Elementary Number Theory Notes

Ahmad Alkadri

Contents

1 Divide and Conquer

Divisibility and Congruence

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose $a|b$ and $a|c$. Then $\exists m, n \in \mathbb{Z}$ such that $b = ma$ and $c = na$. Observe,

$$\begin{aligned} b + c &= ma + na \\ &= (m+n)a \end{aligned}$$

and since $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \Rightarrow (m+n) \in \mathbb{Z}$, it follows that $a|(b+c)$. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose $a|b$ and $a|c$. Then $\exists m, n \in \mathbb{Z}$ such that $b = ma$ and $c = na$. Observe,

$$\begin{aligned} b - c &= ma - na \\ &= (m-n)a \end{aligned}$$

and since $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \Rightarrow (m-n) \in \mathbb{Z}$, it follows that $a|(b-c)$. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose $a|b$ and $a|c$. Then $\exists m, n \in \mathbb{Z}$ such that $b = ma$ and $c = na$. Observe,

$$\begin{aligned} bc &= (ma)(na) \\ &= (mna)a \end{aligned}$$

and since $m \in \mathbb{Z}$, $n \in \mathbb{Z}$, and $a \in \mathbb{Z} \Rightarrow mna \in \mathbb{Z}$, it follows that $a|bc$. □

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

Answer. We can weaken the hypothesis of theorem 1.3 to just supposing that $a, b,$ and $c \in \mathbb{Z}$, and that $a|b$ (note that it is arbitrary whether we choose $a|b$ or $a|c$). From there it follow that $\exists n \in \mathbb{Z}$ such that $b = na$, and hence $bc = (na)c = (nc)a$. Since $n \in \mathbb{Z}$ and $c \in \mathbb{Z} \Rightarrow nc \in \mathbb{Z}$, it follows that $a|bc$.

Keeping the same hypothesis as theorem 1.3, we need only observe from the theorem's proof that we can write

$$bc = (mna)a = (mn)a^2$$

from which it follows immediately that $a^2|bc$.

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?*

Answer. Here is my own conjecture:
Let a, b, c, and d be integers. If $a|b$ and $c|d$, then $ac|bd$.

Proof. Let $a, b, c, d \in \mathbb{Z}$. Suppose $a|b$ and $c|d$. Then $\exists m, n \in \mathbb{Z}$ such that $b = ma$ and $d = nc$. Observe that $bd = (ma)(nc) = (mn)(ac)$. Since $m, n \in \mathbb{Z} \Rightarrow (mn) \in \mathbb{Z}$, it follows that $ac|bd$. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose $a|b$. Then $\exists m \in \mathbb{Z}$ such that $b = ma$. Observe,

$$\begin{aligned} bc &= (ma)(c) \\ &= (mc)a \end{aligned}$$

and since $m \in \mathbb{Z}$ and $c \in \mathbb{Z} \Rightarrow mc \in \mathbb{Z}$, it follows that $a|bc$. □

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

1. *Is* $45 \equiv 9 \pmod 4$*?*
   No. $4 \nmid (45 - 9) = 54$ *since* $54/4 = 13.5 \notin \mathbb{Z}$.

2. *Is* $37 \equiv 2 \pmod 5$*?*
   Yes. $5|(37 - 2) = 35$ *since* $35/5 = 7 \in \mathbb{Z}$.

3. *Is* $37 \equiv 3 \pmod 5$*?*
   No. $5 \nmid (37 - 3) = 34$ *since* $34/5 = 6.8 \notin \mathbb{Z}$.

4. *Is* $37 \equiv -3 \pmod 5$*?*
   Yes. $5|(37 - (-3)) = 40$ *since* $40/5 = 8 \in \mathbb{Z}$.

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

1. $m \equiv 0 \pmod 3$.
   The congruence is satisfied $\forall m \in \mathbb{Z}$ *with* $3|(m-0) = m$. *In other words, the congruence is satisfied by the set* $\bar{0} := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}$ *with* $m = 3k\}$.

2. $m \equiv 1 \pmod 3$.
   The congruence is satisfied $\forall m \in \mathbb{Z}$ *with* $3|(m - 1)$. *In other words, the congruence is satisfied by the set* $\bar{1} := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}$ *with* $m = 3k + 1\}$.

3. $m \equiv 2 \pmod 3$.
   The congruence is satisfied $\forall m \in \mathbb{Z}$ *with* $3|(m - 2)$. *In other words, the congruence is satisfied by the set* $\bar{2} := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}$ *with* $m = 3k + 2\}$.

4. $m \equiv 3 \pmod 3$.
   The congruence is satisfied $\forall m \in \mathbb{Z}$ *with* $3|(m-3)$. *In other words, the congruence is satisfied by the set* $\bar{3} := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}$ *with* $m = 3k+3\}$. *Notice that since* $3k+3 = 3(k+1)$, *and* $k \in \mathbb{Z} \Rightarrow (k+1) \in \mathbb{Z}$, *it follows that* $\bar{0} = \bar{3}$.

5. $m \equiv 4 \pmod 3$.
   The congruence is satisfied $\forall m \in \mathbb{Z}$ *with* $3|(m-4)$. *In other words, the congruence is satisfied by the set* $\bar{4} := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}$ *with* $m = 3k+4\}$. *Notice that since* $3k+4 = 3(k+1)+1$, *and* $k \in \mathbb{Z} \Rightarrow (k+1) \in \mathbb{Z}$, *it follows that* $\bar{1} = \bar{4}$.

Remark. In the above example, the sets $\bar{0}, \bar{1}$, and $\bar{2}$ are elements of the well-known abelian group $\mathbb{Z}/3\mathbb{Z}$ (with respect to both addition and multiplication).

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

Proof. Let $a, n \in \mathbb{Z}$ with $n > 0$. Observe that $n|(a-a) = 0$ since $0 = 0n$ and $0 \in \mathbb{Z}$. Hence, $a \equiv a \pmod n$ by definition. This shows that '$\equiv$' is reflexive. □

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. Let $a, b, n \in \mathbb{Z}$, and suppose $a \equiv b \pmod n$. Then by definition, $n|(a-b)$, so $\exists k \in \mathbb{Z}$ such that $a - b = kn \Rightarrow b - a = (-k)n$. Since $k \in \mathbb{Z} \Rightarrow -k \in \mathbb{Z}$, it follows that $n|(b-a)$, and hence $b \equiv a \pmod n$. This shows that '$\equiv$' is symmetric. □

Theorem 1.11. *Let* a, b, c, *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. Let $a, b, c, n \in \mathbb{Z}$. Suppose that $a \equiv b \pmod n$ and $b \equiv c \pmod n$. Then $\exists r, s \in \mathbb{Z}$ such that $(a-b) = rn$ and $(b-c) = sn$. Observe,

$$\begin{aligned} (a-b)+(b-c) &= rn + sn \\ \Rightarrow (a-c) &= (r+s)n \end{aligned}$$

and since $r, s \in \mathbb{Z} \Rightarrow (r+s) \in \mathbb{Z}$, it follows that $n|(a-c) \iff a \equiv c \pmod n$. This shows that '$\equiv$' is transitive. □

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. Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 0$. Suppose $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Then by definition, $n|(a-b)$ and $n|(c-d)$. Hence $\exists r, s \in \mathbb{Z}$ such that $(a-b) = rn$ and $(c-d) = sn$. Now,

$$\begin{aligned} (a-b)+(c-d) &= rn + sn \\ \Rightarrow (a+c)-(b+d) &= (r+s)n \end{aligned}$$

and since $r, s \in \mathbb{Z} \Rightarrow (r+s) \in \mathbb{Z}$, it follows that $n|(a+c)-(b+d) \iff a + c \equiv b + d \pmod n$. □

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. Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 0$. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then by definition, $n|(a-b)$ and $n|(c-d)$. Hence $\exists r, s \in \mathbb{Z}$ such that $(a-b) = rn$ and $(c-d) = sn$. Now,

$$\begin{aligned} (a-b)-(c-d) &= rn - sn \\ \Rightarrow (a-c)-(b-d) &= (r-s)n \end{aligned}$$

and since $r, s \in \mathbb{Z} \Rightarrow (r-s) \in \mathbb{Z}$, it follows that $n|(a-c)-(b-d) \iff a-c \equiv b-d \pmod{n}$. □

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. Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 0$. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then by definition, $n|(a-b)$ and $n|(c-d)$. Hence $\exists r, s \in \mathbb{Z}$ such that $(a-b) = rn$ and $(c-d) = sn$. Now,

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + (c-d)b \\ &= (rn)c + (sn)b \\ &= (rc + sb)n \end{aligned}$$

and since $r, s, b, c \in \mathbb{Z} \Rightarrow (rc+sb) \in \mathbb{Z}$, it follows that $n|(ac-bd) \iff ac \equiv bd \pmod{n}$. □

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. Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and suppose that $a \equiv b \pmod{n}$. Then $\exists k \in \mathbb{Z}$ such that $(a-b) = kn$. Observe,

$$\begin{aligned} a^2 - b^2 &= (a+b)(a-b) \\ &= (a+b)(kn) \\ &= (ka+kb)n \end{aligned}$$

and since $a, b, k \in \mathbb{Z} \Rightarrow (ka+kb) \in \mathbb{Z}$, it follows that $n|a^2 - b^2 \iff a^2 \equiv b^2 \pmod{n}$. □

Alternatively, the proof to this exercise follows immediately from theorem 1.14 by multiplying $a \equiv b \pmod{n}$ by itself to get $(a)(a) \equiv (b)(b) \pmod{n} \iff a^2 \equiv b^2 \pmod{n}$.

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. Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and suppose that $a \equiv b \pmod{n}$. We already know from exercise 1.15 that $a \equiv b \pmod{n} \Rightarrow a^2 \equiv b^2 \pmod{n}$. Now using theorem 1.14,

$$(a^2)(a) \equiv (b^2)(b) \pmod{n} \iff a^3 \equiv b^3 \pmod{n}$$

□

Exercise 1.17. *Let $a, b,$ 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. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $k > 1$. Suppose that $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$. Then from theorem 1.14, it follows immediately that

$$(a)(a^{k-1}) \equiv (b)(b^{k-1}) \pmod{n} \iff a^k \equiv b^k \pmod{n}$$

□

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. (By Induction) Let $a, b, k, n \in \mathbb{Z}$ with $n > 0$ and $k > 0$. Suppose $a \equiv b \pmod{n}$. Let $P(n)$ be the statement: $a^n \equiv b^n \pmod{n}$.

Base Case ($P(1)$): The base case is trivially established by the supposition that $a \equiv b \pmod{n}$.

Induction Step: The induction step has already been established in exercise 1.17, where it was shown that $P(n-1) \Rightarrow P(n)$ $\forall n \in \mathbb{Z}$ with $n > 1$.

It follows from the principle of mathematical induction that $P(k)$ is true $\forall k \in \mathbb{Z}$ with $k > 0$. □

Exercise 1.19. *Illustrate each of Theorems 1.12-1.18 With an Example Using Actual Numbers.*

1.12: *Take $a = 1, b = 3, c = 2, d = 4,$ and $n = 2$. Then $1 \equiv 3 \pmod{2}$ and $2 \equiv 4 \pmod{2}$, from which it is clear that $1 + 2 \equiv 3 + 4 \pmod{2}$ since $3 \equiv 7 \pmod{2}$.*

1.13: *Take $a = 1, b = 3, c = 2, d = 4,$ and $n = 2$. Then $1 \equiv 3 \pmod{2}$ and $2 \equiv 4 \pmod{2}$, from which it is clear that $1 - 2 \equiv 3 - 4 \pmod{2}$ since $-1 \equiv -1 \pmod{2}$.*

1.14: *Take $a = 1, b = 3, c = 2, d = 4,$ and $n = 2$. Then $1 \equiv 3 \pmod{2}$ and $2 \equiv 4 \pmod{2}$, from which it is clear that $(1)(2) \equiv (3)(4) \pmod{2}$ since $2 \equiv 12 \pmod{2}$.*

1.15: *Take $a = 1, b = 3,$ and $n = 2$. Observe that $1 \equiv 3 \pmod{2}$, and $1^2 \equiv 3^2 \pmod{2}$ since $1 \equiv 9 \pmod{2}$.*

1.16: Take $a = 1, b = 3$, *and* $n = 2$. *Observe that* $1 \equiv 3 \pmod 2$, *and* $1^3 \equiv 3^3 \pmod 2$ *since* $1 \equiv 27 \pmod 2$.

1.17: Simply use 1.15 above with $k = 2$.

1.18: Simply use 1.16 above with $k = 3$.

Question 1.20. *Let* a, b, c, *and* n *be integers for which* $ac \equiv bc \pmod n$. *Can we conclude that* $a \equiv b \pmod n$*?*

Answer. No, we cannot make that conclusion. Take $a = 2, b = 3, c = 4$, and $n = 2$. Then $ac \equiv bc \pmod n$ gives $(2)(4) \equiv (3)(4) \pmod 2$, which is a true statement, but $a \equiv b \pmod n$ gives $2 \equiv 3 \pmod 2$, which is false.

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* $n \equiv m \pmod 3$.

Proof. Let $n \in \mathbb{N}$. Write n in base 10 as $n = a_k a_{k-1} \ldots a_1 a_0$. Let $m := a_k + a_{k-1} + \cdots + a_1 + a_0$. Observe that we can write n as the sum $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10^1 + a_0$. Then,

$$\begin{aligned} n - m &= (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10^1 + a_0) - (a_k + a_{k-1} + \cdots + a_1 + a_0) \\ &= a_k \cdot 9(10^{k-1}) + a_{k-1} \cdot 9(10^{k-2}) + \cdots + a_1 \cdot 9 \\ &= 3\left(a_k \cdot 3(10^{k-1}) + a_{k-1} \cdot 3(10^{k-2}) + \cdots + a_1 \cdot 3\right) \end{aligned}$$

and since $\left(a_k \cdot 3(10^{k-1}) + a_{k-1} \cdot 3(10^{k-2}) + \cdots + a_1 \cdot 3 \in \mathbb{Z}\right)$, it follows that $3|(n - m) \iff n \equiv m \pmod 3$. □

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 $n \in \mathbb{N}$ expressed in base 10, and let m be equal to the sum of its digits. Suppose that n is divisible by 3. Then $\exists k \in \mathbb{Z}$ such that $n = 3k$. By theorem 1.21, we know that $n \equiv m \pmod 3$ so that $3|(n - m)$. Thus, $\exists \ell \in \mathbb{Z}$ such that $n - m = 3\ell \Rightarrow 3k - m = 3\ell \Rightarrow m = 3(k - \ell)$. Since $k, \ell \in \mathbb{Z} \Rightarrow (k - \ell) \in \mathbb{Z}$, it follows that m - the sum of the digits of n - 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 $n \in \mathbb{N}$ expressed in base 10, and let m be equal to the sum of its digits. Suppose that m is divisible by 3. Then $\exists k \in \mathbb{Z}$ such that $m = 3k$. By theorem 1.21, we know that $n \equiv m \pmod 3 \iff 3|(n - m)$. Hence, $\exists \ell \in \mathbb{Z}$ such that $n - m = 3\ell \Rightarrow n - 3k = 3\ell \Rightarrow n = 3(k + \ell)$. Since $k, \ell \in \mathbb{Z} \Rightarrow (k + \ell) \in \mathbb{Z}$, it follows that n is divisible by 3. □

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

From the proof of theorem 1.21, we can see in the last line where we subtracted $n-m$ that instead of factoring 3 out, we can factor out 9 so that

$$n - m = 9\left(a_k \cdot (10^{k-1}) + a_{k-1} \cdot (10^{k-2}) + \cdots + a_1 \cdot\right)$$

which implies that $n \equiv m \pmod{9}$ for all natural numbers n expressed in base 10 with m defined as the sum of their digits. Then by replacing all the "3's" in theorems 1.22 and 1.23 with "9's", we are able to state the following theorem: A natural number n that is expressed in base 10 is divisible by 9 if and only if the sum of its digits is divisible by 9.

The Division Algorithm

Exercise 1.25. *Illustrate the Division Algorithm for:*

1. $m = 25, n = 7$.
   Here, we have $q = 4$ and $r = 1$. Then $0 \leq 1 \leq (7-1)$, and $25 = 7(4) + 1$.

2. $m = 277, n = 4$.
   Here, we have $q = 68$ and $r = 1$. Then $0 \leq 1 \leq (4-1)$, and $277 = 4(69) + 1$.

3. $m = 33, n = 11$.
   Here, we have $q = 3$ and $r = 0$. Then $0 \leq 0 \leq (11-1)$, and $33 = 11(3) + 0$.

4. $m = 33, n = 45$.
   Here, we have $q = 0$ and $r = 33$. Then $0 \leq 33 \leq (45-1)$, and $33 = 45(0) + 33$.

Theorem 1.26. *The existence part of the Division Algorithm:*
Let n and m be natural numbers. Then there exist integers q and r such that

$$m = nq + r$$

Proof. Let $n, m \in \mathbb{N}$. Consider the set $S := \{k \in \mathbb{Z} \mid (k+1)n > m\}$. Then S is non-empty since $(m+1)n > m \Rightarrow m \in S$. By the well-ordering axiom for the natural numbers, S has a least element, say q. We can then write $qn \leq m < (q+1)n \Rightarrow 0 \leq m - nq < n$. Choose $r = m - nq$. It follows that $0 \leq r \leq (n-1)$, and $m = nq + r$. □

Theorem 1.27. *The uniqueness part of the Division Algorithm :*
Let n and m be natural numbers. If q, q' and r, r' are any integers that satisfy

$$\begin{aligned} m &= nq + r \\ &= nq' + r' \end{aligned}$$

with $0 \leq r, r' \leq n-1$, then $q = q'$ and $r = r'$.

Proof. Let $m, n \in \mathbb{N}$. By theorem 1.26, $\exists q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r \leq n - 1$. Suppose that for some $q', r' \in \mathbb{Z}$ we also have that $m = nq' + r'$ and $0 \leq r' \leq n - 1$.
Then $nq + r = nq' + r' \Rightarrow n(q - q') = r' - r$. From theorem 1.26, q is chosen to be the least element of the set $S := \{k \in \mathbb{Z} \mid (k+1)n > m\}$. Hence, $q' = q$ or $q' > q$.
If $q' = q'$, then $n(0) = r' - r \Rightarrow r' = r$, and we are done.
Suppose that $q' > q$. Then $q' - q \geq 1$ since $q', q \in \mathbb{Z}$, which implies $n(q' - q) \geq n$. Recall that $n(q' - q) = r - r'$, which can be rearranged to write $r = n(q' - q) + r'$, and since $r' \geq 0$, this implies that $r \geq n$, a contradiction since r satisfies $0 \leq r \leq n - 1$. Hence, the only possibility is that $q' = q$, which shows uniqueness. □

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 $r_1 = r_2$.*

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$.

($\Rightarrow$) Suppose that $a \equiv b \pmod{n}$.
By definition, $n|(a - b)$, so $\exists k \in \mathbb{Z}$ such that $a - b = kn$. Now, by the Division Algorithm, $\exists!$ $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 \leq n - 1$ such that $a = nq_1 + r_1$ and $b = nq_2 + r_2$. Subtracting these two equations gives

$$\begin{aligned} a - b &= nk \\ \Rightarrow a &= b + nk \\ &= (nq_2 + r_2) + nk \\ &= n(q_2 + k) + r_2 \end{aligned}$$

and by the uniqueness part of the Division Algorithm, it follows that $r_1 = r_2$.

($\Leftarrow$) Conversely, suppose that a and b have the same remainder when divided by n. In other words, suppose that given $a = nq_1 + r_1$ $(0 \leq r_1 \leq n - 1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n - 1)$, we have that $r_1 = r_2 = r$.
Observe,

$$\begin{aligned} a - b &= (nq_1 + r) - (nq_2 + r) \\ &= n(q_1 - q_2) \end{aligned}$$

$$\Rightarrow n|(a - b) \text{ since } (q_1 - q_2) \in \mathbb{Z}$$

$$\iff a \equiv b \pmod{n}$$

□

Greatest Common Divisors and Linear Diophantine Equations

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

Answer. Yes, as the integer 1 will always divide any two integers.

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

Answer. Only in the case where both of the "two" integers is 0 is it possible to have infinitely many common divisors. This is because for any other integer in $\mathbb{Z} \setminus \{0\}$, there is a unique way to prime factorize the integer, which implies that every integer that's not zero has a finite number of divisors, limiting the number of common divisors it's able to have with other integers.

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

1. $(36, 22)$
   Prime factorizing, $36 = 2^2 \cdot 3^2$ *and* $22 = 2 \cdot 11$*. Hence,* $(36, 22) = 2$.

2. $(45, -15)$
   Prime factorizing, $45 = 3^2 \cdot 5$ *and* $-15 = -3 \cdot 5$*. Hence,* $(45, -15) = 15$.

3. $(-296, -88)$
   Prime factorizing, $-296 = -2^3 \cdot 37$ *and* $-88 = 2^3 \cdot 11$*. Hence,* $(-296, 88) = 8$.

4. $(0, 256)$
   By inspection, $(0, 256) = 256$.

5. $(15, 28)$
   Prime factorizing, $15 = 3 \cdot 5$ *and* $28 = 2^2 \cdot 7$*. Hence,* $(15, 28) = 1$.

6. $(1, -2436)$
   By inspection, $(1, -2436) = 1$.

Hence, only pairs 5 and 6 are 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 $a, n, b, r, k \in \mathbb{Z}$ with $a = nb + r$. Furthermore, suppose that $k|a$ and $k|b$. Then $\exists s, t \in \mathbb{Z}$ such that $a = kr$ and $b = kt$. Observe,

$$\begin{aligned} a &= nb + r \\ \Rightarrow kr &= n(kt) + r \\ \Rightarrow r &= k(r - nt) \\ \Rightarrow k|r &\text{ since } (r - nt) \in \mathbb{Z} \end{aligned}$$

□

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

Proof. Let $a, b, n_1, r_1 \in \mathbb{Z}$ with a and b not both 0, and $a = n_1 b + r_1$.
Let $d := (a, b)$ (we can call d the greatest common divisor of a and b with certainty because we know that we cannot have both a and b be zero). Then d divides both a and b. By Theorem 1.32, it follows that $d | r_1$ since $a = n_1 b + r_1$.
We claim that d is also the greatest common divisor of b and r_1. Let $d' = (b, r_1)$. Since d divides both b and r_1, it must be less than or equal to $(b, r_1) = d'$. Furthermore, notice that by renaming variables appropriately, Theorem 1.32 also says that if for some $p \in \mathbb{Z}$ we have $p|b$ and $p|r_1$, then $p|a$. Hence, since $r_1 = -n_1 b + a$, $d'|r_1$, and $d'|b$, it follows that $d'|a$. Since d' divides both a and b, it must be less than or equal to $(a, b) = d$.
Putting everything together, $d' \leq d$ and $d \leq d' \Rightarrow d = d' \Rightarrow (a, b) = (b, r_1)$. □

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

Observe,

$$\begin{aligned}
51 &= 3(15) + 6 \\
&\quad \textit{Take } a = 51, b = 15, n = 3, r = 6 \\
&\quad \textit{Thm 1.32 } \Rightarrow (51, 15) = (15, 6) \\
15 &= 2(6) + 3 \\
&\quad \textit{Take } a = 15, b = 6, n = 2, r = 3 \\
&\quad \textit{Thm 1.32 } \Rightarrow (15, 6) = (6, 3) \\
6 &= 2(3) + 0 \\
&\quad \textit{Take } a = 6, b = 3, n = 2, r = 0 \\
&\quad \textit{Thm 1.32 } \Rightarrow (6, 3) = (3, 0)
\end{aligned}$$

Following the chain of equalities down, it follows that $(51, 15) = (3, 0) = 3$.

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

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

Step 1: *Use the Division Algorithm to find unique $q, r \in \mathbb{Z}$ such that $0 \leq r \leq b - 1$ and $a = nb + r$.*

Step 2: *Take the resulting quotient and remainder, and reinterpret them as, respectively, the dividend and divisor relabelling q as a and r as b, and repeat Step 1. Notice that the $0 \leq r \leq q$ condition guarantees that the new remainder is strictly less than the old remainder.*

Step 3: *Repeat Step 2 until $r = 0$ (this must eventually happen since the remainder is strictly decreasing in each step and satisfies $r \geq 0$). The value of b corresponding to the line containing $r = 0$ is the value of the original desired (a, b).*

Exercise 1.36. *Use the Euclidean Algorithm to find*

1. $(96, 112)$.

$$\begin{aligned} 112 &= 1(96) + 16 \\ 96 &= 6(16) + 0 \end{aligned}$$

Hence, $(96, 112) = 16$.

2. $(162, 31)$.

$$\begin{aligned} 162 &= 5(31) + 7 \\ 31 &= 4(7) + 3 \\ 7 &= 2(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

Hence, $(162, 31) = 1$.

3. $(0, 256)$.

$$0 = 0(256) + 0$$

Hence, $(0, 256) = 256$.

4. $(-288, -166)$.

$$\begin{aligned} -288 &= 2(-166) + 44 \\ -166 &= -4(44) + 10 \\ 44 &= 4(10) + 4 \\ 10 &= 2(4) + 2 \\ 4 &= 2(2) + 0 \end{aligned}$$

Hence, $(-288, -166) = 2$.

5. $(1, -2436)$.

$$-2436 = -2436(1) + 0$$

Hence, $(1, -2436) = 1$.

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

We apply the Euclidean Algorithm to 162 and 31:

$$\begin{aligned} 162 &= 5(31) + 7 \\ 31 &= 4(7) + 3 \\ 7 &= 2(3) + 1 \end{aligned}$$

Back substituting starting with the bottom line, we have

$$\begin{aligned} 7 - 2(3) &= 1 \\ \Rightarrow 7 - 2(31 - 4(7)) &= 1 \\ 9(7) - 2(31) &= 1 \\ \Rightarrow 9(162 - 5(31)) - 2(31) &= 1 \\ 9(162) - 47(31) &= 1 \end{aligned}$$

Hence, $x = 9$ and $y = -47$ satisfy the equation.

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. Let $a, b \in \mathbb{Z}$ with $(a, b) = 1$. Use the Division Algorithm to find the $q_1, r_1 \in \mathbb{Z}$ with $0 \leq r_1 \leq b - 1$ to write

$$a = q_1 b + r_1$$

By theorem 1.32, $(a, b) = (b, r_1)$. Use the Division Algorithm again to find $q_2, r_2 \in \mathbb{Z}$ with $0 \leq r_2 \leq r_1 - 1 < r_1$ to write

$$b = q_2 r_1 + r_2$$

Theorem 1.32 again gives $(b, r_1) = (r_1, r_2)$ and hence $(a, b) = (r_1, r_2)$. Continuing in this fashion, we can generate a sequence of strictly decreasing integers $r_1 > r_2 > \cdots > r_k$ bounded from below by 0. Hence, $\exists n \in \mathbb{N}$ such that $r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$. Moreover, this sequence of numbers satisfies $1 = (a, b) = (r_{i-1}, r_i)$ $\forall 1 \leq i \leq n$. Hence, by the Euclidean Algorithm, $r_n = 1$. Now consider the system of n equations

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + 1 \end{aligned}$$

Starting with the n-th equation, we can now iteratively eliminate the r_k by stepping backwards and substituting the $k - th$ equation in the array. After the resulting equation has been simplified, we will be left with an equation relating a, b, and 1 of the form $ax+by=1$, where $x, y \in \mathbb{Z}$. □

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. Let $a, b \in \mathbb{Z}$ and suppose $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. Let $d = (a, b)$ (we know that not both x and y can be zero since they satisfy $ax + by = 1$). Since $d|a$ and $d|y$, by Theorem 1.32, $d|1 \Rightarrow d = 1$, as desired. □

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 $a, b \in \mathbb{Z}$ not both 0. The proof of this theorem will be done in an analogous manner to Theorem 1.38. Use the Division Algorithm to find the $q_1, r_1 \in \mathbb{Z}$ with $0 \leq r_1 \leq b - 1$ to write

$$a = q_1 b + r_1$$

By Theorem 1.32, $(a, b) = (b, r_1)$. Use the Division Algorithm again to find $q_2, r_2 \in \mathbb{Z}$ with $0 \leq r_2 \leq r_1 - 1 < r_1$ to write

$$b = q_2 r_1 + r_2$$

Theorem 1.32 again gives $(b, r_1) = (r_1, r_2)$ and hence $(a, b) = (r_1, r_2)$. Continuing in this fashion, we can generate a sequence of strictly decreasing integers $r_1 > r_2 > \cdots > r_k$ bounded from below by 0. Hence, $\exists n \in \mathbb{N}$ such that $r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$. Moreover, this sequence of numbers satisfies $1 = (a, b) = (r_{i-1}, r_i)$ $\forall 1 \leq i \leq n$. Hence, by the Euclidean Algorithm, $r_n = (a, b)$. Now consider the system of n equations

$$\begin{array}{rcl}
a & = & q_1 b + r_1 \\
b & = & q_2 r_1 + r_2 \\
r_1 & = & q_3 r_2 + r_3 \\
 & \vdots & \\
r_{n-3} & = & q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} & = & q_n r_{n-1} + (a, b)
\end{array}$$

Starting with the n-th equation, we can now iteratively eliminate the r_k by stepping backwards and substituting the $k-th$ equation in the array. After the resulting equation has been simplified, we will be left with an equation relating a, b, and 1 of the form $ax + by = (a, b)$, where $x, y \in \mathbb{Z}$. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose that $a|bc$ and $(a, b) = 1$.
Since $a|bc$, $\exists k \in \mathbb{Z}$ such that $bc = ka$. Now since $(a, b) = 1$, by Theorem 1.39, $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1 \Rightarrow acx + bcy = c \Rightarrow acx + kay = c \Rightarrow c = a(cx + ky)$. Since $c, x, k, y \in \mathbb{Z} \Rightarrow (cx + ky) \in \mathbb{Z}$, it follows that $a|c$. □

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

Proof. Let $a, b, n \in \mathbb{Z}$. Suppose that $a|n$, $b|n$, and $(a, b) = 1$. Then $\exists r, s \in \mathbb{Z}$ such that $n = ra$ and $n = sb$. By Theorem 1.38, $(a, b) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying both sides of this equation by n,

$$\begin{aligned} axn + byn &= n \\ \Rightarrow ax(sb) + by(ra) &= n \\ \Rightarrow n &= ab(xs + yr) \end{aligned}$$

and since $x, y, r, s \in \mathbb{Z} \Rightarrow (xs + yr) \in \mathbb{Z}$, it follows that $ab|n$. □

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

Proof. Let $a, b, n \in \mathbb{Z}$ with $(a, n) = 1$ and $(b, n) = 1$. Then by Theorem 1.38,
$\exists x_1, x_2, y_1, y_2 \in \mathbb{Z}$ such that $ax_1 + ny_1 = 1$ and $bx_2 + ny_2 = 1$. Multiplying these equations together,

$$\begin{aligned} (ax_1 + ny_1)(bx_2 + ny_2) &= 1 \\ \Rightarrow (ab)(x_1x_2) + (n)(ax_1y_2 + bx_2y_1 + ny_1y_2) &= 1 \end{aligned}$$

and since $(ax_1y_2 + bx_2y_1 + ny_1y_2) \in \mathbb{Z}$, it follows from Theorem 1.39 that $(ab, n) = 1$. □

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

Answer. After observing the results of Theorems 1.41 to 1.43, I believe that adding the condition that $(c, n) = 1$ will allow us to obtain the desired conclusion. We state this as the following Theorem:
Let a, b, c, and n be integers with $n > 0$. Then $ac \equiv bc \pmod{n}$ and $(c, n) = 1$ implies that $a \equiv b \pmod{n}$.

Proof. Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$, $ac \equiv bc \pmod{n}$ and $(c, n) = 1$. Then $\exists k \in \mathbb{Z}$ such that $(ac - bc) = nk \Rightarrow nk = c(a - b)$, and since $(a - b) \in \mathbb{Z}$, it follows that $c|nk$. By Theorem 1.41, $c|nk$ and $(c, n) = 1 \Rightarrow c|k$. Hence $\exists \ell \in \mathbb{Z}$ such that $k = \ell c$. Now, $nk = c(a - b) \Rightarrow n\ell c = c(a - b) \Rightarrow n\ell = (a - b) \Rightarrow n|(a - b) \iff a \equiv b \pmod{n}$. □

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 $a \equiv b \pmod{n}$.*

Proof. See Question 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 that there are integers x and y that satisfy the equation $ax + by = c$. What condition must c satisfy in terms of a and b?

Answer. The first observations that I can make are that a must divide $(c - by)$ and b must divide $(c - ax)$. Another observation is that if $c = (a, b)$, then Theorem 1.40 guarantees that there are integer solutions to the equation. The fact there are integer solutions *only if* $c = (a, b)$ isn't clear to me, but I have a hunch that this is the case.

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

Conjecture. Given integers a, b, and c, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $(a, b)|c$.
Note: I had to adjust my conjecture whilst trying to prove the original one that said $c = (a, b)$ instead of $(a, b)|c$! It became clear to me that c could be any integer multiple of (a, b), not just (a, b) itself.

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

($\Rightarrow$) Suppose that $\exists x, y \in \mathbb{Z}$ such that $ax+by = c$. Let $d = (a, b)$. Then $d|a$ and $d|b \Rightarrow d|ax$ and $d|by \Rightarrow d|c$ since $c = ax + by$. It follows that $(a, b)|c$, as desired.
Remark: Notice that if we let d_i represent an arbitrary common divisor of a and b, then the above argument still holds. It's only in the converse implication, we will see, that it is necessary that d_i be the *greatest* common divisor.

($\Leftarrow$) Conversely, suppose that $(a, b)|c$. If a and b are both zero, then the implication is trivial (choose $c = 0$). Hence, we assume that not both a and 0 is zero.
By Theorem 1.40, $\exists x_0, y_0 \in \mathbb{Z}$ such that $ax_0+by_0 = (a, b)$. Now, $(a, b)|c \Rightarrow \exists k \in \mathbb{Z}$ such that $c = k(a, b)$. Hence, $ax_0k + by_0k = k(a, b) = c$. Thus, if we choose $x = x_0k \in \mathbb{Z}$ and $y = y_0k \in \mathbb{Z}$, then $ax + by = c$, as desired.

□

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 $(a, b)|c$.*

Proof. See Question 1.47. □

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 $ax + by = c$?

Answer. Let $a, b, c \in \mathbb{Z}$, and consider the equation $ax + by = c$ for some $x, y \in \mathbb{Z}$. We know from Theorem 1.48 that $(a, b)|c$. By simply renaming variables, we also know from Theorem 1.48 that $(x, y)|C$. Now, Suppose that $x_0, y_0 \in \mathbb{Z}$ satisfy $ax_0 + by_0 = c$. Moreover, suppose that $x = x_0 + h$ and $y = y_0 + k$ are also solutions for some $h, k \in \mathbb{Z}$. Substituting into the equation gives

$$\begin{aligned} ax + by &= c \\ a(x_0 + h) + b(y_0 + k) &= c \\ ax_0 + by_0 &= c - ah - bk \end{aligned}$$

for equality with the previous equation to hold, it must be the case that

$$\begin{aligned} -ah - bk &= 0 \\ \Rightarrow ah &= -bk \end{aligned}$$

By inspection, with d_i representing any common divisor of a and b, and $r \in \mathbb{Z}$, $h = \frac{rb}{d_i}$ and $k = \frac{-ra}{d_i}$ is always satisfies the above equation. Note that the condition that d_i be a common divisor of a and b is important for $\pm\frac{abr}{d_i}$ to be an integer, and demanding that both a and b show up on both sides of the equation is important for ensuring that the division yields the same value on both sides.

To summarize,

$$x = x_0 + \frac{rb}{d_i} \text{ and } y = y_0 - \frac{ra}{d_i}$$

where $r \in \mathbb{Z}$ and d_i is a common divisor of a and b is another solution to $ax_0 + by_0 = c$.

Exercise 1.50. *(Euler). 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?*

Answer. Let h denote the number of horses bought, and x the number of oxen bought. Then the linear Diophantine equation associated with this problem is

$$31h + 21x = 1770$$

where $h, x \in \mathbb{Z}^+$ (only positive, integer horses and oxen may be bought).

We first find a solution by employing the Division Algorithm on 31 and 21.

$$\begin{aligned} 31 &= 1(21) + 10 \\ 21 &= 2(10) + 1 \end{aligned}$$

Hence,

$$\begin{aligned} 21 - 2(10) &= 1 \\ 21 - 2(31 - 21) &= 1 \\ 31(-2) + 21(3) &= 1 \\ \Rightarrow 31(-3540) + 21(5310) &= 1770 \end{aligned}$$

Hence, $h_0 = -3540$ and $x_0 = 5310$ are two possible integer solutions. Based on Theorem 1.48 and what was shown in Question 1.49, any other solutions we are like to find must be relatively prime since $(31, 21) = 1$. Now, from Question 1.49:

$$h = -3540 + \frac{21r}{d_i} \text{ and } x = 5310 - \frac{31r}{d_i}$$

where $r \in \mathbb{Z}$. Since $(31, 21) = 1$, d_i is necessarily equal to 1. Thus,

$$h = -3540 + 21r \text{ and } x = 5310 - 31r$$

By trial and error, we require $r = 169$ to get $h > 0$. Furthermore, we can increase r up to 171 before x starts becoming negative. Hence, the possible numbers of horses and oxen that the farmer bought are:

$$\begin{aligned} h &= 9 & x &= 71 \\ h &= 30 & x &= 40 \\ h &= 51 & x &= 9 \end{aligned}$$

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. Let $a, b, c, x_0, y_0 \in \mathbb{Z}$ with a and b not both 0 such that $ax_0 + by_0 = c$. Let

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

It is clear that $x, y \in \mathbb{Z}$ since $(a, b)|b$ and $x_0 \in \mathbb{Z} \Rightarrow (x_0 + \frac{b}{(a,b)}) \in \mathbb{Z}$ and $(a, b)|a$ and $y_0 \in \mathbb{Z} \Rightarrow (y_0 + \frac{a}{(a,b)}) \in \mathbb{Z}$. Now observe,

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{(a, b)}\right) + b\left(y_0 - \frac{a}{(a, b)}\right) \\ &= ax_0 + \frac{ab}{(a, b)} + by_0 - \frac{ab}{(a, b)} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

□

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.

Answer. This was already done in Question 1.49.

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*

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

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. Let $a, b, c \in \mathbb{Z}$ with a and b not both 0. Suppose that $x = x_0$ and $y = y_0$ is an integer solution to the equation $ax + by = c$. For some $k \in \mathbb{Z}$, define

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

We can verify through direct substitution that the linear Diophantine equation $ax + by = c$ is satisfied:

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{kb}{(a,b)}\right) + b\left(y_0 - \frac{kb}{(a,b)}\right) \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

the fact that every solution to the linear Diophantine equation is of this form requires a bit of work.
Suppose that $x', y' \in \mathbb{Z}$ also satisfies $ax' + y' = c$. Then,

$$\begin{aligned} ax + by &= ax' + by' \\ \Rightarrow a(x - x') &= -b(y - y') \\ \Rightarrow ak(x - x') &= -bk(y - y') \ \forall k \in \mathbb{Z} \end{aligned}$$

Hence, all possible solutions are of the form $(x - x') = \frac{kb}{d}$ and $(y - y') = -\frac{ka}{d}$ where d is a common divisor of both a and b (i.e. all possible numbers that yield an integer upon division by other means than simply cancelling out k). Since we are multiplying by an arbitrary integer k, however, it is sufficient to use the greatest common divisor, (a, b), to account for all possible solutions. Are of the form $(x - x') = \frac{kb}{d}$ and $(y - y') = -\frac{ka}{d}$, or

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

where x' and y' are any integers that satisfy $ax' + by' = c$. □

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

By inspection, $x_0 = 1$ and $y_0 = 1$ are solutions to the linear Diophantine equation $24x_0 + 9y_0 = 33$. Notice that $(24, 9) = 3$. Hence, by Theorem 1.53, all integer solutions to the above equation are given by:

$$x = 1 + \frac{9k}{3} \textit{ and } y = 1 - \frac{24k}{3}$$
$$\Rightarrow x = 1 + 3k \textit{ and } y = 1 - 8k$$

where $k \in \mathbb{Z}$.

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. Let $a, b \in \mathbb{Z}$, not both 0, and $k \in \mathbb{N}$. We have that $(a, b)|a \Rightarrow (k \cdot (a, b))|ka$ and $(a, b)|b \Rightarrow (k \cdot (a, b))|kb$, which implies that $(k \cdot (a, b))|(ka, kb)$. By Theorem 1.40, $\exists x, y \in \mathbb{Z}$ such that

$$\begin{aligned} ax + by &= (a, b) \\ (ka)x + (kb)y &= k \cdot (a, b) \\ \Rightarrow (ka, kb)|(k \cdot (a, b)) & \quad \text{(by Theorem 1.32)} \end{aligned}$$

Hence, $k|(ka, kb)$ and $(ka, kb)|(k \cdot (a, b)) \Rightarrow (ka, kb) = k \cdot (a, b)$. □

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

We define $\operatorname{lcm}(a, b)$ as follows:
Given two natural numbers a and b, the ***least common multiple*** *of a and b, denoted $\operatorname{lcm}(a, b)$, is the smallest natural number, say c, for which $a|c$ and $b|c$. Any natural number, say m, that satisfies $a|m$ and $b|m$ is referred to as a* ***common multiple*** *of a and b*

Examples:

1. $\operatorname{lcm}(1, n) = n\ \forall n \in \mathbb{N}$ *since $1|n$ and $n|n$, and n cannot divide any natural number smaller than n.*

2. $\forall p, q \in \mathbb{N}$ *with $(p, q) = 1$, $\operatorname{lcm}(p, q) = pq$. To see this, let $\ell = \operatorname{lcm}(p, q)$. Then by definition, $p|\ell$ and $q|\ell$. By Theorem 1.42, since $(p, q) = 1$, it follows that $pq|\ell$. We know that ℓ must satisfy $\ell \leq pq$ since pq is clearly a common multiple of p and q, and the least common multiple must be less than or equal to any common multiple of p and q. Putting these two facts together, $pq|\ell$ and $\ell \leq pq \Rightarrow \ell = pq$, as desired.*

3. $\forall a, b \in \mathbb{N}$ *with $a|b$, $\operatorname{lcm}(a, b) = b$.*

4. $\operatorname{lcm}(6, 12) = 12$.

5. lcm$(9, 24) = 72$.

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

Proof. Let $a, b \in \mathbb{N}$. Let $d = \gcd(a, b)$ and $e = \operatorname{lcm}(a, b)$.

Then $\exists x, y \in \mathbb{Z}$ such that $a = xd$ and $b = yd$. Let $\ell = xyd$. We claim that $\operatorname{lcm}(a, b) = \ell$. Indeed, it is the case that $xd|xyd \Rightarrow a|\ell$ and $yd|xyd \Rightarrow b|\ell$, so ℓ is at the very least a common multiple of a and b. Hence, it is sufficient to show that ℓ is the smallest such common multiple of a and b. We first note that $(x, y) = 1$ since if they had a common factor, we could obtain a greater common divsor than d by multiplying d by this common factor, which contradicts our choice of d as (a, b).

Let m be a common multiple of a and b. We will show that $\ell|m$.
Since $a|n$ and $b|m$, $\exists k_1, k_2 \in \mathbb{Z}$ such that $m = k_1a = k_1xd$ and $m = k_2b = k_2yd$. Moreover, $(x, y) = 1 \Rightarrow \exists r, s \in \mathbb{Z}$ such that $xr + ys = 1$ (by Theorem 1.40). Now,

$$\begin{aligned} xr + ys &= 1 \\ xrm + ysm &= m \\ xr(k_2b) + ys(k_1a) &= m \\ xr(k_2yd) + ys(k_1xd) &= m \\ xyd(rk_2 + sk_1) &= m \\ \ell(rk_2 + sk_1) &= m \end{aligned}$$

and since $(rk_2 + sk_1) \in \mathbb{Z}$, it follows that $\ell|m$. Hence, ℓ is both a common multiple of a and b, and less than or equal to any common multiple of a and b. It follows that $\operatorname{lcm}(a, b) = \ell = xyd$. Finally, observe that

$$\begin{aligned} \gcd(a, b) \cdot \operatorname{lcm}(a, b) &= d \cdot xyd \\ &= (xd)(yd) \\ &= ab \end{aligned}$$

which shows the desired result.

□

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. Let $a, b \in \mathbb{N}$.

($\Rightarrow$). Suppose that $\operatorname{lcm}(a, b) = ab$. By Theorem 1.57, we also have that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. Hence, $\operatorname{lcm}(a, b) = \gcd(a, b) \cdot \operatorname{lcm}(a, b) \Rightarrow \gcd(a, b) = 1$ (since $\operatorname{lcm}(a, b) \geq 1$) $\iff a$ and b are relatively prime

($\Leftarrow$). Suppose that a and b are relatively prime. Then $\gcd(a, b) = 1$. Let $\ell = \operatorname{lcm}(a, b)$. Then by definition, $a|\ell$ and $b|\ell$. By Theorem 1.42, since $(a, b) = 1$, it follows that $ab|\ell$. We know that ℓ must satisfy $\ell \leq ab$ since ab is clearly a common multiple of a and b, and the least common multiple must be less than or equal to any common multiple of a and b. Putting these two facts together, $ab|\ell$ and $\ell \leq ab \Rightarrow \ell = ab$. Hence, $\operatorname{lcm}(a, b) = ab$ as desired.

□

2 Prime Time

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 $n \in \mathbb{N}$ with $n > 1$. We will prove the theorem by using the principle of strong mathematical induction.

For $k > 1$, let $P(k)$ be the statement: if $k \in \mathbb{N}$, then $\exists$ a prime number p such that $p|k$.

Base case ($P(2)$): $P(2)$ is clearly true since for $2 \in \mathbb{N}$, 2 is a prime number that satisfies $2|2$.

Induction Step: Let $k \in \mathbb{N}$ with $k \geq 2$. Suppose that $P(i)$ is true for $1 \leq i \leq k$. Now consider $k+1 \in \mathbb{N}$. Either $(k+1)$ is a product of natural numbers less than $(k+1)$ or it is not. In other words, $(k+1)$ is either prime or composite. If $(k+1)$ is prime, then we are done since we can choose $p = (k+1)$, and it follows immediately that $p|(k+1)$ since $(k+1)|(k+1)$.
Suppose that $(k+1)$ is composite. Then $(k+1)$ can be written as the product of natural numbers less than $(k+1)$, say

$$k+1 = k_1k_2\dots k_n$$

where $k_1, k_2, \dots, k_n$ are natural numbers, strictly less than $k+1$, and can be chosen such that none of them are equal to 1. Consider k_1. Since $k_1 < k+1$, we know from the induction hypothesis that $\exists p \in \mathbb{N}$ prime such that $p|k_1$. Hence, $\exists m \in \mathbb{Z}$ such that $k_1 = mp$. We now have that

$$k+1 = p(mk_2k_3\dots k_n)$$

and since $(mk_2k_3\dots k_n) \in \mathbb{Z}$, it follows that $p|(k+1)$, which shows $P(k+1)$.

By the principle of strong mathematical induction, it follows that $P(n)$ is true $\forall n \in \mathbb{N}$ with $n > 1$. In other words, $\forall n \in \mathbb{N}$ with $n > 1$, $\exists p$ prime such that $p|n$.

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

Here is a list of the primes less than 100: 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 divide n.*

Proof. Let $n \in \mathbb{N}$ with $n > 1$.

(⇒) Suppose that n is prime. Then n is not the product of natural numbers less than n. In particular, since $\sqrt{n} < n$ for $n > 1$, we have that, $\forall$ primes $p \leq \sqrt{n}$, $p \nmid n$.

