1 Solutions

1.1 Chapter 1

1.1.1

(a) Is a subset of $\mathbb{Z}^+$ and therefore is well-ordered.

(b) There is no least element so the set is not well-ordered.

(c) Consider the set $\left\{a \,\middle|\, a \in \mathbb{Z}, a \geq 10\right\}$, it is apparent that this is a subset of $\mathbb{Z}^+$ and therefore is well-ordered. So the set $\left\{\frac{a}{2} \,\middle|\, a \in \mathbb{Z}, a \geq 10\right\}$ is also well-ordered because it holds a least element ($\frac{10}{5}$).

(d) There is no least element so the set is not well-ordered.

1.1.2

Since S is a subset of $\mathbb{Z}^+$ by well-ordering we know that S has a least element, and because $k \in \mathbb{Z}$, k can be 0 and therefore there is no most element.

1.1.3

Proof. Suppose $\sqrt{5}$ is rational and is of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ and $b \neq 0$. Consider the set S,

$$S = \left\{k \mid k, k\sqrt{5} \in \mathbb{Z}^+\right\}$$

We know that S is a subset of $\mathbb{Z}^+$ and that $b \in S$, by well-ordering this implies that S has a least element. Let l be the least element in S.
Consider the properties of l' where $l' = l\sqrt{5} - 2l$,

- $l' = l\sqrt{5} - 2l = l(\sqrt{5} - 2) \implies 0 < l' < l$.
- Since $l \in S$ and $S \subset \mathbb{Z}^+$, both l and $l\sqrt{5} \in \mathbb{Z}^+$ which implies $l' \in \mathbb{Z}^+$.
- Since $l \in \mathbb{Z}^+$ we have $5l \in \mathbb{Z}^+$ and since $l\sqrt{5} \in \mathbb{Z}^+$ we have $l'\sqrt{5} = (l\sqrt{5} - 2l)\sqrt{5} = 5l - 2l\sqrt{5} \in \mathbb{Z}^+$.

It follows that $l' \in S$ but $l' < l$ which contradicts l being the least element in S. □

1.1.4

(a)

$$\begin{aligned}\sum_{k=2}^{10}\frac{1}{k^2-1} &= \sum_{k=2}^{10}\frac{1}{2}\left(\frac{1}{k-1}-\frac{1}{k+1}\right)=\frac{1}{2}\sum_{k=2}^{10}\left(\frac{1}{k-1}-\frac{1}{k+1}\right)\\ &= \frac{1}{2}\left[\left(\frac{1}{1}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{8}-\frac{1}{10}\right)+\left(\frac{1}{9}-\frac{1}{11}\right)\right]\\ &= \frac{1}{2}\left[\frac{1}{1}+\frac{1}{2}-\frac{1}{10}-\frac{1}{11}\right]\\ &= \frac{1}{2}\left(\frac{72}{55}\right)=\frac{36}{55}\end{aligned}$$

(b)

$$\sum_{k=2}^{n}\frac{1}{k^2-1}=\frac{1}{2}\left[\frac{1}{1}+\frac{1}{2}-\frac{1}{n}-\frac{1}{n+1}\right]$$

(c)

$$\sum_{k=1}^{n}\frac{1}{k^2+2k}=\sum_{k=1}^{n}\frac{1}{(k+1)^2-1}=\sum_{k=2}^{n+1}\frac{1}{k^2-1}$$

$$\sum_{k=2}^{n+1}\frac{1}{k^2-1}=\frac{1}{2}\left[\frac{1}{1}+\frac{1}{2}-\frac{1}{n+1}-\frac{1}{n+2}\right]$$

1.1.5

(a) $\prod_{j=2}^{7}\left(1-\frac{1}{j}\right)=\left[\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{4}\cdot\frac{4}{5}\cdot\frac{5}{6}\cdot\frac{6}{7}\right]=\frac{1}{7}$

(b) $\prod_{j=2}^{n}\left(1-\frac{1}{j}\right)=\frac{1}{n}$

(c) $\prod_{j=2}^{n}\left(1-\frac{1}{j^2}\right)=\frac{n+1}{2n}$

1.1.6

Proof.

Base Case:

Let $n=1$, $\sum_{j=1}^{1} j(j+1)=2$ and $\frac{1(1+1)(1+2)}{3}=2$, so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some n.
This implies that $\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$.

Inductive Step:

Then consider the sum to $n+1$:

$$\begin{aligned}\sum_{j=1}^{n+1} j(j+1) &= \sum_{j=1}^{n} j(j+1) + (n+1)((n+1)+1) \\ &= \left[\frac{n(n+1)(n+2)}{3}\right] + (n+1)((n+1)+1) \text{ by IH} \\ &= \frac{1}{3}\left(n(n+1)(n+2) + 3(n+1)(n+2)\right) \\ &= \frac{1}{3}\left(n^3+3n^2+2n+3n^2+9n+6\right) \\ &= \frac{1}{3}\left(n^3+6n^2+11n+6\right) \\ &= \frac{1}{3}\left((n+1)(n+2)(n+3)\right)\end{aligned}$$

Thus for all $n \geq 1$,

$$\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$$

□

1.1.7

Proof.

Base Case:

Rewrite the statement $f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}$ to be $f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$.
Let $n = 1$, $f_1 f_{1+2} - f_{1+1}^2 = 1 \cdot 2 - 1 = 1$ and $(-1)^{1+1} = 1$, so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some n.
This implies that $f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$

Inductive Step:

Then consider the equation to $n+1$:

$$\begin{aligned}
f_{(n+1)}f_{(n+1)+2} - f_{(n+1)+1}^2 &= f_{n+1}f_{n+3} - f_{n+2}^2 \\
&= f_{n+1}\left(f_{n+1} + f_{n+2}\right) - f_{n+2}^2 \\
&= f_{n+1}^2 + f_{n+1}f_{n+2} - f_{n+2}^2 \\
&= f_{n+1}^2 + f_{n+2}\left(f_{n+1} - f_{n+2}\right) \\
&= f_{n+1}^2 + f_{n+2}\left(-f_n\right) \\
&= -\left(f_n f_{n+2} - f_{n+1}^2\right) \\
&= -(-1)^{n+1} \quad \text{by IH} \\
&= (-1)^{n+2}
\end{aligned}$$

Thus for all $n \geq 1$,

$$f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$$

□

1.1.8

Proof.

Base Case:

Let $n = 1$, $2^1 \times 2^1$ is a 2×2 chessboard with a corner missing and can be tiled by one tromino, so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some n. This implies that any $2^n \times 2^n$ chessboard with a corner missing can be tiled with trominoes.

Inductive Step:

Then consider a $2^{n+1} \times 2^{n+1}$ chessboard.

- Divide the $2^{n+1} \times 2^{n+1}$ chessboard into four quadrants of size $2^n \times 2^n$.
- By the Inductive Hypothesis we know that each $2^n \times 2^n$ has one corner missing.
- There are then four empty squares in the $2^{n+1} \times 2^{n+1}$ board.
- Rotate each quadrant such that the four empty squares are in the center of the board.
- Add another tromino into the board leaving only one empty square.
- Rotate the quadrant with the empty square such that the empty square is in the corner of the board.

- Therefore the $2^{n+1} \times 2^{n+1}$ chessboard can be tiled by trominoes with a corner missing.

Thus, every $2^n \times 2^n$ chessboard with a corner missing can be tiled with trominoes.

□

1.1.9

Proof.

Base Case:

Let $n = 1$, $H_{2^1} = \sum_{j=1}^{2^n} \frac{1}{j} = \frac{3}{2}$ and $\frac{3}{2} \leq 2$, so the base case is valid.

Inductive Hypothesis:

Assume from the inductive hypothesis that the conclusion is true for some n.
This implies that $\sum_{j=1}^{2^n} \frac{1}{j} \leq 1 + n$.

Inductive Step:

Then consider the equation to $n + 1$:

$$\begin{aligned}
H_{2^{n+1}} &= \sum_{j=1}^{2^{n+1}} \frac{1}{j} \\
&= \sum_{j=1}^{2^n} \frac{1}{j} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} \\
&\leq [1+n] + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} \qquad \text{by IH} \\
&\leq [1+n] + \frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}} \\
&\leq [1+n] + 2^n \cdot \frac{1}{2^{n+1}} \\
&\leq \frac{3}{2} + n \leq 2 + n
\end{aligned}$$

Thus for all $n \geq 1$,

$$H_{2^n} \leq 1 + n$$

□

1.1.10

Proof.

Inductive Step:

Assume we can do $54, \cdots, k$. Because $k-6$ is in the $54, \cdots, k$ we can do $k-6$ then add a 7-cent stamp. $k-6$ is in $54, \cdots, k$ only if $k-6 \geq 54 \equiv k \geq 60$. Thus, the inductive step is only valid for $k = 60, 61, \cdots$ to get to the next $k+1$.

Base Case:

Must do $54, 55, 56, 57, 58, 59, 60$ as base cases.

$$\begin{aligned}
54 &= 2(\text{7-cent}) + 4(\text{10-cent}) \\
55 &= 5(\text{7-cent}) + 2(\text{10-cent}) \\
56 &= 8(\text{7-cent}) \\
57 &= 1(\text{7-cent}) + 5(\text{10-cent}) \\
58 &= 4(\text{7-cent}) + 3(\text{10-cent}) \\
59 &= 7(\text{7-cent}) + 1(\text{10-cent}) \\
60 &= 6(\text{10-cent})
\end{aligned}$$

□

1.3 Chapter 3

---

1. Use the Euclidean Algorithm to calculate $d = \gcd(510, 140)$ and then use the result to find α and β so that $d = 510\alpha + 140\beta$. $\boxed{10/10}$

   Need to find $\gcd(510, 140)$.

$$\begin{aligned}
510 &= 3(140) + 90 \\
140 &= 1(90) + 50 \\
90 &= 1(50) + 40 \\
50 &= 1(40) + 10 \\
40 &= 4(10) + 0
\end{aligned}$$

So the gcd is 10. Now to find the linear combination.

$$\begin{aligned}10 &= 1(50) - 1(40)\\ &= 1(50) - 1(90 - 1(50))\\ &= 2(50) - 1(90)\\ &= 2(140 - 1(90)) - 1(90)\\ &= 2(140) - 3(90)\\ &= 2(140) - 3(510 - 3(140))\\ &= -3(510) + 11(140)\\ &= \alpha a + \beta b\end{aligned}$$

where $\alpha = -3$ and $\beta = 11$.

