) Let $x \in \mathbb{Z}$ then $x - x = 0 = 0 \cdot n$ hence $n \mid (x - x)$ and we find $x \equiv x \ mod(n)$.
(ii.) Suppose $x \equiv y \ mod(n)$. Observe $n \mid (x - y)$ indicates $x - y = nk$ for some $k \in \mathbb{Z}$. Hence $y - x = n(-k)$ where $-k \in \mathbb{Z}$. Therefore, $n \mid (y - x)$ and we find $y \equiv x \ mod(n)$.
(iii.) Suppose $x \equiv y \ mod(n)$ and $y \equiv z \ mod(n)$. Thus $n \mid (y - x)$ and $n \mid z - y$. Corollary 3.5 indicates n also divides the sum of two integers which are each divisible by n. Thus, $n \mid [(y - x) + (z - y)]$ hence $n \mid (z - x)$ which shows $x \equiv z \ mod(n)$. □

I referenced the Corollary to prove part (iii.) to remind you how our current discussion fits naturally with our previous discussion.

Corollary 4.4. *Let $n \in \mathbb{N}$. Congruence modulo n forms an equivalence relation on $\mathbb{Z}$.*

This immediately informs us of an interesting **partition** of the integers. Recall, a **partition** of a set S is a family of subsets $U_\alpha \subseteq S$ where $\alpha \in \Lambda$ is some index set such that $U_\alpha \cap U_\beta = \emptyset$ for $\alpha \neq \beta$ and $\cup_{\alpha \in \Lambda} U_\alpha = S$. A partition takes a set an parses it into disjoint pieces which cover the whole set. The partition induced from an equivalence relation is simply formed by the **equivalence classes** of the relation. Let me focus on $\mathbb{Z}$ with the equivalence relation of congruence modulo a positive integer n. We define:[5]:

Definition 4.5. equivalence classes of $\mathbb{Z}$ modulo $n \in \mathbb{N}$:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\}$$

Observe, there are several ways to characterize such sets:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\} = \{y \in \mathbb{Z} \mid y - x = nk \text{ for some } k \in \mathbb{Z}\} = \{nk + x \mid k \in \mathbb{Z}\}.$$

I find the last presentation of $[x]$ to be useful in practical computations.

Example 4.6. *Congruence mod(2) partitions $\mathbb{Z}$ into even and odd integers:*

$$[0] = \{2k \mid k \in \mathbb{Z}\} \qquad \& \qquad [1] = \{2k + 1 \mid k \in \mathbb{Z}\}$$

Example 4.7. *Congruence mod(4) partitions $\mathbb{Z}$ into four classes of numbers:*

$$[0] = \{4k \mid k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$

$$[1] = \{4k + 1 \mid k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$

$$[2] = \{4k + 2 \mid k \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$

$$[3] = \{4k + 3 \mid k \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

[5] there are other notations, the concept here is far more important than the notation we currently employ

The patterns above are interesting, there is something special about [0] and [2] in comparison to [1] and [3]. Patterns aside, the notation of the previous two example can be improved. Let me share a natural notation which helps us understand the structure of congruence classes.

Definition 4.8. Coset Notation: *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ we define:*

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \qquad n\mathbb{Z} + a = \{nk + a \mid k \in \mathbb{Z}\}.$$

Observe, in the notation just introduced, we have

$$\boxed{[a] = n\mathbb{Z} + a}$$

Example 4.9. *Congruence mod(2) partititions $\mathbb{Z}$ into even and odd integers:*

$$[0] = 2\mathbb{Z} \qquad \& \qquad [1] = 2\mathbb{Z} + 1.$$

Example 4.10. *Congruence mod(4) partititions $\mathbb{Z}$ into four classes of numbers:*

$$[0] = 4\mathbb{Z}, \quad [1] = 4\mathbb{Z} + 1, \quad [2] = 4\mathbb{Z} + 2, \quad [3] = 4\mathbb{Z} + 3.$$

We should pause to appreciate a subtle aspect of the notation. It is crucial to note $[x] = [y]$ does **not** imply $x = y$. For example, modulo 2:

$$[1] = [3] = [7] = [1000037550385987987987971] \qquad \& \qquad [2] = [-2] = [-42].$$

Or, modulo 9:

$$[1] = [10] = [-8], \qquad \& \qquad [3] = [12] = [-6], \qquad \& \qquad [0] = [90] = [-9].$$

