Number Theory Notebook

Paul Schulze

January 22, 2021

1 Chapter 1

Divisibility and congruence

Theorem 1.1. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof.

(1.1.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.1.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.1.3)	$b + c = a \cdot d_b + a \cdot d_c$	by (1.1.1) and (1.1.2)
(1.1.4)	$b + c = a \cdot (d_b + d_c)$	by distributive property
(1.1.5)	$d_b + d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid (b + c)$	by def'n of divides $\square$

Theorem 1.2. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.*

Proof.

(1.2.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.2.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.2.3)	$b - c = a \cdot d_b - a \cdot d_c$	by (1.2.1) and (1.2.2)
(1.2.4)	$b - c = a \cdot (d_b - d_c)$	by distributive property
(1.2.5)	$d_b - d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid (b - c)$	by def'n of divides $\square$

Theorem 1.3. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.*

Proof.

(1.3.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.3.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.3.3)	$bc = (a \cdot d_b) \cdot (a \cdot d_c)$	by (1.3.1) and (1.3.2)
(1.3.4)	$bc = a \cdot (a \cdot d_b \cdot d_c)$	by associativity and commutativity
(1.3.5)	$a \cdot d_b \cdot d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid bc$	by def'n of divides $\square$

Question 1.4. *Can you weaken the hypothesis of the previous theorem and still prove the conclusion? Can you keep the same hypothesis, but replace the conclusion by the stronger conclusion that $a^2|bc$ and still prove the theorem?*

Yes. You can remove the $a|c$ condition to weaken the hypothesis, or with both $a|b$ and $a|c$ you can show $a^2|bc$.

Question 1.5. *Can you formulate your own conjecture along the lines of the above theorems and then prove it to make it your theorem?*

Yes.

Paul's Conjecture 1. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a^2|bc$.*

Proof. First, take lines (1.3.1) through (1.3.4) of the proof of Theorem 1.3. Then,

$d_b \cdot d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
$a^2 \mid bc$	by def'n of divides $\square$

Theorem 1.6. *Let a, b, and c be integers. If $a|b$, then $a|bc$.*

Proof.

(1.6.1)	$\exists d \in \mathbb{Z} \ni ad = b$	because $a|b$
(1.6.2)	$bc = adc$	by (1.6.1)
(1.6.3)	$dc \in \mathbb{Z}$	because $d \in \mathbb{Z}$ and $c \in \mathbb{Z}$
	$a|bc$	by def'n of divides $\square$

Exercise 1.7. *Answer each of the following questions, and prove that your answer is correct.*

1. *Is* $45 \equiv 9 \pmod 4$*?*
   Yes. $4 \cdot 9 = 36 = 45 - 9$.

2. *Is* $37 \equiv 2 \pmod 5$*?*
   Yes. $5 \cdot 7 = 35 = 37 - 2$.

3. *Is* $37 \equiv 3 \pmod 5$*?*
   No. $37 - 3 = 34$ which is not a multiple of 5.

4. *Is* $37 \equiv -3 \pmod 5$*?*
   Yes. $5 \cdot 8 = 40 = 37 - (-3)$.

Exercise 1.8. *For each of the following congruences, characterize all the integers m that satisfy that congruence.*

1. $m \equiv 0 \pmod 3$
   $m \in \{3z \mid z \in \mathbb{Z}\}$

2. $m \equiv 1 \pmod 3$
   $m \in \{3z + 1 \mid z \in \mathbb{Z}\}$

3. $m \equiv 2 \pmod 3$
   $m \in \{3z + 2 \mid z \in \mathbb{Z}\}$

4. $m \equiv 3 \pmod 3$
   $m \in \{3z \mid z \in \mathbb{Z}\}$

5. $m \equiv 4 \pmod 3$
   $m \in \{3z + 1 \mid z \in \mathbb{Z}\}$

Theorem 1.9. *Let a and n be integers with $n > 0$. Then $a \equiv a \pmod{n}$.*

Proof.

(1.9.1)	$0 \in \mathbb{Z}$	
(1.9.2)	$n \cdot 0 = 0$	
(1.9.3)	$n \mid 0$	By def'n of divides
(1.9.4)	$a - a = 0$	
(1.9.5)	$n \mid (a - a)$	By (1.9.3) and (1.9.4)
	$a \equiv a \pmod{n}$	By def'n of modular congruence ☐

Theorem 1.10. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

Proof.

(1.10.1)	$a \equiv b \pmod{n}$	Given
(1.10.2)	$\exists d \in \mathbb{Z} \ni nd = a - b$	By def'n of modular congruence
(1.10.3)	$-1nd = -1 \cdot (a - b)$	By multiplicative property of equality
(1.10.4)	$n \cdot (-d) = b - a$	By various algebra
(1.10.5)	$-d \in \mathbb{Z}$	By multiplicative closure of $\mathbb{Z}$
(1.10.6)	$n \mid (b - a)$	By (1.10.4), (1.10.5)
	$b \equiv a \pmod{n}$	By def'n of modular congruence ☐

Theorem 1.11. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof.

(1.11.1)	$n \mid a - b$	By $a \equiv b \pmod{n}$
(1.11.2)	$n \mid b - c$	By $b \equiv c \pmod{n}$
(1.11.3)	$\exists d_1 \in \mathbb{Z} \ni nd_1 = a - b$	By (1.11.1)
(1.11.4)	$\exists d_2 \in \mathbb{Z} \ni nd_2 = b - c$	By (1.11.2)
(1.11.5)	$nd_1 + nd_2 = (a - b) + (b - c)$	By additive property of equality
(1.11.6)	$n(d_1 + d_2) = a - c$	By various algebra
(1.11.7)	$d_1 + d_2 \in \mathbb{Z}$	By closure of integers under addition
(1.11.8)	$n \mid (a - c)$	By def'n of divides
	$a \equiv c \pmod{n}$	By def'n of modular congruence ☐

Theorem 1.12. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof.

(1.12.1)	$n \mid (a - b)$	By $a \equiv b \pmod{n}$
(1.12.2)	$\exists d_1 \in \mathbb{Z} \ni nd_1 = a - b$	By def'n divides
(1.12.3)	$n \mid (c - d)$	By $c \equiv d \pmod{n}$
(1.12.4)	$\exists d_2 \in \mathbb{Z} \ni nd_2 = c - d$	By def'n divides
(1.12.5)	$nd_1 + nd_2 = (a - b) + (c - d)$	By additive property of equality
(1.12.6)	$n \cdot (d_1 + d_2) = (a + c) - (b + d)$	By various algebra
(1.12.7)	$d_1 + d_2 \in \mathbb{Z}$	By additive closure of $\mathbb{Z}$
(1.12.8)	$n \mid \left((a + c) - (b + d)\right)$	By def'n of divides
	$a + c \equiv b + d \pmod{n}$	By def'n of modular congruence ☐

Theorem 1.13. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.*

Proof. Notice $-c$ and $-d$ are integers, and $-c \equiv -d \pmod{n}$ (glossing over the proof of that for now). Then simply cite 1.12 and we're done. □

Theorem 1.14. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

Proof.

(1.14.1)	$n \mid (a - b)$	By $a \equiv b \pmod{n}$
(1.14.2)	$\exists k_1 \in \mathbb{Z} \ni a - b = nk_1$	
(1.14.3)	$a = nk_1 + b$	
(1.14.4)	$n \mid (c - d)$	By $c \equiv d \pmod{n}$
(1.14.5)	$\exists k_2 \in \mathbb{Z} \ni c - d = nk_2$	
(1.14.6)	$c = nk_2 + d$	
(1.14.7)	$ac = (nk_1 + b)(nk_2 + d)$	By (1.14.3) and (1.14.6)
(1.14.8)	$ac = n^2 k_1 k_2 + nk_1 d + nk_2 b + bd$	
(1.14.9)	$ac - bd = n \cdot (nk_1 k_2 + k_1 d + k_2 b)$	
(1.14.10)	$n \mid (ac - bd)$	Since $nk_1k_2 + k_1 d + k_2 b \in \mathbb{Z}$
	$ac \equiv bd \pmod{n}$	

□

Exercise 1.15. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.*

Proof.

(1.15.1)	$a \equiv b \pmod{n}$	Given
(1.15.2)	$a \cdot a \equiv b \cdot b \pmod{n}$	1.14
	$a^2 \equiv b^2 \pmod{n}$	

□

Exercise 1.16. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.*

Proof.

(1.16.1)	$a \equiv b \pmod{n}$	Given
(1.16.2)	$a^2 \equiv b^2 \pmod{n}$	1.15
(1.16.3)	$a \cdot a^2 \equiv b \cdot b^2 \pmod{n}$	By 1.14 on (1.16.1) and (1.16.2)
	$a^3 \equiv b^3 \pmod{n}$	

□

Exercise 1.17. *Let a, b, k, and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.*

Proof.

(1.17.1)	$a \equiv b \pmod{n}$	Given
(1.17.2)	$a^{k-1} \equiv b^{k-1} \pmod{n}$	1.15
(1.17.3)	$a \cdot a^{k-1} \equiv b \cdot b^{k-1} \pmod{n}$	By 1.14 on (1.17.1) and (1.17.2)
	$a^k \equiv b^k \pmod{n}$	

□

Theorem 1.18. *Let a, b, k, and n be integers with $n > 0$ and $k > 0$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$*

Proof. Our base case is 1.9. Our induction hypothesis is "a, b, k, and n are integers with $n > 0$ and $k > 1$ such that $\forall j \ni 0 < j < k$, we find $a^j \equiv b^j \pmod{n}$. Notice our induction hypothesis fulfills the criteria for 1.17, and in fact 1.17 covers our induction step. □

Exercise 1.19. *Illustrate each of Theorems 1.12 - 1.18 with an example using actual numbers*

1.12
$2 \equiv 12 \pmod 10$ and $5 \equiv 15 \pmod 10$ imply $7 \equiv 27 \pmod 10$.

1.13
$7 \equiv 27 \pmod 10$ and $12 \equiv 2 \pmod 10$ imply that $-5 \equiv 25 \pmod 10$.