(⇐) Suppose that $\forall$ primes $p \leq \sqrt{n}$, $p \nmid n$. By way of contradiction, suppose that n is composite. Then by Theorem 2.1, $\exists$ a prime number p such that $p|n$. Hence, $\exists k \in \mathbb{N}$ such that $n = kp$. From our assumption, p necessarily satisfies $p > \sqrt{n}$. Moreover, since we are assuming that n is composite (and since $p|n$), $p < n$, and so $k > 1$. Furthermore, since $p > \sqrt{n}$, k satisfies $k \leq \sqrt{n}$. Again by Theorem 2.1, $\exists$ a prime number p' such that $p'|k \Rightarrow \exists k' \in \mathbb{Z}$ such that $k = k'p'$, and since $k \leq \sqrt{n}$, we also have that $k', p' \leq \sqrt{n}$. Then, $n = kp = p'(k'p)$, and since $k'p \in \mathbb{Z}$, we have that $p'|n$. This is a contradiction since p' is a prime number satisfying $p \leq \sqrt{n}$. It follows that n is prime.

□

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

By Theorem 2.3, it is sufficient to check if 101 *is divisible by all prime less than or equal to* $\sqrt{101} < \sqrt{121} = 11$. *Hence, we need only check if 101 is divisible by 2, 3, 5, or 7. A quick shows that 101 is not divisible by any of these primes, so we can conclude that 101 is indeed prime.*

Exercise 2.5. *(Sieve of Eratosthenes). Write down all the natural numbers from 1 to 100, prehaps on a* 10×10 *array. Circle the number 2, the smallest prime. Cross off all numbers divisible by 2. Circle 3, the next number that is not crossed out. Cross off all larger numbers that are divisible by 3. Continue to circle the smallest number that is not crossed out and cross out its multiples. Repeat. Why are the circled numbers all the primes less than 100?*

We illustrate the sieve of Eratosthenes as follows:

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

Note that we employed Theorem 2.3 in the construction of the array by circling the remaining natural numbers in purple after we'd finished crossing off the multiples of 7.
The reason why the circled numbers are primes is because they are not divisible by any primes less than themselves, which is a weaker condition than that given in Theorem 2.3 for a number to be prime.

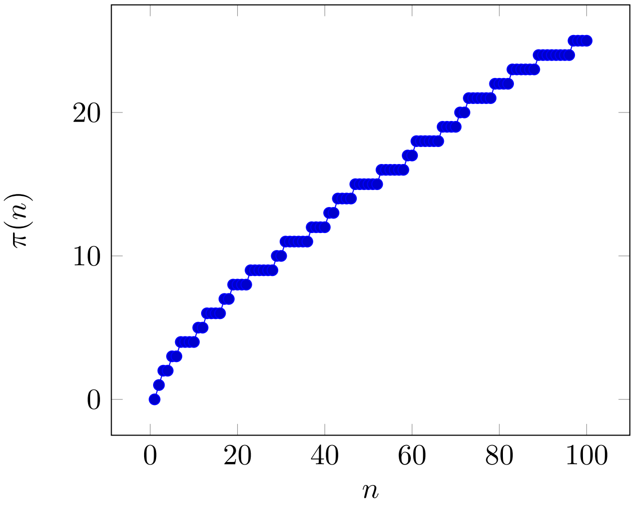
Exercise 2.6. *For each natural number n, define $\pi(n)$ to be the number of primes less than or equal to n.*

1. *Graph $\pi(n)$ for $n = 1, 2, \ldots, 100$.*

   We first make a table for the outputs of $\pi(n)$ (Note: a Python program was written to generate the values for this table).

n	$\pi(n)$						
1	0	26	9	51	15	76	21
2	1	27	9	52	15	77	21
3	2	28	9	53	16	78	21
4	2	29	10	54	16	79	22
5	3	30	10	55	16	80	22
6	3	31	11	56	16	81	22
7	4	32	11	57	16	82	22
8	4	33	11	58	16	83	23
9	4	34	11	59	17	84	23
10	4	35	11	60	17	85	23
11	5	36	11	61	18	86	23
12	5	37	12	62	18	87	23
13	6	38	12	63	18	88	23
14	6	39	12	64	18	89	24
15	6	40	12	65	18	90	24
16	6	41	13	66	18	91	24
17	7	42	13	67	19	92	24
18	7	43	14	68	19	93	24
19	8	44	14	69	19	94	24
20	8	45	14	70	19	95	24
21	8	46	14	71	20	96	24
22	8	47	15	72	20	97	25
23	9	48	15	73	21	98	25
24	9	49	15	74	21	99	25
25	9	50	15	75	21	100	25

Graphing these points gives:



2. *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 function or a decreasing function? Do you suspect that it approaches some specific number (as a limit) as n goes to infinity? Make a conjecture and try to prove it. Proving your conjecture is a difficult challenge. You might use a computer to extend your list of primes to a much larger number and see whether your conjecture seems to be holding up.*

The answer to the above question is given by the very famous Prime Number Theorem (so I unfortunately am not in a position to approach this question as if I have seen it for the first time). The prime number theorem states that $\lim_{n\to\infty} \frac{\pi(n)}{n} \cdot \ln(n) = 1$. In other words, $\pi(n)$ is approximately $\frac{1}{\ln(n)}$ times as large as n. Moreover, $\frac{\pi(n)}{n}$ is generally a decreasing function since $\ln(n)$ being an increasing function implies that its reciprocal is a decreasing function.

Theorem 2.7. (Fundamental Theorem of Arithmetic—Existence Part). *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*

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

Proof. We will prove the Theorem using strong induction. For $k > 1$, let $P(k)$ be the statement that: for the natural number k, $\exists$ distinct prime $p_1, p_2, \ldots, p_m$ and natural numbers $r_1, r_2, \ldots r_m$ such that $k = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$.

Base case ($P(2)$): For the natural number 2, we have that $2 = 2^1$ where $2 \in \mathbb{N}$ is prime and $1 \in \mathbb{N}$, so $P(2)$ follows immediately.
Induction Step: Suppose that $P(i)$ is true $\forall i \in \mathbb{N}$ with $2 \leq i \leq k$. Consider $k+1 \in \mathbb{N}$ (which clearly satisfies $k+1 > 1$).
If $k+1$ is prime, then we are done since we can choose $p_1 = k+1$ and $r_1 = 1$ to express $k+1$ in the form $k+1 = p_1^{r_1}$.
Suppose that $k+1$ is composite. By Theorem 2.1, $\exists p^1 \in \mathbb{N}$ prime such that $p^1 | (k+1) \Rightarrow \exists d \in \mathbb{N}$ such that $k+1 = p^1 d$. Since $k+1$ is composite, we have that $p^1 < (k+1) \Rightarrow d > 1$. Moreover, since $d|(k+1)$, we also have that $d < (k+1)$. We can apply the induction hypothesis to d to find prime $p_1, p_2, \ldots, p_m \in \mathbb{N}$ and $r_1, r_2, \ldots r_m \in \mathbb{N}$ such that

$$d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$$

If p^1 is equal to some p_i for $1 \leq i \leq m$, then we can write

$$k+1 = p_1^{r_1} p_2^{r_2} \ldots p_i^{r_i+1} \ldots p_m^{r_m}$$

Otherwise, we can relabel p as p_{m+1} and choose $r_{m+1} = 1$ to write

$$k+1 = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} p_{m+1}^{r_{m+1}}$$

In either case, we see that $P(k+1)$ follows.

Hence, by the principle of strong mathematical induction, it follows that $P(n)$ is true $\forall n \in \mathbb{N}$ with $n > 1$. □

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

Proof. Let p and $q_1, q_2, \ldots, q_n$ all be primes, and let $k \in \mathbb{N}$. Suppose that $pk = q_1 q_2 \ldots q_n$. Then $p|(q_1 q_2 \ldots q_n)$.

We will prove by induction that if $p|(q_1 q_2 \ldots q_n)$, then $p = q_i$ for some i. Let $P(k)$ be the statement: for prime if $p|q_1 q_2 \ldots q_k$, then $p = q_i$ for some i.

Base Case ($P(1)$): If $p|q_1$, then q_1 prime implies that $p = 1$ or $p = q_1$. Since p is prime, it must be the case that $p = q_1$.

Induction Step: Suppose that $P(k)$ is true for some $k \in \mathbb{N}$, and suppose that $p|q_1 q_2 \ldots q_k q_{k+1} \Rightarrow p|q_{k+1}(q_1 q_2 \ldots q_k)$. If $p = q_{k+1}$, then $P(k+1)$ follows immediately. Otherwise, $p \neq q_{k+1} \Rightarrow (p, q_{k+1}) = 1$ since p and q_{k+1} are distinct primes. Hence, by Theorem 1.41, $p|q_1 q_2 \ldots q_k$. By the induction hypothesis we have that $p|q_i$ for some i, which shows $P(k+1)$.

By the principle of mathematical induction, $\forall n \in \mathbb{N}$, if p and $q_1, q_2, \ldots, q_n$ are all primes with $pk = q_1 q_2 \ldots q_n$ for some $k \in \mathbb{N}$, then $p = q_i$ for some i. □

Theorem 2.9. (Fundamental Theorem of Arithmetic—Uniqueness Part). *Let n be a natural number. Let $\{p_1, p_2, \ldots, p_m\}$ and $\{q_1, q_2, \ldots, q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, \ldots, r_m\}$ and $\{t_1, t_2, \ldots, t_s\}$ be sets of natural numbers such that*

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s} \end{aligned}$$

Then $m = s$ and $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\}$. That is, the sets of prime 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. Let n be a natural number, and let $\{p_1, p_2, \ldots, p_m\}$ and $\{q_1, q_2, \ldots, q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, \ldots, r_m\}$ and $\{t_1, t_2, \ldots, t_s\}$ be sets of natural numbers such that

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s} \end{aligned}$$

Let $P = \{p_1, p_2, \ldots, p_m\}$ and $Q = \{q_1, q_2, \ldots, q_s\}$. Let $p_i \in P$, and let

$$k = \left(\prod_{k=1}^{i-1} p_k^{r_k}\right)\left(\prod_{k=i+1}^{m} p_k^{r_k}\right) = \left(\prod_{k=1}^{m} p_k^{r_k}\right) / p_i^{r_i} \in \mathbb{N}$$

Then $p_i^{r_i} k = q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s} \Rightarrow p_i^{r_i} | q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$, and since each of the q_i are distinct primes, it must be the case that $p_i = q_j$ and $r_i = s_j$ for some $j \in \mathbb{N}$ with $1 \leq j \leq s$ (see Indication 3 further down for a more detailed proof for why this is true). Hence, $p_i \in Q$, and since p_i was an arbitrary element of P, it follows that $P \subseteq Q$. Reversing q_j and p_i and repeating the exact same argument gives the reverse inclusion for $Q \subseteq P$. It follows that $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\}$. Our argument also showed that $r_i = t_j$ if $p_i = q_j$, so we are done. □

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

Observe,

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

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

It is sufficient to determine the number of pairs of prime factors of 2 and 5 that 25! has. Some quick mental counting returns that 25! has 21 factors of 2 and 6 factors of 5. Hence, 25! has 6 zeroes at the end.

Indication 3. Prove the following lemma related to Theorem 2.12:
If a prime p divides a product of primes, then p must equal one of these primes.

Proof. Let p and q_i for some $i \in \mathbb{N}$ denote prime numbers, and suppose that

$$p \mid (q_1 q_2 \dots q_m)$$

We will prove the lemma by induction. Let $P(k)$ be the statement: if p divides a product of k primes, then p must equal one of those primes.

Base Case ($P(1)$): If $p|q_1$, then $\exists d \in \mathbb{N}$ such that $q_1 = pd$. Then we must have $d = 1$ to avoid contradicting the fact that q_1 is prime. Hence $p = q_1$.

Induction Step: Suppose that $P(k)$ is true for some $k \in \mathbb{N}$. Consider $p|q_1(q_2 q_3 \dots q_{k+1})$. If $p|q_1$, then from the base case, $p = q_1$, and so $P(k+1)$ follows immediately. If $p \nmid q_1$, then since p and q_1 are both primes, it must be the case that $(p, q_1) = 1$. From Theorem 1.41, it follows that $p|(q_2 q_3 \dots q_{k+1})$. Now, since p divides a product of k primes, it follows from the induction hypothesis that $p = q_i$ for some $2 \leq i \leq k+1$, which shows $P(k+1)$.

Hence, by the principle of mathematical induction, it follows that if p divides any (finite) product of primes, then p must equal one of those primes. □

Applications of the Fundamental Theorem of Arithmetic

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

Proof. Let a and b be natural numbers greater than 1 and let $p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ be the unique primes factorization of a and let $q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorization of b.

($\Rightarrow$) Suppose that $a|b$.
Then $(p_1^{r_1} p_2^{r_2} \dots p_m^{r_m})|(q_1^{t_1} q_2^{t_2} \dots q_s^{t_s})$. Consider $p_i^{r_i}$ for some $1 \leq i \leq m$. Then we can view the previous statement as p_i dividing the product of primes $q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ r_i many times. By the lemma in Indication 3, we have that $p_i = q_j$ for some $1 \leq j \leq s$. Applying this lemma for each of the r_i factors, we have that there must exist at least r_i many factors of q_j. In other words, $r_i \leq t_j$. Since p_i was arbitrary, the desired statement now follows $\forall i \leq m$.

($\Leftarrow$) Suppose that $\forall i \leq m,\ \exists j \leq s$ such that $p_i = q_j$ and $r_i \leq t_j$. Then, by reindexing the q_j appropriately so that the $i = j$ if $p_i = q_j$, we can write b as

$$b = (p_1^{r_1} p_2^{r_2} \dots p_m^{r_m})(p_1^{t_1-r_1} p_2^{t_2-r_2} \dots p_m^{t_m-r_m})(q_{m+1}^{t_{m+1}} q_{m+2}^{t_{m+2}} \dots q_s^{t_s})$$

$$\Rightarrow b = a\left((p_1^{t_1-r_1} p_2^{t_2-r_2} \dots p_m^{t_m-r_m})(q_{m+1}^{t_{m+1}} q_{m+2}^{t_{m+2}} \dots q_s^{t_s})\right)$$

which shows that $a|b$.

□

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

Proof. Let $a, b \in \mathbb{N}$, and suppose that $a^2|b^2$.
Let $p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of a and b, respectively. Then $a^2|b^2 \Rightarrow \exists k \in \mathbb{N}$ such that $b^2 = ka^2$. Now,

$$\begin{aligned} b^2 &= ka^2 \\ (p_1^{r_1} p_2^{r_2} \dots p_m^{r_m})^2 &= k\left(q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}\right)^2 \\ p_1^{2r_1} p_2^{2r_2} \dots p_m^{2r_m} &= kq_1^{2t_1} q_2^{2t_2} \dots q_s^{2t_s} \end{aligned}$$

Then by Theorem 2.12, since $a^2|b^2$, we have that $\forall i \leq m,\ \exists j \leq s$ such that $p_i = q_j$ and $2r_1 \leq 2t_1 \Rightarrow r_1 \leq t_1$. Hence, by Theorem 2.12 again, it follows that $a|b$. □

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

From unique prime factorization, we know that we can take all the common prime factors that the two numbers have in common. Hence,

$$(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17 = 11^4 \cdot 17 = 248,897$$

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

From unique prime factorization, we know that we need to take the minimum number of prime factors to completely "cover" each number. Hence,

$$\mathrm{lcm}(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17) = 3^{14} \cdot 5^2 \cdot 7^{22} \cdot 11^5 \cdot 13^8 \cdot 17^3$$

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

Conjecture: *Let $a, b \in \mathbb{N}$ and let $p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of a and b, respectively. Let $P = \{p_1, p_2, \dots, p_m\}$ and $Q = \{q_1, q_2, \dots, q_s\}$.*

Define $e_p : P \cup Q \to \mathbb{N}$ by $e_p(p_i) = r_i$ if $p_i \in P$, and $e_p(q) = 1$ if $q \notin P$. Similarly, define $e_q : P \cup Q \to \mathbb{N}$ by $e_q(q_i) = t_i$ if $q_i \in Q$, and $e_q(p) = 1$ if $p \notin Q$. Then

$$\gcd(a, b) = \prod_{p \in P \cap Q} p^{\min(e_p(p), e_q(p))}$$

and

$$\operatorname{lcm}(a, b) = \prod_{p \in P \cup Q} p^{\max(e_p(p), e_q(p))}$$

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?*

Answer. I think that this method is sometimes better than using the Euclidean Algorithm to find (a, b). For cases where the numbers are easy to prime factorize, or a prime factorization is readily available, the above method is much easier and faster. For large numbers where the process of decomposing two numbers into their factors is a sizeable task that involves first finding out whether certain numbers are prime, the Euclidean Algorithm is more efficient.

Indication 4. Show that it is not possible to find $n + 1$ natural numbers $a_1, \dots, a_{n+1}$ less than or equal to $2n$, satisfying the conditions $a_1 = 2$ and for all pairs of numbers (a_i, a_j) in the sequence $\gcd(a_i, a_j) = 1$.

N.B: The above statement supposes that $a_1 < a_2 < \cdots < a_{n+1}$.

Proof. Let $a_1, a_2, \dots, a_{n+1}$ be a sequence of $n + 1$ natural numbers all less than or equal to $2n$ with $a_1 < a_2 < \cdots < a_{n+1}$. Suppose that $a_1 = 2$.
Of the natural numbers less than or equal to $2n$, n of them are divisible by 2, and n of them are not. If any of the a_i is an even number, then we are done since $(a_1, a_i) = 2 \neq 1$. Hence, the other n a_i are necessarily odd numbers if we want to avoid this, but are only $n - 1$ odd numbers that are between 2 and $2n$. Hence, one of the other a_i is an even number, which completes the proof. □

Theorem 2.18. *Given $n + 1$ natural numbers, say $a_1, a_2, \dots, a_{n+1}$, 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. The following argument does not use the Fundamental Theorem of Arithmetic, but it is a proof nonetheless.
Suppose that we have $a_1, a_2, \dots, a_{n+1} \in \mathbb{N}$ with $a_i \leq 2n$ $\forall i \leq n + 1$.
Suppose that x of our $n + 1$ numbers satisfy $1 \leq a_i \leq n$. Then for each of these a_i, $\exists$ a prime p such that $n \leq pa_i \leq 2n$. In other words, there are at least x numbers between n and $2n$ that are multiples of the x numbers we chose. Suppose that we choose y numbers between n and $2n$ (inclusive). Let $X_m = \{a_i \mid a_i \leq n\}$, $X_m = \{k \mid n \leq k \leq 2n \text{ and } a_i | k\}$, and let $Y = \{a_i \mid n \leq a_i \leq 2n\}$. Then by definition, $|X| = x$, $|X_m \geq x$ because of what was

argued before, and $|Y| = y$. If we were to assume that X_m and Y were disjoint, then we would get $x + y \geq n + 1$, a contradiction since there can't be $n + 1$ distinct natural numbers between n and $2n$. Hence, $X_m \cap Y \neq \emptyset$, so $\exists a_i \in X$ and $a_j \in Y$ such that $a_i | a_j$. □

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

Proof. By way of contradiction, suppose that $\exists m, n \in \mathbb{N}$ such that $7m^2 = n^2$. For some $x, y \in \mathbb{N} \cup \{0\}$, let $m = 7^x p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $n = 7^y q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$ (with $p_i \neq 7 \ \forall i \leq m$ and $q_j \neq 7 \ \forall j \leq s$) be the unique prime factorizations of m and n, respectively.
Then $7m^2 = n^2 \Rightarrow 7 \left(7^x p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}\right)^2 = \left(7^y q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}\right)^2 \Rightarrow \left(7^{2x+1}\right) \left(p_1^{2r_1} p_2^{2r_2} \ldots p_m^{2r_m}\right) = \left(7^{2y}\right) \left(q_1^{2t_1} q_2^{2t_2} \ldots q_s^{2t_s}\right)$. By the uniqueness of prime factorizations, it follows that $7^{2x+1} = 7^{2y} \Rightarrow 2x+1 = 2y$, a contradiction since the number on the left hand side is odd, whereas the number on the right hand side is even. It follows that $\nexists m, n \in \mathbb{N}$ such that $7m^2 = n^2$. □

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

Proof. By way of contradiction, suppose that $\exists m, n \in \mathbb{N}$ such that $24m^2 = n^2$. We can rewrite this equation as $(2^3)(3)m^3 = n^3$. For some $x, y \in \mathbb{N} \cup \{0\}$, let $m = 3^x p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $n = 3^y q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$ be the unique prime factorizations of m and n. Then by the uniqueness of the prime factorization, $(2^3)(3)m^2 = n^2 \Rightarrow 2x + 1 = 2y$, a contradiction since the number on the left hand side is odd, whereas the number on the right hand side is even. □

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. By way of contradiction, suppose that $\sqrt{7}$ is rational. Then $\exists n, m \in \mathbb{N}$ such that $\sqrt{7} = \frac{n}{m}$ (note that we can specify that n and m are natural numbers, and not just integers, because $\sqrt{7} > 0$). Then $7m^2 = n^2$, which contradicts Theorem 2.19. Hence, $\sqrt{7}$ is irrational. □

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

Proof. By way of contradiction, suppose that $\sqrt{12}$ is rational. Then $\exists m, n \in \mathbb{N}$ such that $\sqrt{12} = \frac{m}{n} \Rightarrow 12n^2 = m^2 \Rightarrow 3(4n^2) = m^2$. For some $x, y \in \mathbb{N} \cup \{0\}$, let $m = 3^x p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $n = 3^y q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$ be the unique prime factorizations of m and n. Then $3(4n^2) = m^2 \Rightarrow 2y + 1 = 2x$, a contradiction since the LHS is an odd number, whereas the RHS is an even number. Hence, $\sqrt{12}$ is irrational. □

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

Proof. By way of contradiction, suppose that $7^{\frac{1}{3}}$ was rational. Then $\exists m, n \in \mathbb{N}$ such that $7^{\frac{1}{3}} = \frac{m}{n} \Rightarrow 7n^3 = m^3$. For some $x, y \in \mathbb{N} \cup \{0\}$, let $m = 7^x p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ and $n = 7^y q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of m and n. Then $7n^3 = m^3 \Rightarrow 3y + 1 = 3x \Rightarrow 1 = 3(x - y) \Rightarrow 3|1$, a contradiction. Hence, $7^{\frac{1}{3}}$ is irrational. □

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

Conjecture: *For any prime p and natural number $k > 1$, $p^{\frac{1}{k}}$ is irrational.*

Proof. Let p be a prime number and $k \in \mathbb{N}$ with $k > 1$. Suppose by way of contradiction that $p^{\frac{1}{k}}$ is rational. Then $\exists m, n \in \mathbb{N}$ such that $p^{\frac{1}{k}} = \frac{m}{n} \Rightarrow pn^k = m^k$. For some $x, y \in \mathbb{N} \cup \{0\}$, let $m = p^x p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ and $n = p^y q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of m and n. Then, $pn^k = m^k \Rightarrow ky + 1 = kx \Rightarrow 1 = k(x - y) \Rightarrow k|1$, and since $k > 1$, this is a contradiction. Hence, $p^{\frac{1}{k}}$ is irrational. □

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

Proof. Let $a, b, n \in \mathbb{Z}$, and suppose that $a|n$, $b|n$, and $(a, b) = 1$.
Then $\exists x, y \in \mathbb{Z}$ such that $n = xa$ and $n = yb$. Let $p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of a and b, respectively. Then,

$$x\left(p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}\right) = y\left(q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}\right)$$

and since the prime factorization of a number is unique, and none of the $p_i = p_j$ for any $i \leq m$ or $j \leq s$ since $(a, b) = 1$, it follows that we can write $x = k\left(q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}\right)$ and $y = k\left(p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}\right)$ for some $k \in \mathbb{Z}$. Hence,

$$n = xa = k\left(p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}\right)\left(q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}\right) = kab$$

so it follows that $ab|n$. □

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. Let p be a prime and $a \in \mathbb{Z}$.

($\Rightarrow$) We need to prove that if $p \nmid a$ then $(a, p) = 1$. We will prove this by showing the contrapositive: if $(a, p) \neq 1$, then $p|a$.
Suppose that $(a, p) \neq 1$. Let $k = (a, p) \in \mathbb{Z}$.Then $k|a$ and $k|p$. Since p is prime, $k|p \Rightarrow k = 1$ or $k = p \Rightarrow k = p$ since $k \neq 1$ by assumption. Hence, $p|a$.

($\Leftarrow$) We need to show that if $(a, p) = 1$, then $p \nmid a$. We will prove this by showing the contrapositive: if $p|a$, then $(a, p) = 1$.
Suppose that $p|a$. Then since we also have that $p|p$, and any prime is always greater than one, we have that $(a, p) \geq p > 1 \Rightarrow (a, p) \neq 1$.

□

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. Let p be a prime, and $a, b \in \mathbb{Z}$. Suppose that $p|ab$.
If $p|a$, then we are done. Suppose that $p \nmid a$. We will show that $p|b$.
Find $k \in \mathbb{Z}$ such that $ab = kp$. Let $p_1^{r_1}p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1}q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of a and b, respectively. Then,

$$\left(p_1^{r_1}p_2^{r_2} \dots p_m^{r_m}\right)\left(q_1^{t_1}q_2^{t_2} \dots q_s^{t_s}\right) = kp$$

since $p \nmid a$, $p \neq p_i$ for any $i \leq m$ by Theorem 2.12. Since we still have $p|ab$, it must be the case then that $p = q_i$ for some $i \leq s$ by Theorem 2.12 again. By Theorem 2.12 one last time, we can conclude that $p = q_i$ for some $i \leq s \Rightarrow p|b$, as desired. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose that $(b, c) = 1$. Let $p_1^{r_1}p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1}q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of b and c, respectively. Then since $(b, c) = 1$, we have that $p_i \neq q_j$ $\forall i \leq m$ and $j \leq s$. Now, let $d = (a, bc)$. Since $d|b$ and $d|c$, we can prime factorize d as

$$d = \left(p_1^{r'_1}p_2^{r'_2} \dots p_m^{r'_m}\right)\left(q_1^{t'_1}q_2^{t'_2} \dots q_s^{t'_s}\right)$$

where $r'_i \leq r_i$ $\forall i \leq m$ and $t'_j \leq t_j$ $\forall j \leq s$. Notice that there is no possibility of collecting any of the p_i or q_j into one term since $(b, c) = 1$. Then it must be the case that $\left(p_1^{r'_1}p_2^{r'_2} \dots p_m^{r'_m}\right) = (a, b)$ and $\left(q_1^{t'_1}q_2^{t'_2} \dots q_s^{t'_s}\right) = (a, c)$, from which it follows that $(a, bc) = (a, b) \cdot (a, c)$. □

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

Proof. Let $a, b, c \in \mathbb{Z}$, and suppose that $(a, b) = 1$ and $(a, c) = 1$. By Theorem 2.28, $(a, bc) = (a, b) \cdot (a, c) = 1 \cdot 1 = 1$, as desired. □

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

Proof. Let $a, b \in \mathbb{Z}$, and suppose that $(a, b) = d$. Then since $d|a$ and $d|b$, we can write $a = d\left(\frac{a}{d}\right)$ and $b = d\left(\frac{b}{d}\right)$ where $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Then we have $\left(d\left(\frac{a}{d}\right), d\left(\frac{b}{d}\right)\right) = d$. By Theorem 1.55, $\left(d\left(\frac{a}{d}\right), d\left(\frac{b}{d}\right)\right) = d \cdot \left(\frac{a}{d}, \frac{b}{d}\right)$, so $d \cdot \left(\frac{a}{d}, \frac{b}{d}\right) = d \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

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. Let $a, b, u, v \in \mathbb{Z}$, and suppose that $(a, b) = 1$, $u|a$, and $v|b$. Let $p_1^{r_1}p_2^{r_2} \dots p_m^{r_m}$ and $q_1^{t_1}q_2^{t_2} \dots q_s^{t_s}$ be the unique prime factorizations of a and b, respectively.
By Theorem 2.12, since $u|a$ and $v|b$, we can find sets of indices $I \subseteq \{1, 2, \dots, m\}$ and $J \subseteq \{1, 2, \dots, s\}$ such that

$$u = \prod_{i \in I} p_i^{r'_i} \text{ and } v = \prod_{j \in J} q_j^{t'_j}$$

where $r'_i \leq r_i$ $\forall i \in I$ and $t'_j \leq t_j$ $\forall j \in J$. Since $(a, b) = 1$, we know that $p_i \neq q_j$ $\forall i \leq m$ and $j \leq s$. Hence, by Theorem 2.12, we have that $(u, v) = 1$. □

The infinitude of primes

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

Proof. Observe that

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

Hence by Theorem 1.39, $(n, n+1) = 1$. □

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 $k \in \mathbb{N}$. Consider the natural number

$$n = 1 \times 2 \times \cdots \times k + 1$$

Then for any $m \in \mathbb{N}$ with $1 < m < k$,

$$\begin{aligned} n &= (1 \times 2 \times \cdots \times m \times \cdots \times k) + 1 \\ &= m(1 \times 2 \times \cdots \times (m-1) \times (m+1) \times \cdots \times k + 1) + 1 \\ \Rightarrow n &\equiv 1 \pmod{m} \end{aligned}$$

Hence by Theorem 1.28, n has a remainder of 1 whenever it is divided by any m less than k. Thus, no natural number less than k and greater than 1 divides n. □

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

Proof. Let $k \in \mathbb{N}$. By way of contradiction, suppose that there are no primes larger than k. Then we can list all the primes as $p_1, p_2, \ldots, p_m$ for some $m \in \mathbb{N}$ such that $p_i < k \ \forall i \leq m$. Now, let

$$n = 1 \times 2 \times \cdots \times k + 1$$

Then $n > k$ by construction, so it is not prime by assumption. By the Fundamental Theorem of Arithmetic, we can prime factorize n so that

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

where $r_i \in \mathbb{N} \cup \{0\} \ \forall i \leq m$, which means that n is divisible by some $p_i < k$. This contradicts Theorem 2.33, where we showed that a number n of this form is not divisible by any natural number less than k. Hence, we conclude that there must exist a prime number larger than k. □

Theorem 2.35. (Infinitude of Primes Theorem). *There are infinitely many prime numbers.*

Proof. Suppose for contradiction that there is are finitely many primes. Let k be the largest of these primes. Then by Theorem 2.34, there is a prime larger than k, an immediate contradiction. Hence, there are infinitely many primes. □

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

Answer. The most clever part of the above proof is in the argument that $k! + 1$ would be prime if there were a finite number of primes less than k, which is a contradiction. At first sight, it might look like this argument is saying that computing $k! + 1$ is a way of generating larger primes, which is not true! For example $4! + 1 = 25 = 5^2$ is not prime. What this argument does say, however, is that *if* there was a finite number of primes less than k, then $k! + 1$ is prime.

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 $r_1 r_2 \ldots r_m$ is also congruent to 1 modulo 4.*

Proof. Let $r_1, r_2, \ldots, r_m \in \mathbb{N}$ with $r_i \equiv 1 \pmod 4$ $\forall i \leq m$. In other words,

$$\begin{aligned} r_1 &\equiv 1 \pmod 4 \\ r_2 &\equiv 1 \pmod 4 \\ &\vdots \\ r_m &\equiv 1 \pmod 4 \end{aligned}$$

Recall from Theorem 1.14 that we can "multiply" congruence relations, and they will still hold. That is, by Theorem 1.14

$$r_1 r_2 \ldots r_m \equiv \underbrace{1 \times 1 \times \cdots \times 1}_{m \text{ times}} \pmod 4$$

$$\Rightarrow r_1 r_2 \ldots r_m \equiv 1 \pmod 4$$

as desired. □

Theorem 2.38. (Infinitude of $4k + 3$ Primes Theorem). *There are infinitely many primes that are congruent to 3 modulo 4.*

Proof. By way of contradiction, suppose that where are finitely many primes that are congruent to 3 modulo 4, say $p_1, p_2, \ldots, p_m$. Consider

$$r = 4(p_1 p_2 \ldots p_m) + 3$$

Then clearly by construction, $r \equiv 3 \pmod 4$. Since $r > p_i$ $\forall i \leq m$, and it is congruent to 3 modulo 4, by assumption, it is not a prime number. By the fundamental theorem of arithmetic, we can prime factorize r as

$$r = q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$$

Since every natural number n is of the form $n \equiv 0 \pmod 4, n \equiv 1 \pmod 4, n \equiv 2 \pmod 4$, or $n \equiv 3 \pmod 4$, every q_j must also be of one of those forms.

Since each q_j is prime, however, we cannot have $q_j \equiv 0 \pmod 4$ for any $j \leq s$ since this would imply that we can write $q_j = 4k_0$ or for some $k_0 \in \mathbb{Z} \Rightarrow 4|q_j$, which contradicts the fact that q_j is prime.
Furthermore, if $q_j \equiv 2 \pmod 4$, then $q_j = 4k_2 + 2$ for some $k_2 \in \mathbb{Z} \Rightarrow 2|q_j$. This is only possible if $q_j = 2$, but since $r = 4k + 3 = 2(2k + 1) + 1$ where $k = p_1 p_2 \ldots p_m \in \mathbb{Z}$, we have that $2 \nmid r$, which implies that $q_j \neq 2 \ \forall j \leq s$.
Hence, $q_j \not\equiv 0 \pmod 4$ and $q_j \not\equiv 2 \pmod 4 \ \forall j \leq s$.
Now, observe that for all $i \leq m$

$$\begin{aligned} r &= p_i(4p_1p_2 \ldots p_{i-1}p_{i+1} \ldots p_m) + 3 \\ \Rightarrow r &\equiv 3 \pmod{p_i} \\ \Rightarrow p_i &\nmid r \end{aligned}$$

and since we've assumed that $p_1, p_2, \ldots, p_m$ are the only primes of the form $p_i \equiv 3 \pmod 4$, it follows that $q_j \not\equiv 3 \pmod 4 \ \forall j \leq s$. Finally, we have that every prime that divides r is of the form $4q_i + 1$. By Theorem 2.37, it follows that $r \equiv 1 \pmod 4$, which contradicts $r \equiv 3 \pmod 4$. We conclude that there are infinitely many primes that are congruent to 3 modulo 4. □

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

Answer. There aren't very many that I can think of. Observing the fact that the proof of Theorem 2.38 was easy because of what we could say about the form that primes that divide $4k+3$ must have, we see that it is not too hard to show that there are infinitely many primes of the form $6k + 5$. This is because if there were finitely many primes of the form $6k + 5$, say $p_2, p_3, \ldots, p_m$, then we can choose $r = 6(p_1p_2 \ldots p_m) + 5$ where $p_i \neq 5 \ \forall i \leq m$. Since for any $k \in \mathbb{Z}$ we can write $6k + 5 = 2(3k + 2) + 1 = 3(2k + 1) + 2$, it follows that $2 \nmid r$ and $3 \nmid r$. Moreover, if $5|r$, then $5|6(p_2p_3 \ldots p_m)$, which is a contradiction. Hence, any prime dividing r is of the form $6k + 1$. But then the product of all these primes must also be of the form $6k+1$ by the same reasoning as Theorem 2.37, a contradiction. Hence, there are infinitely many primes of the form $6k + 5$.

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

Define the primorial of a natural number k, denoted $k\#$, as the product of all primes less than or equal to k. The current record as of July 2017 according to http://primerecords.dk/aprecords.htm has length 26 and is given by

$$161004359399459161 + 47715109 \cdot 23\# \cdot n, \ \textit{for } n = 0 \textit{ to } 25$$

($23\# = 223092870$*).*

Primes of special form

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

$$\begin{aligned}
(x^m - 1) \div (x - 1) &= x^{m-1} + (x^{m-1} - 1) \div (x - 1) \\
(x^m - 1) \div (x - 1) &= x^{m-1} + x^{m-2} + (x^{m-2} - 1) \div (x - 1) \\
&\vdots \\
(x^m - 1) \div (x - 1) &= x^{m-1} + x^{m-2} + \cdots + x + 1
\end{aligned}$$

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

Proof. Let $n \in \mathbb{N}$, and suppose that $2^n - 1$ is prime. Since $2^n - 1 > 1 \Rightarrow n \geq 2$, we can assume that $n \geq 2$.
Suppose for contradiction that n is composite. Then $\exists a, b \in \mathbb{Z}$ with $x, y > 1$ such that $n = ab$. Letting $x = 2^a$ from exercise 2.42, we have that $((2^a)^b - 1) \div (2^a - 1) = 1 + (2^a) + (2^a)^2 + \cdots + (2^a)^b$. Hence,

$$\begin{aligned}
2^n - 1 &= (2^a)^b - 1 \\
&= (2^a - 1)\left(1 + (2^a) + (2^a)^2 + \cdots + (2^a)^{b-1}\right) \\
&= (2^a - 1)\left(1 + 2^a + 2^{2a} + \cdots + 2^{a(b-1)}\right)
\end{aligned}$$

and since $a, b > 1$, we have that $1 < (2^a - 1), \left(1 + 2^a + 2^{2a} + \cdots + 2^{ab}\right) \in \mathbb{N}$, which shows that $2^n - 1$ is composite, a contradiction. Hence, n must be prime. □

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

Proof. Let $n \in \mathbb{N}$, and suppose that $2^n + 1$ is prime.

We first consider the problem of computing the polynomial division for $(x^a + 1) \div (x + 1)$. Similar to exercise 2.41, observe

$$\begin{aligned}
(x^a + 1) \div (x + 1) &= x^{a-1} - \left(x^{a-1} - 1\right) \div (x + 1) \\
&= x^{a-1} - x^{a-2} + \left(x^{a-2} + 1\right) \div (x + 1) \\
&= x^{a-1} - x^{a-2} + x^{a-3} - \left(x^{a-3} - 1\right) \div (x + 1) \\
&\vdots \\
&= \begin{cases} x^{a-1} - x^{a-2} + \cdots + x - 1 & \text{if } a \text{ is even} \\ x^{a-1} - x^{a-2} + \cdots - x + 1 & \text{if } a \text{ is odd} \end{cases}
\end{aligned}$$

Any natural number can be written as a product of numbers that are either even or not even. Hence, we can write $n = (2^a)b$ where $a \in \mathbb{N} \cup \{0\}$, $b \in \mathbb{N}$, and $b \equiv 1 \pmod 2$ (i.e. b is odd). Then using the above formula,

$$\begin{aligned} 2^n + 1 &= \left(2^{2^a}\right)^b + 1 \\ &= \left(1 - (2^{2^a}) + (2^{2^a})^2 - \cdots + (2^{2^a})^{b-1}\right)(2^{2^a} + 1) \\ &= \left(1 - 2^{2^a} + 2^{2^a \cdot 2} - \cdots + 2^{2^a(b-1)}\right)(2^{2^a} + 1) \end{aligned}$$

and if $b > 1$, then $1 < \left(1 - 2^{2^a} + 2^{2^a \cdot 2} - \cdots + 2^{2^a(b-1)}\right), (2^{2^a} + 1) \in \mathbb{Z}$, which contradicts the fact that $2^n + 1$ is prime. Hence, $b = 1$ so that $n = 2^a$, as desired. □

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

Mersenne Primes: *Theorem 2.42 tells us that we need only check n for which n is prime.*

n	$2^n - 1$
3	7
5	31
7	127

Fermat Primes: *Theorem 2.43 tells us that we need only check n of the form 2^a.*

n	$2^n + 1$
1	2
2	5
4	17
8	257

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

Not today... For now, computer verification of this being true for very large numbers shows that trying to prove that there are indeed infinitely many Mersenne/Fermat primes is the way to go.

Indication 5. Prove that if n is even, $2^n - 1$ is divisible by 3, and if n has the form 2^{3m}, then $2^n - 1$ is divisible by 7. Can you generalize this conclusion?

N.B. To clarify, I believe the above statement is actually trying to say that if n has the form $3m$ (i.e. such that $2^n - 1 = 2^{3m} - 1$) then $2^n - 1$ is divisible by 7. If we consider the statement as is, them $m = 1$ gives $n = 2^3 = 8 \Rightarrow 2^n - 1 = 2^8 - 1 = 255$ which is not divisible by 7.

Proof. Suppose that $n \in \mathbb{N}$ is even. We will first show that $2^n - 1$ is divisible by 3.

Since n is even, $\exists k \in \mathbb{N}$ such that $n = 2k$. Then we can write $2^n - 1 = (2^2)^k - 1$. Observe,

$$\begin{aligned} 2^n - 1 &= (2^2)^k - 1 \\ &= (2^2 - 1)(1 + (2^2) + (2^2)^2 + \cdots + (2^2)^{k-1}) \\ &= 3(1 + (2^2) + (2^2)^2 + \cdots + (2^2)^{k-1}) \end{aligned}$$

which shows that $3|(2^n - 1)$ since $(1 + (2^2) + (2^2)^2 + \cdots + (2^2)^{k-1}) \in \mathbb{Z}$.

Now suppose that n has the form $n = 3m$ for some $m \in \mathbb{N}$ (i.e. suppose that n is divisible by 3). Then,

$$\begin{aligned} 2^n - 1 &= (2^3)^m - 1 \\ &= (2^3 - 1)(1 + (2^3) + (2^3)^2 + \cdots + (2^3)^{m-1}) \\ &= 7(1 + (2^3) + (2^3)^2 + \cdots + (2^3)^{m-1}) \end{aligned}$$

hence, $7|(2^n - 1)$ since $(1 + (2^3) + (2^3)^2 + \cdots + (2^3)^{m-1}) \in \mathbb{Z}$.

In general, if n is divisible by k, then $\exists m \in \mathbb{N}$ such that $n = km$. Now,

$$\begin{aligned} 2^n - 1 &= (2^k)^m - 1 \\ &= (2^k - 1)(1 + (2^3) + (2^3)^2 + \cdots + (2^3)^{m-1}) \end{aligned}$$

and since $(2^k - 1)(1 + (2^3) + (2^3)^2 + \cdots + (2^3)^{m-1}) \in \mathbb{Z}$, it follows that $2^n - 1$ is divisible by $2^k - 1$. □

The distribution of primes

Theorem 2.46. *There exist arbitrarily 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. Recall that for some $n \in \mathbb{N}$, n factorial - denoted $n!$ - is given by $n! := 1 \times 2 \times 3 \cdots \times n$. Now, let $n \in \mathbb{N}$. We want to show that we can construct a string of more than n consecutive composite natural numbers. Consider the following sequence of $n + 1$ natural numbers

$$(n+2)! + 2, (n+2)! + 3, (n+2)! + 4, \ldots, (n+2)! + n + 2$$

the i-th term in this sequence is given by $(n + 2)! + i$. Observe that we can factor this as

$$(n+2)! + i = i \cdot ((n+2)(n+1) \ldots (i+1)(i-1) \ldots (n)(1) + 1)$$

which shows that each term is composite. Since n is an arbitrary natural number, it follows that we can construct arbitrarily long sequences of consecutive natural numbers. □

Question 2.47. (The Twin Primes Question). *Are there infinitely many pairs of prime numbers that differ from one another by two? (The pairs 11 and 13, 29 and 31, 41 and 43 are examples of such twin primes).*

Answer. Not a question I will be seriously attempting today (perhaps someday...)

Exercise 2.48. *Express each of the first 20 even numbers greater than 2 as a sum of two primes. (For example:* $8 = 5 + 3$*).*

Here is verification of Goldbach's Conjecture for the first 20 even natural numbers greater than 2.

n	$p_1 + p_2$
4	$2 + 2$
6	$3 + 3$
8	$3 + 5$
10	$3 + 7$
12	$5 + 7$
14	$3 + 11$
16	$3 + 13$
18	$5 + 13$
20	$3 + 17$
22	$3 + 19$
24	$5 + 19$
26	$3 + 23$
28	$5 + 23$
30	$7 + 23$
32	$3 + 29$
34	$3 + 31$
36	$5 + 31$
38	$7 + 31$
40	$3 + 37$
42	$5 + 37$

From Antiquity to the Internet

Exercise 2.49. *Find the current record for the largest known Mersenne prime.*

According to https://www.mersenne.org/primes/?press=M74207281, the largest known Mersenne prime as of July 2017 is:

$$2^{74,207,281} - 1$$

3 A Modular World

Powers and polynomials modulo n

Exercise 3.1. *Show that 41 divides $2^{20}-1$ by following these steps. Explain why each step is true.*

1. $2^5 \equiv -9 \pmod{41}$.
   Observe that $2^5-(-9)=32+9=41 \Rightarrow 41|(2^5-(-9)) \iff 2^5 \equiv -9 \pmod{41}$.

2. $(2^5)^4 \equiv (-9)^4 \pmod{41}$.
   Recall from Theorem 1.18 that $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$. *It follows immediately from 1 then that* $2^5 \equiv -9 \pmod{41} \Rightarrow (2^5)^4 \equiv (-9)^4 \pmod{41}$

3. $2^{20} \equiv 81^2 \pmod{41} \equiv (-1)^2 \pmod{41}$.
   Making use of some elementary laws of exponents, we have from 2 that $(2^5)^4 \equiv (-9)^4 \pmod{41} \Rightarrow 2^{20} \equiv 81^2 \pmod{41}$. *A quick mental check confirms that* $41|(81-(-1))$, *which implies that* $81 \equiv -1 \pmod{41} \Rightarrow 81^2 \equiv (-1)^2 \pmod{41}$. *Since equivalence modulo n is transitive, it follows that* $2^{20} \equiv 81^2 \pmod{41} \equiv (-1)^2 \pmod{41}$.

4. $2^{20}-1 \equiv 0 \pmod{41}$.
   From 3, we have $2^{20} \equiv (-1)^2 \pmod{41} \Rightarrow 2^{20} \equiv 1 \pmod{41}$, *and subtracting* $1 \equiv 1 \pmod{41}$ *gives the desired* $2^{20}-1 \equiv 0 \pmod{41}$.

Question 3.2. *In your head, can you find the natural number k, $0 \le k \le 11$, such that $k \equiv 37^{453} \pmod{12}$?*

Answer. Observe that $12|(1-37)=-36 \iff 1 \equiv 37 \pmod{12} \Rightarrow 1^{453} \equiv 37^{453} \pmod{12} \Rightarrow 1 \equiv 37^{453} \pmod{12}$. Hence, $k=1$ satisfies the relation.

Question 3.3. *In your head or using paper and pencil, but no calculator, can you find the natural number k, $0 \le k \le 6$, such that $2^{50} \equiv k \pmod{7}$?*

Answer. Notice that $2^6=64$, whereas $7 \times 9 = 63$. This means that $2^6 \equiv 1 \pmod{7} \Rightarrow (2^6)^8 \equiv 1^8 \pmod{7} \Rightarrow 2^{48} \equiv 1 \pmod{7}$, and multiplying by $2^2 \equiv 2^2 \pmod{7}$ gives $2^{50} \equiv 4 \pmod{7}$. Hence, the natural number $k=4$ satisfies the desired relation.

Question 3.4. *Using paper and pencil, but no calculator, can you find the natural number k, $0 \le k \le 11$, such that $39^{453} \equiv k \pmod{12}$?*

Answer. Using similar tricks as before, notice that $39 \equiv 3 \pmod{12} \Rightarrow 39^3 \equiv 3^3 \pmod{12}$, and since $3^3 \equiv 3 \pmod{12}$, it follows that $39^3 \equiv 3 \pmod{12}$. The fact that cubing the congruence leaves 3 unchanged on the right-hand side (since $3^3 \equiv 3 \pmod{12}$) is what we want to take advantage of here. Further observation shows that $453 = 151 \times 3$, so if we apply $3^3 \equiv 3 \pmod{12}$ 151 times, then we obtain $(39^3)^{151} \equiv 3 \pmod{12} \Rightarrow 39^{453} \equiv 3 \pmod{12}$ (a very easy proof by induction can be made to make this more rigorous). It follows that $k=3$ is the desired natural number.

Exercise 3.5. *Show that 39 divides* $17^{48} - 5^{24}$.

