Notes for Proofs in Number Theory

Charles Rocca

Contents

Part I

Number Theory

Chapter 1

On the Structure of Integers

1.1 Divisibility

1.1.1 Divisibility and the Division Algorithm

Divisibility, when one number "goes into" another, is central to most results in elementary number theory which focuses on understanding the basic properties of the integers.

Example 1.1 (Divisibility)**.** Consider why these examples illustrate what we might mean when we say one number divides another.

- ✓ 5 divides 20 since $20 = 4 \cdot 5$
- ✓ 2 divides 14 since $14 = 7 \cdot 2$
- ✓ 30 divides 210 since $210 = 7 \cdot 30$
- ✗ 3 doesn't divide 20 since $6 \cdot 3 < 20 < 7 \cdot 3$
- ✗ 4 doesn't divide 27 since $6 \cdot 4 < 27 < 7 \cdot 4$
- ✗ 5 doesn't divide 39 since $7 \cdot 5 < 39 < 8 \cdot 5$

The following formal definition captures this idea in a precise and constructive way.

Definition 1.1 (Divisibility)**.** Given $a, b \in \mathbb{Z}$, we say b *divides* a and write $b|a$ if and only if there exists a unique quotient $q \in \mathbb{Z}$ such that $a = qb$.

Reflection:

- If a is a non-zero integer, why, using definition 1.1, does it not make sense to talk about 0 dividing a?
- Again, referring to the definition of divisibility, why can't we discuss 0 dividing 0?
- As you go forward think about why the definition that $a = qb$ is more useful than saying something like *"an integer b divides a if it goes into it evenly."*

Here are some immediate and important observations about divisibility.

Lemma 1.1. *Divisibility is transitive*

Proof. Let $a, b, c \in \mathbb{Z}$ and assume that $a|b$ and $b|c$. Then we may write $b = q_b a$ and $c = q_c b$ from which we get

$$c = q_c b = q_c q_b a.$$ (1)

With $q = q_c q_b$ we have $c = qa$, that is $a|c$. (2) Therefore, we have shown that divisibility is a transitive relation. □

Reflection:

- In exercise 1.10 you will prove that divisibility is reflexive. However, divisibility is not symmetric, can you give an example to demonstrate this?

Lemma 1.2. *Given $a, b \in \mathbb{Z}$, both positive, if $b|a$, then $b \leq a$.*

Proof. Suppose that $a, b \in \mathbb{Z}$ are both positive and $b|a$. (1) Then we can write $a = qb$ for some unique $q \in \mathbb{Z}$ and $q \geq 1$. (2)
Case 1 $(q = 1)$**.** If $q = 1$ then $a = qb = b$ and $b = a$.
Case 2 $(q > 1)$**.** If $q > 1$, then

$$a = qb \geq 2b > b.$$ (3)

Hence, in this case $b < a$.
Therefore we see that if a and b are positive integers such that $b|a$, then $b \leq a$. □

Reflection:

- How would the proof change if a and/or b were negative?
- Could we use absolute values to reduce the general case to the case when a and b are positive?
- Why is it important that a is non-zero?

Theorem 1.3 (Linear Combinations)**.** *Given $a, b, c \in \mathbb{Z}$, $c|a$ and $c|b$ if and only if $c|(ax + by)$ for all $x, y \in \mathbb{Z}$.*

Proof. Let $a, b, c \in \mathbb{Z}$ and assume that $c|a$ and $c|b$. We may write $a = q_a c$ and $b = q_b c$ for some unique integers q_a and q_b. (1) Then for any arbitrary $x, y \in \mathbb{Z}$

$$ax + by = q_a cx + q_b cy = (q_a x + q_b y)c$$

so that $c|(ax + by)$. (2)
Now suppose that for all $x, y \in \mathbb{Z}$, $c|(ax + by)$. (3) In particular, if $x = 1$ and $y = 0$, then $c|a$. Similarly, if $x = 0$ and $y = 1$, $c|b$. Hence, c divides both a and b. (4)
Thus, given $a, b, c \in \mathbb{Z}$, $c|a$ and $c|b$ if and only if $c|(ax + by)$ for all $x, y \in \mathbb{Z}$. (5) □

Axiom 1.2 (Well Ordering Principle)**.** Any non-empty subset of the natural numbers, $\mathbb{N}$, has a least element.

Frequently, as we will see, the *Well Ordering Principle (W.O.P.)* is employed when a theorem wants to show a number is the least number with a property and occasionally when it is the greatest. One such application of the W.O.P. is the *Division Algorithm* which defines what we will mean when we talk about dividing one integer by another to find a quotient and remainder.

Theorem 1.4 (Division Algorithm). *Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that*

$$a = qb + r$$

and $0 \leq r, |b|$. The value q is called the quotient *and r is the* remainder.

Proof. Let $a, b \in \mathbb{Z}$ and define

$$T = \{a - kb | k \in \mathbb{Z} \wedge a - kb > 0\}.$$

Note that if $b > 0$ and $k < a/b$, then $a - kb > 0$. Likewise, if $b < 0$ and $k > a/b$, then $a - kb > 0$. Thus we conclude T is a non-empty set of natural numbers.[(1)]
Now, let $r = a - qb$ be the least element in T.[(2)] If $r \geq |b|$ and $b > 0$, then

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

with $r' = a - (q+1)b \geq 0$. However, then $r' \in T$ and $r' < r$, which is a contradiction.[(3)] We arrive at a similar contradiction if $r \geq |b|$ and $b < 0$.[(4)] Therefore, $0 \leq r < |b|$ and $a = qb + r$.
Suppose that $a = q_0 b + r_0$ and $a = q_1 b + r_1$ with $0 \leq r_i < |b|$, so that

$$(q_1 - q_0)b = r_0 - r_1.^{(5)}$$

Then $b | (r_0 - r_1)$, however $0 \leq |r_0 - r_1| < b$, thus $r_0 = r_1$ and $q_1 = q_0$.[(6)] Hence, we have shown that there exists unique q and r so that $a = qb + r$ and $0 \leq r < |b|$. □

Example 1.2 (Division Algorithm). Look each pair of integers a and b below and check that you can find the indicated q and r.

- $a = 35$ and $b = 8$, $35 = 4(8) + 3$
- $a = 35$ and $b = -8$, $35 = -4(-8) + 3$
- $a = -35$ and $b = 8$, $-35 = -5(8) + 5$
- $a = -35$ and $b = -8$, $-35 = 5(-8) + 5$
- $a = 23$ and $b = 5$, $23 = 4(5) + 3$
- $a = -17$ and $b = -2$, $-17 = 9(-2) + 1$
- $a = 55$ and $b = 11$, $55 = 11(5) + 0$
- $a = -27$ and $b = 6$, $-27 = -5(6) + 3$

Reflection:

- For each pair of integers in example 1.2, try and run them through the code in figure 1.1.
- Under which circumstance(s) was the initial guess for q wrong?
- In those circumstances, how did the code fix the value of q?

```python
def divAlg(a,b):
    # initial guess at q
    q=int(a/b)
    # adjust q if r<0
    if a-q*b<0:
        q=int(q/abs(q)*(abs(q)+1))
    # calculate r
    r=a-q*b
    return q,r
```

(a) Implementation Code

```
divAlg(35,8)
(4,3)
divAlg(35,-8)
(-4,3)
divAlg(-35,8)
(-5,5)
divAlg(-35,-8)
(5,5)
```

(b) Output

Figure 1.1: Implementing the Division Algorithm

Definition 1.3 (Even and Odd Integers)**.** An integer n is *even* if and only if $2|n$, i.e. $n = 2q$ for some unique $q \in \mathbb{Z}$. If and integer is not even it is *odd* and we can write it as $n = 2q + 1$ for some unique $q \in \mathbb{Z}$.

Reflection:

- Why does the Division Algorithm guarantee that all integers must be either even or odd?
- Why does it make sense to write odd integers in the form $2q + 1$?

Lemma 1.5. *Every integer is even or odd but not both.*

Proof. Suppose that $n \in \mathbb{Z}$ is both even and odd so that

$$n = 2q_1 = 2q_2 + 1,$$

for some unique $q_1, q_2 \in \mathbb{Z}$. **(1)** Then we may conclude $2(q_1 - q_2) = 1$ which implies 2 divides 1 which is a contradiction. **(2)** Therefore, no integer is simultaneously even and odd. □

Lemma 1.6. *The square of any even integer is also even.*

Proof. Let $n \in \mathbb{Z}$ be and even integer with $n = 2q$. **(1)** Then we may note that

$$\begin{aligned} n^2 &= (2q)^2 \\ &= 2(2q^2), \end{aligned}$$

and hence $n^2 = 2\hat{q}$ with $\hat{q} = 2q^2$ and n^2 is even. **(2)** Since n was an arbitrarily chosen even integer, we conclude that the square of any even integer is also even. □

Corollary 1.7. *If the square of an integer is odd, then the integer is odd.*

Proof. Given an integer n, lemma 1.6 showed that if n is even, then n^2 is also even. Therefore, we may conclude that if n^2 is odd, then n is also odd. [1] □

Reflection:

- In what way did the previous argument require lemma 1.5 and theorem 1.4?

Lemma 1.8. *The square of every integer can be written as either $4n$ or $4n+1$ for some integer n.*

Proof. Assume $a \in \mathbb{Z}$, then either $a = 2q$ or $a = 2q+1$ for some integer q. [1]
Case 1. $(a = 2q)$
If $a = 2q$, then $a^2 = 4q^2 = 4n$, when $n = q^2$.
Case 2. $(a = 2q+1)$
Now, assume that $a = 2q+1$ so that

$$\begin{aligned} a^2 &= (2q+1)^2 \\ &= 4q^2 + 4q + 1 \\ &= 4(q^2+q) + 1 \\ &= 4n + 1, \end{aligned}$$

when $n = q^2 + q$.
Therefore, since the theorem holds in each case we may conclude that the square of every integer is either a multiple of four or one greater than a multiple of 4. [2] □

1.1.2 Primes and Composites

Definition 1.4 (Prime and Composite)**.** A positive integer is called *prime* if it has exactly to divisors, one and its self. Integers with more than two distinct divisors are called composite.

Note that 1 is unique in being neither prime nor composite. The reason for this is related to the Fundamental Theorem of Arithmetic (Theorem 1.24) which we will examine in Section 1.3.

Example 1.3. Which of the first 10 natural numbers (positive integers) are prime and which are composite.

✗ $1 = 1 \cdot 1$

✓ $2 = 1 \cdot 2$

✓ $3 = 1 \cdot 3$

✗ $4 = 1 \cdot 4 = 2 \cdot 2$

✓ $5 = 1 \cdot 5$

✗ $6 = 1 \cdot 6 = 2 \cdot 3$

✓ $7 = 1 \cdot 7$

✗ $8 = 1 \cdot 8 = 2 \cdot 4$

✗ $9 = 1 \cdot 9 = 3 \cdot 3$

✗ $10 = 1 \cdot 10 = 2 \cdot 5$

So, the numbers 2, 3, 5, and 7 are prime, while 4, 6, 8, 9, and 10 are composite, and 1 is neither.

Example 1.4 (Visualizing Primes and Composites)**.** We can visualize primes and composites as groups of pebbles arranged into rectangles. For a prime number of pebbles, like $7 = 1 \cdot 7$, there is really only one way to arrange the pebbles into a rectangle. But for a composite number, like $12 = 1 \cdot 12 = 2 \cdot 6 = 3 \cdot 4$, there are multiple ways to form a rectangle.