1.14
$2 \equiv 7 \pmod 5$ and $3 \equiv 8 \pmod 5$ imply that $6 \equiv 56 \pmod 5$.

1.15
$2 \equiv 7 \pmod 5$ implies that $4 \equiv 49 \pmod 5$.

1.16
$1 \equiv 3 \pmod 2$ implies that $1 \equiv 27 \pmod 2$.

1.17
$1 \equiv 3 \pmod 2$ and $1 \equiv 27 \pmod 2$ imply that $1 \equiv 81 \pmod 2$.

1.18
$1 \equiv 3 \pmod 2$ implies that $1 \equiv 81 \pmod 2$.

Question 1.20. *Let a, b, c, and n be integers for which $ac \equiv bc \pmod n$. Can we conclude that $a \equiv b \pmod n$? If you answer "yes", try to give a proof. If you answer "no", try to give a counterexample.*

No. Notice $1 \cdot 0 \equiv 2 \cdot 0 \pmod 5$ and yet $1 \not\equiv 2 \pmod 5$.

Theorem 1.21. *Let a natural number n be expressed in base 10 as*

$$n = a_k a_{k-1} \ldots a_1 a_0$$

If $m = a_k + a_{k-1} + \cdots + a_1 + a_0$ then $n \equiv m \pmod 3$.

First, a Lemma that will help us later.

Lemma 1.21.1. *Let a be an integer and j a natural number. Then $a \equiv a \cdot 10^j \pmod 3$.*

Proof. Notice that $1 \equiv 10 \pmod 3$. Then, by 1.18, we find $1^j \equiv 10^j \pmod 3$ and thus that $1 \equiv 10^j \pmod 3$. Then, since $a \equiv a \pmod 3$ (by 1.9), we invoke 1.14 to find $a \cdot 1 \equiv a \cdot 10^j \pmod 3$, implying that $a \equiv a \cdot 10^j \pmod 3$. ☐

Now we begin our proof of the theorem in full.

Proof. Notice that n can be written as $a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, or more easily as

$$n = \sum_{i=0}^{k} a_i \cdot 10^i$$

Now notice that

$$m = \sum_{i=0}^{k} a_i$$

By 1.21.1, we notice that $\forall i \; a_i \equiv a_i \cdot 10^i \pmod 3$. Thus, n and m are sums of terms that are congruent modulo 3. By repeatedly invoking 1.12, we eventually find that the two strings of congruent sums are themselves are congruent, i.e. that $n \equiv m \pmod 3$. ☐

Theorem 1.22. *If a natural number is divisible by 3, then, when expressed in base 10, the sum of its digits is divisible by 3.*

Proof. Let the natural number be n, and the sum of its digits m. We're given by the theorem $n \equiv 0 \pmod 3$, and by 1.21 we know $n \equiv m \pmod 3$, so we can cite 1.11 and conclude $m \equiv 0 \pmod 3$, i.e. m is divisible by 3. ☐

Theorem 1.23. *If the sum of the digits of a natural number expressed in base* 10 *is divisible by* 3*, then the number is divisible by* 3 *as well.*

Proof. Let the natural number be n, and the sum of its digits m. We're given by the theorem $m \equiv 0 \pmod 3$, and by 1.21 we know $n \equiv m \pmod 3$, so we can cite 1.11 and conclude $n \equiv 0 \pmod 3$, i.e. n is divisible by 3. $\square$

Exercise 1.24. *Devise and prove other divisibility criteria similar to the preceding one.*

A number is divisible by 2 if and only if its last digit is divisible by 2, because any (base 10) number $n = a_k a_{k-1} \dots a_1 a_0 = a_k a_{k-1} \dots a_1 \cdot 10 + a_0$, and $2|10$ so $2|\dots \cdot 10$. Thus, $2|\dots \cdot 10 + a_0$ iff $2|a_0$.

Similar proofs can be done for 5 and the last digit, 4 and the last 2 digits, 8 and the last 3 digits, 16 and the last 4 digits, 32 and the last 5 digits, etc.

The Division Algorithm

Exercise 1.25. *Illustrate the division algorithm for:*

1. $m = 25$, $n = 7$.
   $25 = 7 \cdot 3 + 4$.

2. $m = 277$, $n = 4$.
   $277 = 4 \cdot 69 + 1$.

3. $m = 33$, $n = 11$.
   $33 = 11 \cdot 3 + 0$.

4. $m = 33$, $n = 45$.
   $33 = 44 \cdot 0 + 33$.

Theorem 1.26. *Prove the existence part of the Division Algorithm. In other words, given natural numbers n and m, show there exist integers q and r such that $m = nq + r$ and $0 \le r \le n - 1$.*

Proof. Let $S = \{x \in \mathbb{Z} \mid nx > m\}$. By the Well-Ordering Axiom, S has a smallest element: call it s. Let $q = s - 1$. This definition gives us two important properties:

1. $nq \le m$, for if $nq > m$ then $q \in S$ with $q < s$, which is impossible since s is the smallest element of S.

2. $m < n(q + 1) = nq + n$, for $q + 1 = s$ and $sx > m$ because $s \in S$.

Now, we define $r = m - nq$, so that by definition $m = nq + r$. Since $nq \le m$, we know $r \ge 0$. Since $m < nq + n$, and yet $m = nq + r$, implying $nq + r < nq + n \implies r < n \implies r \le n - 1$.

Thus, we have found q, r such that $m = nq + r$ and $0 \le r \le n - 1$. $\square$

Theorem 1.27. *Prove the uniqueness part of the Division Algorithm. In other words, given natual numbers n and m, if there are 4 integers q, q', r, and r', such that $m = nq + r = nq' + r'$ with $0 \le r, r' \le n - 1$ then $q = q'$ and $r = r'$.*

Proof. Notice that $nq + r = nq' + r'$ implies that $nq - nq' = r' - r \implies n(q - q') = r' - r$.

Since $0 \le r, r' \le n - 1$, we conclude that $-n + 1 \le r' - r \le n - 1$. By our previous equality, then, $-n + 1 \le n(q - q') \le n - 1 \implies -n < n(q - q') < n$. Since n is a natural number, we can divide by n to get $-1 < q - q' < 1$. Since q and q' are integers, $q - q'$ must also be an integer. The only integer between -1 and 1 is 0, so we conclude $q - q' = 0 \implies q = q'$.

Once we have $q = q'$, we see that $nq + r = nq' + r' \implies nq + r = nq + r' \implies r = r'$. $\square$

Theorem 1.28. *Let a, b, and n be integers with $n > 0$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if and only if when $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$ then $r_1 = r_2$.*

First, we will show that $a \equiv b \pmod{n} \implies r_1 = r_2$.

Proof. Notice by the definition of modular congruence that $a \equiv b \pmod{n}$ implies that $n|(b-a)$, or $\exists d \in \mathbb{Z} \ni nd = b - a$. Using $a = nq_1 + r_1$ and $b = nq_2 + r_2$ we get $nd = nq_1 + r_1 - nq_2 - r_2 = n(q_1 - q_2) + r_1 - r_2$. Then we get $nd - n(q_1 - q_2) = r_1 - r_2$ or $n(d - q_1 + q_2) = r_1 - r_2$.

Since $0 \leq r_1, r_2 \leq n-1$ we find that $-n+1 \leq r_1 - r_2 \leq n-1 \implies -n < r_1 - r_2 < n$. Using our previous equation with $r_1 - r_2$ we get that $-n < n(d - q_1 + q_2) < n$, and dividing by n (which we can do because $n > 0$) we get $-1 < d - q_1 + q_2 < 1$. Since d, q_1, and q_2 are all integers, $d - q_1 + q_2$ is also an integer, and the only integer between -1 and 1 is 0 so we find $d - q_1 + q_2 = 0$.

Plugging this back in to $n(d - q_1 + q_2) = r_1 - r_2$, we find $n \cdot 0 = r_1 - r_2$, which implies $0 = r_1 - r_2$, or $r_1 = r_2$. □

Second, we will show that $r_1 = r_2 \implies a \equiv b \pmod{n}$.

Proof. Notice $a - b = nq_1 + r_1 - (nq_2 + r_2)$. With some simple rearranging, we obtain $a - b = n(q_1 - q_2) + r_1 - r_2$. Since we know $r_1 = r_2$, we know $r_1 - r_2 = 0$, and plugging this in we obtain $a - b = n(q_1 - q_2)$.

Since q_1 and q_2 are integers, $q_1 - q_2$ is also an integer. Thus, n times some integer is $a - b$: in other words, $n|(a - b)$.

Then, by the definition of modular congruence, we obtain $a \equiv b \pmod{n}$. □

Greatest common divisors and linear Diophantine equations

Question 1.29. *Do every two integers have at least one common divisor?*

Yes. For any two integers a and b, $1 \cdot a = a$ and $1 \cdot b = b$ so $1|a$ and $1|b$, making 1 a common divsor of a and b.

Question 1.30. *Can two integers have infinitely many common divisors?*

No, if the two integers are distinct. Any nonzero integer n can only have finitely many divisors, as any integer d such that $d < -|n|$ or $d > |n|$ cannot be a divisor (since $1d$ and $-1d$ have a greater absolute value than n, and $0d = 0 \neq n$). In other words, only the numbers f such that $-n \leq f \leq n$ are "eligibile" to be divisors of n, so there can only be finitely many divisors of n.

Exercise 1.31. *Find the following greatest common divisors. Which pairs are relatively prime?*

1. $(36, 22)$
   2

2. $(45, -15)$
   15

3. $(-296, -88)$
   8

4. $(0, 256)$
   256

5. $(15, 28)$
   1 (relatively prime)

6. $(1, -2436)$
   1 (relatively prime)

Theorem 1.32. *Let a, n, b, r, and k be integers. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.*

Proof. Let $a = d_a k$ and $b = d_b k$, where d_a and d_b are the integers guaranteed by the facts that $k|a$ and $k|b$. Then, we have $d_a k = n d_b k + r$. Isolating r, we get $r = d_a k - n d_b k = k(d_a - n d_b)$. Since n, d_a, and d_b are all integers, we know $d_a - n d_b$ is an integer. Thus, we've found r is equal to k times some integer, so $k|r$. □

Theorem 1.33. *Let a, b, n_1, and r_1 be integers with a and b not both 0. If $a = n_1b + r_1$, then $(a, b) = (b, r_1)$.*

Proof. We will show that the common divisors of a and b are the same as the common divisors of b and r_1, and thus conclude that the greatest element of S is also the greatest element of T.