It is sufficient to show that $17^{48} \equiv 5^{24} \pmod{39}$ *to prove that 39 divides* $17^{48} - 5^{24}$ *(in fact, it is also necessary).*
After some trial and error, the observation was made that $5^4 = 625$*, whereas* $39 \times 16 = 624$. *Thus,* $5^4 \equiv 1 \pmod{39} \Rightarrow 5^{24} \equiv 1 \pmod{39}$.
Some more trial and error revealed that $17^2 = 289$ *with the closest multiple of 39 being* $39 \times 7 = 273$*, and since* $289 - 273 = 16 = 2^4$*, we have that* $17^2 \equiv 2^4 \pmod{39}$. *Furthermore, since* $2(17) - 5 = 39$*, we have that* $2(17) \equiv -5 \pmod{39} \Rightarrow 2^4(17)^4 \equiv 5^4 \pmod{39}$. *Multiplying the last congruence by* $17^2 \equiv 2^4 \pmod{39}$ *gives* $2^4(17)^4 \equiv 2^4 5^4 \pmod{39}$*, and since* $(2^4, 39) = 1$*, it follows from Theorem 1.45 that* $17^4 \equiv 5^4 \pmod{39}$. *By transitivity, since* $5^4 \equiv 1 \pmod{39}$*, we have that* $17^4 \equiv 1 \pmod{39} \Rightarrow 17^{48} \equiv 1 \pmod{39}$.
Combining $5^{24} \equiv 1 \pmod{39}$ *and* $17^{48} \equiv 1 \pmod{39}$*, we finally have that* $17^{48} \equiv 5^{24} \pmod{39}$*, as desired.*

Question 3.6. (Describe technique). *Let* $a, n,$ *and* r *be natural numbers. Describe how to find the number* k $(0 \leq k \leq n-1)$ *such that* $k \equiv a^r \pmod{n}$ *subject to the restraint that you never multiply numbers larger than* n *and that you only have to do about* $\log_2 r$ *such multiplications.*

Answer. Following the restraint that we have to do about $\log_2 r$ such multiplications, we want to express r as a sum of powers of 2. In other words, first find $m_1, m_2, \ldots, m_k \in \mathbb{N}$ with $m_1 < m_2 < \cdots < m_k$ such that

$$r = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$$

Then we can re-express the desired congruence as

$$\left(a^{2^{m_1}}\right)\left(a^{2^{m_2}}\right)\ldots\left(a^{2^{m_k}}\right) \equiv a^r \pmod{n}$$

Since equivalence modulo n is reflexive, we can start with $a \equiv a \pmod{n}$. We then find $a_1 \in \mathbb{N}$ with $0 \leq a_0 \leq n-1$ such that $a \equiv a_0 \pmod{n}$ (note that the existence of such a number is guaranteed by the Division Algorithm). Next, we compute $a^2 \equiv a \cdot a \pmod{n}$ by substituting the previous result to get $a^2 \equiv a_0^2 \pmod{n}$, from which — since $a_0 < n$ — it'll be easier to find $a_1 \in \mathbb{N}$ with $0 \leq a_1 \leq n-1$ such that $a_0^2 \equiv a_1 \pmod{n} \Rightarrow a^2 \equiv a_1 \pmod{n}$. We can find what a raised to the next power of 2 is congruent to by proceeding in exactly the same way; we can find $a^{2^2} \equiv a_1^2 \pmod{n}$ by finding $a_2 \in \mathbb{N}$ with $0 \leq a_2 \leq n-1$ such that $a_1^2 \equiv a_2 \pmod{n}$, from which we obtain $a^{2^2} \equiv a_2 \pmod{n}$. We keep following this procedure to find $a_i \in \mathbb{N}$ with $0 \leq a_i \leq n-1$ such that $a^{2^i} \equiv a_i \pmod{n}$ $\forall i \leq m_k$. Finally, we can write

$$a_{m_1} a_{m_2} \ldots a_{m_k} \equiv a^r \pmod{n}$$

which can be simplified by computing the product on the left-hand side one pair at a time.

Question 3.7. *Let* $f(x) = 13x^{49} - 27x^{27} + x^{14} - 6$. *Is it true that*

$$f(98) \equiv f(-100) \pmod{99}?$$

Answer. Observe that $98 \equiv -100 \pmod{99}$ since $98 - (-100) = 198 = 2(99) \Rightarrow 99|(98 - (-100))$. We can apply Theorem 1.19 to this key result to obtain

$$\begin{aligned} 98^{49} &\equiv (-100)^{49} \pmod{99} && (1) \\ 98^{27} &\equiv (-100)^{27} \pmod{99} && (2) \\ 98^{14} &\equiv (-100)^{14} \pmod{99} && (3) \end{aligned}$$

Furthermore, by the reflexiveness of congruence modulo n, we have that $a \equiv a \pmod{99}\ \forall a \in \mathbb{Z}$. Hence, by multiplying each of $(1), (2)$ and (3) by the appropriate "reflexive" congruence, we can write the following congruences

$$\begin{aligned} 13(98^{49}) &\equiv 13(-100)^{49} \pmod{99} && (4) \\ -27(98^{27}) &\equiv -27(-100)^{27} \pmod{99} && (5) \\ 98^{14} &\equiv (-100)^{14} \pmod{99} && (6) \\ -6 &\equiv -6 \pmod{99} && (7) \end{aligned}$$

Taking the sum of (4) to (7) gives

$$\begin{aligned} 13(98^{49}) - 27(98^{27}) + 98^{14} - 6 &\equiv 13(-100)^{49} - 27(-100)^{27} + (-100)^{14} - 6 \pmod{99} \\ \Rightarrow f(98) &\equiv f(-100) \pmod{99} \end{aligned}$$

So indeed, the statement is true.

Theorem 3.8. *Suppose that* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *is a polynomial of degree* $n > 0$ *with integer coefficients. Let* a, b, *and* m *be integers with* $m > 0$. *If* $a \equiv b \pmod{m}$, *then* $f(a) \equiv f(b) \pmod{m}$.

Proof. Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and suppose that $a \equiv b \pmod{m}$. By Theorem 1.18, for any $k \in \mathbb{N}$, we have that $a^k \equiv b^k \pmod{m}$. Moreover, for any $c \in \mathbb{Z}$, we can use the reflexiveness of the congruence modulo m relation to write $c \equiv c \pmod{m}$. By Theorem 1.14, we can multiply the last two congruences to obtain $ca^k \equiv cb^k \pmod{m}$. Hence, we have that $a_i a^i \equiv a_i b^i \pmod{m}\ \forall 1 \leq i \leq n$ and $a_0 \equiv a_0 \pmod{m}$. By repeated application of Theorem 1.12, we can sum over all i (as well as a_0) to obtain

$$a_n a^n + a_{n-1}a^{n-1} + \cdots + a_0 \equiv a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0 \pmod{m}$$

$$\Rightarrow f(a) \equiv f(b) \pmod{m}$$

□

Corollary 3.9. *Let the natural number n be expressed in base 10 as*

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

Let $m = a_k + a_{k-1} + \cdots + a_1 + a_0$. Then $9|n$ if and only if $9|m$.

Proof. Let $n \in \mathbb{N}$ be expressed in base 10 as

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

and let $m = a_k + a_{k-1} + \cdots + a_1 + a_0$.
Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \ \forall x \in \mathbb{Z}$. Observe,

$$\begin{aligned}
10 &\equiv 1 \pmod 9 \\
\Rightarrow f(10) &\equiv f(1) \pmod 9 \text{ (by Theorem 3.8)} \\
\Rightarrow a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 &\equiv a_k 1^k + a_{k-1} 1^{k-1} + \cdots + a_1 1 + a_0 \pmod 9 \\
&\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9 \\
\Rightarrow n &\equiv m \pmod 9
\end{aligned}$$

Hence, we have that $9|(n-m) \Rightarrow \exists k \in \mathbb{Z}$ such that $n - m = 9k$.

(⇒) Suppose that $9|n$. Then $\exists \ell_1 \in \mathbb{Z}$ such that $n = 9\ell_1$. Hence, $m = 9(\ell_1 - k)$, and since $(\ell_1 - k) \in \mathbb{Z}$, it follows that $9|m$.

(⇐) Conversely, suppose that $9|m$. Then $\exists \ell_2 \in \mathbb{Z}$ such that $m = 9\ell_2$. Hence, $n = 9(\ell_2 + k)$, and since $(\ell_2 + k) \in \mathbb{Z}$, it follows that $9|n$.

□

Indication 2. Consider the keypad presented in the study guide:

$$\begin{array}{ccc}
1 & 2 & 3 \\
4 & 5 & 6 \\
7 & 8 & 9
\end{array}$$

a. First note that by inspection, each way of traversing the keypad as described by the study guide produces a distinct 6-digit number. We first choose whether to go horizontally or vertically. We then choose one of the two directions available to us (i.e. right-to-left or left-to-right / up-down or down-up). We then need to choose one of the three rows twice in order to form our number. Mathematically,

$$\underbrace{\binom{2}{1}}_{\text{horiz/vert}} \underbrace{\binom{2}{1}}_{\text{rl/ud}} \underbrace{\binom{3}{1}}_{\text{3 rows}} \underbrace{\binom{3}{1}}_{\text{3 rows}} = 2^2 \times 3^2 = 36 \text{ distinct 6 digit numbers}$$

b. We want to prove that every number that can be formed in the way described by the study guide is divisible by 37.

   Suppose that "$abcdef$" is a 6 digit number (written in base 10) formed by one of the 36 available ways. Denote this number by N, and write

$$N = 10^5a + 10^4b + 10^3c + 10^2d + 10e + f$$

   Now, a key observation to make is that since the numbers change by the same increments horizontally/vertically, we have that $a - b = b - c = e - d = f - e = \lambda$ where $\lambda = 1, -1, 3$, or -3. The actual value of λ won't matter, however. What matters is that we can write the following equations:

$$\begin{aligned} b &= a - \lambda \\ c &= b - \lambda = a - 2\lambda \\ d &= e - \lambda \\ f &= e + \lambda \end{aligned}$$

   Subbing these into the equation for N,

$$\begin{aligned} N &= 10^5a + 10^4(a-\lambda) + 10^3(a-2\lambda) + 10^2(e-\lambda) + 10e + (e+\lambda) \\ &= 10^3(100a + 10a + a) + (100e + 10e + e) + \lambda(-10^4 - 2\cdot 10^3 - 10^2 + 1) \\ &= 10^3(111)a + (111)e - (12099)\lambda \\ &= 37\left(3\cdot 10^3a + 37e - 327\lambda\right) \end{aligned}$$

   Which shows that $37|N$, as desired!

Corollary 3.10. *Let the natural number n be expressed in base 10 as*

$$n = a_ka_{k-1}\dots a_1a_0.$$

If $m = a_k + a_{k-1} + \cdots + a_1 + a_0$. Then $3|m$ if and only if $3|m$.

Proof. Let $n \in \mathbb{N}$ be expressed in base 10 as

$$n = a_ka_{k-1}\dots a_1a_0.$$

and let $m = a_k + a_{k-1} + \cdots + a_1 + a_0$.
Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0\ \forall x \in \mathbb{Z}$. Observe,

$$\begin{aligned} 10 &\equiv 1 \pmod 3 \\ \Rightarrow f(10) &\equiv f(1) \pmod 3 \text{ (by Theorem 3.8)} \\ \Rightarrow a_k10^k + a_{k-1}10^{k-1} + \cdots + a_110 + a_0 &\equiv a_k1^k + a_{k-1}1^{k-1} + \cdots + a_11 + a_0 \pmod 3 \\ &\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3 \\ \Rightarrow n &\equiv m \pmod 3 \end{aligned}$$

Hence, we have that $3|(n - m) \Rightarrow \exists k \in \mathbb{Z}$ such that $n - m = 3k$.

(⇒) Suppose that $3|n$. Then $\exists \ell_1 \in \mathbb{Z}$ such that $n = 3\ell_1$. Hence, $m = 3(\ell_1 - k)$, and since $(\ell_1 - k) \in \mathbb{Z}$, it follows that $3|m$.

(⇐) Conversely, suppose that $3|m$. Then $\exists \ell_2 \in \mathbb{Z}$ such that $m = 3\ell_2$. Hence, $n = 3(\ell_2 + k)$, and since $(\ell_2 + k) \in \mathbb{Z}$, it follows that $3|n$.

□

Theorem 3.11. *Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial of degree $n > 0$. Then there is an integer k such that if $x > k$, then $f(x) > 0$.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$, and suppose that $a_n > 0$. If we view $f(x)$ as a polynomial with coefficients in $\mathbb{R}$, then we can borrow principles from calculus to prove the above theorem. Observe that

$$\frac{d^n}{dx^n} f(x) = a_n \cdot n! > 0$$

Hence, $\frac{d^{n-1}}{dx^{n-1}} f(x)$ is a monotonically, increaseing function, so $\exists k_0 \in \mathbb{Z}$ large enough such that $\frac{d^{n-1}}{dx^{n-1}} f(x) > 0 \ \forall x > k_0$. This implies that $\frac{d^{n-2}}{dx^{n-2}} f(x)$ is monotonically increasing $\forall x > k_0$. Hence, $\exists k_1 \in \mathbb{Z}$ with $k_1 > k_0$ such that $\frac{d^{n-2}}{dx^{n-2}} f(x) > 0 \ \forall x > k_1$. Continuing this way, we—inductively—arrive at the conclusion that $\exists k_n \in \mathbb{Z}$ such that $f(x) > 0 \ \forall x > k_n$, as desired. □

Theorem 3.12. *Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial of degree $n > 0$ and suppose that $a_n > 0$. Then for any number M there is an integer k (which depends on M) such that if $x > k$, then $f(x) > M$.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$, and suppose that $a_n > 0$. Let $M \in \mathbb{R}$. Define $g(x) := f(x) - M$. Then $g(x)$ is also a polynomial of degree $n > 0$. By Theorem 3.11, $\exists k \in \mathbb{Z}$ such that $x > k \Rightarrow g(x) > 0 \Rightarrow f(x) - M > 0 \Rightarrow f(x) > M$, as desired. □

Theorem 3.13. *Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then $f(x)$ is a composite number for infinitely many integers x.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$ with integer coefficients.
Following the hint, find $a \in \mathbb{Z}$ such that $f(k) > 1 \ \forall k > a$, and say $f(a) = b$. Since $b > 1$, by the Fundamental Theorem of Arithmetic, $\exists p$ prime such that $p|b \Rightarrow f(a) \equiv 0 \pmod{p}$.
Let $k \in \mathbb{Z}$, and let a_i be the coefficient of the smallest degree term with non-zero coefficient. Observe,

$$\begin{aligned} f(ka_i) &= a_n(ka_i)^n + a_{n-1}(ka_i)^{n-1} + \cdots + a_i(ka_i)^i \\ &= a_i \left(a_n k^n a_i^{n-1} + a_{n-1}k^{n-1}a_i^{n-2} + \cdots + (ka_i)^i\right) \end{aligned}$$

which shows that $f(ka_i)$ is composite. Since there are infinitely many choices for k, it follows that $f(x)$ is a composite number for infinitely many integers x. □

Theorem 3.14. *Given any integer a and any natural number n, there exists a unique integer t in the set $\{0, 1, 2, \dots, n-1\}$ such that $a \equiv t \pmod{n}$.*

Proof. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let

$$\bar{n} := \{0, 1, 2, \dots, n-1\}$$

By the Division Algorithm, $\exists! q, t \in \mathbb{Z}$ with $0 \leq t \leq n-1$ such that

$$a = nq + t$$

Then $t \in \bar{n}$, and a has a remainder of t when divided by n. Since $0 \leq t < n$, we can also write $t = 0 \cdot n + t$, meaning that t has also has a remainder of t when divided by n. By Theorem 1.28, since a and t have the same remainder when divided by n,

$$a \equiv t \pmod{n}$$

as desired (note that the uniqueness of t comes from the Division Algorithm). □

Exercise 3.15. *Find three complete residue systems modulo 4: the canonical complete residue system, one containing negative numbers, and one containing no two consecutive numbers.*

Canonical Complete Residue System: $\{0, 1, 2, 3\}$.
Contains Negative Numbers: $\{-3, -2, -1, 0\}$.
No two consecutive Numbers: $\{0, 5, 2, 7\}$.

Theorem 3.16. *Let n be a natural number. Every complete residue system modulo n contains n elements.*

Proof. Let $n \in \mathbb{N}$. Suppose that $\mathcal{R} := \{a_1, a_2, \dots, a_k\}$ is a complete residue system modulo n. We first recall from the Division Algorithm and Theorem 1.28 that $\forall a, b \in \mathbb{Z}$, $\exists! q, r \in \mathbb{Z}$ with $0 \leq r \leq b-1$ such that $a = bq + r$ and $a \equiv r \pmod{b}$ (since a and r have the same remainder when divided by b). If we consider the canonical complete residue system modulo n, $\mathcal{C} := \{0, 1, 2, \dots, n-1\}$. Then in order for each element $r_i \in \mathcal{C}$ to be congruent to some element $a_j \in \mathcal{R}$, it must have the same remainder as r_i. From the uniqueness part of the division algorithm, since the remainder of each a_j when divided by n is unique, and there are n distinct remainders that an integer can take on when divided by n (the set $\mathcal{C}$ containing one of each such integer), it follows that $\mathcal{R}$ must have at least n elements (i.e. $|\mathcal{R}| \geq n$). If $\mathcal{R}$ contains *more* than n elements, then by the same argument as above, since there are only n distinct remainders an integer can have when divided by n, at least two elements have the same remainder. That is, at least two integers are congruent to the same $r_i \in \mathcal{C}$. Hence, in order to have each integer congruent to exactly one element in $\mathcal{R}$, it must be the case that there are exactly n elements in $\mathcal{R}$.

□

Theorem 3.17. *Let n be a natural number. Any set $\{a_1, a_2, \ldots, a_n\}$, of n integers for which no two are congruent modulo n is a complete residue system modulo n.*

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Let $\mathcal{R} := \{a_1, a_2, \ldots, a_n\}$ be a set of n integers for which no two are congruent modulo n. Then, by Theorem 1.18, no two $a_i, a_j \in \mathcal{R}$ with $i \neq j$ have the same remainder when divided by n. Since there are exactly n distinct remainders that an integer can have when divided by n, it follows that $\forall r \in \{0, 1, \ldots, n-1\}$, $\exists a_i \in \mathcal{R}$ such that $a_i \equiv r \pmod{n}$. Furthermore, by the Division Algorithm and Theorem 1.18, since every integer is also congruent to some element in $\{0, 1, \ldots, n-1\}$ modulo n, it follows from the transitive property of congruences that every integer is congruent to exactly one element in $\mathcal{R}$. Hence, by definition, $\mathcal{R}$ is a complete residue system modulo n. □

Linear congruences

Exercise 3.18. *Find all solutions in the appropriate canonical complete residue system modulo n that satisfy the following linear congruences:*

1. $26x \equiv 14 \pmod{3}$.
   Since $14 \equiv 2 \pmod{3}$ and $26 \equiv 2 \pmod{3}$, it follows that $x = 1$ satisfies the linear congruence.

2. $2x \equiv 3 \pmod{5}$.
   We need to find a multiple of 2 that is a multiple of 5 when 3 is subtracted from it. the number 8 satisfies this, hence $x = 4$ satisfies the linear congruence.

3. $4x \equiv 7 \pmod{8}$.
   Trial and error reveals that every n in the canonical complete residue system modulo n fails to satisfy the linear congruence.

4. $24x \equiv 123 \pmod{213}$.
   (as suggested by the textbook, we leave this problem for later).

Theorem 3.19. *Let a, b, and n be integers with $n > 0$. Show that $ax \equiv b \pmod{n}$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.*

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$.

($\Rightarrow$) Suppose that $ax \equiv b \pmod{n}$ has a solution. Then $n|(ax - b) \Rightarrow \exists (-y) \in \mathbb{Z}$ such that $ax - b = -yn \Rightarrow ax + ny = b$, as desired.

($\Leftarrow$) Suppose that $\exists x, y \in \mathbb{Z}$ such that $ax + ny = b \Rightarrow (ax - b) = -ny \Rightarrow n|(ax - b) \iff ax \equiv b \pmod{n}$, which shows that $ax \equiv b \pmod{n}$ has a solution.

□

Theorem 3.20. *Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n)|b$.*

Proof. Let a, b, n be integers with $n > 0$.
If a and b are both zero, then since $0 \equiv 0 \pmod{n}$ and $(0, n)|0$ are always true for $n > 0$, we trivially have that $0 \cdot x \equiv 0 \pmod{n} \iff (0, n)|0$.
Suppose that a and b are not both zero. Then,

$$\begin{aligned} ax \equiv b \pmod{n} \text{ has a solution} &\iff \exists x, y \in \mathbb{Z} \text{ such that } ax + ny = b \text{ (Thm 3.19)} \\ &\iff (a, n)|b \text{ (Thm 1.48)} \end{aligned}$$

as desired. □

Question 3.21. *What does the preceding theorem tell us about the congruence (4) in Exercise 3.18 above?*

Answer. Observe that we can prime factorize 24 and 213 as $24 = 2^3 \cdot 3$ and $213 = 3 \cdot 71$, respectively. Hence, $(24, 213) = 3$. Since $123 = 3(41) \Rightarrow 3|123 \Rightarrow (24, 213)|213$, it follows that there is a solution for congruence (4) in exercise 3.18.

Exercise 3.22. *Use the Euclidean Algorithm to find a member x of the canonical complete residue system modulo 213 that satisfies $24x \equiv 123 \pmod{213}$. Find all members x of the canonical complete residue system modulo 213 that satisfy $24x \equiv 123 \pmod{213}$.*

From question 3.21, we know that there exists a solution for $24x \equiv 123 \pmod{213}$. We want to find integers x, y such that $24x + y213 = 123$. Using the division algorithm,

$$\begin{aligned} 213 &= 8(24) + 21 \\ 24 &= 1(21) + 3 \\ 21 &= 7(3) + 0 \end{aligned}$$

Then,

$$\begin{aligned} 24 - 21 &= 3 \\ 24 - (213 - 8(24)) &= 3 \\ 9(24) - 213 &= 3 \end{aligned}$$

Now, since $123 = 3 \cdot 41$, we can multiply both sides of the above equation by 41 to obtain

$$369(24) - 41(213) = 123$$

Which shows that $24(369) \equiv 123 \pmod{213}$. In order to get solutions that are in the canonical complete residue system modulo 213, we can use Theorem 1.53 to get all the other solutions of $24x + 213y = 123$. In particular, we only need to know that all solutions for x are given by

$$x = 369 + \frac{213k}{(24, 213)} = 369 + 71k$$

where $k \in \mathbb{Z}$. By successively trying smaller and smaller k, we find that $k = -3, -4, -5$ give all the solutions in the canonical complete residue system modulo n. That is, $x = 156, 85, 14$ are all the desired solutions.

Question 3.23. *Let $a, b,$ and n be integers with $n > 0$. How many solutions are there to the linear congruence $ax \equiv b \pmod{n}$ in the canonical complete residue system modulo n? Can you describe a technique to find them?*

Answer. The first step in trying to solve the linear congruence $ax \equiv b \pmod{n}$ is to check if $(a, n)|b$, which allows us conclude by Theorem 3.20 whether or not a solution exists. The next step is to find a solution to the linear Diophantine equation $ax + ny = b$ using the Euclidean Division Algorithm. Once we have found x_0, y_0 such that $ax_0 + ny_0 = b$, then the general solution for x is given by Theorem 1.53 as

$$x = x_0 + \frac{kn}{(a,n)},\ k \in \mathbb{Z}$$

which shows that there are $(a, n) - 1$ distinct solutions x modulo n. In order to get solutions in the canonical complete residue system specifically, intelligent trial and error using the equation above can be done to get solutions in $\{0, 1, \ldots, n - 1\}$.

Theorem 3.24. *Let $a, b,$ and n be integers with $n > 0$. Then*

1. *The congruence $ax \equiv b \pmod{n}$ is solvable in integers if and only if $(a, n)|b$;*
2. *If x_0 is a solution to the congruence $ax \equiv b \pmod{n}$, then all solutions are given by*

   $$x + \left(\frac{n}{(a,n)} \cdot m\right) \pmod{n}$$

   for $m = 0, 1, 2, \ldots, (a, n) - 1$; and
3. *If $ax \equiv b \pmod{n}$ has a solution, then there are exactly (a, n) solutions in the canonical complete residue system modulo n.*

Proof. Let $a, b, \in \mathbb{Z}$ with $n > 0$.

1. This is just Theorem 3.20.
2. This was addressed in Question 3.23, but we will repeat the argument here more formally.

   Suppose that x_0 is a solution to the congruence $ax \equiv b \pmod{n}$. Then by Theorem 3.19, we can also find $y_0 \in \mathbb{Z}$ such that $ax_0 + ny_0 = b$. It follows from Theorem 1.53 that every solution for x to the linear Diophantine equation $ax + ny = b$ is given by

   $$x = x_0 + \left(\frac{n}{(a,n)} \cdot k\right),\ k \in \mathbb{Z}$$

   which is equivalent to saying that all solutions are given by

   $$x + \left(\frac{n}{(a,n)} \cdot m\right) \pmod{n}$$

   for $m = 0, 1, 2, \ldots, (a, n) - 1$.

3. Suppose that $ax \equiv b \pmod{n}$ has a solution. Then by part 2 of this Theorem and Theorem 3.17, it follows that there are exactly (a, n) solutions in the canonical complete residue system modulo n.

□

Systems of linear congruences: the Chinese Remainder Theorem

Exercise 3.25. *A band of 17 pirate stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The coins were redistributed, but this time an equal division left 10 coins. Again they fought about who should get the remaining coins and another pirate was killed. Now, fortunately, the coins could be divided evenly among the surviving 15 pirates. What was the fewest number of coins that could have been in the sack?*

Answer. Let x represent the number of cold coins. Then we have the following system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod{17} \qquad (1) \\ x &\equiv 10 \pmod{16} \qquad (2) \\ x &\equiv 0 \pmod{15} \qquad (3) \end{aligned}$$

From congruence (3), we know that x has to be a multiple of 15. In other words,

$$x = 15k, \ \exists k \in \mathbb{Z}$$

We will attempt to solve congruence (1) using this substitution.

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ \Rightarrow 15k &\equiv 3 \pmod{17} \\ \Rightarrow 75k &\equiv 15 \pmod{17} \\ \Rightarrow 5k &\equiv 1 \pmod{17} \text{ (since } (15, 17) = 1) \\ \Rightarrow 5k &\equiv 35 \pmod{17} \text{ (add 2 multiples of 17)} \\ \Rightarrow k &\equiv 7 \pmod{17} \text{ (since } (5, 17) = 1) \end{aligned}$$

Combining this with the previous result, we now have that $x \equiv 15 \cdot 7 \pmod{15 \cdot 17} \iff x \equiv 105 \pmod{255}$. In other words, $x = 105 + 255m$ for some $m \in \mathbb{Z}$. Now,

$$\begin{aligned} x &\equiv 10 \pmod{16} \\ \Rightarrow 105 + 255m &\equiv 10 \pmod{16} \end{aligned}$$

Observing that $105 \equiv 9 \pmod{16}$,

$$\begin{aligned}
\Rightarrow 255m &\equiv 1 \pmod{16} \\
\Rightarrow 255m &\equiv 65 \pmod{16} \text{ (adding 4 multiples of 16)} \\
\Rightarrow 51m &\equiv 13 \pmod{16} \text{ (since } (5,16)=1) \\
\Rightarrow 51m &\equiv -3 \pmod{16} \\
\Rightarrow 17m &\equiv -1 \pmod{16} \\
\Rightarrow -17m &\equiv 17 \pmod{16} \\
\Rightarrow m &\equiv 15 \pmod{16}
\end{aligned}$$

Hence, $m = 15 + 16n$ for some $n \in \mathbb{Z}$Combining all of the previous result, we have that $x = 105 + 255(15 + 16n) = 3930 + 4080n \Rightarrow x \equiv 3930 \pmod{4080}$.

Hence, the fewest number of coins that could have been in the sack is **3930 coins**.

Exercise 3.26. (Brahmagupta, 7th century A.D.). *When eggs in a basket are removed two, three, four, five, or six at a time, there remain, respectively, one, two, three, four, or five eggs. When they are taken out seven at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.*

Answer. Just like before, we write down the linear congruences described by the problem:

$$\begin{aligned}
x &\equiv 1 \pmod{2} && (1) \\
x &\equiv 2 \pmod{3} && (2) \\
x &\equiv 3 \pmod{4} && (3) \\
x &\equiv 4 \pmod{5} && (4) \\
x &\equiv 5 \pmod{6} && (5) \\
x &\equiv 0 \pmod{7} && (6)
\end{aligned}$$

Use congruence (7) to write $x = 7a$ for some $a \in \mathbb{Z}$. We can use congruence (1) to write $7a \equiv 1 \pmod{2} \Rightarrow 7a \equiv 7 \pmod{2} \Rightarrow a \equiv 1 \pmod{2} \Rightarrow a = 1 + 2b$ for some $b \in \mathbb{Z}$. Hence, $x = 7(1 + 2b) = 7 + 14b$ for some $b \in \mathbb{Z}$. Now use congruence (2) to write $7 + 14b \equiv 2 \pmod{3} \Rightarrow 14b \equiv -5 \pmod{3} \Rightarrow 14b \equiv -14 \pmod{3} \Rightarrow b \equiv -1 \pmod{3} \Rightarrow b \equiv 2 \pmod{3} \Rightarrow b = 2 + 3c$ for some $c \in \mathbb{Z}$. Combining this with the previous result, we have $x = 7 + 14(2 + 3c) = 35 + 42c$. Notice that this satisfies congruence (5) as well.

We already have an equation that satisfies $(1), (2), (5)$ and (7). We now substitute into (4) to get $35 + 42c \equiv 4 \pmod{5} \Rightarrow 42c \equiv 4 \pmod{5} \Rightarrow 21c \equiv 2 \pmod{5} \Rightarrow 7c \equiv -1 \pmod{5} \Rightarrow c \equiv 2 \pmod{5} \Rightarrow c = 2 + 5d$ for some $d \in \mathbb{Z}$. Hence, $x = 35 + 42(2 + 5d) = 119 + 210d$.

It remains to satisfy congruence (3). Substituting we have $119+210d \equiv 3 \pmod{4} \Rightarrow 210d \equiv 0 \pmod{4} \Rightarrow 2d \equiv 0 \pmod{4} \Rightarrow 2d = 4e$ for some $e \in \mathbb{Z}$. Hence, $x = 119 + 210(2e) =$

$119 + 420e$. In other words, $x \equiv 119 \pmod{420}$

Finally, we conclude that the smallest number of eggs that could have been contained in the basket is **119 eggs**.

Theorem 3.27. *Let a, b, m, and n be integers with $m > 0$ and $n > 0$. Then the system*

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

has a solution if and only if $(n, m)|a - b$.

Proof. Let $a, b, m, n \in \mathbb{Z}$ with $m, n > 0$. Consider the system

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

($\Rightarrow$) Suppose that the above system has a solution, say $x' \in \mathbb{Z}$. Then $n|(x' - a)$ and $m|(x' - b)$ so that $x' - a = rn$ and $x' - b = sm$ for some $r, s \in \mathbb{Z}$. Subtracting the first equation from the second gives $a - b = sm - rn$. Since (m, n) divides each term in the right hand side of the previous equation, it follows that it must divide the left hand side as well. Namely, it follows that $(m, n)|a - b$.

($\Leftarrow$) Suppose that $(n, m)|a - b$. By Theorem 1.40, $\exists r, s \in \mathbb{Z}$ such that $(n, m) = rn - sm$. Let $k := \frac{a-b}{(n,m)} \in \mathbb{Z}$. Multiplying both sides of the previous equation by k gives

$$\begin{array}{rcl} (n, m) & = & rn - sm \\ \Rightarrow k \cdot (n, m) & = & krn - ksm \\ \Rightarrow a - b & = & krn - ksm \\ \Rightarrow a - krn & = & b - ksm \end{array}$$

Now define $x := a - krn = b - ksm \in \mathbb{Z}$. We claim that this x satisfies the above system of linear congruences. This is immediate since $x - a = -krn \Rightarrow n|x - a \Rightarrow x \equiv a \pmod{n}$ and $x - b = -ksm \Rightarrow m|x - b \Rightarrow x \equiv b \pmod{m}$. Hence, the system has a solution.

□

Theorem 3.28. *Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m, n) = 1$. Then the system*

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

has a unique solution modulo mn.

Proof. Omitted. □

Theorem 3.29. (Chinese Remainder Theorem). *Suppose $n_1, n_2, \dots, n_L$ are positive integers that are pairwise relatively prime, that is, $(n_i, n_j) = 1$ for $i \neq j$, $1 \leq i, j \leq L$. Then the system of L congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product $n_1 n_2 n_3 \dots n_L$.

Proof. Omitted. □

Proofs For Marking:

1. Theorem 4.6 (pp.3)
2. Theorem 4.9 (pp.4)
3. Theorem 4.10 (pp.5)
4. Theorem 4.15 (pp.7)
5. Theorem 4.21 (pp.9)
6. Theorem 4.42 (pp.25)

Last name: Alkadri **First name:** Ahmad
Student number: 3283215

4 Fermat's Little Theorem and Euler's Theorem

Orders of an integer modulo n

Exercise 4.1. *For $i = 0, 1, 3, 4, 5$ and 6, find the number in the canonical complete residue system to which 2^i is congruent modulo 7. In other words, compute* $2^0 \pmod 7, 2^1 \pmod 7, \ldots, 2^6 \pmod 7$.

Here is a table summarizing the results:

i	$2^i \pmod 7$	$n \in \{0, 1, \ldots, n-1\}$ *s.t.* $n \equiv 2^i \pmod 7$
0	$1 \pmod 7$	1
1	$2 \pmod 7$	2
2	$4 \pmod 7$	4
3	$8 \pmod 7$	1
4	$16 \pmod 7$	2
5	$32 \pmod 7$	4
6	$64 \pmod 7$	1

Theorem 4.2. *Let a and n be natural numbers with $(a, n) = 1$. Then $(a^j, n) = 1$ for any natural number j.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$. Suppose that $(a, n) = 1$. Let $a = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $n = q_1^{t_1} q_2^{t_2} \ldots q_s^{t_s}$ be the unique prime factorizations of a and n (which we can find by the Fundamental Theorem of Arithmetic). Since a and n are co-prime (i.e. $(a, n) = 1$), we must have that $p_i \neq q_k$ for any $i \leq m$ or $k \leq s$. Let $j \in \mathbb{N}$. Observe that since $a^j = p_1^{jr_1} p_2^{jr_2} \ldots p_m^{jr_m}$ we also have that a^j and n share no common prime factors. Hence, $(a^j, n) = 1$. □

Theorem 4.3. *Let $a, b,$ and n be integers with $n > 0$ and $(a, n) = 1$. If $a \equiv b \pmod n$, then $(b, n) = 1$.*

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose that $(a, n) = 1$ and $a \equiv b \pmod n$. Since $(a, n) = 1$, by Theorem 1.38, $\exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Now since $a \equiv b \pmod n \iff n | a - b$, $\exists z \in \mathbb{Z}$ such that $a = b + zn$. Using this last equation to substitute for a in the first equation yields,

$$\begin{aligned} ax + ny &= 1 \\ a(b + zn) + ny &= 1 \\ ab + (az + y)n &= 1 \end{aligned}$$

Since $a, (az + y) \in \mathbb{Z}$, we have by Theorem 1.39 that $(b, n) = 1$. □

Theorem 4.4. *Let a and n be natural numbers. Then there exist natural numbers i and j, with $i \neq j$, such that $a^i \equiv a^j \pmod n$.*

Proof. Let $a, n \in \mathbb{N}$. Consider the canonical complete residue system modulo n $\mathcal{C} = \{0, 1, \ldots, n-1\}$. Let $k \in \mathbb{N}$. Then by Theorem 3.14, we have that $a^k \equiv r \pmod{n}$ for some $r \in \mathcal{C}$. Since there are only n distinct values that r can take on, in a group of any $n+1$ natural numbers, there must be some $i, j \in \mathbb{N}$ with $i \neq j$ in that group that satisfy $a^i \equiv r \pmod{n}$ and $a^j \equiv r \pmod{n}$ for some $r \in \mathcal{C}$, and hence $a^i \equiv a^j \pmod{n}$. □

Theorem 4.5. *Let a, b, c, and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and $(c, n) = 1$, then $a \equiv b \pmod{n}$.*

Proof. Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$. Suppose that $ac \equiv bc \pmod{n}$ and $(c, n) = 1$. By Theorem 1.38, $\exists x, y \in \mathbb{Z}$ such that $cx + ny = 1$. Furthermore, $\exists k \in \mathbb{Z}$ such that $ac - bc = n$. Now,

$$\begin{aligned} ac - bc &= n \\ c(a-b) &= n \\ cx(a-b) &= nx \\ (1-ny)(a-b) &= nx \\ (a-b) - n(ya - yb) &= nx \\ a - b &= n(x + ya - yb) \end{aligned}$$

Hence, $n | a - b$ so that $a \equiv b \pmod{n}$. □

Theorem 4.6. *Let a and n be natural numbers with $(a, n) = 1$. Then there exists a natural number k such that $a^k \equiv 1 \pmod{n}$.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$. By Theorem 4.4, $\exists i, j \in \mathbb{N}$ with $i \neq j$ such that $a^i \equiv a^j \pmod{n}$. Without loss of generality, suppose that $j > i$. Let $k := j - i$. Then $k \in \mathbb{N}$, and we can write $a^i(1) \equiv a^i a^{j-i} \pmod{n} \iff a^i(1) \equiv a^i a^k \pmod{n}$. Observe that we also have from Theorem 4.2 that $(a, n) = 1 \Rightarrow (a^i, n) = 1$. Hence, by Theorem 4.5, $a^i(1) \equiv a^i a^k \pmod{n} \Rightarrow 1 \equiv a^k \pmod{n} \iff a^k \equiv 1 \pmod{n}$, as desired. □

Fermat's Little Theorem

Question 4.7. *Choose some relatively prime natural numbers a and n and compute the order of a modulo n. Form a conjecture concerning how large the order of a modulo n can be, depending on n.*

Answer. Consider the following table.

a	n	$a^i \equiv r \pmod{n}$	$\mathrm{ord}_n(a)$
6	35	$6 \equiv 6 \pmod{35}$	
		$6^2 \equiv 1 \pmod{35}$	2
2	21	$2 \equiv 2 \pmod{21}$	
		$2^5 \equiv 11 \pmod{21}$	
		$2^6 \equiv 1 \pmod{21}$	6
4	15	$4 \equiv 4 \pmod{15}$	
		$4^2 \equiv 1 \pmod{15}$	
2	27	$2 \equiv 2 \pmod{27}$	
		$2^5 \equiv 5 \pmod{27}$	
		$2^8 \equiv 13 \pmod{27}$	
		$2^10 \equiv 25 \pmod{27}$	
		$2^11 \equiv 23 \pmod{27}$	
		$2^12 \equiv 19 \pmod{27}$	
		$2^13 \equiv 11 \pmod{27}$	
		$2^15 \equiv 17 \pmod{27}$	
		$2^16 \equiv 7 \pmod{27}$	
		$2^18 \equiv 1 \pmod{27}$	18

Based on the observations above, I conjecture that the order of a modulo n must be less than or equal to the number of natural numbers less than n that are coprime with n (in fact, we can form the multiplicative group of integers modulo n in exactly this way, and its order is calculated by counting the number of natural numbers less than n that are relatively prime to n).

Theorem 4.8. *Let a and n be natural numbers with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. Then the numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$, and let $k = \mathrm{ord}_n(a)$. Let $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$. Without loss of generality, suppose that $i > j$. By way of contradiction, suppose that $a^i \equiv a^j \pmod{n}$. Rewrite this as $a^{i-j}a^j \equiv a^j \pmod{n}$. By Theorem 4.2, $(a, n) = 1 \Rightarrow (a^j, n) = 1$. Hence, by Theorem 4.5 we have $a^{i-j} \equiv 1 \pmod{n} \Rightarrow \mathrm{ord}_n(a) \leq i - j < k = \mathrm{ord}_n(a)$, a contradiction. Hence, the numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n. □

Theorem 4.9. *Let a and n be natural numbers with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, \ldots, a^k$.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$, and let $k = \mathrm{ord}_n(a)$. Let $m \in \mathbb{N}$. If $m \leq k$ then it follows immediately that a^m is congruent modulo n to one of $a^1, a^2, \ldots, a^k$ since a^m is equal to one of these numbers.

Suppose that $m > k$. Use the Division Algorithm to find $q, r \in \mathbb{N}$ with $0 \leq r \leq k-1$ such that $m = qk + r$. Observe,

$$\begin{aligned} a^k &\equiv 1 \pmod{n} \\ \Rightarrow \left(a^k\right)^q &\equiv 1^q \pmod{n} \\ \Rightarrow a^{qk} &\equiv 1 \pmod{n} \\ \Rightarrow \left(a^{qk}\right) a^r &\equiv 1 \cdot a^r \pmod{n} \\ \Rightarrow a^{qk+r} &\equiv a^r \pmod{n} \\ \Rightarrow a^m &\equiv a^r \pmod{n} \end{aligned}$$

If $r > 0$, then $1 \leq r < k$, which shows that a^m is congruent modulo n to one of $a^1, a^2, \ldots, a^{k-1}$.
If $r = 0$, then since $a^0 = 1$, and $a^k \equiv 1 \pmod{n}$, it would follow in that case that $a^m \equiv a^k \pmod{n}$, which shows the desired result. □

Theorem 4.10. *Let a and n be natural numbers with $(a, n) = 1$, let $k = \text{ord}_n(a)$, and let m be a natural number. Then $a^m \equiv 1 \pmod{n}$ if and only if $k|m$.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$. Let $k = \text{ord}_n(a)$ and $m \in \mathbb{N}$.

($\Rightarrow$) Suppose that $a^m \equiv 1 \pmod{n}$. Then we know that $m > k$, as otherwise we contradict the minimality of k in being the order of a modulo n. Hence we can use the Division Algorithm to find $q, r \in \mathbb{Z}$ such that $m = qk + r$, $0 \leq r < k$, and $q > 1$ (since $m > k$). Now, by way of contradiction suppose that $r > 0$. Then $a^k \equiv 1 \pmod{n} \Rightarrow a^{qk} \equiv 1 \pmod{n} \Rightarrow a^{qk+r} \equiv a^r \pmod{n}$. Hence, by the transitive property of the congruence relation, we have that $a^r \equiv 1 \pmod{n}$, which contradictions that minimality of k since $0 < r < k$ (note that $r > 0 \Rightarrow r \in \mathbb{N}$). Hence, we must have $r = 0$, which implies that $m = qk$ and hence $k|m$.

($\Leftarrow$) Conversely, suppose that $k|m$. Then $\exists q \in \mathbb{N}$ such that $m = qk$. Now observe,

$$\begin{aligned} a^k &\equiv 1 \pmod{n} \\ \Rightarrow \left(a^k\right)^q &\equiv 1^q \pmod{n} \\ \Rightarrow a^{qk} &\equiv 1 \pmod{n} \\ \Rightarrow a^m &\equiv 1 \pmod{n} \end{aligned}$$

as desired.

□

Theorem 4.11. *Let a and n be natural numbers with $(a, n) = 1$. Then $\text{ord}_n(a) < n$.*

Proof. Let $a, n \in \mathbb{N}$ with $(a, n) = 1$. Let $k = \text{ord}_n(a)$ (which exists by Theorem 4.6). Consider the set $\mathcal{A} = \{a^1, a^2, \ldots, a^n\}$. Theorem 4.2 gives us that $(a^j, n) = 1\ \forall j \in \mathbb{N}$. Hence, $n \nmid (a^j - 0)\ \forall a^j \in \mathcal{A} \Rightarrow a^j \not\equiv 0 \pmod{n}\ \forall a^j \in \mathcal{A}$. Recall $\mathcal{C} = \{0, 1, \ldots, n-1\}$, the canonical complete residue system modulo n. Since none of the elements in $\mathcal{A}$ are equivalent to 0 modulo n, we have that each of the n elements of $\mathcal{A}$ are congruent to one of the remaining $n - 1$ elements of $\mathcal{C}$. It follows that $\exists a^i, a^j \in \mathcal{A}$ with $i \neq j$ such that $a^i \equiv a^j \pmod{n}$. Without loss of generality, suppose that $i > j$. Then, $a^{i-j}a^j \equiv a^j \pmod{n} \Rightarrow a^{i-j} \equiv 1 \pmod{n} \Rightarrow (i - j) \geq \text{ord}_n(a)$. Since $i, j < n$, it follows that $i - j < n$ so that $\text{ord}_n(a) < n$. □

Exercise 4.12. *Compute* $a^{p-1} \pmod{p}$ *for various numbers a and primes p, and make a conjecture.*

Consider the following table:

a	p	$a^{p-1} \pmod{p}$
4	2	0
5	7	1
6	3	0

Based on these results, my conjecture is that

$$a^{p-1} \equiv \begin{cases} 0 \pmod{p} \text{ if } p|a \\ 1 \pmod{p} \text{ if } p \nmid a \end{cases}$$

Theorem 4.13. *Let p be a prime and let a be an integer not divisible by p; that is,* $(a, p) = 1$. *Then* $\{a, 2a, 3a, \ldots, pa\}$ *is a complete residue system modulo p.*

Proof. Let p be a prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Notice that the condition that $p \nmid a$ is equivalent to saying that $(a, p) = 1$ since p is a prime number. Let $\mathcal{A} = \{a, 2a, \ldots, \ldots, \ldots, pa\}$ and $\mathcal{P} = \{1, 2, 3, \ldots, p\}$. We already know that $\mathcal{P}$ is a complete residue system modulo p. Suppose that for some $an, am \in \mathcal{A}$ (where $n, m \in \mathcal{P}$ with $n \neq m$) we have that $an \equiv am \pmod{p}$. Since $(a, p) = 1$, Theorem 4.5 gives us that $n \equiv m \pmod{p}$, and since $\mathcal{P}$ is a complete residue system modulo p, it follows that $n = m$. It follows that the elements of $\mathcal{A}$ are pairwise incongruent modulo p, and since there are p elements in $\mathcal{A}$, we can conclude by Theorem 3.17 that $\mathcal{A}$ is a complete residue system modulo p. □

Theorem 4.14. *Let p be a prime and let a be an integer not divisible by p. Then*

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

Proof. Let p be a prime let $a \in \mathbb{Z}$ with $p \nmid a$. Since p is prime, the condition $p \nmid a$ is equivalent to saying $(a, p) = 1$. By Theorem 4.13, $\mathcal{C} := \{a, 2a, \ldots, pa\}$ is a complete residue system modulo p. We also have that $\mathcal{P} := \{1, 2, \ldots, p\}$ is a complete residue system modulo p. Now, observe that $p|p(a-1) \Rightarrow ap \equiv p \pmod{p}$. Hence, the remaining elements

$\{a, 2a, 3a, \ldots, (p-1)a\}$ is congruent to exactly on of the elements in $\{1, 2, 3, \ldots, p-1$, and so we can multiply these congruences to obtain

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

as desired. □

Theorem 4.15. (Fermat's Little Theorem, Version I) *If p is prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$.*

Proof. Let p be a prime, and $a \in \mathbb{Z}$ with $(a, p) = 1$. By Theorem 4.13,

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$$
$$\Rightarrow a^{p-1} \cdot (2 \cdot \cdots \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$$

Since p is prime, each of the elements $\{2, \ldots, p-1\}$ is relatively prime to p. Hence, by repeated application of Theorem 4.5 we have that

$$a^{p-1} \equiv 1 \pmod{p}$$

as desired. □

Theorem 4.16. (Fermat's Little Theorem, Version II) *If p is a prime and a is any integer, then $a^p \equiv a \pmod{p}$.*

Proof. Let p be a prime and let $a \in \mathbb{Z}$. First observe that by Theorem 4.14, for any $b \in \mathbb{Z}$ with $(b, p) = 1$, we have that $b^{p-1} \equiv 1 \pmod{p} \Rightarrow b^{p-1} \cdot b \equiv 1 \cdot b \pmod{p} \Rightarrow b^p \equiv b \pmod{p}$. By the Fundamental Theorem of Arithmetical, we can factorize a such that $a = p^\alpha q_1^{t_1} q_2^{t_2} \ldots q_m^{t_m}$ where $\alpha \in \mathbb{N} \cup \{0\}$, and $q_i \neq p \ \forall i \leq m$. Let $b := q_1^{t_1} q_2^{t_2} \ldots q_m^{t_m}$. Then it follows that $(b, p) = 1$ since they don't share any prime factors, so we have that $b^p \equiv b \pmod{p}$. Moreover, since $p | \, (p^\alpha)^p - p$, we have that $p^\alpha \equiv p \pmod{p}$. Multiplying these last two congruences together gives $(p^\alpha)^p \, b^p \equiv p^\alpha b \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$. □

Theorem 4.17. *The two versions of Fermat's Little Theorem stated above are equivalent to one another, that is, each one can be deduced from the other.*

Proof. Let p be a prime.

