Solutions to Elementary Number Theory (Second Edition) by David M. Burton

Samy Lahlou

February 10, 2026

Preface

The goal of this document is to share my personal solutions to the exercises in the Second Edition of Elementary Number Theory by David M. Burton during my reading. To make my solutions clear, for each exercise, I will assume nothing more than the content of the book and the results proved in the preceding exercises. Moreover, it should be noted that a lot of the exercises can be done very easily using a calculator or using a computer program. It is for this reason that I chose to do every exercise with **no calculator and without writing any computer program**. I took this decision because I believe that I will learn more in this way.

As a disclaimer, the solutions are not unique and there will probably be better or more optimized solutions than mine. Feel free to correct me or ask me anything about the content of this document at the following address:

samy.lahloukamal@mail.mcgill.ca

Contents

Chapter 1

Some Preliminary Considerations

1.1 Mathematical Induction

1. Establish the formulas below by mathematical induction:

(a) $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ for all $n \geqslant 1$;

(b) $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for all $n \geqslant 1$;

(c) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \dfrac{n(n+1)(n+2)}{3}$ for all $n \geqslant 1$;

(d) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(4n^2-1)}{3}$ for all $n \geqslant 1$;

(e) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$ for all $n \geqslant 1$;

Solution

(a) First, when $n = 1$, we have that both sides of the equation are equal to 1, so the basis for the induction is verified. Suppose now that the equation holds for a natural number k, then adding $k+1$ on both sides gives us

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1).$$

But since

$$\frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2},$$

then

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

which implies that the equation holds for $k+1$. Therefore, by induction, it holds for all $n \geqslant 1$.

(b) First, when $n = 1$, we have that both sides of the equation are equal to 1, so the basis for the induction is verified. Suppose now that the equation holds for a natural number k, then adding $2k + 1$ on both sides gives us

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2$$

which implies that the equation holds for $k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

(c) First, when $n = 1$, we have that both sides of the equation are equal to 2, so the basis for the induction is verified. Suppose now that the equation holds for a natural number k, then adding $(k + 1)(k + 2)$ on both sides gives us

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k + 1) + (k + 1)(k + 2) = \frac{k(k + 1)(k + 2)}{3} + (k + 1)(k + 2).$$

But since

$$\frac{k(k + 1)(k + 2)}{3} + (k+1)(k+2) = (k+1)(k+2)\left(\frac{k}{3} + 1\right) = \frac{(k + 1)(k + 2)(k + 3)}{3},$$

then

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k + 1) + (k + 1)(k + 2) = \frac{(k + 1)(k + 2)(k + 3)}{3}$$

which implies that the equation holds for $k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

(d) First, when $n = 1$, we have that both sides of the equation are equal to 1, so the basis for the induction is verified. Suppose now that the equation holds for a natural number k, then adding $(2k + 1)^2$ on both sides gives us

$$1^2 + 3^2 + 5^2 + \cdots + (2k - 1)^2 + (2k + 1)^2 = \frac{k(4k^2 - 1)}{3} + (2k + 1)^2.$$

But since

$$\begin{aligned}\frac{k(4k^2 - 1)}{3} + (2k + 1)^2 &= \frac{4k^3 - k + 3(2k + 1)^2}{3} \\ &= \frac{4k^3 - k + 12k^2 + 12k + 3}{3} \\ &= \frac{4k^3 + 12k^2 + 11k + 3}{3} \\ &= \frac{(k + 1)(4k^2 + 8k + 3)}{3} \\ &= \frac{(k + 1)(4(k + 1)^2 - 1)}{3},\end{aligned}$$

then

$$1^2 + 3^2 + 5^2 + \cdots + (2k - 1)^2 + (2k + 1)^2 = \frac{(k + 1)(4(k + 1)^2 - 1)}{3}$$

which implies that the equation holds for $k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

(e) First, when $n = 1$, we have that both sides of the equation are equal to 1, so the basis for the induction is verified. Suppose now that the equation holds for a natural number k, then adding $(k+1)^3$ on both sides gives us

$$1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3.$$

But since

$$\left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 = (k+1)^2\left(\frac{k^2}{2^2} + (k+1)\right) = \left(\frac{(k+1)(k+2)}{2}\right)^2,$$

then

$$1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

which implies that the equation holds for $k+1$. Therefore, by induction, it holds for all $n \geqslant 1$.

2. If $r \neq 1$, show that

$$a + ar + ar^2 + \ldots ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

for any positive integer n.

Solution
When $n = 1$, both sides of the equation are equal to $a(r+1)$ so the basis for induction is verified. Suppose now that the equation holds for a positive integer k, then adding ar^{k+1} on both sides of the equation gives us

$$a + ar + ar^2 + \ldots ar^k + ar^{k+1} = \frac{a(r^{k+1} - 1)}{r - 1} + ar^{k+1}.$$

But since

$$\frac{a(r^{k+1} - 1)}{r - 1} + ar^{k+1} = \frac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r - 1} = \frac{a(r^{k+2} - 1)}{r - 1},$$

then

$$a + ar + ar^2 + \ldots ar^k + ar^{k+1} = \frac{a(r^{k+2} - 1)}{r - 1}$$

and so the equation holds for all $k+1$. Therefore, it holds for all $n \geqslant 1$.

3. Use the Second Principle of Finite Induction to establish that

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a + 1)$$

for all $n \geqslant 1$.

Solution
When $n = 1$, both sides of the equation are equal to $a - 1$, so the basis for the

induction is verified. Suppose now that there exists a positive integer k such that the equation holds for all $n = 1, ..., k$. From the identity

$$a^{n+1} - 1 = (a+1)(a^n - 1) - a(a^{n-1} - 1),$$

and by the inductive hypothesis for $n = k$ and $n = k - 1$, we obtain:

$$\begin{aligned} a^{n+1} - 1 &= (a+1)(a-1)(a^{n-1} + \cdots + 1) - a(a-1)(a^{n-2} + \cdots + 1) \\ &= (a-1)[(a+1)(a^{n-1} + \cdots + 1) - a(a^{n-2} + \cdots + 1)] \\ &= (a-1)[(a+1)(a^{n-1} + \cdots + 1) - (a^{n-1} + \cdots + 1 - 1)] \\ &= (a-1)[(a+1)(a^{n-1} + \cdots + 1) - (a^{n-1} + \cdots + 1) + 1] \\ &= (a-1)[a(a^{n-1} + \cdots + 1) + 1] \\ &= (a-1)(a^n + a^{n-1} + \cdots + a + 1) \end{aligned}$$

which proves that the equation holds for $n = k+1$. Therefore, by induction, it holds for all $n \geqslant 1$.

4. Prove that the cube of any integer can be written as the difference of two squares.

Solution
Using part (e) of exercice 1, we get

$$\begin{aligned} n^3 &= (1^3 + 2^3 + \cdots + n^3) - (1^3 + 2^3 + \ldots (n-1)^3) \\ &= \left[\frac{n(n+1)}{2}\right]^2 - \left[\frac{n(n-1)}{2}\right]^2 \end{aligned}$$

which proves that any cube can be written as the difference of two squares.

5.

(a) Find the values of $n \leqslant 7$ for which $n! + 1$ is a perfect square (it is unknown whether $n! + 1$ is a square for any $n > 7$).

(b) True or false? For positive integers m and n, $(mn)! = m!n!$ and $(m+n)! = m! + n!$.

Solution

(a) For $n = 0, 1$, we have $n! + 1 = 2$ which is not a square. For $n = 2$, we have $2! + 1 = 3$ which is not a square. For $n = 3$, we have $3! + 1 = 7$ which is not a square. When $n = 4$ and $n = 5$, we obtain $4! + 1 = 5^2$ and $5! + 1 = 11^2$. For $n = 6$, we get $6! + 1 = 721$ which is strictly between $26^2 = 676$ and $27^2 = 729$ so it cannot be a square. Finally, for $n = 7$, we obtain $7! + 1 = 71^2$.

(b) In both cases, $m = n = 2$ is a counterexample since $(m+n)! = (mn)! = 24$ and $m!n! = m! + n! = 4$.

6. Prove that $n! > n^2$ for every integer $n \geqslant 4$, while $n! > n^3$ for every integer $n \geqslant 6$.

Solution
When $n = 4$, then $n! = 24$ and $n^2 = 16$ so the strict inequality is satisfied. Now that the basis for the induction is verified, suppose that the inequality is satisfied for a positive integer k, then multiplying on both sides by $k+1$ gives the inequality

$$(k+1)! > k^2(k+1) \geqslant (k+1)(k+1) = (k+1)^2$$

using the fact that $k^2 \geqslant k+1$ for all $k \geqslant 2$. Thus, since the inequality is also satisfied by $k+1$, then it is for all $n \geqslant 4$ by induction.

When $n = 6$, then $n! = 720$ and $n^3 = 216$ so the strict inequality is satisfied. Now that the basis for the induction is verified, suppose that the inequality is satisfied for a positive integer k, then multiplying on both sides by $k+1$ gives the inequality

$$(k+1)! > k^3(k+1) \geqslant (k+1)^2(k+1) = (k+1)^3$$

using the fact that $k^3 \geqslant (k+1)^2$ for all $k \geqslant 4$. Thus, since the inequality is also satisfied by $k+1$, then it is for all $n \geqslant 6$ by induction.

7. Use mathematical induction to derive the formula

$$1 \cdot (1!) + 2 \cdot (2!) + 3 \cdot (3!) + \cdots + n \cdot (n!) = (n+1)! - 1$$

for all $n \geqslant 1$.

Solution
If $n = 1$, then both expressions on the two side of the desired equation are equal to 1; so the basis for the induction is verified. Next, if we suppose that the equation holds for a positive integer k, then adding $(k+1) \cdot (k+1)!$ on both sides gives us

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

which shows that the equation also holds for $n = k+2$. Therefore, by induction, it holds for all $n \geqslant 1$.