Let S be the set of common divisors of a and b, and let T be the set of common divisors of b and r_1. We will show $S = T$ by double inclusion.

First, let's show $S \subset T$. Take an arbitrary $s \in S$. Since $s|a$ and $s|b$, we conclude $\exists d_a, d_b \in \mathbb{Z} \ni a = sd_a, b = sd_b$. We can then rearrange $a = n_1b + r_1$ to read $r_1 = a - n_1b$, and then plug in our previous two equations to get $r_1 = sd_a - n_1sd_b \implies r_1 = s(d_a - n_1d_b)$. Since d_a, d_b, and n_1 are all integers, we know $d_a - n_1d_b$ is an integer, thus implying that $s|r_1$. Since we know $s|b$ since $s \in S$, we conclude $s \in T$. Thus, any arbitrary $s \in S$ is an element of T, so $S \subset T$.

Showing that $T \subset S$ proceeds in much the same way. Take $t \in T$, conclude since $t|b$ and $t|r_1$ we find $\exists d_bd_r \in \mathbb{Z} \ni b = td_b, r_1 = td_r$, and then plug those in to $a = n_1b + r_1$ to get $a = n_1td_b + td_r \implies a = t(n_1d_b + d_r)$. Since n_1, d_b, and d_r are integers, we find $t|a$, and since $t|b$ because $t \in T$, we thus conclude $t \in S$. Thus any arbitrary $t \in T$ is an element of S, so $T \subset S$.

Thus, by double inclusion, $S = T$. This implies that the greates element of S, i.e. (a, b), is equal to the greatest element of T, i.e. (b, r_1). □

Exercise 1.34. *Use the preceding theorem to show that if $a = 51$ and $b = 15$, then $(51, 15) = (6, 3) = 3$.*

Proof. Since $51 = 3 \cdot 15 + 6$, we find $(51, 15)$, we cite 1.33 to see $(51, 15) = (15, 6)$. Then, since $15 = 2 \cdot 6 + 3$, we again cite 1.33 to find $(15, 6) = (6, 3)$. We see that $(6, 3) = 3$ by inspection. Then, since equality is transitive, we conclude $(51, 15) = (6, 3) = 3$. □

Exercise 1.35. *Using the previous theorem and the Division Algorithm successively, devise a procedure for finding the greatest common divisor of two integers.*

Well you kind of gave the game away when you said to use 1.33 and the divsion algorithm successively huh. If you're trying to find (a, b), you simply invoke the division algorithm to get $a = nb + r$ (assuming WLOG that $a \geq b$), and then rewrite (a, b) as (b, r). Then, you use the divion algorithm to get $b = nr + r'$, simplifying to (r, r'), etc. etc., until at some point you have $(x, 0)$, which by inspection is equal to x.

You will always reach $(x, 0)$ because the divison algorithm produces a remainder r that is strictly less than the smaller input b, so (informally) the smaller of the two numbers you're working with always gets smaller while never going negative.

Exercise 1.36. *Use the Euclidean Algorithm to find the following.*

1. $(96, 112)$
$112 = 1 \cdot 96 + 16$, simplifying the problem to $(96, 16)$. Then $96 = 5 \cdot 16 + 0$, so we get $(16, 0) = 16$

2. $(162, 31)$
$162 = 5 \cdot 31 + 7 \implies (31, 7) \implies 31 = 4 \cdot 7 + 3 \implies (7, 3) \implies 7 = 2 \cdot 3 + 1 \implies (3, 1) = 1.$

3. $(0, 256)$
Since everything divides 0, this is trivially 256.

4. $(-288, -166)$
$-166 = 1 \cdot -288 + 122 \implies (-288, 122) \implies -288 = -3 \cdot 122 + 78 \implies (122, 78) \implies 122 = 1 \cdot 78 + 44 \implies (78, 44) \implies 78 = 1 \cdot 44 + 34 \implies (44, 34) \implies 44 = 1 \cdot 34 + 10 \implies (34, 10) = 2$ by inspection.

5. $(1, -2436)$
Since the only integers that divide 1 are -1, 0, and 1, we trivially find 1.

Exercise 1.37. *Find integers x and y such that $162x + 31y = 1$.*

By division algorithm, $162 = 5 \cdot 31 + 7 \implies 7 = 1 \cdot 162 + (-5) \cdot 31$.

By division algorithm, $31 = 4 \cdot 7 + 3 \implies 3 = 1 \cdot 31 + (-4) \cdot 7 = 1 \cdot 31 + (-4) \cdot (1 \cdot 162 + (-5) \cdot 31) = (-4) \cdot 162 + 21 \cdot 31$.

By division algorithm, $7 = 2 \cdot 3 + 1 \implies 1 = 1 \cdot 7 + (-2) \cdot 3 = 1 \cdot (1 \cdot 162 + (-5) \cdot 31) + (-2) \cdot ((-4) \cdot 162 + 21 \cdot 31) = 9 \cdot 162 + (-47) \cdot 31$.

Thus, we've found our solution $x = 9$ and $y = -47$.

Theorem 1.38. *Let a and b be integers. If $(a, b) = 1$, then there exist integers x and y such that $ax + by = 1$.*

Proof. If either a or b is negative, replace it with $-a$ or $-b$ for the rest of this proof. At then end, you can replace either x or y with $-x$ or $-y$ to get an answer; for instance, if $a = -3$, we can replace $a = 3$, do the proof to obtain x_0 and y_0 such that $3x_0 + by_0 = 1$ and then realize that $(-3)(-x_0) + by_0 = 1$, which since $-x_0$ is still an integer still suffices. Now we will only be worrying about non-negative a and bs.

We will demonstrate an algorithm to find x and y. WLOG, assume $a \geq b$. Invoke the division algorithm to get $a = n_1 b + r_1$. Then invoke it again to get $b = n_2 r_1 + r_2$. Then invoke it again to get $r_1 = n_3 r_2 + r_3$. Etc. etc. etc.

We will show that the series "remainder" generated by this algorithm eventually has to hit 0: in other words, $\exists i \in \mathbb{N} \ni r_i = 0$. To do this, we must notice that for any index j, since r_j is generated by calling the division algorithm on r_{j-2} and r_{j-1}, we find that $r_j \leq r_{j-1} - 1$. Notice, then, that we can apply this to r_{j-1} to obtain $r_{j-1} \leq r_{j-2} - 1$, and then plug that in to our previous inequality to get $r_j \leq r_{j-1} - 1 \leq r_{j-2} - 2$.

By inspection (i.e. I'm lazy and don't want to formalize this), we notice we can continually apply this. We will apply this to r_b, and notice that $r_b \leq r_{b-1} - 1 \leq r_{b-2} - 2 \leq \cdots \leq r_1 - (b-1) \leq b - b$. Since $b - b = 0$, we find $r_b \leq 0$, but since r_b is a remainder from the division algorithm we know $r_b \geq 0$, so we conclude $r_b = 0$.

Notice we have *not* proven that r_b is the *first* 0, only that the remainders must *eventually* reach 0 at *some* point.

Now, keep invoking the division algorithm until the "remainder" generated by the algorithm is 0: we will label that step $k + 1$, so that we find $r_{k-1} = n_{k+1} r_k + 0$. We will show that r_k is 1.

By invoking 1.33 repeatedly, we find that $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = (r_k, r_{k+1})$. Since $r_{k+1} = 0$, we conclude $(a, b) = (r_k, 0)$. Since 0 divides everything, $(r_k, 0) = r_k$, so $(a, b) = r_k$, and since a and b are relatively prime we conclude $1 = r_k$.

Now, we take all of our equations and rewrite them to solve for the remainder. For example, $a = n_1 b + r_1$ becomes $r_1 = a + (-n_1)b$, and $b = n_2 r_1 + r_2$ becomes $r_2 = b + (-n_2) r_1$.

This gives us a bunch of equations of the form $r_j = \delta_j r_{j-2} + \gamma_j r_{j-1}$. This incldues one for r_k, namely $r_k = \delta_k r_{k-2} + \gamma_k r_{k-1}$. We can then substitute in lower indices of r for r_{k-2} and r_{k-1}, using the generic equation, to get something like $r_k = \delta_k(\delta_{k-2} r_{k-4} + \gamma_{k-2} r_{k-3}) + \gamma_k(\delta_{k-1} r_{k-3} + \gamma_{k-1} r_{k-2})$.

That looks horrifying, but the important bit is that we notice if we simplify it we get $r_k = Ar_{k-4} + Br_{k-3} + Cr_{k-2}$ with $A, B, C \in \mathbb{Z}$. That is, *by replacing all r_j's with their respective equations, we have reduced the highest index on an r in the right hand side by* 1. Previously, the highest index was $k - 1$, but now it's $k - 2$, because we had an equation to represent r_{k-1} in terms of r_{k-3} and r_{k-4}.

Notice, though, that not all r's satisfy this property: namely, r_1 and r_2 simplify down to a and b, which then don't have equations of their own. So, we apply the equations for r_k through r_1 in "reverse" order, pairing down the maximum index of k each time, until we're left with only r_1's and r_2's on the left hand side and can apply those equations to get a linear expression in a and b on the right hand side.

We've been talking a lot about the right hand side, but remember, the left hand side is r_k, and we've shown $r_k = 1$, so we've just found a linear expression in a and b that is equal to 1. In other words, $1 = ax + by$ for some $x, y \in \mathbb{Z}$. □

Theorem 1.39. *Let a and b be integers. If there exist integers x and y with $ax + by = 1$, then $(a, b) = 1$.*

Proof. Readers of the last proof will be glad to hear this one is much simpler.