Yet, modulo 9, $[1] \neq [3]$. Of course, I just said $[1] = [3]$. How can this be? Well, context matters. In some sense, the notation $[x]$ is dangerous and $[x]_n$ would be better. We could clarify that $[1]_2 = [3]_2$ whereas $[1]_9 \neq [3]_9$. I don't recall such notation used in any text. What is more common is to use the *coset notation* to clarify:

$$2\mathbb{Z} + 1 = 2\mathbb{Z} + 3 \qquad \text{whereas} \qquad 9\mathbb{Z} + 1 \neq 9\mathbb{Z} + 3.$$

Proposition 4.11. *Let $n \in \mathbb{N}$. We have $[x] = [y]$ if and only if $x \equiv y \ mod(n)$. Or, in the coset notation $n\mathbb{Z} + x = n\mathbb{Z} + y$ if and only if $y - x \in n\mathbb{Z}$.*

Proof: Observe $x \in [x]$. If $[x] = [y]$ then $x \in [y]$ hence there exists $k \in \mathbb{Z}$ for which $x = y + nk$ hence $x - y = nk$ and we find $x \equiv y \ mod(n)$. Conversely, if $x \equiv y \ mod(n)$ then there exists $k \in \mathbb{Z}$ such that $y - x = nk$ thus $x = y - nk$ and $y = x + nk$. Suppose $a \in [x]$ then there exists $j \in \mathbb{Z}$ for which $a = nj + x$ hence $a = nj + y - nk = n(j - k) + y \in [y]$. We have shown $[x] \subseteq [y]$. Likewise, if $b \in [y]$ then there exists $j \in \mathbb{Z}$ for which $b = nj + y$ hence $b = nj + x + nk = n(j + k) + x \in [x]$. Thus $[y] \subseteq [x]$ and we conclude $[x] = [y]$. $\square$

Notice the proposition above allows us to calculate as follows: for $n \in \mathbb{N}$

$$n\mathbb{Z} + na + b = n\mathbb{Z} + b \qquad \text{or} \qquad [na + b] = [b]$$

for $a, b \in \mathbb{Z}$. There is more.

Proposition 4.12. *Let $n \in \mathbb{N}$. If $[x] = [x']$ and $[y] = [y']$ then*

(i.) $[x + y] = [x' + y']$,

(ii.) $[xy] = [x'y']$

(iii.) $[x - y] = [x' - y']$

Proof: Suppose $[x] = [x']$ and $[y] = [y']$. It follows there exists $j, k \in \mathbb{Z}$ such that $x' = nj + x$ and $y' = nk + y$. Notice $x' \pm y' = nj + x \pm (nk + y) = n(j \pm k) + x \pm y$. Therefore, $x \pm y \equiv x' \pm y'$ $mod(n)$ and by Proposition 4.11 we find $[x \pm y] = [x' \pm y']$. This proves $(i.)$ and $(iii.)$. Next, consider:

$$x'y' = (nj + x)(nk + y) = n(jkn + jy + xk) + xy$$

thus $x'y' \equiv xy$ $mod(n)$ we apply Proposition 4.11 once more to find $[xy] = [x'y']$. □

We ought to appreciate the content of the proposition above as it applies to congruence modulo n. In fact, the assertions below all apear in the proof above.

Corollary 4.13. *Let $n \in \mathbb{N}$. If $x \equiv= x'$ and $y \equiv y'$ modulo n then*

(i.) $x + y \equiv x' + y'$ $mod(n)$,

(ii.) $xy \equiv x'y'$ $mod(n)$,

(iii.) $x - y \equiv x' - y'$ $mod(n)$,

Example 4.14. *Suppose $x + y \equiv 3$ and $x - y \equiv 1$ modulo 4. Then, by Corollary 4.13 we add and substract the given congruences to obtain:*

$$2x \equiv 4 \qquad 2y \equiv 2$$

There are 4 cases to consider. Either $x \in [0]$, $x \in [1]$, $x \in [2]$ or $x \in [3]$. Observe,

$$\begin{array}{ll} 2(0) \equiv 0 \equiv 4, & 2(0) \not\equiv 2 \\ 2(1) \equiv 2 \not\equiv 4, & 2(1) \equiv 2 \\ 2(2) \equiv 4, & 2(2) \equiv 4 \not\equiv 2 \\ 2(3) \equiv 2 \not\equiv 4, & 2(3) \equiv 2. \end{array}$$

It follows that $x \in [0] \cup [2]$ and $y \in [1] \cup [3]$ forms the solution set of this system of congruences.