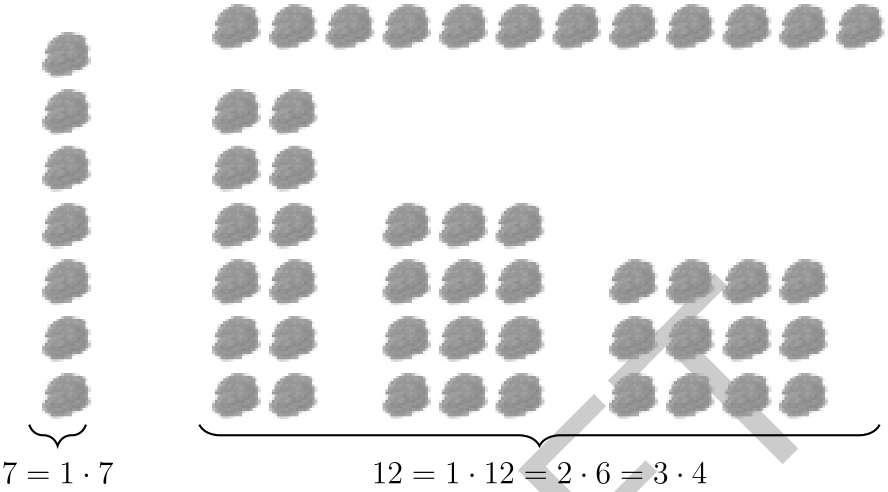
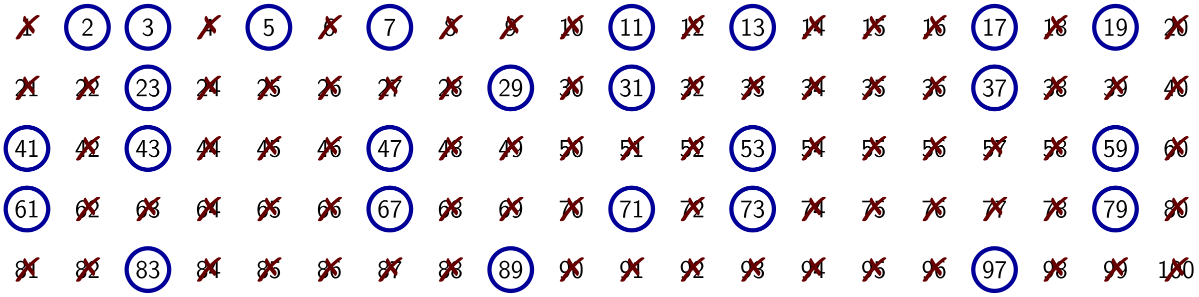


Figure 1.2: Prime and Composite Pebbles

Example 1.5 (Sieve of Eratosthenes)**.** Prime numbers are not predictably distributed or easy to find or generate. One of the earliest algorithms for finding primes is the *Sieve of Eratosthenes* (≈300BCE). To find all the prime numbers from 1 to 100 begin by writing out the numbers, then cross out 1, which is not prime, then repeat the following steps:

1. Circle the smallest number that is not crossed off, it is prime.
2. Cross off all the multiples of that number.
3. Repeat until all the numbers are circled or crossed off.



$\cancel{1}$	2	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$	11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	29	$\cancel{30}$	31	$\cancel{32}$	$\cancel{33}$	$\cancel{34}$	$\cancel{35}$	$\cancel{36}$	37	$\cancel{38}$	$\cancel{39}$	$\cancel{40}$
41	$\cancel{42}$	43	$\cancel{44}$	$\cancel{45}$	$\cancel{46}$	47	$\cancel{48}$	$\cancel{49}$	$\cancel{50}$	$\cancel{51}$	$\cancel{52}$	53	$\cancel{54}$	$\cancel{55}$	$\cancel{56}$	$\cancel{57}$	$\cancel{58}$	59	$\cancel{60}$
61	$\cancel{62}$	$\cancel{63}$	$\cancel{64}$	$\cancel{65}$	$\cancel{66}$	67	$\cancel{68}$	$\cancel{69}$	$\cancel{70}$	71	$\cancel{72}$	73	$\cancel{74}$	$\cancel{75}$	$\cancel{76}$	$\cancel{77}$	$\cancel{78}$	79	$\cancel{80}$
$\cancel{81}$	$\cancel{82}$	83	$\cancel{84}$	$\cancel{85}$	$\cancel{86}$	$\cancel{87}$	$\cancel{88}$	89	$\cancel{90}$	$\cancel{91}$	$\cancel{92}$	$\cancel{93}$	$\cancel{94}$	$\cancel{95}$	$\cancel{96}$	97	$\cancel{98}$	$\cancel{99}$	$\cancel{100}$

Figure 1.3: Sieve of Eratosthenes for 1-100

These examples seem to show that all integers should be broken down into one of three categories, 1, prime, or composite, and all composites have a prime divisor. The latter fact can be shown using the Well Ordering Principle, Axiom 1.2.

Lemma 1.9. *Every composite integer is divisible by a prime number.*

Proof. Suppose there exist composite integers which are not divisible by any prime, let S be the non-empty set of all such integers, and let $n \in S$ be the least element. (1) Since, n is composite we may write $n = a \cdot b$ for some integers a and b greater than 1. (2) If a or b are prime then we get a contradiction. (3) Without loss of generality, assume a is composite with prime divisor p. (4) Then, $p|n$ and we again have a contradiction. (5) Therefore, there can not exists an integer n which is composite and not divisible by a prime. □

Reflection:

- The previous proof, as written, technically only addresses positive integers, why?
- How could we rewrite the proof so that both positive and negative integers are addressed?

A significant result regarding prime numbers is that there are infinitely many of them, which was proved at least as early as the 4^{th} century BCE in Euclid's Elements. An extraordinary element of this fact is how relatively straight forward it is to show.

Theorem 1.10 (Infinite Primes)**.** *Given any finite set of prime numbers, there exists a prime not in the set.*

Proof. Consider a finite set of primes $S = \{p_1, p_2, p_3, \ldots, p_n\}$ with $n \geq 1$ and construct a new number

$$Q = (p_1 p_2 p_3 \cdots p_n) + 1.$$

Since we are adding 1, Q is greater than p_i for all i and greater than 1. (1) Writing,

$$1 = Q - (p_1 p_2 p_3 \cdots p_n),$$

we conclude that Q is not divisible by p_i for any i; if it were, then p_i would divide 1. (2) The integer Q is either prime or composite since it is greater than 1. (3) If Q is prime we are done, if not we can factor it until we find a prime factor which is not in the set S. (4) Therefore, given any finite set of prime numbers there is a prime not in the set, hence there are infinitely many primes. □

The next couple of theorems help us put bounds on the size and number of primes up to a certain value. The first, which we shall prove, bounds the size of the n^{th} prime. The second, whose proof is beyond this course, helps predict the number of primes that are less than a given number.

Theorem 1.11 (n^{th} Prime)**.** *The n^{th} prime, p_n, is less than or equal to $2^{2^{n-1}}$.*

Proof.
Base Case $(\mathbf{p_n = 2,\ n = 1})$: The first prime number is $p = 2$ and

$$2 \leq 2^1 = 2^{2^0} = 2^{2^1-1}.$$

Therefore, the theorem is true when $n = 1$.

Induction Step $(\mathbf{p_n > 2,\ n > 1})$**:** Assume that the theorem is true for all $1 \le k \le (n-1)$, i.e.

$$p_k \le 2^{2^{k-1}},$$

when $1 \le k \le (n-1)$. Now we note that $p_n \le (p_1p_2p_3\cdots p_{n-1})+1$. $^{\mathbf{(1)}}$ Applying the induction assumption,

$$\begin{aligned}(p_1p_2p_3\cdots p_{n-1})+1 &\le \left(2^{2^0}2^{2^1}2^{2^2}\cdots 2^{2^{n-2}}\right)+1^{\mathbf{(2)}}\\ &= \left(2^{\sum_{i=0}^{n-2}2^i}\right)+1^{\mathbf{(3)}}\\ &= \left(2^{2^{n-1}-1}\right)+1^{\mathbf{(4)}}\\ &< \left(2^{2^{n-1}-1}\right)+\left(2^{2^{n-1}-1}\right)\\ &= \left(2^{2^{n-1}}\right).^{\mathbf{(5)}}\end{aligned}$$

Therefore, we conclude $p_n \le 2^{2^{n-1}}$, and by the principle of mathematical induction the result will hold for all n. □

Theorem 1.12 (Prime Number Theorem)**.** *If we let $\pi(n)$ be the number of primes less than or equal to n, then*

$$\pi(n) \approx \frac{n}{\log(n)},$$

for sufficiently large values of n.

In place of a proof (which is well beyond the scope of this course), table 1.1 shows values for $\pi(n)$, $n/\log(n)$, and their ratio, $\pi(n) : (n/\log(n))$, for some values up to $n = 10^{10}$.

n	$\pi(n)$	$n/\log(n)$	$\pi(n) : (n/\log(n))$
10^1	4	4.34	0.9210340
10^2	25	21.71	1.1512925
10^3	168	144.76	1.1605029
10^4	1229	1085.74	1.1319508
10^5	9592	8685.89	1.1043198
10^6	78498	72382.41	1.0844899
10^7	664579	620420.69	1.0711748
10^8	5761455	5428681.02	1.0612992
10^9	50847534	48254942.43	1.0537270
10^{10}	455052511	434294481.90	1.0477971

Table 1.1: Examining the Prime Number Theorem for $10 \le n \le 10^{10}$.

As we will see in the Fundamental Theorem of Arithmetic (theorem 1.24), prime numbers are the fundamental building blocks of the natural numbers. But, first we need to learn a little more about divisors.

1.1.3 Exercises

1.1 Calculation. Given $a = 84$ and $b = 7$, does b divide a? Find q and r such that $a = qb + r$.

1.2 Calculation. Given $a = 13$ and $b = 12$, does b divide a? Find q and r such that $a = qb + r$.

1.3 Calculation. Given $a = 98$ and $b = 32$, does b divide a? Find q and r such that $a = qb + r$.

1.4 Calculation. Given $a = 84$ and $b = 42$, does b divide a? Find q and r such that $a = qb + r$.

1.5 Calculation. Given $a = 74$ and $b = 37$, does b divide a? Find q and r such that $a = qb + r$.

1.6 Calculation. Extend example 1.5 to find the primes from 100 to 200.

1.7 Calculation. The values

$$(2) + 1 = 3, \ (2 \cdot 3) + 1 = 7, \text{ and } (2 \cdot 3 \cdot 5) + 1 = 31$$

are all prime. Find the first prime p such that $n = (2 \cdot 3 \cdot 5 \cdots p) + 1$ is not prime and then find the factors of n.

1.8 Calculation. Theorem 1.11 gives a very poor upper bound for the n^{th} prime, to see this find the 10^{th} prime number and compare its value to the upper bound given in the theorem.

1.9 Code. This code will implement the Sieve of Eratosthenes (example 1.5). Looking at the code, describe how it implements each step in the algorithm for the Sieve of Eratosthenes.

```
def sieve(Max=100):
    L=[i for i in range(2,Max+1)]
    Primes=[]
    while len(L)>0:
        Primes.append(L[0])
        New_L=L.copy()
        for i in L:
            if i%L[0]==0:
                New_L.remove(i)
        L=New_L.copy()
    return Primes
```

```
P=sieve()
print(P)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83,
89, 97, 101]
```

1.10 Claim. Divisibility is reflexive.

1.11 Claim. Given $a, b \in \mathbb{Z}$, if $a \neq 0$ and $b|a$, then $|b| \leq |a|$.

1.12 Claim. Every odd integer can be written in the form $2q - 1$ for some integer q.

1.13 Claim. The square of an odd integer is also odd.

1.14 Claim. If the square of an integer is even, then the integer is also even.

1.15 Claim. The square of an integer is divisible by 3 if and only if the integer is divisible by 3.

1.16 Claim. If $a, b \in \mathbb{Z}$ and $b|a$, then $bx|ax$ for all $x \in \mathbb{Z}$.

1.17 Claim. If $a, b \in \mathbb{Z}$ and $b|a$, then $b|a^k$ for all $k \in \mathbb{N}$.

1.18 Claim. If $a, b \in \mathbb{Z}$ and $b|a$, then $b^l|a^k$ for all $l, k \in \mathbb{N}$ with $l \leq k$.

1.19 Claim. The square of every integer can be written as either $3n$ or $3n+1$ for some integer n.

1.20 Reflection. Each of the following statements are true, similar, and related:

- If n is an even integer, then n^2 is an even integer.
- If n is an even integer, then n^2 divisible by four.
- If n is an odd integer, then n^2 is an odd integer.
- If n is an odd integer, then $n^2 - 1$ is divisible by four.
- If n is an integer, then n^2 is of the form $4n$ or $4n+1$.