2. Use the Euclidean Algorithm to show that if $k \in \mathbb{Z}^+$ that $3k+2$ and $5k+3$ are relatively prime. $\boxed{8/10}$

   Need to show that $\gcd(3k+2, 5k+3) = 1$ for all $k \in \mathbb{Z}^+$.

$$\begin{aligned}5k+3 &= 1(3k+2) + (2k+1)\\ 3k+2 &= 1(2k+1) + (k+1)\\ 2k+1 &= 1(k+1) + k\\ k+1 &= 1(k) + 1\end{aligned}$$

   So the $\gcd(3k+2, 5k+3) = 1$, therefore $3k+2$ and $5k+3$ are relatively prime.

3. How many zeros are there at the end of (1000!)? Do not do this by brute force. Explain your method. $\boxed{10/10}$

   Zeros at the end of numbers are from multiples of 10 which are pairs of 2 and 5, so we find the number of pairs of 2's and 5's to find the number of zeros. Let $d_n(x)$ represent the sum of the numbers divisible by all powers of n less than x.

$$d_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$$

$$d_5(1000!) = 200 + 40 + 8 + 1 = 249$$

   Thus, there can only be 249 pairs of 2's and 5's, so there are only 249 10's, so there are 249 zeros at the end of (1000!).

4. Let $a = 1038180$ and $b = 92950$. First find the prime factorizations of a and b. Then use these to calculate $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$. $\boxed{10/10}$

Find the prime factorization of a.

$$\begin{aligned}1038180 &= 2^2(259545)\\ &= 2^2 3^1(86515)\\ &= 2^2 3^1 5^1(17303)\\ &= 2^2 3^1 5^1 11^3(13)\\ &= 2^2 3^1 5^1 11^3 13^1\end{aligned}$$

Find the prime factorization of b.

$$\begin{aligned}92950 &= 2^1(46475)\\ &= 2^1 5^2(1859)\\ &= 2^1 5^2 11^1(169)\\ &= 2^1 5^2 11^1 13^2\end{aligned}$$

Now, to find the $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

$$\gcd(a, b) = \gcd(2^2 3^1 5^1 11^3 13^1, 2^1 5^2 11^1 13^2) = 2^1 5^1 11^1 13^1 = 1430$$

$$\operatorname{lcm}(a, b) = \operatorname{lcm}(2^2 3^1 5^1 11^3 13^1, 2^1 5^2 11^1 13^2) = 2^2 3^1 5^2 11^3 13^2 = 67481700$$

5. Which pairs of integers have gcd of 18 and lcm of 540? Explain. $\boxed{10/10}$

Find the prime factorization of 18.

$$\begin{aligned}18 &= 2^1(9)\\ &= 2^1 3^2\end{aligned}$$

Find the prime factorization of 540.

$$\begin{aligned}540 &= 2^2(135)\\ &= 2^2 3^3(5)\\ &= 2^2 3^3 5^1\end{aligned}$$

From the prime factors of 18 and 540 we know that $x = 2^a 3^b 5^c$ and $y = 2^e 3^f 5^g$. The gcd is the minimum power of common prime factors, similarly the lcm is the maximum power of common prime factors. Therefore, the list of all possible pairs of integers is:

$$\begin{aligned}x &= 2^1 3^2 5^0, y = 2^2 3^3 5^1\\ x &= 2^1 3^3 5^0, y = 2^2 3^2 5^1\\ x &= 2^2 3^2 5^0, y = 2^1 3^3 5^1\\ x &= 2^2 3^3 5^0, y = 2^1 3^2 5^1\end{aligned}$$

6. Suppose that $a \in \mathbb{Z}$ is a perfect square divisible by at least two distinct primes. Show that a has at least seven distinct factors. $\boxed{5/10}$

   Since a is a perfect square it can be represented by the form $a = b^2$, and since a has at *least* 2 prime factors we can say that $b = p_1^{\alpha} p_2^{\beta}$. It follows that $a = p_1^{2\alpha} p_2^{2\beta}$. Therefore a has factors $1, p_1, p_2, p_1, p_2, p_1^2, p_2^2, a$.

7. Show that if $a, b \in \mathbb{Z}^+$ with $a^3 \Big| b^2$ then $a \Big| b$. $\boxed{10/10}$

   Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$. Since $a^3 \mid b^2$ we know that,

   $$p_1^{3\alpha_1} p_2^{3\alpha_2} \cdots p_n^{3\alpha_n} \Big| p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_n^{2\beta_n}$$

   Therefore, $3\alpha_n \leq 2\beta_n$. Now to show $a \mid b$ we need to show that $\alpha \leq \beta$.

   $$3\alpha \leq 2\beta \implies \alpha \leq \frac{2\beta}{3} \leq \beta$$

   Thus, if $a^3 \mid b^2$ then $a \mid b$.

8. For which positive integers m is each of the following statements true: $\boxed{6/10}$

   (a) $34 \equiv 10 \mod m$

   $$m = 12, 24$$

   (b) $1000 \equiv 1 \mod m$

   $$m = 3, 9, 27, 37, 111, 333, 999$$

   (c) $100 \equiv 0 \mod m$

   $$m = 1, 2, 4, 5, 10, 20, 25, 50, 100$$

1.4 Chapter 4

1. Calculate the least positive residues modulo 47 of each of the following with justification:

   (a) 2^{543}

   Using binary expansion we see that $2^1 \equiv 2 \text{ mod } 47$, $2^2 \equiv 4 \text{ mod } 47$, $2^4 \equiv 16 \text{ mod } 47$, $2^8 \equiv 21 \text{ mod } 47$, $2^{16} \equiv 18 \text{ mod } 47$, $2^{32} \equiv 42 \text{ mod } 47$, $2^{64} \equiv 25 \text{ mod } 47$, $2^{128} \equiv 14 \text{ mod } 47$, $2^{256} \equiv 8 \text{ mod } 47$, and $2^{512} \equiv$

17 mod 47.
Then $543 = 512 + 16 + 8 + 4 + 2 + 1$ so,

$$\begin{aligned} 2^{543} = 2^{512}2^{16}2^{8}2^{4}2^{2}2^{1} \equiv & \\ & \equiv 17 \cdot 18 \cdot 21 \cdot 16 \cdot 4 \cdot 2 \bmod 47 \\ & \equiv 822528 \bmod 47 \\ & \equiv 28 \bmod 47 \end{aligned}$$

So 28 is the least non-negative residue.

(b) 32^{932}

Using binary expansion we see that $32^1 \equiv 32 \bmod 47$, $32^2 \equiv 37 \bmod 47$, $32^4 \equiv 6 \bmod 47$, $32^8 \equiv 47 \bmod 47$, $32^{16} \equiv 27 \bmod 47$, $32^{32} \equiv 24 \bmod 47$, $32^{64} \equiv 12 \bmod 47$, $32^{128} \equiv 3 \bmod 47$, $32^{256} \equiv 9$, and $32^{512} \equiv 34$. Then $932 = 512 + 256 + 128 + 32 + 4$ so,

$$\begin{aligned} 32^{932} = 32^{512}32^{256}32^{128}32^{32}32^{4} \equiv & \\ & \equiv 34 \cdot 9 \cdot 3 \cdot 24 \cdot 6 \bmod 47 \\ & \equiv 132192 \bmod 47 \\ & \equiv 28 \bmod 47 \end{aligned}$$

So 28 is the least non-negative residue.

(c) $46^{327349287323}$

Since $46 \equiv -1 \bmod 47$ we know $46^{327349287323} \equiv (-1)^{327349287323}$. We also know $2 \nmid 327349287323$ so $(-1)^{327349287323} \equiv (-1)^1 \equiv -1 \equiv 46 \bmod 47$. So 46 is the least non-negative residue.

2. Exhibit a complete set of residues mod 17 composed entirely of multiples of 3.

   Let $S = \{0, 1, 2, \cdots, 16\}$ be the set of residues mod 17. Because $\gcd(3, 17) = 1$ the set consisting of only multiples of 3 would be,

$$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48\}$$

3. Show that if $a, b, m \in \mathbb{Z}$ with $m > 0$ and if $a \equiv b \bmod m$ then $\gcd(a, m) = \gcd(b, m)$.

   If $a \equiv b \bmod m$ then $\exists x \in \mathbb{Z}$ such that $a = b + xm$. So $\gcd(a, m) = \gcd(b + xm, m) = \gcd(b, m)$.

4. Suppose p is prime and $x \in \mathbb{Z}$ satisfies $x^2 \equiv x \bmod p$. Prove that $x \equiv 0 \bmod p$ or $x \equiv 1 \bmod p$. Show with a counterexample that this fails if p is not prime.

Because $x^2 \equiv x \bmod p$ we know that $x^2 - x \equiv 0 \bmod p$, which is the same as $x(x-1) \equiv 0 \bmod p$. This implies that either $p \mid x$, $p \mid (x-1)$, or both.

$$p \mid x \implies x \equiv 0 \bmod p$$

$$p \mid (x-1) \implies x \equiv 1 \bmod p$$

If p is not prime, say $p = 6$ we see,

$$3^2 \equiv 3 \bmod 6$$

Where $3 \not\equiv 0 \bmod 6$ and $3 \not\equiv 1 \bmod 6$. So p must be prime for the statement to hold true.

5. Show that if n is an odd positive integer or if n is a positive integer divisible by 4 that:

$$1^3 + 2^3 + ... + (n-1)^3 \equiv 0 \bmod n$$

There are two cases to look at, when n is an odd positive integer and when n is divisible by 4.

- If n is an odd positive integer then $n-1$ is even so we have an even amount of numbers. Consider the set $S = \{1^3, 2^3, \cdots, (n-1)^3\}$. Then consider two subsets of S, both with $(n-1)/2$ elements S_1 and S_2, where

$$\sum S = \sum S_1 + \sum S_2 = 1^3 + 2^3 + \cdots + (n-1)^3$$

The set $S_1 = \{1^3, 2^3, 3^3, \cdots\}$ and the set $S_2 = \{\cdots, (n-3)^3, (n-2)^3, (n-1)^3\}$. Because we know that $a - b \equiv -b \bmod a$ we also know that $(a-b)^3 \equiv (-b)^3 \bmod a$. So we can say that for all elements in $S_2 \bmod n$, $S_2 = \{\cdots, (-3)^3, (-2)^3, (-1)^n\}$. Now if we look at $\sum S_1 + \sum S_2 \bmod n$ we see that the first element of S_1 is cancelled out by the last element of S_2 and so forth until there are no elements left. Thus, $1^3 + 2^3 + ... + (n-1)^3 \equiv 0 \bmod n$.