The method I used to solve the above example was not too hard since there were just 4 cases to consider. I suppose, if we wished to solve the same problem modulo 42 we probably would like to learn a better method.

Proposition 4.12 justifies that the definition below does give a **binary operation** on the set of equivalence classes modulo n. Recall, a *binary operation* on a set S is simply a *function* from $S \times S$ to S. It is a single-valued assignment of pairs of S-elements to S-elements.

Definition 4.15. modular arithmetic: *let $n \in \mathbb{N}$, define*

$$[x] + [y] = [x + y] \qquad \& \qquad [x][y] = [xy]$$

for all $x, y \in \mathbb{Z}$. Or, if we denote the set of all equivalence classes modulo n by $\mathbb{Z}/n\mathbb{Z}$ then write: for each $n\mathbb{Z} + x, n\mathbb{Z} + y \in \mathbb{Z}/n\mathbb{Z}$

$$(n\mathbb{Z} + x) + (n\mathbb{Z} + y) = n\mathbb{Z} + x + y \qquad \& \qquad (n\mathbb{Z} + x)(n\mathbb{Z} + y) = n\mathbb{Z} + xy.$$

Finally, we often use the notation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Notice the operation defined above is a binary operation on $\mathbb{Z}/n\mathbb{Z}$ (not $\mathbb{Z}$). Many properties of integer arithmetic transfer to $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned}
[a] + [b] &= [b] + [a] \\
[a][b] &= [b][a] \\
[a]([b] + [c]) &= [a][b] + [a][c] \\
([a] + [b])[c] &= [a][c] + [b][c] \\
([a] + [b]) + [c] &= [a] + ([b] + [c]) \\
([a][b])[c] &= [a]([b][c]) \\
[a] + [0] &= [0] + [a] = [a] \\
[1][a] &= [a][1].
\end{aligned}$$

Furthermore, for $k \in \mathbb{N}$,

$$\begin{aligned}
[a_1] + [a_2] + \cdots + [a_k] &= [a_1 + a_2 + \cdots + a_k] \\
[a_1][a_2] \cdots [a_k] &= [a_1 a_2 \cdots a_k] \\
[a]^k &= [a^k].
\end{aligned}$$

Example 4.16. *Simplify* $[1234]$ *modulo* 5. *Notice,*

$$1234 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 4.$$

However, $10 = 2(5)$ *thus,*

$$1234 = 1 \times 2^3 5^3 + 2 \times 2^2 5^2 + 3 \times 2 \cdot 5 + 4.$$

Note, $[5] = [0]$ *hence* $[5^k] = [0]$ *for* $k \in \mathbb{N}$. *By the properties of modular arithmetic it is clear that the* $10's$, $100's$ *and* $1000's$ *digits are irrelevant to the result. Only the first digit matters,* $[1234] = [4]$.

It is not hard to see the result of the example above equally well applies to larger numbers; if a_k, $a_{k-1}, \ldots, a_2, a_1$ are the digits in a decimal representation of an integer then $[a_k a_{k-1} \cdots a_2 a_1] = [a_1]$ $mod(5)$.

Example 4.17. *Calculate the cube of* 51 *modulo* 7*.*

$$[51^3] = [51][51][51] = [51]^3 = [49+2]^3 = [2]^3 = [8].$$

Of course, you can also denote the same calculation via congruence:

$$51^3 = 51 \cdot 51 \cdot 51 \equiv 2 \cdot 2 \cdot 2 = 8 \quad \Rightarrow \quad [51^3] = [8].$$

The next example is a cautionary tale:

Example 4.18. *Simplify* 7^{100} *modulo* 6*. Consider,*

$$[7^{100}] = [7]^{100} = [1]^{100} = [1^{100}] = [1].$$

or, (incorrectly !)

$$[7^{100}] = [7^{[100]}] = [7^{[6(16)+4]}] = [7^4] = [28] = [4].$$

The point is this: it is **not** *true that* $[a^k] = [a^{[k]}]$.