In what ways are these related to one another, i.e. are they equivalent or do they imply one another? Which of these statements are *stronger* results and why?

1.2 Greatest Common Divisor

1.2.1 Definitions and Bezout's Lemma

Definition 1.5 (Greatest Common Divisor)**.** Given integers a and b, not both zero, we define the *greatest common divisor (g.c.d.)* of a and b, denoted (a, b), to be the greatest positive integer d such that $d|a$ and $d|b$.

Example 1.6. The following examples can be checked by examining all the factors of each number.

1. $(a, b) = 17$ when $a = 34$ and $b = 51$
2. $(a, b) = 1$ when $a = -68$ and $b = 95$
3. $(a, b) = 5$ when $a = 55$ and $b = 95$
4. $(a, b) = 13$ when $a = 0$ and $b = -13$
5. $(a, b) = 31$ when $a = 310$ and $b = 403$

Many ideas in Number Theory center on pairs of integers with a greatest common divisor of 1, as a consequence we give these pairs of integers a special name.

Definition 1.6 (Relatively Prime)**.** Two integers are *relatively prime* if their greatest common divisor is 1.

Here is a quick little result about greatest common divisors.

Lemma 1.13. *If* $a, b \in \mathbb{Z}$, $b > 0$ *and* $b|a$, *then* $(a, b) = b$.

Proof. Let $a, b \in \mathbb{Z}$, $b > 0$, and assume $b|a$. Since $b|b$ and $b|a$, b is a common divisor. Also, all divisors of b will be less than or equal to b. **(1)** Therefore, we conclude that $(a, b) = b$. **(2)** □

Reflection:

- How would things change if $b < 0$?
- How might we restate the theorem in order to address the case when $b < 0$?
- Under what circumstance might we have $(a, b) = b$, $b > 0$, and $a < b$?

When looking for or proving results about the greatest common divisor there are two key results we will use over and over again, *Bezout's Lemma (Theorem 1.14)* and the *Euclidean Algorithm (Theorem 1.19)*. The first characterizes the g.c.d. in a useful way that we can use to explore its properties. The latter gives an efficient way to calculate the g.c.d..

Theorem 1.14 (Bezout's Lemma)**.** *The greatest common divisor of two integers, not both zero, is equivalent to the least positive linear combination of the two integers.*

Proof. Let $a, b \in \mathbb{Z}$ and let $d = (a, b)$ be their greatest common divisor. If we let

$$S = \{ax + by > 0 | x, y \in \mathbb{Z}\},$$

then at least one of a, b, $-a$, or $-b$ is in S so that it is non-empty. (1) Let $c = ax_0 + by_0$ be the least element in S. (2) Applying Theorem 1.3 we may conclude that $d|c$ and so $0 < d \leq c$.
From the Division Algorithm (Theorem 1.4) we can write $a = qc + r$ for come unique $q, r \in \mathbb{Z}$ with $0 \leq r < c$. Since $c = ax_0 + by_0$, the remainder r will also be a linear combination of a and b:

$$\begin{aligned} r &= a - qc \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + b(-qy_0). \end{aligned}$$

If r were non-zero then we would have a contradiction. (3) Therefore, $c|a$ and by similar argument $c|b$. (4) We may now conclude that $0 < c \leq d$. (5)
Since we have shown that $c \leq d$ and $d \leq c$ we know $c = d$ and the greatest common divisor of two integers, not both zero, is equal to the least positive linear combination of the two integers. □

Reflection:

- Where in the previous proof did we use the assumption that at least one of the integers was non-zero?
- In general, why does the definition of greatest common divisor depend on at least one of the integers being non-zero?
- If both integers were zero, what would be the largest positive integer which would divide them both?

Lemma 1.15. *If $a, b, c \in \mathbb{Z}$, $c|ab$, and $(a, c) = 1$, i.e. a and c are relatively prime, then $c|b$.*

Proof. Let $a, b, c \in \mathbb{Z}$ assume that $c|ab$ and that

$$1 = (a, c) = ax + by.$$ (1)

Then we can write b as

$$b = abx + cby$$

and, since $c|ab$, conclude that $c|b$. (2) □

Lemma 1.16. *If $a, b, c \in \mathbb{Z}$, $c > 0$, and $d = (a, b)$ is the greatest common divisor of a and b, then cd is the greatest common divisor of ca and cb, i.e. $cd = (ca, cb)$.*

Proof. Assume that $a, b, c \in \mathbb{Z}$, $c > 0$, and

$$d = (a, b) = ax + by.$$ [1]

We can then write

$$cd = cax + cby$$

and conclude that $cd \geq (ca, cb)$. [2] However, since $cd|ca$ and $cd|cb$ we can conclude that $cd \leq (ca, cb)$. [3] Therefore we can conclude that $cd = (ca, cb)$ as desired. □

Reflection:

- Why did we assume that c was positive in the previous lemma?
- If we dropped the requirement that c is positive, how could we change the conclusion of the lemma and the proof so they are still true?

Lemma 1.17. *Given $a, b, c \in \mathbb{Z}$, $d = (a, b)$ divides c if and only if there exists $x, y \in \mathbb{Z}$ such that $c = ax + by$.*

Proof. Let $a, b, c \in \mathbb{Z}$ be given, assume $d = (a, b)$ and $d|c$. [1] Then, $c = qd$ and $d = ax_0 + by_0$ for some $q, x_0, y_0 \in \mathbb{Z}$. [2] From this we can say

$$c = qd = a(qx_0) + b(qy_0).$$

Thus, with $x = qx_0$ and $y = qy_0$, $c = ax + by$.
Now assume that $c = ax + by$ for some $x, y \in \mathbb{Z}$. [3] Since $a = q_a d$ and $b = q_b d$ we have

$$c = ax + by = q_a dx + q_b dy = (q_a x + q_b y)d,$$

so that $d|c$. [4]
We have shown that, $d = (a, b)$ divides c if and only if there exists $x, y \in \mathbb{Z}$ such that $c = ax + by$. □

1.2.2 The Euclidean Algorithm

Lemma 1.18. *Given $a, b, q \in \mathbb{Z}$, $(a, b) = (a - qb, b)$.*

Proof. Let $a, b, q \in \mathbb{Z}$, $d_0 = (a, b)$, and $d_1 = (a - qb, b)$. Since d_0 divides a and b, it also divides the linear combination $a - qb$ and so $d_0 \leq d_1$. [1] Similarly, since d_1 divides $a - qb$ and b, it divides the linear combination

$$a = (a - qb) + qb,$$

and thus $d_1 \leq d_0$. [2] Since $d_0 \leq d_1$ and $d_1 \leq d_0$, we conclude that $d_0 = d_1$. □

Theorem 1.19 (Euclidean Algorithm)**.** *Given non-zero integers a and b, if we let $r_0 = a$, $r_1 = b$, and for $i \geq 0$, find q_i and r_{i+2} using the Division Algorithm (Theorem 1.4) so that*

$$r_i = q_i r_{i+1} + r_{i+2}, \tag{1.1}$$

then $d = (a, b)$ is the absolute value of the last non-zero remainder.

Example 1.7. Using the Euclidean Algorithm, we can find the greatest common divisor of $a = 55$ and $b = 8$. Begin by letting $r_0 = 55$ and $r_1 = 8$ then following the recursive definition given in equation 1.1 we get the following

$$\begin{aligned} 55 &= 6 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0. \end{aligned}$$

Therefore, the greatest common divisor of $a = 55$ and $b = 8$ is $d = 1$; a and b are relatively prime.

Example 1.8. Using the Euclidean Algorithm, we can find the greatest common divisor of $a = -14$ and $b = -35$. Begin by letting $r_0 = -14$ and $r_1 = -35$ then following the recursive definition given in equation 1.1 we get the following

$$\begin{aligned} -14 &= 1 \cdot -35 + 21 \\ -35 &= -2 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Therefore, the greatest common divisor of $a = -14$ and $b = -35$ is $d = 7$.

Proof of Theorem 1.19. Let, $a, b \in \mathbb{Z}$ and rename them $r_0 = a$ and $r_1 = b$. Then we can apply the recursive definition in equation 1.1, $r_i = q_i r_{i+1} + r_{i+2}$, in order to find subsequent remainders. Note that, since $0 \leq r_{i+2} < |r_{i+1}|$, the values of the remainders decrease at each step and eventually reach zero. (1) Also, we know from lemma 1.18 that

$$(r_i, r_{i+1}) = (r_i - q_i r_{i+1}, r_{i+1}) = (r_{i+2}, r_{i+1}),$$

that is the g.c.d. is the same for all pairs of remainders. (2) If we let r_n be the last non-zero remainder, then $r_n | r_{n-1}$ so that $(r_{n-1}, r_n) = |r_n|$, and thus $(a, b) = |r_n|$. (3) □

Reflection:

- Try to find values of a and b such that the r_n from the proof is negative and so we need to use $|r_n|$ as the g.c.d..

The Euclidean Algorithm can be implemented in just a few lines of code as in figure 1.4. Note that here we took advantage of the result in exercise 1.29 rather than using the division algorithm as implemented in figure 1.1.

```python
def Euclid(a,b):
    r=[abs(a),abs(b)] # (a,b)=(|a|,|b|)
    while r[1]!=0:
        q=int(r[0]/r[1]) # find q
        r=[r[1],r[0]-q*r[1]] # update r
        print("%d=%d(%d)+%d"%(q*r[0]+r[1],q,r[0],r[1]))
    return(abs(r[0]))
```

(a) Implementation Code

```
Euclid(-14,-35)
14=0(35)+14
35=2(14)+7
14=2(7)+0
7
```

(b) Output

Figure 1.4: Euclidean Algorithm Coding

1.2.3 The Euclidean Algorithm and Bezout's Lemma

Example 1.9. Using our calculations from the Euclidean Algorithm we can find the x and y in Bezout's Lemma (Theorem 1.14) such that $(a, b) = ax + by$. To see how this works let's find x and y when $a = 55$ and $b = 8$ as in example 1.7. Looking below you can see that we first apply the Euclidean algorithm to find that (55,8)=1, then we backtrack from the bottom up to find the desired coefficients:

$$\begin{aligned} 55 &= 6 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 8 - 7^{(1)} \\ &= 8 - (55 - 6 \cdot 8)^{(2)} \\ &= 7 \cdot 8 - 55.^{(3)} \end{aligned}$$

Thus

$$ax + by = 55(-1) + 8(7) = 1$$

which was guaranteed to exist in Bezout's Lemma. However, if we let $x = 7$ and $y = -48$ we get

$$ax + by = 55(7) + 8(-48) = 385 - 384 = 1,$$

so there is more than one solution.

Example 1.10. Let's again use calculations from the Euclidean Algorithm we can find x and y as in Bezout's Lemma (Theorem 1.14), this time with $a = -14$ and $b = -35$ as in example 1.8:

$$\begin{aligned} -14 &= 1 \cdot -35 + 21 \\ -35 &= -2 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0 \end{aligned} \qquad \begin{aligned} 7 &= -35 + 2 \cdot 21^{(1)} \\ &= -35 + 2 \cdot (-14 - (-35)^{(2)} \\ &= -14(2) + (-35)(-1).^{(3)} \end{aligned}$$

And so,

$$ax + by = -14(2) + (-35)(-1) = 7$$

which was guaranteed to exist in Bezout's Lemma. However, if we let $x = -3$ and $y = 1$ we get

$$ax + by = -14(-3) + (-35)(1) = 42 - 35 = 7,$$

so there is, again, more than one solution.