8.

(a) Verify that

$$2 \cdot 6 \cdot 10 \cdot 14 \cdot \ldots \cdot (4n-2) = \frac{(2n)!}{n!}$$

for all $n \geqslant 1$.

(b) Use part (a) to to obtain the inequality $2^n(n!)^2 \leqslant (2n)!$ for all $n \geqslant 1$.

Solution

(a) Let's prove it by induction on n. When $n = 1$, then both expressions on the two sides of the equation are equal to 2, so the basis for the induction is verified. Now, if we suppose that the equation holds for a positive integer k, then by multiplying both sides by $(4k + 2)$ gives us

$$2 \cdot 6 \cdot 10 \cdot \ldots \cdot (4n+2) = \frac{(2n)!}{n!}(4n+2) = \frac{(2n)!}{n!} \cdot \frac{(2n+1)(2n+2)}{n+1} = \frac{(2(n+1)!)}{(n+1)!}.$$

Thus, the equation also holds for $n = k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

(b) First fix a $n \geqslant 1$ and notice that

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \leqslant 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1).$$

Next, multiplying both sides by 2^n and using part (a) gives us

$$2^n \cdot n! \leqslant 2 \cdot 6 \cdot 10 \cdot \ldots \cdot (4n-2) = \frac{(2n)!}{n!}.$$

Finally, multiplying both sides by $n!$ gives us the desired inequality.

9. Establish the Bernoulli inequality: if $1 + a > 0$, then

$$(1+a)^n \leqslant 1 + na$$

for all $n \geqslant 1$.

Solution

Let's prove it by induction on n. When $n = 1$, then $(1+a)^n = 1+a \geqslant 1+a = 1+na$, and so the basis for induction is verified. Next, suppose that the inequality holds for a positive integer k, then multiplying both sides by $(1 + a)$ preserves the inequality since it is positive. Hence, we obtain:

$$\begin{aligned}(1+a)^{k+1} &= (1+a)(1+a)^k \\ &\geqslant (1+a)(1+ka) \\ &= 1 + (k+1)a + ka^2 \\ &\geqslant 1 + (k+1)a\end{aligned}$$

which shows that the inequality must also hold for $n = k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

10. Prove by mathematical induction that

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}$$

for all $n \geqslant 1$.

Solution

When $n = 1$, both sides of the inequality are equal to 1, so the inequality holds and so the basis for the induction is verified. Next, if we suppose that the inequality holds for a positive integer k, then adding $\frac{1}{(k+1)^2}$ on both sides gives us

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(k+1)^2}\leqslant 2-\frac{1}{k}+\frac{1}{(k+1)^2}.$$

But notice that

$$\begin{aligned} 0\leqslant 1 &\implies 2k+k^2\leqslant 1+2k+k^2\\ &\implies 2k+k^2\leqslant (k+1)^2\\ &\implies 1-\frac{(k+1)^2}{k}\leqslant -(k+1)\\ &\implies \frac{1}{(k+1)^2}-\frac{1}{k}\leqslant -\frac{1}{(k+1)} \end{aligned}$$

and so

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(k+1)^2}\leqslant 2+\frac{1}{(k+1)^2}-\frac{1}{k}\leqslant 2-\frac{1}{k+1}.$$

Thus, the inequality holds for $n=k+1$. Therefore, by induction, the inequality holds for all $n\geqslant 1$.

1.2 The Binomial Theorem

1. Prove that for $n \geqslant 1$:

(a) $\displaystyle\binom{2n}{n} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} 2^n.$

(b) $\displaystyle\binom{4n}{2n} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (4n-1)}{[1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)]^2} \binom{2n}{n}.$

Solution

(a) Let's prove it by induction. When $n = 1$, we have

$$\binom{2n}{n} = 2$$

and

$$\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} 2^n = 2$$

and so it holds in that case. If we now suppose that it holds when $n = k$ for some integer $k \geqslant 1$, then it follows that

$$\frac{(2k)!}{(k!)^2} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k-1)}{k!} 2^k.$$

Multiplying both sides by $\frac{(2k+1)(2k+2)}{(k+1)^2}$ gives us

$$\begin{aligned}\binom{2(k+1)}{k+1} &= \frac{(2k+1)(2k+2)}{(k+1)^2} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k-1)}{k!} 2^k \\ &= 2\frac{(2k+1)}{k+1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k-1)}{k!} 2^k \\ &= \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k+1)}{(k+1)!} 2^{k+1}\end{aligned}$$

which shows that the equation also holds for $n = k+1$. Therefore, by induction, it holds for all integers $n \geqslant 1$.

(b) First, notice that by part (a), it suffices to prove that

$$\binom{4n}{2n} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (4n-1)}{n! \cdot 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)} 2^n$$

holds for all $n \geqslant 1$. Let's prove it by induction on n. When $n = 1$, then both sides are equal to 6 and so the statement holds in that case. Suppose now that it holds for some integer $n = k \geqslant 1$, then

$$\frac{(4k)!}{(2k!)^2} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (4k-1)}{k! \cdot 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k-1)} 2^k.$$

Multiplying both sides by $\frac{(4k+1)(4k+2)(4k+3)(4k+4)}{(2k+1)^2(2k+2)^2}$ gives us

$$\begin{aligned}\binom{4(k+1)}{2(k+1)} &= \frac{(4k+1)(4k+2)(4k+3)(4k+4)}{(2k+1)^2(2k+2)^2}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(4k-1)}{k!\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2k-1)}2^k\\ &= \frac{(4k+2)(4k+4)}{(2k+1)(2k+2)^2}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(4k+1)}{k!\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2k+1)}2^k\\ &= \frac{4k+4}{(2k+2)(2k+2)}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(4k+1)}{k!\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2k+1)}2^{k+1}\\ &= \frac{1}{k+1}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(4k+1)}{k!\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2k+1)}2^{k+1}\\ &= \frac{1\cdot 3\cdot 5\cdot\cdots\cdot(4k+1)}{(k+1)!\cdot 1\cdot 3\cdot 5\cdot\cdots\cdot(2k+1)}2^{k+1}\end{aligned}$$

which shows that the equation also holds for $n = k+1$. Therefore, by induction, it holds for all integers $n \geqslant 1$.

2. If $2 \leqslant k \leqslant n-2$, show that

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}, \qquad n \geqslant 4.$$

Solution
This simply follows from Pascal's Rule:

$$\begin{aligned}\binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k} &= \left[\binom{n-2}{k-2} + \binom{n-2}{k-1}\right] + \left[\binom{n-2}{k-1} + \binom{n-2}{k}\right]\\ &= \binom{n-1}{k-1} + \binom{n-1}{k}\\ &= \binom{n}{k}.\end{aligned}$$

3. For $n \geqslant 1$, derive each of the identities below:

(a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$; [*Hint:* Let $a = b = 1$ in the binomial theorem.]

(b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$;

(c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}$; [*Hint:* After expanding $n(1+b)^{n-1}$ by the binomial theorem, let $b = 1$: note also that

$$n\binom{n-1}{k} = (k+1)\binom{n}{k+1}.]$$

(d) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n$;

(e) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots$

$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$; [*Hint:* Use parts (a) and (b).]

(f) $\binom{n}{0} - \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} - \cdots + \frac{(-1)^n}{n+1}\binom{n}{n} = \frac{1}{n+1}$; [*Hint:* the left-hand side equals

$\frac{1}{n+1}\left[\binom{n+1}{1} - \binom{n+1}{2} + \binom{n+1}{3} - \cdots + (-1)^n\binom{n+1}{n+1}\right]$.]

Solution

(a) Taking $a = b = 1$ in the Binomial Theorem gives us

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}.$$

(b) Taking $a = 1$ and $b = -1$ in the Binomial Theorem gives us

$$0 = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots (-1)^n \binom{n}{n}.$$

(c) From the hint, it follows that

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n\binom{n-1}{0} + n\binom{n-1}{1} + \cdots + n\binom{n-1}{n-1} = n2^{n-1}$$

where the last equality follows from part (a).

(d) Taking $a = 1$ and $b = 2$ in the Binomial Theorem gives us

$$3^n = (1+2)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ldots 2^n \binom{n}{n}.$$

(e) From part (b), we have that

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$$

Thus, using part (a), we get

$$\begin{aligned} \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots &= \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots \\ &= \frac{1}{2}\left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}\right] \\ &= 2^{n-1} \end{aligned}$$

(f) Using the hint, we easily get

$$\begin{aligned}
&\binom{n}{0}-\frac{1}{2}\binom{n}{1}+\frac{1}{3}\binom{n}{2}-\cdots+\frac{(-1)^n}{n+1}\binom{n}{n}\\
=&\frac{1}{n+1}\left[\binom{n+1}{1}-\binom{n+1}{2}+\binom{n+1}{3}-\cdots+(-1)^n\binom{n+1}{n+1}\right]\\
=&\frac{1}{n+1}\left(1-\left[\binom{n}{0}-\binom{n+1}{1}+\binom{n+1}{2}-\binom{n+1}{3}+\cdots+(-1)^{n+1}\binom{n+1}{n+1}\right]\right)\\
=&\frac{1}{n+1}(1-0)\\
=&\frac{1}{n+1}
\end{aligned}$$

4. Prove that for $n \geqslant 1$:

(a) $\binom{n}{r}<\binom{n}{r+1}$ if and only if $0 \leqslant r < \frac{1}{2}(n-1)$.

(b) $\binom{n}{r}>\binom{n}{r+1}$ if and only if $n-1 \geqslant r > \frac{1}{2}(n-1)$.

(c) $\binom{n}{r}=\binom{n}{r+1}$ if and only if n is an odd integer, and $r=\frac{1}{2}(n-1)$.