- If n is divisble by 4 then $n-1$ is odd so we have an odd amount of numbers. Consider the set $S = \{1^3, 2^3, \cdots, (n-1)^3\}$. Then consider two subsets of S, both with $(n-1)/2 - 1$ elements S_1 and S_2, where

$$\sum S = \sum S_1 + \left(\frac{n}{2}\right)^3 + \sum S_2 = 1^3 + 2^3 + \cdots + (n-1)^3$$

The set $S_1 = \{1^3, 2^3, 3^3, \cdots\}$ and the set $S_2 = \{\cdots, (n-3)^3, (n-2)^3, (n-1)^3\}$. Because we know that $a - b \equiv -b \bmod a$ we also know that $(a-b)^3 \equiv (-b)^3 \bmod a$. So we can say that for all elements in $S_2 \bmod n$, $S_2 = \{\cdots, (-3)^3, (-2)^3, (-1)^n\}$. Now if we look at

$\sum S$ mod n, like in the case above we can see that sets S_1 and S_2 will cancel one another out. This leaves us with

$$1^3 + 2^3 + ... + (n-1)^3 \equiv \left(\frac{n}{2}\right)^3 \text{ mod } n$$

Because we know that $4 \mid n$ we know that $n = 4x$ for some $x \in \mathbb{Z}$. It follows that,

$$\left(\frac{n}{2}\right)^3 = \frac{n^3}{8} = \frac{64x^3}{8} = 8x^3 = (2x^2)n$$

So

$$\left(\frac{n^3}{2}\right)^3 \equiv (2x^2)n \equiv 0 \text{ mod } n$$

Thus, $1^3 + 2^3 + ... + (n-1)^3 \equiv 0$ mod n.

6. Find all solutions (mod the given value) to each of the following.

   (a) $10x \equiv 25$ mod 75

   Because the gcd$(10, 75) = 5$ and $5 \mid 25$ we know that solutions exist. Let $x_0 \equiv 10$ mod 75, so all solutions are then

   $$x \equiv 10 + k \cdot \frac{75}{\text{gcd}(10, 75)} \text{ mod } 75, \text{ for } k = 0, 1, 2, 3, 4$$

   $$x \equiv 10 + 15k \text{ mod } 75, \text{ for } k = 0, 1, 2, 3, 4$$

   Therefore, $x \equiv 10, 25, 40, 55, 70$.

   (b) $9x \equiv 8$ mod 12

   Because the gcd$(9, 12) = 3$ and $3 \nmid 8$ so there are no solutions.

7. Solve each of the following linear congruences using inverses.

   (a) $3x \equiv 5$ mod 17

   Since 6 is the inverse of 3 mod 17 we get, $6 \cdot 3x \equiv 6 \cdot 5$ mod 17 which implies

   $$x \equiv 30 \text{ mod } 17 \equiv 13 \text{ mod } 17$$

   Therefore, $x \equiv 13$.

   (b) $10x \equiv 3$ mod 11

   Since 10 is the inverse of 10 mod 11 we get, $10 \cdot 10x \equiv 10 \cdot 3$ mod 11 which implies

   $$x \equiv 30 \text{ mod } 11 \equiv 8 \text{ mod } 11$$

   Therefore, $x \equiv 8$.

8. What could the prime factorization of m look like so that $6x \equiv 10 \bmod m$ has at least one solution? Explain.

   In order for $ax \equiv b \bmod m$ to have a solution(s), $\gcd(a, m) \mid b$. So in the context of this problem we have that $\gcd(6, m) \mid 10$. We are looking for an m such that $\gcd(6, m) = 2$. One possible m could be $m = 2^1$.

9. Use the Chinese Remainder Theorem to solve:
   A troop of monkeys has a store of bananas. When they arrange them into 7 piles, none remain. When they arrange them into 10 piles there are 3 left over. When they arrange them into 11 piles there are 2 left over. What is the smallest positive number of bananas they can have? What is the second smallest positive number?

   Let x be the number of bananas, we have

$$\begin{aligned} x &\equiv 0 \bmod 7 \\ x &\equiv 3 \bmod 10 \\ x &\equiv 2 \bmod 11 \end{aligned}$$

   Test to see if all m_i are pairwise coprime, $\gcd(7, 10) = \gcd(7, 11) = \gcd(10, 11) = 1$. This means that $M = 770$, $M_1 = 110$, $M_2 = 77$, and $M_3 = 70$.

   Solve for y_1:

$$\begin{aligned} 110y_1 &\equiv 1 \bmod 7 \\ 5y_1 &\equiv 1 \bmod 7 \\ y_1 &= 3 \end{aligned}$$

   Solve for y_2:

$$\begin{aligned} 77y_2 &\equiv 1 \bmod 10 \\ 7y_2 &\equiv 1 \bmod 10 \\ y_2 &= 3 \end{aligned}$$

   Solve for y_3:

$$\begin{aligned} 70y_3 &\equiv 1 \bmod 11 \\ 4y_3 &\equiv 1 \bmod 11 \\ y_3 &= 3 \end{aligned}$$

   So we then get

$$x = (0)(110)(3) + (3)(77)(3) + (2)(70)(3) \equiv 1113 \bmod 770$$

$$x \equiv 343 \bmod 770$$

   The smallest number of bananas they can have is 343 and the second smallest is 1113.

10. Solve the system of linear congruences:

$$\begin{aligned} 2x + 1 &\equiv 3 \bmod 10 \\ x + 2 &\equiv 7 \bmod 9 \\ 4x &\equiv 1 \bmod 7 \end{aligned}$$

Rewrite the system of linear congruences to be (properties of congruences):

$$\begin{aligned} 2x &\equiv 2 \bmod 10 \\ x &\equiv 5 \bmod 9 \\ 4x &\equiv 1 \bmod 7 \end{aligned}$$

Which then becomes

$$\begin{aligned} x &\equiv 1 \bmod 5 \\ x &\equiv 5 \bmod 9 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

Then test to see if all m_i are pairwise coprime, $\gcd(5,9) = \gcd(5,7) = \gcd(7,9) = 1$. This means that $M = 315$, $M_1 = 63$, $M_2 = 35$, and $M_3 = 45$.

Solve for y_1:

$$\begin{aligned} 63y_1 &\equiv 1 \bmod 5 \\ 3y_1 &\equiv 1 \bmod 5 \\ y_1 &= 2 \end{aligned}$$

Solve for y_2:

$$\begin{aligned} 35y_2 &\equiv 1 \bmod 9 \\ 8y_2 &\equiv 1 \bmod 9 \\ y_2 &= 8 \end{aligned}$$

Solve for y_3:

$$\begin{aligned} 45y_3 &\equiv 1 \bmod 7 \\ 3y_3 &\equiv 1 \bmod 7 \\ y_3 &= 5 \end{aligned}$$

So we then get

$$x = (1)(63)(2) + (5)(35)(8) + (2)(45)(5) \equiv 1976 \bmod 315$$

$$x \equiv 86 \bmod 315$$

1.6 Chapter 6

1. Use Fermat's Little Theorem to find the least nonnegative residue of $2^{1000003} \mod 17$.

   Well $17 \nmid 2$ so $2^{16} \equiv 1 \bmod 17$. Then $1000003 = 16(62500) + 3$ so

   $$\begin{aligned} 2^{1000003} = 2^{16^{62500}} 2^3 &\equiv (1)^{62500} 2^3 \bmod 17 \\ &\equiv 2^3 \bmod 17 \\ &\equiv 8 \bmod 17 \end{aligned}$$

   So 8 is the least non-negative residue.

2. Use Fermat's Little Theorem to solve the following, giving the result as the least nonnegative residue.

   (a) $7x \equiv 12 \mod 17$

   By FLiT we know $7^{17-1} \equiv 1 \bmod 17$, it follows that $7^{16} \cdot 12 \equiv 1 \bmod 17$ therefore $7x = 7^{16} \cdot 12 = 7^{15} \cdot 12$. Then reduce $7^{15} \cdot 12 \bmod 17$. So 9 is the least non-negative residue.

   (b) $10x \equiv 13 \mod 19$

   By FLiT we know $10^{19-1} \equiv 1 \bmod 19$, it follows that $10^{18} \cdot 13 \equiv 1 \bmod 19$ therefore $10x = 10^{18} \cdot 13 = 10^{17} \cdot 13$. Then reduce $10^{17} \cdot 13 \bmod 19$. So 7 is the least non-negative residue.

3. Use Fermat's Little Theorem to show that $30 \big| (n^9 - n)$ for all positive integers n.

   Proof. Note that $30 = 2 \cdot 3 \cdot 5$, from Fermat's Little Theorem we know that $a^p \equiv a \bmod p$ when p is prime. Let,

   $$\begin{aligned} x &= (n^5 - n)(n^4 + 1) \\ y &= (n^3 - n)(n^2 + 1)(n^4 + 1) \\ z &= (n^2 - n)(n^3 + n^2 + n + 1)(n^4 + 1) \end{aligned}$$

   Note that $x = y = z = n^9 - n$. Then observe the following,

   - By FLiT $5 \mid n^5 - n \implies 5 \mid x \implies 5 \mid n^9 - n$.
   - By FLiT $3 \mid n^3 - n \implies 3 \mid y \implies 3 \mid n^9 - n$.
   - By FLiT $2 \mid n^2 - n \implies 2 \mid z \implies 2 \mid n^9 - n$.

   It follows that $2 \cdot 3 \cdot 5 \mid n^9 - n \implies 30 \mid n^9 - n$. □

4. The definition of n being a Fermat pseudoprime to base b does not actually require that $\gcd(b, n) = 1$ because it's not possible to have $b^{n-1} \equiv 1 \mod n$ with $\gcd(b, n) \neq 1$. Prove this.

   Proof. Let $\gcd(b, n) = a$ where $a \neq 1$, this implies there exists a prime p such that $p \mid b$ and $p \mid n$. It follows that there exists a linear combination of b and n such that $xb + yn = 1$ for $x, y \in \mathbb{Z}$. But if $p \mid b$ and $p \mid n$ then $p \mid xb + yn = 1 \implies p \mid 1$ but this is a contradiction to the fact that p is prime. □

5. We didn't exclude even integers from the definition of a Fermat Pseudoprime. Some books do. Show that with our definition 4 is a Fermat Pseudoprime to a certain base.

   From $5^{4-1} = 5^3 \equiv 1 \mod 4$, we see that 4 is a Fermat Pseudoprime to the base 5.

6. Prove that if n is an odd Fermat Pseudoprime to some base then it must be so to an even number of bases.

   Proof. Let n be an odd Fermat Pseudoprime, then let b be a base of n where $b^{n-1} \equiv 1 \mod n$. Because n is odd $n - 1$ is even, this means that $b^{n-1} = (-b)^{n-1}$, it follows that any base b has a pair $-b$ that is also a base as long as $-b \not\equiv b \mod n$.

   If $-b \equiv b \mod n$ then n would divide $2b$ but since n is odd this implies $n \mid b$. Then, $b^{n-1} \equiv 0 \mod n$ which contradicts $b^{n-1} \equiv 1 \mod n$.