In each of the previous examples we saw how we could write the g.c.d. of two integers as a linear combination of those integers, as promised by Bezout's Lemma. But we also saw that there was more than one way to do this; Theorem 1.20 characterizes all of the possible combinations.

Theorem 1.20. *If $a, b \in \mathbb{Z}$ and $c = ax_0 + by_0$, then all solutions to $c = ax + by$ are of the form*

$$x_t = x_0 + t \cdot \frac{b}{(a,b)} \text{ and } y_t = y_0 - t \cdot \frac{a}{(a,b)}, \tag{1.2}$$

for some $t \in \mathbb{Z}$.

Proof. Let $a, b, c \in \mathbb{Z}$ with $c = ax_0 + by_0$ for some integers x_0, y_0. If $d = (a, b)$, then a/d and b/d are integers. (1) Therefore,

$$x_t = x_0 + t\frac{b}{d} \text{ and } y_t = y_0 - t\frac{a}{d}$$

will be integers for any integer t. Then, the linear combination $ax_t + by_t$ is an integer and

$$\begin{aligned} ax_t + by_t &= ax_0 + t\frac{ab}{d} + by_0 - t\frac{ab}{d} \text{ (2)} \\ &= ax_0 + by_0 \text{ (3)} \\ &= c. \text{ (4)} \end{aligned}$$

Now, assume that $c = a\overline{x} + b\overline{y}$ for some integers $\overline{x}$ and $\overline{y}$, so that $ax_0 + by_0 = a\overline{x} + b\overline{y}$ and

$$a(x_0 - \overline{x}) = b(\overline{y} - y_0). \text{ (5)} \tag{1.3}$$

If we write $b = q_b d$ so that

$$a(x_0 - \overline{x}) = q_b d(\overline{y} - y_0),$$

then we can use Lemma 1.15 and exercise Claim 1.33 to conclude that a divides $d(\overline{y} - y_0)$. (6) Hence,

$$t = \frac{d(y_0 - \overline{y})}{a}, \tag{1.4}$$

is an integer and $\overline{y} = y_0 - ta/d$. (7) Substituting t from equation 1.4 into equation 1.3 and solving for $\overline{x}$ we get $\overline{x} = x_0 + tb/d$, as desired.

Thus we conclude that all possible solutions to $c = ax + by$ have the desired form. (8) □

Reflection:

- Look carefully at the structure of the proof of Theorem 1.20; how does it insure that all linear combinations can be written like the equations on line (1.2)?

Example 1.11. In example 1.9 where $a = 55$ and $b = 8$ we had

$$1 = 55(-1) + 8(7) = 55(7) + 8(-48).$$

But now, using Theorem 1.20 we can write down infinitely many integer solutions to the expression

$55x + 8y = 1$:

t	$x_t = x_0 + t\dfrac{b}{(a,b)}$	$y_t = y_0 - t\dfrac{a}{(a,b)}$
-1	$x_{-1} = -9$	$y_{-1} = 62$
2	$x_2 = 15$	$y_2 = -103$
-2	$x_{-2} = -17$	$y_{-2} = 117$
$\vdots$	$\vdots$	$\vdots$

Finally, let's look at another example of the Euclidean Algorithm, however this time we will see how we may calculate the coefficients x and y, so that $d = (a,b) = ax + by$, as we go.

Example 1.12. Using the Euclidean Algorithm find $d = (197, 21)$ and x and y such that

$$d = 197x + 21y.$$

This is similar to the previous examples except that we calculate x and y as we go.

$$\begin{aligned}
r_{k-1} &= q(r_k) + r_{k+1} & r_{k+1} &= r_{k-1} - q(r_k) \\
197 &= 9(21) + 8 & 8 &= 197 - 9(21) \\
21 &= 2(8) + 5 & 5 &= 21 - 2(8) = 197(-2) + 21(19)^{(1)} \\
8 &= 1(5) + 3 & 3 &= 8 - 1(5) = 197(3) + 21(-28)^{(2)} \\
5 &= 1(3) + 2 & 2 &= 5 - 1(3) = 197(-5) + 21(47)^{(3)} \\
3 &= 1(2) + 1 & 1 &= 3 - 1(2) = 197(8) + 21(-75)^{(4)}
\end{aligned}$$

Notice that at each step we rearranged $r_{k-1} = q(r_k) + r_{k+1}$ into $r_{k+1} = r_{k-1} - q(r_k)$ and then used the coefficients from the previous steps to write this as

$$r_{k+1} = 197x_{k+1} + 21y_{k+1}.$$

In this way we end with

$$1 = 197(8) + 21(-75)$$

without having to back track like we did in examples 1.9 and 1.10.

Example 1.13. Using the Euclidean Algorithm find $d = (130, 55)$ and x and y such that

$$d = 130x + 55y.$$

As in the previous example 1.12, we will calculate x and y as we go.

$$\begin{aligned}
r_{k-1} &= q(r_k) + r_{k+1} & r_{k+1} &= r_{k-1} - q(r_k) \\
130 &= 2(55) + 20 & 20 &= 130 - 2(55) = 130(1) + 55(-2) \\
55 &= 2(20) + 15 & 15 &= 55 - 2(20) = 130(-2) + 55(5)^{(1)} \\
20 &= 1(15) + 5 & 5 &= 20 - 1(15) = 130(3) + 55(-7)^{(2)}
\end{aligned}$$

So, we end with

$$5 = 130(3) + 55(-7)$$

again without having to back track like we did in examples 1.9 and 1.10.

What we demonstrated in examples 1.12 and 1.13 is called the *Extended Euclidean Algorithm*. The process used in these examples will work for any integers a and b, as we will show in the following theorem.

Theorem 1.21 (Extended Euclidean Algorithm)**.** *Given integers a and b, if we apply the Euclidean Algorithm (Theorem 1.19) in order to find $d = (a, b)$, then each remainder r_i in the process can be written as a linear combination of a and b.*

Proof. Let a and b be integers and let $r_0 = a$ and $r_1 = b$ as in theorem 1.19 (the Euclidean Algorithm).
Base Case ($\mathbf{i = 0, 1, 2}$): Since we can write $r_0 = a(1) + b(0)$ and $r_1 = a(0) + b(1)$, the theorem holds for $i = 0$ and 1. Further, we can write

$$r_0 = qr_1 + r_2^{(1)}$$

so that we have $r_2 = r_0 - qr_1$ which is equivalent to

$$r_2 = a(1) + b(-q).^{(2)}$$

Therefore, the theorem is true for r_2.
Induction Step: Now assume that the theorem holds for all integers up to some value k, i.e. for $0 \leq i \leq k$ we may write $r_i = ax_i + by_i$ for some integers x_i and y_i. $^{(3)}$ If we divide r_{k-1} by r_k to get $r_{k-1} = qr_k + r_{k+1}$, then we can rewrite this as

$$\begin{aligned} r_{k+1} &= r_{k-1} - qr_k \\ &= (ax_{k-1} + by_{k-1}) - q(ax_k + by_k)^{(4)} \\ &= a(x_{k-1} - qx_k) + b(y_{k-1} - qy_k)^{(5)} \\ &= ax_{k+1} + by_{k+1} \end{aligned}$$

where $x_{k+1} = x_{k-1} - qx_k$ and $y_{k+1} = y_{k-1} - qy_k$. Therefore, by the principle of mathematical induction, the theorem will hold for all k in the natural numbers. □

The code in figure 1.5 implements the *Extended Euclidean Algorithm* using the process described in the induction step of Theorem 1.21. Notice the output matches the work we did in example 1.13. Also, here we used the division algorithm function (figure 1.1) rather than the trick we used when implementing just the regular Euclidean Algorithm (figure 1.4); why do you think this is the case?

1.2.4 Exercises

For calculations 1.21 through 1.25 use the *Euclidean Algorithm* to find $d = (a, b)$ for the given pairs of values, and then write two solutions to $d = ax + by$. When finding the initial pair of values for x and y you can either back track from the end of the Euclidean Algorithm or use the Extended Euclidean Algorithm to calculate them as you go. (Hint: Look carefully at examples 1.7 through 1.13.)

1.21 Calculation. $a = 82$ and $b = 40$.

1.22 Calculation. $a = 72$ and $b = 27$.

```
def Ext_Euclid(a,b):
    R=[a,b] # Set a,b to r_0 and r_1
    x=[1,0] # a=1*r_1+0*r_2
    y=[0,1] # b=0*r_1+1*r_2
    while R[1]!=0:
        q,r=divAlg(R[0],R[1]) # Get q and r
        R=[R[1],r] # Update the r's
        x=[x[1],x[0]-q*x[1]] # Update the x's
        y=[y[1],y[0]-q*y[1]] # Update the y's
        print("%d=%d(%d)+%d(%d)"%(R[0],a,x[0],b,y[0]))
    return abs(R[0]),x[0],y[0]
```

(a) Implementation Code

```
Ext_Euclid(130,55)
55=130(0)+55(1)
20=130(1)+55(-2)
15=130(-2)+55(5)
5=130(3)+55(-7)
(5, 3, -7)
```

(b) Output

Figure 1.5: Extended Euclidean Algorithm

1.23 Calculation. $a = 23$ and $b = 92$.

1.24 Calculation. $a = 88$ and $b = 40$.

1.25 Calculation. $a = 82$ and $b = 5$.

1.26 Calculation. The greatest common divisor of 51 and 33 is 3. Use this information to write 15 as a linear combination of 51 and 33. (Hint: Look carefully at theorem 1.17 and its proof.)

1.27 Calculation. The greatest common divisor of 780 and 165 is 15. Use this information to write 75 as a linear combination of 780 and 165. (Hint: Look carefully at theorem 1.17 and its proof.)

1.28 Code. For each of these refer to the code in figure 1.5 and the proof of theorem 1.21.

1. In the proof we calculate $r_{k+1} = r_{k-1} - qr_k$, where in the code is this carried out?

2. Likewise where does the code calculate $x_{k+1} = x_{k-1} - qx_k$ and $y_{k+1} = y_{k-1} - qy_k$?

3. The inductively defined process in the proof requires us to keep track of the previous two values of r, x, and y, how does the code manage this?

1.29 Claim. If $a, b \in \mathbb{Z}$, then $(a, b) = (|a|, |b|)$.

1.30 Claim. If two integers, a and b, are relatively prime then for all integers, c, there exists x and y such that $c = ax + by$.

1.31 Claim. If $a, b, c \in \mathbb{Z}$ and c divides both a and b, then c divides (a, b).

1.32 Claim. If $a, b, c \in \mathbb{Z}$, $d = (a, b)$ and $c|d$, then $d/c = (a/c, b/c)$.

1.33 Claim. If $a, b \in \mathbb{Z}$ and $d = (a, b)$, then $(a/d, b/d) = 1$.

1.3 Fundamental Theorem of Arithmetic

1.3.1 The Fundamental Theorem

In this section we focus on proving the Fundamental Theorem of Arithmetic (Theorem 1.24) which demonstrates how prime numbers are the building locks of all integers. We begin by refining and extending Lemma 1.15, Claim 1.17, and Claim 1.14 specifically for prime numbers.