(I ⇒ II). We have already shown this in the proof of Version II of Fermat's Little Theorem.

(II ⇒ I). Let $a \in \mathbb{Z}$ so that $(a, p) = 1$. By version II of Fermat's Little Theorem, we have that $a^p \equiv a \pmod{p} \Rightarrow a^{p-1}a \equiv a \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$ (using the fact that $(a, p) = 1$ and Theorem 4.5), which shows version I of Fermat's Little Theorem.

□

Theorem 4.18. *Let p be a prime and a be an integer. If $(a, p) = 1$, then $\operatorname{ord}_n(a)$ divides $p - 1$, that is, $\operatorname{ord}_p(a) | p - 1$.*

Proof. Let p be a prime and $a \in \mathbb{Z}$ with $(a,p)=1$. Then by Theorem 4.15, $a^{p-1} \equiv 1 \pmod{p}$. It follows immediately from Theorem 4.10 that $\text{ord}_p(a)|p-1$. □

Exercise 4.19. *Compute each of the following without the aid of a calculator or computer.*

1. $512^{372} \pmod{13}$.
2. $3444^{3233} \pmod{17}$.
3. $123^{456} \pmod{23}$.

Observe,

1. *First observe that* $512 = 2^9$ *is relatively prime to 13. Hence, we can start use Fermat's Little Theorem to get*

$$\begin{aligned} 512^{12} &\equiv 1 \pmod{13} \\ \left(512^{12}\right)^{31} &\equiv 1 \pmod{13} \\ 512^{372} &\equiv 1 \pmod{13} \end{aligned}$$

2. *First observe that* $3444 = 861 \cdot 2^2 = 287 \cdot 2^2 \cdot 3 \Rightarrow 17 \nmid 3444 \Rightarrow (3444, 17) = 1$. *Hence, we can start use Fermat's Little Theorem to get*

$$\begin{aligned} 3444^{16} &\equiv 1 \pmod{17} \\ \left(3444^{16}\right)^{202} &\equiv 1 \pmod{13} \\ 3444^{3232} &\equiv 1 \pmod{13} \\ 3444^{3233} &\equiv 3444 \pmod{13} \end{aligned}$$

3. *First observe that* $123 = 41 \cdot 3 \Rightarrow (123, 23) = 1$. *Hence, we can start use version II of Fermat's Little Theorem to get*

$$\begin{aligned} 123^{22} &\equiv 1 \pmod{23} \\ \left(123^{22}\right)^{20} &\equiv 1 \pmod{23} \\ 123^{440} &\equiv 1 \pmod{23} \end{aligned}$$

Moreover,

$$\begin{aligned} 123 &\equiv 8 \pmod{23} \\ 123^2 &\equiv -5 \pmod{23} \\ 123^4 &\equiv 2 \pmod{23} \\ 123^8 &\equiv 4 \pmod{23} \\ 123^{16} &\equiv 16 \pmod{23} \end{aligned}$$

Multiplying these two results together gives

$$123^{456} \equiv 16 \pmod{23}$$

Exercise 4.20. *Find the remainder upon division of* 314^{159} *by 31.*

Observe that 31 is a prime and $314 = 2 \cdot 157 \Rightarrow (314, 31) = 1$. *Hence, we can use Fermat's Little Theorem to write* $314^{30} \equiv 1 \pmod{31} \Rightarrow 314^{150} \equiv 1 \pmod{31}$. *Moreover, we have that* $314 \equiv 4 \pmod{31} \Rightarrow 314^3 \equiv 2 \pmod{31} \Rightarrow 314^9 \equiv 8 \pmod{31}$. *Multiplying these two results together gives* $314^{159} \equiv 8 \pmod{31}$ *so that the remainder upon division of* 314^{159} *by 31 is 8.*

Theorem 4.21. *Let n and m be natural numbers that are relatively prime, and let a be an integer. If* $x \equiv a \pmod{n}$ *and* $x \equiv a \pmod{m}$, *then* $x \equiv a \pmod{nm}$.

Proof. Let $n, m \in \mathbb{N}$ with $(n, m) = 1$. Let $a \in \mathbb{Z}$. Suppose that $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$. Then $\exists r, s \in \mathbb{Z}$ such that $rn = x - a = sm$. Since $(n, m) = 1$, by Theorem 1.38 $\exists u, v \in \mathbb{Z}$ such that $un + vm = 1$. Now observe,

$$\begin{aligned} x - a &= rn \cdot 1 \\ &= rn(un + vm) \\ &= n(u(rn) + rvm) \\ &= n(usm + rvm) \\ &= nm(us + rv) \end{aligned}$$

and since $(us + rv) \in \mathbb{Z}$, we have that $nm | x - a \iff x \equiv a \pmod{nm}$, as desired. □

Exercise 4.22. *Find the remainder of* 4^{72} *is divided by 91* $(= 7 \cdot 13)$.

By Fermat's Little Theorem, we have that $4^6 \equiv 1 \pmod{7} \Rightarrow 4^{72} \equiv 1 \pmod{7}$ *and* $4^{12} \equiv 1 \pmod{13} \Rightarrow 4^{72} \equiv 1 \pmod{13}$. *Hence, By Theorem 4.21* $4^{72} \equiv 1 \pmod{91}$.

Exercise 4.23. *Find the natural number* $k < 117$ *such that* $2^{117} \equiv k \pmod{117}$. *(Notice that 117 is not prime).*

Observe that $117 = 3^2 \cdot 13$. *Moreover, we can deduce from Fermat's Little Theorem that* $2^{12} \equiv 1 \pmod{13} \Rightarrow 2^{108} \equiv 1 \pmod{13}$. *Observe also that* $2^4 \equiv 3 \pmod{13} \Rightarrow 2^8 \equiv 9 \pmod{13} \Rightarrow 2^9 \equiv 5 \pmod{13}$. *Hence,* $2^{117} \equiv 5 \pmod{13}$. *Now,* $2^3 \equiv -1 \pmod{9} \Rightarrow 2^{117} \equiv (-1)^{39} \pmod{9} \equiv 8 \pmod{9}$. *Notice that we can rewrite each of these congruences as* $2^{117} \equiv (5 + 3 \cdot 13) \pmod{13}$ *and* $2^{117} \equiv (8 + 4 \cdot 9) \pmod{9} \Rightarrow 2^{117} \equiv 44 \pmod{13}$ *and* $2^{117} \equiv 44 \pmod{9}$. *Hence by Theorem 4.21* $2^{117} \equiv 44 \pmod{117}$, *so* $k = 44$.

An alternative route to Fermat's Little Theorem

Theorem 4.24. (Binomial Theorem). *Let a and b be numbers and let n be a natural number. Then*

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Proof. Let $a, b \in \mathbb{R}$ and let $n \in \mathbb{N}$. We will prove the Binomial Theorem by induction. Let $P(n) := (a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i$.

Base Case ($n = 1$): $P(1)$ follows immediately since

$$\begin{aligned}
\sum_{i=0}^{1}\binom{1}{i}a^{1-i}b^i &= \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1 \\
&= (a+b)^1
\end{aligned}$$

Induction Step: Suppose that $P(k)$ is true for some $k \in \mathbb{N}$. Observe,

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)^k(a+b) \\
&= \left(\sum_{i=0}^{k}\binom{k}{i}a^{k-i}b^i\right)(a+b) \\
&= \sum_{i=0}^{k}\binom{k}{i}a^{(k+1)-i}b^i + \sum_{i=0}^{k}\binom{k}{i}a^{k-i}b^{i+1} \\
&= \sum_{i=0}^{k}\binom{k}{i}a^{(k+1)-i}b^i + \sum_{i=1}^{k+1}\binom{k}{i-1}a^{k-(i-1)}b^i \\
&= \left(\binom{k}{0}a^{(k+1)-0}b^0 + \sum_{i=1}^{k}\binom{k}{i}a^{(k+1)-i}b^i\right) + \left(\sum_{i=1}^{k}\binom{k}{i-1}a^{(k+1)-i}b^i + \binom{k}{(k+1)-1}a^0b^{k+1}\right) \\
&= \binom{k}{0}a^{(k+1)-0}b^0 + \sum_{i=1}^{k}\left(\binom{k}{i} + \binom{k}{i-1}\right)a^{(k+1)-i}b^i + \binom{k}{(k+1)-1}a^0b^{k+1} \\
&= \sum_{i=1}^{k}\left(\frac{k!}{i!(k-i)!} + \frac{k!}{(i-1)!(k-i+1)!}\right)a^{(k+1)-i}b^i + \binom{k}{0}a^{(k+1)-0}b^0 + \binom{k}{(k+1)-1}a^0b^{k+1} \\
&= \sum_{i=1}^{k}\left(\left(\frac{1}{i} + \frac{1}{k-i+1}\right)\frac{k!}{(i-1)!(k-i)!}\right)a^{(k+1)-i}b^i + \binom{k}{0}a^{(k+1)-0}b^0 + \binom{k}{(k+1)-1}a^0b^{k+1} \\
&= \sum_{i=1}^{k}\left(\left(\frac{k+1}{(i)(k-i+1)}\right)\frac{k!}{(i-1)!(k-i)!}\right)a^{(k+1)-i}b^i + \binom{k}{0}a^{(k+1)-0}b^0 + \binom{k}{(k+1)-1}a^0b^{k+1} \\
&= \sum_{i=1}^{k}\binom{k+1}{i}a^{(k+1)-i}b^i + \binom{k+1}{0}a^{(k+1)-0}b^0 + \binom{k+1}{k+1}a^{(k+1)-(k+1)}b^{k+1} \\
&= \sum_{i=0}^{k+1}\binom{k+1}{i}a^{(k+1)-i}b^i
\end{aligned}$$

which shows $P(k+1)$.

Hence by the principle of mathematical induction, $P(n)$ is true $\forall n \in \mathbb{N}$. □

Lemma 4.25. *If p is prime and i is a natural number less than p, then p divides $\binom{p}{i}$.*

Proof. Let p be a prime, and let $i \in \mathbb{N}$ with $i < p$. We already know that $\binom{p}{i} \in \mathbb{N}$. We first want to show that $\frac{(p-1)!}{i!(p-i)!} \in \mathbb{N}$. Observe that $\frac{p(p-1)!}{i!(p-i)!} = \binom{p}{i} \Rightarrow p(p-1)(p-2)\dots(p-i+1) = \binom{p}{i}i! \Rightarrow i!|p(p-1)(p-2)\dots(p-i+1)$, and since p is prime, it follows that $i!|(p-1)(p-2)\dots(p-i+1) \iff i!|\frac{(p-1)!}{(p-i)!} \Rightarrow \frac{(p-1)!}{i!(p-i)!} \in \mathbb{N}$. Now since $\binom{p}{i} = p \cdot \frac{(p-1)!}{i!(p-i)!}$, it follows that $p|\binom{p}{i}$, as desired. □

Theorem 4.26. (Fermat's Little Theorem, Version II). *If p is a prime and a is an integer, then $a^p \equiv a \pmod{p}$.*

Proof. Let p be a prime and $a \in \mathbb{Z}$.

We first make an intermediate observation based on the preceding text. Let $x, y \in \mathbb{Z}$. Consider $(x+y)^p$. By Theorem 4.24, $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i}y^i$. From Lemma 4.25, we know that p divides every term in the expansion of $(x+y)^p$ except for x^p and y^p. Hence, $(x+y)^p \equiv x^p + y^p \pmod{p}$. We now proceed with a proof of Fermat's Little Theorem using induction.

Base Case ($a = 0$): $0^p \equiv 0 \pmod{p}$ is immediate.

Induction Step 1: Let $k \in \mathbb{Z}$ with $k \geq 0$ and suppose that $k^p \equiv k \pmod{p}$. From before, we know that $(k+1)^p \equiv k^p + 1 \pmod{p}$. The induction hypothesis gives us that $k^p \equiv k \pmod{p}$, which when combined with $1^p \equiv 1 \pmod{p}$ gives us $k^p + 1^p \equiv k + 1 \pmod{p}$. Hence, $(k+1)^p \equiv k + 1 \pmod{p}$. By the principle of mathematical induction, Fermat's Little Theorem follows $\forall k \in \mathbb{Z}$ with $k \geq 0$.

Induction Step 2: Let $k \in \mathbb{Z}$ with $k \leq 0$ and suppose that $k^p \equiv k \pmod{p}$. Similar to before, $(k-1)^p \equiv k^p + (-1)^p \pmod{p}$. Using the induction hypothesis, $k^p \equiv k \pmod{p}$. If $p = 2$, then $(-1)^2 \equiv -1 \pmod{2}$ is easily verified. If $p \neq 2$, then p must be an odd number so that $(-1)^p = -1 \Rightarrow (-1)^p \equiv -1 \pmod{p}$. Hence, $k^p + (-1)^p \equiv k - 1 \pmod{p}$, which implies that $(k-1)^p \equiv k - 1 \pmod{p}$. By the principle of mathematical induction, Fermat's Little Theorem follows $\forall k \in \mathbb{Z}$ with $k \leq 0$.

It now follows that $a^p \equiv a \pmod{p}$ $\forall a \in \mathbb{Z}$. □

Euler's Theorem and Wilson's Theorem

Question 4.27. *The numbers $1, 5, 7,$ and 11 are all natural numbers less than or equal to 12 that are relatively prime to 12, so $\phi(12) = 4$.*

1. *What is $\phi(7)$?*
   $\phi(7) = 6$.

2. *What is $\phi(15)$?*
   $\phi(15) = 8$.

3. *What is $\phi(21)$?*
   $\phi(21) = 12$.

4. *What is $\phi(35)$?*
   $\phi(35) = 24$.

Theorem 4.28. *Let a, b and n be integers such that $(a, n) = 1$ and $(b, n) = 1$. Then $(ab, n) = 1$.*

Proof. Let $a, b, n \in \mathbb{Z}$ such that $(a, n) = 1$ and $(b, n) = 1$. Then by Theorem 1.38, $\exists x, y, u, v \in \mathbb{Z}$ such that $ax + ny = 1$ and $bu + nv = 1$. Now,

$$\begin{aligned} ax \cdot 1 + ny &= 1 \\ \Rightarrow ax(bu + nv) + ny &= 1 \\ \Rightarrow ab(xu) + n(y + axv) &= 1 \end{aligned}$$

Hence by Theorem 1.39, $(ab, n) = 1$. □

Theorem 4.29. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$. and $(a, n) = 1$, then $(b, n) = 1$.*

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose that $a \equiv b \pmod{n}$ and $(a, n) = 1$. By Theorem 1.38, $\exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Moreover, $\exists z \in \mathbb{Z}$ such that $a - b = nz$. Observe,

$$\begin{aligned} ax + ny &= 1 \\ (b + nz)x + ny &= 1 \\ bx + n(zx + y) &= 1 \end{aligned}$$

Hence, by Theorem 1.39, $(b, n) = 1$. □

Theorem 4.30. *Let a, b, c, and n be integers with $n > 0$. If $ab \equiv ac \pmod{n}$ and $(a, n) = 1$, then $b \equiv c \pmod{n}$.*

Proof. Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$. Suppose that $ab \equiv ac \pmod{n}$ and $(a, n) = 1$. By Theorem 1.38, $\exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Moreover, $\exists z \in \mathbb{Z}$ such that $ab - ac = nz$. Now observe,

$$\begin{aligned} ab - ac &= nz \\ a(b - c) &= nz \\ (ax)(b - c) &= n(xz) \\ (1 - ny)(b - c) &= n(xz) \\ b - c &= n(xz + by - cy) \end{aligned}$$

Hence $n|(b-c)$ so that $b \equiv c \pmod{n}$. □

Theorem 4.31. *Let n be a natural number and let $x_1, x_2, \ldots, x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Then $ax_i \not\equiv ax_j \pmod{n}$.*

Proof. Let $n \in \mathbb{N}$, and let $x_1, x_2, \ldots, x_{\phi(n)}$ be the distinct natural numbers that satisfy $x_i \leq n$ and $(x_i, n) = 1 \ \forall 1 \leq i \leq \phi(n)$. Let $a \in \mathbb{Z} \setminus \{0\}$ such that $(a, n) = 1$, and let $1 \leq j < i \leq \phi(n)$ (notice we have assumed without loss of generality that $i > j$). By way of contradiction suppose that $ax_i \equiv ax_j \pmod{n}$. Since each $x_1, x_2, \ldots, x_{\phi(n)}$ is strictly less than n and greater than 0, it is an element of the canonical complete residue class modulo n. In other words, it must be the case that $x_i \not\equiv x_j \pmod{n}$. However, since $(a, n) = 1$, by Theorem 4.30, $ax_i \equiv ax_j \pmod{n} \Rightarrow x_i \equiv x_j \pmod{n}$, a contradiction. Hence, $ax_i \not\equiv ax_j \pmod{n}$. □

Theorem 4.32. (Euler's Theorem). *If a and n are integers with $n > 0$ and $(a, n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof. Let $a, n \in \mathbb{Z}$ with $n > 0$ and $(a, n) = 1$. Let $\mathcal{X} = \{x_1, x_2, \ldots, x_{\phi(n)}\}$ be the set of distinct natural numbers less than or equal to n that are relatively prime to n. Furthermore, define $\mathcal{A} = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\}$. We first make the observation that $\forall x_i \in \mathcal{A}$, Theorem 4.28 gives us that $(a, n) = 1$ and $(x_i, n) = 1 \Rightarrow (ax_i, n) = 1$. By Theorem 4.29, this means that if $ax_i \equiv b \pmod{n}$ for some $b \in \mathbb{Z}$, then b must satisfy $(b, n) = 1$. Since all possible integers in the canonical complete residue system modulo n that are relatively prime to n are given in the set $\mathcal{X}$, it follows that $ax_i \equiv x_j \pmod{n}$ for some $x_j \in \mathcal{X}$. Since each element in $\mathcal{A}$ is congruent to an element in $\mathcal{X}$ modulo n. Moreover, by Theorem 4.31, since none of the elements in $\mathcal{A}$ are congruent to each other, there is a one-to-one correspondence between elements of $\mathcal{A}$ and elements of $\mathcal{X}$ that are congruent to each other. Hence, we can multiply these $\phi(n)$ congruences to obtain

$$\begin{aligned} ax_1 \cdot ax_2 \cdot \cdots \cdot ax_{\phi(n)} &\equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\phi(n)} \pmod{n} \\ \Rightarrow a^{\phi(n)}(x_1 \cdot x_2 \cdot \cdots \cdot x_{\phi(n)}) &\equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\phi(n)} \pmod{n} \end{aligned}$$

and since each element in $\mathcal{X}$ is relatively prime to n, we can apply Theorem 4.30 $\phi(n)$ times to obtain

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

as desired. □

Corollary 4.33. (Fermat's Little Theorem). *If p is a prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$.*

Proof. Let p be a prime and $a \in \mathbb{Z}$ with $(a,p) = 1$. By Euler's Theorem,

$$a^{\phi(p)} \equiv 1 \pmod{p}$$

since every natural number less than p is relatively prime to p, we have $\phi(p) = p-1$ so that

$$a^{(p-1)} \equiv 1 \pmod{p}$$

□

Exercise 4.34. *Compute each of the following without the aid of a calculator or computer.*

1. $12^{49} \pmod{15}$.

First observe that $3^4 \equiv -1 \pmod{15} \Rightarrow 3^{48} \equiv 1 \pmod{15} \Rightarrow 3^{49} \equiv 3 \pmod{15}$. *We also have that* $\phi(15) = 8$. *Since* $(4,15) = 1$, *we can apply Euler's Theorem to get* $4^8 \equiv 1 \pmod{15} \Rightarrow 4^{48} \equiv 1 \pmod{15} \Rightarrow 4^{49} \equiv 4 \pmod{15}$. *Multiplying the two results gives* $12^{49} \equiv 12 \pmod{15}$.

2. $139^{112} \pmod{27}$.

Since $3 \nmid 139$, $(139, 27) = 1$. *We also have that* $\phi(27) = 18$. *By Euler's Theorem,* $139^{18} \equiv 1 \pmod{27} \Rightarrow 139^{108} \equiv 1 \pmod{27}$. *Observe also that* $139 \equiv 4 \pmod{27} \Rightarrow 139^4 \equiv 13 \pmod{27}$. *Hence,* $139^{112} \equiv 13 \pmod{27}$.

Exercise 4.35. *Find the last digit in the base 10 representation of the integer* 13^{474}.

We are basically being asked to compute $13^{474} \pmod{10}$. *Note that* $\phi(10) = 4$ *Since* $(13, 10) = 1$, *we can apply Euler's Theorem to obtain* $13^4 \equiv 1 \pmod{10} \Rightarrow 13^{472} \equiv 1 \pmod{10} \Rightarrow 13^{474} \equiv 9 \pmod{10}$. *Hence, the last digit is a 9.*

Theorem 4.36. *Let p be a prime and let a be an integer such that $1 \leq a < p$. Then there exists a unique natural number b less than p such that $ab \equiv 1 \pmod{p}$.*

Proof. Let p be a prime, and let $a \in \mathbb{Z}$ with $1 \leq a < p$. If $p = 2$, then it must be the case that $a = 1$, and we trivially have that $1 \cdot 1 \equiv 1 \pmod{2}$. Suppose that $p > 2$. Then by Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a \cdot a^{p-2} \equiv 1 \pmod{p}$. Since $p > 2$, we have that $a^{p-2} \in \mathbb{Z}$ with $a^{p-2} \geq 1$ (with $a^{p-2} = 1$ if and only if $a = 1$). Hence, we can use the Division Algorithm to find unique $q, b \in \mathbb{Z}$ with $0 \leq b < p$ such that $a^{p-2} = qp + b$. Since p is prime, however, and $a \nmid p \Rightarrow a^{p-2} \nmid p$, it must be the case that $1 \leq b < p$. Now observe that $a \cdot a^{p-2} \equiv 1 \pmod{p} \Rightarrow a \cdot (qp + b) \equiv 1 \pmod{p} \Rightarrow ab \equiv 1 \pmod{p}$, as desired. □

Exercise 4.37. *Let p be a prime. Show that the natural numbers 1 and $p-1$ are their own inverses modulo p.*

$1 \cdot 1 \equiv 1 \pmod{p}$ *is immediate because of the reflexive property of congruence modulo p. In the case of $p-1$, observe that $(p-1)(p-1) = p^2 - 2p + 1$, which clearly leaves a remainder of 1 when divided by p. Hence,* $(p-1)(p-1) \equiv 1 \pmod{p}$.

Theorem 4.38. *Let p be a prime and let a and b be integers such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$. Then $a \neq b$.*

Proof. Let p be a prime, and let $a, b \in \mathbb{Z}$ such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$. By way of contradiction, suppose that $a = b$. Then $a^2 \equiv 1 \pmod{p} \Rightarrow p|(a^2-1) \Rightarrow p|(a-1)$ or $p|(a+1)$. If $p|a-1$, then $a \equiv 1 \pmod{p}$, but the only $1 \leq a \leq p-1$ for which this holds is $a = 1$, a contradiction. Suppose that $p|(a+1)$. Then $a \equiv -1 \pmod{p} \Rightarrow a \equiv p-1 \pmod{p}$, but the only $1 \leq a \leq p-1$ for which this holds is $a = p-1$, a contradiction. Hence, $a \neq b$. □

Exercise 4.39. *Find all pairs of numbers a and b in $\{2, 3, \ldots, 11\}$ such that $ab \equiv 1 \pmod{13}$.*

The results are in the following table:

a	b
2	7
3	9
4	10
5	8
6	11
7	2
8	5
9	3
10	4
11	6

Theorem 4.40. *If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}$.*

Proof. Let p be a prime with $p > 2$. Consider $S := \{2, 3, 4, \ldots, p-2\}$. Note that $|S| = p-3$ is an even number since $p > 2$ implies that p is an odd number, so $p-3$ is even. For every $a \in S$, we can apply Theorems 4.38 and 4.39 to find a unique $b \in S$ such that $ab \equiv 1 \pmod{p}$. In other words, we can divide S up perfectly into pairs $\{(a_1, b_1), (a_2, b_2), \ldots, a_{\frac{p-3}{2}}, b_{\frac{p-3}{2}}\}$ such that $a_i b_i \equiv 1 \pmod{p}$ $\forall 1 \leq i \leq \frac{p-3}{2}$. Multiplying each of these congruences together and using the commutative property of multiplication gives

$$\begin{aligned} \prod_{i=1}^{\frac{p-3}{2}} a_i b_i &\equiv 1 \pmod{p} \\ \Rightarrow 2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) &\equiv 1 \pmod{p} \end{aligned}$$

as desired. □

Theorem 4.41. (Wilson's Theorem). *If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Let p be a prime. If $p = 2$, then $(p-1)! = (2-1)! = 1$, and we clearly have that $1 \equiv -1 \pmod{2}$. Suppose that $p > 2$. Then by Theorem 4.40,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}$$

Multiplying by the congruence $p - 1 \equiv p - 1 \pmod{p}$ gives

$$(p-1)! \equiv p - 1 \pmod{p}$$

We also have that $p - 1 \equiv -1 \pmod{p}$ since $p|p \Rightarrow p|((p-1) - (-1))$. Hence,

$$(p-1)! \equiv -1 \pmod{p}$$

as desired. □

Theorem 4.42. (Converse of Wilson's Theorem). *If n is a natural number such that*

$$(n-1)! \equiv -1 \pmod{n}$$

then n is prime.

Proof. Let $n \in \mathbb{N}$, and suppose that $(n-1)! \equiv -1 \pmod{n}$. By way of contradiction, suppose that n is not prime. Then $\exists a \in \mathbb{N}$ with $1 < a < n$ such that $a|n$. Moreover, since $(n-1)! = 2 \cdot 3 \cdot \cdots \cdot a \cdot \cdots \cdot (n-1)$, we have that $a|(n-1)!$. Observe also that $(n-1)! \equiv -1 \pmod{n} \iff n|((n-1)!+1) \Rightarrow a|((n-1)!+1)$ since $a|n$. Hence, $\exists x, y \in \mathbb{Z}$ such that $ax = (n-1)!$ and $ay = (n-1)!+1 \Rightarrow a(y-x) = 1 \Rightarrow a|1 \Rightarrow a = 1$, a contradiction. Hence, n must be prime. □

Appendix A: Tables for Exercise 4.1.1

We first note that the following Python Script was used to generate the LaTeX code for the appropriate tables:

Python Code:

```
A = [2, 3]
N = [i for i in range(1,37)]
K = [i for i in range(1,11)]

result = ''
for n in N:
        for k in K:
                for a in A:
                        result += str(k) + ' & ' + str(n) + ' & ' + \
                        '$' + str(a) + '^{' + str(k) + '}' + ' \mod{' +
                        str(a**k % n) + '$'
                        if a != A[-1]:
                                result += ' & '
                        else:
                                result += '\\\ \n'

print(result)
```

The output of this result in tabular form is:

$a = 2$: k	n	$a^k \pmod{n}$	$a = 3$: k	n	$a^k \pmod{n}$
1	1	$2^1 \pmod{1} = 0$	1	1	$3^1 \pmod{1} = 0$
2	1	$2^2 \pmod{1} = 0$	2	1	$3^2 \pmod{1} = 0$
3	1	$2^3 \pmod{1} = 0$	3	1	$3^3 \pmod{1} = 0$
4	1	$2^4 \pmod{1} = 0$	4	1	$3^4 \pmod{1} = 0$
5	1	$2^5 \pmod{1} = 0$	5	1	$3^5 \pmod{1} = 0$
6	1	$2^6 \pmod{1} = 0$	6	1	$3^6 \pmod{1} = 0$
7	1	$2^7 \pmod{1} = 0$	7	1	$3^7 \pmod{1} = 0$
8	1	$2^8 \pmod{1} = 0$	8	1	$3^8 \pmod{1} = 0$
9	1	$2^9 \pmod{1} = 0$	9	1	$3^9 \pmod{1} = 0$
10	1	$2^{10} \pmod{1} = 0$	10	1	$3^{10} \pmod{1} = 0$
1	2	$2^1 \pmod{2} = 0$	1	2	$3^1 \pmod{2} = 1$
2	2	$2^2 \pmod{2} = 0$	2	2	$3^2 \pmod{2} = 1$
3	2	$2^3 \pmod{2} = 0$	3	2	$3^3 \pmod{2} = 1$
4	2	$2^4 \pmod{2} = 0$	4	2	$3^4 \pmod{2} = 1$
5	2	$2^5 \pmod{2} = 0$	5	2	$3^5 \pmod{2} = 1$
6	2	$2^6 \pmod{2} = 0$	6	2	$3^6 \pmod{2} = 1$

7	2	$2^{7} \pmod{2} = 0$	7	2	$3^{7} \pmod{2} = 1$
8	2	$2^{8} \pmod{2} = 0$	8	2	$3^{8} \pmod{2} = 1$
9	2	$2^{9} \pmod{2} = 0$	9	2	$3^{9} \pmod{2} = 1$
10	2	$2^{10} \pmod{2} = 0$	10	2	$3^{10} \pmod{2} = 1$
1	3	$2^{1} \pmod{3} = 2$	1	3	$3^{1} \pmod{3} = 0$
2	3	$2^{2} \pmod{3} = 1$	2	3	$3^{2} \pmod{3} = 0$
3	3	$2^{3} \pmod{3} = 2$	3	3	$3^{3} \pmod{3} = 0$
4	3	$2^{4} \pmod{3} = 1$	4	3	$3^{4} \pmod{3} = 0$
5	3	$2^{5} \pmod{3} = 2$	5	3	$3^{5} \pmod{3} = 0$
6	3	$2^{6} \pmod{3} = 1$	6	3	$3^{6} \pmod{3} = 0$
7	3	$2^{7} \pmod{3} = 2$	7	3	$3^{7} \pmod{3} = 0$
8	3	$2^{8} \pmod{3} = 1$	8	3	$3^{8} \pmod{3} = 0$
9	3	$2^{9} \pmod{3} = 2$	9	3	$3^{9} \pmod{3} = 0$
10	3	$2^{10} \pmod{3} = 1$	10	3	$3^{10} \pmod{3} = 0$
1	4	$2^{1} \pmod{4} = 2$	1	4	$3^{1} \pmod{4} = 3$
2	4	$2^{2} \pmod{4} = 0$	2	4	$3^{2} \pmod{4} = 1$
3	4	$2^{3} \pmod{4} = 0$	3	4	$3^{3} \pmod{4} = 3$
4	4	$2^{4} \pmod{4} = 0$	4	4	$3^{4} \pmod{4} = 1$
5	4	$2^{5} \pmod{4} = 0$	5	4	$3^{5} \pmod{4} = 3$
6	4	$2^{6} \pmod{4} = 0$	6	4	$3^{6} \pmod{4} = 1$
7	4	$2^{7} \pmod{4} = 0$	7	4	$3^{7} \pmod{4} = 3$
8	4	$2^{8} \pmod{4} = 0$	8	4	$3^{8} \pmod{4} = 1$
9	4	$2^{9} \pmod{4} = 0$	9	4	$3^{9} \pmod{4} = 3$
10	4	$2^{10} \pmod{4} = 0$	10	4	$3^{10} \pmod{4} = 1$
1	5	$2^{1} \pmod{5} = 2$	1	5	$3^{1} \pmod{5} = 3$
2	5	$2^{2} \pmod{5} = 4$	2	5	$3^{2} \pmod{5} = 4$
3	5	$2^{3} \pmod{5} = 3$	3	5	$3^{3} \pmod{5} = 2$
4	5	$2^{4} \pmod{5} = 1$	4	5	$3^{4} \pmod{5} = 1$
5	5	$2^{5} \pmod{5} = 2$	5	5	$3^{5} \pmod{5} = 3$
6	5	$2^{6} \pmod{5} = 4$	6	5	$3^{6} \pmod{5} = 4$
7	5	$2^{7} \pmod{5} = 3$	7	5	$3^{7} \pmod{5} = 2$
8	5	$2^{8} \pmod{5} = 1$	8	5	$3^{8} \pmod{5} = 1$
9	5	$2^{9} \pmod{5} = 2$	9	5	$3^{9} \pmod{5} = 3$
10	5	$2^{10} \pmod{5} = 4$	10	5	$3^{10} \pmod{5} = 4$
1	6	$2^{1} \pmod{6} = 2$	1	6	$3^{1} \pmod{6} = 3$
2	6	$2^{2} \pmod{6} = 4$	2	6	$3^{2} \pmod{6} = 3$
3	6	$2^{3} \pmod{6} = 2$	3	6	$3^{3} \pmod{6} = 3$
4	6	$2^{4} \pmod{6} = 4$	4	6	$3^{4} \pmod{6} = 3$
5	6	$2^{5} \pmod{6} = 2$	5	6	$3^{5} \pmod{6} = 3$
6	6	$2^{6} \pmod{6} = 4$	6	6	$3^{6} \pmod{6} = 3$
7	6	$2^{7} \pmod{6} = 2$	7	6	$3^{7} \pmod{6} = 3$
8	6	$2^{8} \pmod{6} = 4$	8	6	$3^{8} \pmod{6} = 3$

9	6	$2^{9} \pmod{6} = 2$	9	6	$3^{9} \pmod{6} = 3$
10	6	$2^{10} \pmod{6} = 4$	10	6	$3^{10} \pmod{6} = 3$
1	7	$2^{1} \pmod{7} = 2$	1	7	$3^{1} \pmod{7} = 3$
2	7	$2^{2} \pmod{7} = 4$	2	7	$3^{2} \pmod{7} = 2$
3	7	$2^{3} \pmod{7} = 1$	3	7	$3^{3} \pmod{7} = 6$
4	7	$2^{4} \pmod{7} = 2$	4	7	$3^{4} \pmod{7} = 4$
5	7	$2^{5} \pmod{7} = 4$	5	7	$3^{5} \pmod{7} = 5$
6	7	$2^{6} \pmod{7} = 1$	6	7	$3^{6} \pmod{7} = 1$
7	7	$2^{7} \pmod{7} = 2$	7	7	$3^{7} \pmod{7} = 3$
8	7	$2^{8} \pmod{7} = 4$	8	7	$3^{8} \pmod{7} = 2$
9	7	$2^{9} \pmod{7} = 1$	9	7	$3^{9} \pmod{7} = 6$
10	7	$2^{10} \pmod{7} = 2$	10	7	$3^{10} \pmod{7} = 4$
1	8	$2^{1} \pmod{8} = 2$	1	8	$3^{1} \pmod{8} = 3$
2	8	$2^{2} \pmod{8} = 4$	2	8	$3^{2} \pmod{8} = 1$
3	8	$2^{3} \pmod{8} = 0$	3	8	$3^{3} \pmod{8} = 3$
4	8	$2^{4} \pmod{8} = 0$	4	8	$3^{4} \pmod{8} = 1$
5	8	$2^{5} \pmod{8} = 0$	5	8	$3^{5} \pmod{8} = 3$
6	8	$2^{6} \pmod{8} = 0$	6	8	$3^{6} \pmod{8} = 1$
7	8	$2^{7} \pmod{8} = 0$	7	8	$3^{7} \pmod{8} = 3$
8	8	$2^{8} \pmod{8} = 0$	8	8	$3^{8} \pmod{8} = 1$
9	8	$2^{9} \pmod{8} = 0$	9	8	$3^{9} \pmod{8} = 3$
10	8	$2^{10} \pmod{8} = 0$	10	8	$3^{10} \pmod{8} = 1$
1	9	$2^{1} \pmod{9} = 2$	1	9	$3^{1} \pmod{9} = 3$
2	9	$2^{2} \pmod{9} = 4$	2	9	$3^{2} \pmod{9} = 0$
3	9	$2^{3} \pmod{9} = 8$	3	9	$3^{3} \pmod{9} = 0$
4	9	$2^{4} \pmod{9} = 7$	4	9	$3^{4} \pmod{9} = 0$
5	9	$2^{5} \pmod{9} = 5$	5	9	$3^{5} \pmod{9} = 0$
6	9	$2^{6} \pmod{9} = 1$	6	9	$3^{6} \pmod{9} = 0$
7	9	$2^{7} \pmod{9} = 2$	7	9	$3^{7} \pmod{9} = 0$
8	9	$2^{8} \pmod{9} = 4$	8	9	$3^{8} \pmod{9} = 0$
9	9	$2^{9} \pmod{9} = 8$	9	9	$3^{9} \pmod{9} = 0$
10	9	$2^{10} \pmod{9} = 7$	10	9	$3^{10} \pmod{9} = 0$
1	10	$2^{1} \pmod{10} = 2$	1	10	$3^{1} \pmod{10} = 3$
2	10	$2^{2} \pmod{10} = 4$	2	10	$3^{2} \pmod{10} = 9$
3	10	$2^{3} \pmod{10} = 8$	3	10	$3^{3} \pmod{10} = 7$
4	10	$2^{4} \pmod{10} = 6$	4	10	$3^{4} \pmod{10} = 1$
5	10	$2^{5} \pmod{10} = 2$	5	10	$3^{5} \pmod{10} = 3$
6	10	$2^{6} \pmod{10} = 4$	6	10	$3^{6} \pmod{10} = 9$
7	10	$2^{7} \pmod{10} = 8$	7	10	$3^{7} \pmod{10} = 7$
8	10	$2^{8} \pmod{10} = 6$	8	10	$3^{8} \pmod{10} = 1$
9	10	$2^{9} \pmod{10} = 2$	9	10	$3^{9} \pmod{10} = 3$
10	10	$2^{10} \pmod{10} = 4$	10	10	$3^{10} \pmod{10} = 9$

1	11	$2^1 \pmod{11} = 2$	1	11	$3^1 \pmod{11} = 3$
2	11	$2^2 \pmod{11} = 4$	2	11	$3^2 \pmod{11} = 9$
3	11	$2^3 \pmod{11} = 8$	3	11	$3^3 \pmod{11} = 5$
4	11	$2^4 \pmod{11} = 5$	4	11	$3^4 \pmod{11} = 4$
5	11	$2^5 \pmod{11} = 10$	5	11	$3^5 \pmod{11} = 1$
6	11	$2^6 \pmod{11} = 9$	6	11	$3^6 \pmod{11} = 3$
7	11	$2^7 \pmod{11} = 7$	7	11	$3^7 \pmod{11} = 9$
8	11	$2^8 \pmod{11} = 3$	8	11	$3^8 \pmod{11} = 5$
9	11	$2^9 \pmod{11} = 6$	9	11	$3^9 \pmod{11} = 4$
10	11	$2^{10} \pmod{11} = 1$	10	11	$3^{10} \pmod{11} = 1$
1	12	$2^1 \pmod{12} = 2$	1	12	$3^1 \pmod{12} = 3$
2	12	$2^2 \pmod{12} = 4$	2	12	$3^2 \pmod{12} = 9$
3	12	$2^3 \pmod{12} = 8$	3	12	$3^3 \pmod{12} = 3$
4	12	$2^4 \pmod{12} = 4$	4	12	$3^4 \pmod{12} = 9$
5	12	$2^5 \pmod{12} = 8$	5	12	$3^5 \pmod{12} = 3$
6	12	$2^6 \pmod{12} = 4$	6	12	$3^6 \pmod{12} = 9$
7	12	$2^7 \pmod{12} = 8$	7	12	$3^7 \pmod{12} = 3$
8	12	$2^8 \pmod{12} = 4$	8	12	$3^8 \pmod{12} = 9$
9	12	$2^9 \pmod{12} = 8$	9	12	$3^9 \pmod{12} = 3$
10	12	$2^{10} \pmod{12} = 4$	10	12	$3^{10} \pmod{12} = 9$
1	13	$2^1 \pmod{13} = 2$	1	13	$3^1 \pmod{13} = 3$
2	13	$2^2 \pmod{13} = 4$	2	13	$3^2 \pmod{13} = 9$
3	13	$2^3 \pmod{13} = 8$	3	13	$3^3 \pmod{13} = 1$
4	13	$2^4 \pmod{13} = 3$	4	13	$3^4 \pmod{13} = 3$
5	13	$2^5 \pmod{13} = 6$	5	13	$3^5 \pmod{13} = 9$
6	13	$2^6 \pmod{13} = 12$	6	13	$3^6 \pmod{13} = 1$
7	13	$2^7 \pmod{13} = 11$	7	13	$3^7 \pmod{13} = 3$
8	13	$2^8 \pmod{13} = 9$	8	13	$3^8 \pmod{13} = 9$
9	13	$2^9 \pmod{13} = 5$	9	13	$3^9 \pmod{13} = 1$
10	13	$2^{10} \pmod{13} = 10$	10	13	$3^{10} \pmod{13} = 3$
1	14	$2^1 \pmod{14} = 2$	1	14	$3^1 \pmod{14} = 3$
2	14	$2^2 \pmod{14} = 4$	2	14	$3^2 \pmod{14} = 9$
3	14	$2^3 \pmod{14} = 8$	3	14	$3^3 \pmod{14} = 13$
4	14	$2^4 \pmod{14} = 2$	4	14	$3^4 \pmod{14} = 11$
5	14	$2^5 \pmod{14} = 4$	5	14	$3^5 \pmod{14} = 5$
6	14	$2^6 \pmod{14} = 8$	6	14	$3^6 \pmod{14} = 1$
7	14	$2^7 \pmod{14} = 2$	7	14	$3^7 \pmod{14} = 3$
8	14	$2^8 \pmod{14} = 4$	8	14	$3^8 \pmod{14} = 9$
9	14	$2^9 \pmod{14} = 8$	9	14	$3^9 \pmod{14} = 13$
10	14	$2^{10} \pmod{14} = 2$	10	14	$3^{10} \pmod{14} = 11$
1	15	$2^1 \pmod{15} = 2$	1	15	$3^1 \pmod{15} = 3$
2	15	$2^2 \pmod{15} = 4$	2	15	$3^2 \pmod{15} = 9$

3	15	$2^{3} \pmod{15} = 8$	3	15	$3^{3} \pmod{15} = 12$
4	15	$2^{4} \pmod{15} = 1$	4	15	$3^{4} \pmod{15} = 6$
5	15	$2^{5} \pmod{15} = 2$	5	15	$3^{5} \pmod{15} = 3$
6	15	$2^{6} \pmod{15} = 4$	6	15	$3^{6} \pmod{15} = 9$
7	15	$2^{7} \pmod{15} = 8$	7	15	$3^{7} \pmod{15} = 12$
8	15	$2^{8} \pmod{15} = 1$	8	15	$3^{8} \pmod{15} = 6$
9	15	$2^{9} \pmod{15} = 2$	9	15	$3^{9} \pmod{15} = 3$
10	15	$2^{10} \pmod{15} = 4$	10	15	$3^{10} \pmod{15} = 9$
1	16	$2^{1} \pmod{16} = 2$	1	16	$3^{1} \pmod{16} = 3$
2	16	$2^{2} \pmod{16} = 4$	2	16	$3^{2} \pmod{16} = 9$
3	16	$2^{3} \pmod{16} = 8$	3	16	$3^{3} \pmod{16} = 11$
4	16	$2^{4} \pmod{16} = 0$	4	16	$3^{4} \pmod{16} = 1$
5	16	$2^{5} \pmod{16} = 0$	5	16	$3^{5} \pmod{16} = 3$
6	16	$2^{6} \pmod{16} = 0$	6	16	$3^{6} \pmod{16} = 9$
7	16	$2^{7} \pmod{16} = 0$	7	16	$3^{7} \pmod{16} = 11$
8	16	$2^{8} \pmod{16} = 0$	8	16	$3^{8} \pmod{16} = 1$
9	16	$2^{9} \pmod{16} = 0$	9	16	$3^{9} \pmod{16} = 3$
10	16	$2^{10} \pmod{16} = 0$	10	16	$3^{10} \pmod{16} = 9$
1	17	$2^{1} \pmod{17} = 2$	1	17	$3^{1} \pmod{17} = 3$
2	17	$2^{2} \pmod{17} = 4$	2	17	$3^{2} \pmod{17} = 9$
3	17	$2^{3} \pmod{17} = 8$	3	17	$3^{3} \pmod{17} = 10$
4	17	$2^{4} \pmod{17} = 16$	4	17	$3^{4} \pmod{17} = 13$
5	17	$2^{5} \pmod{17} = 15$	5	17	$3^{5} \pmod{17} = 5$
6	17	$2^{6} \pmod{17} = 13$	6	17	$3^{6} \pmod{17} = 15$
7	17	$2^{7} \pmod{17} = 9$	7	17	$3^{7} \pmod{17} = 11$
8	17	$2^{8} \pmod{17} = 1$	8	17	$3^{8} \pmod{17} = 16$
9	17	$2^{9} \pmod{17} = 2$	9	17	$3^{9} \pmod{17} = 14$
10	17	$2^{10} \pmod{17} = 4$	10	17	$3^{10} \pmod{17} = 8$
1	18	$2^{1} \pmod{18} = 2$	1	18	$3^{1} \pmod{18} = 3$
2	18	$2^{2} \pmod{18} = 4$	2	18	$3^{2} \pmod{18} = 9$
3	18	$2^{3} \pmod{18} = 8$	3	18	$3^{3} \pmod{18} = 9$
4	18	$2^{4} \pmod{18} = 16$	4	18	$3^{4} \pmod{18} = 9$
5	18	$2^{5} \pmod{18} = 14$	5	18	$3^{5} \pmod{18} = 9$
6	18	$2^{6} \pmod{18} = 10$	6	18	$3^{6} \pmod{18} = 9$
7	18	$2^{7} \pmod{18} = 2$	7	18	$3^{7} \pmod{18} = 9$
8	18	$2^{8} \pmod{18} = 4$	8	18	$3^{8} \pmod{18} = 9$
9	18	$2^{9} \pmod{18} = 8$	9	18	$3^{9} \pmod{18} = 9$
10	18	$2^{10} \pmod{18} = 16$	10	18	$3^{10} \pmod{18} = 9$
1	19	$2^{1} \pmod{19} = 2$	1	19	$3^{1} \pmod{19} = 3$
2	19	$2^{2} \pmod{19} = 4$	2	19	$3^{2} \pmod{19} = 9$
3	19	$2^{3} \pmod{19} = 8$	3	19	$3^{3} \pmod{19} = 8$
4	19	$2^{4} \pmod{19} = 16$	4	19	$3^{4} \pmod{19} = 5$