By definition, $(a, b)|a$ and $(a, b)|b$. Then, $(a, b)|ax$ and $(a, b)|by$ by 1.6. Then, $(a, b)|ax + by$ by 1.1. Then, since $ax + by = 1$, we find $(a, b)|1$. We know $1|a$ and $1|b$, so $(a, b) \geq 1$. The only number ≥ 1 that divides 1 is 1, so since $(a, b) \geq 1$ and $(a, b)|1$ we conclude $(a, b) = 1$. □

Theorem 1.40. *For any integers a and b not both 0, there are integers x and y such that $ax + by = (a, b)$.*

Proof. Let $c = a/(a, b)$ and $d = b/(a, b)$. Notice that since $(c, d)|c$ and $a = c \cdot (a, b)$ we find $((c, d) \cdot (a, b))\,|a$, and similarly since $(c, d)|d$ and $b = d \cdot (a, b)$ we find $((c, d) \cdot (a, b))\,|b$.

Since c and d are integers not both 0, (c, d) must be a positive integer. Since $(c, d) \cdot (a, b)$ is a common factor of a and b, and (a, b) is the *greatest* common factor of a and b, we find $(c, d) \cdot (a, b) \leq (a, b) \implies (c, d) = 1$.

Thus, we invoke 1.38 to find integers x and y such that $cx + dy = 1$. Then, we multiply both sides by (a, b) to find that $(a, b) \cdot cx + (a, b) \cdot dy = (a, b)$. Since $a = (a, b) \cdot c$ and $b = (a, b) \cdot d$ we conclude $ax + by = (a, b)$. □

Theorem 1.41. *Let a, b, and c be integers. If $a|bc$ and $(a,b) = 1$, then $a|c$.*

Proof. Since $(a,b) = 1$, we can invoke 1.38 to find $x, y \in \mathbb{Z} \ni ax + by = 1$.

Now, since $a|bc$, we can cite 1.6 to obtain $a|bcy$.

Since $a \cdot 1 = a$ we find $a|a$, and then by 1.6 we get $a|acx$.

Then, by 1.1 we get $a|(acx+bcy)$. We can then do some simple algebraic rearrangement to get $a|\left(c \cdot (ax + by)\right) \implies a|(c \cdot 1) \implies a|c$. □

Theorem 1.42. *Let a, b, and n be integers. If $a|n$, $b|n$, and $(a,b) = 1$, then $ab|n$*

Proof. Since $a|n$ and $b|n$ we find integers k, j such that $ak = n$ and $bj = n$. By the transitive property of equality, $ak = bj$. Since j is an integer, we conclude $b|ak$. Since $(a,b) = 1$, we invoke 1.41 to find $b|k$. Thus, we invoke an integer d such that $bd = k$. Substiuting this into $ak = n$, we find $abd = n$, and since d is an integer we conclude $ab|n$. □

Theorem 1.43. *Let a, b, and n be integers. If $(a,n) = 1$ and $(b,n) = 1$, then $(ab,n) = 1$.*

Proof. Invoking 1.38 twice, we find two pairs of integers, x_a, y_a, x_b, and y_b such that $ax_a + ny_a = 1$ and $bx_b + ny_b = 1$. We notice then that $(ax_a + ny_a) \cdot (bx_b + ny_b) = 1 \cdot 1 = 1$, and we simplify the left-hand side to $ax_abx_b + ax_any_b + ny_abx_b + ny_any_b = ab(x_ax_b) + n(ax_ay_b + y_abx_b + ny_ay_b) = 1$, and then by closure of the integers and 1.39 we find that $(ab,n) = 1$. □

Question 1.44. *What hypotheses about a, b, c, and n could be added so that $ac \equiv bc \pmod{n}$? State an appropriate theorem and prove it before reading on.*

I know this from Math Seminar. *$ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ if and only if $(c,n) = 1$.*

Proof. First, we will show that $ac \equiv bc \pmod{n}$ and $(c,n) = 1$ imply that $a \equiv b \pmod{n}$.

Notice that $ac \equiv bc \pmod{n}$ implies $n|(bc - ac)$. By distribution, we obtain $n|\left(c(b-a)\right)$. Then, since $(c,n) = 1$, we cite 1.41 to obtain $n|(b-a)$, which by definition means $a \equiv b \pmod{n}$.

Now, we will show that if $(c,n) > 1$, then $ac \equiv bc \pmod{n}$ does *not* imply $a \equiv b \pmod{n}$.

We will do this by example. Notice that $n|\left(c \cdot (n/(c,n))\right)$: the right-hand side can be rearranged to read $n \cdot (c/(c,n))$ and $c/(c,n)$ is an integer because (c,n) is a factor of c. Then, since $n|n$, we cite 1.6 to find $n|\left(n \cdot (c/(c,n))\right)$. We then cite the facts that $n|0$ and 1.2 to find $n|\big((c \cdot (n/(c,n))) - 0\big)$, and we can substitue in $c \cdot 0$ for 0 to find $n|\big((c \cdot (n/(c,n))) - c \cdot 0\big)$. We then, by definition, obtain $c \cdot (n/(c,n)) \equiv c \cdot 0 \pmod{n}$.

However, since $n > 0$ (because congruence "modulo n" is defined) and $(c,n) > 1$, we find that $0 < n/(c,n) < n$. This implies that $n/(c,n) \not\equiv 0 \pmod{n}$, despite teh fact that $c \cdot (n/(c,n)) \equiv c \cdot 0 \pmod{n}$, giving us our counterexample. □

Theorem 1.45. *Let a, b, c, and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and $(c,n) = 1$, then $a \equiv b \pmod{n}$.*

See 1.44.

Question 1.46. *Suppose a, b, and c are integers and that there is a solution to the linear Diophantine equation $ax + by = c$. That is, suppose there are integer x and y that satisfy the equation $ax + by = c$. What condition must c satisfy in terms of a and b?*

Since $(a,b)|(ax + by)$, we conclude $(a,b)|c$.

Question 1.47. *Can you make a conjecture by completing the following statement?*

Paul's Conjecture 2. *Given integers a, b, and c, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $(a,b)|c$.*

Proof. Notice that an integer solution to $ax + by = c$ implies that, since $(a,b)|a$ and $(a,b)|b \implies (a,b)|(ax + by)$ (1.6 and 1.1), we conclude $(a,b)|c$.

Now, notice $(a,b)|c \implies \exists d \in \mathbb{Z} \ni d(a,b) = c$. We invoke 1.40 to find integers w and z such that $aw + bz = (a,b)$. Then, we can multiply both sides by d to obtain $d(aw + bz) = d(a,b)$, which simplifies to $awd + bzd = c$, giving us the solution $x = wd$ and $y = zd$. □

Theorem 1.48. *Given integers a, b, and c with a and b not both 0, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $(a,b)|c$.*

See Paul's Conjecture 2.

Question 1.49. *For integers a, b, and c, consider the linear Diophantine equation $ax + by = c$. Suppose integers x_0 and y_0 satisfy the equation: that is, $ax_0 + by_0 = c$. What other values*

$$x = x_0 + h \text{ and } y = y_0 + k$$

also satisfy $ax+by = c$? Formulate a conjecture that answers this question. Devise some numerical examples to ground your exploration. For example, $6(-3) + 15 \cdot 2 = 12$. Can you find other integers x and y such that $6x + 15y = 12$? How many other pairs of integers x and y can you find? Can you find infintely many other solutions?

Paul's Conjecture 3. *The integers $x_1 = x_0 + h$ and $y_1 = y_0 + k$ satisfy the equation $ax_1 + by_1 = c$ if and only if $\frac{b}{(a,b)}|h$ and $k = -\frac{ah}{b}$).*

Proof. First, notice $ax_1 + by_1 = c$ if and only if $a(x_0 + h) + b(y_0 + k) = c$. Then with rearrangement, we find this is equivalent to $ax_0 + by_0 + ah + bk = c \iff c + ah + bk = c \iff ah + bk = 0$. Then, we find $bk = -ah \iff k = -(ah/b)$.

Notice that this "if-and-only-if chain" doesn't show that k is an *integer.* Thus, we will show that k is an integer if and only if $(b/(a,b))|h$, the other condition, to complete our proof.

First, notice $\frac{b}{(a,b)}|h \implies \exists d \in \mathbb{Z} \ni \frac{b}{(a,b)}d = h$. Then, $\frac{b}{(a,b)}da = ah$. This can be rewritten as $b \cdot (d\frac{a}{(a,b)}) = ah$, and since $a/(a,b)$ is an integer we conclude $b|ah$. In other words, $k = -(ah/b)$ is an integer.

Going the opposite direction is much the same: $k = -(ah/b)$ being an integer implies $b|ah$, implying $bd = ah$, implying $bd/(a,b) = ah/(a,b)$, implying $\frac{b}{(a,b)}|\frac{ah}{(a,b)}$. Then, we notice that since there exist integers γ and δ such that $a\gamma + b\delta = (a,b)$ (1.40), we find $\frac{a}{(a,b)}\gamma + \frac{b}{(a,b)}\delta = \frac{(a,b)}{(a,b)} = 1$, which by 1.39 implies that $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$. Thus, we cite 1.41 with $\frac{b}{(a,b)}|\frac{ah}{(a,b)}$ to find $\frac{b}{(a,b)}|h$. ☐

Exercise 1.50. *A farmer lays out the sum of 1,770 crowns in purchasing horses and oxen. He pays 31 crowns for each horse and 21 crowns for each ox. What are the possible numbers of horses and oxen that the farmer bought?*

51 horses and 9 oxen is the first situation I found. Using Paul's Conjecture 3, we can find that further solutions can be found by subtracting 21 from the number of horses while adding 31 to the number of oxen (trust me it makes sense).

30 horses and 40 oxen.

9 horses and 71 oxen.

Theorem 1.51. *Let a, b, c, x_0, and y_0 be integers with a and b not both 0 such that $ax_0+by_0 = c$. Then the integers*

$$x = x_0 + \frac{b}{(a,b)} \text{ and } y = y_0 - \frac{a}{(a,b)}$$

also satisfy the linear Diophantine equation $ax + by = c$.