Solution

(a) Let $0 \leqslant r \leqslant n-1$ be an integer, then

$$\begin{aligned}
\binom{n}{r}<\binom{n}{r+1} &\iff \frac{n!}{(n-r)!r!}<\frac{n!}{(n-r-1)!(r+1)!}\\
&\iff (n-r-1)!(r+1)!<(n-r)!r!\\
&\iff r+1<n-r\\
&\iff r<\frac{1}{2}(n-1).
\end{aligned}$$

(b) Let $0 \leqslant r \leqslant n-1$ be an integer, then

$$\begin{aligned}
\binom{n}{r}>\binom{n}{r+1} &\iff \frac{n!}{(n-r)!r!}>\frac{n!}{(n-r-1)!(r+1)!}\\
&\iff (n-r-1)!(r+1)!>(n-r)!r!\\
&\iff r+1>n-r\\
&\iff r>\frac{1}{2}(n-1).
\end{aligned}$$

(c) Let $0 \leqslant r \leqslant n-1$ be an integer, then

$$\begin{aligned}
\binom{n}{r}=\binom{n}{r+1} &\iff \frac{n!}{(n-r)!r!}=\frac{n!}{(n-r-1)!(r+1)!}\\
&\iff (n-r-1)!(r+1)!=(n-r)!r!\\
&\iff r+1=n-r\\
&\iff r=\frac{1}{2}(n-1)\\
&\iff n=2r+1.
\end{aligned}$$

5. For $n \geqslant 1$, show that the expressions $\dfrac{(2n)!}{n!(n+1)!}$ and $\dfrac{(3n)!}{6^n n!}$ are both integers.

Solution
For the first expression, it suffices to notice that

$$\begin{aligned}\binom{2n}{n} - \binom{2n}{n+1} &= \frac{(2n)!}{n!n!} - \frac{(2n)!}{(n-1)!(n+1)!}\\ &= \frac{(2n)!(n+1) - (2n)!n}{n!(n+1)!}\\ &= \frac{(2n)!}{n!(n+1)!}.\end{aligned}$$

Since the binomial coefficients are integers, then it follows that the expression $\frac{(2n)!}{n!(n+1)!}$ is also an integer. For the second expression, let's prove it by induction. When $n = 1$, we have

$$\frac{(3n)!}{6^n n!} = \frac{3!}{6 \cdot 1} = 1$$

which proves that it holds for $n = 1$. Suppose now that the expression is an integer for some $n = k \geqslant 1$, then

$$\begin{aligned}\frac{(3(k+1))!}{6^{k+1}(k+1)!} &= \frac{(3k+1)(3k+2)(3k+3)}{6(k+1)} \cdot \frac{(3k)!}{6^k k!}\\ &= \frac{(3k+1)(3k+2)}{2} \cdot \frac{(3k)!}{6^k k!}\end{aligned}$$

where $\frac{(3k)!}{6^k k!}$ is an integer by the inductive hypothesis. Moreover, notice that $3k+1$ and $3k+2$ are two consecutive numbers and so one of them must be divisible by two. Thus, $\frac{(3k+1)(3k+2)}{2}$ is also an integer. Therefore, the case $n = k+1$ also holds since $\frac{(3(k+1))!}{6^{k+1}(k+1)!}$ can be written as the product of two integers.

6.

(a) For $n \geqslant 2$, prove that

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3}.$$

[*Hint* Use induction and Pascal's rule.]

(b) From part (a) and the fact that $\dbinom{m}{2} + \dbinom{m+1}{2} = m^2$ for $m \geqslant 2$, deduce the formula

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution

(a) Let's prove it by induction on n. When $n = 2$, we have

$$\binom{2}{2} + \cdots + \binom{n}{2} = \binom{2}{2} = 1 = \binom{3}{3} = \binom{n+1}{3}$$

and so the proposition holds in that case. Suppose now that the proposition holds for $n = k \geqslant 2$, then

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{k}{2} = \binom{k+1}{3}.$$

Adding $\binom{k+1}{2}$ on both sides gives

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{k+1}{2} = \binom{k+1}{2} + \binom{k+1}{3} = \binom{k+2}{3}$$

and so the proposition holds for $n = k + 1$. Therefore, by induction, it holds for all $n \geqslant 2$.

(b) Using the fact that $\binom{m}{2} + \binom{m+1}{2} = m^2$, we can write

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + n^2 &= 1 + \left[\binom{2}{2} + \binom{3}{2}\right] + \left[\binom{3}{2} + \binom{4}{2}\right] + \cdots + \left[\binom{n}{2} + \binom{n+1}{2}\right] \\
&= 2\left[\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n}{2}\right] + \binom{n+1}{2} \\
&= 2\binom{n+1}{3} + \binom{n+1}{2} \\
&= \frac{2(n+1)n(n-1)}{6} + \frac{(n+1)n}{2} \\
&= \frac{2(n+1)n(n-1) + 3(n+1)n}{6} \\
&= \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

which proves the desired formula.

7. For $n \geqslant 1$, verify that

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \binom{2n+1}{3}.$$

Solution

Let's prove it by induction on n. When $n = 1$, we have

$$1^2 + \cdots + (2n-1)^2 = 1 = \binom{3}{3} = \binom{2n+1}{3}.$$

Thus, the proposition holds for $n = 1$. Suppose now that it holds for $n = k \geqslant 1$, then

$$\begin{aligned}1^2+3^2+5^2+\cdots+(2k+1)^2 &= (1^2+3^2+5^2+\cdots+(2k-1)^2)+(2k+1)^2\\ &= \binom{2k+1}{3}+(2k+1)^2\\ &= \frac{(2k+1)(2k)(2k-1)}{6}+(2k+1)(2k+1)\\ &= \frac{(2k+1)[2k(2k-1)+6(2k+1)]}{6}\\ &= \frac{(2k+1)(4k^2+10k+6)}{6}\\ &= \frac{(2k+3)(2k+2)(2k+1)}{6}\\ &= \binom{2(k+1)+1}{3}\end{aligned}$$

which shows that it holds for $n=k+1$. Therefore, by induction, the proposition holds for all $n\geqslant 1$.

8. Establish the inequality $2^n < \binom{2n}{n} < 2^{2n}$ for $n>1$.

Solution

Let's prove it by induction on n. When $n=2$, we have

$$2^n = 4 < 6 = \binom{2n}{2} < 16 = 2^{2n}$$

and so it holds for this case. Suppose now that holds for an integer $n=k\geqslant 2$, then

$$2^k < \binom{2k}{k} < 2^{2k}.$$

Multiplying both sides by $\frac{(2k+2)(2k+1)}{(n+1)^2} = 2\frac{2k+1}{k+1}$ gives us

$$2^{k+1}\leqslant 2^k\cdot 2\frac{2k+1}{k+1} < \binom{2(k+1)}{k+1} < 2^{2k}\cdot 2\frac{2k+1}{k+1}\leqslant 2^{2(k+1)}$$

which shows that it holds for $n=k+1$. Therefore, by induction, the proposition holds for all integers $n>1$.

1.3 Early Number Theory

1.

(a) A number is triangular if and only if it is of the form $n(n+1)/2$ for some $n \geqslant 1$.

(b) The integer n is a triangular number if and only if $8n+1$ is a perfect square.

(c) The sum of any two consecutive triangular number is a perfect square.

(d) If n is a triangular number, then so are $9n+1$, $25n+3$ and $49n+6$.

Solution

(a) We already proved in the previous sections that

$$1+2+3\cdots+n=\frac{n(n+1)}{2}$$

so it directly follows that a number of the form of one of the side of the equation can be equivalently written in the form of the other side of the equation.

(b) First, let n be a triangular number, then there is an integer k for which $n = k(k+1)/2$. It follows that

$$8n+1=4k(k+1)+1=4k^2+4k+1=(2k+1)^2$$

which shows that $8n+1$ is a perfect square. Suppose now that $8n+1$ is a perfect square for a given integer n. Since $8n+1$ is odd, then it must be the square of an odd number: $8n+1=(2k+1)^2$. Thus:

$$\begin{aligned} 8n+1=(2k+1)^2 &\implies 8n+1=4k^2+4k+1 \\ &\implies n=\frac{1}{2}k^2+\frac{1}{2}k \\ &\implies n=\frac{k(k+1)}{2}. \end{aligned}$$

Since n can be written as $k(k+1)/2$, then it is a triangular number.

(c) Let a and b be triangular numbers, then a can be written as $n(n+1)/2$. Since b must have the same form while being the direct successor of a, then b must be equal to $(n+1)(n+2)/2$. Hence:

$$\begin{aligned} a+b &= \frac{n(n+1)}{2}+\frac{(n+1)(n+2)}{2} \\ &= \frac{n^2+n+n^2+3n+2}{2} \\ &= \frac{2n^2+4n+2}{2} \\ &= n^2+2n+1 \\ &= (n+1)^2 \end{aligned}$$

and so the sum of two consecutive triangular numbers is a perfect square.

(d) Let n be a triangular number, then n can be written as $k(k+1)/2$. It follows that

$$\begin{aligned}9n+1 &= 9\cdot\frac{k(k+1)}{2}+1\\ &= \frac{1}{2}(9k(k+1)+2)\\ &= \frac{1}{2}(9k^2+9k+2)\\ &= \frac{1}{2}((3k+1)^2+(3k+1))\\ &= \frac{(3k+1)((3k+1)+1)}{2},\end{aligned}$$

$$\begin{aligned}25n+3 &= 25\cdot\frac{k(k+1)}{2}+3\\ &= \frac{1}{2}(25k(k+1)+6)\\ &= \frac{1}{2}(25k^2+25k+6)\\ &= \frac{1}{2}((5k+2)^2+(5k+2))\\ &= \frac{(5k+2)((5k+2)+1)}{2}\end{aligned}$$

$$\begin{aligned}49n+6 &= 49\cdot\frac{k(k+1)}{2}+6\\ &= \frac{1}{2}(49k(k+1)+12)\\ &= \frac{1}{2}(49k^2+49k+12)\\ &= \frac{1}{2}((7k+3)^2+(7k+3))\\ &= \frac{(7k+3)((7k+3)+1)}{2}\end{aligned}$$

and so $9n+1$, $25n+3$ and $49n+6$ are all triangular numbers.