Naturally, as we discuss $\mathbb{Z}_n$ it is convenient to have a particular choice of representative for this set of residues. Two main choices: the *set of least non-negative residues*

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

alternatively, *set of least absolute value residues* or simply *least absolute residues*

$$\mathbb{Z}_n = \{[0], [\pm 1], [\pm 2], \ldots\}$$

where the details depend on if n is even or odd. For example,

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\} = \{[-2], [-1], [0], [1], [2]\}$$

or,

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\} = \{[-2], [-1], [0], [1]\}$$

Honestly, if we work in the particular context of $\mathbb{Z}_n$ then there is not much harm in dropping the $[\cdot]$-notation. Sometimes, I use $[x] = \bar{x}$. Whichever notation we choose, we must be careful to not fall into the trap of assuming the usual properties of $\mathbb{Z}$ when calculating in the specific context of modular arithmetic. The example that follows would be very clumsy to write in the $[\cdot]$-notation.

Example 4.19. *Consider* $f(x) = x^2 + 2x + 3$ *for* $x \in \mathbb{Z}_5$*. We can determine if* f *has a zero by explicit calculation modulo* 5*:*

$$f(-2) = (-2)^2 + 2(-2) + 3 = 3$$

$$f(-1) = (-1)^2 + 2(-1) + 3 = 2$$

$$f(0) = (0)^2 + 2(0) + 1 = 3$$

$$f(1) = 1 + 2 + 3 \equiv 1$$

$$f(2) = 4 + 4 + 3 \equiv 1$$

Therefore, $f(x)$ *has no zero for* $x \in \mathbb{Z}_5$*.*

The examples below are from Jones and Jones' *Elementary Number Theory* pages 42-43.

Example 4.20. *Calculate the least positive residue of* 28×33 *modulo* 35. *Note that* $28 \equiv 28 - 35 = -7$ *and* $33 \equiv 33 - 35 = -2$ *hence* $28 \times 33 \equiv (-7) \times (-2) = 14$. *Or,* $[28][33] = [14]$.

Example 4.21. *Calculate the least absolute residue of* 15×59 *mod*(75). *Observe* $59 \equiv 59 - 75 = -16$ *thus*

$$59 \times 15 \equiv -16 \times 15 = (-1 - 15) \times 15 = -15 - 3(75) \equiv -15.$$

Since $|-15| = 15 \leq 75/2$ *it is clear* -15 *is the least absolute residue modulo* 75.

Example 4.22. *To calculate* 3^8 *modulo 13 we break the problem into several doublings;* $3^8 = ((3^2)^2)^2$. *At each stage we take care to use modular arithmetic to simplify:*

$$3^2 = 9 \equiv -4$$

modulo 13. *Next,*

$$3^4 = (3^2)^2 \equiv (-4)^2 = 16 \equiv 3$$

thus

$$3^8 = (3^4)^2 \equiv 3^2 = 9.$$

Example 4.23. *Prove that* $a(a+1)(a+2)$ *is divisible by* 6 *for each integer* a. *In other words, we wish to show* $a(a+1)(a+2) \equiv 0$ *mod*(6). *Note* $\mathbb{Z}_6 = \{[0], [\pm 1], [\pm 2], [3]\}$ *so consider:*

$$\begin{aligned}
a = 0: &\quad a(a+1)(a+2) = 0,\\
a = \pm 1: &\quad a(a+1)(a+2) = (\pm 1)(1 \pm 1)(2 \pm 1) = \{6, 0\} \equiv 0,\\
a = \pm 2: &\quad a(a+1)(a+2) = (\pm 2)(1 \pm 2)(2 \pm 2) = \{12, 0\} \equiv 0,\\
a = 3: &\quad a(a+1)(a+2) = (3)(3+1)(3+2) = 60 \equiv 0.
\end{aligned}$$

Therefore, $a(a+1)(a+2) \equiv 0$ *modulo* 6 *for all* $a \in \mathbb{Z}$ *hence* $6 \mid a(a+1)(a+2)$ *for all* $a \in \mathbb{Z}$.

The claim in the example above is very obviously true if we just think about some cases $1 \cdot 2 \cdot 3$,$2 \cdot 3 \cdot 4$,...$10 \cdot 11 \cdot 12$, $11 \cdot 12 \cdot 13$ etc. You can see the reason a 6 appears is that in any triple of successive integers you have at least one number divisible by 3 and at least one number divisible by 2. This suggests a different method of proof.