Proof. Notice these integers satisfy the requirements for Paul's Conjecture 3 (I'm too lazy to show how but 1.53 will force me to). ☐

Question 1.52. *If a, b, and c are integers with a and b not both 0, and the linear diophantine equation $ax + by = c$ has at least one integer solution, can you find a general expression for all the integer solutions to that equation? Prove your conjecture.*

Paul's Conjecture 4. *The set of all pairs of integers (x_1, y_1) such that $ax_1 + by_1 = c$ can be written as*

$$\left\{\left(x_0 + \frac{bd}{(a,b)}, y_0 - \frac{ad}{(a,b)}\right) \mid d \in \mathbb{Z}\right\}$$

Proof. Paul's Conjecture 3 can easily be extended here: if we let the integer solution given be x_0 and y_0, such that $ax_0 + by_0 = c$, we want to find a general expression for all integers $x_1 = x_0 + h$ and $y_1 = y_0 + k$ where $\frac{b}{(a,b)}|h$ and $k = -\frac{ah}{b}$.

The set of all integers h such that $\frac{b}{(a,b)}|h$ can be expressed as $\{\frac{bd}{(a,b)} \mid d \in \mathbb{Z}\}$. The corresponding k value for any h is $-\frac{ah}{b} = -\frac{a(bd/(a,b)}{b} = -\frac{ad}{(a,b)}$. Thus, any pair of $x_1 = x_0 + \frac{bd}{(a,b)}$ and $y_1 = y_0 - \frac{ad}{(a,b)}$ satisfies the Diophantine equation $ax_1 + by_1 = c$. ☐

Theorem 1.53. *Let a, b, and c be integers with a and b not both 0. If $x = x_0$, $y = y_0$ is an integer solution to the equation $ax + by = c$ (that is, $ax_0 + by_0 = c$) then for every integer k, the numbers*

$$x = x_0 + \frac{kb}{(a,b)} \text{ and } y = y_0 - \frac{ka}{(a,b)}$$

are integers that also satisfy the linear Diophantine equation $ax + by = c$. Moreover, every solution to the linear Diophantine equation $ax + by = c$ is of this form.

Proof. This is just a less pretentious way of saying Paul's Conjecture 4 that doesn't involve set notation. ☐

Exercise 1.54. *Find all integer solutions to the equation $24x + 9y = 33$.*

$(x, y) \in \{(1 + 3k, 1 - 8k) \mid k \in \mathbb{Z}\}$.

Theorem 1.55. *If a and b are integers, not both 0, and k is a natural number, then $\gcd(ka, kb) = k \cdot \gcd(a, b)$.*

Proof. First, we notice that $k \cdot (a, b)$ is indeed a common factor of ka and kb, since $(a, b)|a$ we conclude $k(a, b)|ka$, and similarly for $k(a, b)|kb$.

Now, we invoke 1.40 to find integers x and y such that $ax + by = (a, b)$. We can mulitply both sides by k to find $k(ax + by) = kax + kby = k(a, b)$, and then from that invoke 1.48 with ka and kb to find that $(ka, kb)|k(a, b)$. Since (ka, kb) is the *greatest* common factor of ka and kb, and $k(a, b)$ is a common factor of ka and kb, we conclude $k(a, b) \leq (ka, kb)$. However, since $k(a, b)$ is positive and $(ka, kb)|k(a, b)$, we conclude $k(a, b) \geq (ka, kb)$. Thus, we conclude $k(a, b) = (ka, kb)$. ☐

Exercise 1.56. *For natural numbers a and b, give a suitable defintion for "least common multiple of a and b," denoted $\operatorname{lcm}(a, b)$. Construct and compute some examples.*

Define $\operatorname{lcm}(a, b)$ as the smallest positive number x such that $a|x$ and $b|x$.
Some examples include $\operatorname{lcm}(3, 6) = 6$, $\operatorname{lcm}(1, 50) = 50$, and $\operatorname{lcm}(2, 5) = 10$.

Theorem 1.57. *If a and b are natural numbers, then $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.*

Proof. Notice by 1.55 that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = \gcd(a \operatorname{lcm}(a, b), b \operatorname{lcm}(a, b))$.

Since $a | \operatorname{lcm}(a, b)$ we can write $\operatorname{lcm}(a, b) = ak$ for some integer k. Similarly, we can write $\operatorname{lcm}(a, b) = bj$ for an integer j. Then, we simplify our expression to $\gcd(a \operatorname{lcm}(a, b), b \operatorname{lcm}(a, b)) = \gcd(abj, bak)$. Then, citing 1.55 again, we find this equal to $ab \gcd(j, k)$.

Notice that since $\gcd(j, k)|j$, we can write $j = x \gcd(j, k)$, and likewise we can write $k = y \gcd(j, k)$. Then, we notice $ak = bj \implies ay \gcd(j, k) = bx \gcd(j, k)$. Since $ay = bx$ is a common mulitple of a and b, and $ay \gcd(j, k)$ is the *least* common mulitple of a and b, we find $ay \gcd(j, k) \leq ay$, which implies $\gcd(j, k) = 1$.

Putting this all together, we find $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab \gcd(j, k) = ab$. ☐

Corollary 1.58. *If a and b are natural numbers, then $\operatorname{lcm}(a, b) = ab$ if and only if a and b are relatively prime.*

Proof. By 1.57, we find $ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b) \implies \operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$. Thus, a and b are relatively prime if and only if $\gcd(a, b) = 1 \iff \operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)} = ab$. ☐

2 Chapter 2

Fundamental Theorem of Arithmetic

Theorem 2.1. *If n is a natural number greater than 1, then there exists a prime p such that $p|n$.*

Proof. Let $S = \{k \in \mathbb{Z} \mid k > 1, k|n\}$. By the Well-Ordering Principle, S has a smallest element, call it s. Notice that if $s = a \cdot b$ (where a and b are natural numbers), then $a, b \leq s$, $a|n$, and $b|n$. Since s is the smallest number besides 1 that divides n, we conclude a and b cannot both be less than s (since if either is 1, the other must be s). Thus, s is a prime number such that $s|n$. $\square$

Exercise 2.2. *Write down the primes less than 100 without the aid of a calculator or a table of primes and think about how you decide whether each number you select is prime or not.*

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$

Theorem 2.3. *A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divde n.*

Proof. We can easily see that if there is a prime p such that $p \leq \sqrt{n}$ and $p|n$, then n is not prime (since $p \leq \sqrt{n} < n$ and $pk = n$ for some natural k).

Thus, we must show that if for all primes $p \leq \sqrt{n}$, p does not divide n, then n is prime. To do this we will assume n is composite and show that there must be a prime $p \leq \sqrt{n}$ that *does* divide n.

Since n is composite, we can write $n = ab$, where a and b are natural numbers both less than n. Since they are both less than n, neither can be 1 (or else $ab < n$, a contradiction). We also know that one must be less than or equal to $\sqrt{n}$ (if both a and b are greater than $\sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$ which is a contradiction). Without loss of generality, assume that a is one guaranteed such that $1 < a \leq \sqrt{n}$.

Since $a > 1$, by 2.1 we find there exists a prime $p|a$, and since $p \leq a \leq \sqrt{n}$ and $p|a$ while $a|n$, that means we've found a prime $p \leq \sqrt{n}$ such that $p|n$.

Thus, if n is composite there exists a prime $p \leq \sqrt{n}$ such that $p|n$, which lets us conclude the contrapositive that if there is no such $p \leq \sqrt{n}$ such that $p|n$, n must be prime. $\square$

Exercise 2.4. *Use the preceding theorem to verify that 101 is prime.*

The only primes less than or equal to $\sqrt{101}$ are 2, 3, 5, and 7, none of which divide 101. Thus, 101 is prime.

Exercise 2.5. *Do the sieve of eratosthenes. Why are the circled numbers all of the primes less than 100?*

I did this for 2.2. In order for a number n to be circled, it can't be a multiple of any other prime number p such that $p < n$. By 2.3, this implies n is prime. (Notice this only works because we start at 2, the first prime, which means the second circle is prime, so the third circle is prime, etc.)

Exercise 2.6. *For each natural number n, define $\pi(n)$ to be the number of primes less than or equal to n. Make a guess about approximately how large $\pi(n)$ is relative to n. In particular, do you suspect that $\frac{\pi(n)}{n}$ is generally an increasing or decreasing function? Do you suspect that it approaches osme specific limit as $n \to \infty$? etc. etc.*

Man $\frac{\pi(n)}{n}$ sure seems to, uh, go down. Some python I wrote indicates that it (VERY slowly) works its way down, the lowest I've seen is about 0.12. Maybe it converges to something nice like .1, although I doubt it and suspect it works down to 0.

Theorem 2.7. *Every natural number greater than 1 is either a prime number or it can be expressed as a finite product of prime numbers. That is, for every natural number n greater than 1, there exist distinct primes $p_1, p_2, \ldots, p_m$ and natural numbers $r_1, r_2, \ldots, r_m$ such that*

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

Proof. Since $n > 1$, it is either prime or composite. If n is prime, we're done. If not, let j and k be the natural numbers greater than 1 such that $n = jk$.

Since j and k are natural numbers greater than 1, they are either prime or composite. If they're both prime, we're done. In the other case, let's assume without loss of generality that j is composite and k is prime. Then, we can split j into natural numbers greater than 1, call them a and b so that $j = ab$. Then, $n = abk$.

Now, a and b must either be prime or composite. If they are both prime, we're done. If not, ... etc. etc.

Notice that since $j, k < n$ and $a, b < j$, etc. etc., the numbers we're working with get smaller with every step. Since these numbesr must also be natural numbers, they can't get smaller *forever*: in other words, this process must cease at some point (if it didn't, it would imply there are infintiely many natural numbers taht are less than n, which is absurd). When this process terminates, we'll find that n is a product of primes. $\square$

Theorem 2.8. *Let p and $q_1, q_2, \ldots, q_n$ all be primes and let k be a natural number such that $pk = q_1 q_2 \cdots q_n$. Then $p = q_i$ for some i.*

Proof. We will do a proof by contradiciton (!!). Assume that $p \neq q_i$ for any i.

Take any q_i. The divisors of p are 1 and p, and the divisors of q_i are 1 and q_i, since both are prime. Since we know $p \neq q_i$, we find that $(p, q_i) = 1$. Thus, by 1.41, since we know $p|(q_1 \cdots q_n$, we find $p|(q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_n)$.