2. If t_n denotes the nth triangular number, prove that in terms of the binomial coefficients

$$t_n = \binom{n+1}{2}, \qquad n \geqslant 1.$$

Solution

Let $n \geqslant 1$. We already proved that we can write t_n as $n(n+1)/2$, so using the definition of the binomial coefficients, we have that

$$\binom{n+1}{2} = \frac{(n+1)!}{(n-1)!2!} = \frac{(n+1)n}{2} = t_n$$

which proves the desired formula.

3. Derive the following formula for the sum of triangular numbers, attributed to the Hindu mathematician Aryabhatta (circa 500 A.D.):

$$t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}, \qquad n \geqslant 1.$$

[*Hint:* Group the terms on the left-hand side in pairs, noting the identity $t_{k-1} + t_k = k^2$.]

Solution

Let's prove it by cases. If $n = 2k$, then

$$\begin{aligned} t_1 + t_2 + \cdots + t_{2k-1} + t_{2k} &= (t_1 + t_2) + \cdots + (t_{2k-1} + t_{2k}) \\ &= 2^2 + 4^2 + \cdots + (2k)^2 \\ &= 4(1^2 + 2^2 + \cdots + k^2) \\ &= 4 \cdot \frac{k(k+1)(2k+1)}{6} \\ &= \frac{2k(2k+2)(2k+1)}{6} \\ &= \frac{n(n+2)(n+1)}{6}. \end{aligned}$$

Suppose now that $n = 2k + 1$, then using the previous result:

$$\begin{aligned} t_1 + t_2 + \cdots + t_{n-1} + t_n &= \frac{(n-1)n(n+1)}{6} + \frac{n(n+1)}{2} \\ &= \frac{n(n+1)(n-1+3)}{6} \\ &= \frac{n(n+1)(n+2)}{6}. \end{aligned}$$

Therefore, the formula is true for all $n \geqslant 1$.

4. Prove that the square of any odd multiple of 3 is the difference of two triangular numbers; specifically that

$$9(2n+1)^2 = t_{9n+4} - t_{3n+1}.$$

Solution

By direct calculation:

$$\begin{aligned} t_{9n+4} - t_{3n+1} &= \frac{(9n+4)(9n+5)}{2} - \frac{(3n+1)(3n+2)}{2} \\ &= \frac{81n^2 + 81n + 20 - 9n^2 - 9n - 2}{2} \\ &= \frac{72n^2 + 72n + 18}{2} \\ &= 36n^2 + 36n + 9 \\ &= 9(4n^2 + 4n + 1) \\ &= 9(2n+1)^2. \end{aligned}$$

5. In the sequence of triangular numbers, find

(a) two triangular numbers whose sum and difference are also triangular numbers;

(b) three successive triangular numbers whose product is a perfect square;

(c) three successive triangular numbers whose sum is a perfect square.

Solution

(a) Take $15 = 1+2+3+4+5$ and $21 = 1+2+3+4+5+6$ since their sum is $36 = 1+2+3+4+5+6+7+8$ and their difference is $6 = 1+2+3$.

(b) Take

$$\begin{aligned}300 &= 1+2+3+\cdots+24,\\ 325 &= 1+2+3+\cdots+25,\\ 351 &= 1+2+3+\cdots+26\end{aligned}$$

since their product is

$$300 \cdot 325 \cdot 351 = (5850)^2.$$

(c) Take $15 = 1+2+3+4+5$, $21 = 1+2+3+4+5+6$ and $28 = 1+2+3+4+5+6+7$ since their sum is

$$15 + 21 + 28 = 64 = 8^2.$$

6.

(a) If the triangular number t_n is a perfect square, prove that $t_{4n(n+1)}$ is also a square.

(b) Use part (a) to find three examples of squares which are also triangular numbers.

Solution

(a) Suppose that t_n is a perfect square, then there exists a k such that $k^2 = n(n+1)/2$. It follows that

$$\begin{aligned}t_{4n(n+1)} &= \frac{4n(n+1)[4n(n+1)+1]}{2}\\ &= 2^2 \cdot \frac{n(n+1)}{2} \cdot (4n^2+4n+1)\\ &= (2k(2n+1))^2\end{aligned}$$

which shows that $t_{4n(n+1)}$ is a square.

(b) Using part (a), it suffices to find one such number to deduce infinitely many others. Since $6^2 = 1+2+3+4+5+6+7+8 = t_8$, then t_{288} and t_{332928} must also be squares.

7. Show that the difference between squares of two consecutive triangular numbers is always a cube.

Solution
Let t_n and t_{n+1} be two consecutive triangular numbers, then

$$\begin{aligned} t_{n+1}^2 - t_n^2 &= \frac{(n+1)^2(n+2)^2}{4} - \frac{n^2(n+1)^2}{4} \\ &= \frac{(n+1)^2}{4}\left[(n+2)^2 - n^2\right] \\ &= \frac{(n+1)^2}{4}(4n+4) \\ &= (n+1)^3. \end{aligned}$$

8. Prove that the sum of the reciprocals of the first n triangular numbers is less than 2; that is,

$$1/1 + 1/3 + 1/6 + 1/10 + \cdots + 1/t_n < 2.$$

[*Hint:* Observe that $\dfrac{2}{n(n+1)} = 2\left(\dfrac{1}{n} - \dfrac{1}{n+1}\right)$.]

Solution
By direct calculation:

$$\begin{aligned} \frac{1}{1} + \frac{1}{3} + \frac{1}{10} + \cdots + \frac{1}{t_n} &= \frac{2}{1\cdot 2} + \frac{2}{2\cdot 3} + \frac{2}{3\cdot 4} + \cdots + \frac{2}{n(n+1)} \\ &= 2\left(\frac{1}{1} - \frac{1}{2}\right) + 2\left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + 2\left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 2\left(\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1}\right) \\ &= 2\left(1 - \frac{1}{n+1}\right) \\ &< 2. \end{aligned}$$

9.

(a) Establish the identity $t_x = t_y + t_z$, where

$$x = 1/2\; n(n+3) + 1, \quad y = n+1, \quad z = 1/2\; n(n+3),$$

and $n \geqslant 1$, thereby proving that there are infinitely many triangular numbers which are the sum of two other such numbers.

(b) Find three examples of triangular numbers which are sums of two other triangular numbers.

Solution

(a) By direct calculation:

$$\begin{aligned}
t_y + t_z &= \frac{y(y+1)}{2} + \frac{z(z+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} + \frac{\frac{n(n+3)}{2}\left(\frac{n(n+3)}{2}+1\right)}{2} \\
&= \frac{(n+1)(n+2)}{2} + \frac{n(n+3)(n(n+3)+2)}{8} \\
&= \frac{[n(n+3)]^2 + 2n(n+3) + 4(n+1)(n+2)}{8} \\
&= \frac{[n(n+3)]^2 + 2n(n+3) + 4n^2 + 4 \cdot 3n + 8}{8} \\
&= \frac{[n(n+3)]^2 + 2n(n+3) + 4n(n+3) + 8}{8} \\
&= \frac{[n(n+3)]^2 + 6n(n+3) + 8}{8} \\
&= \frac{[n(n+3)+2][n(n+3)+4]}{8} \\
&= \frac{\left(\frac{n(n+3)}{2}+1\right)\left(\frac{n(n+3)}{2}+2\right)}{2} \\
&= \frac{x(x+1)}{2} \\
&= t_x.
\end{aligned}$$

(b) By taking plugging $n = 1$, $n = 2$ and $n = 3$ in the previous equation, we obtain that $t_3 = t_2 + t_2$, $t_6 = t_5 + t_3$ and $t_{10} = t_9 + t_4$.

Chapter 2

Divisibility Theory in the Integers

2.1 The Division Algorithm

1. Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leqslant r < 3b$.

Solution By the division algorithm, we know that there exist unique q_0 and r_0 such that $a = q_0 b + r_0$ and $0 \leqslant r_0 < b$. This implies that if we let $q = q_0 - 2$ and $r = r_0 + 2b$, then $a = qb + r$ with $2b \leqslant r < 3b$. To prove that q and r are unique, let q' and r' be integers such $a = q'b + r'$ and $2b \leqslant r' < 3b$, then equivalently: $a = (q' + 2)b + (r' - 2b)$ where $0 \leqslant r' - 2b < 3b$. But by uniqueness of q_0 and r_0, we have $r' - 2b = r_0$ and so $r' = r_0 + 2b = r$ by definition of r. This concludes the proof.

2. Show that any integer of the form $6k + 5$ is also of the form $3k + 2$, but not conversely.

Solution Let n be an integer of the form $6k + 5$, then

$$n = 3 \cdot 2k + 3 + 2 = 3(2k + 1) + 2$$

which proves that n is of the form $3k+2$. However, the converse does not hold since the integer $8 = 3 \cdot 2 + 2$ can also be written as $6 \cdot 1 + 2$. This shows that the converse cannot hold since otherwise, we would have a number that has both forms $6k + 2$ and $6k + 5$ which would contradict the uniqueness part of the Division Algorithm.

3. Use the Division Algorithm to establish that

(a) the square of any integer is either of the form $3k$ or $3k + 1$;

(b) the cube of any integer has one of the forms $9k$, $9k + 1$ or $9k + 8$;

(c) the fourth power of any integer is either of the form $5k$ or $5k + 1$.

Solution

(a) Let n be an integer, then by the Division Algorithm, we have that n has one of the following forms: $3k$, $3k+1$ or $3k+2$. Let's split the proof in these three cases. If $n = 3k$, then $n^2 = 3(3k^2)$. If $n = 3k + 1$, then $n^2 = 3(3k^2 + 2k) + 1$.