5	19	$2^{5} \pmod{19} = 13$	5	19	$3^{5} \pmod{19} = 15$
6	19	$2^{6} \pmod{19} = 7$	6	19	$3^{6} \pmod{19} = 7$
7	19	$2^{7} \pmod{19} = 14$	7	19	$3^{7} \pmod{19} = 2$
8	19	$2^{8} \pmod{19} = 9$	8	19	$3^{8} \pmod{19} = 6$
9	19	$2^{9} \pmod{19} = 18$	9	19	$3^{9} \pmod{19} = 18$
10	19	$2^{10} \pmod{19} = 17$	10	19	$3^{10} \pmod{19} = 16$
1	20	$2^{1} \pmod{20} = 2$	1	20	$3^{1} \pmod{20} = 3$
2	20	$2^{2} \pmod{20} = 4$	2	20	$3^{2} \pmod{20} = 9$
3	20	$2^{3} \pmod{20} = 8$	3	20	$3^{3} \pmod{20} = 7$
4	20	$2^{4} \pmod{20} = 16$	4	20	$3^{4} \pmod{20} = 1$
5	20	$2^{5} \pmod{20} = 12$	5	20	$3^{5} \pmod{20} = 3$
6	20	$2^{6} \pmod{20} = 4$	6	20	$3^{6} \pmod{20} = 9$
7	20	$2^{7} \pmod{20} = 8$	7	20	$3^{7} \pmod{20} = 7$
8	20	$2^{8} \pmod{20} = 16$	8	20	$3^{8} \pmod{20} = 1$
9	20	$2^{9} \pmod{20} = 12$	9	20	$3^{9} \pmod{20} = 3$
10	20	$2^{10} \pmod{20} = 4$	10	20	$3^{10} \pmod{20} = 9$
1	21	$2^{1} \pmod{21} = 2$	1	21	$3^{1} \pmod{21} = 3$
2	21	$2^{2} \pmod{21} = 4$	2	21	$3^{2} \pmod{21} = 9$
3	21	$2^{3} \pmod{21} = 8$	3	21	$3^{3} \pmod{21} = 6$
4	21	$2^{4} \pmod{21} = 16$	4	21	$3^{4} \pmod{21} = 18$
5	21	$2^{5} \pmod{21} = 11$	5	21	$3^{5} \pmod{21} = 12$
6	21	$2^{6} \pmod{21} = 1$	6	21	$3^{6} \pmod{21} = 15$
7	21	$2^{7} \pmod{21} = 2$	7	21	$3^{7} \pmod{21} = 3$
8	21	$2^{8} \pmod{21} = 4$	8	21	$3^{8} \pmod{21} = 9$
9	21	$2^{9} \pmod{21} = 8$	9	21	$3^{9} \pmod{21} = 6$
10	21	$2^{10} \pmod{21} = 16$	10	21	$3^{10} \pmod{21} = 18$
1	22	$2^{1} \pmod{22} = 2$	1	22	$3^{1} \pmod{22} = 3$
2	22	$2^{2} \pmod{22} = 4$	2	22	$3^{2} \pmod{22} = 9$
3	22	$2^{3} \pmod{22} = 8$	3	22	$3^{3} \pmod{22} = 5$
4	22	$2^{4} \pmod{22} = 16$	4	22	$3^{4} \pmod{22} = 15$
5	22	$2^{5} \pmod{22} = 10$	5	22	$3^{5} \pmod{22} = 1$
6	22	$2^{6} \pmod{22} = 20$	6	22	$3^{6} \pmod{22} = 3$
7	22	$2^{7} \pmod{22} = 18$	7	22	$3^{7} \pmod{22} = 9$
8	22	$2^{8} \pmod{22} = 14$	8	22	$3^{8} \pmod{22} = 5$
9	22	$2^{9} \pmod{22} = 6$	9	22	$3^{9} \pmod{22} = 15$
10	22	$2^{10} \pmod{22} = 12$	10	22	$3^{10} \pmod{22} = 1$
1	23	$2^{1} \pmod{23} = 2$	1	23	$3^{1} \pmod{23} = 3$
2	23	$2^{2} \pmod{23} = 4$	2	23	$3^{2} \pmod{23} = 9$
3	23	$2^{3} \pmod{23} = 8$	3	23	$3^{3} \pmod{23} = 4$
4	23	$2^{4} \pmod{23} = 16$	4	23	$3^{4} \pmod{23} = 12$
5	23	$2^{5} \pmod{23} = 9$	5	23	$3^{5} \pmod{23} = 13$
6	23	$2^{6} \pmod{23} = 18$	6	23	$3^{6} \pmod{23} = 16$

7	23	$2^7 \pmod{23} = 13$	7	23	$3^7 \pmod{23} = 2$
8	23	$2^8 \pmod{23} = 3$	8	23	$3^8 \pmod{23} = 6$
9	23	$2^9 \pmod{23} = 6$	9	23	$3^9 \pmod{23} = 18$
10	23	$2^{10} \pmod{23} = 12$	10	23	$3^{10} \pmod{23} = 8$
1	24	$2^1 \pmod{24} = 2$	1	24	$3^1 \pmod{24} = 3$
2	24	$2^2 \pmod{24} = 4$	2	24	$3^2 \pmod{24} = 9$
3	24	$2^3 \pmod{24} = 8$	3	24	$3^3 \pmod{24} = 3$
4	24	$2^4 \pmod{24} = 16$	4	24	$3^4 \pmod{24} = 9$
5	24	$2^5 \pmod{24} = 8$	5	24	$3^5 \pmod{24} = 3$
6	24	$2^6 \pmod{24} = 16$	6	24	$3^6 \pmod{24} = 9$
7	24	$2^7 \pmod{24} = 8$	7	24	$3^7 \pmod{24} = 3$
8	24	$2^8 \pmod{24} = 16$	8	24	$3^8 \pmod{24} = 9$
9	24	$2^9 \pmod{24} = 8$	9	24	$3^9 \pmod{24} = 3$
10	24	$2^{10} \pmod{24} = 16$	10	24	$3^{10} \pmod{24} = 9$
1	25	$2^1 \pmod{25} = 2$	1	25	$3^1 \pmod{25} = 3$
2	25	$2^2 \pmod{25} = 4$	2	25	$3^2 \pmod{25} = 9$
3	25	$2^3 \pmod{25} = 8$	3	25	$3^3 \pmod{25} = 2$
4	25	$2^4 \pmod{25} = 16$	4	25	$3^4 \pmod{25} = 6$
5	25	$2^5 \pmod{25} = 7$	5	25	$3^5 \pmod{25} = 18$
6	25	$2^6 \pmod{25} = 14$	6	25	$3^6 \pmod{25} = 4$
7	25	$2^7 \pmod{25} = 3$	7	25	$3^7 \pmod{25} = 12$
8	25	$2^8 \pmod{25} = 6$	8	25	$3^8 \pmod{25} = 11$
9	25	$2^9 \pmod{25} = 12$	9	25	$3^9 \pmod{25} = 8$
10	25	$2^{10} \pmod{25} = 24$	10	25	$3^{10} \pmod{25} = 24$
1	26	$2^1 \pmod{26} = 2$	1	26	$3^1 \pmod{26} = 3$
2	26	$2^2 \pmod{26} = 4$	2	26	$3^2 \pmod{26} = 9$
3	26	$2^3 \pmod{26} = 8$	3	26	$3^3 \pmod{26} = 1$
4	26	$2^4 \pmod{26} = 16$	4	26	$3^4 \pmod{26} = 3$
5	26	$2^5 \pmod{26} = 6$	5	26	$3^5 \pmod{26} = 9$
6	26	$2^6 \pmod{26} = 12$	6	26	$3^6 \pmod{26} = 1$
7	26	$2^7 \pmod{26} = 24$	7	26	$3^7 \pmod{26} = 3$
8	26	$2^8 \pmod{26} = 22$	8	26	$3^8 \pmod{26} = 9$
9	26	$2^9 \pmod{26} = 18$	9	26	$3^9 \pmod{26} = 1$
10	26	$2^{10} \pmod{26} = 10$	10	26	$3^{10} \pmod{26} = 3$
1	27	$2^1 \pmod{27} = 2$	1	27	$3^1 \pmod{27} = 3$
2	27	$2^2 \pmod{27} = 4$	2	27	$3^2 \pmod{27} = 9$
3	27	$2^3 \pmod{27} = 8$	3	27	$3^3 \pmod{27} = 0$
4	27	$2^4 \pmod{27} = 16$	4	27	$3^4 \pmod{27} = 0$
5	27	$2^5 \pmod{27} = 5$	5	27	$3^5 \pmod{27} = 0$
6	27	$2^6 \pmod{27} = 10$	6	27	$3^6 \pmod{27} = 0$
7	27	$2^7 \pmod{27} = 20$	7	27	$3^7 \pmod{27} = 0$
8	27	$2^8 \pmod{27} = 13$	8	27	$3^8 \pmod{27} = 0$

9	27	$2^{9} \pmod{27} = 26$	9	27	$3^{9} \pmod{27} = 0$
10	27	$2^{10} \pmod{27} = 25$	10	27	$3^{10} \pmod{27} = 0$
1	28	$2^{1} \pmod{28} = 2$	1	28	$3^{1} \pmod{28} = 3$
2	28	$2^{2} \pmod{28} = 4$	2	28	$3^{2} \pmod{28} = 9$
3	28	$2^{3} \pmod{28} = 8$	3	28	$3^{3} \pmod{28} = 27$
4	28	$2^{4} \pmod{28} = 16$	4	28	$3^{4} \pmod{28} = 25$
5	28	$2^{5} \pmod{28} = 4$	5	28	$3^{5} \pmod{28} = 19$
6	28	$2^{6} \pmod{28} = 8$	6	28	$3^{6} \pmod{28} = 1$
7	28	$2^{7} \pmod{28} = 16$	7	28	$3^{7} \pmod{28} = 3$
8	28	$2^{8} \pmod{28} = 4$	8	28	$3^{8} \pmod{28} = 9$
9	28	$2^{9} \pmod{28} = 8$	9	28	$3^{9} \pmod{28} = 27$
10	28	$2^{10} \pmod{28} = 16$	10	28	$3^{10} \pmod{28} = 25$
1	29	$2^{1} \pmod{29} = 2$	1	29	$3^{1} \pmod{29} = 3$
2	29	$2^{2} \pmod{29} = 4$	2	29	$3^{2} \pmod{29} = 9$
3	29	$2^{3} \pmod{29} = 8$	3	29	$3^{3} \pmod{29} = 27$
4	29	$2^{4} \pmod{29} = 16$	4	29	$3^{4} \pmod{29} = 23$
5	29	$2^{5} \pmod{29} = 3$	5	29	$3^{5} \pmod{29} = 11$
6	29	$2^{6} \pmod{29} = 6$	6	29	$3^{6} \pmod{29} = 4$
7	29	$2^{7} \pmod{29} = 12$	7	29	$3^{7} \pmod{29} = 12$
8	29	$2^{8} \pmod{29} = 24$	8	29	$3^{8} \pmod{29} = 7$
9	29	$2^{9} \pmod{29} = 19$	9	29	$3^{9} \pmod{29} = 21$
10	29	$2^{10} \pmod{29} = 9$	10	29	$3^{10} \pmod{29} = 5$
1	30	$2^{1} \pmod{30} = 2$	1	30	$3^{1} \pmod{30} = 3$
2	30	$2^{2} \pmod{30} = 4$	2	30	$3^{2} \pmod{30} = 9$
3	30	$2^{3} \pmod{30} = 8$	3	30	$3^{3} \pmod{30} = 27$
4	30	$2^{4} \pmod{30} = 16$	4	30	$3^{4} \pmod{30} = 21$
5	30	$2^{5} \pmod{30} = 2$	5	30	$3^{5} \pmod{30} = 3$
6	30	$2^{6} \pmod{30} = 4$	6	30	$3^{6} \pmod{30} = 9$
7	30	$2^{7} \pmod{30} = 8$	7	30	$3^{7} \pmod{30} = 27$
8	30	$2^{8} \pmod{30} = 16$	8	30	$3^{8} \pmod{30} = 21$
9	30	$2^{9} \pmod{30} = 2$	9	30	$3^{9} \pmod{30} = 3$
10	30	$2^{10} \pmod{30} = 4$	10	30	$3^{10} \pmod{30} = 9$
1	31	$2^{1} \pmod{31} = 2$	1	31	$3^{1} \pmod{31} = 3$
2	31	$2^{2} \pmod{31} = 4$	2	31	$3^{2} \pmod{31} = 9$
3	31	$2^{3} \pmod{31} = 8$	3	31	$3^{3} \pmod{31} = 27$
4	31	$2^{4} \pmod{31} = 16$	4	31	$3^{4} \pmod{31} = 19$
5	31	$2^{5} \pmod{31} = 1$	5	31	$3^{5} \pmod{31} = 26$
6	31	$2^{6} \pmod{31} = 2$	6	31	$3^{6} \pmod{31} = 16$
7	31	$2^{7} \pmod{31} = 4$	7	31	$3^{7} \pmod{31} = 17$
8	31	$2^{8} \pmod{31} = 8$	8	31	$3^{8} \pmod{31} = 20$
9	31	$2^{9} \pmod{31} = 16$	9	31	$3^{9} \pmod{31} = 29$
10	31	$2^{10} \pmod{31} = 1$	10	31	$3^{10} \pmod{31} = 25$

1	32	$2^{1} \pmod{32} = 2$	1	32	$3^{1} \pmod{32} = 3$
2	32	$2^{2} \pmod{32} = 4$	2	32	$3^{2} \pmod{32} = 9$
3	32	$2^{3} \pmod{32} = 8$	3	32	$3^{3} \pmod{32} = 27$
4	32	$2^{4} \pmod{32} = 16$	4	32	$3^{4} \pmod{32} = 17$
5	32	$2^{5} \pmod{32} = 0$	5	32	$3^{5} \pmod{32} = 19$
6	32	$2^{6} \pmod{32} = 0$	6	32	$3^{6} \pmod{32} = 25$
7	32	$2^{7} \pmod{32} = 0$	7	32	$3^{7} \pmod{32} = 11$
8	32	$2^{8} \pmod{32} = 0$	8	32	$3^{8} \pmod{32} = 1$
9	32	$2^{9} \pmod{32} = 0$	9	32	$3^{9} \pmod{32} = 3$
10	32	$2^{10} \pmod{32} = 0$	10	32	$3^{10} \pmod{32} = 9$
1	33	$2^{1} \pmod{33} = 2$	1	33	$3^{1} \pmod{33} = 3$
2	33	$2^{2} \pmod{33} = 4$	2	33	$3^{2} \pmod{33} = 9$
3	33	$2^{3} \pmod{33} = 8$	3	33	$3^{3} \pmod{33} = 27$
4	33	$2^{4} \pmod{33} = 16$	4	33	$3^{4} \pmod{33} = 15$
5	33	$2^{5} \pmod{33} = 32$	5	33	$3^{5} \pmod{33} = 12$
6	33	$2^{6} \pmod{33} = 31$	6	33	$3^{6} \pmod{33} = 3$
7	33	$2^{7} \pmod{33} = 29$	7	33	$3^{7} \pmod{33} = 9$
8	33	$2^{8} \pmod{33} = 25$	8	33	$3^{8} \pmod{33} = 27$
9	33	$2^{9} \pmod{33} = 17$	9	33	$3^{9} \pmod{33} = 15$
10	33	$2^{10} \pmod{33} = 1$	10	33	$3^{10} \pmod{33} = 12$
1	34	$2^{1} \pmod{34} = 2$	1	34	$3^{1} \pmod{34} = 3$
2	34	$2^{2} \pmod{34} = 4$	2	34	$3^{2} \pmod{34} = 9$
3	34	$2^{3} \pmod{34} = 8$	3	34	$3^{3} \pmod{34} = 27$
4	34	$2^{4} \pmod{34} = 16$	4	34	$3^{4} \pmod{34} = 13$
5	34	$2^{5} \pmod{34} = 32$	5	34	$3^{5} \pmod{34} = 5$
6	34	$2^{6} \pmod{34} = 30$	6	34	$3^{6} \pmod{34} = 15$
7	34	$2^{7} \pmod{34} = 26$	7	34	$3^{7} \pmod{34} = 11$
8	34	$2^{8} \pmod{34} = 18$	8	34	$3^{8} \pmod{34} = 33$
9	34	$2^{9} \pmod{34} = 2$	9	34	$3^{9} \pmod{34} = 31$
10	34	$2^{10} \pmod{34} = 4$	10	34	$3^{10} \pmod{34} = 25$
1	35	$2^{1} \pmod{35} = 2$	1	35	$3^{1} \pmod{35} = 3$
2	35	$2^{2} \pmod{35} = 4$	2	35	$3^{2} \pmod{35} = 9$
3	35	$2^{3} \pmod{35} = 8$	3	35	$3^{3} \pmod{35} = 27$
4	35	$2^{4} \pmod{35} = 16$	4	35	$3^{4} \pmod{35} = 11$
5	35	$2^{5} \pmod{35} = 32$	5	35	$3^{5} \pmod{35} = 33$
6	35	$2^{6} \pmod{35} = 29$	6	35	$3^{6} \pmod{35} = 29$
7	35	$2^{7} \pmod{35} = 23$	7	35	$3^{7} \pmod{35} = 17$
8	35	$2^{8} \pmod{35} = 11$	8	35	$3^{8} \pmod{35} = 16$
9	35	$2^{9} \pmod{35} = 22$	9	35	$3^{9} \pmod{35} = 13$
10	35	$2^{10} \pmod{35} = 9$	10	35	$3^{10} \pmod{35} = 4$
1	36	$2^{1} \pmod{36} = 2$	1	36	$3^{1} \pmod{36} = 3$
2	36	$2^{2} \pmod{36} = 4$	2	36	$3^{2} \pmod{36} = 9$

3	36	$2^3 \pmod{36} = 8$	3	36	$3^3 \pmod{36} = 27$
4	36	$2^4 \pmod{36} = 16$	4	36	$3^4 \pmod{36} = 9$
5	36	$2^5 \pmod{36} = 32$	5	36	$3^5 \pmod{36} = 27$
6	36	$2^6 \pmod{36} = 28$	6	36	$3^6 \pmod{36} = 9$
7	36	$2^7 \pmod{36} = 20$	7	36	$3^7 \pmod{36} = 27$
8	36	$2^8 \pmod{36} = 4$	8	36	$3^8 \pmod{36} = 9$
9	36	$2^9 \pmod{36} = 8$	9	36	$3^9 \pmod{36} = 27$
10	36	$2^{10} \pmod{36} = 16$	10	36	$3^{10} \pmod{36} = 9$

5 Public Key Cryptography

Let's decrypt

Theorem 5.1. *If p and q are distinct prime numbers and W is a natural number with $(W, pq) = 1$, then $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.*

Proof. Let p and q be distinct primes. Then $\phi(p) = p - 1$ and $\phi(q) = q - 1$. Let $W \in \mathbb{N}$ with $(W, pq) = 1$. Then by Euler's Theorem, $W^{\phi(p)} \equiv 1 \pmod{p}$ and $W^{\phi(q)} \equiv 1 \pmod{q} \Rightarrow W^{\phi(p)\phi(q)} \equiv 1 \pmod{p}$ and $W^{\phi(p)\phi(q)} \equiv 1 \pmod{q}$. Since p and q being distinct prime implies that $(p, q) = 1$, we can use Theorem 4.21 to obtain $W^{\phi(p)\phi(q)} \equiv 1 \pmod{pq} \Rightarrow W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$, as desired.

□

As an interesting note, prior knowledge from group theory tells us that $\phi(n)$ is the order of the group of integers modulo n (under multiplication) $\mathbb{Z}/n\mathbb{Z}$, and since the groups $\mathbb{Z}/(mn)\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic if $(m, n) = 1$, we get that $\phi(mn) = \phi(m)\phi(n)\ \forall m, n \in \mathbb{Z}$ with $(m, n) = 1$. While the case where n and m are primes was relatively straightforward to prove, this general multiplicative property of Euler's ϕ-function is much harder to prove directly (and also not required here).

Theorem 5.2. *Let p and q be distinct primes, k be a natural number, and W be a natural number less than pq. Then*

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}$$

Proof. Let p, q be distinct primes, and $k \in \mathbb{N}$. Let $W \in \mathbb{N}$ with $W < pq$. Then $(W, pq) = 1$ or $(W, pq) \neq 1$. If $(W, pq) \neq 1$, then by the Fundamental Theorem of Arithmetic, $p|W$ or $q|W$.

Suppose that $(W, pq) = 1$. Then by Theorem 5.1, $W^{(p-1)(q-1)} \equiv 1 \pmod{pq} \Rightarrow W^{(p-1)(q-1)k} \equiv 1 \pmod{pq} \Rightarrow W^{(p-1)(q-1)k}W \equiv W \pmod{pq} \Rightarrow W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}$.

Now suppose that $p|W$ or $q|W$. Without loss of generality, say $p|W$. Then $\exists n \in \mathbb{N}$ such that $W = pn$. Since $W < pq$, it must be the case that $n \neq q$ from which we can conclude that $(n, q) = 1$ since q is prime. Since we also have that $(p, q) = 1$, we have that $(pn, q) = 1 \Rightarrow (W, q) = 1$. By Euler's Theorem, $W^{\phi(q)} \equiv 1 \pmod{q} \Rightarrow W^{(q-1)} \equiv 1 \pmod{q} \Rightarrow W^{k(p-1)(q-1)} \equiv 1 \pmod{q} \Rightarrow W^{1+k(p-1)(q-1)} \equiv W \pmod{q}$. Now, since $p|(W - 0)$, we have that $W \equiv 0 \pmod{p} \Rightarrow W^{1+k(p-1)(q-1)} \equiv 0 \pmod{p}$. Using the transitive property of the congruence relation with $W \equiv 0 \pmod{p}$, we have that $W^{1+k(p-1)(q-1)} \equiv W \pmod{p}$. Since $(p, q) = 1$, we can now use Theorem 4.21 to conclude that $W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}$. □

Theorem 5.3. *Let p and q be distinct primes and E be a natural number relatively prime to $(p-1)(q-1)$. Then there exist natural numbers D and y such that*

$$ED = 1 + y(p-1)(q-1)$$

Proof. Let p, q be distinct primes, and $E \in \mathbb{N}$ with $(E, (p-1)(q-1)) = 1$. For convenience, define $r := (p-1)(q-1)$. Consider the linear Diophantine equation $Ex = 1 + yr$. Since $(E, r) = 1$, by Theorem 1.38, $\exists x_0, y_0 \in \mathbb{Z}$ such that $Ex_0 = 1 + y_0 r$. By Theorem 1.53, every other solution to the linear Diophantine equation (after making the appropriate substitutions for y_0 being on the right-hand side of the equation) is given by $x = x_0 + \frac{kr}{(E,r)}$ and $y = y_0 + \frac{kE}{(E,r)}$ for some $k \in \mathbb{Z}$. Recalling that $(E, r) = 1$, this simplifies to $x = x_0 + kr$ and $y = y_0 + kE$. Substituting into the linear Diophantine equation gives

$$E(x_0 + kr) \quad = \quad 1 + (y_0 + kE)r$$

If $x_0, y_0 > 0$, then we are done since we would have natural number solutions. Otherwise, since $E, r \in \mathbb{N}$, they satisfy $E, r > 0$. Hence, $\exists k \in \mathbb{N}$ large enough such that $x_0 + kr > 0$ and $y_0 + kE > 0$. By letting k' be the smallest such k that accomplishes this, we then have $D := x_0 + k'r \in \mathbb{N}$ and $y := y_0 + k'E \in \mathbb{N}$ that satisfy the desired equation. □

Theorem 5.4. *Let p and q be distinct primes, W be a natural number less than pq, and E, D, and y be natural numbers such that $ED = 1 + y(p-1)(q-1)$. Then*

$$W^{ED} \equiv W \pmod{pq}$$

Proof. Let p, q be distinct primes, and $W \in \mathbb{N}$ with $W < pq$. Let $E, D, y \in \mathbb{N}$ such that $ED = 1 + y(p-1)(q-1)$. Then it follows immediately from Theorem 5.2 that $W^{1+y(p-1)(q-1)} \equiv W \pmod{pq} \Rightarrow W^{ED} \equiv W \pmod{pq}$. □

Exercise 5.5. *Consider two distinct prime p and q. Describe every step of the RSA Public Key Coding System. State what numbers you choose to make public, what messages can be encoded, how messages should be encoded, and how messages are decoded. What number should be called the encoding exponent and what number should be called the decoding exponent?*

Consider the primes $p = 5$ and $q = 11$. We need to choose a natural number E that's relatively prime to $(5-1)(11-1) = 40$, say $E = 9$. We then need to find the natural number D such that $ED = 1 + y(p-1)(q-1)$ for some $y \in \mathbb{N}$. For this, we use the division algorithm:

$$\begin{aligned} 40 &= 9(4) + 4 \\ 9 &= 4(2) + 1 \\ \Rightarrow 9 &= 2(40 - 9(4)) + 1 \\ \Rightarrow 9(9) &= 1 + 2(5-1)(11-1) \end{aligned}$$

Hence, $D = 9$. We would then make $E = 9$ and $pq = 55$ public, and call E the "encoding exponent". Note that we would *not* make the factored form of pq public, only the overall product (though in this case it's easy to guess the factored form). The number D would remain secret, and is called the "decoding exponent". Ideally, we would prefer $E \neq D$ over the case that we have here. Any message, W, that's coming in would need to be smaller than $pq = 55$, so in the real world we'd want to pick very large primes to ensure that this is not a problem. Now, if the sender wants to send us a secret message, say $W = 2$, then they would encode their message by computing $W^E \pmod{pq}$, which in this case is $2^9 \pmod{55} = 17$. Letting $N = W^E \pmod{pq}$ represent the encoded message, on our end, we would recover the original message by computing $N^D \pmod{pq}$. We can use a computer to verify that $17^9 \pmod{55} = 2$, which is the original W!

Here is a step by step summary:

1. Pick two distinct primes p and q.

2. Pick some $E \in \mathbb{N}$ that's relatively prime to $(p-1)(q-1)$.

3. Find $D \in \mathbb{N}$ such that $ED = 1 + y(p-1)(q-1)$ for some $y \in \mathbb{N}$.

4. Make E (the encoding exponent) and the overall product of pq public.

5. The user encodes their message W by computing $W^E \pmod{pq}$. The user will have to know to pick $W < pq$.

6. Raise the encoded message by D (the decoding exponent) and mod it by pq. This will recover W.

Exercise 5.6. *Describe an RSA Public Key Code System based on the primes 11 and 17. Encode and decode several messages.*

Letting $p = 11$ and $q = 17$, we have that $(p-1)(q-1) = (10)(16) = 160$. Choose $E = 9$, which is relatively prime to $160 = 2^5 \cdot 5$. We now proceed with the division algorithm to find D:

$$\begin{aligned}
160 &= 9(17) + 7 \\
9 &= 7(1) + 2 \\
7 &= 2(3) + 1 \\
\Rightarrow 7 &= 3(9-7) + 1 \\
7(4) &= 3(9) + 1 \\
\Rightarrow (160 - 9(17))(4) &= 3(9) + 1 \\
9(-71) &= 1 + (-4)(160)
\end{aligned}$$

Since $(9, 160) = 1$, recall from Theorem 1.53 that every other solution to the linear Diophantine equation $9x = 1 + y160$ is given by $x = -71 + 160k$ and $y = -4 + 9k$ for some

$k \in \mathbb{Z}$. In this case, choose $k = 1$ to obtain

$$9(89) \quad = \quad 1 + 5(160) = 1 + 5(11-1)(17-1)$$

Hence, $D = 89$.

Now, we make $E = 9$ and $pq = (11)(17) = 187$ public. To encode a message $W \in \mathbb{N}$ with $W < 187$, the sender should compute $W^9 \pmod{187}$. We keep $D = 89$ secret, and decode an encrypted message by raising the message to 89 and computing the result modulo 187.

Here are some example messages.

Message (W)	Encoded ($N := W^E \pmod{pq}$)	Decoded ($N^D \pmod{pq}$)
1	1	1
2	138	2
5	97	5
17	68	17
56	12	56
100	100	100

Exercise 5.7. *You are a secret agent. An evil spy with shallow number theory skills uses the RSA Public Key Coding System in which the public modulus is $n = 1537$, and the encoding exponent is $E = 47$. You intercept one of the encoded secret messages being sent to the evil spy, namely the number 570. Using your superior number theory skills, decode this message, thereby saving countless people from the fiendish plot of the evil spy.*

We have that $pq = 1537$, $E = 47$, and $N := W^{47} \pmod{1537} = 570$. We begin by factoring $pq = 1537$. After some trial and error, we find that $1537 = (29)(53)$. Hence, $(p-1)(q-1) = (28)(52) = 1456$. We now need to find $D, y \in \mathbb{N}$ such that $47D = 1 + y1456$. Proceeding with the Division Algorithm:

$$\begin{aligned}
1456 &= 47(30) + 46 \\
47 &= 46(1) + 1 \\
\Rightarrow 47 &= (1456 - 47(30)) + 1 \\
47(31) &= 1 + 1(1456)
\end{aligned}$$

Hence, $D = 31$. We can now decode the message by computing $570^{31} \pmod{1537}$, which from the assistance of a computer comes out to be 131.

Exercise 5.8. *Suppose an RSA Public Key Coding System publishes n (which is equal to the product of two undisclosed primes p and q) and E, with E relatively prime to $(p-1)(q-1)$. Suppose someone wants to send a secret message and so encodes the message number W (less than n) by finding the number m less than n such that $m \equiv W^E \pmod{n}$. Suppose you intercept this number m and you are able to factor n. How can you figure out the original message W?*

If the RSA system is used, factoring n should yield exactly two prime factors. Arbitrarily assign one of these to be p and the other q. We can figure out the original messages W by following these steps:

1. Compute $r := (p-1)(q-1)$.

2. Consider the linear Diophantine equation $Ex = 1 + yr$. Use the Division Algorithm to find solutions x_0 and y_0.

3. Since $(E, r) = 1$, we have from Theorem 1.53 (after making the appropriate substitutions) that all other solutions to the above linear Diophantine equation are given by $x = x_0 + rk$ and $y = y_0 + Ek$ for some $k \in \mathbb{Z}$. Deduce the appropriate k that gives both $x, y \in \mathbb{N}$. The resulting x will be equal to D.

4. Compute $m^D \pmod{pq}$. The result will be the original message W.

Applications Exercise 5.9. *You have seen the application of number theory to RSA cryptography. Find out all you can about the role of number theory in some other types of "codes" such as bar codes, ISBN codes, and credit card number "codes".*

Number Theory is mainly used in bar codes, ISBN codes, and credit card number codes to perform what's called a digit check. A digit check is a redundancy check that uses some algorithm on the input to retrieve a digit that must be consistent with a particular digit in the input in order for the input to be considered valid. This is particularly useful when the input is sometimes expected to be entered manually, as it will be very difficult for a human to guess an input that will pass the consistency (digit) check. For example, bar codes code for a universal product code (UPC) that points to a particular product that the customer is purchasing. UPC's are 12 digits long, with the very last digit acting as the "check digit". If we let $a_1 a_2 \ldots a_{12}$ denote the string of digits for a UPC number, then the digit check is done by checking if

$$a_{12} = 10 - \left[\left(3 \sum_{\substack{i=1 \\ i \text{ odd}}}^{11} a_i + \sum_{\substack{i=2 \\ i \text{ even}}}^{10} a_i \right) \pmod{10} \right] \pmod{10}$$

if either any of the digits are different, the digit check will fail and the computer will reject the UPC input immediately. The only way to "fool" the system is by entering almost entirely different digits and getting lucky, or by pre-emptively computing $a_1 2$. Sources:

1. http://mathworld.wolfram.com/ISBN.html
2. http://mathworld.wolfram.com/UPC.html

6 Polynomial Congruences and Primitive Roots

Lagrange's Theorem

Theorem 6.1. *Let $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$ with integer coefficients and assume $a_n \neq 0$. Then an integer r is a root of $f(x)$ if and only if there exists a polynomial $g(x)$ of degree $n-1$ with integer coefficients such that $f(x) = (x-r)g(x)$.*

Proof. Let Let $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$ with $a_i \in \mathbb{Z}\ \forall 0 \leq i \leq n$ and $a_n \neq 0$.

($\Rightarrow$) Suppose that $r \in \mathbb{Z}$ is a root of $f(x)$. Then $f(r) = 0 \Rightarrow a_nr^n + a_{n-1}r^{n-1} + \cdots + a_0$. We claim that $x - r$ divides $f(x)$. Observe,

$$\begin{aligned}
\frac{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0}{x-r} &= a_nx^{n-1} + \frac{(a_{n-1} + a_nr)x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0}{x-r} \\
&= a_nx^{n-1} + (a_{n-1} + a_nr)x^{n-2} + \frac{(a_{n-2} + a_{n-1}r + a_nr^2)x^{n-2} + \cdots + a_0}{x-r} \\
&\vdots \\
&= a_nx^{n-1} + (a_{n-1} + a_nr)x^{n-2} + \cdots + (a_1 + a_2r + \ldots a_nr^{n-1}) + \\
&\quad + \frac{a_0 + a_1r + a_2r^2 + \cdots + a_nr^n}{x-r}
\end{aligned}$$

and since $f(r) = 0$, we have,

$$\frac{f(x)}{x-r} = a_nx^{n-1} + (a_{n-1} + a_nr)x^{n-2} + \cdots + (a_1 + a_2r + \ldots a_nr^{n-1})$$

If we let $g(x)$ to be equal to the right hand side of the above equation, we get

$$f(x) = (x-r)g(x)$$

as desired. Notice that $g(x)$ must have degree $n-1$, as otherwise it contradicts the fact that $f(x)$ is of degree n. Moreover, since all the coefficients used to construct g are sums of integers, g also has integer coefficients, so we are done this direction.

($\Leftarrow$) Conversely, suppose $\exists$ a polynomial $g(x)$ of degree $n-1$ with integer coefficients such that $f(x) = (x-r)g(x)$. Then $f(r) = (r-r)g(r) = 0$, so r is a root of f by definition.

□

Theorem 6.2. *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$ with integer coefficients and $a_n \neq 0$. Let p be a prime number and r an integer. Then, if $f(r) \equiv 0 \pmod{p}$, there exists a polynomial $g(x)$ of degree $n-1$ such that*

$$(x-r)g(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + b_0$$

where $a_0 \equiv b_0 \pmod{p}$.

Proof. Let Let $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree $n > 0$ with $a_i \in \mathbb{Z}\ \forall 0 \leq i \leq n$ and $a_n \neq 0$. Let p be a prime, and $r \in \mathbb{Z}$. Suppose that $f(r) \equiv 0 \pmod{p}$. Then $\exists k \in \mathbb{Z}$ such that $f(r) = pk$. Define $h(x) = f(x) - pk$. Then $h(r) = f(r) - pk = pk - pk = 0$, so r is a root of h. Hence, by Theorem 6.1 $\exists$ a polynomial $g(x)$ of degree $n-1$ such that $h(x) = (x-r)g(x) \Rightarrow (x-r)g(x) = f(x) - pk = a_nx^n + a_{n-1}x^{n-1} + \cdots + (a_0 - pk)$. Hence, if we let $b_0 = a_0 - pk$, then $(x-r)g(x) = f(x) - pk = a_nx^n + a_{n-1}x^{n-1} + \cdots + b_0$ and $b_0 = a_0 - pk \Rightarrow p|(a_0 - b_0) \Rightarrow a_0 \equiv b_0 \pmod{p}$.

Note: Since $0 \equiv a_0 - b_0 \pmod{p}$, we can conclude that $f(x) \equiv (x-r)g(x) \pmod{p}$. □

Theorem 6.3. (Lagrange's Theorem). *If p is a prime and $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with integer coefficients and $a_n \neq 0$, then $f(x) \equiv 0 \pmod{p}$ has at most n non-congruent solutions modulo p.*

Proof. Let p be a prime and $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with $a_i \in \mathbb{Z}\ \forall 0 \leq i \leq n$ and $a_n \neq 0$. By way of contradiction, suppose that $f(x) \equiv 0 \pmod{p}$ has more than n non-congruent solutions modulo p. Let $r_1, r_2, \ldots, r_{n+1}$ be any $n+1$ of these non-congruent solutions. By Theorem 6.2, there exist a polynomial of degree $n-1$ such that

$$(x - r_1)g_1(x) \equiv f(x) \pmod{p}$$

Moreover, since $f(r_i) \equiv 0 \pmod{p}\ \forall 1 \leq i \leq n+1$, we have that $(r_i - r_1)g_1(r_i) \equiv 0 \pmod{p} \Rightarrow (r_i - r_1)g_1(r_i) + pk = 0$ for some $k \in \mathbb{Z}$. The left hand side of this equation is a polynomial of degree $n-1$, and we have n different roots of that polynomial, which contradicts the Fundamental Theorem of Algebra. Hence, $f(x) \equiv 0 \pmod{p}$ has at most n non-congruent solutions modulo p. □

Primitive roots

Theorem 6.4. *Suppose p is a prime and* $\text{ord}_p(a) = d$. *Then for each natural number i with $(i,d) = 1$,* $\text{ord}_p(a^i) = d$.

Proof. Let p be a prime, and $\text{ord}_p(a) = d$. Let $i \in \mathbb{N}$ with $(i,d) = 1$. Let $d' = \text{ord}_p(a^i)$. We need to show that $d' = d$. Since $a^d \equiv 1 \pmod{p}$, we immediately have that $(a^d)^i \equiv 1 \pmod{p} \Rightarrow (a^i)^d \equiv 1 \pmod{p}$ so that $d'|d$ by Theorem 4.10. Moreover, since $\left(a^i\right)^{d'} \equiv 1 \pmod{p} \Rightarrow a^{id'} \equiv 1 \pmod{p}$, we also have that $d|id'$ (by Theorem 4.10). Since, $(i,d) = 1$ we can conclude by Theorem 1.41 that $d|d'$. Hence, $d'|d$ and $d|d' \Rightarrow d = d'$ so that $\text{ord}_p(a^i) = d$. □

Theorem 6.5. *For a prime p and natural number d, at most $\phi(d)$ incongruent integers modulo p have order d modulo p.*

Proof. Let p be a prime and $d \in \mathbb{N}$. Consider the congruence $x^d \equiv 1 \pmod{p}$ where d is the order of x. Since $\{0, 1, 2, \ldots, p-1\}$ forms a complete residue system modulo p, it is sufficient to consider solutions $x \in \mathbb{Z}$ for which $x \in \{0, 1, 2, \ldots, p-1\}$ when looking for incongruent solutions. Then $(x, p) = 1$ since p is prime, so $\text{ord}_p(x) = d | p-1$ by Theorem 4.18. Hence, $\exists k \in \mathbb{N}$ such that $dk = p - 1$. Now, by Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$ for any choice of x. If we let $g(x) := 1 + x^d + x^{2d} + x^{3d} + \cdots + x^{d(k-1)}$, observe that we have $(x^d - 1)g(x) = x^{dk} - 1 = x^{p-1} - 1$. Since Fermat's Little Theorem tells us that every integer in the canonical complete residue system modulo p satisfies $x^p - 1 \equiv 0 \pmod{p}$, we have that $(x^d - 1)g(x) \equiv 0 \pmod{p}$ also has exactly $p - 1 = dk$ solutions, which must come from $x^d - 1$ or $g(x)$ (by Theorem 6.1). By Lagrange's Theorem, $x^d - 1 \equiv 0 \pmod{p}$ has at most d non-congruent solutions, and $g(x) \equiv 0 \pmod{p}$ has at most $d(k-1)$ solutions. Since $d + d(k-1) = dk = p - 1$, it follows that $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions. Of these d solutions, □

Theorem 6.6. *Let p be a prime and suppose g is a primitive root modulo p. Then the set $\{0, g, g^2, g^3, \ldots, g^{p-1}\}$ forms a complete residue system modulo p.*

Proof. Let p be a prime, and g a primitive root modulo p. Let $G := \{0, g, g^2, g^3, \ldots, g^{p-1}\}$. Since G contains p members, it is sufficient to show that they are all pairwise incongruent modulo p to prove that G is a complete residue system modulo p. It is clear that for any $g^i \in G \setminus \{0\}$, we have that $g^i \not\equiv 0 \pmod{p}$ since otherwise we can multiply by g^{p-1-i} to obtain $1 \equiv 0 \pmod{p}$, a contradiction. Now let $1 \leq i < j \leq p-1$. By way of contradiction, suppose that $g^i \equiv g^j \pmod{p}$. Then $(g^i)(g^{p-1-j}) \equiv (g^j)(g^{p-1-j}) \pmod{p} \Rightarrow g^{(p-1)-(j-i)} \equiv 1 \pmod{p}$. Since $j - i > 0$, we have that $(p-1) - (j-i) < p - 1$, which contradicts the fact that g is a primitive root modulo p. Hence, the elements of G are pairwise incongruent modulo p so that we have a complete residue system modulo p. □

Exercise 6.7. *For each of the primes p less than 20, find a primitive root and make a chart showing what powers of the primitive root give each of the natural numbers less than p.*

Consider the following table:

p	g	$g^1, g^2, \ldots, g^{p-1} \pmod{p}$
2	1	1
3	2	$2, 1$
5	2	$2, 4, 3, 1$
7	3	$3, 2, 6, 4, 5, 1$
11	2	$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$
13	2	$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$
17	3	$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$
19	2	$2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1$

Theorem 6.8. *Every prime p has a primitive root.*

Exercise 6.9. *Consider the prime $p = 13$. For each divisor $d = 1, 2, 3, 4, 6, 12$ of $12 = p-1$, mark which of the natural numbers in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ have order d.*

We know from Theorem 6.5 that at most $\phi(d)$ numbers have order d, so we can stop looking for numbers that have the order of a given divisor once we reach this number. Now, let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

For $d = 1$, we only have $1 \in S$ with this order 1. We now have $S = \{\cancel{1}, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

For $d = 2$, only 12 has order d. Now, $S = \{\cancel{1}, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \cancel{12}\}$.

For $d = 3$, the numbers 3 and 9 have order d. Hence, $S = \{\cancel{1}, 2, \cancel{3}, 4, 5, 6, 7, 8, \cancel{9}, 10, 11, \cancel{12}\}$.

5 and 8 have order $d = 4$, so now $S = \{\cancel{1}, 2, \cancel{3}, 4, \cancel{5}, 6, 7, \cancel{8}, \cancel{9}, 10, 11, \cancel{12}\}$.

4 and 10 have order $d = 6$, so $S = \{\cancel{1}, 2, \cancel{3}, \cancel{4}, \cancel{5}, 6, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\}$.

Finally, we see that $2, 6, 7$, and 11 have order $p - 1 = 12$.

Euler's ϕ-function and sums of divisors

Exercise 6.10. *Compute each of the following sums.*

1. $\displaystyle\sum_{d|6} \phi(d)$

$$\sum_{d|6} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$$

2. $\displaystyle\sum_{d|10} \phi(d)$

$$\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$$

3. $\displaystyle\sum_{d|24} \phi(d)$

$$\begin{aligned}\sum_{d|24} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + +\phi(8) + \phi(12) + \phi(24) \\ &= 1 + 1 + 2 + 2 + 2 + 4 + 4 + 8 \\ &= 24\end{aligned}$$

4. $\sum_{d|36} \phi(d)$

$$\begin{aligned}\sum_{d|36} \phi(d) &= \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(9)+\phi(12)+\phi(18)+\phi(36)\\ &= 1+1+2+2+2+6+4+6+12\\ &= 36\end{aligned}$$

5. $\sum_{d|27} \phi(d)$

$$\begin{aligned}\sum_{d|27} \phi(d) &= \phi(1)+\phi(3)+\phi(9)+\phi(27)\\ &= 1+2+6+18\\ &= 27\end{aligned}$$

Based on the results above, my "sweeping conjecture" is that $\sum_{d|n} \phi(d) = n$ *for all* $n \in \mathbb{N}$.

Lemma 6.11. *If* p *is a prime, then*

$$\sum_{d|p} \phi(d) = p$$

Proof. Let p be a prime. Then the only divisors of p are 1 and p. Since $\phi(1) = 1$ and $\phi(p) = p - 1$ for any prime, we have that $\sum_{d|p} \phi(d) = \phi(1) + \phi(p) = 1 + (p - 1) = p$, as desired. □

Lemma 6.12. *If* p *is a prime, then*

$$\sum_{d|p^k} \phi(d) = p^k$$

Proof. Let p be a prime. We prove the Lemma by induction. For the base case, it is clear that $\sum_{d|p^1} \phi(d) = p^1$ by Lemma 6.11. For the induction step, suppose that $\sum_{d|p^k} \phi(d) = p^k$ for some $k \in \mathbb{N}$. Since the prime factorization of p^{k+1} is clearly shown to contain only factors of p, we have that the divisors of p^{k+1} are $\{1, p, p^2, \ldots, p^{k+1}\}$. Then,

$$\begin{aligned}\sum_{d|p^{k+1}} \phi(d) &= \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^{k+1})\\ &= \sum_{d|p^k} \phi(d) + \phi(p^{k+1})\\ &= p^k + \phi(p^{k+1})\end{aligned}$$

To evaluate $\phi(p^{k+1})$, notice that there are p^{k+1} numbers less than or equal to p^{k+1}, and the only numbers that are not relatively prime to p^{k+1} are the ones that have a factor of p in them. Since there are exactly p^k choices for a number x less than or equal to p^{k+1} such that $xp \leq p^{k+1}$, there are p^k number less than or equal to p^{k+1} that are *not* relatively prime to p^{k+1}. Hence, $\phi(p^{k+1}) = p^{k+1} - p^k$. Finally, we have that

$$\begin{aligned} \sum_{d|p^{k+1}} \phi(d) &= p^k + \phi(p^{k+1}) \\ &= p^k + (p^{k+1} - p^k) \\ &= p^{k+1} \end{aligned}$$

Hence, by the principle of mathematical induction, the Lemma is proved for any $k \in \mathbb{N}$. □

Lemma 6.13. *If p and q are two different primes, then*

$$\sum_{d|pq} \phi(d) = pq$$

Proof. Let p and q be two different primes. Since the prime factorization of pq is immediate, we know that the only divisors of pq are $1, p, q$, and pq. Hence,

$$\begin{aligned} \sum_{d|pq} \phi(d) &= \phi(1) + \phi(p) + \phi(q) + \phi(pq) \\ &= 1 + (p-1) + (q-1) + \phi(pq) \end{aligned}$$

In order to evaluate $\phi(pq)$, we will to count the number of $n \in \mathbb{N}$ with $n \leq pq$ such that $\gcd(n, pq) \neq 1$. Define $P := \{p, 2p, 3p, \ldots, qp\}$ and $Q := \{q, 2q, 3q, \ldots, pq\}$. The sets P and Q each give elements (not equal to 1) that divide pq. Since any element, say a, that divides pq and isn't equal to 1 must (by prime factorization), contain a factor of p or q, it must satisfy $a \in P$ or $a \in Q$. We claim that $a \in P$ and $a \in Q$ if and only if $a = pq$. Indeed, if $a = pq$, then clearly $a \in P$ and $a \in Q$. Conversely, if $a \in P$ and $a \in Q$, then $a = npq$ for some $n \in \mathbb{N}$. The only way that a can satisfy $a \leq pq$ is if $npq \leq pq \Rightarrow n = 1$ so that $a = pq$. Hence, $P \cap Q = \{pq\}$. In summary, we have that $P \cup Q$ gives all the elements that divide pq, and $|P \cup Q| = |P| + |Q| - |P \cap Q| = q + p - 1$. Hence, the number of relatively prime elements less than or equal to pq is $\phi(pq) = pq - (q + p - 1) = (p-1)(q-1)$. Finally,

$$\begin{aligned} \sum_{d|pq} \phi(d) &= 1 + (p-1) + (q-1) + (p-1)(q-1) \\ &= p + q - 1 + (pq - p - q + 1) \\ &= pq \end{aligned}$$

as desired. □

Lemma 6.14. *If n and m are relatively prime natural numbers, then*

$$\left(\sum_{d|m}\phi(d)\right)\cdot\left(\sum_{d|n}\phi(d)\right)=\sum_{d|mn}\phi(d)$$

Proof. Let $m,n\in\mathbb{N}$ with $(m,n)=1$. Define $\mathcal{D}_m=\{a_1,a_2,\ldots,a_r\}$ and $\mathcal{D}_n=\{b_1,b_2,\ldots,b_s\}$ to be the sets of all divisors of, respectively, m and n. Then,

$$\begin{aligned}\left(\sum_{d|m}\phi(d)\right)\cdot\left(\sum_{d|n}\phi(d)\right) &= (\phi(a_1)+\phi(a_2)+\cdots+\phi(a_r))(\phi(b_1)+\phi(b_2)+\cdots+\phi(b_s))\\ &= \sum_{i=1}^{r}\sum_{j=1}^{s}\phi(a_i)\phi(b_j)\\ &= \sum_{i=1}^{r}\sum_{j=1}^{s}\phi(a_ib_j)\text{ (by Theorem 6.23 and since }(m,n)=1)\end{aligned}$$

and since $\{a_ib_j\mid 1\le i\le r, 1\le j\le s\}$ gives all the divisors of mn, it follows that the last line above is equal to $\sum_{d|mn}\phi(d)$. Thus,

$$\left(\sum_{d|m}\phi(d)\right)\cdot\left(\sum_{d|n}\phi(d)\right)=\sum_{d|mn}\phi(d)$$

as desired. □

Theorem 6.15. *If n is a natural number, then*

$$\sum_{d|n}\phi(d)=n$$

Proof. Let $n\in\mathbb{N}$. Then by the Fundamental Theorem of Arithmetic, we can prime factorize n as $n=p_1^{r_1}p_2^{r_2}\ldots p_m^{r_m}$ where $p_i\neq p_j$ $\forall i\neq j$. Hence, we have $(p_i^{r_i},p_j^{r_j})=1$ $\forall i\neq j$. Thus, through repeated application of Lemma 6.14 we have

$$\sum_{d|n}\phi(d)=\left(\sum_{d|p_1^{r_1}}\phi(d)\right)\left(\sum_{d|p_2^{r_2}}\phi(d)\right)\cdots\left(\sum_{d|p_m^{r_m}}\phi(d)\right)$$

We can now apply Lemma 6.12 to get

$$\sum_{d|n}\phi(d)=(p_1^{r_1})(p_2^{r_2})\ldots(p_m^{r_m})=n$$

as desired. □

Exercise 6.16. *For a natural number n consider the fractions*

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}$$

all written in reduced form. For example, with $n = 10$ we would have

$$\frac{1}{10}, \frac{1}{5}, \frac{3}{10}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{7}{10}, \frac{4}{5}, \frac{9}{10}, \frac{1}{1}$$

Try to find a natural one-to-one correspondence between the reduced fractions and the numbers $\phi(d)$ for $d|n$. Show how that observation provides a very clever proof to the preceding theorem.