We can use this process to "remove" each q_i term from the multiplaction, finding that $p|1$. Since p is a prime, we know $p > 1$, giving us a contradiciton. Thus, our assumption is false, and there exist a q_i such that $p = q_i$. $\square$

Theorem 2.9. *Let n be a natural number. Let $P = \{p_1, p_2, \ldots, p_m\}$ and $Q = \{q_1, q_2, \ldots, q_s\}$ be sets of primes with $p_1 \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, \ldots, r_m\}$ and $\{r_1, r_2, \ldots, t_s\}$ be sets of natural numbers such that*

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t1} q_2^{t_2} \cdots q_s^{t_s} \end{aligned}$$

Then $m = s$ and $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots q_s\}$. That is, the sets of primes are equal but their elements are not necessarily listed in the same order; that is, p_i may or may not equal q_i. Moreover, if $p_i = q_j$ then $r_i = t_j$. In other words, if we express the same natural number as a product of powers of distinct primes, then the expressions are identical except for the ordering of the factors.

Proof. We will start with the proof that $P = Q$, by double inclusion.

Take $p \in P$. It's clear $p|n$ (since p is a part of a product that equals n), and thus that $p|(q_1^{t_1} \cdots q_s^{t_s})$. We can then use a similar logic that we used in the proof of 2.8: if $p \notin Q$, then for all q_i we find that $(p, q_i) = 1$, and using this by 1.41 we can slowly remove terms from the product on the right until we eventually reach $p|1$, which is absurd, implying that the assumption $p \notin Q$ is false. Thus, $\forall p \in P,\ p \in Q$, or in other words $P \subset Q$.

Take the bit above and swap around the letters and you find $Q \subset P$, completing our double inclusion proof that $P = Q$.

Our logic that $p_i = q_j$ implies $r_i = t_j$ will feel very similar.

Since $n = m$, we know that $p_1^{r_1} \cdots p_m^{r_m} = q_1^{t_1} \cdots q_m^{t_m}$ (since $P = Q$ we know $|P| = |Q|$ and thust $m = s$).

Notice this means $p_i^{r_i}|(q_1^{t_1} \cdots q_m^{t_m})$. As above, we continually cite 1.41 to remove terms from the right hand side.

We can do this even when raising p_i to a power because, as per the first half of this proof, any prime factorizaion of $p_i^{r_i}$ will contain only the same primes as the factorization "$p_i^{r_i}$," and thus will only contain p_i. In other words, it's impossible to create a product that is equal to $p_i^{r_i}$ using any other primes, and thus no other prime divides $p_i^{r_i}$ so it cannot have any common factors with other prime numbers.

Notice, however, that $(p_i^{r_i}, q_j) = q_j = p_i$, so we cannot remove those terms, leaving us with $p_i^{r_i}|q_j^{t_j}$. This lets us conclude that (since both numbers are positive) $p_i^{r_i} \leq q_j^{t_j}$, which implies $r_i \leq t_j$.

Now, as above, we take the logic above and swap all of the letters to conclude that $q_j^{t_j}|p_i^{r_i}$, and thus that $q_j^{t_j} \leq p_i^{r_i}$ and finally that $t_j \leq r_i$.

Since $t_j \leq r_i \leq t_j$, we conclude $r_i = t_j$, completing our proof that $p_i = q_j$ implies $r_i = t_j$. $\square$

Exercise 2.10. *Express $n = 12!$ as a product of primes.*

$$\begin{aligned} 12! &= 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= (2^2 \cdot 3) \cdot 11 \cdot (2 \cdot 5) \cdot (3^2) \cdot (2^3) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2^2) \cdot 3 \cdot 2 \\ &= 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \end{aligned}$$

Exercise 2.11. *Determine the number of zeroes at the end of* 25!

In which base?

In base 10 what this is really asking is how many 2s and 5s divide 25!. I promise you on my life that 2s are not going to be the limiting factor here, so we can focus on how high of a power of 5 divides 25!.

We get one 5 from $5, 10, 15$, and 20. We get two from 25. That gives us $5^6|25!$, so there are 6 zeroes on the end of 25!.

(As promised, $2^{23}|25!$, so 2 is not even remotely close to limiting the number of 0s).

Applications of the Fundamental Theorem of Arithmetic

Theorem 2.12. *Let a and b be natural numbers greater than 1 and let $p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be the unique prime factorization of b. Then $a|b$ if and only if for all $i \le m$ there exists a $j \le s$ such that $p_i = q_j$ and $r_i \le t_j$.*

Proof. Woo boy. Let's start by showing $a|b$ implies... all of that.

We know that $a|b$ means $ak = b$. This means that $p_1^{r_1}\cdots p_m^{r_m}k = q_1^{t_1}\cdots q_s^{t_2}$. Since k is an integer (and a natural number, given both a and b are natural) we know that it has its own unique prime factorization. Thus, the prime factorization of a times the prime factorization of k must be equal to the prime factorization of b (since $ak = b$ and prime factorizations are unique).

When we multiply the prime factorization of a by that k, we cannot remove any of the terms $p_1 \dots p_m$, nor can we reduce any of the exponents $r_1 \dots r_m$, since the prime factorization of k will not contain the multiplicative inverse of any prime. Thus, in order for our product to be the prime factorization of b, all of the primes $p_1 \dots p_m$ must also be included in the prime factorization of b, and all of the exponents $r_1 \dots r_m$ must be less than or equal to the corresponding exponents in the prime factorization of b.

Now the other direction. If we know that for all $i \le m$ there exists a $j \le s$ such that $p_1 = q_j$ and $r_1 \le t_j$, then we can rewrite b as $(p_1^{r_1}\cdots p_m^{r_m})\cdot(q_1^{t_1'}\cdots q_s^{t_s'})$, where $t_1' \dots t_s'$ are the exponents on the relative prime modified to accomodate "moving" $p_1^{r_1}$ through $p_m^{r_m}$ to the front of the product (these exponents notably may be 0). Since $q_1^{t_1'}\cdots q_s^{t_s'}$ is an integer (call it k) and $p_1^{r_1}\cdots p_m^{r_m}$, we've shown that $b = ak$, or in other words $a|b$. □

Theorem 2.13. *If a and b are natural numbers and $a^2|b^2$, then $a|b$.*

Proof. Let $a = p_1^{r_1}\cdots p_m^{r_m}$ and $b = q_1^{t_1}\cdots q_s^{t_s}$ be the unique prime factorizations of these numbers.

Notice that $a^2 = p_1^{2r_1}\cdots p_m^{2r_m}$ and $b^2 = q_1^{2t_1}\cdots q_s^{2t_s}$, and that these are the prime factorizations of these numbers.

By 2.12, we find $a^2|b^2$ implies that for all $i \le m$ there exists a $j \le s$ such that $p_i = q_j$ and $2r_i \le 2t_j$. This implies that $r_i \le t_j$, so we conclude that for all $i \le m$ there exists a $j \le s$ such that $p_i = q_j$ and $r_i \le t_j$. By 2.12, this means $a|b$. □

Exercise 2.14. *Find* $(3^14 \cdot 7^22 \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$

$11^4 \cdot 17$

Exercise 2.15. *Find* $\operatorname{lcm}(3^14 \cdot 7^22 \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$

$3^14 \cdot 5^2 \cdot 7^22 \cdot 11^5 \cdot 13^8 \cdot 17^3$

Exercise 2.16. *Make a conjecture that generalizes the ideas you used to solve the two previous exercises.*

Paul's Conjecture 5. *Let the primes be denoted p_i, where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, etc.*

Let $a = p_1^{r_1}p_2^{r_2}\cdots$ and $b = p_1^{t_1}p_2^{t_2}\cdots$ be the prime factorizations of natural numbers a and b, where r_i and t_j can be 0 to indicate the absence of a prime. Then

$$\gcd(a,b) = p_1^{\min(r_1,t_1)}p_2^{\min(r_2,t_2)}\cdots = \prod_{i\in\mathbb{N}} p_i^{\min(r_i,t_i)} \text{ and}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(r_1,t_1)}p_2^{\max(r_2,t_2)}\cdots = \prod_{i\in\mathbb{N}} p_i^{\max(r_i,t_i)}.$$

Question 2.17. *Do you think this method is always better, always worse, or sometimes better and sometimes worse than using the Euclidean Algorithm to find (a, b)? Why?*

For large numbers, for humans, this method is probably better because you can use divisibility rules to easily start prime factorizing the number and make it smaller and easier to work with (although, for numbers that are the products of only large primes like $29 \cdot 31$ or something this might be painful).

For computers the Euclidean Algorithm is almost certainly better, because you can easily find the quotient/remainder through repeated addition and it's very fast.

Theorem 2.18. *Given $n+1$ natural numbers, say $a_1, a_2, \ldots, a_{n+1}$, all less than or equal to $2n$, then there exists a pair, say a_i and a_j with $i \neq j$, such that $a_i | a_j$.*

Proof. Credit to Sam.

We'll use the pigeonhole principle. We'll form sets S_1 through S_{2n-1} for all *odd* indices, with each set $S_t = \{t \cdot 2^n \mid n \in \mathbb{N} \cup \{0\}\}$.

Notice that if any two of our numbers a_i and a_j fall into the same S_t, then $a_i = t \cdot 2^n$ and $a_j = t \cdot 2^m$. Assuming WLOG that $n \leq m$, we find $a_j = a_i \cdot 2^{m-n}$, which since 2^{m-n} is an integer (as $m - n \geq 0$) shows $a_i | a_j$. Thus, we only need show that two of our a's fall into the same set.

Notice then that every a_i will fall into at least (in fact, exactly) one S_t. Take a_i's prime factorization, let it be $p_1^{r_1} \cdots p_m^{r_m}$.

Then if $2 \neq p_v$ for any $v \leq n$, since a_i is odd we find $a_i = a_i \cdot 2^0$ and thus $a_i \in S_{a_i}$.