If $n = 3k + 2$, then $n^2 = 3(3k^2 + 4k + 1) + 1$. Therefore, for any integer n, n^2 has either the form $3k$ or $3k + 1$.

(b) Let n be an integer, then by the Division Algorithm, we have that n has one of the following forms: $3k$, $3k+1$ or $3k+2$. Let's split the proof in these three cases. If $n = 3k$, then $n^3 = 9(3k^3)$. If $n = 3k+1$, then $n^3 = 9(3k^3+3k^2+k)+1$. If $n = 3k + 2$, then $n^3 = 9(3k^3 + 6k^2 + 4k) + 8$.. Therefore, for any integer n, n^3 has either the form $9k$, $9k + 1$ or $9k + 8$.

(c) Let n be an integer, then by the Division Algorithm, we have that n has one of the following forms: $5k$, $5k + 1$, $5k + 2$, $5k + 3$ or $5k + 4$. Let's split the proof in these five cases. If $n = 5k$, then $n^4 = 5(5^3k^4)$. If $n = 5k + 1$, then

$$n^4 = 5(5^3k^4 + 4 \cdot 5^2k^3 + 6 \cdot 5k^2 + 4k) + 1.$$

If $n = 5k + 2$, then

$$n^4 = 5(5^3k^4 + 2 \cdot 4 \cdot 5^2k^3 + 4 \cdot 6 \cdot 5k^2 + 8 \cdot 4k + 3) + 1.$$

If $n = 5k + 3$, then

$$n^4 = 5(5^3k^4 + 3 \cdot 4 \cdot 5^2k^3 + 9 \cdot 6 \cdot 5k^2 + 27 \cdot 4k + 16) + 1.$$

If $n = 5k + 4$, then

$$n^4 = 5(5^3k^4 + 4 \cdot 4 \cdot 5^2k^3 + 16 \cdot 6 \cdot 5k^2 + 64 \cdot 4k + 51) + 1.$$

Therefore, for any integer n, n^4 has either the form $5k$ or $5k + 1$.

4. Prove that $3a^2 - 1$ is never a perfect square. [*Hint:* Problem 3(a).]

Solution It suffices to notice that $3a^2 - 1 + 3(a^2 - 1) + 2$ and to use the fact that no square can be of the form $3k + 2$ from Exercise 3(a).

5. For $n \geqslant 1$, prove that $n(n + 1)(2n + 1)/6$ is an integer. [Hint: By the Division Algorithm, n has one of the forms $6k$, $6k + 1$, ..., $6k + 5$; establish the result in each of these six cases.]

Solution Let n be an integer, then by the Division Algorithm, we have that n has one of the following forms: $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$ or $6k + 5$. Let's split the proof in these six cases. If $n = 6k$, then

$$\frac{n(n+1)(2n+1)}{6} = k(n+1)(2n+1).$$

If $n = 6k + 1$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{n(6k+2)(12k+3)}{6} = n(3k+1)(4k+1).$$

If $n = 6k + 2$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6k+2)(6k+3)(2n+1)}{6} = (3k+1)(2k+1)(2n+1).$$

If $n = 6k + 3$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6k+3)(6k+4)(2n+1)}{6} = (2k+1)(3k+2)(2n+1).$$

If $n = 6k + 4$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{(6k+4)(n+1)(12k+9)}{6} = (3k+2)(n+1)(4k+3).$$

If $n = 6k + 5$, then

$$\frac{n(n+1)(2n+1)}{6} = \frac{n(6k+6)(2n+1)}{6} = n(k+1)(2n+1).$$

Therefore, $n(n + 1)(2n + 1)/6$ is an integer.

6. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^2$), then it must be either of the form $7k$ of $7k + 1$.

Solution Let's look at possible remainders for squares and cubes of integers when divided by 7. Since every integer can be written as $7k$, $7k + 1$, ..., $7k + 6$, then we get

$$\begin{aligned}
(7k)^2 &= 7(7k^2) + 0\\
(7k+1)^2 &= 7(7k^2 + 2k) + 1\\
(7k+2)^2 &= 7(7k^2 + 2\cdot 2k) + 4\\
(7k+3)^2 &= 7(7k^2 + 3\cdot 2k + 1) + 2\\
(7k+4)^2 &= 7(7k^2 + 4\cdot 2k + 2) + 2\\
(7k+5)^2 &= 7(7k^2 + 5\cdot 2k + 3) + 4\\
(7k+6)^2 &= 7(7k^2 + 6\cdot 2k + 5) + 1
\end{aligned}$$

and

$$\begin{aligned}
(7k)^3 &= 7(7^2k^3) + 0\\
(7k+1)^3 &= 7(7^2k^3 + 3\cdot 7k^2 + 3k) + 1\\
(7k+2)^3 &= 7(7^2k^3 + 3\cdot 2\cdot 7k^2 + 4\cdot 3k + 1) + 1\\
(7k+3)^3 &= 7(7^2k^3 + 3\cdot 3\cdot 7k^2 + 9\cdot 3k + 3) + 6\\
(7k+4)^3 &= 7(7^2k^3 + 3\cdot 4\cdot 7k^2 + 16\cdot 3k + 9) + 1\\
(7k+5)^3 &= 7(7^2k^3 + 3\cdot 5\cdot 7k^2 + 25\cdot 3k + 17) + 6\\
(7k+6)^3 &= 7(7^2k^3 + 3\cdot 6\cdot 7k^2 + 36\cdot 3k + 30) + 6.
\end{aligned}$$

Therefore, the only possible remainders after dividing a square by 7 are 0, 1, 2 and 4; and the only possible remainders after dividing a cube by 7 are 0, 1 and 6. Thus, if a number is a square and a cube at the same time, then it can only be of the form $7k$ or $7k + 1$ since 0 and 1 are the only common remainders after dividing 7 for squares and cubes.

7. Obtain the following version of the Division Algorithm: For integers a and b, with $b \neq 0$, there exist unique integers q and r satisfying $a = qb + r$, where

$-\frac{1}{2}|b| < r \leqslant \frac{1}{2}|b|$. [*Hint:* First write $a = q'b + r'$, where $0 \leqslant r' < |b|$. When $0 \leqslant r' \leqslant \frac{1}{2}|b|$, let $r = r'$ and $q = q'$; when $\frac{1}{2}|b| < r' \leqslant |b|$, let $r = r' - |b|$ and $q = q' + 1$ if $b > 0$ or $q = q' - 1$ if $b < 0$.]

Solution The hint already gives a major part of the exercice but let's still do it. First, by the Division Algorithm, there exist unique integers q' and r' such that $a = q'b + r'$ and $0 \leqslant r' < |b|$. Consider the two following cases: either $0 \leqslant r' \leqslant \frac{1}{2}|b|$ or $\frac{1}{2}|b| < r' < |b|$. In the first case, let $q = q'$ and $r = r'$ to obtain $a = qb + r$ with $-\frac{1}{2}|b| < r \leqslant \frac{1}{2}|b|$. Similarly, if $\frac{1}{2}|b| < r' < |b|$, let $r = r' - |b|$ and $q = q' + 1$ if $b > 0$ or $q = q' - 1$ if $b. < 0$. From this, we get that $a = qb + r$ with $-\frac{1}{2}|b| < r \leqslant \frac{1}{2}|b|$.

To prove the uniqueness of q and r, suppose that there exist integers q_0 and r_0 such that $a = q_0 b + r_0$ and $-\frac{1}{2}|b| < r_0 \leqslant \frac{1}{2}|b|$. If $0 \leqslant r_0 \leqslant \frac{1}{2}|b| < |b|$, then by uniqueness of q' and r', we get that $q_0 = q'$ and $r_0 = r'$. Moreover, since $0 \leqslant r' \leqslant \frac{1}{2}|b|$, then by definition of q and r in that case, we get that $q_0 = q$ and $r_0 = r$. Otherwise, $-\frac{1}{2}|b| < r_0 < 0$. If $b > 0$, then we can write

$$a = (q_0 - 1)b + (r_0 + b)$$

with $\frac{1}{2}|b| < r_0 + b < |b|$. By uniqueness of q' and r', we get $q' = q_0 - 1$ and $r_0 + b = r'$. But since in that case $r = r' - b$ and $q = q' + 1$, then $r_0 = r$ and $q_0 = q$. Otherwise, if $b < 0$, then we can write

$$a = (q_0 + 1)b + (r_0 + |b|)$$

with $\frac{1}{2}|b| < r_0 + |b| < |b|$. By uniqueness of q' and r', we get $q' = q_0 + 1$ and $r_0 + |b| = r'$. But since in that case $r = r' - |b|$ and $q = q' - 1$, then $r_0 = r$ and $q_0 = q$. Therefore, in all possible cases, $r_0 = r$ and $q_0 = q$. It follows that q and r are unique.

8. Prove that no integer in the sequence

$$11,\ 111,\ 1111,\ 11111,\ \ldots$$

is a perfect square. [*Hint:* A typical term $111\ldots111$ can be written as $111\ldots111 = 111\ldots108 + 3 = 4k + 3$.]

Solution Since every element in the sequence can be written in the form $4k + 3$, then using one of the example in the section stating that squares must have the form $4k$ or $4k + 1$, it follows that no element in the sequence can be a square.

9. Show that the cube of any integer is of the form $7k$ or $7k \pm 1$.

Solution Let's look at possible remainders of cubes of integers when divided by 7.