Notice that $d|n$ if and only if $\frac{d}{n}$ can be reduced. This means that the numbers that appear in the denominators are all the possible divisors of n. Moreover, the number of times a given divisor d appears in the denominator is exactly equal to $\phi(d)$. Since all the divisors appear together in exactly n times, the previous theorem follows immediately.

Theorem 6.17. *Every prime p has $\phi(p-1)$ primitive roots.*

Proof. Let p be a prime. We claim that exactly $\phi(p-1)$ of the integers in $G := \{1, 2, \ldots, p-1\}$ are primitive roots modulo p. Firstly, we note that each of the $g \in G$ has an order d that satisfies $d|(p-1)$ by Theorem 4.18. Moreover, Theorem 6.5 tells us that there are at most $\phi(d)$ integers in G that have order d. Since Theorem 6.15 tells us that $\phi(p-1) = \sum_{d|\phi(p-1)} \phi(d)$, we actually see that at least $\phi(p-1)$ integers must have order $p-1$. Since only at most $\phi(p-1)$ integers can have order $p-1$, however, it follows that there are exactly $\phi(p-1)$ with order $p-1$. That is, p has $\phi(p-1)$ primitive roots. □

Euler's ϕ-function is multiplicative

Exercise 6.18. *Make a conjecture about the value of $\phi(p)$ for a prime p. Prove your conjecture.*

Conjecture: $\forall$ primes p, $\phi(p) = p - 1$.

Proof. Since p is prime, every element less than p - by definition - does not divide p, and since there are $p-1$ numbers less than p, it follows that $\phi(p) = p - 1$. □

Exercise 6.19. *Make a conjecture about the value of $\phi(p^k)$ for a prime p and natural numbers k. Prove your conjecture.*

Conjecture: $\forall$ primes p and $k \in \mathbb{N}$, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Proof. See Lemma 6.12. □

Theorem 6.20. *If n is a natural number and A is a complete residue system modulo n, then the number of numbers in A that are relatively prime to n is equal to $\phi(n)$.*

Proof. Let $n \in \mathbb{N}$ and A be a complete residue system modulo n. Suppose $A = \{a_1, a_2, \ldots, a_n\}$. Then $A = \{1 + k_1 n, 2 + k_2 n, \ldots, n + k_n n\}$ for some $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ since each element must be congruent to some element in the canonical complete residue system modulo n. Then $\forall 1 \leq i \leq n$, $\exists 1 \leq j \leq n$ such that $a_i = j + k_j n$. This implies that $(j, n) = 1$ if and only if $(a_j, n) = 1$. Hence, there are exactly the same number of elements in A that are relatively prime to n as there are in the canonical complete residue system modulo n. It follows that there are $\phi(n)$ numbers in A that are relatively prime to n. □

Theorem 6.21. *If n is a natural number, k is an integer, and m is an integer relatively prime to n, then the set of n integers*

$$\{k, k + m, k + 2m, k + 3m, \ldots, k + (n - 1)m\}$$

is a complete residue system modulo n.

Proof. Let $n \in \mathbb{N}$ and $k \in \mathbb{Z}$. Let $m \in \mathbb{Z}$ with $(m, n) = 1$. Suppose by way of contradiction that $k + im \equiv k + jm \pmod{n}$ for some $0 \leq i < j \leq (n - 1)$. Then $im \equiv jm \pmod{n}$, and since $(m, n) = 1$, we can divide through by m so that $i \equiv j \pmod{n}$, which is a contradiction since i and j are supposed to be different elements of the complete residue system $\{0, 1, 2, \ldots, n - 1\}$. Hence, the elements of S are pairwise incongruent modulo n, and since there are n of them, it follows that S is a complete residue system modulo n. □

Exercise 6.22. *Consider the relatively prime natural numbers 9 and 4. Write down all the natural numbers less than or equal to $36 = 9 \cdot 4$ in a rectangular array that is 9 wide and 4 high. Then circle those numbers in that array that are relatively prime to 36. Try some other examples using relatively prime natural numbers.*

Here is the given example with $36 = 4 \cdot 9$:

$$\begin{array}{ccccccccc}
\textcircled{1} & 2 & 3 & 4 & \textcircled{5} & 6 & \textcircled{7} & 8 & 9 \\
10 & \textcircled{11} & 12 & \textcircled{13} & 14 & 15 & 16 & \textcircled{17} & 18 \\
\textcircled{19} & 20 & 21 & 22 & \textcircled{23} & 24 & \textcircled{25} & 26 & 27 \\
28 & \textcircled{29} & 30 & \textcircled{31} & 32 & 33 & 34 & \textcircled{35} & 36
\end{array}$$

Let's try this with $15 = 3 \cdot 5$:

$$\begin{array}{ccccc}
\textcircled{1} & \textcircled{2} & 3 & \textcircled{4} & 5 \\
6 & \textcircled{7} & \textcircled{8} & 9 & 10 \\
\textcircled{11} & 12 & \textcircled{13} & \textcircled{14} & 15
\end{array}$$

Let's examine the first case (of $36 = 4 \cdot 9$). Notice that for any $x = ab$, an integer y is relatively prime to x if and only if it is relatively prime to a and relatively prime to b (the Fundamental Theorem of Arithmetic makes this apparent). Since each column forms a complete residue system modulo 4 (by Theorem 6.21 and the fact that $(4, 9(= 1)$, it must (by Theorem 6.20) have $\phi(4)$ elements that are relatively prime to 4. Moreover, each row forms a complete residue system modulo 9, so it must have $\phi(9)$ elements that are relatively prime to 9. Hence, the number of elements that are both relatively prime to 4 and 9, and thus relatively prime to 36, is $\phi(4)\phi(9) = 2 \cdot 6 = 12$.

Theorem 6.23. *If n and m are relatively prime natural numbers, then*

$$\phi(mn) = \phi(m)\phi(n)$$

Proof. Let $n, m \in \mathbb{N}$ with $(n, m) = 1$. We can write out the mn numbers in an array that is m wide and n high like so:

$$\begin{array}{cccc} 1 & 2 & \ldots & m \\ 1+m & 2+m & \ldots & m+(1)m \\ \vdots & \vdots & \ddots & \vdots \\ 1+(n-1)m & 2+(n-1)m & \ldots & m+(n-1)m \end{array}$$

notice that the elements in each column form a set of the form $\{k, k+m, k+2m, \ldots, k+(n-1)m\}$ for some $k \in \mathbb{N}$ with $1 \leq k \leq m$. Hence, since we also have that $(m, n) = 1$, by Theorem 6.21 each column forms a complete residue system modulo n. By Theorem 6.20, this means that each column has $\phi(n)$ elements that are relatively prime to n. Moreover, each row is clearly a complete residue system modulo m, and has (by Theorem 6.20) $\phi(m)$ elements that are relatively prime to m. Since $\forall x, y \in \mathbb{N}$ with $x = ab$ for some $a, b \in \mathbb{N}$, $(x, y) = 1$ if and only if $(y, a) = 1$ and $(y, b) = 1$ (follows from the Fundamental Theorem if Arithmetic), a number is relatively prime to m if and only if it is relatively prime to m *and* relatively prime to n. Since we can select $\phi(m)$ elements from each row that are relatively prime to m, and $\phi(n)$ columns where these numbers are also relatively prime to n, we have that there are $\phi(m)\phi(n)$ numbers that are relatively prime to mn. That is, $\phi(mn) = \phi(m)\phi(n)$. □

Exercise 6.24. *Compute each of the following.*

1. $\phi(3)$

$$\phi(3) = (3-1) = 2$$

2. $\phi(5)$

$$\phi(5) = (5-1) = 4$$

3. $\phi(15)$

$$\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 8$$

4. $\phi(45)$

$$\phi(45) = \phi(3^2)\phi(5) = 3(3-1)(5-1) = 24$$

5. $\phi(98)$

$$\phi(98) = \phi(2)\phi(7^2) = (2-1)7(7-1) = 42$$

6. $\phi(5^6 11^4 17^{10})$

$$\phi(5^6 11^4 17^{10}) = 5^5(5-1)11^3(11-1)17^9(17-1) = (5^5 11^3 17^9)640$$

Question 6.25. *To what power would you raise 15 to be certain that you would get an answer that is congruent to 1 modulo 98? Why?*

Answer. First notice that since $15 = 3 \cdot 5$ and $98 = 2 \cdot 7^2$, $(15, 98) = 1$. Hence, by Euler's Theorem $15^{\phi(98)} \equiv 1 \pmod{98}$. Hence, we just need to compute $\phi(98)$. From Exercise 6.24 5, $\phi(98) = 42$. Thus, I would raise 15 to the 42nd power to be certain that I have a number congruent to 1 modulo 98.

Question 6.26. *How many primitive roots does the prime 251 have?*

Answer. By Theorem 6.17, 251 has $\phi(251-1)$ primitive roots. Observe,

$$\phi(250) = \phi(2 \cdot 5^3) = \phi(2)\phi(5^3) = (2-1)5^2(5-1) = 100$$

Hence, 251 has 100 primitive roots.

Roots modulo a number

Exercise 6.27. *Try, using paper and pencil, to solve several congruences of the form* $x^k \equiv b \pmod{5}$ *and* $x^k \equiv b \pmod{6}$*.*

When $k = 1$, solutions are trivial. Here are some other cases.

$$x^4 \equiv 1 \pmod{5}$$

By Euler's Theorem, any number relatively prime to 5 is a solution. In general, $x = 1$ will always be a solutions when $b = 1$. Let us now consider

$$x^4 \equiv 5 \pmod{5}$$

Then any multiple of 5 is a solution. In general, when b is a multiple of n, any multiple of $x = an$ will also be a solution.

$$x^4 \equiv 4 \pmod{5}$$

The above congruence doesn't appear to have any solutions.

We now consider congruences mod 6.

$$x^2 \equiv 1 \pmod 6$$

By Euler's Theorem, any number relatively prime to 6 is a solution.

$$x^2 \equiv 2 \pmod 6$$

This congruence doesn't appear to have solutions.

$$x^2 \equiv 3 \pmod 6$$

This appears to have solutions $x = 3, 9, 15, 21, \ldots$.

Exercise 6.28. *Compute* $a^9 \pmod 5$ *for several choices of* a*. Can you explain what happens? Now compute* $a^{17} \pmod{15}$ *for several choices of* a*. Does your previous explanation apply here too?*

Here is are a couple tables summarizing the results:

a	$a^9 \pmod 5$
0	0
1	1
2	2
3	3
4	4

In general, if an a is a multiple of 5, then $a^9 \pmod 5$ is clearly 0. Otherwise, that a is relatively prime to 5 and we can use Euler's Theorem to get $a^{\phi(5)} \equiv 1 \pmod 5 \Rightarrow a^4 \equiv 1 \pmod 5 \Rightarrow a^9 \equiv a \pmod 5$. Notice that for the next table, however, 15 is not prime, so there are many numbers for which this may not hold.

a	$a^9 \pmod{15}$
0	0
1	1
2	2
3	3
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14

Interestingly enough, the same result holds, even though our explanation isn't valid anymore.

Theorem 6.29. *If a is an integer and v and n are natural numbers such that $(a, n) = 1$, then $a^{v\phi(n)+1} \equiv a \pmod{n}$.*

Proof. Let $a \in \mathbb{Z}$, and let $v, n \in \mathbb{N}$ with $(a, n) = 1$. Then by Euler's Theorem, $a^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow {a^{\phi(n)}}^{v} \equiv 1^{v} \pmod{n} \Rightarrow a^{v\phi(n)} \equiv 1 \pmod{n} \Rightarrow a^{v\phi(n)} \cdot a \equiv 1 \cdot a \pmod{n} \Rightarrow a^{v\phi(n)+1} \equiv a \pmod{n}$ □

Question 6.30. *Consider the congruence $x^5 \equiv 2 \pmod{7}$. Can you think of an appropriate operation we can apply to both sides of the congruence that would allow us to "solve" for x? If so, is the value obtained for x a solution to the original congruence?*

Answer. In light of Theorem 6.29, we want to exponentiate the congruence such that the exponent of 5 becomes something of the form $v\phi(7) + 1 \Rightarrow 6v + 1 = 5k$. Notice that since 5 and 6 are relatively prime, such a solutions should indeed exist. By inspection, $v = 4$ and $k = 5$ gives us the desired solution. Hence, $x^{4\phi(7)+1} \equiv 2^5 \pmod{7} \Rightarrow x \equiv 2^5 \pmod{7} \Rightarrow x \equiv 4 \pmod{7}$. Substituting this into the original congruence shows that this is indeed a solution.

Question 6.31. *Consider the congruence $x^3 \equiv 7 \pmod{10}$. Can you think of an appropriate operation we can apply to both sides of the congruence that would allow us to "solve" for x? If so, is the value obtained for x a solution to the original congruence?*

Answer. We want to find $u, v \in \mathbb{N}$ such that $v\phi(10) + 1 = 3u$. By inspection, $v = 2$ and $u = 3$ satisfy this (note that $\phi(10) = 4$). Hence, $x^{2\phi(10)+1} \equiv 7^3 \pmod{10} \Rightarrow x \equiv 3 \pmod{10}$. This indeed is a solution to the original congruence.

Theorem 6.32. *If k and n are natural numbers with $(k, \phi(n)) = 1$, then there exist positive integers u and v satisfying $ku = \phi(n)v + 1$.*

Proof. Let $k, n \in \mathbb{N}$ with $(k, \phi(n)) = 1$. Then by Theorem 1.38, $\exists u_0, v_0 \in \mathbb{Z}$ such that $ku_0 = \phi(n)v_0 + 1$. Theorem 1.53 gives all other solutions to the linear Diophantine equation $ku = \phi(n)v_0 + 1$ (after making the appropriate substitutions for $\phi(n)$ being on the right hand side) as $u = u_0 + \frac{r\phi(n)}{(k,\phi(n))}$ and $v = v_0 + \frac{rk}{(k,\phi(n)}$ for some $r \in \mathbb{Z}$. Since $(k, \phi(n)) = 1$, this simplifies to $u = u_0 + r\phi(n)$ and $v = v_0 + rk$. Since both k and $\phi(n)$ are greater than zero, it follows that $\exists r \in \mathbb{N}$ big enough such that $u > 0$ and $v > 0$. If we let r' be the smallest such natural number that accomplishes this, then $u = u_0 + r'\phi(n)$ and $v = v_0 + r'k$ are natural numbers that give the desired result. □

Exercise 6.33. *Use your observations so far to find solutions to the following congruences. Be sure to check that your answers are indeed solutions.*

1. $x^7 \equiv 4 \pmod{11}$

Noting that $\phi(11) = 10$, *we need to solve the linear Diophantine equation* $7u = 10v+1$. *By inspection,* $u = 3$ *and* $v = 2$ *satisfy this. Hence,* $x^{2\phi(11)+1} \equiv 4^3 \pmod{11} \Rightarrow x \equiv 9 \pmod{11}$.

2. $x^5 \equiv 11 \pmod{18}$

$\phi(18) = \phi(2)\phi(3^2) = 6$. $5u = 6v + 1$ *has a solution* $v = 4$ *and* $u = 5$. *Hence,* $x^{4\phi(18)+1} \equiv 11^5 \pmod{18} \Rightarrow x \equiv 5 \pmod{18}$.

3. $x^7 \equiv 2 \pmod 8$

$\phi(8) = 4$. $7u = 4v+1$ *has a solution* $v = 5$ *and* $u = 3$. *Hence,* $x^{5\phi(8)+1} \equiv 2^3 \pmod 8 \Rightarrow x \equiv 0 \pmod 8$. *This, however, is not a solution to the original congruence.*

Question 6.34. *What hypothesis on* k, b, *and* n *do you think are necessary for your method to produce a solution to the congruence* $x^k \equiv b \pmod n$*? Make a conjecture and prove it.*

Answer. In order for the linear Diophantine equation $ku = v\phi(n) + 1$ to have a solution, $(k, \phi(n)) = 1$ is necessary. Once we have this, we can apply Theorem 6.29 to get $x \equiv b^u \pmod n$. As suggested by the third example in Exercise 6.33, it is likely sufficient to have $(b, n) = 1$ in order to have a solution. Indeed, observe that $b^{ku} \equiv b \pmod n \Rightarrow b^{v\phi(n)+1} \equiv b \pmod n$ is true by Theorem 6.29 under the hypothesis that $(b, n) = 1$.

Theorem 6.35. *If* b *is an integer and* k *and* n *are natural numbers such that* $(k, \phi(n)) = 1$ *and* $(b, n) = 1$, *then* $x^k \equiv b \pmod n$ *has a unique solution modulo* n. *Moreover, that solution is given by*

$$x \equiv b^u \pmod n$$

where u *and* v *are positive integers such that* $ku = \phi(n)v + 1$.

Proof. Let $b \in \mathbb{Z}$ and $k, n \in \mathbb{N}$ such that $(k, \phi(n)) = 1$ and $(b, n) = 1$. Then by Theorem 6.32, $\exists u, v \in \mathbb{Z}$ with $u, v > 0$ such that $ku = \phi(n)v + 1$. Raising the congruence $x^k \equiv b \pmod n$ to the uth power gives $x^{ku} \equiv b^u \pmod n \Rightarrow x^{v\phi(n)+1} \equiv b^u \pmod n$, and by Theorem 6.29, $x^{v\phi(n)+1} \equiv x \pmod n$ so that $x \equiv b^u \pmod n$. To confirm that this is indeed a solution, we raise this to the kth power and see that $x^k \equiv b^{ku} \pmod n \equiv b^{v\phi(n)+1} \pmod n$, and since $(b, n) = 1$, we have by Theorem 6.29 again that $x^k \equiv b \pmod n$.

For uniqueness, suppose that $x \equiv s \pmod n$ is also a solution to $x^k \equiv b \pmod n$ where $s \neq r$ and s is an element of the canonical complete residue system modulo n. Then $s^k \equiv b \pmod n \Rightarrow s^{uk} \equiv b^u \pmod n \Rightarrow s \equiv b^u \pmod n$. Hence, the solution is uniquely given by $x \equiv b^u \pmod n$. □

Exercise 6.36. *Find the 49th root of 100 modulo 151.*

We need to solve the congruence $x^{49} \equiv 100 \pmod{151}$. Notice that 151 is prime, so $\phi(151) = 150$. Since $(49, 150) = 1$ and $(100, 151) = 1$, $\exists$ a unique solution by Theorem 6.35. Noting that $\phi(151) = 150$, we need to solve the linear Diophantine equation $49u = 150v + 1$. Using the Division Algorithm,

$$\begin{aligned} 150 &= 49(3) + 3 \\ 49 &= 3(16) + 1 \\ \Rightarrow 49 &= 16(150 - 3(49)) + 1 \\ 49(49) &= 150(16) + 1 \end{aligned}$$

Hence, by Theorem 6.35 we have the solution $x \equiv 100^{49} \pmod{151}$. This simplifies to $x \equiv 103 \pmod{151}$. Hence, the 49th root of 100 modulo 151 is 103.

Theorem 6.37. *If a is an integer, v is a natural number, and n is a product of distinct primes, then $a^{v\phi(n)+1} \equiv a \pmod{n}$.*

Proof. Let $a \in \mathbb{Z}$ and $v \in \mathbb{N}$ Suppose that $n = p_1 p_2 \dots p_k \in \mathbb{N}$ is a product of distinct primes (that is, $p_i \neq p_j \ \forall i \neq j$). Either $(a, n) = 1$ or $(a, n) \neq 1$.

If $(a, n) = 1$, then this is just Theorem 6.29 and it follows that $a^{v\phi(n)+1} \equiv a \pmod{n}$.

If $(a, n) \neq 1$, let $d = (a, n)$ and $e := \frac{n}{d} \in \mathbb{N}$. Then d and e must be the product of distinct primes to that $(a, e) = 1, (n, e) = 1$, and $(d, e) = 1$. Then by Euler's Theorem, $a^{\phi(e)} \equiv 1 \pmod{e} \Rightarrow a^{v\phi(e)\phi(d)+1} \equiv a \pmod{e}$, and since Euler's ϕ-function is multiplicative, we have that $\phi(e)\phi(d) = \phi(ed) = \phi(n)$, and hence $a^{v\phi(n)+1} \equiv a \pmod{e}$. Now, since $d|a$, we have $a \equiv 0 \pmod{d} \Rightarrow a^{v\phi(n)+1} \equiv 0 \pmod{d}$, and we can use the transitive property of congruence modulo d to conclude $a^{v\phi(n)+1} \equiv a \pmod{d}$. Finally, by Theorem 4.21 (and the fact that $(e, d) = 1$) we have $a^{v\phi(n)+1} \equiv a \pmod{de} \Rightarrow a^{v\phi(n)+1} \equiv a \pmod{n}$, as desired. □

Theorem 6.38. *If n is a natural number that is a product of distinct primes, and k is a natural number such that $(k, \phi(n)) = 1$, then $x^k \equiv b \pmod{n}$ has a unique solution modulo n for any integer b. Moreover, that solution is given by*

$$x \equiv b^u \pmod{n}$$

where u and v are positive integers such that $ku - \phi(n)v = 1$.

Proof. Let $n \in \mathbb{N}$ with $n = p_1 p_2 \dots p_k$ and $p_i \neq p_j \ \forall i \neq j$. Let $k \in \mathbb{N}$ with $(k, \phi(n)) = 1$. Consider the congruence $x^k \equiv b \pmod{n}$ for some $b \in \mathbb{Z}$.

We first show the existence of a solution and its form. Since $(k, \phi(n)) = 1$, (by Theorem 6.32) $\exists u, v \in \mathbb{N}$ such that $ku = v\phi(n) + 1$. Raising the given congruence to the uth power yields $x^{ku} \equiv b^u \pmod{n} \Rightarrow x^{v\phi(n)+1} \equiv b^u \pmod{n}$, and by Theorem 6.37 and the fact that n is a product of distinct primes, $x^{v\phi(n)+1} \equiv x \pmod{n}$ so that $x \equiv b^u \pmod{n}$. To confirm that this is indeed a solution, observe that we can use Theorem 6.37 again to conclude that $b^{uk} \equiv b^{v\phi(n)+1} \pmod{n} \equiv b \pmod{n}$.

For uniqueness, suppose that $x \equiv s \pmod{n}$ is also a solution to the congruence. Then $x^k \equiv s^k \pmod{n} \equiv b \pmod{n} \Rightarrow s^{uk} \equiv b^u \pmod{n}$, and again by Theorem 6.37, $s^{uk} \equiv s^{v\phi(n)+1} \pmod{n} \equiv s \pmod{n}$ so that $s \equiv b^u \pmod{n}$. Hence, the solution is uniquely given by $x \equiv b^u \pmod{n}$. □

Exercise 6.39. *Find the 37th root of 100 modulo 210.*

We need to solve the congruence $x^{37} \equiv 100 \pmod{210}$. Since $210 = 2 \cdot 3 \cdot 5 \cdot 7$ is a product of distinct primes, the conditions of Theorem 6.38 are met. Note that $\phi(210) = (2-1)(3-1)(5-1)(7-1) = 48$. We now need to solve the linear Diophantine equation $37u = 48v + 1$ (which has a solution since $(37, 48) = 1$). Using the Division Algorithm,

$$\begin{aligned}
48 &= 37(1) + 11\\
37 &= 11(3) + 4\\
11 &= 4(2) + 3\\
4 &= 3(1) + 1\\
\Rightarrow 4 &= (11 - 4(2)) + 1\\
4(3) &= 11 + 1\\
\Rightarrow 3(37 - 11(3)) &= 11 + 1\\
37(3) &= 11(10) + 1\\
\Rightarrow 37(3) &= 10(48 - 37) + 1\\
37(13) &= 48(10) + 1
\end{aligned}$$

Hence, $x \equiv 100^{13} \pmod{210}$ is the solution. This simplifies to $x \equiv 100 \pmod{210}$. Hence, 100 is the 37th root of 100 modulo 210.

Theorem 6.40. *Let p be a prime, b an integer, and k a natural number. Then the number of kth roots of b modulo p is either 0 or $(k, p-1)$.*

Proof. Omitted. □

7 The Golden Rule: Quadratic Reciprocity

Quadratic Residues

Theorem 7.1. *Let p be a prime and let $a, b,$ and c be integers with a not divisible by p. Then there are integers b' and c' such that that set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to the set of solutions to a congruence of the form $x^2 + b'x + c' \equiv 0 \pmod{p}$.*

Proof. Let p be prime, and $a, b, c \in \mathbb{Z}$ with $p \nmid a$. Then since p is prime, it must be the case that $(p, a) = 1$. Hence, $\exists a' \in \{1, 2, \ldots, p-1\}$ such that $a' \cdot a = 1$. Then if we define $b' := a'b$ and $c' := a'c$, we have that $ax^2 + bx + c \equiv 0 \pmod{p} \iff (aa')x^2 + (a'b)x + (a'c) \equiv 0 \pmod{p} \iff x^2 + b'x + c' \equiv 0 \pmod{p}$, as desired. □

Theorem 7.2. *Let p be a prime, and let b and c be integers. Then there exists a linear change of variable, $y = x + \alpha$ with α an integer, transforming the congruence $x^2 + bx + c \equiv 0 \pmod{p}$ into a congruence of the form $y^2 \equiv \beta \pmod{p}$ for some integer β.*

Proof. Let p be a prime, and $b, c \in \mathbb{Z}$. Consider the congruent $x^2 + bx + c \equiv 0 \pmod{p}$. Observe that

$$\begin{aligned} x^2 + bx + c &= (x^2 + bx + \frac{b^2}{4}x) + c - \frac{b^2}{4} \\ &= (x^2 + \frac{b}{2})^2 + (c - \frac{b^2}{4}) \\ &= \left(\frac{1}{4}\right)\left((2x+b)^2 - (b^2 - 4c)\right) \end{aligned}$$

Thus, $x^2 + bx + c \equiv 0 \pmod{p} \iff (x + b/2)^2 + c - b^2/4) \equiv 0 \pmod{p}$ so that if we let $y = x + b/2$ and $\beta = b^2 - 4c$ then we have $y^2 \equiv \beta \pmod{p}$. □

Theorem 7.3. *Let p be an odd prime. Then half the numbers not congruent to 0 in any complete residue system modulo p are perfect squares modulo p and half are not.*

Proof. Let p be an odd prime. Then by Theorem 6.8, $\exists g \in \{1, 2, \ldots, p-1\}$ such that g is a primitive root modulo p. Moreover, by Theorem 6.6, $G := \{0, g, g^2, g^3, \ldots, g^{p-1}\}$ forms a complete residue system modulo p. We are interested in the numbers not congruent to zero, and hence the set $G^\times = \{g, g^2, g^3, \ldots, g^{p-1}\}$. Notice that since p is odd, $p-1$ is even. Hence, half the numbers $1, 2, \ldots, p-1$ are even and half of them are odd. It follows immediately that half the numbers are perfect squares modulo p, and half are not. □

Exercise 7.4. *Determine which of the numbers $1, 2, 3, \ldots, 12$ are perfect squares modulo 13. For each such perfect square, list the number or numbers in the set whose square is that number.*

We first need to find a primitive root modulo 13. Observe that $g = 2$ is one such primitive root, and $G^\times = \{g, g^2, \dots, g^{p-1}\} = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$. Every second number in $G^\times$ will be a perfect square (that is, $\{1, 3, 4, 9, 10, 12\}$). The following table summarizes which numbers will square to that perfect square:

$g \in \{1, 2, \dots, 12\}$	$g^2 \pmod{13}$
1	1
2	4
3	9
4	3
5	12
6	10
7	8
8	12
9	3
10	9
11	4
12	1

Question 7.5. *Can you characterize perfect squares modulo a prime p in terms of their representation as a power of a primitive root?*

Answer. Let p be an odd prime, and $g \in \{1, 2, \dots, p-1\}$ be a primitive root modulo p. Then as we saw in the proof of Theorem 7.3, a perfect square n can be written as $n = \left(g^i\right)^2$ for some $i \in \{1, 2, \dots, \frac{p-1}{2}\}$.

Theorem 7.6. *Let p be a prime. Then half the numbers not congruent to 0 modulo p in any complete residue system modulo p are quadratic residues modulo p and half are quadratic non-residues modulo p.*

Proof. With the definition that a perfect square modulo p is called a quadratic residue, this is just Theorem 7.3. □

Theorem 7.7. *Suppose p is an odd prime and p does not divide either of the two integers a or b. Then*

1. *If a and b are both quadratic residues modulo p, then ab is a quadratic residue modulo p;*

2. *If a is a quadratic residue modulo p and b is a quadratic non-residue modulo p, then ab is a quadratic non-residue modulo p;*

3. *If a and b are both quadratic non-residues modulo p, then ab is a quadratic residue modulo p.*

Proof. Let p be an odd prime, and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$.

1. Suppose that both a and b are quadratic residues modulo p. Then $\exists c, d \in \mathbb{Z}$ such that $a \equiv c^2 \pmod{p}$ and $b \equiv d^2 \pmod{p}$. Multiplying these two congruences gives $ab \equiv (cd)^2 \pmod{p}$, and since $(cd) \in \mathbb{Z}$, ab is a quadratic residue modulo p by definition.

2. Suppose that a is a quadratic residue modulo p. Without loss of generality, suppose that $b \neq 0$ (as we will eventually be interested in values of b that are quadratic non-residues). If b were a quadratic residue modulo p, then we would have ab be a quadratic residue modulo p by 1. Since such values for b are exactly half of the available choices, and we produce half of the available outputs, it follows from Theorem 7.6 that the other half of the options available to us must produce quadratic non-residues. That is, if b is a quadratic non-residue, then ab is a quadratic non-residue.

3. Suppose that a is a quadratic non-residue modulo p. Similar to 2, if b were a quadratic residue, then ab would be a quadratic non-residue by 2. Since half of the available non-zero options for b are quadratic residues, which results in half of the available non-zero outputs being quadratic non-residues, it follows that the remaining values of b will produce quadratic residues by Theorem 7.6. That is, if b is a quadratic non-residue, then ab is a quadratic residue.

□

Theorem 7.8. *Suppose p is an odd prime and p does not divide either a or b. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof. This is just Theorem 7.7 with the understanding that $\forall a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$ if and only if a is a quadratic residue modulo p, and $\left(\frac{a}{p}\right) = -1$ if and only if a is a quadratic non-residue modulo p. □

Theorem 7.9. (Euler's Criterion). *Suppose p is an odd prime and p does not divide the natural number a. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$; and a is a quadratic non-residue modulo p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$. This criterion can be abbreviated using the Legendre symbol:*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Proof. Let p be an odd prime, and $a \in \mathbb{Z}$ with $p \nmid a$.

($\Rightarrow$) Suppose that a is a quadratic residue modulo p. Then $\exists b \in \mathbb{Z}$ such that $a \equiv b^2 \pmod{p}$. Moreover, since $p \nmid a$, we must have that $p \nmid b$ as otherwise we would have $a \equiv 0 \pmod{p}$, which contradicts $p \nmid a$. Since $p \nmid b$ and p is prime, we have $(p, b) = 1$ so that by Fermat's Little Theorem $b^{p-1} \equiv 1 \pmod{p} \Rightarrow (b^2)^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p} \Rightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$.

($\Leftarrow$) Conversely, suppose that $a^{(p-1)/2} \equiv 1 \pmod{p}$. Since p is prime, $\exists g \in \{1, 2, \ldots, p-1\}$ such that g is a primitive root (by Theorem 6.8). Moreover, Theorem 6.6 implies that $a \equiv g^k \pmod{p}$ for some $k \in \mathbb{Z}$. Hence, $g^{k(p-1)/2} \equiv 1 \pmod{p}$, and since g has order $p-1$, by Theorem 4.10 $p-1 | k \cdot \frac{p-1}{2} \Rightarrow (p-1)c = k\frac{p-1}{2}$ for some $c \in \mathbb{Z}$, and hence $k = 2c$ so that k is even. Hence, g^k is a quadratic residue modulo p, and since $a \equiv g^k \pmod{p}$, it follows that a is a quadratic residue modulo p.

We've now shown that a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

To show that a is a quadratic non-residue modulo p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$, it is sufficient to show that $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$ (since the contrapositive of the statement we just proved is a is a quadratic non-residue modulo p if and only if $a^{(p-1)/2} \not\equiv 1 \pmod{p}$).
To this end, observe that by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Which implies that $a^{(p-1)/2}$ is an inverse of itself. By Theorem 4.38, this happens if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$. It not follows that $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$, and hence a is a quadratic non-residue modulo p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Summarizing these results using the Legendre symbol yields:

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

□

Theorem 7.10. *Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only if p is of the form $4k+1$ for some integer k. Or, equivalently*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

Proof. Let p be an odd prime. Then $p = 2r+1$ for some $r \in \mathbb{N}$.

($\Rightarrow$) Suppose that -1 is a quadratic residue modulo p. We need to show that $2|r$. By Euler's Criterion, $(-1)^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow (-1)^r \equiv 1 \pmod{p}$, and since the order of (-1) modulo p is always 2 for any $p > 2$ (which we have since p is odd), it follows from Theorem 4.10 that $2|r$ so that $r = 2k$ for some $k \in \mathbb{N}$. It now follows that $p = 4k+1$.

($\Leftarrow$) Suppose that $p = 4k+1$ for some $k \in \mathbb{N}$. By Fermat's Little Theorem, $(-1)^{p-1} \equiv 1 \pmod{p} \Rightarrow (-1)^{2k} \equiv 1 \pmod{p}$, and since $\frac{p-1}{2} = \frac{(4k+1)-1}{2} = 2k$, it follows from Euler's criterion that -1 is a quadratic residue modulo p.

We now have that $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod 4$. Notice that in order for p to be odd, if $p \not\equiv 1 \pmod 4$, then the only other available option is $p \equiv 3 \pmod 4$. Hence, $\left(\frac{-1}{p}\right) = -1$ if and $p \equiv 3 \pmod 4$. Putting these together gives

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

as desired.

□

Theorem 7.11. *Let k be a natural number and $p = 4k + 1$ be a prime congruent to 1 modulo 4. Then*

$$(\pm(2k)!)^2 \equiv -1 \pmod p$$

Proof. Let $k \in \mathbb{N}$, and $p = 4k + 1$ be a prime. We know from Theorem 7.10 that -1 is a quadratic residue modulo Then by Wilson's Theorem, $(p-1)! \equiv -1 \pmod p \Rightarrow -1 \equiv 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \dots \cdot (p-1) \pmod p$. Notice that $\frac{p+1}{2} \equiv (-1) \cdot \frac{p-1}{2} \pmod p$, $\frac{p+2}{2} \equiv (-1) \cdot \frac{p-2}{2} \pmod p$, ..., $p-1 \equiv (-1) \cdot 1 \pmod p$ so that $\frac{p+1}{2} \cdot \frac{p+2}{2} \cdot \dots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{(p-1)/2} \pmod p \equiv \left(\frac{p-1}{2}\right)!$ since $(p-1)/2 = 2k$ is even. Hence, $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p$ so that $(\pm(2k)!)^2 \equiv -1 \pmod p$, as desired. □

Theorem 7.12. (Infinitude of $4k + 1$ Prime Theorem). *There are infinitely many primes congruent to 1 modulo 4.*

Proof. By way of contradiction, suppose that there were finitely many primes of the form $4k + 1$, say $p_1, p_2, \dots, p_r$. Define $N := (2p_1p_2 \dots p_r)^2 + 1 \in \mathbb{N}$. Then N is a number of the form $4k + 1$. First notice that each

By the Fundamental Theorem of Arithmetic, N has a unique prime factorization. Let q be some prime factor of N. Notice that $-1 = (2p_1p_2 \dots p_r)^2 - qk$ where $k := \frac{N}{q} \in \mathbb{Z}$. Hence, $-1 \equiv (2p_1p_2 \dots p_r)^2 \pmod q$ so that -1 is a quadratic residue modulo q, which happens if and only if q is a prime of the form $4k + 1$ (by Theorem 7.10). q cannot be any one of the $p_1, p_2, \dots, p_r$, however, as otherwise $N = (2p_1p_2 \dots p_r)^2 + 1$ would imply that $q|1$, which contradicts q being prime. Hence, we have found another prime q of the form $4k+1$, which contradicts the fact that $p_1, p_2, \dots, p_r$ were all such primes. It follows that there are infinitely many primes of the form $4k + 1$. □

Gauss' Lemma and quadratic reciprocity

Lemma 7.13. *Let p be a prime, a an integer not divisible by p, and $r_1, r_2, \dots, r_{\frac{(p-1)}{2}}$ the representatives of $a, 2a, \dots, \frac{p-1}{2}a$ in the complete residue system*

$$\left\{ -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-2}{2} \right\}$$

Then

$$r_1 \cdot r_2 \cdot \dots \cdot r_{\frac{(p-1)}{2}} = (-1)^g \left(\frac{p-1}{2}\right)!$$

where g is the number of r_i's which are negative.

Proof. Let p be a prime, and $a \in \mathbb{Z}$ with $p \nmid a$. Then $(p, a) = 1$. Let $r_1, r_2, \dots, r_{\frac{(p-1)}{2}}$ the representatives of $a, 2a, \dots, \frac{p-1}{2}a$ in the complete residue system

$$\Big\{ -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-2}{2} \Big\}$$

Following the hint, we note that we want to show that it is never the case that $r_i \equiv -r_j \pmod{p}$ for some $i, j \in \{1, 2, \dots, \frac{p-1}{2}\}$ since we can then conclude that $|r_i| \neq |r_j|$ for all i and j. Since there are $\frac{p-1}{2}$ choices of r_i and $\frac{p-1}{2}$ total options for distinct magnitudes that r_i can have, it follows that $|r_1 r_2 \dots r_{\frac{p-1}{2}}| = \left(\frac{p-1}{2}\right)!$. To get rid of the absolute value sign, we just let g be the number of r_i's that are negative, from which it follows that $r_1 \cdot r_2 \cdot \dots \cdot r_{\frac{(p-1)}{2}} = (-1)^g \left(\frac{p-1}{2}\right)!$.

Now, suppose by way of contradiction that we had $r_i \equiv -r_j \pmod{p}$ for some $i, j \in \{1, 2, \dots, \frac{p-1}{2}\}$. Then we have $ia \equiv -ia \pmod{p} \Rightarrow i \equiv -i \pmod{p}$ since $(a, p) = 1$, a contradiction since $\{-\frac{p-1}{2}, \dots, -i, \dots, -1, 0, 1, \dots, i, \dots, \frac{p-2}{2}\}$ is a complete residue system modulo p. Hence, it is never the case that $r_i \equiv -r_j \pmod{p}$ for some i and j. The lemma now follows from our previous discussion. □

Theorem 7.14. (Gauss' Lemma). *Let p be a prime and a an integer not divisible by p. Let g be the number of negative representatives of $a, 2a, \dots, \frac{p-1}{2}a$ in the complete residue system $\{-\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}\}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^g$$

Proof. Let p be a prime, and $a \in \mathbb{Z}$ with $p \nmid a$. Let g be the number of negative representatives of $a, 2a, \dots, \frac{p-1}{2}a$ in the complete residue system $\{-\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}\}$. Furthermore, let $r_1, r_2, \dots, r_{\frac{(p-1)}{2}}$ the representatives of $a, 2a, \dots, \frac{p-1}{2}a$ in the complete residue system $\{-\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-2}{2}\}$. Then we can multiply the congruences $ia \equiv r_i \pmod{p}$ for $1 \leq i \leq \frac{p-1}{2}$ together to obtain

$$(a)(2a) \dots \left(\frac{p-1}{2}a\right) \equiv r_1 r_2 \dots r_{\frac{(p-1)}{2}} \pmod{p}$$

$$\Rightarrow a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv r_1 r_2 \dots r_{\frac{(p-1)}{2}} \pmod{p}$$

We can apply Lemma 7.13 to the right hand side of the above congruence to obtain

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^g \left(\frac{p-1}{2}\right)! \pmod p$$

and since $1, 2, 3, \ldots \frac{p-1}{2}$ are all relatively prime to p (since p is prime), we can repeatedly apply Theorem 4.30 to obtain

$$a^{(p-1)/2} \equiv (-1)^g \pmod p$$

We now apply Euler's Criterion to the left hand side to obtain

$$\left(\frac{a}{p}\right) \equiv (-1)^g \pmod p$$

as desired. □

Question 7.15. *Does the prime's residue class modulo 4 determine whether or not 2 is a quadratic residue? Consider the primes' residue class modulo 8 and see whether the residue class seems to correlate with whether or not 2 is a quadratic residue. Make a conjecture.*

Answer. Let p be a prime. We saw that with -1, it was sufficient to look at p's residue class modulo 4 in order to determine whether or not -1 was a quadratic residue. Notice, however, that this is not sufficient for 2 as both 7 and 11 are congruent to 3 modulo 4, but 2 is a quadratic residue modulo 7 and a quadratic non-residue modulo 11.

The book provides the following list of primes for which 2 is a quadratic residue:

$$7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97.103, 113, 127$$

and the following primes for which 2 is a quadratic non-residue:

$$3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109$$

Considering the primes' residue class modulo 8, the primes above for which 2 is a quadratic residue are congruent to 1 or 7 modulo 8, and all the primes above for which 2 is a quadratic non-residue are congruent to 3 or 5 modulo 8.

Theorem 7.16. *Let p be an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

Proof. Let p be an odd prime. Let g be the number of negative representatives of $2, 2(2), 3(2), \ldots, \frac{p-1}{2}(2)$ in the complete residue system $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$. Then by Gauss' Lemma,

$$\left(\frac{2}{p}\right) = (-1)^g$$

We are interested in the number of negative representatives of $S := \{2, 4, 6, \ldots, p-1\}$. This is equivalent to counting the number of elements of S that are greater than $\frac{p-1}{2}$ (note that $2\left(\frac{p-1}{2}\right) = p-1 \Rightarrow 2\left(\frac{p-1}{2}\right) \equiv -1 \pmod{p}$). In other words, we are interested in how many natural numbers between $\frac{p-1}{2}$ and $p-1$ (inclusive of $p-1$ and non-inclusive of $\frac{p-1}{2}$) are even. Hence, we narrow S down to $S' := \{\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1\}$ (from now on, let S' be an *ordered* set with the elements ordered in increasing order). The size of the list $\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$ is $\frac{p-1}{2}$, so $|S'| = \frac{p-1}{2}$. Notice that the last element of S' is always an even number. Hence, if $|S'| \equiv 0 \pmod{4}$ and the first element of S' is odd, or if $|S'| \equiv 3 \pmod{4}$ and the first element of S' is even, then S' will have an even number of even numbers. Notice that since $|S'| = \frac{p-1}{2}$ and the first element of S' is $\frac{p+1}{2}$, this happens if and only if $p \equiv 1$ or $7 \pmod{8}$ (observe that $p \equiv \alpha \pmod{8}$ for some $\alpha = 1, 3, 5,$ or 7 implies $\frac{p-1}{2} = 4k + \beta$ for some $\beta = 0, 1, 2,$ or 3 and $k \in \mathbb{N}$). Similarly, S' will have an odd number of even numbers if $|S'| \equiv 1 \pmod{4}$ and the first element of S' is even, or if $|S'| \equiv 2 \pmod{4}$ and the first element of S' is odd. This happens if and only if $p \equiv 3$ or $5 \pmod{8}$. It now follows that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

□

Exercise 7.17. *Table 1 shows* $\left(\frac{p}{q}\right)$ *for the first several odd primes. For example, the table indicates that* $\left(\frac{7}{3}\right) = 1$*, but that* $\left(\frac{3}{7}\right) = -1$*. Make another table that shows when* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *and when* $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$*.*

See pp. 93 of the book for "Table " referenced above. For the primes, $3, 5, 7, \ldots, 47$, we will construct a similar table that displays "=" if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, and "≠" if $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$.

	3	5	7	11	13	17	19	23	29	31	37	41	43	47
3		$=$	$\neq$	$\neq$	$=$	$=$	$\neq$	$\neq$	$=$	$\neq$	$=$	$=$	$\neq$	$\neq$
5			$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
7				$\neq$	$=$	$=$	$\neq$	$\neq$	$=$	$\neq$	$=$	$=$	$\neq$	$\neq$
11					$=$	$=$	$\neq$	$\neq$	$=$	$\neq$	$=$	$=$	$\neq$	$\neq$
13						$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
17							$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
19								$\neq$	$=$	$\neq$	$=$	$=$	$\neq$	$\neq$
23									$=$	$\neq$	$=$	$=$	$\neq$	$\neq$
29										$=$	$=$	$=$	$=$	$=$
31											$=$	$=$	$\neq$	$\neq$
37												$=$	$=$	$=$
41													$=$	$=$
43														$\neq$
47														

Table 2: Array showing when $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ for p read across the top and q down the side.

Exercise 7.18. *Make a conjecture about the relationship between* $\left(\frac{p}{q}\right)$ *and* $\left(\frac{q}{p}\right)$ *depending on* p *and* q.

Based on table 2 above, we conjecture that if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, if $p \equiv q \equiv 3 \pmod 4$ then $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$.