Lemma 1.22. *If a prime integer divides a product of two integers, then it divides at least one of the factors.*

Proof. Let a and b be integers and p be a prime integer which divides ab. If p divides a we are done. Suppose that p does not divide a, then $(a, p) = 1$. (1) Therefore, we may write $1 = ax + py$ so that $b = abx + pby$. (2) Thus, since $p|ab$, we know $p|abx + pby = b$. (3) □

Corollary 1.23. *If $a_i \in \mathbb{Z}$ for all $1 \leq i \leq n$ and for some $n \in \mathbb{N}$, and a prime p divides the product of the a_i, then $p|a_j$ for some j.*

Proof.
Base Case ($\mathbf{n = 1, 2}$): If there is only a single factor a_1 in the product and $p|a_1$, then it is true $p|a_1$. If $n = 2$ so that $p|a_1a_2$, then, by Lemma 1.22, $p|a_1$ or $p|a_2$. (1)
Induction Step ($\mathbf{n \geq 1}$): Assume that for any set of integers $\{a_1, a_2, \ldots, a_k\}$ with $1 \leq k \leq n-1$, if $p|(a_1a_2 \cdots a_k)$, then $p|a_j$ for some $1 \leq j \leq k$. (2) Now suppose that

$$p|(a_1a_2 \cdots a_{n-1} \cdot a_n)$$

for some set of integers $\{a_1, a_2, \ldots, a_n\}$. Let $a = (a_1a_2 \cdots a_{n-1})$, so we may write $p|a \cdot a_n$. Then by lemma 1.22, $p|a$ or $p|a_n$. If $p|a_n$, then we are done. (3) If not, then we apply the induction assumption in order to conclude that $p|a_j$ for some $1 \leq j \leq n-1$. (4)
Therefore, by the principle of mathematical induction, if a prime divides any finite product of integers, then it must divide at least one of the factors. □

Reflection:

- In the previous proof, did we explicitly assume that the a_i were different from one another?
- Why doesn't it matter if some or all of the a_i are the same?

Theorem 1.24 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than one is either prime or may be written uniquely as a product of primes.*

Proof. Let n be a natural number. If n is prime, then we are done. (1) Suppose that n is the least composite which we have not written as a product of primes. (2) By lemma 1.9 n is divisible by some prime p; $n = qp$ for a unique quotient q. (3) If q is prime then $n = qp$ is a product of primes. If q is composite then, since we assumed n was the least composite not written as a product of

primes, we may write q, and thus n, as a product of primes. (4)
Now suppose that n has two prime factorization

$$n = p_1 p_2 p_3 \cdots p_r$$

and

$$n = q_1 q_2 q_3 \cdots q_s.$$

with $r \leq s$. (5) Then,

$$p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$$

and we get that p_1 divides some q_i by corollary 1.23. Without loss of generality assume $i = 1$ so that $p_1 | q_1$. (6) However, for all i, q_i is prime hence $p_1 = q_1$. (7) Canceling the first factors we get

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

Proceeding in this way we can cancel each p_i until we are left with

$$1 = q_{s-r} \cdots q_s.$$ (8)

If $s > r$ this would be a contradiction, (9) therefore $s = r$ and the prime factorizations are the same.
So we have shown that every natural number greater than 1 is either prime or is a composite which may be written uniquely as a product of primes. □

1.3.2 Factoring Integers

Lemma 1.25. *Every composite natural number has a prime factor which is less than or equal to its square root.*

Example 1.14. Before we look at the proof of lemma 1.25 consider the following examples.

1. With $n = 42 = 3 \cdot 7 \cdot 2$, compare prime factors to $\sqrt{n}$:

$$2 < 3 < 6.4807\ldots < 7$$

2. With $n = 126 = 3 \cdot 2 \cdot 7 \cdot 3$, compare prime factors to $\sqrt{n}$:

$$2 < 3 < 3 < 7 < 11.2249\ldots$$

3. With $n = 10 = 5 \cdot 2$, compare prime factors to $\sqrt{n}$:

$$2 < 3.1622\ldots < 5$$

4. With $n = 6 = 2 \cdot 3$, compare prime factors to $\sqrt{n}$:

$$2 < 2.4494\ldots < 3$$

Reflection:

- In the examples, was there always a prime factor less than the square root as predicted?
- Was there always a prime factor greater than the square root?
- Under what circumstances were we guaranteed to be a prime factor greater than the square root?
- Will a composite number always have a factor greater then its square root?

Proof. Let $n \in \mathbb{N}$ with prime factors p and q so that $pq|n$. (1) Suppose that both these factors are greater then $\sqrt{n}$. (2) Then we have

$$pq > p\sqrt{n} > \sqrt{n}^2 = n$$

which is a contradiction. (3) Therefore, we know that every composite natural number has at least one prime factor less than or equal to its square root. □

Put in simple divisibility tests, $1, 2, 2^k, 3, 5, 9$

Put in stuff about using the Euclidean algorithm to try and find factors fast, i.e. if a number if divisible by 2,3,5,7 or 11 then its gcd with 2310=2*3*5*7*11 will be greater than 1. Or if you randomly try numbers and compute gcds you can try and find factors.

Fermat?

Pollard Roe?

1.3.3 Exercises

In each of the exercises 1.34 to 1.38 find the unique prime factorization of n.

1.34 Calculation. $n = 3528$

1.35 Calculation. $n = 7875$

1.36 Calculation. $n = 16302$

1.37 Calculation. $n = 56595$

1.38 Calculation. $n = 14535$

For exercises 1.39 to 1.42 for the given n, find p such that $\sqrt{n} < p$.

1.39 Calculation. $n = 2 \cdot 3 \cdot p$

1.40 Calculation. $n = 7 \cdot 31 \cdot p$

1.41 Calculation. $n = 2 \cdot 11 \cdot 13 \cdot p$

1.42 Calculation. $n = 5 \cdot 19 \cdot \cdot 31 \cdot p$

1.43 Claim. If $p, n \in \mathbb{Z}$, p is prime, and $p|n$, then $p^k|n^k$ for all $k \in \mathbb{N}$.

1.44 Claim. If $p, n \in \mathbb{Z}$, p is prime, and for some k $p|n^k$, then $p|n$.

1.45 Claim. If $p, n \in \mathbb{Z}$, p is prime, and $p|n$, then $p^l|n^k$ for all $l, k \in \mathbb{N}$ with $l \leq k$.

1.46 Claim. Given $p, n \in \mathbb{Z}$, p prime, $p|n^k$ if and only if $p^k|n^k$.

1.47 Claim. Given $a, b \in \mathbb{Z}$, $a, b \neq 0$, if for some $n \in \mathbb{N}$, $a^n | b^n$, then $a|b$.

1.48 Claim. Given $a, b \in \mathbb{Z}$, $a, b \neq 0$, $a|b$ if and only if $a^k | b^k$ for all $k \in \mathbb{N}$.

1.49 Claim. Every composite natural number has a factor greater than or equal to its square root.

1.50 Code. Answer the following by referencing the code in figure 1.6.

1. The code looks for the g.c.d. of n and another number, why is this better than just trying to divide n by the random numbers? That is why is this more likely to find factors using fewer loops?

2. In what way *might* we improve the efficiency of this code using some of what we learned about primes?

3. What will this code return whenever you input a prime?

```
def poor_tester(n):
    sn=ceil(sqrt(n))
    trials = 0
    max_trials = ceil(sn/4)
    Comparisons=[]
    Factor=n
    while trials<max_trials and Factor==n:
        Test=rd.choice(range(sn))
        if Test not in Comparisons:
            Comparisons.append(Test)
            if 1<gcd(n,Test)<n:
                Factor=gcd(n,Test)
            else: trials+=1
    return Factor,int(n/Factor)
```

(a) Implementation Code

The code tries to find factors of a given number n by randomly testing one quarter of all the numbers from 0 to $\sqrt{n}$ as follows: For each number $Test$ tested

1. Find $d = (Test, n)$

2. If $1 < d < n$, return $(d, n/d)$

3. If $d = 1$, choose new $Test$

(b) Description

Figure 1.6: A Poor Factorization Algorithm

1.51 Reflection. Looking at exercises 1.43 to 1.46, which of these require a prime number and which can be extended to be true for any pair of numbers? If they can be extended, what would their statements be?

1.52 Reflection. Why is the claim in exercise 1.47 trickier to prove than the claim in exercise 1.48?

1.53 Reflection. A classic example of a fallacious proof by induction is the proof that all horses are the same color. Look up an example of this proof and compare it to the proof of Corollary 1.23. What insures the proof in the corollary works while the proof about horses does not? (Hint: How do their base cases differ?)

1.54 Reflection. Looking at exercises 1.39 to 1.42, what theorem did we learn about earlier that will guarantee that we can always find a solution to this type of problem?

1.4 Least Common Multiple

1.4.1 A Definition and Two Quick Results

Definition 1.7 (Least Common Multiple)**.** Given $a, b \in \mathbb{Z}$ the *least common multiple* of a and b, denoted $[a, b]$, is the least positive integer l such that $a|l$ and $b|l$.

Example 1.15. Find the least common multiple of $a = 69$ and $b = 46$. The product of two integers is always divisible by both, so we know the l.c.m. is no greater than $69 \times 46 = 3174$. Also, it can't be smaller than the larger of the two numbers, so in this case it is no less than $a = 69$. One strategy might be to look at all the multiples of a and b up to 3174 until we find one they share:

i	1	2	3	4	5	6	7	8	9	...
$46i$	46	92	**138**	184	230	276	322	368	414	...
$69i$	69	**138**	207	276	345	414	483	552	621	...

Table 1.2: Multiples of $a = 69$ and $b = 46$

In this case we quickly find $l = [a, b] = 138$. But, this isn't a particularly good strategy.

Example 1.16. Find the least common multiple of $a = 67$ and $b = 47$. These are only slightly different from the values in the previous example, so we can try the same strategy. The product of two integers is $67 \times 47 = 3149$ and the larger of the two numbers is $a = 67$; we examine multiples of a and b between 67 and 3149.

i	1	2	3	4	5	6	$\cdots$	46	47	$\cdots$	66	67
$47i$	47	94	141	188	235	282	$\cdots$	2162	2209	$\cdots$	3102	**3149**
$67i$	67	134	201	268	335	402	$\cdots$	3082	**3149**	$\cdots$	4422	4489

Table 1.3: Multiples of $a = 67$ and $b = 47$

Unfortunately, this time we end up looking at 47 different multiples of $a = 67$ before discovering that the l.c.m. is $l = [a, b] = 3149$.

As the previous two examples demonstrate, trial and error is not a reliable way to try and find the least common multiple of two numbers. The following results will give us a much better way to find the l.c.m. of two integers.

Lemma 1.26. *The least common multiple of two integers divides all other common multiples.*

Proof. Let $a, b, m \in \mathbb{Z}$, assume that a and b both divide m, and finally, let $l = [a, b]$, the least common multiple. Taking $m = ql + r$ with $0 \leq r < l$ we can write $r = m - ql$. (1) Now applying lemma 1.3 we conclude that r is divisible by both a and b. (2) Since, l is the least common multiple, we conclude that $r = 0$ and $l|m$. (3) Therefore, every common multiple of a and b is divisible by $l = [a, b]$. □

Example 1.17. Looking back at example 1.16 with $a = 67$, $b = 47$, and $a \times b = 3149$, lemma 1.26 tells us that to find $l = [a, b]$ we just need to look at the factors of 3149. The only factors of 3147 are 1, 47, 67, and 3147; only 3147 is a common multiple so we know $l = 3147$.

While this gives us a must faster result in this case, this strategy could still be hit or miss. The real benefit of lemma 1.26 is that is helps us prove theorem 1.27 which connects the l.c.m. to the g.c.d. so that we could use the Euclidean Algorithm to find the l.c.m..

Theorem 1.27. *The absolute value of the product of two non-zero integers is equal to the product of their g.c.d. and l.c.m.; given* $\forall a, b \in \mathbb{Z}$ *if* $a, b \neq 0$, *then* $|a \cdot b| = (a, b)[a, b]$.