Since every integer can be written as $7k$, $7k+1$, ..., $7k+6$, then we get

$$\begin{aligned}
(7k)^3 &= 7(7^2k^3)+0\\
(7k+1)^3 &= 7(7^2k^3+3\cdot 7k^2+3k)+1\\
(7k+2)^3 &= 7(7^2k^3+3\cdot 2\cdot 7k^2+4\cdot 3k+1)+1\\
(7k+3)^3 &= 7(7^2k^3+3\cdot 3\cdot 7k^2+9\cdot 3k+4)-1\\
(7k+4)^3 &= 7(7^2k^3+3\cdot 4\cdot 7k^2+16\cdot 3k+9)+1\\
(7k+5)^3 &= 7(7^2k^3+3\cdot 5\cdot 7k^2+25\cdot 3k+18)-1\\
(7k+6)^3 &= 7(7^2k^3+3\cdot 6\cdot 7k^2+36\cdot 3k+31)-1.
\end{aligned}$$

It follows that every cube must be of the form $7k$ or $7k \pm 1$.

10. For $n \geqslant 1$, establish that the integer $n(7n^2+5)$ is of the form $6k$.

Solution Notice that n must have one of the following form: $6k$, $6k+1$, ..., $6k+5$. If $n=6k$, then

$$n(7n^2+5)=6[k(7n^2+5)].$$

If $n=6k+1$, then

$$n(7n^2+5)=n(7\cdot 6^2k^2+2\cdot 7\cdot 6k+7+5)=6[n(7\cdot 6k^2+2k+2)].$$

If $n=6k+2$, then

$$n(7n^2+5)=(6k+2)(7\cdot 6^2k^2+7\cdot 4\cdot 6k+33)=6[(3k+1)(84k^2+56k+11)].$$

If $n=6k+3$, then

$$n(7n^2+5)=(6k+3)(7\cdot 6^2k^2+7\cdot 6\cdot 6k+68)=6[(2k+1)(126k^2+126k+34)].$$

If $n=6k+4$, then

$$n(7n^2+5)=(6k+4)(7\cdot 6^2k^2+7\cdot 8\cdot 6k+117)=6[(3k+2)(84k^2+112k+39)].$$

If $n=6k+5$, then

$$n(7n^2+5)=n(7\cdot 6^2k^2+7\cdot 10\cdot 6k+180)=6[n(42k+70k+30)]$$

Therefore, since it holds for all possible cases, it is clear that $n(7n^2+5)$ is of the form $6k$.

11. If n is an odd integer, show that n^4+4n^2+11 is of the form $16k$.

Solution If n is an odd integer, then it can be written as $n=4k+1$ or $4k-1$ (Exercise 7). If $n=4k+1$, then:

$$\begin{aligned}
n^4+4n^2+11 &= (4k+1)^4+4(4k+1)^2+11\\
&= 4^4k^4+4\cdot 4^3k^3+6\cdot 4^2k^2+4\cdot 4k+1+4\cdot 4^2k^2+4\cdot 4\cdot 2k+4+11\\
&= 16(16k^4+16k^3+10k^2+3k+1).
\end{aligned}$$

If $n = 4k - 1$, then:

$$\begin{aligned} n^4 + 4n^2 + 11 &= (4k-1)^4 + 4(4k-1)^2 + 11 \\ &= 4^4k^4 - 4 \cdot 4^3k^3 + 6 \cdot 4^2k^2 - 4 \cdot 4k + 1 + 4 \cdot 4^2k^2 - 4 \cdot 4 \cdot 2k + 4 + 11 \\ &= 16(16k^4 - 16k^3 + 10k^2 - 3k + 1). \end{aligned}$$

Therefore, since it holds for all possible cases, it is clear that $n^4 + 4n^2 + 11$ is of the form $16k$.

2.2 The Greatest Common Divisor

1. If $a \mid b$, show that $(-a) \mid b$, $a \mid (-b)$ and $(-a) \mid (-b)$.

Solution Since $a \mid b$, then there exists and integer k such that $b = ka$. Rewriting this equation as $b = (-k)(-a)$ lets us conclude that $(-a) \mid b$. Similarly, we can multiply both sides by -1 to obtain the new equation $-b = -ka$. Interpreting this equation as $(-b) = (-k)a$ implies that $a \mid (-b)$, and interpreting it as $(-b) = k(-a)$ implies that $(-a) \mid (-b)$.

2. Given integers a, b, c, d, verifiy that

(a) if $a \mid b$, then $a \mid bc$;

(b) if $a \mid b$ and $a \mid c$, then $a^2 \mid bc$;

(c) $a \mid b$ if and only if $ac \mid bc$, where $c \neq 0$;

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

Solution

(a) Since $a \mid b$, then there exists an integer k such that $b = ka$. Multiplying by c on both sides of the previous equation implies $bc = (kc)a$ and so $a \mid bc$.

(b) Since $a \mid b$ and $a \mid c$, then there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 a$. Multiplying these two equations together gives us $bc = (k_1 k_2)a^2$ which implies that $a^2 \mid bc$.

(c) Suppose that c is non-zero. By definition, $a \mid b$ if and only if $b = ka$ for some integer k. Since c is non-zero, then this equation holds if and only if $bc = k(ac)$. Again, by definition, this equation holds if and only if $ac \mid bc$. Therefore, $a \mid b$ if and only if $ac \mid bc$.

(d) Since $a \mid b$ and $c \mid d$, then there exist integers k_1 and k_2 such that $b = k_1 a$ and $d = k_2 c$. Multiplying these two equations together gives us $bd = (k_1 k_2)(ac)$ which implies that $ac \mid bd$.

3. Prove or disprove: if $a \mid (b + c)$, then either $a \mid b$ or $a \mid c$.

Solution This is false because $2 \mid 1 + 1$ but 2 does not divide 1.

4. For $n \geqslant 1$, use mathematical induction to establish each of the following divisibility statements:

(a) $8 \mid 5^{2n} + 7$;
[*Hint:* $5^{2k+1} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$.]

(b) $15 \mid 2^{4n} - 1$;

(c) $5 \mid 3^{3n+1} + 2^{n+1}$;

(d) $21 \mid 4^{n+1} + 5^{2n-1}$;

(e) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.

Solution

(a) When $n = 1$, we have that $5^{2n} + 7 = 25 + 7 = 32 = 8 \cdot 4$ and so $8 \mid 5^{2n} + 7$. Suppose now that $8 \mid 5^{2k} + 7$ for some $k \geqslant 1$, then $8 \mid 5^2(5^{2k} + 7)$; and notice that $8 \mid 7(1 - 5^2)$ since $7(1 - 5^2) = 7 \cdot (-3) \cdot 8$, then

$$8 \mid 5^2(5^{2k} + 7) + 7(1 - 5^2) = 5^{2(k+1)} + 7.$$

Since it also holds for $n = k + 1$, then it holds for all $n \geqslant 1$ by induction.

(b) When $n = 1$, we have that $2^{4n} - 1 = 16 - 1 = 15 \cdot 1$ and so $15 \mid 2^{4n} - 1$. Suppose now that $15 \mid 2^{4k} - 1$ for some $k \geqslant 1$, then $15 \mid 2^4(2^{4k} - 1)$; and notice that $15 \mid 2^4 - 1$, then

$$15 \mid 2^4(2^{4k} - 1) + 2^4 - 1 = 2^{4(k+1)} - 1.$$

Since it also holds for $n = k + 1$, then it holds for all $n \geqslant 1$ by induction.

(c) When $n = 1$, we have that $3^{3n+1} + 2^{n+1} = 85 = 5 \cdot 9$ and so $5 \mid 3^{3n+1} + 2^{n+1}$. Suppose now that $5 \mid 3^{3k+1} + 2^{k+1}$ for some $k \geqslant 1$, then $5 \mid 3^3(3^{3k+1} + 2^{k+1})$; and since $5 \mid 2 - 3^3 = -25$, then

$$5 \mid 3^3(3^{3k+1} + 2^{k+1}) + (2 - 3^3)2^{k+1} = 3^{3(k+1)+1} + 2^{(k+1)+1}.$$

Since it also holds for $n = k + 1$, then it holds for all $n \geqslant 1$ by induction.

(d) When $n = 1$, we have that $4^{n+1} + 5^{2n-1} = 16 + 5 = 21 \cdot 1$ and so $21 \mid 4^{n+1} + 5^{2n-1}$. Suppose now that $21 \mid 4^{k+1} + 5^{2k-1}$ for some $k \geqslant 1$, then $21 \mid 4(4^{k+1} + 5^{2k-1})$; and since $21 \mid (5^2 - 1)5^{2k-1}$, then

$$21 \mid 4(4^{k+1} + 5^{2k-1}) + (5^2 - 4)5^{2k-1} = 4^{(k+1)+1} + 5^{2(k+1)-1}.$$

Since it also holds for $n = k + 1$, then it holds for all $n \geqslant 1$ by induction.

(e) Let's use the Second Principle of Mathematical Induction. First notice that when $n = 1$, we have

$$2 \cdot 7^n + 3 \cdot 5^n - 5 = 14 + 15 - 5 = 24 \cdot 1$$

so it holds in that case. Moreover, when $n = 2$, then

$$2 \cdot 7^n + 3 \cdot 5^n - 5 = 98 + 75 - 5 = 168 = 24 \cdot 7$$

so it holds in that case as well. Suppose now that $24 \mid 2 \cdot 7^q + 3 \cdot 5^q - 5$ for all integers q smaller than or equal to some integer $k \geqslant 2$. Notice that

$$\begin{aligned} & 2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5 \\ =& 7(2 \cdot 7^k + 3 \cdot 5^k - 5) - 7 \cdot 3 \cdot 5^k + 5(2 \cdot 7^k + 3 \cdot 5^k - 5) - 2 \cdot 5 \cdot 7^k + 55 \\ =& 12(2 \cdot 7^k + 3 \cdot 5^k - 5) - 35(2 \cdot 7^{k-1} + 3 \cdot 5^{k-1} - 5) - 24 \cdot 5. \end{aligned}$$

But since by our assumption 24 divides $2 \cdot 7^k + 3 \cdot 5^k - 5$, $2 \cdot 7^{k-1} + 3 \cdot 5^{k-1} - 5$ and $24 \cdot 5$, then 24 divides any linear combinations of these three terms. In particular, 24 divides the one above which is equal to $2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5$. Thus, the statement holds for the case $n = k + 1$. Therefore, by induction, it holds for all $n \geqslant 1$.