Example 4.24. *Prove that* $a(a+1)(a+2)$ *is divisible by* 6 *for each integer* a. *Once again, we wish to show* $a(a+1)(a+2) \equiv 0$ *mod*(6). *Observe, if* $2 \mid x$ *and* $3 \mid x$ *then* $x = 2j$ *and* $x = 3k$ *for some* $j, k \in \mathbb{Z}$. *It follows from the prime factorization of integers that* $3 \mid j$ *and* $2 \mid k$ *hence*[6] *there exists* $m \in \mathbb{Z}$ *for which* $j = 3m$ *and we find* $x = 2j = 2(3m) = 6m$ *which proves* $6 \mid x$. *Therefore, if we are able to show* $a(a+1)(a+2)$ *is divisible by* 2 *and* 3 *it follows* $a(a+1)(a+2)$ *is divisible by* 6. *Consider congruence modulo 2:*

$$\begin{aligned}
a = 0: &\quad a(a+1)(a+2) = 0,\\
a = 1: &\quad a(a+1)(a+2) = (1)(2)(3) \equiv 0.
\end{aligned}$$

[6]yes, I could just as well have messed with k

Next, the modulo 3 case:

$$\begin{aligned} a = 0: &\qquad a(a+1)(a+2) = 0, \\ a = 1: &\qquad a(a+1)(a+2) = (1)(2)(3) \equiv 0, \\ a = 2: &\qquad a(a+1)(a+2) = (2)(3)(4) \equiv 0. \end{aligned}$$

Thus $a(a+1)(a+2) \equiv 0$ *modulo 6 and we conclude* $6 \mid a(a+1)(a+2)$ *for each* $a \in \mathbb{Z}$.

Notice I had to invoke the Fundalmental Theorem of Arithmetic in the example above. Let me state it without proof here:

Theorem 4.25. *Let* $n \in \mathbb{N}$ *then there exist a unique set of distinct primes* $p_1, p_2, \ldots, p_k$ *and multiplicities* $r_1, r_2, \ldots, r_k$ *for which* $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$.

Proof: elsewhere[7]. □

We already saw a specific case of the theorem below in action to solve Example 4.24.

Theorem 4.26. *Let* $n \in \mathbb{N}$ *such that there exist a unique set of distinct primes* $p_1, p_2, \ldots, p_k$ *and multiplicities* $r_1, r_2, \ldots, r_k$ *for which* $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. *Then* $a \equiv b \ mod(n)$ *if and only if* $a \equiv b \ mod(p_i^{r_i})$ *for each* $i = 1, 2, \ldots k$.

Proof: postponed. □

I should caution the reader. These notes are not meant to be a complete exposition. I merely intend to complement Stillwell. Mostly I'm working through some sections in Jones and Jones' excellent text *Elementary Number Theory*. It is worth noting I have left out discussion of divisibility theorems for primes and the least common multiple. These topics are interesting, but, I forge ahead for brevity.

The theme of this section is illustrate the structure and utility of modular arithmetic. The Theorem below is certainly a showcase of the technique. The problem of determining if $f(x) = 0$ for some $x \in \mathbb{Z}$ is somewhat daunting as there are infinitely many integers. However, for polynomial $f(x)$ we are able to answer this question by analyzing the corresponding polynomial over $\mathbb{Z}_n$. Let's study an example before I state the general theorem.

Example 4.27. *Show* $f(x) = x^5 - x^2 + x - 3$ *has no integer roots. Consider, modulo 4,*

$$f(0) = -3, \qquad f(1) = 1 - 1 + 1 - 3 = -2,$$

$$f(-1) = -1 - 1 - 1 - 3 = -6 \equiv 2, \qquad f(2) = 32 - 4 + 2 - 3 \equiv -1.$$

This means there is no integer for which $f(x) = 0$. *Why? Because* $\mathbb{Z} = 4\mathbb{Z} \cup (4\mathbb{Z}+1) \cup (4\mathbb{Z}+2) \cup (4\mathbb{Z}+3)$ *and we have shown each partition gives no value in* $4\mathbb{Z}$ *hence no integer input into* $f(x)$ *returns a value of* 0.