Theorem 7.19. (Quadratic Reciprocity Theorem—Reciprocity Part). *Let* p *and* a *be odd primes, then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 1 \pmod 3 \end{cases}$$

Proof. Omitted. □

Theorem. (Law of Quadratic Reciprocity). *Let* p *and* a *be odd primes, then*

1. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$

2. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8,, \end{cases}$

3. $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$

Exercise 7.20. (Computational Technique). *Given a prime, p, show how you can determine whether a number a is a quadratic residue modulo p. Equivalently, show how to find* $\left(\frac{a}{p}\right)$*. To illustrate your method, compute* $\left(\frac{1248}{93}\right)$ *and some other examples.*

Let p be some prime, and $a \in \mathbb{Z}$. An optional first step is to reduce a modulo p so that $a \equiv r \pmod{p}$ for some $r \in \{0, 1, 2, \ldots, p-1\}$ and then proceed with the following steps with r instead of a. Next, prime factorize a as $a = \pm p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ where ± is there in case $a < 0$. Since $p \nmid a$, p cannot divide any of the prime factors of a so that

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{p_1^{r_1}}{p}\right)\left(\frac{p_2^{r_2}}{p}\right)\ldots\left(\frac{p_k^{r_k}}{p}\right)$$

Now, notice that for all $1 \leq i \leq k$,

$$\begin{aligned}
\left(\frac{p_i^{r_i}}{p}\right) &= \left(\frac{\underbrace{p_i p_i \ldots p_i}_{i \text{ times}}}{p}\right) \\
&= \underbrace{\left(\frac{p_i}{p}\right)\left(\frac{p_i}{p}\right)\ldots\left(\frac{p_i}{p}\right)}_{i \text{ times}} \text{ (by Theorem 7.8)} \\
&= \left(\frac{p_i}{p}\right)^i
\end{aligned}$$

Hence,

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{p_1}{p}\right)^{r_1}\left(\frac{p_2}{p}\right)^{r_2}\ldots\left(\frac{p_k}{p}\right)^{r_k}$$

We know how to evaluate $\left(\frac{-1}{p}\right)$ from part 1 of the Law of Quadratic Reciprocity. If $p_1 = 2$, then we evaluate $\left(\frac{2}{p}\right)$ according to part 2 of the Law of Quadratic reciprocity. The remaining prime factors will be odd, and may be evaluated by an iterative approach that reduces the congruence $\left(\frac{q}{p}\right)$ to one where we need to evaluate the Legendre symbol for either 1 or 2 modulo a prime. We first reduce all of the primes modulo p, and factor any further factors that appear. We then use part 3 of the Law of Quadratic Reciprocity to end up with Legendre symbols of the form

$$\left(\frac{p}{p_1}\right), \left(\frac{p}{p_2}\right), \ldots, \left(\frac{p}{p_k}\right)$$

where $p_1, p_2, \ldots, p_k < p$ so that the "numerator" of the Legendre symbol may be further reduced. We then factor any new composites that arise, and use part 3 of the Law of Quadratic Reciprocity in exactly the same way. Continuing like this, we will always obtain smaller and smaller "numerators", and will eventually end up with either 2 or 1 with possible factors of -1 along the way. Once this happens, we evaluate this final Legendre symbols with 2 in them using part 2 of the Law of Quadratic Reciprocity, and put everything together to evaluate the original Legendre symbol.

We note that in the example given by the book, 93 is not a prime, so the above method is not applicable. In fact, none of what we have talked about is applicable here...
Let us instead consider $\left(\frac{1248}{97}\right)$. We first reduce 1248 so by $1248 \equiv 84 \pmod{97}$ so that $\left(\frac{1248}{97}\right) = \left(\frac{84}{97}\right)$. We then note that $84 = 2^2 \cdot 3 \cdot 7$. Hence, $\left(\frac{1248}{97}\right) = \left(\frac{2}{97}\right)^2 \left(\frac{3}{97}\right) \left(\frac{7}{97}\right)$. Since $97 \pmod 8 = 1$, $\left(\frac{2}{97}\right) = 1 \Rightarrow \left(\frac{2}{97}\right)^2 = 1$. For $\left(\frac{3}{97}\right)$, notice that $97 \pmod 4 = 1$ so that $\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) = \left(\frac{1}{97}\right) = 1$. For $\left(\frac{7}{97}\right)$, $97 \pmod 4 = 1$ so that $\left(\frac{7}{97}\right) = \left(\frac{97}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right)$. Notice that $7 \pmod 8 = 7$ so $\left(\frac{2}{7}\right) = 1$, and $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{7}\right) = -1$. Hence, $\left(\frac{1248}{97}\right) = (1)^2 \cdot (1) \cdot (-1) = -1$. Hence, 1248 is a quadratic non-residue modulo 97.

Exercise 7.21. *Find all the quadratic residues modulo 23.*

We utilize the Algorithm laid out in Exercise 7.20 to solve this problem:

n	$\left(\frac{n}{23}\right)$
1	$\left(\frac{1}{23}\right) = 1$
2	$\left(\frac{2}{23}\right) = 1$
3	$\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1$
4	$\left(\frac{4}{23}\right) = 1$
5	$\left(\frac{5}{23}\right) = -1$
6	$\left(\frac{6}{23}\right) = 1$
7	$\left(\frac{7}{23}\right) = -1$
8	$\left(\frac{8}{23}\right) = 1$
9	$\left(\frac{9}{23}\right) = 1$
10	$\left(\frac{10}{23}\right) = -1$
11	$\left(\frac{11}{23}\right) = -1$
12	$\left(\frac{12}{23}\right) = 1$
13	$\left(\frac{13}{23}\right) = 1$
14	$\left(\frac{14}{23}\right) = -1$
15	$\left(\frac{15}{23}\right) = -1$
16	$\left(\frac{16}{23}\right) = 1$
17	$\left(\frac{17}{23}\right) = -1$
18	$\left(\frac{18}{23}\right) = 1$
19	$\left(\frac{19}{23}\right) = -1$
20	$\left(\frac{20}{23}\right) = -1$
21	$\left(\frac{21}{23}\right) = -1$
22	$\left(\frac{22}{23}\right) = -1$

Hence, the quadratic residues modulo 23 are: $1, 2, 3, 4, 6, 8, 9, 12, 13, 16,$ and 18.

Sophie Germain is germane, Part II

Theorem 7.22. *Let p be a prime of the form $p = 2q + 1$ where q is a prime. Then every natural number $a, 0 < a < p - 1$, is either a quadratic residue or a primitive root modulo p.*

Proof. Let p be a prime of the form $p = 2q+1$ for some prime q. Let $a \in \mathbb{N}$ with $0 < a < p-1$. We first note that the order of a must divide $p - 1$, and since $p - 1 = 2q$, the order of a must be $1, 2, q$, or $2q$. By Theorem 4.38, the only a with order 1 or 2 are, respectively, 1 and $p - 1$. In both of these cases, a will be a quadratic residue modulo p, and cannot be primitive roots since primitive roots must have order $2q$ (and $q > 1$ since q is prime).

If $1 < a < p - 1$, then a has order q or $2q$. If a has order $2q$, then a must be primitive root since $2q = p - 1$. In this case, we can apply Euler's Criterion to see that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p} \Rightarrow a^q \equiv \left(\frac{a}{p}\right) \pmod{p}$. We cannot have $a^q \equiv 1 \pmod{p}$, however, as otherwise this contradicts a being a primitive root with order $2q > q$. Hence, a here is a primitive root and a quadratic non-residue modulo p.

If a has order $2q$, then it follows immediately that a is a quadratic residue since $a^{2q} \equiv (a^q)^2 \pmod{p}$. Moreover, a cannot be a primitive root since all primitive roots modulo p have order $2q > q$.

It follows every natural number $a, 0 < a < p-1$, is either a quadratic residue or a primitive root modulo p. □

Theorem 7.23. *Let p be a prime congruent to 3 modulo 4. Let a be a natural number with $1 < a < p - 1$. Then a is a quadratic residue modulo p if and only if $p - a$ is a quadratic non-residue modulo p.*

Proof. Let p be prime such that $p \equiv 3 \pmod{4}$, and let $a \in \mathbb{N}$ with $1 < a < p - 1$. Then $\exists k \in \mathbb{N}$ such that $p = 4k + 3$, and p is an odd prime.

($\Rightarrow$). Suppose that a is a quadratic residue modulo p. By Euler's Criterion, $a^{(p-1)/2} = 1$. Then $(p - a)^{(p-1)/2} \pmod{p} \equiv (-a)^{(p-1)/2} \pmod{p} \equiv (-1)^{(p-1)/2} \cdot a^{(p-1)/2} \pmod{p} \equiv (-1)^{(p-1)/2}$, and since $\frac{p-1}{2} = 2k+1$—an odd number—we have $(-1)^{(p-1)/2} \pmod{p} = -1$ so that $(p-a)^{(p-1)/2} \equiv -1 \pmod{p}$, and by Euler's Criterion, $p-a$ is a quadratic non-residue modulo p.

($\Leftarrow$). Suppose that $p - a$ is a quadratic non-residue modulo p. Then by Euler's Criterion, $(p - a)^{(p-1)/2} \equiv -1 \pmod{p} \Rightarrow (-a)^{(p-1)/2} \equiv -1 \pmod{p} \Rightarrow (-1)^{(p-1)/2} \cdot a^{(p-1)/2} \equiv -1 \pmod{p}$. Note that since $\frac{p-1}{2} = 2k + 1$ is odd, $(-1)^{(p-1)/2} = -1$ so that $(-1) \cdot a^{(p-1)/2} \equiv -1 \pmod{p} \Rightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$. By Euler's Criterion, it follows that a is a quadratic residue modulo p.

□

Theorem 7.24. *Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Then $p \equiv 3 \pmod 4$.*

Proof. Let p be a prime such that $p = 2q + 1$ where q is an odd prime. Since q is odd, $\exists k \in \mathbb{N}$ such that $q = 2k + 1$. Hence, $p = 2(2k + 1) + 1 = 4k + 3 \Rightarrow p \equiv 3 \pmod 4$, as desired. □

Theorem 7.25. *Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Let a be a natural number, $1 < a < p - 1$. Then a is a quadratic residue if and only if $p - a$ is a primitive root modulo p.*

Proof. Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Let $a \in \mathbb{N}$ with $1 < a < p - 1$. Then by Theorem 7.24, we have $p \equiv 3 \pmod 4$. We now use Theorem 7.23 to conclude that a is a quadratic residue if and only if $p - a$ is a quadratic non-residue modulo p. But from Theorem 7.22, we know that $0 < 1 < p - a < p - 1$ must either be a quadratic residue, or a primitive root modulo p. Hence, a is a quadratic residue if and only if $p - a$ is a primitive root modulo p. □

Theorem 7.26. *Let p be a prime and a be an integer. Then a^2 is not a primitive root modulo p.*

Note: *The Theorem is not true for $p = 2$, since 1 is both a quadratic residue modulo 2 and a primitive root modulo 2. We need the condition that p is odd for this to be true.*

Proof. Let p be a prime, and $a \in \mathbb{Z}$. As discussed above, we need $p \neq 2$ for the Theorem so that p is odd. We have that a^2 is a quadratic residue by definition. Suppose by way of contradiction that a^2 is a primitive root modulo p. Then $\text{ord}_p(a^2) = p-1$, and by Theorem 4.10 $p - 1$ must divide any exponent $k \in \mathbb{N}$ for which $(a^2)^k \equiv 1 \pmod p$. Since a^2 is a quadratic residue, by Euler's Criterion $(a^2)^{(p-1)/2} \equiv 1 \pmod p \Rightarrow p - 1 | \frac{p-1}{2} \Rightarrow \frac{1}{2} \in \mathbb{Z}$, a contradiction. Hence, a^2 is not a primitive root modulo p. □

Theorem 7.27. *Let p be a prime and let i and j be natural numbers with $i \neq j$ satisfying $1 < i, j < \frac{p}{2}$. Then $i^2 \not\equiv j^2 \pmod p$.*

Proof. Let p be a prime, and let $i, j \in \mathbb{N}$ with $i \neq j$ and $1 < i, j < \frac{p}{2}$. Suppose by way of contradiction that $i^2 \equiv j^2 \pmod p \Rightarrow p|(i^2 - j^2) \Rightarrow p|(i - j)(i + j)$ so that $p|(i - j)$ or $p|(i + j)$ by Theorem 2.27. Since $1 < i, j < \frac{p}{2}$, we have $2 < i + j < p$, and hence $p \nmid (i + j)$ since p is prime. Thus, $p|(i-j)$. Again, since $1 < i, j < \frac{p}{2}$, we have $(1-\frac{p}{2}) < i-j < (\frac{p}{2}-1)$, so we must have $i - j = 0$ since p is prime, and hence $i = j$ (a contradiction). Thus, $i^2 \not\equiv j^2 \pmod p$. □

Theorem 7.28. *Let p be a prime of the form $2q + 1$ where q is an odd prime. Then the complete set of numbers that are not primitive roots modulo p are $1, -1, 2^2, 3^2, \ldots, q^2$.*

Proof. Let p be a prime of the form $p = 2q+1$ where q is an odd prime. From the discussion in Theorem 7.22, we know that any element modulo p must have order $1, 2, q$, or $2q$, that 1 is the only element of order 1, $p - 1 \equiv -1 \pmod{p}$ is the only element of order 2, and that primitive roots have order $2q$. From this, we know that $1, -1$ are not primitive roots. Theorem 7.22 also tells us that for some $a \in \mathbb{N}$ with $0 < a < p - 1$, a is either a quadratic residue or a primitive rood modulo p. Since Theorem 7.6 tells us that exactly have of all such $a \in \mathbb{N}$ with $0 < a < p$ are quadratic residues, it is sufficient to find all $\frac{p-1}{2} - 1 = q - 1$ quadratic residues between 1 and $p - 1$ in order to have the complete set of numbers that are not primitive roots. Notice that the numbers $2^2, 3^2, 4^2, \ldots, q^2$ are all quadratic residues by definition, and are not primitive roots modulo p by Theorem 7.26. Moreover, Theorem 7.27 tells us that these numbers are pairwise incongruent since each number i satisfies $1 < i \leq q < \frac{p}{2} = q + \frac{1}{2}$. Hence, the complete set of numbers that are not primitive roots modulo p are indeed $1, -1, 2^2, 3^2, \ldots, q^2$. □

Theorem 7.29. *Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Then the complete set of primitive roots modulo p are $-2^2, -3^2, \ldots, -q^2$.*

Proof. Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. By Theorem 7.28, the complete set of numbers that are not primitive roots modulo p are $1, -1, 2^2, 3^2, \ldots, q^2$. By Theorem 7.22, this implies that any remaining elements that are not congruent to any of $1, -1, 2^2, 3^2, \ldots, q^2$ must be primitive roots. Recall that $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\} = \{-q, \ldots, -1, 0, 1, \ldots, q\}$ is a complete residue system modulo p. By Theorem 7.27, however, we must also have that $\{-q^2, \ldots, -3^2, -2^2, -1, 0, 1, 2^2, \ldots q^2\}$ is also a complete residue system modulo p. It follows that the complete set of primitive roots modulo p are $-2^2, -3^2, \ldots, -q^2$. □

Exercise 7.30. *Verify that the primitive roots modulo 23 that we listed earlier in this section are in fact the same as those given by Miller's Theorem.*

We first note that $23 = 2(11)+1$, and 11 is an odd prime. We need to compute $-2^2, -3^2, \ldots, -23^2$ modulo 23. Observe,

i	$-i^2 \pmod{23}$
2	$-2^2 \pmod{23} = -4 = 19$
3	$-3^2 \pmod{23} = -9 = 14$
4	$-4^2 \pmod{23} = -16 = 7$
5	$-5^2 \pmod{23} = -25 = 21$
6	$-6^2 \pmod{23} = -36 = 10$
7	$-7^2 \pmod{23} = -49 = 20$
8	$-8^2 \pmod{23} = -64 = 5$
9	$-9^2 \pmod{23} = -81 = 11$
10	$-10^2 \pmod{23} = -100 = 15$
11	$-11^2 \pmod{23} = -121 = 17$

Which is the same list of numbers obtained before for the primitive roots of 23.

Exercise 7.31. *List the primitive roots and quadratic residues modulo 47.*

We first note that $47 = 2(23) + 1$, and 23 is an odd prime. Following the same procedure as before, we use Miller's Theorem to produce the following table:

i	$-i^2 \pmod{23}$
2	$-2^2 \pmod{23} = -4 = 43$
3	$-3^2 \pmod{23} = -9 = 38$
4	$-4^2 \pmod{23} = -16 = 31$
5	$-5^2 \pmod{23} = -25 = 22$
6	$-6^2 \pmod{23} = -36 = 11$
7	$-7^2 \pmod{23} = -49 = 45$
8	$-8^2 \pmod{23} = -64 = 30$
9	$-9^2 \pmod{23} = -81 = 13$
10	$-10^2 \pmod{23} = -100 = 41$
11	$-11^2 \pmod{23} = -121 = 20$
12	$-12^2 \pmod{23} = -144 = 44$
13	$-13^2 \pmod{23} = -169 = 19$
14	$-14^2 \pmod{23} = -196 = 39$
15	$-15^2 \pmod{23} = -225 = 10$
16	$-16^2 \pmod{23} = -256 = 26$
17	$-17^2 \pmod{23} = -289 = 40$
18	$-18^2 \pmod{23} = -324 = 5$
19	$-19^2 \pmod{23} = -361 = 15$
20	$-20^2 \pmod{23} = -400 = 23$
21	$-21^2 \pmod{23} = -441 = 29$
22	$-22^2 \pmod{23} = -484 = 33$
23	$-23^2 \pmod{23} = -529 = 35$

8 Pythagorean Triples, Sums of Squares, and Fermat's Last Theorem

Pythagorean Triples

Theorem 8.1. *If (a, b, c) is a Pythagorean triple, then at least one of a or b is even.*

Proof. Let (a, b, c) be a Pythagorean triple. If a is even, then we are done. Without loss of generality then, suppose that a is odd. Suppose by way of contradiction that b is also odd. Then $\exists r, s \in \mathbb{N}$ such that $a = 2r + 1$ and $b = 2s + 1$. Observe that $a^2 = 4r^2 + 4r + 1 = 4(r^2 + r) + 1$ and $b^2 = 4s^2 + 4s + 1 = 4(s^2 + s) + 1$ so that b^2 and c^2 are odd and $a^2 + b^2 \equiv 2 \pmod 4) \Rightarrow c^2 \equiv 2 \pmod 4$. Hence, $a^2 + b^2 = c^2$ is even. Through prime factorization, we see that c must also be even, and thus c^2 is a multiple of four so that $c^2 \equiv 0 \pmod 4$. This is a contradiction since $0 \not\equiv 2 \pmod 4$. Hence, b must be even.

It follows that at least one of a or b is even. □

Exercise 8.2. *Find at least seven different Pythagorean triples. Make a note of your methods.*

Here is a list of seven Pythagorean triples:

1. $(3, 4, 5)$
2. $(6, 8, 10)$
3. $(9, 12, 15)$
4. $(5, 12, 13)$
5. $(10, 24, 26)$
6. $(15, 36, 39)$
7. $(8, 15, 17)$

One easy method for generating Pythagorean triples is to take any multiple of an existing Pythagorean triple.

Exercise 8.3. *Find at least five primitive Pythagorean triples.*

Here is a list of 5 primitive Pythagorean triples:

1. $(3, 4, 5)$
2. $(9, 12, 15)$
3. $(8, 15, 17)$

4. $(7, 24, 25)$

5. $(20, 21, 29)$

Theorem 8.4. *In any primitive Pythagorean triple, one leg is odd, one leg is even, and the hypotenuse is odd.*

Proof. Let (a, b, c) be a primitive Pythagorean triple. By Theorem 8.1, we can—without loss of generality—choose a to be even. We first show that b must be odd. Suppose by way of contradiction that b is even. Then $\exists r, s \in \mathbb{N}$ such that $a = 2r$ and $b = 2s$. Then $c^2 = a^2 + b^2 = 4r^2 + 4s^2 = 4(r^2 + s^2) \Rightarrow 4|c^2 \Rightarrow 2|c$. But then a, b, and c all have a common factor of 2, which contradicts the fact that (a, b, c) is a primitive Pythagorean triple. Hence, b is odd. Since a is even and b is odd, a^2 is even and b^2 is odd, and hence their sum $c^2 = a^2 + b^2$ is odd. It follows that c is odd, and we are done. □

Theorem 8.5. *Let s and t be any two different natural numbers with $s > t$. Then*

$$(2st, (s^2 - t^2), (s^2 + t^2))$$

is a Pythagorean triple.

Proof. Let $s, t \in \mathbb{N}$ with $s > t$. We can verify directly that $(2st, (s^2 - t^2), (s^2 + t^2))$ is a Pythagorean triple. Observe,

$$\begin{aligned}(2st)^2 + (s^2 - t^2)^2 &= (4s^2t^2) + (s^4 - 2s^2t^2 + t^4) \\ &= s^4 + 2s^2t^2 + t^4 \\ &= (s^2 + t^2)^2\end{aligned}$$

as desired. □

Lemma 8.6. *Let (a, b, c) be a primitive Pythagorean triple where a is the even number. Then $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are perfect squares, say s^2 and t^2 respectively; and s and t are relatively prime.*

Proof. Let (a, b, c) be a primitive Pythagorean triple with a even (comes WLOG from Theorem 8.1). Then $4|a^2$. Observe that $a^2 = c^2 - b^2 = (c + b)(c - b)$, and since $\frac{a^2}{4} \in \mathbb{Z}$ we have $\frac{a^2}{4} = \frac{c+b}{2} \cdot \frac{c-b}{2} \in \mathbb{Z}$. Since a and c are both odd (by Theorem 8.4), their sum and differences even, and thus $\frac{c+b}{2} \in \mathbb{N}$ and $\frac{c-b}{2} \in \mathbb{N}$. Moreover, if d is a common divisor of $\frac{c+b}{2}$ and $\frac{c-b}{2}$, then d must also divide their sum and difference, which is c and b respectively. But since (a, b, c) is a primitive Pythagorean triple, d must be equal to 1. Hence, $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are relatively prime. Since their product is also equal to a square, we have from prime factorization that each of them must be a square itself. Hence, $\frac{c+b}{2} = s^2$ and $\frac{c-b}{2} = t^2$ for some $s, t \in \mathbb{N}$. Since s^2 and t^2 are relatively prime, it follows that s and t don't share any prime factors, and are hence relatively prime as well. □

Theorem 8.7. (Pythagorean Triple Theorem). *Let (a, b, c) be a triple of natural numbers with a even, b odd, and c odd. Then (a, b, c) is a primitive Pythagorean triple if and only if there exist relatively prime positive integers s and t, one even and one odd, such that $a = 2st, b = (s^2 - t^2)$, and $c = (s^2 + t^2)$.*

Proof. Let (a, b, c) be a triple of natural numbers with a even, b odd, and c odd.

($\Rightarrow$) Suppose that (a, b, c) is a primitive Pythagorean triple. Then by Lemma 8.6, $\exists s, t \in \mathbb{N}$ such that $(s, t) = 1$, $s^2 = \frac{c+b}{2}$, and $t^2 = \frac{c-b}{2}$. Then we immediately have that $s^2-t^2 = b$ and $s^2 + t^2 = c$. Now observe,

$$\begin{aligned} 2st &= 2\sqrt{\frac{c+b}{2}} \cdot \sqrt{\frac{c-b}{2}} \\ &= 2\sqrt{\frac{(c+b)(c-b)}{4}} \\ &= \sqrt{c^2 - b^2} \\ &= \sqrt{a^2} \\ &= a \end{aligned}$$

Finally, notice that since c is odd and $c = s^2 + t^2$, one of t^2 and s^2 must be even and one must be odd. From prime factorization, this happens if and only if one of s and t is even and one is odd.

($\Leftarrow$) Conversely, suppose that $\exists s, t \in \mathbb{N}$ with $(s, t) = 1$, and one of s, t even and one odd such that $a = 2st, b = (s^2 - t^2)$, and $c = (s^2 + t^2)$. In order to have $b \in \mathbb{N}$ we need $s > t$. By Theorem 8.5, we know that (a, b, c) is a Pythagorean triple. Notice that since of one of s and t is even and one is odd, we automatically have that $a = 2st$ is even, $b = s^2 - t^2$ is odd, and $c = s^2 + t^2$ is even.

To see why (a, b, c) must be a primitive Pythagorean triple, suppose by way of contradiction that $\exists d \in \mathbb{N}$ with $d > 1$ and $d|a$, $d|b$, and $d|c$. We know that $d > 2$ since b and c are odd. Hence, $d|a = 2st$ implies that $d|s$ or $d|t$ since $(s, t) = 1$. If $d|s$, then $c = s^2 + t^2 \Rightarrow d|t$, a contradiction since $(s, t) = 1$. Similarly, if $d|t$, then $c = s^2 + t^2 \Rightarrow d|s$, also a contradiction since $(s, t) = 1$. It follows that (a, b, c) must be a primitive Pythagorean triple.

□

Exercise 8.8. *Using the above formulas make a lengthy list of primitive Pythagorean triples.*

We simply need to choose relatively prime prime natural numbers s, t with one even and one odd and then utilize Theorem 8.7. We can make use of the following pairs of (s, t):

$(3,2),(7,4),(6,5),(8,5),(22,21),(56,3),(17,14)$, and $(18,7)$.

(s,t)	(a,b,c)
$(3,2)$	$(12,5,13)$
$(7,4)$	$(56,33,65)$
$(6,5)$	$(60,11,61)$
$(8,5)$	$(80,39,89)$
$(22,21)$	$(924,43,925)$
$(56,3)$	$(336,3127,3145)$
$(17,14)$	$(476,93,485)$
$(18,7)$	$(252,275,373)$

Exercise 8.9. *Make a conjecture that describes those natural numbers that can appear as legs in a primitive Pythagorean triple.*

Based on the fact that $a = 2st$, and one of s or t must be even, I conjecture that it must be the case that $4|a$.

Theorem 8.10. *In every primitive Pythagorean triple, one leg is an odd integer greater than 1 and the other is a positive multiple of 4.*

Proof. Let (a, b, c) be a primitive Pythagorean triple. Then by the Pythagorean Triple Theorem, $\exists s, t \in \mathbb{N}$, one even and one odd, with $(s, t) = 1$ such that $a = 2st, b = s^2 - t^2$, and $c = s^2 + t^2$. We also know from Theorem 8.4 that one leg is even, one leg is odd, and the hypotenuse is odd. a has already implicitly been chosen to be the even leg since we wrote $a = 2st$, so b must be the odd leg. Observe that since one of s or t is even, that $a = 2st$ must be divisible by two factors of 2. That is, $4|a$. Moreover, since $s \neq t$, $b = s^2 - t^2 > 1$. To summarize, we have that a is a positive multiple of 4, and b is an odd integer greater than 1, so we are done. □

Theorem 8.11. *Any odd number greater than* 1 *can occur as a leg in a primitive Pythagorean triple.*

Proof. This follows immediately from the Pythagorean Triple Theorem since we can choose s or t to be any odd number greater than 1 that we'd like, and then choose the other variable to be any even natural number relatively prime to our chosen odd number. The resulting $a = 2st, b = s^2 - t^2$, and $c = s^2 + t^2$ will be a primitive Pythagorean triple. □

Theorem 8.12. *Any positive multiple of* 4 *can occur as a leg in a primitive Pythagorean triple.*

Proof. This follows immediately from the Pythagorean Triple Theorem since we can choose s or t to be any positive multiple of 4 that we'd like, and then choose the other variable to be any odd integer greater than one that's also relatively prime to our chosen multiple of 4. The resulting $a = 2st, b = s^2 - t^2$, and $c = s^2 + t^2$ will be a primitive Pythagorean triple. □

Sums of Squares

Question 8.13. *Make a list of the first fifteen primes and write each as the sum of as few squares of natural numbers as possible. Which ones can be written as the sum of two squares? Make a conjecture about which primes can be written as the sum of two squares of natural numbers.*

Answer. This first 15 primes are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

Here is a table showing the sum of each of these primes in terms of as few squares as possible:

p	$p = x_1^2 + x_2^2 + \cdots + x_k^2$
2	$1^2 + 1^2$
3	$1^2 + 1^2 + 1^2$
5	$1^2 + 2^2$
7	$1^2 + 1^2 + 1^2 + 2^2$
11	$1^2 + 1^2 + 3^2$
13	$2^2 + 3^2$
17	$1^2 + 4^2$
19	$1^2 + 3^2 + 3^2$
23	$1^2 + 2^2 + 3^2 + 3^2$
29	$2^2 + 5^2$
31	$1^2 + 1^2 + 2^2 + 5^2$
37	$1^2 + 6^2$
41	$4^2 + 5^2$
43	$3^2 + 3^2 + 5^2$
47	$1^2 + 1^2 + 3^2 + 6^2$

Judging by the above results, we are able to write a prime as a sum of the square of two natural numbers if $p \pmod 4 = 1$ or $p \pmod 4 = 2$. The only case observed above where $p \pmod 4 = 2$, however, was $p = 2$.

Theorem. *Let p be a prime. Then p can be written as the sum of two squares of natural numbers if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Theorem 8.14. *Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Then either $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof. Let p be a prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{N}$. If $p = 2$, then we have $p \equiv 2 \pmod 4$. Otherwise, if $p \neq 2$, then p must be an odd prime, and we must have either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.
By way of contradiction, suppose that $p \equiv 3 \pmod 4$. Then by Theorem 7.10, -1 is a quadratic non-residue modulo p. Observe that $p = a^2 + b^2 \Rightarrow a^2 + b^2 \equiv 0 \pmod p \Rightarrow a^2 \equiv -b^2 \pmod p \Rightarrow \left(\frac{a+kp}{b}\right)^2 \equiv -1 \pmod p$ for some $k \in \mathbb{N} \Rightarrow -1$ is a quadratic residue modulo p, a contradiction. Hence, $p \equiv 1 \pmod 4$. □

Lemma 8.15. *Let p be a prime and let a be a natural number not divisible by p. Then there exist integers x and y such that $ax \equiv y \pmod{p}$ with $0 < |x|, |y| < \sqrt{p}$.*

Proof. Let p be a prime and $a \in \mathbb{N}$ with $p \nmid a$. Then $(a, p) = 1$. Notice that there are at least $2(\sqrt{p} - 1)$ choices for each of x and y if $0 < |x|, |y| < \sqrt{p}$, so in total we have at least $2(\sqrt{p} - 1) \cdot 2(\sqrt{p} - 1) = 4(p - 2\sqrt{p} + 1) > 2p$ combinations for pairs (x, y). Since there are only p distinct residue classes modulo p, it follows that there must exist some integers x, y satisfying $ax \equiv y \pmod{p}$. □

Theorem 8.16. *Let p be a prime such that $p \equiv 1 \pmod{4}$. Then p is equal to the sum of two squares of natural numbers.*

Proof. Let p be a prime with $p \equiv 1 \pmod{4}$. Then by the Law of Quadratic Reciprocity, -1 must be a quadratic residue modulo p. Hence, $\exists a \in \mathbb{N}$ such that $-1 \equiv a \pmod{p}$. Now, by Lemma 8.15, $\exists x, y \in \mathbb{Z}$ with $0 < |x|, |y| < \sqrt{p}$ such that $ax \equiv y \pmod{p} \Rightarrow -x^2 \equiv y^2 \pmod{p} \Rightarrow x^2 + y^2 \equiv 0 \pmod{p} \Rightarrow x^2 + y^2 = kp$ for some $k \in \mathbb{N}$. Notice, however, that $0 < |x|, |y| < \sqrt{p}$ means that $x^2 + y^2 < 2p$. Hence $k = 1$ so that $x^2 + y^2 = p$, as desired. □

Exercise 8.17. *Check the following identity:*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2$$

Observe,

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= ((ac)^2 + 2abcd + (bd)^2) + ((bc)^2 - 2abcd + (ad)^2) \\ &= (ac + bd)^2 + (bc - ad)^2\end{aligned}$$

as desired.

Theorem 8.18. *If an integer x can be written as the sum of two squares of natural numbers and an integer y can be written as the sum of two squares of natural numbers, then xy can be written as the sum of two squares of natural numbers.*

Proof. Suppose that $x, y \in \mathbb{N}$ can be written as the sum of two squares of natural numbers, say $x = a^2 + b^2$ and $y = c^2 + d^2$ for some $a, b, c, d \in \mathbb{N}$. Then we can simply apply the identity in Exercise 8.17 to see that

$$xy = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2$$

and since $|ac + bd|, |bc - ad| \in \mathbb{N}$, we have found natural numbers whose squares sum to xy, as desired. □

Exercise 8.19. *For each of the following numbers, (i) determine the number's prime factorization and (ii) write the number as the sum of two squares of natural numbers.*

1. 205
(i) $205 = 5 \cdot 41$
(ii) Notice that $5 \equiv 1 \pmod 4$ *and* $41 \equiv 1 \pmod 4$ *so we should be able to write each one as a sum of squares of natural numbers. Indeed, referring back to our table in exercise 8.13,* $5 = 1^2 + 2^2$ *and* $41 = 4^2 + 5^2$*. Using the identity in exercise 8.17,* $205 = (1^2 + 2^2)(4^2 + 5^2) = (4 + 10)^2 + (8 - 5)^2 = 14^2 + 3^2$*. That is,*

$$205 = 14^2 + 3^2$$

2. 6409
(i) $6409 = 13 \cdot 17 \cdot 29$.
(ii) Observe, $13 = 2^2+3^2, 17 = 1^2+4^2, 29 = 2^2+5^2$*. So* $(13)(17) = (2+12)^2+(8-3)^2 = 14^2 + 5^2 \Rightarrow (13)(17)(29) = (28 + 25)^2 + (10 - 70)^2 = 53^2 + 60^2$*. Hence,*

$$6409 = 53^2 + 60^2$$

3. 722
(i) $722 = 2 \cdot 19 \cdot 19$.
(ii) Notice that $19 \equiv 3 \pmod 4$*, so we cannot write* 19 *as a sum of squares of natural numbers. No need to despair, however, as this is actually even easier to evaluate! Notice that* $2 = 1^2 + 1^2$ *so that* $722 = (1^2 + 1^2) \cdot 19^2 = 19^2 + 19^2$*. That is,*

$$722 = 19^2 + 19^2$$

4. 11745
(i) $11745 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 29 = 3^4 \cdot 5 \cdot 29$.
(ii) Notice that $5 = 1^2+2^2$ *and* $29 = 2^2+5^2$*, so* $(5)(29) = (2+10)^2+(4-5)^2 = 1^2+12^2$*. Hence,* $3^4(5 \cdot 29) = (9^2)(1^2) + (9^2)(12^2) = 9^2 + 108^2$*. Finally,*

$$11745 = 9^2 + 108^2$$

Question 8.20. *Which natural numbers can be written as the sum of two squares of natural numbers? State and prove the most general theorem possible about which natural numbers can be written as the sum of two squares of natural numbers, and prove it.*

Answer. Based on the technique that we developed in Exercise 8.19, I'd say that if each prime factor of a number n is congruent to 1 modulo 4, then we can write each factor as a sum of squares of naturals, and then repeatedly apply Theorem 8.18 to write the whole product (and thus n) as a sum of squares of naturals. If any primes that are not congruent to 1 modulo 4 appear, then so long as they appear to an even power, we can keep them aside and multiply them in at the end to still end up with a sum of squares of naturals.

Theorem 8.21. *A natural number n can be written as a sum of two squares of natural numbers if and only if every prime congruent to* 3 *modulo* 4 *in the unique prime factorization of n occurs to an even power.*

Proof. Let $n \in \mathbb{N}$. Suppose that $n = 2^m p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ is the prime factorization of n where $m \in \mathbb{N} \cup \{0\}$, p_i is prime for all $1 \leq i \leq k$, and $r_i \in \mathbb{N}$ for all $1 \leq i \leq k$. For the prime factor 2, we simply write $2 = (1^2 + 1^2)$. For the prime factors that are congruent to 1 modulo 4 (if there are any), we know that we can write each of them as the sum of two squares of natural numbers by Theorem 8.16. Hence, by repeated application of Theorem 8.18, we can write the product of 2^m and all the primes congruent to 1 modulo 4 as the sum of squares of two natural numbers, say $c^2 + d^2$. Let the primes that are congruent to 3 modulo 4 be denoted by $p_{j_1}, p_{j_2}, \ldots, p_{j_s}$. Then we have $n = (c^2 + d^2) p_{j_1}^{r_{j_1}} p_{j_2}^{r_{j_2}} \ldots p_{j_s}^{r_{j_s}}$ (note: if there are no prime factors that are congruent to 1 modulo 4, then both directions of the Theorem follows immediately from the previous equation).

($\Rightarrow$) Suppose that n can be written as a sum of two squares of natural numbers, say $n = a^2 + b^2$ for some $a, b \in \mathbb{N}$. Hence, $a^2 + b^2 = (c^2 + d^2) p_{j_1}^{r_{j_1}} p_{j_2}^{r_{j_2}} \ldots p_{j_s}^{r_{j_s}}$. Further refine this product so that $a^2 + b^2 = (c_1^2 + d_1^2)m$ where m is the product of all the prime factors of n that are congruent to 3 modulo 4, and have an odd exponent. Assuming there is at least one such prime factor, say p, then $m > 1$. We know that $p|n$ and $p|m$ so that $a^2 + b^2 \equiv 0 \pmod{p}$, but we already showed earlier that this happens only if $p \equiv 1 \pmod{4}$. Hence, there cannot be any prime factors that are both congruent to 3 modulo 4, and appear to an odd exponent.

($\Leftarrow$) Suppose that every prime congruent to 3 modulo 4 in the unique prime factorization of n occurs to an even power. Then we have $n = (cp_{j_1}^{r_{j_1}/2} p_{j_2}^{r_{j_2}/2} \ldots p_{j_s}^{r_{j_s}/2})^2 + (d^2 p_{j_1}^{r_{j_1}/2} p_{j_2}^{r_{j_2}/2} \ldots p_{j_s}^{r_{j_s}/2})^2$ which shows that n can be written as the sum of squares of two natural numbers, as desired.

□

Pythagorean triples revisited

Theorem 8.22. *If (a, b, c) is a primitive Pythagorean triple, then c is a product of primes each of which is congruent to* 1 *modulo* 4*.*

Proof. Let (a, b, c) be a primitive Pythagorean triple. Then by the Pythagorean Triple Theorem, $c = s^2 + t^2$ for some $s, t \in \mathbb{N}$, one even and one odd, with $(s, t) = 1$. By Theorem 8.21, this happens if and only if every prime congruent to 3 modulo 4 of c occurs to an even power. From the construction of the proof in Theorem 8.21, however, we know that any prime p for which $p \equiv 3 \pmod{4}$ must divide each term in the sum of squares. Since $(s, t) = 1$, however, it must be the case that c has no prime factors that are congruent to 3 modulo 4. Moreover, since c is odd (by Theorem 8.4), c also doesn't have a prime factor congruent to 2 modulo 4. It follows that all prime factors of c are congruent to 1 modulo 4. □

Theorem 8.23. *If the natural number c is a product of primes each of which is congruent to* 1 *modulo* 4*, then there exist integers a and b such that (a, b, c) is a primitive Pythagorean triple.*

Proof. Let $c \in \mathbb{N}$ such that c is a product of primes, each of which is congruent to 1 modulo 4. Then c^2 is also a product of primes, each of which is congruent to 1 modulo 4, and by Theorem 8.16, we can write each of these primes as a sum of squares of natural numbers. Through repeated application of Theorem 8.18, we can write the product of these sums of squares as a single sum of squares, say $a^2 + b^2$ for some $a, b \in \mathbb{N}$. It follows that $a^2 + b^2 = c^2$, so that (a, b, c) is a Pythagorean triple. The fact this is a primitive Pythagorean triple follows from that fact that c has no prime factors that are congruent to 3 modulo 4. □

Fermat's Last Theorem

Theorem. Fermat's Last Theorem, proved by Andrew Wiles in 1994). *For natural number $n \geq 3$, there are no natural numbers x, y, z such that $x^n + y^n = z^n$.*

Theorem 8.24. *There are no natural numbers x, y, and z such that $x^4 + y^4 = z^2$.*

Proof. Consider the equation $x^4 + y^4 = z^2$. By way of contradiction, suppose that there is a solution $x = a, y = b$, and $z = c$ for some $a, b, c \in \mathbb{N}$. Then we'd have $a^4 + b^4 = c^2 \Rightarrow (a^2)^2 + (b^2)^2 = c^2$ so that (a^2, b^2, c) is a Pythagorean triple. Without loss of generality, we can assume that a^2, b^2, and c have no common factors since we can always reduce the equation $(a^2)^2 + (b^2)^2 = c^2$ to get such a solution. Furthermore, we can without loss of generality once more assume that a^2 is even and b^2 is odd by Theorem 8.4. Now, by the Pythagorean Triple Theorem (Theorem 8.7), $\exists s, t \in \mathbb{N}$, one even and one odd, with $(s, t) = 1$ such that $a^2 = 2st, b^2 = s^2 - t^2$, and $c = s^2 + t^2$.

Now, observe that $b^2 = s^2 - t^2 \Rightarrow b^2 + t^2 = s^2$, and since $(s, t) = 1$, we have that b, t, and s don't share any common factors so that (b, t, s) is a primitive Pythagorean Triple. By Theorem 8.4, since s is the hypotenuse of this Pythagorean triple, it follows that s is odd. It follows then that t must be even since one of s or t is even and one is odd. Applying the Pythagorean Triple Theorem once more (Theorem 8.7), $\exists u, v \in \mathbb{N}$, one even and one odd, with $(u, v) = 1$ such that $t = 2uv, b = u^2 - v^2$, and $s = u^2 + v^2$ (notice that we must have $t = 2uv$ since t is known to be even).

Going back to the primitive Pythagorean triple (a^2, b^2, c), notice that $a^2 = 2st$ implies that $2st$ is a perfect square. Hence, since $(s, t) = 1$, however, it follows that one of them must be equal to an odd natural number squared, and the other must be equal to 2 times an odd natural number squared. Since we already know that t is even, we have that $t = 2m^2$ and $s = n^2$ for some $m, n \in \mathbb{N}$. Substituting $t = 2m^2$ into $t = 2uv$ gives $2m^2 = 2uv \Rightarrow m^2 = uv$. Since $(u, v) = 1$, however, it follows that each must be a square itself. That is, $u = p^2$ and $v = q^2$ for some $p, q \in \mathbb{N}$ with $(p, q) = 1$ and one of p or q even and the other odd.

To summarize, we have the equations $s = u^2 + v^2, u = p^2, v = q^2$, and $s = n^2$. Combining these together gives $p^4 + v^4 = n^2$. It remains to show that $n < c$. For this, we use the final equation we haven't used: $c = s^2 + t^2 \Rightarrow c = n^4 + t^2 \Rightarrow n^4 = c - t^2 < c \Rightarrow n < c^{1/4} < c$.

Thus, from our original solutions (a, b, c), we have produced a new solution (p, v, n) where $n < c$. This implies that we can always produce solutions for which the right-hand-side in $x^4 + y^4 = z^2$ is smaller than our previous solution. This is a contradiction, since any monotonically decreasing sequence of natural numbers must be finite. It follows that $x^4 + y^4 = z^2$ has no solutions. □

9 Rationals Close to Irrationals and the Pell Equation

A plunge into rational approximation

Theorem 9.1. *Let α be an irrational number and let b be a natural number. Then there exists an integer a such that*

$$\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{2b}$$

Proof. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $b \in \mathbb{N}$. Let β be the largest integer such that $\beta < \alpha b$, and γ be the smallest integer such that $\gamma > \alpha b$. Since $\alpha \notin \mathbb{Q}$, we must have either $|\alpha b - \beta| < \frac{1}{2}$ or $|\alpha b - \gamma| < \frac{1}{2}$. Define a to be either β or γ, depending on which of these inequalities is satisfied. Then $|\alpha b - a| < \frac{1}{2} \Rightarrow |b| \cdot \left|\alpha - \frac{a}{b}\right| < \frac{1}{2} \Rightarrow b \cdot \left|\alpha - \frac{a}{b}\right| < \frac{1}{2}$ since $b \in \mathbb{N} \Rightarrow |b| = b$. It follows that $\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{2b}$, as desired. □

Exercise 9.2. *Among the first eleven multiples of $\sqrt{2}$,*

$$0\sqrt{2}, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots, 10\sqrt{2}$$

find the two whose difference is closest to a positive integer. Feel free to use a calculator. Use those two multiples to find a good rational approximation for $\sqrt{2}$. By good, we mean that you find integers a and b such that

$$\left|\frac{a}{b} - \sqrt{2}\right| \leq \frac{1}{b^2}$$

We use the following Python code to find the closest two multiples to a positive integer:

```
import math

min_dist = 10
closest_mults = [0,0]

for i in range(0,10 + 1):
    for j in range(0, 10 + 1):
        if i != j:
            diff = abs(i * math.sqrt(2) - j * math.sqrt(2))
            dist = abs(diff - round(diff))

            if dist < min_dist:
                min_dist = dist
                closest_mults = [i,j]

print(closest_mults)
```

The code returned that $0\sqrt{2}$ and $5\sqrt{2}$ return the closest difference to a positive integer. In fact, $5\sqrt{2} - 0\sqrt{2} = 7.071067... \approx 7 \Rightarrow \sqrt{2} \approx \frac{7}{5}$. Observe that $\left|\frac{7}{5} - \sqrt{2}\right| = 0.0142135...$ and $\frac{1}{5^2} = 0.04$ so that $\left|\frac{7}{5} - \sqrt{2}\right| \leq \frac{1}{5^2}$.

Exercise 9.3. *Repeat the previous exercise for* $\sqrt{7}$ *using the first* 13 *multiples of* $\sqrt{7}$.

A simple modification of the above code to include the first 13 multiples of $\sqrt{7}$ returns that $\left|4\sqrt{7} - 7\sqrt{7}\right| = 7.93725... \approx 8 \Rightarrow 3\sqrt{7} \approx 8 \Rightarrow \sqrt{7} \approx \frac{8}{3}$. Observe, $\left|\frac{8}{3} - \sqrt{7}\right| = 0.0209153...$ and $\frac{1}{3^2} = 0.1111....$, so $\left|\frac{8}{3} - \sqrt{7}\right| \leq \frac{1}{3^2}$.

Exercise 9.4. *Repeat the previous exercise for* π*, using the first 15 multiples of* π.

Again, a simple modification of the code in exercise 9.2 gives $|6\pi - 13\pi| = 21.9911... \approx 22 \Rightarrow \pi \approx \frac{22}{7}$. Indeed, $\left|\frac{22}{7} - \pi\right| = 0.00126449...$ and $\frac{1}{7^2} = 0.020408163...$ so that $\left|\frac{22}{7} - \pi\right| \leq \frac{1}{7^2}$.

Question 9.5. *Let* α *be an irrational number.*

1. *Imagine making a list of the first* 11 *multiples of* α*. Can you predict how close to an integer the nearest difference between two of those numbers must be?*

   Answer. Since the first multiple of α is going to be 0, the first 2 multiples of α must have a distance from a positive integer of less than 1. If we consider the first 3 multiples, the most we can spread out the differences of these multiples by is $\frac{1}{3}$. In general, we can make the difference between the nearest two numbers less than or equal to $\frac{1}{m}$ if we consider the first m multiples of a number. So for 11, we'd expect the closest difference to an integer to be $\frac{1}{11}$ away from an integer.

2. *Now imagine making a list of* 11 *multiples of* α*, but not the first* 11*. Can you still predict how close to an integer the nearest difference between two of those numbers must be?*

   Answer. The reasoning here does not change if the first multiple of α is any non-zero multiple. We should still be able to make the difference between some two multiples of α that belong to a consecutive set of 11 multiples less than or equal to $\frac{1}{11}$.

3. *Now imagine making a list of* 50 *multiples of* α*, rather than just* 11*. Can you predict how close to an integer the nearest difference between two of those numbers must be?*

   Answer. We already addressed the general case in part 1. The closest difference will be $\frac{1}{50}$.

4. *What is the general relationship between how many multiples of* α *we consider and how well we can rationally approximate* α *using our multiples?*

   Answer. As mentioned in part 1, given m multiples of α, we can get a rational approximation that is at least $\frac{1}{m}$ away from the true value.