   So it is not possible for $-b \equiv b \mod n$, therefore any base b of n has a respective pair $-b$ such that n has an even number of bases. □

7. Prove that 1105 is a Carmichael number.

   Proof. Note that $1105 = 5 \cdot 13 \cdot 17$. Suppose b satisfies $\gcd(b, 1105) = 1$. Then,

   - $\gcd(b, 5) = 1$ so by FLiT $b^4 \equiv 1 \mod 5$. So $b^{1104} = (b^4)^{276} \equiv 1 \mod 5$ so $5 \mid b^{1104} - 1$.
   - $\gcd(b, 13) = 1$ so by FLiT $b^{12} \equiv 1 \mod 13$. So $b^{1104} = (b^{12})^{92} \equiv 1 \mod 13$ so $13 \mid b^{1104} - 1$.
   - $\gcd(b, 17) = 1$ so by FLiT $b^{16} \equiv 1 \mod 17$. So $b^{1104} = (b^{16})^{69} \equiv 1 \mod 17$ so $17 \mid b^{1104} - 1$.

   So $5 \cdot 13 \cdot 17 \mid b^{1104} - 1 \implies 1105 \mid b^{1104} - 1$. Therefore $b^{1104} \equiv 1 \mod 1105$. □

8. Use Euler's Theorem to find the units digit of 7^{999999}.

   The units digit is the least non-negative residue mod 10. Since $\phi(10) = 4$ we have $7^4 \equiv 1 \bmod 10$ and so:

   $$7^{999999} = (7^4)^{249999} 7^3 \equiv 7^3 \equiv 3 \bmod 10$$

   The units digit of 7999999 is 3.

9. Solve each of the following using Euler's Theorem. Solutions should be least nonnegative residues.

   (a) $5x \equiv 3 \mod 14$

   Since $\gcd(5, 14) = 1$ then $5^{\phi(14)} \equiv 1 \bmod 14$. Then $5^6 = 5^5 \cdot 5 \equiv 1 \bmod 14$ where $5^5 \equiv 3$ is the inverse. Then $5x \equiv 3 \bmod 14$ can be reduced to $x \equiv 3 \cdot 3 \bmod 14$. So 9 is the least non-negative residue.

   (b) $4x \equiv 7 \mod 15$

   Since $\gcd(4, 15) = 1$ then $4^{\phi(15)} \equiv 1 \bmod 15$. Then $4^8 = 4^7 \cdot 4 \equiv 1 \bmod 15$ where $4^7 \equiv 4$ is the inverse. Then $4x \equiv 7 \bmod 15$ can be reduced to $x \equiv 7 \cdot 4 \bmod 15$. So 13 is the least non-negative residue.

   (c) $3x \equiv 5 \mod 16$

   Since $\gcd(3, 16) = 1$ then $3^{\phi(16)} \equiv 1 \bmod 16$. Then $3^8 = 3^7 \cdot 3 \equiv 1 \bmod 16$ where $3^7 \equiv 11$ is the inverse. Then $3x \equiv 5 \bmod 16$ can be reduced to $x \equiv 5 \cdot 11 \bmod 16$. So 7 is the least non-negative residue.

10. Prove that if $\gcd(a, 30) = 1$ then $60 \mid a^4 + 59$.

    Proof. Note that $60 = 5 \cdot 12$, because $\gcd(a, 30) = 1$ we know $\gcd(a, 5) = 1$ and $\gcd(a, 12) = 1$.

    - $a^{\phi(5)} = a^4 \equiv 1 \bmod 5$, so $5 \mid a^4 - 1$.
    - $a^{\phi(12)} = a^4 \equiv 1 \bmod 12$, so $12 \mid a^4 - 1$.

    Since $\gcd(5, 12) = 1$ it follows that $60 \mid a^4 - 1 \implies 60 \mid (a^4 - 1) + 60 \implies 60 \mid a^4 + 59$. □

1.7 Chapter 7

1. Find all n satisfying $\phi(n) = 18$.

   Suppose $p \mid n$, then $p - 1 \mid \phi(n)$ so $p - 1 = 1, 2, 3, 6, 9, 18 \implies p = 2, 3, 4, 7, 10, 19$. But 4 and 10 are not prime so $p = 2, 3, 7, 19$. Therefore $n = 2^\alpha 3^\beta 7^\gamma 19^\delta$ for some α, β, γ, and δ. Then,

- If $2^\alpha \mid n$ with $\alpha > 0$ then $2^{\alpha-1} \mid \phi(n)$ so $\alpha = 0, 1, 2$.
- If $3^\beta \mid n$ with $\beta > 0$ then $3^{\beta-1} \mid \phi(n)$ so $\beta = 0, 1, 2, 3$.
- If $7^\gamma \mid n$ with $\gamma > 0$ then $7^{\gamma-1} \mid \phi(n)$ so $\gamma = 0, 1$.
- If $19^\delta \mid n$ with $\delta > 0$ then $19^{\delta-1} \mid \phi(n)$ so $\delta = 0, 1$.

Then these are the cases,

- $n = 2^0 3^0 7^0 19^0 = 1$
- $\boxed{n = 2^0 3^0 7^0 19^1 = 19}$
- $n = 2^0 3^0 7^1 19^0 = 7$
- $n = 2^0 3^0 7^1 19^1 = 133$
- $n = 2^0 3^1 7^0 19^0 = 3$
- $n = 2^0 3^1 7^0 19^1 = 57$
- $n = 2^0 3^1 7^1 19^0 = 21$
- $n = 2^0 3^1 7^1 19^1 = 399$
- $n = 2^0 3^2 7^0 19^0 = 9$
- $n = 2^0 3^2 7^0 19^1 = 171$
- $n = 2^0 3^2 7^1 19^0 = 63$
- $n = 2^0 3^2 7^1 19^1 = 1197$
- $\boxed{n = 2^0 3^3 7^0 19^0 = 27}$
- $n = 2^0 3^3 7^0 19^1 = 513$
- $n = 2^0 3^3 7^1 19^0 = 189$
- $n = 2^0 3^3 7^1 19^1 = 3591$
- $n = 2^1 3^0 7^0 19^0 = 2$
- $\boxed{n = 2^1 3^0 7^0 19^1 = 38}$
- $n = 2^1 3^0 7^1 19^0 = 14$
- $n = 2^1 3^0 7^1 19^1 = 266$
- $n = 2^1 3^1 7^0 19^0 = 6$
- $n = 2^1 3^1 7^0 19^1 = 114$
- $n = 2^1 3^1 7^1 19^0 = 42$
- $n = 2^1 3^1 7^1 19^1 = 798$
- $n = 2^1 3^2 7^0 19^0 = 18$
- $n = 2^1 3^2 7^0 19^1 = 342$
- $n = 2^1 3^2 7^1 19^0 = 126$
- $n = 2^1 3^2 7^1 19^1 = 2394$
- $\boxed{n = 2^1 3^3 7^0 19^0 = 54}$
- $n = 2^1 3^3 7^0 19^1 = 1026$
- $n = 2^1 3^3 7^1 19^0 = 378$
- $n = 2^1 3^3 7^1 19^1 = 7182$
- $n = 2^2 3^0 7^0 19^1 = 4$
- $n = 2^2 3^0 7^0 19^1 = 76$
- $n = 2^2 3^0 7^1 19^1 = 28$
- $n = 2^2 3^0 7^1 19^1 = 532$
- $n = 2^2 3^1 7^0 19^1 = 12$
- $n = 2^2 3^1 7^0 19^1 = 228$
- $n = 2^2 3^1 7^1 19^1 = 84$
- $n = 2^2 3^1 7^1 19^1 = 1596$
- $n = 2^2 3^2 7^0 19^1 = 36$
- $n = 2^2 3^2 7^0 19^1 = 684$
- $n = 2^2 3^2 7^1 19^1 = 252$
- $n = 2^2 3^2 7^1 19^1 = 4788$
- $n = 2^2 3^3 7^0 19^1 = 108$
- $n = 2^2 3^3 7^0 19^1 = 2052$
- $n = 2^2 3^3 7^1 19^1 = 756$
- $n = 2^2 3^3 7^1 19^1 = 14364$

Then evaluating all n as $\phi(n)$ we get that for $n = 19, 27, 38, 54$, $\phi(n) = 18$.

2. Show there are no n with $\phi(n) = 14$.

   Suppose $\phi(n) = 14$ for some n, then $7 \mid p^\alpha - p^{\alpha-1}$ for some odd prime p. Since the factors of 14 are 2 and 7 we have two cases. If $p = 7$ and $\alpha > 1$ which implies $6 \mid 14$ which is not true. Or if $7 \mid p - 1$ but $p - 1$ is even, so $p = 15$ which is not prime. Therefore there are no n with $\phi(n) = 14$.

3. For what values of n is $\phi(n)$ odd? Justify.

   Since $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ we know that it will be even for all $p > 2$, therefore n cannot have any prime factors greater than 2. It follows that for $n = 1, 2$ $\phi(n)$ is odd.

4. Prove that $f(n) = \gcd(n, 3)$ is multiplicative. (This is actually true if 3 is replaced by any positive integer.)

   Proof. We wish to show $f(mn) = f(m) \cdot f(n)$ when $\gcd(m, n) = 1$. Suppose that $\gcd(m, n) = 1$, then $\gcd(\gcd(m, 3), \gcd(n, 3)) = p$ for $p \in \mathbb{Z}^+$. This implies that $p \mid \gcd(m, 3)$ and $p \mid \gcd(n, 3)$ which implies $p \mid m$ and

$p \mid n$, but since $\gcd(m,n) = 1$ we have $p = 1$.
Let $\gcd(m,3) = x$, this implies $x \mid 3$ and $x \mid m$. Then,

$$x \mid m \implies x \mid mn \implies x \mid \gcd(mn,3)$$

Likewise, let $\gcd(n,3) = y$, this implies $y \mid 3$ and $y \mid n$. Then,

$$y \mid n \implies y \mid mn \implies y \mid \gcd(mn,3)$$

Then because $x \mid \gcd(mn,3)$ and $y \mid \gcd(mn,3)$ and $\gcd(x,y) = 1$ we have, $xy \mid \gcd(mn,3)$. Thus, $\gcd(mn,3) = \gcd(m,3) \cdot \gcd(n,3)$ and $f(n)$ is multiplicative. □

5. Find $\tau(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$

   $$= (1+1)(2+1)(3+1)(5+1)(4+1)(5+1)(5+1) = 2 \cdot 3 \cdot 4 \cdot 6 \cdot 5 \cdot 6 \cdot 6 = 25920$$

6. Find $\sigma(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$

   $$= \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{5^4-1}{5-1}\right)\left(\frac{11^6-1}{11-1}\right)\left(\frac{13^5-1}{15-1}\right)\left(\frac{17^6-1}{17-1}\right)\left(\frac{19^6-1}{19-1}\right)$$

7. Find $\tau(20!)$.

   First we need the prime factorization of $20!$,

   $$\begin{aligned} 20! = &(2)(3)\left(2^2\right)(5)(2 \cdot 3)(7)\left(2^3\right)\left(3^2\right)(2 \cdot 5)(11)\left(2^2 \cdot 3\right) \\ &(13)(2 \cdot 7)(3 \cdot 5)\left(2^4\right)(17)\left(2 \cdot 3^2\right)(19)\left(2^2 \cdot 5\right) \end{aligned}$$

   Thus, $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. Therefore, $\tau(20!) = (18+1)(8+1)(4+1)(2+1)(1+1)(1+1)(1+1)(1+1) = 41040$.