Proof. Let a and b be non-zero integers, $d = (a, b)$, and $l = [a, b]$. We will consider the case when a and b are positive; for negative values consider their absolute values and follow the same proof. By lemma 1.26, $ab = ql$ for some unique q. (1) Note that $a|l$ and $b|l$, thus $a = q(l/b)$, $b = q(l/a)$, and we conclude that q divides a and b. (2) Therefore,

$$ab = ql \leq dl.^{(3)}$$

Next, since d divides a and b, there exists a unique q' such that $q'd = ab$. (4) Then we have

$$q' = a\left(\frac{b}{d}\right) = b\left(\frac{a}{d}\right),$$

that is q' is a common multiple of a and b. (5) From this we conclude that

$$dl \leq q'd = ab.^{(6)}$$

Finally, since it is the case that $ab \leq dl$ and $dl \leq= ab$, we conclude that $ab = dl$. □

Example 1.18. Let $a = 210$ and $b = 165$ and find their least common multiple $l = [a, b]$. First we find their g.c.d., $d = (a, b)$, using the Euclidean Algorithm:

$$\begin{aligned} 210 &= 1(165) + 45 \\ 165 &= 3(45) + 30 \\ 45 &= 1(30) + 15 \\ 30 &= 2(15) + 0. \end{aligned}$$

Then, applying lemma 1.27, we get $l = [a, b] = ab/d$ and thus $l = 2310$. So, we can now find the l.c.m. without having to use any sort of trial and error.

In section 1.3 we will see how to use the prime factors of two numbers, which are unique according to the Fundamental Theorem of Arithmetic (theorem 1.24), to find the l.c.m. and g.c.d.. It is tempting to consider this a more efficient method than any of the above approaches, including example 1.18 where we used the Euclidean Algorithm. However, identifying the factors of a number is not always practical for the sorts of large numbers used in real world applications. To help understand this consider the following example where we use the same strategy as example 1.18.

Example 1.19. Use theorem 1.27 and the Euclidean Algorithm to find the l.c.m of $a = 91349$ and $b = 48683$. If we begin by finding the g.c.d. of a and b using the Euclidean Algorithm:

$$\begin{aligned} 91349 &= 1(48683) + 42666 \\ 48683 &= 1(42666) + 6017 \\ 42666 &= 7(6017) + 547 \\ 6017 &= 11(547) + 0. \end{aligned}$$

With the value $d = (a, b) = 547$ found we can now apply theorem 1.27 to get

$$l = [a, b] = ab/d = 8130061.$$

Reflection:

- In corollary 1.28 we learn how to use the factors of two numbers to identify their g.c.d. and l.c.m.. To understand why this is an interesting, but less than practical strategy in general try to find the factors of $a = 91349$ and $b = 48683$.
- Or try and find the factors of two even larger numbers like $a = 2674590683$ and $b = 4589793251$.
- When you get tired of looking for factors of $a = 2674590683$ and $b = 4589793251$, try using the Euclidean Algorithm to find their g.c.d. and l.c.m. instead; only 9 iterations are needed to find the greatest common divisor.

Lemma 1.28. *Finding (a, b) and $[a, b]$ (maybe make on an exercise.)*

Lemma 1.29. $d = (a, b) \to d^n = (a^n, b^n)$

1.4.2 Exercises

In exercises 1.55 to 1.60, a and b always refer to natural numbers, also assume $d = (a, b)$ and $l = [a, b]$.

1.55 Calculation. Given $a = 60$ and $b = 21$ find values for $d = (a, b)$ and $l = [a, b]$.

1.56 Calculation. Given $a = 51$ and $b = 34$ find values for $d = (a, b)$ and $l = [a, b]$.

1.57 Calculation. Given $d = 11$ and $a = 77$ find possible values for b and $l = [a, b]$.

1.58 Calculation. Given $d = 14$ and $b = 7$ find possible values for a and $l = [a, b]$.

1.59 Calculation. Given $l = 190$ and $a = 95$ find possible values for b and $d = (a, b)$.

1.60 Calculation. Given $d = 5$ and $l = 680$ find possible values for a and b.

1.61 Reflection. Looking at 1.55 through 1.60, which ones had unique solutions and which did not? Why?

1.62 Claim. Given the least common multiple of two integers a and b, $l = [a, b]$, prove that there exists x and y such that $l = ax + by$.

Chapter 2

Modular Mathematics

2.1 Equivalencies

Definition 2.1 (Modular Equivalence)**.** Given $a, b, n \in \mathbb{Z}$ with $n \neq 0$, we say a *is equivalent to* b *modulo* n, $a \equiv b \pmod{n}$, if and only if $n|(a-b)$.

Example 2.1. For the given $a, b, n \in \mathbb{Z}$ decide if $a \equiv b \pmod{n}$:

1. $12 \equiv 33 \pmod{7}$ since $7|(12-33)$ ✓
2. $45 \not\equiv 13 \pmod{7}$ since $7 \not| (45-13)$ ✗
3. $4 \equiv -6 \pmod{5}$ since $5|4-(-6)$✓
4. $13 \not\equiv -7 \pmod{15}$ since $15 \not| (13-(-7))$ ✗
5. $4 \underline{\quad} 19 \pmod{5}$ since $\underline{\qquad\qquad\qquad}$
6. $73 \underline{\quad} 25 \pmod{12}$ since $\underline{\qquad\qquad\qquad}$
7. $17 \underline{\quad} -39 \pmod{7}$ since $\underline{\qquad\qquad\qquad}$
8. $75 \underline{\quad} 9 \pmod{6}$ since $\underline{\qquad\qquad\qquad}$

Theorem 2.1. *Modular equivalence is an equivalence relation.*

Proof. Given $a, b, c, n \in \mathbb{Z}$ with $n \neq 0$, it is clear that $n|(a-a)$ **(1)** and that if $n|(a-b)$, then $n|(b-a)$; **(2)** thus the relation is reflexive and symmetric. **(3)** Now, suppose $n|(a-b)$, $(a-b) = q_0 n$, and $n|(b-c)$, $(b-c) = q_1 n$. **(4)** Then,

$$\begin{aligned}
(a-c) &= (a-b+b-c)^{(5)} && (2.1)\\
&= q_0 n + q_1 n^{(6)} && (2.2)\\
&= (q_0+q_1)n && (2.3)
\end{aligned}$$

and therefore $n|(a-c)$; modular equivalence is transitive. **(7)** We therefore see that modular equivalence is an equivalence relation. □

Lemma 2.2. *Given $a, b, n, l \in \mathbb{Z}$, $l, n > 0$, and assuming $l|n$, if $a \equiv b \pmod{n}$, then $a \equiv b \pmod{l}$.*

Proof. Let $a, b, n, l \in \mathbb{Z}$, $l, n > 0$, and assume $l|n$. Further assume $a \equiv b \pmod{n}$ so that $a - b = qn$.$^{(1)}$ Then we can write

$$a - b = q(q'l) = (qq')l$$

for some $q' \in \mathbb{Z}$.$^{(2)}$ Therefore, $a \equiv b \pmod{l}$ as desired.$^{(3)}$ □

Lemma 2.3. *Given $a, b, m, n \in \mathbb{Z}$, $n, m > 0$; $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{[n, m]}$.*

Proof. Let $a, b, m, n \in \mathbb{Z}$ and $n, m > 0$. Assume $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$ so that

$$a - b = q_n n = q_m m$$

for appropriate q_n and q_m.$^{(1)}$ Then, by lemma 1.26, $[m, n]|(a - b)$ and $a \equiv b \pmod{[a, b]}$.$^{(2)}$ The converse is left as an exercise for the reader. (Exercise 2.24) □

Corollary 2.4. *Given $a, b, m, n \in \mathbb{Z}$, $n, m > 0$, and $(n, m) = 1$; if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{nm}$.*

The proof of Corollary 2.4 is left to the reader in exercise 2.25.

Example 2.2. Look at the following examples for which $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$, in which cases is $a \equiv b \pmod{nm}$ and in which is only $a \equiv b \pmod{[a, b]}$ true?

1. $17 \equiv 7 \pmod{5}$ and $17 \equiv 7 \pmod{2}$ are they congruent modulo $5 \cdot 2 = 10$? Yes ✔

2. $25 \equiv 1 \pmod{6}$ and $25 \equiv 1 \pmod{8}$ are they congruent modulo $6 \cdot 8 = 48$? No ✗

3. $162 \equiv 12 \pmod{10}$ and $162 \equiv 12 \pmod{15}$ are they congruent modulo $10 \cdot 15 = 150$? Yes ✔

4. $84 \equiv 7 \pmod{11}$ and $84 \equiv 7 \pmod{7}$ are they congruent modulo $11 \cdot 7 = 77$? ____________

5. $25 \equiv 85 \pmod{6}$ and $25 \equiv 85 \pmod{10}$ are they congruent modulo $6 \cdot 10 = 60$? ____________

6. $31 \equiv 7 \pmod{12}$ and $31 \equiv 7 \pmod{8}$ are they congruent modulo $12 \cdot 8 = 96$? ____________

Reflection:

- Looking at the examples, why is it that Corollary 2.4 is not a biconditional?

2.2 Arithmetic and Linear Equations

The following function will justify proving results for modular arithmetic while only considering values between 0 and a given modulus n.

Theorem 2.5. *Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $r_a = r_b$, where $a = q_a n + r_a$ and $b = q_b n + r_b$ as in the Division Algorithm (Theorem 1.4, p. 9).*

The proof of the Theorem 2.5 is a straightforward application of the definition of modular equivalence and the Division Algorithm and so is left as exercise 2.28.

Theorem 2.6 (Modular Arithmetic)**.** *Given $a, b, c, d, n \in \mathbb{Z}$, $n > 0$, if*

$$a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n},$$

then:

1. $a + c \equiv b + d \pmod{n}$,
2. $a - c \equiv b - d \pmod{n}$, *and*
3. $ac \equiv bd \pmod{n}$.

The proofs that addition and subtraction are well defined are fairly straight forward and are left to the reader (exercise 2.23). Here we look at the proof that multiplication is well defined.

Proof. Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$ with

$$a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n}.$$

Then $a - b = q_0 n$ and $c - d = q_1 n$ for some $q_0, q_1 \in \mathbb{Z}$. [(1)] Then

$$\begin{aligned} ac - bd &= ac - bc + bc - bd^{(2)} && (2.4)\\ &= (a - b)c + (c - d)b && (2.5)\\ &= (q_0 c)n + (q_1 b)n^{(3)} && (2.6)\\ &= (q_0 c + q_1 b)n, && (2.7) \end{aligned}$$

and $ac \equiv bd \pmod{n}$. [(4)] □

Division, in the sense of the Division Algorithm (Theorem 1.4, p.9) or in the rational numbers, $\mathbb{Q}$, is in general well defined because of the *zero product property*, $ab = 0$ if and only if $a = 0$ or $b = 0$. However, this property is not a given when working with integers modulo n.

Definition 2.2 (Zero Divisors)**.** Given $a, b, n \in \mathbb{Z}$, $n > 0$, and $a, b \neq 0$, if $ab \equiv 0 \pmod{n}$, then we say they are *zero divisors* modulo n.

Example 2.3. For each given set of numbers, a, b, n, determine if a and b and zero divisors modulo n:

1. $a = 5$, $b = 6$, $n = 10$: $5 \cdot 6 \equiv 0 \pmod{10}$, Yes ✓
2. $a = 7$, $b = 3$, $n = 6$: $7 \cdot 3 \equiv 3 \pmod{6}$, No ✗
3. $a = 8$, $b = 5$, $n = 11$: $8 \cdot 5 \equiv 7 \pmod{11}$, No ✗
4. $a = 10$, $b = 14$, $n = 70$: $10 \cdot 14 \equiv 0 \pmod{70}$, Yes ✓
5. $a = 13$, $b = 5$, $n = 23$: ________________________________
6. $a = 5$, $b = 6$, $n = 15$: ________________________________
7. $a = 14$, $b = 17$, $n = 34$: ________________________________
8. $a = 30$, $b = 12$, $n = 31$: ________________________________

Reflection:

- Looking at the examples above, what can we say about the modulus n each time there are zero divisors?
- Is there any particular pattern to the modulus n when we didn't have zero divisors?
- Look at exercise 2.26 for the general conclusion.