Theorem 9.6. *Let* K *be a positive integer. Then, among any* K *real numbers, there is a pair of them whose difference is within* $1/K$ *of being an integer.*

Proof. Let $K \in \mathbb{N}$. Consider $r_1, r_2, \dots, r_K \in \mathbb{R}$. Since we are only concerned with how close the decimal part of differences of these real numbers, it is sufficient to show that the difference in the decimal part of these real numbers is within $1/K$ of being an integer. Let $d_1, d_2, \dots, d_K$ be the decimal parts of, respectively, $r_1, r_2, \dots, r_K$. WLOG, suppose that $d_1 < d_2 < \cdots < d_K$. By way of contradiction, suppose that there does not exist some pair d_i, d_j that satisfy $|d_i - d_j| \leq 1/K$. Then we must have $d_1 < d_2 + 1/K, d_2 < d_3 + 1/K, \dots d_{K-1} < d_K + 1/K \Rightarrow d_1 < d_K + (K-1)(1/K) \Rightarrow d_1 - d_K < 1 - 1/K$, a contradiction since this says that the difference between d_1 and d_K is less within $1/K$ of the integer 1. Hence, there must exist some pair of real numbers whose difference is within $1/K$ of being an integer. □

Theorem 9.7. *Let α be a positive irrational number and K be a positive integer. Then there exist positive integers $a, b,$ and c with $0 \leq a < b \leq K$ and $0 \leq c \leq K\alpha$ such that*

$$\left|\frac{c}{b-a} - \alpha\right| \leq \frac{1}{(b-a)^2}$$

Proof. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ with $\alpha > 0$ and $K \in \mathbb{N}$. consider the first K multiples of $0 < \alpha$, $\alpha, 2\alpha, \dots, K\alpha$. Then by Theorem 9.6, $\exists$ multiples $a\alpha, b\alpha$ and a positive integer c such that the $a\alpha$ and $b\alpha$ differ by less than $1/K$ from c. WLOG, we can assume $a < b$ and $0 < c \leq K\alpha$ (since it doesn't matter which way we take the difference, and the difference cannot exceed the largest multiple $K\alpha$). Moreover, we clearly already have $0 \leq a < b \leq K$. Putting this all together, we have

$$||b\alpha - a\alpha| - c| \leq \frac{1}{K}$$

$$\Rightarrow |c - (b-a)\alpha| \leq \frac{1}{K}$$

and since $a < b \leq K \Rightarrow b - a < K \Rightarrow \frac{1}{K} < \frac{1}{b-a}$, we have

$$\Rightarrow |c - (b-a)\alpha| \leq \frac{1}{b-a}$$

dividing by $b - a$ gives,

$$\Rightarrow \left|\frac{c}{b-a} - \alpha\right| \leq \frac{1}{(b-a)^2}$$

as desired. □

Theorem 9.8. (Dirichlet's Rational Approximation Theorem, Version I). *Let α be any real number. Then there exist infinitely many rational numbers $\frac{a}{b}$ satisfying*

$$\left|\frac{a}{b} - \alpha\right| \leq \frac{1}{b^2}$$

Proof. Let $\alpha \in \mathbb{R}$. By relabelling c as a and $b-a$ as b in Theorem 9.7, we know that there exists at least one rational number $\frac{a}{b}$ satisfying $\left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2}$. By way of contradiction, suppose that there are finitely many such $\frac{a}{b}$ that satisfy this. Recall from the proof of Theorem 9.7, that we had $b-a < K \Rightarrow \frac{1}{K} < \frac{1}{b-a}$, which in our case gives $\frac{1}{K} < \frac{1}{b}$. We simply choose K sufficiently large so that $\frac{1}{K} < \left|\frac{a}{b}-\alpha\right|$ for every such $\frac{a}{b}$. But then by Theorem 9.7 again, there exists another rational $\frac{a}{b}$ that satisfies $\left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2}$, a contradiction. Hence, there are infinitely many rational numbers $\frac{a}{b}$ that satisfy $\left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2}$. □

Theorem. (Dirichlet's Rational Approximation Theorem, Version II). *Let α be any real number. Then there exist infinitely many integers a and b satisfying*

$$|a-b\alpha| \leq \frac{1}{b}$$

Theorem 9.9. *Show that Versions I and II of Dirichlet's Rational Approximation Theorem can be deduced from one another.*

Proof. Let $\alpha \in \mathbb{R}$.

(I $\Rightarrow$ II) Suppose that there exist infinitely many rational number $\frac{a}{b}$ satisfying $\left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2}$. Then WLOG we can assume that $b > 0$ since we can always choose one of a or b to be less than zero if $\frac{a}{b}$. Then $|b| = b$, and

$$\begin{aligned} &\left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2} \\ \iff\ & |b| \cdot \left|\frac{a}{b}-\alpha\right| \leq |b| \cdot \frac{1}{b^2} \\ \iff\ & |a-b\alpha| \leq \frac{1}{b} \end{aligned}$$

Observe there must exist infinitely many different a and b that satisfy the above equation since in order to have infinitely many different rationals $\frac{a}{b}$, a and b must vary between each distinct rational number. This shows Version II.

(I $\Leftarrow$ II) The converse is very similar. Suppose that there exist infinitely many integers a and b satisfying $|a-b\alpha| \leq \frac{1}{b}$. Then since $0 \leq |a-b\alpha|$, we must have $0 \leq \frac{1}{b} \Rightarrow b > 0$ so that $|b| = b$. Hence,

$$\begin{aligned} &|a-b\alpha| \leq \frac{1}{b} \\ \iff\ & \frac{1}{|b|} \cdot |a-b\alpha| \leq \frac{1}{|b|} \cdot \frac{1}{b} \\ \iff\ & \left|\frac{a}{b}-\alpha\right| \leq \frac{1}{b^2} \end{aligned}$$

To see why $\frac{a}{b}$ must produce infinitely many rational numbers, suppose by way of contradiction that $\frac{a}{b}$ produced finitely many rational numbers. Then since there are infinitely many choices for $b > 0$, we can choose a sufficiently large b so that $\frac{1}{b^2} < \left|\frac{a}{b} - \alpha\right|$ for every such $\frac{a}{b}$. But then the corresponding $\frac{a}{b}$ to this b will produce a new smallest rational $\frac{a}{b}$, a contradiction. Hence, there are infinitely many rational numbers $\frac{a}{b}$ that satisfy $\left|\frac{a}{b} - \alpha\right| \leq \frac{1}{b^2}$, which shows Version I.

□

Theorem. (Dirichlet's Rational Approximation Theorem, Version III). *Let N be a positive integer that is not a square. Then there exist infinitely many positive integers a and b satisfying*

$$\left|a - b\sqrt{N}\right| \leq \frac{1}{b}$$

Exercise 9.10. *Show that if N is a natural number which is not a square and $x = a$ and $y = b$ is a positive integer solution to the Pell equation $x^2 - Ny^2 = 1$, then $\frac{a}{b}$ gives a good rational approximation to $\sqrt{N}$.*

Let $N \in \mathbb{N}$ with N not a perfect square. Then $\sqrt{N} \in \mathbb{R} \setminus \mathbb{Q}$. Suppose that $x = a$ and $y = b$ is a positive integer solution to the Pell equation $x^2 - Ny^2 = 1$. Then observe that $a^2 - Nb^2 = 1 \Rightarrow (a - \sqrt{N}b)(a + \sqrt{N}b) = 1 \Rightarrow (\frac{a}{b} - \sqrt{N})(\frac{a}{b} + \sqrt{N}) = \frac{1}{b^2}$. Since $N \geq 1 \Rightarrow \sqrt{N} \geq 1 \Rightarrow \frac{a}{b} + \sqrt{N} > 1$ since a and b are positive integers, we have that $\left|\frac{a}{b} - \sqrt{N}\right| \left|\frac{a}{b} + \sqrt{N}\right| = \left|\frac{1}{b^2}\right| \Rightarrow \left|\frac{a}{b} - \sqrt{N}\right| (\frac{a}{b} + \sqrt{N}) = \frac{1}{b^2} \Rightarrow \left|\frac{a}{b} - \sqrt{N}\right| < \frac{1}{b^2}$ since $\frac{a}{b} + \sqrt{N} > 1$. This shows that $\frac{a}{b}$ is always within $\frac{1}{b^2}$ of $\sqrt{N}$, which typically means that we will have at least a couple decimals of accuracy.

Theorem 9.11. *Let N be a positive integer that is not square. If $x = a$ and $y = b$ is a solution in positive integers to $x^2 - Ny^2 = 1$, then*

$$\left|\frac{a}{b} - \sqrt{N}\right| < \frac{1}{b^2}$$

Proof. We repeat the proof laid out in Exercise 9.10.
Let $N \in \mathbb{N}$ with N not a perfect square. Suppose that $x = a$ and $y = b$ is a positive integer solution to the Pell equation $x^2 - Ny^2 = 1$. Then observe that $a^2 - Nb^2 = 1 \Rightarrow (a - \sqrt{N}b)(a + \sqrt{N}b) = 1 \Rightarrow (\frac{a}{b} - \sqrt{N})(\frac{a}{b} + \sqrt{N}) = \frac{1}{b^2}$. Since $N \geq 1$, we have $\sqrt{N} \geq 1 \Rightarrow \frac{a}{b} + \sqrt{N} > 1$ since a and b are positive integers. Now, $\left|\frac{a}{b} - \sqrt{N}\right| \left|\frac{a}{b} + \sqrt{N}\right| = \left|\frac{1}{b^2}\right| \Rightarrow \left|\frac{a}{b} - \sqrt{N}\right| (\frac{a}{b} + \sqrt{N}) = \frac{1}{b^2} \Rightarrow \left|\frac{a}{b} - \sqrt{N}\right| < \frac{1}{b^2}$ since $\frac{a}{b} + \sqrt{N} > 1$, as desired. □

Out with the trivial

Question 9.12. *For every natural number N, there are some trivial values of x and y that satisfy the Pell equation $x^2 - Ny^2 = 1$. What are those trivial solutions?*

Answer. Trivial solutions have $y = 0$ so that $x^2 = 1$, from which we have $(x, y) = (1, 0)$ and $(x, y) = (-1, 0)$ are always solutions.

Question 9.13. *For what values of the natural number N can you easily show that there are no non-trivial solutions to the Pell equation $x^2 - Ny^2 = 1$?*

Answer. Observe that $x^2 - Ny^2 = 1 \Rightarrow (x - \sqrt{N}y)(x + \sqrt{N}y) = 1$. If $(x - \sqrt{N}y), (x + \sqrt{N}y) \in \mathbb{Z}$, then $(x - \sqrt{N}y) = 1$ and $(x + \sqrt{N}y) = 1$, or $(x - \sqrt{N}y) = -1$ and $(x + \sqrt{N}y) = -1$. If $(x - \sqrt{N}y) = 1$ and $(x + \sqrt{N}y) = 1$, then adding the equations gives $2x = 2 \Rightarrow x = 1 \Rightarrow y = 0$. In the other case, we also end up with trivial solutions. In other words, if N is a perfect square, then the only solutions are non-trivial.

Theorem 9.14. *If the natural number N is a perfect square, then the Pell equation*

$$x^2 - Ny^2 = 1$$

has no non-trivial integer solutions.

Proof. Let $N \in \mathbb{N}$ with N a perfect square. Then $\exists n \in \mathbb{N}$ such that $\sqrt{N} = n$. Consider the Pell equation $x^2 - Ny^2 = 1$. We have,

$$\begin{aligned} x^2 - Ny^2 &= 1 \\ \Rightarrow (x - \sqrt{N}y)(x + \sqrt{N}y) &= 1 \\ \Rightarrow (x - ny)(x + ny) &= 1 \end{aligned}$$

Since we have $(x - ny), (x + ny) \in \mathbb{N}$, the only way their product can come out to be equal to 1 is if $(x - ny) = 1$ and $(x + ny) = 1$, or $(x - ny) = -1$ and $(x + ny) = -1$.

Suppose that $(x - ny) = 1$ and $(x + ny) = 1$. Adding these two equations gives $2x = 2 \Rightarrow x = 1$. Substituting $x = 1$ into $x + ny = 1$ gives $1 + ny = 1 \Rightarrow ny = 0 \Rightarrow y = 0$ since $n \in \mathbb{N}$ implies that $n \neq 0$. Hence, we only have the trivial solution $x = 1$ and $y = 0$.

Suppose that $(x - ny) = -1$ and $(x + ny) = -1$. Similar to the above, adding the equations gives $2x = -2 \Rightarrow x = -1$. Substituting this into $x + ny = -1 \Rightarrow -1 + ny = -1 \Rightarrow ny = 0 \Rightarrow y = 0$ since $n \in \mathbb{N}$ implies that $n \neq 0$. This gives the trivial solution $x = -1$ and $y = 0$.

In either case, we see that if N is a perfect square, then the Pell equation $x^2 - Ny^2 = 1$ has no non-trivial solutions. □

Exercise 9.15. *Find, by trial and error, at least two non-trivial solutions to each of the Pell equations $x^2 - 2y^2 = 1$ and $x^2 - 3y^2 = 1$.*

First consider the Pell equation $x^2 - 2y^2 = 1$. Consider the following table that illustrates our trial and error procedure:

x	y	$x^2 - 2y^2$
1	1	-1
3	1	①
9	2	①

Hence, two non-trivial solutions are $(x, y) = (3, 1)$ and $(x, y) = (9, 2)$.

Now consider the Pell equation $x^2 - 3y^2 = 1$. Consider the following table that illustrates our trial and error procedure:

x	y	$x^2 - 3y^2$
2	1	$\textcircled{1}$
3	2	-3
7	4	$\textcircled{1}$

Hence, two non-trivial solutions are $(x, y) = (2, 1)$ and $(x, y) = (7, 4)$.

New solutions from old

Question 9.16. *To know all the integer solutions to a Pell equation, why does it suffice to know just the postiive integer solutions?*

Answer. Since we are squaring any integer solutions, multiplying a solution by -1 does not change the fact that it's a solution. In fact, if $x = a$ and $y = b$ are integer solutions to $x^2 - Ny^2 = 1$, then so are $x = \pm a$ and $y = \pm b$. In other words, since we can make any negative solution positive (and vice versa), it is sufficient to consider only the positive integer solutions.

Theorem 9.17. *Suppose N is a natural number and the Pell equation $x^2 - Ny^2 = 1$ has two solutions, namely, $a^2 - Nb^2 = 1$ and $c^2 - Nd^2 = 1$ for some integers a, b, c, and d. Then $x = ac + Nbd$ and $y = ad + bc$ is also an integer solution to the Pell equation $x^2 - Ny^2 = 1$. That is,*

$$(ac + Nbd)^2 - N(ad + bc)^2 = 1$$

Proof. Let $N \in \mathbb{N}$. Suppose that the Pell equation $x^2 - Ny^2 = 1$ has two solutions, namely, $a^2 - Nb^2 = 1$ and $c^2 - Nd^2 = 1$ for some $a, b, c, d \in \mathbb{Z}$. Observe,

$$\begin{aligned}
(a^2 - Nb^2) \cdot 1 &= 1 \cdot 1 \\
\Rightarrow (a^2 - Nb^2) \cdot (c^2 - Nd^2) &= 1 \\
\Rightarrow (ac)^2 - N(ad)^2 - N(bc)^2 + (Nbd)^2 &= 1 \\
\Rightarrow \left((ac)^2 + 2abcdN + (Nbd)^2\right) - N\left((ad)^2 + 2abcd + (bc)^2\right) &= 1 \\
\Rightarrow (ac + Nbd)^2 - N(ad + bc)^2 &= 1
\end{aligned}$$

Which shows that $x = ac + Nbd$ and $y = ad + bc$ also satisfy the Pell equation $x^2 - Ny^2 = 1$. □

Securing the elusive solution

Theorem 9.18. *Let N be a natural number and suppose that x and y are positive integers satisfying $\left|x - y\sqrt{N}\right| < \frac{1}{y}$. Then*

$$x + y\sqrt{N} < 3y\sqrt{N}$$

Proof. Let $N \in \mathbb{N}$. Suppose that $x, y \in \mathbb{N}$ satisfy $\left|x - y\sqrt{N}\right| < \frac{1}{y}$. Observe,

$$\begin{aligned} x + y\sqrt{N} &= \left|x + y\sqrt{N}\right| \text{ (since } x, y, \sqrt{N} > 0) \\ &= \left|(x - y\sqrt{N}) + 2y\sqrt{N}\right| \\ &\leq \left|x - y\sqrt{N}\right| + 2y\sqrt{N} \text{ (triangle inequality)} \\ &< \frac{1}{y} + 2y\sqrt{N} \end{aligned}$$

Notice that $y \geq 1 \Rightarrow y^2 \geq 1 \Rightarrow y \geq \frac{1}{y} \Rightarrow y\sqrt{N} \geq \frac{1}{y}$ since $N \in \mathbb{N}$ implies that $\sqrt{N} \geq 1$. Thus, we can combine this with the above result to obtain

$$x + y\sqrt{N} < y\sqrt{N} + 2y\sqrt{N} = 3y\sqrt{N}$$

as desired. □

Theorem 9.19. *Let N be a natural number and suppose that x and y are positive integers satisfying $\left|x - y\sqrt{N}\right| < \frac{1}{y}$. Then*

$$\left|x^2 - Ny^2\right| < 3\sqrt{N}$$

Proof. Let $N \in \mathbb{N}$, and suppose that $x, y \in \mathbb{N}$ satisfy $\left|x - y\sqrt{N}\right| < \frac{1}{y}$. By Theorem 9.18, we have that $x + y\sqrt{N} < 3y\sqrt{N}$. Moreover, since $x, y, \sqrt{N} > 0$, we have that $x + y\sqrt{N} > 0$ so that $x + y\sqrt{N} = \left|x + y\sqrt{N}\right|$. Hence,

$$\begin{aligned} x + y\sqrt{N} &< 3y\sqrt{N} \\ \Rightarrow \left|x + y\sqrt{N}\right| \cdot \left|x - y\sqrt{N}\right| &< 3y\sqrt{N} \cdot \left|x - y\sqrt{N}\right| \end{aligned}$$

and since $\left|x - y\sqrt{N}\right| < \frac{1}{y}$, we have

$$\begin{aligned} \left|(x + y\sqrt{N}) \cdot (x - y\sqrt{N})\right| &< 3y\sqrt{N} \cdot \frac{1}{y} \\ \Rightarrow \left|x^2 - Ny^2\right| &< 3\sqrt{N} \end{aligned}$$

as desired. □

Theorem 9.20. *There exists a non-zero integer K such that the equation*

$$x^2 - Ny^2 = K$$

has infinitely many solutions in positive integers.

Proof. Let $N \in \mathbb{N}$ with N not a perfect square. Then by Dirichlet's Rational Approximation Theorem, Version III, $\exists$ infinitely many $x, y \in \mathbb{N}$ such that $\left|x - y\sqrt{N}\right| < \frac{1}{y}$. By Theorem 9.19, we know that all such x, y satisfy $\left|x^2 - Ny^2\right| < 3\sqrt{N}$. That is, each of the infinitely many $x^2 - Ny^2$ can only take one of finitely many integer values between 0 and $3\sqrt{N}$. Hence, $\exists K \in \mathbb{Z}$ with $0 \leq K < 3\sqrt{N}$ such that $x - Ny^2 = K$ has infinitely many solutions. □

Lemma 9.21. *Let n be a natural number and suppose that $(x_i, y_i), i = 1, 2, 3, \ldots$ are infinitely many ordered pairs of integers. Then there exist distinct natural numbers j and k such that*

$$x_j \equiv x_k \pmod{n} \quad \textit{and} \quad y_j \equiv y_k \pmod{n}$$

Proof. Since there are only n distinct residue classes modulo n, we know that know that there is an infinite subset of the pairs of integers $(x_{i_j}, y_{i_j}), j = 1, 2, 3, \ldots$ such that $x_{i_r} \equiv x_{i_s} \pmod{n}$ $\forall 1 \leq r, s$. Again, since there are only n distinct residue classes modulo n, we know that there exists an infinite subset of this set of x_i, say $(x_{i_{j_k}}, y_{i_{j_k}}), k = 1, 2, 3, \ldots$ such that $y_{i_{j_r}} \equiv y_{i_{j_s}} \pmod{n}$ $\forall 1 \leq r, s$. Choosing any of one these gives the desired result. □

Lemma 9.22. *Let N be a natural number and K be a non-zero integer and let (x_j, y_j) and (x_k, y_k) be two distinct integer solutions to $x^2 - Ny^2 = K$ satisfying*

$$x_j \equiv x_k \pmod{|K|} \quad \textit{and} \quad y_j \equiv y_k \pmod{|K|}$$

Then

$$x = \frac{x_j x_k - y_j y_k N}{K} \quad \textit{and} \quad y = \frac{x_j y_k - x_k y_j}{K}$$

are integers satisfying $x^2 - Ny^2 = 1$.

Proof. Let $N \in \mathbb{N}$ and $K \in \mathbb{Z}$ with $K \neq 0$. Suppose that (x_j, y_j) and (x_k, y_k) are distinct integer solutions to $x^2 - Ny^2 = K$ that satisfy $x_j \equiv x_k \pmod{|K|}$ and $y_j \equiv y_k \pmod{|K|}$.

We first show that $\frac{x_j x_k - y_j y_k N}{K}$ and $\frac{x_j y_k - x_k y_j}{K}$ are integers. Observe that $x_j \equiv x_k \pmod{|K|} \Rightarrow x_j^2 \equiv x_j x_k \pmod{|K|}$ and $y_j \equiv y_k \pmod{|K|} \Rightarrow y_j^2 \equiv y_j y_k \pmod{|K|} \Rightarrow Ny_j^2 \equiv y_j y_k N \pmod{|K|}$. Subtracting these two congruences gives $x_j^2 - Ny_j^2 \equiv x_j x_k - y_j y_k N \pmod{|K|} \Rightarrow K \equiv x_j x_k - y_j y_k N \pmod{|K|}$. Hence, $x_j x_k - y_j y_k N$ is divisible by K so that $x := \frac{x_j x_k - y_j y_k N}{K}$ is an integer. For the fraction, observe $y_j \equiv y_k \pmod{|K|} \Rightarrow x_j y_k \equiv x_j y_j \pmod{|K|}$ and $x_k y_j \equiv x_k y_k \pmod{|K|}$. We can also multiply $x_j \equiv x_k \pmod{|K|}$ and $y_j \equiv y_k \pmod{|K|}$ to get $x_j y_j \equiv x_k y_k \pmod{|K|}$. Using the transitive property of congruence modulo $|K|$, we combine all three of these congruences to get $x_j y_k \equiv x_k y_j \pmod{|K|} \Rightarrow x_j y_k - x_k y_j \equiv 0 \pmod{|K|} \Rightarrow |K| \,|(x_j y_k - x_k y_j)$ so that $y := \frac{x_j y_k - x_k y_j}{K}$ is an integer. Note that $K \neq 0$ is necessary for the x and y to be defined (i.e. to avoid division by 0).

We verify directly that x and y are solutions to the Pell equation $x^2 - Ny^2 = 1$. Observe,

$$\begin{aligned}
x^2 - Ny^2 &= \left(\frac{x_jx_k - y_jy_kN}{K}\right)^2 - N\left(\frac{x_jy_k - x_ky_j}{K}\right)^2 \\
&= \frac{(x_j^2x_k^2 - 2x_jx_ky_jy_kN + y_j^2y_k^2N^2) - N(x_j^2y_k^2 - 2x_jx_ky_jy_k + x_k^2y_j^2)}{K^2} \\
&= \frac{(x_j^2x_k^2 + y_j^2y_k^2N^2) - N(x_j^2y_k^2 + x_k^2y_j^2)}{K^2} \\
&= \frac{x_j^2(x_k^2 - Ny_k^2) - Ny_j^2(x_k^2 - Ny_k^2)}{K^2} \\
&= \frac{(x_k^2 - Ny_k^2)(x_j^2 - Ny_j^2)}{K^2} \\
&= \frac{K \cdot K}{K^2} \\
&= 1
\end{aligned}$$

as desired. □

Theorem 9.23. *If N is a positive integer that is not a square, then the Pell equation $x^2 - Ny^2 = 1$ has a non-trivial solution in positive integers.*

Proof. Let $N \in \mathbb{N}$ with N not a perfect square. Then by Theorem 9.20, the Pell equation $x^2 - Ny^2 = 1$ has infinitely many positive integer solutions $(x_i, y_i), i = 1, 2, 3, \ldots$. From these infinite solutions, by Lemma 9.21, $\exists j, k \in \mathbb{N}$ with $j \neq k$ such that $x_j \equiv x_k \pmod{|K|}$ and $y_j \equiv y_k \pmod{|K|}$. Finally, by Lemma 9.22, $x := \frac{x_jx_k - y_jy_kN}{K}$ and $y := \frac{x_jy_k - x_ky_j}{K}$ will be integers that satisfy $x^2 - Ny^2 = 1$. If either x or y are not positive, then we can multiply the negative one(s) by -1 to get positive integers that still satisfy the Pell equation $x^2 - Ny^2 = 1$, so we are done. □

Exercise 9.24. *Follow the steps of the preceeding theorems to find several solutions to the Pell equations $x^2 - 5y^2 = 1$ and $x^2 - 6y^2 = 1$ and then give some good rational approximation to $\sqrt{5}$ and $\sqrt{6}$.*

We start with the Pell equation $x^2 - 5y^2 = 1$. We first consider $x^2 - 5y^2 = K$. Observe that $(x, y) = (4, 2)$ and $(x, y) = (4, -2)$ give $x^2 - 5y^2 = -4$. We also have $4 \equiv 4 \pmod 4$ and $2 \equiv -2 \pmod 4$. Let $x = \frac{(4)(4)-(2)(-2)(5)}{-4} = -9$ and $y = \frac{(4)(-2)-(4)(2)}{-4} = 4$. Thus, $(x, y) = (9, 4)$ is a non-trivial solution to the Pell equation $x^2 - 5y^2 = 1$. Combining this solution with itself gives $x = (9)(9) + (5)(4)(4) = 161$ and $y = (9)(4) + (4)(9) = 72$. Thus a good rational approximation to $\sqrt{5}$ is $\sqrt{5} \approx \frac{161}{72}$.

Now consider the Pell equation $x^2 - 6y^2 = 1$. Observe that $(x, y) = (7, 3)$ and $(x, y) = (17, -7)$ satisfy $x^2 - 6y^2 = -5$, as well as $17 \equiv 7 \pmod 5$ and $3 \equiv -7 \pmod 5$. Now, $x = \frac{(17)(7)-(3)(-7)(6)}{-5} = -49$ and $y = \frac{(7)(-7)-(17)(3)}{-5} = 20$. Hence, $(x, y) = (49, 20)$ is a non-trivial solution to the Pell equation $x^2 - 6y^2 = 1$. Combining this solution with itself gives $x = (49)(49) + (6)(20)(20) = 4801$ and $y = (49)(20) + (20)(49) = 1960$. Thus a good rational approximation to $\sqrt{6}$ is $\sqrt{6} \approx \frac{4801}{1960}$.

The structure of the solutions to the Pell equations

Theorem 9.25. *Let N be a natural number and $r_1, r_2, s_1,$ and s_2 be integers. If $\alpha = r_1 + s_1\sqrt{N}$ and $\beta = r_2 + s_2\sqrt{N}$ both give solutions to the Pell equation $x^2 - Ny^2 = 1$, then so does $\alpha\beta$.*

Proof. Let $N \in \mathbb{N}$, and $r_1, r_2, s_1, s_2 \in \mathbb{Z}$. Suppose that $\alpha := r_1 + s_1\sqrt{N}$ and $\beta = r_2 + s_2\sqrt{N}$ both give solutions to the Pell equation $x^2 - Ny^2 = 1$. Observe,

$$\begin{aligned} \alpha\beta &= (r_1 + s_1\sqrt{N})(r_2 + s_2\sqrt{N}) \\ &= (r_1r_2 + Ns_1s_2) + (r_1s_2 + r_2s_1)\sqrt{N} \end{aligned}$$

We need to show that $x = r_1r_2 + Ns_1s_2$ and $y = r_1s_2 + r_2s_1$ satisfy the Pell equation $x^2 - Ny^2 = 1$. We have

$$\begin{aligned} x^2 - Ny^2 &= (r_1r_2 + Ns_1s_2)^2 - N(r_1s_2 + r_2s_1)^2 \\ &= r_1^2r_2^2 + N^2s_1^2s_2^2 - N(r_1^2s_2^2 + r_2^2s_1^2) \\ &= r_1^2(r_2^2 - Ns_2^2) - Ns_1^2(r_2^2 - Ns_2^2) \\ &= (r_1^2 - Ns_1^2)(r_2^2 - Ns_2^2) \\ &= 1 \cdot 1 \\ &= 1 \end{aligned}$$

Hence $\alpha\beta$ is also a solution. □

Theorem 9.26. *Let N be a natural number and r and s integers. If $\alpha = r + s\sqrt{N}$ gives a solution to $x^2 - Ny^2 = 1$, then so does $1/\alpha$.*

Proof. Let $N \in \mathbb{N}$, and $r, s \in \mathbb{Z}$. Suppose that $\alpha := r + s\sqrt{N}$ gives a solution to the Pell equation $x^2 - Ny^2 = 1$. Observe,

$$\begin{aligned} \frac{1}{\alpha} &= \frac{1}{r + s\sqrt{N}} \cdot \frac{r - s\sqrt{N}}{r - s\sqrt{N}} \\ &= \frac{r - s\sqrt{N}}{r^2 - Ns^2} \\ &= r - s\sqrt{N} \text{ (since } r^2 - Ns^2 = 1) \end{aligned}$$

and since $r^2 - N(-s)^2 = r^2 - Ns^2 = 1$, we have that $\frac{1}{\alpha}$ also gives a solution to $x^2 - Ny^2 = 1$. □

Corollary 9.27. *Let N be a natural number and r and s integers. If $\alpha = r + s\sqrt{N}$ gives a solution to $x^2 - Ny^2 = 1$, then so does α^k for any integer k.*

Proof. Let $N \in \mathbb{N}$, and $r, s \in \mathbb{Z}$. Suppose that $\alpha := r+s\sqrt{N}$ gives a solution to $x^2-Ny^2 = 1$. We prove the Corollary by induction.

For some $k \in \mathbb{Z}$, let $P(k)$ be the statement: α^k gives a solution to $x^2 - Ny^2 = 1$.

For the first induction step, suppose that α^k gives a solution to $x^2 - Ny^2 = 1$. Then by Theorem 9.25, so does $\alpha^k \cdot \alpha = \alpha^{k+1}$.

For the second induction step, if α^k gives a solution to $x^2 - Ny^2 = 1$. Then by Theorem 9.26, $\frac{1}{\alpha}$ is a solution since α is, so we can use Theorem 9.25 to conclude that $\alpha^k \cdot \frac{1}{\alpha} = \alpha^{k-1}$ is also a solution.

By the principle of mathematical induction, it follows that α^k is a solution $\forall k \in \mathbb{Z}$. □

Exercise 9.28. *Let N be a natural number and r and s integers. Show that if $r + s\sqrt{N}$ gives a solution to $x^2 - Ny^2 = 1$, then so do each of*

$$r - s\sqrt{N}, \ -r + s\sqrt{N}, \quad \textit{and} \quad -r - s\sqrt{N}$$

Let $N \in \mathbb{N}$, and $r, s \in \mathbb{Z}$ such that $r + s\sqrt{N}$ gives a solution to $x^2 - Ny^2 = 1$. The desired result follow from that simple fact that $(-r)^2 = r^2$ and $(-s)^2 = s^2$. Using this, we see that $(r)^2 + N(-s)^2 = (-r)^2 + Ns^2 = (-r)^2 + N(-s)^2 = r^2 + Ns^2 = 1$. Hence, each of $r - s\sqrt{N}$, $-r + s\sqrt{N}$, and $-r - s\sqrt{N}$ give solutions to $x^2 - Ny^2 = 1$.

Theorem 9.29. *Let N be a positive integer that is not a square. Let A be the set of all real numbers of the form $r + s\sqrt{N}$, with r and s positive integers, that give solutions to $x^2 - Ny^2 = 1$. Then*

1. *there is a smallest element α in A,*
2. *the real numbers $\alpha^k, k = 1, 2, \ldots$ give all positive integer solutions to $x^2 - Ny^2 = 1$.*

Proof. Let $N \in \mathbb{N}$ with N not a perfect square. Define $A := \{r + s\sqrt{N} \mid r, s \in \mathbb{N} \text{ and } r^2 - Ns^2 = 1\}$.

1. Consider the Pell equation $x^2-Ny^2 = 1$. First notice that none of the trivial solutions to this Pell equation lie in A since $y = 0 \Rightarrow y \notin \mathbb{N}$. By Theorem 9.23 $\exists$ a non-trivial solution, say $\beta = a + b\sqrt{N}$ with $a, b \in \mathbb{N}$ to the Pell equation $x^2 - Ny^2 = 1$. Hence, A is not empty. For some solution $r + s\sqrt{N}$, let us call r the "integer part" and s the "irrational" part of the solution (analogous to the "real" and "imaginary" part of a complex number). Define $R := \{r \mid r + s\sqrt{N} \in A, \ \exists s \in \mathbb{N}\}$ and $S := \{s \mid r + s\sqrt{N} \in A, \ \exists r \in \mathbb{N}\}$ (i.e., R is the set of the "integer part" of all elements in A and S is the set of the "irrational part" of all elements in A). By definition, $R \subseteq \mathbb{N}$ and $S \subseteq \mathbb{Z}$. Moreover, since A is not empty, so are R and S. Hence, by the Well-Ordering axiom of the naturals, R has a least element, say $r \in R$, and a corresponding element $s \in S$ such

that $\alpha := r + s\sqrt{N} \in A$. We claim that this is the smallest element in A. To see why this is the case, observe that since r is the minimal element in R, the only way that α could be smaller is if s were smaller. However, since $r^2 - Ns^2 = 1 \Rightarrow r^2 = Ns^2 + 1$, if s is any smaller, then r must also be smaller, a contradiction. Hence, minimizing r also minimizes α so that $\alpha = r + s\sqrt{N}$ is indeed the smallest element in A.

2. For the Pell equation $x^2 - Ny^2 = 1$, we know from part 1 that $\exists \alpha \in A$ such that α is the smallest element in A. Moreover, we know from Corollary 9.27 that $\alpha^k \in A$ $\forall k = 1, 2, \ldots$. To show that this gives all positive integer solutions to the Pell equation $x^2 - Ny^2 = 1$, it is sufficient to show that every element in A is of the form α^k for some $k = 1, 2, \ldots$. By way of contradiction, suppose that $\exists$ a non trivial solution $\beta = u + v\sqrt{N} \in A$ with $\beta \neq \alpha^k$ for any $k = 1, 2, \ldots$. Then we must have $\alpha^m < \beta < \alpha^{m+1}$ for some $m \in \{1, 2, \ldots\}$. By Theorem 9.26, $\frac{1}{\alpha^m}$ is also a solution to the Pell equation $x^2 - Ny^2 = 1$. Using Theorem 9.27, we see that $\alpha^m \cdot \frac{1}{\alpha^m}$, $\beta \cdot \frac{1}{\alpha^m}$, and $\alpha^{m+1} \cdot \frac{1}{\alpha^m}$ are also solutions to the Pell equation $x^2 - Ny^2 = 1$. Hence, we have $1 < \frac{\beta}{\alpha^m} < \alpha$ where $\frac{\beta}{\alpha^m}$ is a solution. To get the contradiction, we need to show that the solution $\gamma := \frac{\beta}{\alpha^m}$ belongs to A, as this will contradict the minimality of α. We claim that any solution $\gamma = p + q\sqrt{N}$ that satisfies $\gamma > 1$ will have $p > 0$ and $q > 0$. Indeed, notice that since $(p + q\sqrt{N})(p - q\sqrt{N}) = p^2 - Nq^2 = 1$, we have that $p + q\sqrt{N} > 1 \Rightarrow p - q\sqrt{N} < 1 \Rightarrow q > 0$ since $\sqrt{N} > 0$. But then $p^2 - Nq^2 = 1 \Rightarrow p > q$ so that $p > q > 0$. Thus, $1 < \frac{\beta}{\alpha^m} \Rightarrow \frac{\beta}{\alpha^m}$ gives a positive solution to $x^2 - Ny^2 = 1 \Rightarrow \frac{\beta}{\alpha^m} \in A$. This is a contradiction since $\frac{\beta}{\alpha^m} < \alpha$. Thus, every element is of the form α^k for some $k = 1, 2, \ldots$.

□

10 The Search for Primes

Is it prime?

Exercise 10.1. *If n is a d-digit number, explain why the trial division primality test requires roughly $10^{d/2}$ trials.*

Suppose that n is a d-digit number. Then there are roughly 10^d numbers that are less than or equal to n. Since we only need to test up to $\sqrt{n}$ if we're using trial division, there are $\sqrt{10^d} = 10^{d/2}$ trials to run.

Exercise 10.2. *If n is a d-digit number, explain why the Wilson's Theorem primality test requires roughly 10^d multiplications.*

If n is a d-digit number, then there are roughly 10^d numbers less than n. Since we need to multiply all numbers up to (but not including) n in order to compute $(n-1)!$, we will need to carry out 10^d multiplications.

Question 10.3. *Suppose that Algorithm A requires d^2 steps and Algorithm B requires 2^d steps, where d is the number of digits in the number to be tested. Suppose our computer can carry out one million steps per second. How long would it take for our computer to carry out each algorithm when the number to be tested has 200 digits?*

Answer. We have that Algorithm A requires d^2 steps, and Algorithm B requires 2^d, with our computer capable of performing 10^6 steps per second. If $d = 200$, then for A, we have:

$$t_a = (200 \text{ steps})^2 / \frac{10^6 \text{ steps}}{1s} = 4 \times 10^{-2}\ s$$

and for B we have:

$$t_b = 2^{200} \text{ steps} / \frac{10^6 \text{ steps}}{1s} \approx 1.6069 \times 10^{54}$$

and we see that Algorithm A is faster by 56 orders of magnitude!

Fermat's Little Theorem and probable primes

Exercise 10.4. *Show that the algorithm described in Question 3.6 for computing $a^r \pmod{n}$ is a polynomial time algorithm in the number of digits in r.*

We already know from Question 3.6 that computing $a^r \pmod{n}$ requires $\log_2 r$ steps. Suppose that r is expressed in base 10 as the string

$$r = d_k d_{k-1} \dots d_1 d_0$$

Then in base 10,

$$r = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0$$

Observe that

$$a^r = a^{d_k 10^k} a^{d_{k-1} 10^{k-1}} \dots a^{d_1 10} a^{d_0}$$

And since each $a^{d_i 10^i}$ takes $\log_2(d_i 10^i) = i \log_2(1) + \log_2(d_i)$ steps to compute, a^r will take $m_1 + m_2 + \cdots + m_k$ steps to compute. Hence, in total we have $\sum_{i=0}^{k}(i \log_2(1) + \log_2(d_i))$ computations to carry out, which shows that computing $a^r \pmod{n}$ is a polynomial time algorithm.

Exercise 10.5. *State the contrapositive of Fermat's Little Theorem.*

Let $p \in \mathbb{N}$. If $\exists a \in \mathbb{N}$ with $a < p$ such that $a^{p-1} \not\equiv 1 \pmod{p}$, then p is not prime.

Exercise 10.6. *Use Fermat's Little Theorem to show that $n = 737$ is composite.*

We can verify this with $a = 2$. Observe,

$$\begin{aligned}
2 \pmod{737} = 2 \pmod{737} &= 2 \\
\Rightarrow 2^2 \pmod{737} = 4 \pmod{737} &= 4 \\
\Rightarrow 2^4 \pmod{737} = 16 \pmod{737} &= 16 \\
\Rightarrow 2^8 \pmod{737} = 256 \pmod{737} &= 256 \\
\Rightarrow 2^{16} \pmod{737} = 65536 \pmod{737} &= 680 \\
\Rightarrow 2^{32} \pmod{737} = 462400 \pmod{737} &= 301 \\
\Rightarrow 2^{64} \pmod{737} = 90601 \pmod{737} &= 687 \\
\Rightarrow 2^{128} \pmod{737} = 471969 \pmod{737} &= 289 \\
\Rightarrow 2^{256} \pmod{737} = 83521 \pmod{737} &= 240 \\
\Rightarrow 2^{512} \pmod{737} = 57600 \pmod{737} &= 114
\end{aligned}$$

And since $737 = 512 + 128 + 64 + 32 + 1$, we have

$$\begin{aligned}
2^{737-1} \pmod{737} &= 2^{512} 2^{128} 2^{64} 2^{32} \pmod{737} \\
&= (114)(289)(687)(301) \pmod{737} \\
&= 86 \neq 1
\end{aligned}$$

Hence, 737 is composite.

Question 10.7. *State the converse to Fermat's Little Theorem. Do you think the converse to Fermat's Little Theorem is true?*

Answer. The converse is:
Let $p \in \mathbb{N}$. If $a^{p-1} \equiv 1 \pmod{p}$ $\forall a \in \mathbb{N}$ with $a < p$, then p is a prime.

I think that this is true. If n is composite, then there must be some integer less than, say c such that $c | n \Rightarrow c^{n-1} \equiv 0 \pmod{n}$. But we are assuming that $c^{n-1} \equiv 1 \pmod{n}$, and $1 \equiv 0 \pmod{n}$ is a contradiction for any $n > 1$. Thus, n is prime.

Theorem 10.8. *Let n be a natural number greater than 1. Then n is prime if and only if $a^{n-1} \equiv 1 \pmod{n}$ for all natural numbers a less than n.*

Proof. Let $n \in \mathbb{N}$ with $n > 1$.

($\Rightarrow$) If n is prime, then this is just Fermat's Little Theorem, and it follows that $a^{n-1} \equiv 1 \pmod{n}$ $\forall a \in \mathbb{N}$ with $a < n$.

($\Leftarrow$) Suppose that $a^{n-1} \equiv 1 \pmod{n}$ $\forall a \in \mathbb{N}$ with $a < n$. By way of contradiction, suppose that n is composite. Then $\exists k \in \mathbb{N}$ with $k < n$ such that $k|n \Rightarrow k \equiv 0 \pmod{n} \Rightarrow k^{n-1} \equiv 0 \pmod{n}$. By assumption, however, we also have that $k^{n-1} \equiv 1 \pmod{n}$ so that $1 \equiv 0 \pmod{n}$. This is a contradiction for any $n > 1$. Hence, n is prime.

□

Question 10.9. *Does the previous theorem give a polynomial or exponential time primality test?*

Answer. From exercise 10.4, we know that computing $a^{n-1} \pmod{n}$ for a single value of a is done in polynomial time. Notice, however, that as we increase the number of digits in n by 1, we have approximately 10 times more numbers a that we need to test. Hence, Theorem 10.8 gives an exponential time primality test.

Exercise 10.10. *Compute $2^{n-1} \pmod{n}$ for all odd numbers n less than 100. If you have access to a computer, and some computing software, keep going. Test any conjectures you make along the way. State a probable prime test based on your observations.*

We use the following Python code to compute $2^{n-1} \pmod{n}$ for the first 100 naturals. We also include whether n is prime or composite:

```
n_max = 100

def is_prime(n):
    primes = [2]
    for i in range(3, n + 1):
        div = all([i % p for p in primes])
        if div:
            primes.append(i)
    if n in primes:
        return True
    else:
        return False

result = []
for n in range(1,n_max + 1):
    mod = 2 ** (n - 1) % n
    line = ”%i␣&␣%i␣&␣” % (n,mod)
    n_class = is_prime(n)
    if n_class:
        n_class = ”True”
    else:
        n_class = ”False”
    line += n_class
    result.append(line)

for s1, s2 in zip(result[0:(n_max//2)], result[(n_max//2):]):
    print(s1 + ”␣&␣” + s2 + ”␣\\\␣”)
```

The result is the following table:

n	2^{n-1} (mod n)	n is prime	n	2^{n-1} (mod n)	n is prime
1	0	False	51	4	False
2	0	True	52	8	False
3	1	True	53	1	True
4	0	False	54	14	False
5	1	True	55	49	False
6	2	False	56	16	False
7	1	True	57	4	False
8	0	False	58	2	False
9	4	False	59	1	True
10	2	False	60	8	False
11	1	True	61	1	True
12	8	False	62	2	False
13	1	True	63	4	False
14	2	False	64	0	False
15	4	False	65	16	False
16	0	False	66	32	False
17	1	True	67	1	True
18	14	False	68	8	False
19	1	True	69	4	False
20	8	False	70	22	False
21	4	False	71	1	True
22	2	False	72	32	False
23	1	True	73	1	True
24	8	False	74	2	False
25	16	False	75	34	False
26	2	False	76	8	False
27	13	False	77	9	False
28	8	False	78	32	False

29	1	True	79	1	True
30	2	False	80	48	False
31	1	True	81	40	False
32	0	False	82	2	False
33	4	False	83	1	True
34	2	False	84	32	False
35	9	False	85	16	False
36	32	False	86	2	False
37	1	True	87	4	False
38	2	False	88	40	False
39	4	False	89	1	True
40	8	False	90	32	False
41	1	True	91	64	False
42	32	False	92	8	False
43	1	True	93	4	False
44	8	False	94	2	False
45	31	False	95	54	False
46	2	False	96	32	False
47	1	True	97	1	True
48	32	False	98	58	False
49	15	False	99	58	False
50	12	False	100	88	False

Based on this, it looks like if $2^{n-1} \pmod{n} = 1$, then n is prime, and if $2^{n-1} \pmod{n}$ is anything else then n is composite. In order to test this conjecture, we use the following Python code on all natural numbers up to 1000:

```
n_max = 1000

def is_prime(n):
        primes = [2]
        for i in range(3, n + 1):
                div = all([i % p for p in primes])
                if div:
                        primes.append(i)
        if n in primes:
                return True
        else:
                return False

fail = []
for n in range(1,n_max + 1):
        if is_prime(n) and (2 ** (n - 1) % n) != 1:
```

```
        fail.append(n)
    elif not is_prime(n) and (2 ** (n - 1) % n) == 1:
        fail.append(n)
print(fail)
```

Of the first 1000 natural numbers, only $2, 341, 561$, and 645 fail this test. That gives us a $996/1000 = 99.6\%$ probability of success if we are using this test on the first 1000 naturals.

AKS primality

Theorem 10.11. *Let a and n be relatively prime natural numbers. Then n is prime if and only if $(x+a)^n \equiv x^n + a \pmod{n}$ for every integer x.*

Proof. Let $, n \in \mathbb{N}$ with $(a, n) = 1$.

($\Rightarrow$) Suppose that n is prime. Recall from the Binomial Theorem that $\forall x \in \mathbb{Z}$,

$$(x+a)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} a^i$$

We also have from Lemma 4.25 that since n is prime, $n | \binom{n}{i}$ $\forall 0 < i < n$. Hence, $\binom{n}{i} \equiv 0 \pmod{n} \Rightarrow \binom{n}{i} x^{n-i} a^i \equiv 0 \pmod{n}$ so that the only non-zero terms in the expansion of $(x+a)^n$ are the terms corresponding to $i = 0$ and $i = n$. That is, we have

$$(x+a)^n \equiv x^n + a^n \pmod{n}$$

But then by Fermat's Little Theorem, $a^n \equiv a \pmod{n} \Rightarrow x^n + a^n \equiv x^n + a \pmod{n}$ so that

$$(x+a)^n \equiv x^n + a \pmod{n}$$

as desired.

($\Leftarrow$) Suppose that $\forall x \in \mathbb{Z}$, we have $(x+a)^n \equiv x^n + a \pmod{n}$. Once again, By the Binomial Theorem, we know that we must have $\binom{n}{i} \equiv 0 \pmod{n}$ $\forall 0 < i < n$. Suppose by way of contradiction that n is composite. Then $\exists$ a prime $p \in \mathbb{N}$ such that $n = p^r k$ for some $r, k \in \mathbb{N}$ with $(p, k) = 1$ (that is, r is the number of factors of p that n has). Then $0 < p^r < n$, and we must have $p^r | \binom{n}{p^r}$ since $n | \binom{n}{p^r}$. Notice, however, that

$$\binom{n}{p^r} = \frac{n(n-1)(n-2)\ldots(n-p^r+1)}{p^r!}$$

and since all the factors of p in $n(n-1)(n-2)\ldots(n-p^r+1)$ are accounted for by $p^r!$ since we have at least $1 + 2 + \cdots + r = \frac{(r+1)r}{2}$ factors of p in $p!$. This contradicts $p^r | \binom{n}{p^r}$. Hence, n is prime.

□