5. Prove that for any integer a one of the integers a, $a+1$, $a+4$ is divisible by 3. [*Hint:* By the Division Algorithm, the integer a must be of the forms $3k$, $3k+1$, or $3k+2$.]

Solution Consider the three following cases: When $a = 3k$, then a is obviously divisible by 3. When $a = 3k+1$, then $a+2 = 3k+1+2 = 3(k+1)$ which makes it divisible by 3. Finally, when $a = 3k+2$, then $a+4 = 3(k+2)$ and so it is divisible by 3. Therefore, in all possible cases for a, one of a, $a+2$, $a+4$ must be divisible by 3.

6. For an arbitrary integer a, verify that

(a) $2 \mid a(a+1)$, and $3 \mid a(a+1)(a+2)$;

(b) $3 \mid a(2a^2+7)$;

(c) if a is odd, then $32 \mid (a^2+3)(a^2+7)$.

Solution

(a) Consider the two following cases for a: when $a = 2k$, then $2 \mid a$ which implies that $2 \mid a(a+1)$. When $a = 2k+1$, then $2 \mid 2(k+1) = a+1$ and so $2 \mid a(a+1)$. Thus, $2 \mid a(a+1)$ for all integers a. Let's use the same technique for the second statement by considering the three following cases: when $a = 3k$, then $3 \mid a$ and so $3 \mid a(a+1)(a+2)$. When $a = 3k+1$, then $3 \mid 3(k+1) = a+2$ and so $3 \mid a(a+1)(a+2)$. When $a = 3k+1$, then $3 \mid 3(k+1) = a+1$ and so $3 \mid a(a+1)(a+2)$. Therefore, $3 \mid a(a+1)(a+2)$ for all integers a.

(b) Consider the three following cases: When $a = 3k$, then $3 \mid a$ and so $3 \mid a(2a^2+7)$. When $a = 3k+1$, then

$$2a^2+7 = 2 \cdot 3^2k^2 + 4 \cdot 3k + 2 + 7 = 3(6k^2+4k+3)$$

and so $3 \mid 2a^2+7$ which impliues that $3 \mid a(2a^2+7)$. When $a = 3k+2$, then

$$2a^2+7 = 2 \cdot 3^2k^2 + 4 \cdot 2 \cdot 3k + 8 + 7 = 3(6k^2+8k+5)$$

and so $3 \mid 2a^2+7$ which impliues that $3 \mid a(2a^2+7)$. Therefore, $3 \mid a(2a^2+7)$ for all integers a.

(c) Let a be an odd integer, then a must be of the form $2k+1$. It follows that

$$\begin{aligned}(a^2+3)(a^2+7) &= ((2k+1)^2+3)((2k+1)^2+7)\\ &= (4k^2+4k+4)(4k^2+4k+8)\\ &= 16(k^2+k+1)(k^2+k+2).\end{aligned}$$

Now, if we let $m = k^2+k+1$, then we already proved that 2 must divide $m(m+1)$ and so $(k^2+k+1)(k^2+k+2) = 2q$. Thus,

$$(a^2+3)(a^2+7) = 32q$$

which implies that $32 \mid (a^2+3)(a^2+7)$.

7. Prove that if a and b are both odd integers, then $16 \mid a^4 + b^4 - 2$.

Solution If a and b are both odd integers, then there exist integers k and q such that $a = 2k + 1$ and $b = 2q + 1$. It follows that

$$\begin{aligned} a^4 + b^4 - 2 &= (2k+1)^4 + (2q+1)^4 - 2 \\ &= 2^4k^4 + 4 \cdot 2^3k^3 + 6 \cdot 2^2k^2 + 4 \cdot 2k \\ &\quad + 2^4q^4 + 4 \cdot 2^3q^3 + 6 \cdot 2^2q^2 + 4 \cdot 2q \\ &= 16(k^4 + q^4 + 2k^3 + 2q^3) + 8(3k^2 + k) + 8(3q^2 + q). \end{aligned}$$

Let's focus on the term $3k^2 + k$. If k is even, then it follows that $3k^2 + k$ is even as well. If k is odd, then $3k^2$ must also be odd. But then, $3k^2 + k$ is even since it is the sum of two odd numbers. Therefore, $3k^2 + k$ is even for all k. It follows that $3k^2 + k = 2k_0$ for some integer k_0. The same argument shows that $3q^2 + q = 2q_0$ for some integer q_0. Hence, we can rewrite the above equation as follows:

$$a^4 + b^4 - 2 = 16(k^4 + q^4 + 2k^3 + 2q^3 + k_0 + q_0)$$

from which we directly see that $16 \mid a^4 + b^4 - 2$.

8. Prove that

(a) the sum of the squares of two odd integers cannot be a perfect square;

(b) the product of four consecutive integers is 1 less than a perfect square.

Solution

(a) Let $2k + 1$ and $2q + 1$ be two odd integers, then the sum of their squares

$$(2k+1)^2 + (2q+1)^2 = 4k^2 + 4k + 1 + 4q^2 + 4q + 1 = 4(k^2 + q^2 + k + q) + 2$$

is of the form $4m + 2$. However, we already proved that perfect squares must have the forms $4n$ or $4n + 1$. Therefore, the sum of two odd integers cannot be a square.

(b) Let a be an integer, then

$$\begin{aligned} a(a+1)(a+2)(a+3) &= a(a^2 + 3a + 2)(a+3) \\ &= a(a^3 + 6a^2 + 11a + 6) \\ &= [a^4 + 6a^3 + 11a^2 + 6a + 1] - 1 \\ &= (a^2 + 3a + 1)^2 - 1. \end{aligned}$$

Since it holds for all integers a, then the product of any four consecutive integers is 1 less than a square.

9. Establish that the difference of two consecutive cubes is never divisible by 2.

Solution Let a be an integer, then

$$(a+1)^3 - a^3 = 3(a^2 + a) + 1.$$

Since taking the square of a number preserves its parity, then a^2 and a must have the same parity. It follows that their sum must be even and so $a^2 + a = 2k$. Thus:

$$(a+1)^3 - a^3 = 2(3k) + 1$$

which implies that the difference of two cubes is always odd.

10. For a nonzero integer a, show that $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$, and $\gcd(a, 1) = 1$.

Solution We know that the greatest common divisor of a and b can be intepreted as the smallest positive linear combination of a and b. But since the positive linear combinations of a and 0 are precisely the positive multiples of a, then it follows that $\gcd(a, 0) = |a|$ since $|a|$ is the least positive multiple of a. Similarly, the positive linear combinations of a and a are precisely the positive multiples of a and so $\gcd(a, a) = |a|$ for the same reasons. Finally, since

$$a \cdot 0 + 1 \cdot 1 = 1,$$

then $\gcd(a, 1) = 1$ by Theorem 2-4.

11. If a and b are integers, not both of which are zero, verify that

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

Solution Notice that

$$(-a)(-x) + by = ax + (-b)(-y) = (-a)(-x) + (-b)(-y)$$

implies that the set of positive linear combinations of a and b is precisely equal to the set of linear combinations of $-a$ and b, a and $-b$, and $-a$ and $-b$. Therefore, it follows that

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

12. Prove that, for a positive integer n and any integer a, $\gcd(a, a+n)$ divides n; hence, $\gcd(a, a+1) = 1$.

Solution First, we know that $\gcd(a, a+n)$ must divide any linear combination of a and $a+n$. In particular, it must divide

$$a \cdot (-1) + (a+n) \cdot 1 = n.$$

13. Given integers a and b, prove that

(a) there exist integers x and y for which $c = ax + by$ if and only if $\gcd(a, b) \mid c$.

(b) if there exist integers x and y for which $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

Solution

(a) If c is a linear combination of a and b, then $\gcd(a,b)$ divides it since it divides both a and b. If $\gcd(a,b) \mid c$, then $c = k \cdot \gcd(a,b)$. But since there exist integers x_0 and y_0 such that $\gcd(a,b) = ax_0 + by_0$, then $c = a(kx_0) + b(ky_0)$. Therefore, c is a linear combination of a and b if and only if it is a multiple of $\gcd(a,b)$.

(b) We know that if $\gcd(a,b) = ax + by$, then $ax + by$ is the least positive linear combination of a and b. By contradiction, if $\gcd(x,y) \neq 1$, then $\gcd(x,y) > 1$ and so

$$0 < a\left(\frac{x}{\gcd(x,y)}\right) + b\left(\frac{y}{\gcd(x,y)}\right) < ax + by$$

which contradicts the fact that $ax+by$ is the smallest positive linear combination. Therefore, $\gcd(x,y) = 1$.

14. For any integer a, show that

(a) $\gcd(2a+1, 9a+4) = 1$;

(b) $\gcd(5a+2, 7a+3) = 1$;

(c) if a is odd, then $\gcd(3a, 3a+2) = 1$.

Solution

(a) It suffices to notice that

$$(2a+1)\cdot 5 + (9a+4)\cdot(-1) = 1.$$

(b) It suffices to notice that

$$(5a+2)\cdot(-4) + (7a+3)\cdot 3 = 1.$$

(c) We know that $\gcd(3a, 3a+2)$ divides any linear combination of $3a$ and $3a+2$. In particular, it must divide

$$3a\cdot(-1) + (3a+2)\cdot 1 = 2.$$

Hence, $\gcd(3a, 3a+2)$ is either 1 or 2. By contradiction, if $\gcd(3a, 3a+2) = 2$, then $2 \mid 3a$. Moreover, since $\gcd(2,3) = 1$, then $2 \mid 3a$ implies that $2 \mid a$ which is impossible since a is odd. Therefore, $\gcd(3a, 3a+2) = 1$.

15. If a and b are integers, not both of which are zero, prove that $\gcd(2a-3b, 4a-5b)$ divides b; hence, $\gcd(2a+3, 4a+5) = 1$.