If $2 = p_v$ for some $v \leq n$, then we notive $a_i = 2^{r_v} \cdot (p_1^{r_1} \cdots p_{v-1}^{r_{v-1}} p_{v+1}^{r_{v+1}} \cdots p_m^{r_m})$. Let's define that second term as k. Since all of the p's are unique, we know that k is odd, and thus $a_i = S_k$.

Since there are only sets S for each of the odd numbers between 1 and $2n$, there are exactly n sets. Since there are $n+1$ numbers in our set of a's, by the pigeonhole principle, we know there must be a_i, a_j such that $i \neq j$, $a_i \in S_t$, and $a_j \in S_t$ for some t. As we showed earlier, this implies that either $a_i | a_j$ or vice versa, completing our proof. ☐

Theorem 2.19. *There do not exist natural numbers m and n such that $7m^2 = n^2$.*

Proof. In the prime factorization of n^2 the exponent on 7 must be even, as it is double the exponent on 7 in the prime factoization of n.

In the prime factorization of $7m^2$, the exponent on 7 must be odd, as it is double the exponent on 7 in the prime factorization of m *plus one* (for multiplying by 7).

Since prime factorizations are unique, $7m^2$ and n^2 having different exponents (for the same number cannot be both even *and* odd) implies they are different numbers and thus not equal. ☐

Theorem 2.20. *There do not exist natural numbers m and n such that $24m^3 = n^3$.*

Proof. Notice $24m^3 = 2^3 \cdot 3 \cdot m^3$.

Then, apply the logic above to the exponent on 3 in the prime factorization of these two numbers; it must be a multiple of 3 in n^3, and yet it must be one *more* than a multiple of 3 in $24m^3 = 2^3 \cdot 3 \cdot m^3$. Since the same number cannot be both (as $0 \not\equiv 1 \pmod 3$), the prime factorizations of n^3 and $24m^3$ are not the same and thus the numbers cannot be equal. ☐

Exercise 2.21. *Show that $\sqrt{7}$ is irrational. That is, there do not exist natural numbers n and m such that $\sqrt{7} = \frac{n}{m}$.*

Proof. If there were such numbers n and m, then we would find $\sqrt{7} \cdot m = n$, implying $7m^2 = n^2$, a contradiction with 2.19. Thus, no such numbers exist. ☐

Exercise 2.22. *Show that $\sqrt{12}$ is irrational.*

If $\sqrt{12} = \frac{a}{b}$ for integers a, b, then $12b^2 = a^2$, which is impossible due to the smame logic we used in 2.20.

Exercise 2.23. *Show that $7^{\frac{1}{3}}$ is irrational.*

If $7^{\frac{1}{3}} = \frac{a}{b}$, then $7b^3 = a^3$. This is impossible for integers a and b, as the prime factorization of $7b^3$ has an exponent on 7 that is one *greater* than a multiple of 3, while the prime factoization of a^3 has an exponnet on 7 that *is* a multiple of 3.

Question 2.24. *What other numbers can you show to be irrational? Make and prove the most general conjecture you can.*

Paul's Conjecture 6. *Let w be an integer, with $w = p_1^{r_1} \cdot p_2^{r_2} \cdots p_t^{r_t}$ its prime factorization. $w^{\frac{n}{m}}$ (where n and m are integers) is irrational if for any one prime p_i with $1 \leq i \leq t$ it is the case that $m \nmid (n \cdot r_i)$.*

Proof. Say it is the case there exists a p_i such that $m \nmid (n \cdot r_i)$. We then find $p_i^{r_i} | w_i$, so let's invoke k such that $w = kp_i^{r_i}$. Notice $p_i \nmid k$ due to the fact that $k = \frac{w}{p_i^{r_i}}$ which has no p_i's in its prime factorization. We then find $w^{\frac{n}{m}} = k^{\frac{n}{m}} \cdot p_i^{\frac{nr_i}{m}}$.

Say $w^{\frac{n}{m}} = k^{\frac{n}{m}} \cdot p_i^{\frac{nr_i}{m}} = \frac{a}{b}$. To show $w^{\frac{n}{m}}$ is irrational, we will asssume a and b are both integers and . Rearranging the equation, we find $k^{\frac{n}{m}} \cdot p_i^{\frac{nr_i}{m}} \cdot b = a$, and then raising both sides to the mth powerwe find $k^n \cdot p_i^{nr_i} \cdot b^m = a^m$. Now both sides of this equation are integers, which means we can compare their prime factorizations. Specifically, we are going to look at the exponent on p_i in these prime factorizations. k has no impact on this exponent (since $p_i \not| k$). b^m provides some multiple of m to this exponent, while p_i provides nr_i; in other words, the exponent on p_i on the left side is of the form $\alpha m + nr_i$ for some integer α. On the left, since we only have a^m, we have an exponent of the form βm for some integer β. Since these two are equal, we find $\alpha m + nr_i = \beta m$, which tells us $m|(\alpha m + nr_i)$, which then since $m|\alpha m$ we cite 1.2 to find $m|nr_i$, a contradiction.

Thus, a and b cannnot both be integers, and thus $w^{\frac{n}{m}}$ is irrational. $\square$

Theorem 2.25. *Let a, b, and n be integers. If $a|n$, $b|n$, and $(a,b)=1$, then $ab|n$.*

Proof. Let $n = p_1^{r_1} \cdots p_m^{r_m}$ be the prime factorization of n. Then, by 2.12, we can write $a = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $b = p_1^{\beta_1} \cdots p_m^{\beta_m}$, where for all i with $1 \le i \le m$ we know $0 \le \alpha_i, \beta_i \le r_i$.

Say $ab \not| n$. Since $ab = p_1^{\alpha_1+\beta_1} \cdots p_m^{\alpha_m+\beta_m}$, we invoke 2.12 to find there must be some j such that $1 \le j \le m$ and $\alpha_j + \beta_j > r_j$ (since all of the primes in the prime factorization of ab are represented in p_1 through p_m). However, since $\alpha_j \le r_j$, this implies $\beta_j \ge 1$, and similarly that $\alpha_j \ge 1$. This means that since $p_j^{\alpha_j}|a$, we know $p_j|a$, and similarly that $p_j|b$ making p_j a common divisor of a and b. Since p_j is prime, $p_j > 1$, and since $(a,b)=1$, we find that p_j is a common divisor of a and b greater than their greatest common divisor, a contradction. Thus, our assumption that $ab \not| n$ is false, and we find $ab|n$. $\square$

Theorem 2.26. *Let p be a prime and let a be an integer. Then p does not divide a if and only if $(a,p)=1$.*

Proof. That p does not divide a if $(a,p)=1$ is trivial, since if it did it would be a common divisor (as $p|p$) that is greater than 1 (since p is prime) which is impossible since $(a,p)=1$.

All that is left is to show that $p \not| a$ implies that $(a,p)=1$. Since p is prime, its only (natural) divisors are 1 and p. Thus, these are the only candidates for (a,p). Since $p \not| a$, though, p is not a common divisor, and thus the only possiblity for (a,p) is 1. $\square$

Theorem 2.27. *Let p be a prime and let a and b be integers. If $p|ab$, then $p|a$ or $p|b$.*

Proof. By 2.12, we know p has to show up in the prime factorization of ab. Since the prime factorization of ab only includes primes found in either the factorization of either a or b (as it can be obtained by replacing a and b with their prime factorizations and moving the terms around), this means p must show up in the prime factorization of a or b, and thus by 2.12 either $p|a$ or $p|b$. $\square$

Theorem 2.28. *Let a, b, and c be integers. If $(b,c)=1$, then $(a,bc) = (a,b)\cdot(a,c)$.*

Proof. We invoke 1.40 twice to find integers x_1, x_2, y_1, y_2 such that $ax_1 + bx_2 = (a,b)$ and $ay_1 + cy_2 = (a,c)$. Then, we multiply the two equations together to get $(ax_1+bx_2)\cdot(ay_1+cy_2) = (a,b)\cdot(a,c)$. With some rearrangement we find $a^2x_1y_1 + abx_2y_1 + acx_1y_2 + bcx_2y_2 = (a,b)\cdot(a,c)$, which with distributivity we find means $a(ax_1y_1 + bx_2y_1 + cx_1y_2) + bc(x_2y_2) = (a,b)\cdot(a,c)$. Since $ax_1y_1 + bx_2y_1 + cx_1y_2$ and x_2y_2 are integers, we invoke 1.48 to find $(a,bc)|\left((a,b)\cdot(a,c)\right)$. Thus, $(a,bc) \le (a,b)\cdot(a,c)$.

We know that $(a,b)|a$ and that $(a,c)|a$. We also know that $\big((a,b),(a,c)\big) = 1$ (if it didn't, it would be a common factor of b and c greater than 1 which is impossible). Thus, we cite 1.42 to find $((a,b)\cdot(a,c))\,|a$. Thus, since it is a common factor, it is less than the greatest common factor, so we conclude $(a,b)\cdot(a,c) \le (a,bc)$.

Thus we have $(a,bc) \le (a,b)\cdot(a,c) \le (a,bc)$, so we conclude $(a,bc) = (a,b)\cdot(a,c)$. $\square$

Theorem 2.29. *Let a, b, and c be integers. If $(a,b)=1$ and $(a,c)=1$, then $(a,bc)=1$*

Proof. This is just 1.43. $\square$

Theorem 2.30. *Let a and b be integers. If $(a,b)=d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. By 1.40, we know there are integers x, y such that $ax + by = d$. We can then divide both sides by d to find $\frac{a}{d}x + \frac{b}{d}y = 1$. By 1.39, we conclude $(\frac{a}{d}, \frac{b}{d}) = 1$. $\square$

Theorem 2.31. *Let a, b, u, and v be integers. If $(a,b)=1$ and $u|a$ and $v|b$, then $(u,v)=1$.*

Proof. Notice that Since $(u,v)|u$ and $u|a$, we know $(u,v)|a$. Similarly, we know $(u,v)|b$. Thus, since (u,v) is a common factor of a and b, we know $(u,v) \le (a,b) = 1$. However, since 1 is a common factor of u and v, we also know $(u,v) \ge 1$. Thus, $1 \le (u,v) \le 1$, which implies $(u,v)=1$. $\square$

The infinitude of primes

Theorem 2.32. *For all natural numbers n, $(n, n+1) = 1$.*

Proof. Since 1 is a common factor of n and $n+1$, we know $(n, n+1) \geq 1$.