8. Classify all n with $\tau(n) = 30$. Explain!

   Suppose $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with $a_i > 0$, it follows that $\tau(n) = (1+\alpha_1) \cdots (1+\alpha_k) = 30$. Since $(1+\alpha_i) \geq 2$ we get the following cases:

   - $k = 15$ and $a_1 = \cdots = a_{15} = 1$.
   - $k = 10$ and $a_1 = \cdots = a_{10} = 2$.
   - $k = 6$ and $a_1 = \cdots = a_6 = 4$.
   - $k = 5$ and $a_1 = \cdots = a_5 = 5$.
   - $k = 3$ and $a_1 = \cdots = a_3 = 9$.
   - $k = 1$ and $a_1 = 29$.

   Then we have,

   - $n = p_1 \cdots p_{15}$

- $n = p_1^2 \cdots p_{10}^2$
- $n = p_1^4 \cdots p_6^4$
- $n = p_1^5 \cdots p_5^5$
- $n = p_1^9 p_2^9 p_3^9$
- $n = p_1^{29}$

9. Prove that $\sigma(n) = k$ has at most a finite number of solutions when k is a positive integer.

   Proof. Since $\sigma(n)$ is multiplicative we know that $1 \mid n$ and $n \mid n$ implies that $\sigma(n) \geq 1 + n$. It follows then that $\sigma(n) = k \implies 1 + n \leq k \implies n \leq k - 1$. Thus, $\sigma(n) = k$ has a finite number of solutions. □

10. Show that if a and b are positive integers and p and q are distinct odd primes then $n = p^a q^b$ is deficient.

    We wish to show $\sigma(n) < 2n$,

$$\sigma(p^a q^b) = \left(\frac{p^{a+1} - 1}{p - 1}\right)\left(\frac{q^{b+1} - 1}{q - 1}\right) < \left(\frac{p^{a+1}}{p - 1}\right)\left(\frac{q^{b+1}}{q - 1}\right) = \left(\frac{p}{p - 1}\right)\left(\frac{q}{q - 1}\right) p^a q^b$$

    Since we wish to show $\sigma(n) < 2n$ we then need $\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right) < 2$.

$$\begin{aligned}
\left(\frac{p}{p - 1}\right)\left(\frac{q}{q - 1}\right) &< 2 \\
pq &< 2(p - 1)(q - 1) \\
pq &< 2\left(pq - p - q + 1\right) \\
pq &< 2pq - 2p - 2q + 2 \\
0 &< pq - 2p - 2q + 2 \\
0 &< (p - 2)(q - 2) - 2 \\
-2 &< (p - 2)(q - 1)
\end{aligned}$$

    Recall that p and q are *distinct* odd primes, so let's assume that $p > q > 2$. Since let $p = 5$ and $q = 3$, we then see $2 < (5-2)(3-2)$, thus the inequality holds. Therefore $p^a q^b$ is deficient.

11. Prove that a perfect square cannot be a perfect number.

    Proof. Let n be a perfect square, first observe that when n is even by Euler's Theorem $n = 2^{p-1}\left(2^p - 1\right) \implies \sqrt{n} = \sqrt{2^{p-1}\left(2^p - 1\right)}$ but then this implies that $\sqrt{n} \notin \mathbb{Z}$ which contradicts n being a perfect square. Therefore n must be odd. So $n = 2^k \left(p_1^{\alpha_1} \cdots p_i^{\alpha_i}\right)$, note that for $p_1^{\alpha_1} \cdots p_i^{\alpha_i}$ each p and α is even. Then it follows that n has an odd number of odd divisors. Thus $\sigma(n)$ is an odd number, but a perfect number is when $\sigma(n) = 2n$ which implies $\sigma(n)$ must be an even number. Therefore a perfect square cannot be a perfect number. □

12. Use Theorem 7.12 to determine whether each of the following Mersenne numbers is a Mersenne prime:

    Personally, I found it easiest to create a simple python script to test for primality of Mersenne numbers.

```
import math

def Mersenne_Prime (n):
  M = 2**n -1

  for k in range (1, int(math.sqrt(M))):
    factor = (2*n)*k +1
    if M % factor == 0:
      print(M/factor)
      return false

  return True
```

    (a) M_{11}

    First we see $M_{11} = 2^{11} - 1 = 2047$, then the factors of 2047 are of the form $2(11)k + 1 = 22k + 1$. Look at k up to $\sqrt{2047} \approx 45.24$. We find that $2047 = 23 \cdot 89$, therefore M_{11} is not prime.

    (b) M_{21}

    First we observe that $21 = 3 \cdot 7$, then by the definition of a Mersenne prime, since 21 is not prime then M_{21} is not prime.

    (c) M_{31}

    First we see $M_{31} = 2^{31} - 1 = 2147483647$, then the factors of 2147483647 are of the form $2(31)k + 1 = 62k + 1$. Look at k up to $\sqrt{2147483647} \approx 46340.95$. We find that there is no factor of 2147483647 of the form $62k + 1$ for $k \leq 46341$, therefore M_{31} is prime.

1.9 Chapter 9

1.9.1

1. $\mathrm{ord}_{21}8$

Since $\phi(21) = 12$ we have $\text{ord}_{21} = 1, 2, 3, 4, 6, 12$. Then we see,

$$\begin{aligned} 8^1 &\equiv 8 \bmod 21 \\ 8^2 &\equiv 1 \bmod 21 \end{aligned}$$

Therefore, $\text{ord}_{21}8 = 2$.

2. $\text{ord}_{25}8$

Since $\phi(25) = 20$ we have $\text{ord}_{25} = 1, 2, 4, 5, 10, 20$. Then we see,

$$\begin{aligned} 8^1 &\equiv 8 \bmod 25 \\ 8^2 &\equiv 14 \bmod 25 \\ 8^4 &\equiv 21 \bmod 25 \\ 8^5 &\equiv 18 \bmod 25 \\ 8^{10} &\equiv 24 \bmod 25 \\ 8^{20} &\equiv 1 \bmod 25 \end{aligned}$$

Therefore, $\text{ord}_{25}8 = 20$.

1.9.2

We wish to find a primtive root r such that $r^{\phi(n)} \equiv 1 \bmod n$. First we see that $\phi(50) = 20$ so we want to find an r for $r^{20} \equiv 1 \bmod 50$. Let $r = 3$, we can then observe:

$$\begin{aligned} 3^1 &\equiv 3 \bmod 50 \\ 3^2 &\equiv 9 \bmod 50 \\ 3^4 &\equiv 31 \bmod 50 \\ 3^5 &\equiv 43 \bmod 50 \\ 3^{10} &\equiv 49 \bmod 50 \\ 3^{20} &\equiv 1 \bmod 50 \end{aligned}$$

So we have $r = 3$ as a primitive root for $n = 50$. Then we see that there are a total of $\phi(\phi(50)) = \phi(20) = 8$ primitive roots for $n = 50$. Take k with

$\gcd(k, \phi(50)) = 1 \implies \gcd(k, 20) = 1$. So $k = 1, 3, 7, 9, 11, 13, 17, 19$. Then,

$$\begin{aligned}
3^1 &\equiv 3 \bmod 50 \\
3^3 &\equiv 27 \bmod 50 \\
3^7 &\equiv 37 \bmod 50 \\
3^9 &\equiv 33 \bmod 50 \\
3^{11} &\equiv 47 \bmod 50 \\
3^{13} &\equiv 23 \bmod 50 \\
3^{17} &\equiv 13 \bmod 50 \\
3^{19} &\equiv 17 \bmod 50
\end{aligned}$$

So we get $3, 13, 17, 23, 27, 33, 37, 47$ as the primitive roots of $n = 50$.

1.9.3

Proof. Since $\text{ord}_p a = 2k$ we have that $a^{2k} \equiv 1 \bmod p$ which implies that $p \mid \left(a^{2k} - 1\right)$ where $a^{2k} - 1 = (a^k + 1)(a^k - 1)$. So we have two cases,

- If $p \mid (a^k + 1)$ then we get $a^k \equiv -1 \bmod p$.
- If $p \mid (a^k - 1)$ then we get $a^k \equiv 1 \bmod p$, but this contradicts the fact that $\text{ord}_p a = 2k$.

Thus, p can only divide $a^k + 1$ and therefore $a^k \equiv -1 \bmod p$. □

1.9.4

Since $\text{ord}_m a = m-1$ we know that because $\text{ord}_m a \mid \phi(m)$ we have $(m-1) \mid \phi(m)$. But from the definition of the Euler Phi function we know that $\phi(m) \leq m - 1$ so therefore $\phi(m) = m - 1$. Then it follows that m must be prime.

1.9.5

Proof. Using the proof in problem three we can see:

$$\text{ind}_r a + \left(\frac{p-1}{2}\right) \implies \text{ind}_r a + \text{ind}_r (p-1) \implies \text{ind}_r (ap - a)$$

It then follows that $\text{ind}_r(p - a) \equiv \text{ind}_r(ap - a) \bmod p - 1$. From here we can "un-index" to then get $(p-a) \equiv (ap-a) \bmod p$ which we know to be true from the definition of congruence. Thus, $\text{ind}_r(p-a) \equiv \text{ind}_r a + \left(\frac{p-1}{2}\right) \bmod p-1$. □

1.9.6

We will show $\text{ord}_n(ab) = (\text{ord}_n a)(\text{ord}_n b)$ by two directions, first the left side divides the right and then the right side divides the left.