Definition 2.3 (Inverses)**.** Given $a, b, n \in \mathbb{Z}$, $n > 0$, we say that

1. a and b are *additive inverses* modulo n if and only if $a + b \equiv 0 \pmod{n}$, and
2. a and b are *multiplicative inverses* modulo n if and only if $ab \equiv 1 \pmod{n}$.

For the additive inverse of a we normally write $-a$ and for the multiplicative inverse a^{-1}.

Finding additive inverses is done with subtraction, i.e. $-a \equiv n - a \pmod{n}$. Multiplicative inverses are a little trickier, but, when they exist we can use the *Euclidean Algorithm* (Theorem 1.19, p. 20) to find them.

Example 2.4. Let $n = 17$ and $a = 5$, then using the Euclidean Algorithm we can write

$$5(7) + 17(-2) = 1,$$

and then $5(7) \equiv 1 \pmod{17}$. Therefore, $5^{-1} \pmod{17} = 7$.

Similarly, again with $n = 17$, if $a = 8$, then

$$8(-2) + 17(1) = 1,$$

so that $8(-2) \equiv 1 \pmod{17}$. Thus $8^{-1} \equiv -2 \equiv 15 \pmod{17}$.

Lemma 2.7. *Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then a has a multiplicative inverse a^{-1} modulo n if and only if they are relatively prime.*

Proof. Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$, and assume there exists a multiplicative inverse a^{-1}. Then we may write

$$\left(a \cdot a^{-1}\right) - 1 = qn^{(1)}$$

or equivalently

$$\left(a \cdot a^{-1}\right) - qn = 1.$$

However, by Bezout's Lemma (p. 18) this is possible if and only if $d = (a, n) = 1$. (2) □

Reflection:

- The previous lemma is a biconditional, why are there not two parts to this proof as with other biconditionals we have looked at?

We can generalize lemma 2.7 to include the case when $d = (a, n) > 1$ with an almost identical proof.

Lemma 2.8. *Given $a, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, the equation*

$$ax \equiv c \pmod{n}$$

has a solution if and only if $d = (a, n)$ divides c.

Proof. Let $a, c \in \mathbb{Z}$, $n \in \mathbb{N}$, and assume that for some $x_0 \in \mathbb{Z}$

$$ax_0 \equiv c \pmod{n}.$$

Then we may write

$$ax_0 - c = qn \text{ or } ax_0 - qn = c.$$

By lemma 1.17 (p. 19) this is true if and only if $d = (a, n)$ divides c. □

The following theorem, while more general, is an immediate consequence of the previous lemma. As such, the proof of Theorem 2.9 is left for the reader as exercise 2.27.

Theorem 2.9. *Given $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, the equation*

$$ax + b \equiv c \pmod{n}$$

has a solution if and only if $d = (a, n)$ divides $c - b$.

We end this section by looking at how we can solve basic systems of equations with modular arithmetic.

Theorem 2.10 (Chinese Remainder Theorem)**.** *Given* $m_1, m_2, \cdots, m_k \in \mathbb{N}$ *such that* $(m_i, m_j) = 1$ *when* $i \neq j$ *(they a pairwise relatively prime) and the system of equations:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} && (2.8)\\ x &\equiv a_2 \pmod{m_2} && (2.9)\\ &\vdots \qquad\quad \vdots && (2.10)\\ x &\equiv a_k \pmod{m_k}, && (2.11) \end{aligned}$$

there exists a unique solution modulo $M = m_1 m_2 \ldots m_k$.

The proof we will look at for this is constructive, so it will be beneficial to look at an example first.

Example 2.5. Let's construct a solution to

$$\begin{aligned} x &\equiv 1 \pmod 3 && (2.12)\\ x &\equiv 3 \pmod 5 && (2.13)\\ x &\equiv 2 \pmod 7. && (2.14) \end{aligned}$$

First we let $M = 3 \cdot 5 \cdot 7$, $M_1 = M/3 = 35$, $M_2 = M/5 = 21$, and $M_3 = M/7 = 15$. Next we need the inverses of M_1, M_2, and M_3 modulo 3, 5, and 7 respectively:

$$\begin{aligned} M_1^{-1} \pmod 3 &= 35^{-1} \pmod 3 = 2^{-1} \pmod 3 = 2 && (2.15)\\ M_2^{-1} \pmod 5 &= 21^{-1} \pmod 5 = 1^{-1} \pmod 5 = 1 && (2.16)\\ M_3^{-1} \pmod 7 &= 15^{-1} \pmod 7 = 1^{-1} \pmod 7 = 1, && (2.17) \end{aligned}$$

This is where we needed to know the moduli were relatively prime. Now we can construct our solution:

$$\begin{aligned} x &\equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} \pmod M && (2.18)\\ &\equiv 1 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105} && (2.19)\\ &\equiv 70 + 63 + 30 \pmod{105} && (2.20)\\ &\equiv 63 - 5 \pmod{105} && (2.21)\\ &\equiv 58 \pmod{105}. && (2.22) \end{aligned}$$

Which we can verify is the solution since

$$58 = 19 \cdot 3 + 1 = 11 \cdot 5 + 3 = 8 \cdot 7 + 2,$$

and it is unique because we reduced modulo $M = 105$ which is the least common multiplier of the individual moduli.

Now the proof of the Chinese Remainder Theorem follows the same steps as the example.

Proof. Let $m_1, m_2, \cdots, m_k \in \mathbb{N}$ such that $(m_i, m_j) = 1$ when $i \neq j$ (they a pairwise relatively prime) and consider the system of equations:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} && (2.23)\\ x &\equiv a_2 \pmod{m_2} && (2.24)\\ &\vdots \qquad\quad \vdots && (2.25)\\ x &\equiv a_k \pmod{m_k}. && (2.26) \end{aligned}$$

Let $M = m_1 m_2 \dots m_k$ and for each i define $M_i = M/m_i$. Note that, since the m_i are pairwise relatively prime, $(m_i, M_i) = 1$ for all i. (1) Now for each i find $M_i^{-1} \pmod{m_i}$, which exists by lemma 2.7. We now construct x:

$$x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1} \pmod{M}. \tag{2.27}$$

We can see that x is a solution by noting that for $i \neq j$ $M_j \equiv 0 \pmod{m_i}$,(2) so that $x \equiv a_i M_i M_i^{-1} \pmod{m_i}$. However, by construction, $M_i M_i^{-1} \equiv 1 \pmod{m_i}$,(3) and so $x \equiv a_i \pmod{m_i}$ as desired.
Finally, if x and y are solutions modulo M. Then for all i, $x \equiv y \equiv a_i \pmod{m_i}$. (4) However, using corollary 2.4 (p.34), we can conclude that $x \equiv y \pmod{M}$. (5) That is, the solution is unique.

□

2.3 Functions

Lemma 2.11. *Given a prime $p \in \mathbb{N}$ the only $a \in \mathbb{Z}$ such that $a^2 \equiv 1 \pmod{p}$ are equivalent to either 1 or $p-1$.*

Proof. Let $p \in \mathbb{N}$ be prime, $a \in \mathbb{Z}$, assume that $a^2 \equiv 1 \pmod{p}$, and $1 \leq a \leq p-1$. Then we may write

$$qp = a^1 - 2 = (a-1)(a+1)^{(1)}$$

and note that $p|(a-1)$ or $p|(a+1)$. (2) However, since $1 \leq a \leq p-1$, $(a-1)$ and $(a+1)$ are in the range from 0 to p. (3) Therefore, either $a-1=0$ so that $a=1$, or $a+1=p$ so that $a=p-1$. (4)
To extend this to the rest of the integers, note that every integer is equivalent to a unique remainder between 0 and $p-1$. (5) Hence, given an arbitrary $a \in \mathbb{Z}$, first reduce it to its equivalent remainder, then apply the previous argument. □

Theorem 2.12 (Wilson's Theorem)**.** *Given $p \in \mathbb{N}$ prime, $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Let $p \in \mathbb{N}$ be prime. Since p is prime every integer $1 \leq a \leq (p-1)$ has an inverse. (1) By lemma 2.11 only 1 and $p-1$ are their own inverses (2) and so we may pair up the other inverses and cancel them off in the product $(p-1)! \pmod{p}$:

$$(p-1)! = (p-1)(p-2)\cdots 2 \cdots 1 \equiv (p-1)\cdot 1 \equiv (p-1) \pmod{p}.^{(3)} \tag{2.28}$$

Since $p-1 \equiv -1 \pmod{p}$ we can conclude that $(p-1)! \equiv -1 \pmod{p}$. □

For the next lemma, and subsequent results, it will be convenient to use Theorems 2.6 and 2.1 to define a new set on which addition, subtraction, and multiplication, are well defined.

Definition 2.4 (Integers Modulo n)**.** Define $\mathbb{Z}_n$ to be the set of equivalence classes of integers modulo n. Formally this means $\mathbb{Z}_n = \{[1], [2], \ldots, [n-1]\}$ where

$$[k] = \{k + i \cdot n | \forall i \in \mathbb{Z}\}.$$

We will however normally leave of the brackets and just write $\mathbb{Z}_n = \{1, 2, \ldots, n-1\}$ unless there is the potential for confusion.

Note that division, i.e. multiplicative inverses, in $\mathbb{Z}_n$ is not generally well defined except under the conditions given in lemme 2.7.

Lemma 2.13. *Given integer a, k with a relatively prime to a natural number n we can define a bijection, $f(x)$, from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ by $f(x) = ax + k \pmod{n}$.*

Proof. Let $n \in \mathbb{N}$, $a, k \in \mathbb{Z}$, and assume $a, n) = 1$. Define $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f(x) = ax + k \pmod{n}$.

If we were to suppose that $ax + k = ay + k$ in $\mathbb{Z}_n$, then $ax \equiv ay \pmod{n}$. (1) Since (a,n)=1, we may cancel the a(2) leaving us with $x \equiv y \pmod{n}$, i.e. $x = y$ in $\mathbb{Z}_n$. Therefore, f is a one to one function.

Now, again since $(a, n) = 1$, for any $y \in \mathbb{Z}_n$, there exists $x \in \mathbb{Z}_n$ such that $ax = y - k$ in $\mathbb{Z}_n$, so that $f(x) = y$. (3) Thus, f is also onto, and so a bijection. □

Definition 2.5 (Residue Systems)**.** Given $n \in \mathbb{Z}$ a *complete residue system* for the integers modulo n consists of one representative from each of the equivalence classes modulo n. A *reduced residue system* consists only of representatives from classes of integers relatively prime to n.

Example 2.6. Here are some examples of complete and reduced residue systems modulo n for various n, note that the sets are not unique.

1. With $n = 10$:
   (a) Complete Residue System: $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
   (b) Complete Residue System: $S = \{20, 11, -8, 33, 44, -65, 16, 77, -82, 109\}$
   (c) Reduced Residue System: $R = \{1, 3, 7, 9\}$
   (d) Reduced Residue System: $R = \{-9, -27, 37, 19\}$
2. With $n = 6$:
   (a) Complete Residue System: $S = \{0, 1, 2, 3, 4, 5\}$
   (b) Complete Residue System: $S = \{24, 37, -27, 22, -1\}$
   (c) Reduced Residue System: $R = \{1, 5\}$
   (d) Reduced Residue System: $R = \{-17, 59\}$
3. With $n = 12$:
   (a) Complete Residue System: $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
   (b) Complete Residue System: $S = \Big\{ \qquad\qquad\qquad\qquad\qquad\qquad \Big\}$
   (c) Reduced Residue System: $R = \{1, 5, 7, 11\}$
   (d) Reduced Residue System: $R = \Big\{ \qquad\qquad\qquad\qquad\qquad\qquad \Big\}$

This corollary follows from lemma 2.13.