[7] don't worry, not **that** elsewhere, it's safe enough to prove

Theorem 4.28. *Let $f(x) \in \mathbb{Z}[x]$, that is let $f(x)$ be a polynomial with integer coefficients, and suppose $n \in \mathbb{N}$. If $a \equiv b \ mod(n)$ then $f(a) \equiv f(b) \ mod(n)$.*

Proof: Suppose $a \equiv b \ mod(n)$ and $f(x) = c_m x^m + \cdots + c_1 x + c_0$ where $c_m, \ldots, c_1, c_0 \in \mathbb{Z}$. Consider then, by repeated application of Corollary 4.13 we have:

$$f(a) = c_m a^m + \cdots + c_1 a + c_0 \equiv c_m b^m + \cdots + c_1 b + c_0 = f(b). \quad \square$$

To solve Example 4.27 we used the **contrapositive**. Let me remind you: the contrapositive allows us to know that when $P \Rightarrow Q$ is true then $\widetilde{Q} \Rightarrow \widetilde{P}$ is true. Here I use P, Q to denote statements and $\widetilde{P}, \widetilde{Q}$ to denote the negation of those statements. Suppose $f(a) = 0$ for some some $a \in \mathbb{Z}$. Then a clear implication is that $f(a) \equiv 0 \ mod(n)$ for all $n \in \mathbb{N}$. In this case P is the statement about integer zeros whereas Q is the statement about the congruence of $f(a)$ modulo n for all $n \in \mathbb{N}$. The contrapositive negates Q to the statement *there exists* $n \in \mathbb{N}$ for which $f(a) \not\equiv 0 \ mod(n)$. On the other hand, the negation of P is simply $f(a) \neq 0$. To finish the thought, the contrapositive of the theorem suggests that if we can find an n such that $f(a) \not\equiv 0$ for all $a \in \mathbb{Z}$ then it follows $f(a) \neq 0$ for all $a \in \mathbb{Z}$.

This method is not generally successful in proving the non-existence of integer zeros for polynomials over the integers. See page 45 of Jones and Jones' *Elementary Number Theory* for comments.

There is a large difference between ordinary arithmetic in $\mathbb{Z}$ and that of $\mathbb{Z}_n$. We already saw in Example 4.14 the solution set of a system of equations in $\mathbb{Z}_4$ had four distinct solutions. In the context of systems of equations over $\mathbb{Z}$ we either obtain no solutions, one solution, or infinitely many. This distinction is largely tied to the fact that some numbers in $\mathbb{Z}_n$ do not have multiplicative inverses. For example, in $\mathbb{Z}_4$ the fact that $[2][2] = [0]$ implies there cannot be $[x]$ such that $[2][x] = [1]$ since that would give us $[2][2][x] = [0][x]$ implying $[2][1] = [2] = [0]$ which is absurd. Apparently, only certain numbers in $\mathbb{Z}_n$ have multiplicative inverses. Let us characterize which numbers have inverses modulo n. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ we seek to solve:

$$[a][x] = [1] \quad \Rightarrow \quad ax - 1 = nk$$

for some $k \in \mathbb{Z}$. This gives,

$$ax + nk = 1$$

If a and n have a common factor larger than 1 then we obtain a contradiction since 1 has no divisors. Thus, in the case there is a solution, we must have $gcd(a, n) = 1$. This is fortunate news since we have a nice method to calculate $gcd(a, n)$ and the criteria that a^{-1} exist in $\mathbb{Z}_n$ is simply that a is **relatively prime** or, if you prefer, **coprime**.

Example 4.29. *In Example 3.12 we found $gcd(62, 626) = 2$. This shows 62 does not have a multiplicative inverse modulo 626. Also, it shows 626 does not have a multiplicative inverse modulo 62.*

Example 4.30. *In Example 3.13 we found $gcd(11, 240) = 1$ and $1 = -109(11) + 5(240)$. From this we may read several things:*

$$[-109]^{-1} = [11] \ mod(240) \qquad \& \qquad [-109]^{-1} = [11] \ mod(5)$$

and,

$$[5]^{-1} = [240]\ mod(11) \qquad \& \qquad [5]^{-1} = [240]\ mod(109).$$

In terms of least positive residues the last statement reduces to $[5]^{-1} = [22]$. *Of course, we can check this;* $[5][22] = [110] = [1]$.

With this our introduction comes to an end. We'll pick back up here in the next episode. There we will discuss the general solution of $ax \equiv b$ modulo n. How to solve multiple congruences with respect to different moduli (Chinese Remainder Theorem) and finally the beautiful technique of Hensel which rests on an intuition derived from the p-adic numbers.