Since $(n, n+1)|n$ and $(n, n+1)|n+1$, we know by 1.2 that $(n, n+1)|((n+1)-n)$, or in other words $(n, n+1)|1$. Since $(n, n+1)$ is natural, we know $(n, n+1) \leq 1$.

Thus, we know $1 \leq (n, n+1) \leq 1$, and thus we conclude $(n, n+1) = 1$. ☐

Theorem 2.33. *Let k be a natural number. Then there exists a natural number n (which will be much larger than k) such that no natural number less than k and greater than 1 divides n.*

Proof. Let $n = \prod_{i=2}^{k-1}(i) + 1$. For any a such that $1 < a < k$, we find $a|(n-1)$ (as a is in the product that defines $n-1$). Since $(n-1, n) = 1$ by 2.32 and $a > 1$, we know that a cannot be a common factor of of $n-1$ and n. Since $a|(n-1)$, we then conclude $a \not| n$. Thus, no number a between 1 and k divides n. ☐

Theorem 2.34. *Let k be a natural number. Then there exists a prime larger than k.*

Proof. Assume there exists a k such that no prime is larger than k. By 2.33, there exists an n such that no number between 1 and $k+1$ divides n. Since all primes are in that range, that means no prime number divides n. This is a contradiction with 2.7, proving our assumption absurd. Thus, no k exists such that no prime is larger than k: in other words, for every k there exists a prime larger than k. ☐

Theorem 2.35. *There are infinitely many prime numbers.*

Proof. Assume there are finitely many primes. Then by 2.34 there is a prime larger than the largest prime. Absurd. ☐

Question 2.36. *What were the most clever or most difficult parts in your proof of the Infintude of Primes Theorem?*

The most clever thing I did was take Algebra II BC, so that I had already seen this proof. If you would like to know more go back in time and ask 9th grade me, I don't remember this being that difficult but I was more heavily guided then.

Theorem 2.37. *If $r_1, r_2, \ldots, r_m$ are natural numbers and each one is congruent to 1 modulo 4, then the product $r_1 r_2 \cdots r_m$ is also congruent to 1 modulo 4.*

Proof. $r_1 r_2 \cdots r_m \equiv 1 \cdot 1 \cdots 1 \equiv 1 \pmod 4$. ☐

Theorem 2.38. *There are infinitely many prime numbers that are congruent to 3 modulo 4.*

Proof. Let's say that n is the biggest prime that is congruent to 3 modulo 4. Let $m = \prod_{p \in \mathbb{P}}^{n} p$.

Notice that $2|m$ (as there is a factor of 2 in the product) but $4 \not| m$ (since $2 \not| (m/2)$, as $(m/2)$'s prime factorization has no remaining 2's). Thus, $m \equiv 2 \pmod 4$.

Let us examine $m+1$. We know that $m+1 \equiv 3 \pmod 4$. We also know that, since no prime less than or equal to n divides $m+1$ and n is the biggest prime such that $n \equiv 3 \pmod 4$, no prime that is equivalent to 3 modulo 4 divides $m+1$.

Notice that $m+1$ must have a prime factorization that includes at least 1 prime that is equivalent to 3 modulo 4 (as by 2.37 the product solely of primes that are equivalent to 1 will also be equivalent to 1, which $m+1$ is not). The prime factors of $m+1$ cannot be equivalent to 0 or 2 (as there are no primes divisible by 4 and thus none equivalent to 0, and there is only one even prime that is equivalent to 2 we already know $2 \not| (m+1)$). Thus, there has to be a prime that is equivalent to 3 modulo 4 in the prime factorization.

Since this number cannot be any prime between 0 and n, we've found a prime greater than n that is equivalent to 3 modulo 4.

Thus, our assumption that a biggest prime congruent to 3 modulo 4 is false. Thus, since at least one prime congruent to 3 modulo 4 exists (3, for example), there must be infinitely many such primes. ☐

Question 2.39. *Are there other theorems like the previous one that you can prove?*

There should be, given I caught part of Nir's talk last year, but I have an awful memory.

You can pretty directly use the above technique to show that there are infinitely many primes that *aren't* equivalent to 1 modulo basically-any-number.

You could use this to show there are infinitely many primes congruent to 5 modulo 6, as said primes can't be congruent to 2, 3, 4, or (as goes without saying) 0 and have to be *something* other than 1. Highly composite numbers like 12 are also probably good for this (in this case, we conclude there are infinitely many primes that are either 5, 7, or 11 modulo 12).

Exercise 2.40. *Find the current record for the longest arithmetic progression of primes.*

It seems to be 27 primes, discovered in 2019 by Rob Gahan and... PrimeGrid? I assume that's some kind of distributed computing project.

$224584605939537911 + 81292139 \cdot 23\# \cdot n$, for $0 \leq n < 27$.

(For a prime p, the primorial $p\#$ is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \cdots \cdot p$.)

Primes of special form

Exercise 2.41. *Use polynomial long division to compute* $(x^m - 1) \div (x - 1)$.

$$x^{m-1} + x^{m-2} + \cdots + x + 1 = \sum_{i=0}^{m-1} x^i$$

Theorem 2.42. *If n is a natural number and $2^n - 1$ is prime, then n must be prime.*

Proof. Assume $n = ab$. To show n is prime, we will show that a and b can only be 1 and n: to do this, we will show that a must either be 1 or n, and then b must be the opposite choice to satisfy $n = ab$.

$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = \frac{(2^a)^b - 1}{2^a - 1}(2^a - 1)$. By 2.41 (with $x = 2^a$ and $m = b$) we find this is equal to $((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1) \cdot (2^a - 1)$. Since this product of integers is equal to $2^n - 1$, which is prime, we conclude that the integers are 1 and $2^n - 1$.

This leaves us with two possibilities for what $2^a - 1$ could be: 1 or $2^n - 1$. In the case $2^a - 1 = 1$, we find $2^a = 2 \implies a = 1$. In the case $2^a - 1 = 2^n - 1$, we find $2^a = 2^n \implies a = n$. Thus, for any integers a and b such that $n = ab$, we've found that a and b must be 1 and n: in other words, n is prime. $\square$

Theorem 2.43. *If n is a natural number and $2^n + 1$ is prime, then n must be a power of* 2.

Proof. Notice that n is a power of 2 if and only if it has no odd divisors other than 1 (if n isn't a power of 2, its prime factorization contains an odd number or it is 1; if n is a power of 2, it has no odd divisors other than 1 by 2.12.

Let $n = ab$, where b is an odd number. Such a factorization will always exist because we can always take $b = 1$ and $a = n$.

$2^n + 1 = 2^{ab} + 1 = (2^a)^b + 1 = \frac{(2^a)^b + 1}{2^a + 1}(2^a + 1)$. By polynomial long division (do it yourself), we find this is equal to $((2^a)^{b-1} - (2^a)^{b-2} + \cdots + 1) \cdot (2^a + 1)$ (the final 1 in the first term is positive because b is odd, not that it matters). As before, since this product of integers is equal to $2^n + 1$, a prime, we conclude the integers are 1 and $2^n + 1$.

We know $2^a + 1 \neq 1$ because that would imply $2^a = 0$, which is impossible. Thus, we conclude $2^a + 1 = 2^n + 1 = 2^{ab} + 1$, implying $a = ab \implies b = 1$. Thus, the only odd number that divides n is 1. In other words, n is a power of 2. $\square$

Exercise 2.44. *Find the first few Mersenne primes and Fermat primes.*

Mersenne: $3, 7, 31, 127$.

Fermat: $3, 17, 257$.

Exercise 2.45. *For an A in the class and a Ph.D. in mathematics, prove that there are infintely many Mersenne primes (or Fermat primes) or prove that there aren't (your choice).*

Our traditional approach of assuming there are finitely many Mersenne primes and then constructing a new one is flawed because there doesn't seem to be a way to create a product of said Mersenne primes that we can then modify to get a new Mersenne prime (or mulitple of a new Mersenne prime).

I think what would really help us would be some way to tell if $2^n - 1$ is prime in terms of n, so that we could more easily prove the infinitude or finitude of the set of exponents. We know that n must be prime, but that isn't sufficient (e.g. $2^1 1 - 1 = 2047 = 23 \cdot 89$).

The distribution of primes

Theorem 2.46. *There exist arbitraily long strings of consecutive composite numbers. That is, for any natural number n there is a string of more than n consecutive composite numbers.*

Proof. For any n, define k as follows.

$$k = \prod_{p \in \mathbb{P}}^{n+1} p^{\lceil \log_p (n+1) \rceil}$$

We will show that the string $k+2 \ldots k+n+1$ is a string of n consecutive composite numbers. In other words, for all i with $2 \leq i \leq (n+1)$, there exists some $p \neq k+i$ such that $p|(k+i)$.

In fact, we will show that such a p is less than or equal to n (this obviously implies $p \neq k+i$ given that $k+i > n$).

Let us examine the prime factorization of i. Since it is less than or equal to $n+1$, we know that its prime factors are also less than or equal to $n+1$. In fact, for any term $p_i^{r_i}$ in the prime factorization, we know $p_i^{r_i} \leq i \leq n+1 = p_i^{\log_{p_i}(n+1)}$, implying that $r_i \leq \log_{p_i}(n+1) \leq \lceil \log_{p_i}(n+1) \rceil$. By 2.12, we then notice that $i|k$ (as k's prime factorization is equal to its definition above). Thus, we can write $k+i$ as $i \cdot (\frac{k}{i}+1)$, where $\frac{k}{i}+1$ is an integer. Thus we conclude $i|(k+i)$, and since $i \neq 1$ as $2 \leq 1$ and $i \neq k+1$ because $k \neq 0$ (something something irrelevant edge case where n is small) we conclude that $k+i$ is composite, as it has a factor that is neither 1 nor itself.

Thus, the sequence $k+2 \ldots k+n+1$ is a string of n consecutive composite numbers for any n. $\square$