Corollary 2.14. *Given $n \in \mathbb{N}$, if $S = \{s_0, s_1, \ldots, s_{n-1}\}$ is a complete residue system modulo n, then*

$$aS + k = \{as_0 + k, as_1 + k, \ldots, as_{n-1} + k\}$$

is also complete whenever $a, k \in \mathbb{Z}$ and $(a, n) = 1$.

This corollary follows mostly from lemma 2.13, with the additional requirement of showing that if r_i and a are relatively prime to n then so is ar_i, but this is true from lemma 2.7 (p. 37).

Corollary 2.15. *Given $n \in \mathbb{N}$, if $R = \{r_0, r_1, \dots, r_l\}$ is a reduced residue system modulo n, then*

$$aR = \{ar_0, ar_1, \dots, ar_{n-1}\}$$

is also a reduced residue system.

Example 2.7. To understand what the previous corollaries are telling us, and why they are reasonable, lets revisit example 2.6.

1. With $n = 10$, $a = 3$, and $k = 1$:

   (a) Complete Residue System: Given $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$,

   $$aS + k = \{1, 4, 7, 0, 3, 6, 9, 2, 5, 8\}$$

   (b) Reduced Residue System: Given $R = \{1, 3, 7, 9\}$,

   $$aR = \{3, 9, 1, 7\}$$

   (c) Not a Reduced Residue System: Given $R = \{1, 3, 7, 9\}$,

   $$aR + k = \{4, 0, 2, 8\}$$

2. With $n = 6$, $a = 5$, $k = -2$:

   (a) Complete Residue System: Given $S = \{0, 1, 2, 3, 4, 5\}$,

   $$aS + k = \{4, 3, 2, 1, 0, 5\}$$

   (b) Reduced Residue System: Given $R = \{1, 5\}$,

   $$aR = \{5, 1\}$$

   (c) Not a Reduced Residue System: Given $R = \{1, 5\}$,

   $$aR + k = \{3, 5\}$$

3. With $n = 12$, $a = 7$, and $k = 2$:

   (a) Complete Residue System: Given $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$,

   $$aS + k = \Big\{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Big\}$$

   (b) Reduced Residue System: Given $R = \{1, 5, 7, 11\}$,

   $$aR = \Big\{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Big\}$$

   (c) Not a Reduced Residue System: Given $R = \{1, 5, 7, 11\}$,

   $$aR + k = \Big\{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Big\}$$

Lemma 2.16 (Freshman's Delight). *Given a prime p, $\binom{p}{k}$ is divisible by p for $0 < k < p$ and so*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Proof. Let $p \in \mathbb{N}$ be a prime number and $k \in \mathbb{N}$ with $0 < k < p$. Then we calculate p choose k as follows

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \tag{2.29}$$

$$= \frac{p \cdot (p-1) \dots (k+2) \cdot (k+1)}{(p-k) \cdot (p-k-1) \dots 2 \cdot 1}. \tag{2.30}$$

However, since $p - k < p$, when reduced there will still be a factor of p.[1]
Now, by the Binomial Theorem, we write

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p.$$

From above, when we reduce this modulo p all the terms where $0 < k < p$ are equivalent to 0 and so $(a+b)^p = a^p + b^b$. □

Theorem 2.17 (Fermat's Little Theorem). *Given $p \in \mathbb{N}$ prime and $a \in \mathbb{Z}$ with (a,p)=1, $a^{p-1} \equiv 1 \pmod{p}$*

Proof 1 of F.L.T. using Induction. Let $p \in \mathbb{N}$ prime and consider the case when $a = 1$. Then

$$a^{p-1} = 1^{p-1} = 1 \equiv 1 \pmod{p}. \tag{2.31}$$

Now suppose the theorem holds for some $a \in \mathbb{N}$ and look at $a+1)^{p-1}$. By the Freshman's Delight (Theorem 2.16)

$$(a+1)^{p-1} \equiv a^{p-1} + 1^{p-1} \equiv a+1 \pmod{p}.\text{[1]} \tag{2.32}$$

Finally, for negative a note that if p is odd, then $p-1$ is even and $a^{p-1} = |a|^{p-1}$; then apply the previous argument. If $p = 2$, then $p - 1 = 1$ so that $a^{p-1} = a$, but since $(a, 2) = 1$, a is odd and $a \equiv 1 \pmod{2}$.
Thus, by the Principle of Mathematical Induction, $a^{p-1} \equiv 1 \pmod{p}$ □

Proof 2 of F.L.T. using Wilson's. Let $p \in \mathbb{N}$ prime and $a \in \mathbb{Z}$ with (a,p)=1. Further, let

$$R = \{1, 2, 3, \dots, p-1\}$$

which is a reduced residue system modulo p. Thus

$$R = \{a, 2a, 3a, \dots, (p-1)a\}$$

is also reduced residue system modulo p by corollary 2.15. Therefore $R = aR$ and

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p} \qquad (2.33) \\ & a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p}. \qquad (2.34) \end{aligned}$$

Using Wilson's Theorem (Theorem 2.12) this reduces to

$$-1 \equiv -1 \cdot a^{p-1} \pmod{p}, \tag{2.35}$$

i.e. $a^{p-1} \equiv 1 \pmod{p}$. □

Proof 3 of F.L.T. using a Reduced Residue System. Let $p \in \mathbb{N}$ prime and $a \in \mathbb{Z}$ with (a,p)=1. Further, let

$$R = \{1, 2, 3, \ldots, p-1\}$$

which is a reduced residue system modulo p. Thus

$$R = \{a, 2a, 3a, \ldots, (p-1)a\}$$

is also reduced residue system modulo p by corollary 2.15. Therefore $R = aR$ and

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}. \tag{2.36}$$

Since, R is a reduced residue system each element has a multiplicative inverse so that we may reduce the previous expression to $a^{p-1} \equiv 1 \pmod{p}$ □

Though the previous two proofs are almost identical, the latter will be easier to generalize to the case when the modulus is not prime.

Definition 2.6 (Euler's ϕ-Function)**.** Given a natural number n define $\phi(n)$ to be the number of natural numbers less than or equal to n which are relatively prime to it. Note that by the definition of a reduced residue system, $\phi(n)$ is the cardinality of the reduced residue system.

Theorem 2.18 (Calculating $\phi(n)$)**.** *Given* $n, m, p \in \mathbb{Z}$*,*

1. *if* p *is prime* $\phi(p^k) = (p-1)p^{k-1}$*, and*

2. *if* $m, n) = 1$*, then* $\phi(mn) = \phi(m)\phi(n)$*.*

As a result of the second condition above, we say that Euler's ϕ-function is a *multiplicative function*.

Proof of Theorem 2.18. TBD □

Theorem 2.19 (Euler's Theorem)**.** *Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Euler's Theorem. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with (a,n)=1. Further, let

$$R = \left\{r_1, r_2, r_3, \ldots, r_{\phi(n)}\right\}$$

which is a reduced residue system modulo p. Thus

$$aR = \left\{ar_1, ar_2, ar_3, \ldots, ar_{\phi(n)}\right\}$$

is also reduced residue system modulo n by corollary 2.15. Therefore $R = aR$ and

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(n)} \equiv ar_1 \cdot ar_2 \cdot ar_3 \cdots ar_{\phi(n)} \pmod{n}. \tag{2.37}$$

Since, R is a reduced residue system each element has a multiplicative inverse so that we may reduce the previous expression to $a^{\phi(n)} \equiv 1 \pmod{p}$ □

Note (Euler vs. Fermat). When n is prime, then we should note that $\phi(n) = n - 1$ and so Euler's Theorem and Fermat's Little Theorem are the same.

2.4 Exercises

For exercises 2.1 to 2.6 determine if the given values of a and b and equivalent modulo n.

2.1 Calculation. $n = 17,\ a = 12,\ b = 42$

2.2 Calculation. $n = 16, a = 26, b = 44$

2.3 Calculation. $n = 8, a = 35, b = 11$

2.4 Calculation. $n = 19, a = 32, b = 16$

2.5 Calculation. $n = 13, a = 37, b = 19$

2.6 Calculation. $n = 12, a = 26, b = 74$

For exercises 2.7 to 2.12 find the additive and multiplicative inverses for a modulo n or say why they don't exist.

2.7 Calculation. $n = 17, a = 3$

2.8 Calculation. $n = 20, a = 7$

2.9 Calculation. $n = 35, a = 15$

2.10 Calculation. $n = 35, a = 17$

2.11 Calculation. $n = 30, a = 14$

2.12 Calculation. $n = 210, a = 17$

2.13 Calculation. Find the value of $\phi(n)$ for $n = 29$

2.14 Calculation. Find the value of $\phi(n)$ for $n = 91$

2.15 Calculation. Find the value of $\phi(n)$ for $n = 123$

2.16 Calculation. Find the value of $\phi(n)$ for $n = 84$

2.17 Calculation. Find the value of $\phi(n)$ for $n = 159$

2.18 Calculation. Find the value of $\phi(n)$ for $n = 81$

2.19 Calculation. Use the Chinese Remainder Theorem (Theorem 2.10, p. 38) to solve the system of equations.

$$x \equiv 2 \pmod 3 \tag{2.38}$$
$$x \equiv 0 \pmod 7 \tag{2.39}$$
$$x \equiv 4 \pmod{11} \tag{2.40}$$

2.20 Calculation. Use the Chinese Remainder Theorem (Theorem 2.10, p. 38) to solve the system of equations.

$$x \equiv 0 \pmod 2 \tag{2.41}$$
$$x \equiv 10 \pmod{11} \tag{2.42}$$
$$x \equiv 2 \pmod{19} \tag{2.43}$$

2.21 Calculation. Use the Chinese Remainder Theorem (Theorem 2.10, p. 38) to solve the system of equations.

$$
\begin{aligned}
x &\equiv 5 \pmod{7} \tag{2.44}\\
x &\equiv 7 \pmod{12} \tag{2.45}\\
x &\equiv 0 \pmod{13} \tag{2.46}
\end{aligned}
$$

2.22 Calculation. Use the Chinese Remainder Theorem (Theorem 2.10, p. 38) to solve the system of equations.

$$
\begin{aligned}
x &\equiv 3 \pmod{5} \tag{2.47}\\
x &\equiv 7 \pmod{11} \tag{2.48}\\
x &\equiv 2 \pmod{17} \tag{2.49}
\end{aligned}
$$

2.23 Claim. Given $n \in \mathbb{N}$, show that addition and subtraction are well defined modulo n. (This is parts (1) and (2) of Theorem 2.6, 35.)

2.24 Claim. Given $a, b, m, n \in \mathbb{Z}$, $n, m > 0$; show that if $a \equiv b \pmod{[n, m]}$, then $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$. (Note that this is the converse portion for Lemma 2.3 on 34.)

2.25 Claim. Given $a, b, m, n \in \mathbb{Z}$, $n, m > 0$, and $n, m) = 1$; if $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{nm}$. (Note that this is Corollary 2.4 on 34.)

2.26 Claim. Given $n \in \mathbb{N}$, there exist zero divisors modulo n if and only if n is composite.

2.27 Claim. Given $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, the equation

$$ax + b \equiv c \pmod{n}$$

has a solution if and only if $d = (a, n)$ divides $c - b$. (This is Theorem 2.9 on p. 37.)

2.28 Claim. Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $r_a = r_b$, where $a = q_a n + r_a$ and $b = q_b n + r_b$ as in the Division Algorithm (Theorem 1.4, p. 9). (This is theorem 2.5 from p. 35.)

Part II

Appendices

Direct Proofs

Contrapositive Proofs

Contradiction Proofs

Induction Proofs

General Index