- Observe that $(ab)^{\text{ord}_n a \cdot \text{ord}_n b} = a^{\text{ord}_n a \cdot \text{ord}_n b} \cdot b^{\text{ord}_n a \cdot \text{ord}_n b} = 1^{\text{ord}_n b} \cdot 1^{\text{ord}_n a} \equiv 1 \bmod n$. This implies that $\text{ord}_n(ab) \mid (\text{ord}_n a)(\text{ord}_n b)$.
- We know that $(ab)^{\text{ord}_n(ab)} \equiv 1$, so we can see the following.

  $$\begin{aligned} (ab)^{\text{ord}_n(ab)} &\equiv 1 & (ab)^{\text{ord}_n(ab)} &\equiv 1 \\ \left((ab)^{\text{ord}_n(ab)}\right)^{\text{ord}_n a} &\equiv 1^{\text{ord}_n a} & \left((ab)^{\text{ord}_n(ab)}\right)^{\text{ord}_n b} &\equiv 1^{\text{ord}_n b} \\ b^{\text{ord}_n(ab) \cdot \text{ord}_n a} &\equiv 1 & a^{\text{ord}_n(ab) \cdot \text{ord}_n b} &\equiv 1 \end{aligned}$$

  Looking at $b^{\text{ord}_n(ab) \cdot \text{ord}_n a} \equiv 1$ we see that $\text{ord}_n b \mid (\text{ord}_n(ab))(\text{ord}_n a)$. But, since $\text{ord}_n a$ and $\text{ord}_n b$ are coprime to one another we get, $\text{ord}_n b \mid \text{ord}_n(ab)$. Likewise, the same can be said about $\text{ord}_n a$, therefore $\text{ord}_n a \mid \text{ord}_n(ab)$. Then we have $(\text{ord}_n a)(\text{ord}_n b) \mid \text{ord}_n(ab)$.

Then we see that since $\text{ord}_n(ab) \mid (\text{ord}_n a)(\text{ord}_n b)$ and $(\text{ord}_n a)(\text{ord}_n b) \mid \text{ord}_n(ab)$ we get $\text{ord}_n(ab) = (\text{ord}_n a)(\text{ord}_n b)$.

1.9.7

Proof. Since $p \equiv 1 \bmod 4$ let $p = 4k+1$ for some $k \in \mathbb{Z}$. We know that for a primtive root r, $r^{\phi(p)/2} \equiv -1 \bmod p$. It then follows that $r^{((4k+1)-1)/2} = r^{4k/2} = r^{2k} \equiv -1 \bmod p$. Thus, $(-r)^{2k} \equiv -1 \bmod p$ and then taking $-r$ to some power gives us congruence to r. Therefore $-r$ is a primtive root of p. □

1.9.8

1.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_7 a$	12	11	8	10	3	7	1	9	4	2	5	6

2.

$$\begin{aligned} x^2 &\equiv 12 \bmod 13 \\ \text{ind}_7(x^2) &\equiv \text{ind}_7 12 \bmod \phi(13) \\ 2\text{ind}_7 x &\equiv 6 \bmod 12 \\ \text{ind}_7 x &\equiv 3 \bmod 6 \\ \text{ind}_7 x &\equiv 3, 9 \bmod 12 \\ x &\equiv 5, 8 \bmod 13 \end{aligned}$$

3.

$$\begin{aligned}4^x &\equiv 12 \bmod 13\\ \text{ind}_7 4^x &\equiv \text{ind}_7 12 \bmod \phi(13)\\ x\text{ind}_7 4 &\equiv 6 \bmod 12\\ 10x &\equiv 6 \bmod 12\\ 5x &\equiv 3 \bmod 6\\ (5)(5x) &\equiv (5)(3) \bmod 6\\ x &\equiv 3 \bmod 6\\ x &\equiv 3, 9 \bmod 12\end{aligned}$$

1.9.9

1. The problem with this is the use of the fraction $\frac{a}{b}$, we can not always guarantee $\frac{a}{b}$ to be an integer, furthermore there is no such thing as "divison" in this context.

2. We know that if $\gcd(b, \phi(n)) = 1$ then $\exists b'$ such that $b \cdot b' \equiv 1 \bmod \phi(n)$. Then we can substitute $\text{ind}_r(\frac{a}{b})$ with $\text{ind}_r(a \cdot b')$. Formally, if $\gcd(a, n) = \gcd(b, n) = 1$ and r is a primitive root then,

$$\text{ind}_r a - \text{ind}_r b \equiv \text{ind}_r(a \cdot b') \bmod \phi(n)$$

3. *Proof.* Suppose $\gcd(a, n) = \gcd(b, n) = 1$ and r is a primitive root. Observe then,

$$\begin{aligned}\text{ind}_r a - \text{ind}_r b \bmod \phi(n) &\equiv r^{\text{ind}_r a} \cdot r^{-\text{ind}_r b} \bmod n\\ &\equiv r^{\text{ind}_r a} \cdot r^{\text{ind}_r b'} \bmod n\\ &\equiv r^{\text{ind}_r (a \cdot b')} \bmod n\\ &\equiv \text{ind}_r(a \cdot b') \bmod \phi(n)\end{aligned}$$

Thus, we see then that $\text{ind}_r a - \text{ind}_r b \equiv \text{ind}_r(a \cdot b') \bmod \phi(n)$. □

1.9.10

Proof. If r_1 and r_2 are primitive roots for some odd prime p we know that, $r_1^{(p-1)} \equiv r_2^{(p-1)} \equiv 1$ but $r_1^{(p-1)/2} \equiv r_2^{(p-1)/2} \equiv -1$. In the first case we see that $(r_1 \cdot r_2)^{(p-1)} \equiv r_1^{(p-1)} \cdot r^{(p-1)} \equiv 1$ so that works. In the second case we see that $(r_1 \cdot r_2)^{(p-1)/2} \equiv r_1^{(p-1)/2} \cdot r_2^{(p-1)/2} \equiv -1 \cdot -1 \equiv 1$. Therefore $r_1 r_2$ is not a primitive root of p. □

1.11 Chapter 11

1.11.1

Observe,

$$\begin{array}{cccc}
1^2 \equiv 1 \text{ mod } 17 & 5^2 \equiv 8 \text{ mod } 17 & 9^2 \equiv 13 \text{ mod } 17 & 13^2 \equiv 16 \text{ mod } 17 \\
2^2 \equiv 4 \text{ mod } 17 & 6^2 \equiv 2 \text{ mod } 17 & 10^2 \equiv 15 \text{ mod } 17 & 14^2 \equiv 9 \text{ mod } 17 \\
3^2 \equiv 9 \text{ mod } 17 & 7^2 \equiv 15 \text{ mod } 17 & 11^2 \equiv 2 \text{ mod } 17 & 15^2 \equiv 4 \text{ mod } 17 \\
4^2 \equiv 16 \text{ mod } 17 & 8^2 \equiv 13 \text{ mod } 17 & 12^2 \equiv 8 \text{ mod } 17 & 16^2 \equiv 1 \text{ mod } 17
\end{array}$$

From here we can see that $1, 2, 4, 8, 9, 13, 15$, and 16 are Quadratic Residues mod 17.

1.11.2

(a)

$$\left(\frac{3}{17}\right) \equiv 3^{(17-1)/2} = 3^8 \equiv 16 \equiv -1 \text{ mod } 17$$

Thus, 3 is a QNR mod 17.

(b) By Gauss's Lemma we have the set $\{3, 2 \cdot 3, \cdots, ((17-1)/2) \cdot 3\}$ which is $\{3, 6, 9, 12, 15, 18, 21, 24\}$. Then we take them mod 17, to get $\{3, 6, 9, 12, 15, 1, 4, 7\}$. We want to see how many are greater than $17/2 = 8.5$, we then see that 3 are greater than 8.5. Then $(-1)^3 = -1$, so we have $\left(\frac{3}{17}\right) = -1$ and therefore 3 is a QNR mod 17.

1.11.3

Proof. We wish to show that $\text{ord}_q(-4) = \phi(q)$. Since we know q to be an odd prime, we have that $\phi(q) = q - 1 \implies (2p+1) - 1 = 2p$. So we then get $\text{ord}_q(-4) \mid 2p$, of which $\text{ord}_q(-4) = 1, 2, p$, or $2p$.

- If $\text{ord}_q(-4) = 1$ then $(-4)^1 \equiv 1 \text{ mod } q \implies q \mid -5 \implies q = 5$, but this implies that $p = 2$ since $q = 2p + 1$, and we know both p and q to be odd primes, so $\text{ord}_q(-4) \neq 1$.
- If $\text{ord}_q(-4) = 2$ then $(-4)^2 \equiv 1 \text{ mod } q \implies s \mid 15 \implies q = 5, 3$, but this implies p to be either be $1, 2$, and we know both p and q to be odd primes, so $\text{ord}_q(-4) \neq 2$.
- If $\text{ord}_q(-4) = p$ then $(-4)^p \equiv 1 \text{ mod } q \implies \frac{-4}{q} \equiv 1 \text{ mod } q \implies \frac{-1}{2p+1}(1) \equiv 1 \text{ mod } q \implies -1 \equiv 1 \text{ mod } q$, but this implies $q \mid 2$ which is false.

Thus, by process of elimination the only value that $\text{ord}_q(-4)$ is equivalent to is $2p$. □

1.11.4

Proof. We will first prove 4 to be a Quadratic Residue,

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 = 1$$

Then, to prove $\frac{p-1}{4}$,

$$\left(\frac{\frac{p-1}{4}}{p}\right) = \left(\frac{\frac{p-1}{4}}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = 1$$

We can substitute in $\left(\frac{4}{p}\right)$ during the second step because in the first part of the proof we showed $\left(\frac{4}{p}\right)$ to be a Quadratic Residue. Thus, both -4 and $(p-1)/4$ are Quadratic Residues of p when $p \equiv 1 \bmod 4$. □

1.11.5

(a)

$$\begin{aligned}\left(\frac{21}{59}\right) &= \left(\frac{3}{59}\right)\left(\frac{7}{59}\right) \text{ by splitting.}\\ &= \left[-\left(\frac{59}{3}\right)\right]\left[-\left(\frac{59}{7}\right)\right] \text{by LoQR since } 3,7 \equiv 3 \bmod 4.\\ &= \left(\frac{2}{3}\right)\left(\frac{3}{7}\right) \text{ by reducing.}\\ &= (-1)^1\left[-\left(\frac{7}{3}\right)\right] \text{by 2 rule and LoQR since } 3 \equiv 3 \bmod 4.\\ &= \left(\frac{1}{3}\right) \text{ by reducing.}\\ &= 1\end{aligned}$$

(b)

$$\begin{aligned}
\left(\frac{1463}{89}\right) &= \left(\frac{7}{89}\right)\left(\frac{11}{89}\right)\left(\frac{19}{89}\right) \text{ by splitting.}\\
&= \left(\frac{89}{7}\right)\left(\frac{89}{11}\right)\left(\frac{89}{19}\right) \text{ by LoQR.}\\
&= \left(\frac{5}{7}\right)\left(\frac{1}{11}\right)\left(\frac{13}{19}\right) \text{ by reducing.}\\
&= \left(\frac{7}{5}\right)\left(\frac{19}{13}\right) \text{ by LoQR.}\\
&= \left(\frac{2}{5}\right)\left(\frac{6}{13}\right) \text{ by reducing.}\\
&= (-1)^{(25-1)/8}\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) \text{ by 2 rule and splitting.}\\
&= (-1)(-1)^{(13^2-1)/8}\left(\frac{13}{3}\right) \text{ by 2 rule and LoQR.}\\
&= \left(\frac{1}{3}\right) \text{ by reducing.}\\
&= 1
\end{aligned}$$

(c)

$$\begin{aligned}
\left(\frac{1547}{1913}\right) &= \left(\frac{7}{1913}\right)\left(\frac{13}{1913}\right)\left(\frac{17}{1913}\right) \text{ by splitting.}\\
&= \left(\frac{1913}{7}\right)\left(\frac{1913}{13}\right)\left(\frac{1913}{17}\right) \text{ by LoQR.}\\
&= \left(\frac{1}{7}\right)\left(\frac{2}{13}\right)\left(\frac{9}{17}\right) \text{ by reducing.}\\
&= (-1)^{(13^2-1)/8}\text{by 2 rule}\\
&= -1
\end{aligned}$$

1.11.6

We have two main cases, $p \equiv 1$ or $p \equiv 3 \bmod 4$.

1. If $p \equiv 1 \bmod 4 \implies \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. Then,
   - $p \equiv 1 \bmod 3 \implies \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1 \implies p \equiv 1 \bmod 12$
   - $p \equiv 2 \bmod 3 \implies \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1 \implies p \equiv 5 \bmod 12$
2. If $p \equiv 3 \bmod 4 \implies \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Then,
   - $p \equiv 1 \bmod 3 \implies -\left(\frac{p}{3}\right) = - \leq 13 = -1 \implies p \equiv 7 \equiv -5 \bmod 12$
   - $p \equiv 2 \bmod 3 \implies -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = 1 \implies p \equiv 11 \equiv -1 \bmod 12$

1.11.7

By the Law of Quadratic Residues since $5 \equiv 1 \bmod 4$ we have that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Then because $\gcd(5,p) = 1$ we know that $p \bmod 5$ can only be $1, 2, 3$ or 4.

- $p \equiv 1 \bmod 5 \implies \left(\frac{1}{5}\right) = 1$
- $p \equiv 2 \bmod 5 \implies \left(\frac{2}{5}\right) = -1$
- $p \equiv 3 \bmod 5 \implies \left(\frac{3}{5}\right) = -1$
- $p \equiv 4 \bmod 5 \implies \left(\frac{4}{5}\right) = 1$

So we see that in order for $\left(\frac{5}{p}\right) = 1$, p must be either 1 or 4 mod 5.

1.11.8

(a)

$$\begin{aligned}
\left(\frac{5}{21}\right) &= \left(\frac{21}{5}\right) \text{ by LoQR since } 5 \equiv 1 \bmod 4. \\
&= \left(\frac{1}{5}\right) \text{ by reducing.} \\
&= 1
\end{aligned}$$

(b)

$$\begin{aligned}
\left(\frac{1009}{2307}\right) &= \left(\frac{2307}{1009}\right) \text{ by LoQR since } 1009 \equiv 1 \bmod 4. \\
&= \left(\frac{289}{1009}\right) \text{ by reducing.} \\
&= \left(\frac{1009}{289}\right) \text{ by LoQR since } 289 \equiv 1 \bmod 4. \\
&= \left(\frac{142}{289}\right) \text{ by reducing.} \\
&= \left(\frac{2}{289}\right)\left(\frac{71}{289}\right) \text{ by splitting.} \\
&= \left(\frac{289}{71}\right) \text{ by 2 rule and LoQR since } 289 \equiv 1 \bmod 4. \\
&= \left(\frac{5}{71}\right) \text{ by reducing.} \\
&= \left(\frac{71}{5}\right) \text{ by LoQR since } 5 \equiv 1 \bmod 4. \\
&= \left(\frac{1}{5}\right) \text{ by reducing.} \\
&= 1
\end{aligned}$$

(c)

$$\begin{aligned}
\left(\frac{27}{101}\right) &= \left(\frac{101}{27}\right) \text{ by LoQR since } 101 \equiv 1 \bmod 4. \\
&= \left(\frac{20}{27}\right) \text{ by reducing.} \\
&= \left(\frac{4}{27}\right)\left(\frac{5}{27}\right) \text{ by splitting.} \\
&= \left(\frac{27}{5}\right) \text{ by LoQR since } 5 \equiv 1 \bmod 4. \\
&= \left(\frac{2}{5}\right) \text{ by reducing.} \\
&= -1
\end{aligned}$$

1.11.9

Observe that $\left(\frac{n}{3}\right)\left(\frac{n}{5}\right) = \left(\frac{n}{15}\right) = \left(\frac{15}{n}\right) = 1$. It follows then that for $n \equiv 1 \bmod 4$ we have cases, $\left(\frac{n}{3}\right) = 1$ and $\left(\frac{n}{5}\right) = 1$, and $\left(\frac{n}{3}\right) = -1$ and $\left(\frac{n}{5}\right) = -1$.

- If $\left(\frac{n}{3}\right) = 1$ and $\left(\frac{n}{5}\right) = 1$ then $n \equiv 1 \bmod 3$ and $n \equiv 1, 4 \bmod 5$.
- If $\left(\frac{n}{3}\right) = -1$ and $\left(\frac{n}{5}\right) = -1$ then $n \equiv 2 \bmod 3$ and $n \equiv 2, 3 \bmod 5$.

Then, for $n \equiv 3 \bmod 4$ we have cases, $\left(\frac{n}{3}\right) = 1$ and $\left(\frac{n}{5}\right) = -1$, and $\left(\frac{n}{3}\right) = -1$ and $\left(\frac{n}{5}\right) = 1$.

- If $\left(\frac{n}{3}\right) = 1$ and $\left(\frac{n}{5}\right) = -1$ then $n \equiv 1 \bmod 3$ and $n \equiv 2, 3 \bmod 5$.
- If $\left(\frac{n}{5}\right) = -1$ and $\left(\frac{n}{5}\right) = 1$ then $n \equiv 2 \bmod 3$ and $n \equiv 1, 4 \bmod 5$.

1.11.10

First observe that the prime factorization of a can include primes to both even and odd powers. Let p denote prime factors of a to odd powers, similarly let q denote prime factors of a to even powers. We then see, $a = p_1 \cdots p_i q_1 \cdots q_j$. Then from rules of the Jacobi Symbol we can split $\left(\frac{a}{n}\right)$, it follows then that we do not care about the prime factors of a raised to even powers (denoted q) since their Jacobi Symbol will always be 1. So then we get $\left(\frac{a}{n}\right) = \left(\frac{p_1}{n}\right) \cdots \left(\frac{p_i}{n}\right)$ We then need to handle the specific case of when p_1 is 2. If $p_1 = 2$ we have:

$$\begin{aligned}
\left(\frac{a}{n}\right) &= \left(\frac{p_1}{n}\right) \cdots \left(\frac{p_i}{n}\right) \\
&= \left(\frac{2}{n}\right) \cdots \left(\frac{p_i}{n}\right) \\
&= \left(\frac{2}{n}\right) \cdots \left(\frac{n}{p_i}\right) \\
&= (-1) \cdots (1) \\
&= -1
\end{aligned}$$

In order for this to work we would need n such that $n \equiv 5 \bmod 8$ (2 rule) and $n \equiv 1 \bmod p_k$ for all k (LoQR used in line 3). Then for the more general case of $p_1 > 2$ we have:

$$\begin{aligned}\left(\frac{a}{n}\right) &= \left(\frac{p_1}{n}\right)\cdots\left(\frac{p_i}{n}\right)\\ &= \left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_1}\right)\\ &= \left(\frac{x}{p_1}\right)\cdots(1)\\ &= -1\end{aligned}$$

In order for this to work we would need n such that $n \equiv x \bmod p_1$ (where x is a QNR of p_1), $n \equiv 1 \bmod 4$, and $n \equiv 1 \bmod p_k$ for all k. Thus, we get

$$\text{if } p_1 = 2, n \equiv \begin{cases} 5 \bmod 8 \\ 1 \bmod p_k & \forall k \end{cases} \qquad \text{if } p_1 > 2, n \equiv \begin{cases} x \bmod p_1 & (x \text{ is a QNR of } p_1) \\ 1 \bmod 4 \\ 1 \bmod p_k & \forall k \end{cases}$$

1.8 Chapter 8

1.8.1

For each letter we use $C \equiv 11P + 8 \bmod 26$ and get `ZSYJAVJGSJJQSEA` as the ciphertext.

1.8.2

(a) First observe that the two most frequent letters in the ciphertext are `S` and `N`, so lets assume that these correspond to `E` and `T` respectively. Then we have

$$\begin{aligned}18 &\equiv 4a + b \bmod 26\\ 13 &\equiv 19a + b \bmod 26\end{aligned}$$

This then gives us

$$\begin{aligned}-5 &\equiv a(19-4) \bmod 26\\ -5 &\equiv a(15) \bmod 26\\ (5)(3a) &\equiv -5 \bmod 26\\ -5(5)(3a) &\equiv -5(-5) \bmod 26\\ 3a &\equiv 25 \bmod 26\\ a &\equiv 17 \bmod 26\end{aligned}$$

Then we find $b \equiv 18 - 4a = 18 - 4(17) \equiv 2 \bmod 26$. Together, we get that $a = 17, b = 2$.

(b) First observe that the multiplicative inverse of $a = 17$ is $a^{-1} = 23$. Then we get $P = 23(C-2) \bmod 26$, resulting in `YESTHEALIENSHAVELOCATEDITWHATNEXT`.

1.8.3

	NE	ED	BA	CK	UP	NO	WX	
	1304	0403	0100	0210	2015	1314	2223	
	1304^{71}	403^{71}	100^{71}	210^{71}	2015^{71}	1314^{71}	2223^{71}	
$\equiv$	2755	3464	2222	3183	1023	2590	2540	mod 3637

Then we get `2755 3464 2222 3183 1023 2590 2540` as our ciphertext.

1.8.4

(a) We know that d has to satisfy $71(d) \equiv 1 \bmod 3636$. Observe then that $71^{\phi(3636)} \equiv 1 \bmod 3636$ so then we see that $d \equiv 71^{\phi(3636)-1} \equiv 2663 \bmod 3636$.

(b)

	1333	0513	0452	0767	2130	1395	1097	3597
	1333^{2663}	513^{2663}	452^{2663}	767^{2663}	2130^{2663}	1395^{2663}	1097^{2663}	3597^{2663}
$\equiv$	1200	1308	0002	1413	1907	0411	1414	1804
	MA	NI	AC	ON	TH	EL	OO	SE

Thus, the message is `MANIACONTHELOOSE`.

1.8.5

(a) $e \cdot \text{ind}_r 18 \equiv \text{ind}_r 11 \bmod 28$

(b) First note that $\text{ind}_2 18 = 11$ and $\text{ind}_2 11 = 25$ so we then get $11e \equiv 25 \bmod 28 \implies e = 15$.

(c) We want to find d such that $15d \equiv 1 \bmod 28 \implies d = 15$.

(d) Take the ciphertext and decrypt it like so, $P \equiv C^{15} \bmod 29$,

`18 12 00 17 19 24 15 00 13 19 18` $\Longrightarrow$ `SMARTYPANTS`

1.8.6

(a) i. The message becomes `EV EI SL IS TE NI NG` which in turn then becomes,

`0421 0408 1811 0818 1904 1308 1306`

ii. Take the text and sign it like so, $S \equiv P^{2599} \bmod 3551$,

```
0724 2163 0430 2945 2663 3473 0993
```

iii. Encrypt the text like so, $C \equiv S^{27} \bmod 4189$,

```
3425 0345 0521 3573 1463 1546 0567
```

(b) i. Take the text and decrypt it like so, $S \equiv C^{1203} \bmod 4189$

```
1616 2799 3244 1237 1617 0457
```

ii. Take the text and unsign it like so, $P \equiv S^{103} \bmod 3511$

`1800 2104 2414 2017 1804 1105` $\Longrightarrow$ `SAVEYOURSELF`

1.8.7

First we factor $n = 288319 = 401 \cdot 719$, then $\phi(n)$ follows as $\phi(n) = (p-1)(q-1) = 400 \cdot 718 = 287200$. Then we want to find d such that $(5201)d \equiv 1 \bmod 287200$, which results in $d = 272401$. Then we decrypt the message like so, $P \equiv C^{272401} \bmod 288319$

```
220724 181412 041908 120418 082104 010411 080421 040300 181200 132400 181808
230812 151418 180801 110419 070813 061801 040514 170401 170400 100500 181923
```

Thus, the message is

```
WHYSOMETIMESIVEBELIEVEDASMANYASSIXIMPOSSIBLETHINGSBEFOREBREAKFASTX
```

1.8.8

Since we have $\gcd(e_1, e_2) = 1$ we need to find α and β such that $\alpha e_1 + \beta e_2 = 1$. Using the Euclidean Algorithm we get $\alpha = -24$ and $\beta = 49$. Since $\alpha = -24$ we have to first find the multiplicative inverse of C_1 before we can raise it to the power of α. We get $4280^{-1} \equiv 1097 \bmod 4757$. Then, all together we have

$$1097^{24} \cdot 330^{49} \equiv 2404 \bmod 4757$$

Thus, $P = 2404$.

1.8.9

We have the system of linear congruences,

$$\begin{aligned} x &\equiv 1533 \bmod 5353 \\ x &\equiv 3561 \bmod 5251 \\ x &\equiv 835 \bmod 5893 \end{aligned}$$

We get $x = 2893640625 = P^3 = (1425)^3 \implies P =$`1425`.

1.8.10

(a) We have that $\overline{C} \equiv Cr^e \equiv 156 \cdot 888^{27} \equiv 1099 \bmod 4189$.

(b) We get that $r^{-1} = 2203$ then we take the trash and multiplies it by the inverse of r, $2203 \cdot 662 \equiv 614 \bmod 4189$ so we get P to be `0614`.

1.12 Additional Topics

1.12.1

(a) Set $x_0 = 2$ and $f(x) = x^2 + 1$. Then we have,

$$\begin{aligned}
&x_1 \equiv 2^2 + 1 \equiv 5 \bmod 143 && \\
&x_2 \equiv 5^2 + 1 \equiv 26 \bmod 143 && \gcd(26-5, 143) = 1 \\
&x_3 \equiv 26^2 + 1 \equiv 104 \bmod 143 && \\
&x_4 \equiv 104^2 + 1 \equiv 92 \bmod 143 && \gcd(92-26, 143) = 11
\end{aligned}$$

So we get 11 as a factor of 143.

(b) Set $x_0 = 2$ and $f(x) = x^2 + 1$. Then we have,

$$\begin{aligned}
&x_1 \equiv 2^2 + 1 \equiv 5 \bmod 5473 && \\
&x_2 \equiv 5^2 + 1 \equiv 26 \bmod 5473 && \gcd(26-5, 5473) = 1 \\
&x_3 \equiv 26^2 + 1 \equiv 677 \bmod 5473 && \\
&x_4 \equiv 677^2 + 1 \equiv 4071 \bmod 5473 && \gcd(4071-26, 5473) = 1 \\
&x_5 \equiv 4071^2 + 1 \equiv 798 \bmod 5473 && \\
&x_6 \equiv 798^2 + 1 \equiv 1937 \bmod 5473 && \gcd(1937-677, 5473) = 1 \\
&x_7 \equiv 1937^2 + 1 \equiv 2965 \bmod 5473 && \\
&x_8 \equiv 2965^2 + 1 \equiv 1588 \bmod 5473 && \gcd(1588-4071, 5473) = 13
\end{aligned}$$

So we get 13 as a factor of 5473.

(c) Set $x_0 = 2$ and $f(x) = x^2 + 1$. Then we have,

$$\begin{aligned}
&x_1 \equiv 2^2 + 1 \equiv 5 \bmod 234643 && \\
&x_2 \equiv 5^2 + 1 \equiv 26 \bmod 234643 && \gcd(26-5, 234643) = 1 \\
&x_3 \equiv 26^2 + 1 \equiv 677 \bmod 234643 && \\
&x_4 \equiv 677^2 + 1 \equiv 223687 \bmod 234643 && \gcd(223687-26, 234643) = 1 \\
&x_5 \equiv 223687^2 + 1 \equiv 131364 \bmod 234643 && \\
&x_6 \equiv 131364^2 + 1 \equiv 150348 \bmod 234643 && \gcd(150348-677, 234643) = 97
\end{aligned}$$

So we get 97 as a factor of 234643.

1.12.2

Suppose we know X and $-Y$. Note that from $-Y$ we can easily get Y. Then observe that $X + Y \equiv a + a \equiv 2a \bmod p$ and $X + Y \equiv a + (-a) \equiv 0 \bmod q$. So we have that $q \mid (X + Y)$ and $p \nmid (X + Y)$ (we know that $p \nmid (X + Y)$ since $p \mid (X + Y) \implies p \mid 2a \implies p \mid a \implies a \equiv 0 \bmod p$ which is a contradiction). So we know $\gcd(X + Y, n) = q$ then it follows that $p = \frac{n}{q}$ and now we have both p and q, the factors of n.

1.12.3

From Alice's choice of $p = 67$ and $q = 83$ we have $n = 5561$, and she sends n to Bob. Bob chooses $b = 123$, and finds $S \equiv b^2 \equiv 4007 \bmod 5561$, then he sends 4007 to Alice. Alice then solves the equation $x^2 \equiv 4007 \bmod 5561$,

- First we have,

$$\left.\begin{array}{r} x \equiv 4007^{(67+1)/4} \equiv 56 \bmod 67 \\ x \equiv 4007^{(83+1)/4} \equiv 40 \bmod 83 \end{array}\right\} \implies X \equiv 123$$

  Which gives us $X = 123$ and $-X = 5438$.

- Then we have,

$$\left.\begin{array}{r} x \equiv 4007^{(67+1)/4} \equiv 56 \bmod 67 \\ x \equiv -4007^{(83+1)/4} \equiv 43 \bmod 83 \end{array}\right\} \implies Y \equiv 458$$

  Which gives us $Y = 458$ and $-Y = 5103$.

Alice then sends Bob on from the set of these four numbers, $\{123, 458, 5103, 5438\}$. If Alice chooses either 458 or 5103 then Bob will be able to factor n (Bob can do this through $\gcd(123 - a, 5561)$ where a is either 458 or 5103, this will result in a factor of n) and thus win the coinflip!

1.12.4

1. Choose $p = 3001$ to find a primitive root of p we need an r such that $\gcd(r, p) = 1$ and $\text{ord}_p r = \phi(p) \implies \text{ord}_{3001} r = 3000 \implies r^{3000} \bmod 3001 \implies r = 14$.

2. Suppose we choose $a = 2718$, then $b \equiv 14^{2718} \equiv 1079 \bmod 3001$. The public key is then $(p, r, b) \implies (3001, 14, 1079)$.

3. Suppose Alice wants to send Bob `ELGAMALCRYPTOSYSTEM`. Then she uses the encryption function $\mathcal{E}(P) = (14^k, P \cdot 1079^k) \bmod 3001$ on the plaintext, where $1 \le k \le p - 2$.

	EL	GA	MA	LC	RY	PT	OS	YS	TE	MX
$P =$	0411	0600	1200	1102	1724	1519	1418	2418	1904	1223

$$\begin{aligned}
k &= 1, & \mathcal{E}(411) &= (14^1, 411 \cdot 1079^1) \equiv (14, 2322) \bmod 3001\\
k &= 2, & \mathcal{E}(600) &= (14^2, 600 \cdot 1079^2) \equiv (196, 1830) \bmod 3001\\
k &= 3, & \mathcal{E}(1200) &= (14^3, 1200 \cdot 1079^3) \equiv (2744, 2825) \bmod 3001\\
k &= 4, & \mathcal{E}(1102) &= (14^4, 1102 \cdot 1079^4) \equiv (2404, 183) \bmod 3001\\
k &= 5, & \mathcal{E}(1724) &= (14^5, 1724 \cdot 1079^5) \equiv (645, 2838) \bmod 3001\\
k &= 6, & \mathcal{E}(1519) &= (14^6, 1519 \cdot 1079^6) \equiv (27, 1407) \bmod 3001\\
k &= 7, & \mathcal{E}(1418) &= (14^7, 1418 \cdot 1079^7) \equiv (378, 682) \bmod 3001\\
k &= 8, & \mathcal{E}(2418) &= (14^8, 2418 \cdot 1079^8) \equiv (2291, 872) \bmod 3001\\
k &= 9, & \mathcal{E}(1904) &= (14^9, 1904 \cdot 1079^9) \equiv (2064, 570) \bmod 3001\\
k &= 1, & \mathcal{E}(1223) &= (14^1, 1223 \cdot 1079^1) \equiv (14, 2178) \bmod 3001
\end{aligned}$$

Then our encrypted message is:

```
(14, 2322) (196, 1830) (2744, 2825) (2404, 183) (645, 2838)
  (27, 1407) (378, 682) (2291, 872) (2064, 570) (14, 2178)
```