Solution Since $\gcd(2a-3b, 4a-5b)$ divides all linear combinations of $2a-3b$ and $4a-5b$, then it divides

$$(2a-3b)\cdot(-2) + (4a-5b)\cdot 1 = b.$$

16. Given an odd integer a, establish that

$$a^2 + (a+2)^2 + (a+4)^2 + 1$$

is divisible by 12.

Solution Since a is odd, then $a = 2k + 1$ for some integer k. Thus:

$$\begin{aligned} a^2 + (a+2)^2 + (a+4)^2 + 1 &= (2k+1)^2 + (2k+3)^2 + (2k+5)^2 + 1 \\ &= 12k^2 + 36k + 36 \\ &= 12(k^2 + 3k + 3). \end{aligned}$$

Therefore, $12 \mid a^2 + (a+2)^2 + (a+4)^2 + 1$.

17. Prove that $(2n)!/n!(n+1)!$ is an integer for all $n \geqslant 0$.
[*Hint:* Note that $\binom{2n}{n}(2n+1) = \binom{2n+1}{n+1}(n+1)$.]

Solution Using the definition of the binomial coefficients, we have that

$$\frac{(2n)!}{n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n}.$$

Hence, it suffices to show that $n+1$ divides $\binom{2n}{n}$. But since

$$\binom{2n}{n}(2n+1) = \binom{2n+1}{n+1}(n+1),$$

then by definition, $n+1$ divides $\binom{2n}{n}(2n+1)$. However, from the fact that

$$2(n+1) - (2n+1) = 1,$$

we have that $\gcd(2n+1, n+1) = 1$ which lets us conclude, by Euclid's Lemma, that $n+1$ divides $\binom{2n}{n}$. Therefore, $(2n)!/n!(n+1)!$ is an integer.

18. Prove: the product of any three consecutive integers is divisible by 6; the product of any four consecutive integers is divisible by 24; the product of any five consecutive integers is divisible by 120. [*Hint:* See Corollary 2 to Theorem 2-4.]

Solution First, we know that for any integer a, one of a and $a+1$ is divisible by 2 by considering the cases where a is even and odd. Similarly, we know that one of a, $a+1$, $a+2$ must be divisible by 3 by considering the cases $a = 3k$, $a = 3k+1$, $a = 3k+2$. In the same way, one of a, $a+1$, $a+2$, $a+3$ is divisible by 4 and another of them is divisible by 2 which makes the product of the four factors divisible by 8. Finally, As we did above, we can easily prove that one of a, $a+1$, $a+2$, $a+3$, $a+4$ is divisible by 5. Hence, it follows from Corollary 2 that the product of three consecutive factors is divisble by 6 since $\gcd(2,3) = 1$; the product of four factors is divisible by 24 since $\gcd(3,8) = 1$; and the product of five factors is divisible by 120 since $\gcd(24,5) = 1$.

19. Establish each of the assertions below:

(a) If a is an arbitrary integer, then $6 \mid a(a^2 + 11)$.

(b) If a is an odd integer, then $24 \mid a(a^2 - 1)$. [*Hint:* The square of an odd integer is of the form $8k + 1$.]

(c) If a and b are odd integers, then $8 \mid (a^2 - b^2)$.

(d) If a is an integer not divisible by 2 or 3, then $24 \mid (a^2 + 23)$. [*Hint:* Any integer a must assume one of the forms $6k$, $6k + 1$, ..., $6k + 5$.]

Solution

(a) Let's split the proof in six cases. If $a = 6k$, then $6 \mid a$ and so $6 \mid a(a^2 + 11)$. If $a = 6k + 1$, then

$$a^2 + 11 = 6^2k^2 + 2 \cdot 6k + 12 = 6(6k^2 + 2k + 2)$$

and so $6 \mid a(a^2 + 11)$. If $a = 6k + 2$, then

$$a(a^2 + 11) = (6k + 2)(6^2k^2 + 4 \cdot 6k + 15) = 6(3k + 1)(12k^2 + 8k + 5)$$

and so $6 \mid a(a^2 + 11)$. If $a = 6k + 3$, then

$$a(a^2 + 11) = (6k + 3)(6^2k^2 + 6^2k + 20) = 6(2k + 1)(18k^2 + 18k + 10)$$

and so $6 \mid a(a^2 + 11)$. If $a = 6k + 4$, then

$$a(a^2 + 11) = (6k + 4)(6^2k^2 + 8 \cdot 6k + 27) = 6(3k + 2)(12k^2 + 16k + 9)$$

and so $6 \mid a(a^2 + 11)$. If $a = 6k + 5$, then

$$a(a^2 + 11) = a(6^2k^2 + 10 \cdot 6k + 36) = 6a(6k^2 + 10k + 6)$$

and so $6 \mid a(a^2 + 11)$. Therefore, $6 \mid a(a^2 + 11)$ for all integers a.

(b) First, rewrite $a(a^2 - 1)$ as $(a - 1)a(a + 1)$ which shows that it is the product of three succesive integers. Hence, it must be divisible by 3. Since a is odd, then $a - 1$ is even and so $(a - 1)(a + 1)$ is of the form $m(m + 2)$ where m is even. By considering the cases $m = 4k$ and $m = 4k + 2$, we get that $(a - 1)(a + 1)$ must be divisible by 8. Thus, $a(a^2 - 1)$ is divisible by both 8 and 3. Since $\gcd(8, 3) = 1$, then $24 \mid a(a^2 - 1)$.

(c) If $a = 2k + 1$ and $b = 2q + 1$, then

$$a^2 - b^2 = (2k - 2q)(2k + 2q + 2) = 4(k - q)(k + q + 1).$$

If k and q have the same parity, then $k - q$ is even and so $a^2 - b^2 = 8k_0$. If k and q have distinct parities, then $k + q + 1$ is even and so $a^2 - b^2 = 8k_0$. Thus, in all possible cases, $8 \mid (a^2 - b^2)$.

(d) If a is not divisble by 2 or by 3, then it must have the form $6k + 1$ or $6k + 5$. In the case $a = 6k + 1$, we have

$$a^2 + 23 = 36k^2 + 12k + 24 = 12(3k^2 + k) + 24.$$

Since $3k^2$ has the same parity as k, then $3k^2 + k$ must be even, and so it can be written as $2k_0$. Hence, $a^2 + 23 = 24(k_0 + 1)$ which implies that $24 \mid (a^2 + 23)$. Next, if $a = 6k + 5$, then equivalently, it has the form $a = 6q - 1$. In that case,

$$a^2 + 23 = 36k^2 - 12k + 24 = 12(3k^2 - k) + 24.$$

Using the same argument as above, $3k^2 - k = 2k_0$ and so $a^2 + 23 = 24(k_0 + 1)$ which proves that $24 \mid (a^2 + 23)$.

20. Confirm the following properties of the greatest common divisor:

(a) If $\gcd(a,b) = 1$, and $\gcd(a,c) = 1$, then $\gcd(a,bc) = 1$. [*Hint:* Since $1 = ax + by = au + cv$ for some x, y, u, v, $1 = (ax+by)(au+cv) = a(aux+byu)+bc(yv)$.]

(b) If $\gcd(a,b) = 1$, and $c \mid a$, then $\gcd(b,c) = 1$.

(c) If $\gcd(a,b) = 1$, then $\gcd(ac,b) = \gcd(c,b)$.

(d) If $\gcd(a,b) = 1$, and $c \mid a+b$, then $\gcd(a,c) = \gcd(b,c) = 1$. [*Hint:* Let $d = \gcd(a,c)$. Then $d \mid a$, $d \mid c$ implies that $d \mid (a+b) - a$, or $d \mid b$.]

(e) If $\gcd(a,b) = 1$, $d \mid ac$, and $d \mid bc$, then $d \mid c$.

(f) If $\gcd(a,b) = 1$, then $\gcd(a^2,b^2) = 1$. [*Hint:* First show that $\gcd(a^2,b) = \gcd(a,b^2) = 1$.]

Solution

(a) We know that there exist integers x, y, u, v such that $ax+by = 1$ and $au+cv = 1$. Multiplying these two equations gives us $a(aux + byu) + bc(yv) = 1$ and so $\gcd(a,bc) = 1$.

(b) Since $\gcd(a,b) = 1$, then there exist integers x and y such that $ax + by = 1$. Since $c \mid a$, then there exists an integer k such that $a = kc$. Replacing the value of a with this new expression in the linear combination gives us $c(kx)+by = 1$. Therefore, $\gcd(c,b) = 1$.

(c) Since $\gcd(c,b)$ divides both ac and b, then it divides $\gcd(ac,b)$. Conversely, $\gcd(ac,b)$ divides b. Moreover, since $\gcd(ac,b)$ divides b and $\gcd(a,b) = 1$, then $\gcd(a,\gcd(ac,b)) = 1$. It follows that from the fact that $\gcd(ac,b) \mid ac$, we get that $\gcd(ac,b) \mid c$. Thus, $\gcd(ac,b) \mid \gcd(c,b)$ since it divides both c and b. Therefore, $\gcd(ac,b) = \gcd(c,b)$ since both divide the other and both are positive.

(d) Let $d_a = \gcd(a,c)$, then by definition, $d_a \mid a$ and $d_a \mid c$. From the fact that $c \mid a+b$, we get that d_a divides both a and $a+b$. It follows that $d_a \mid (a+b) - a = b$. Since it divides both a and b, then it divides $\gcd(a,b) = 1$. Therefore, $\gcd(a,c) = d_a = 1$. The proof is strictly the same for $d_b = \gcd(b,c)$.

(e) If $\gcd(a,b) = 1$, then there exist integers x and y such that $ax + by = 1$. Since d divides both ac and bc, then it divides any of their linear combinations. In particular, d divides

$$acx + bcy = c(ax + by) = c.$$

(f) Using part (c) of this exercise with $c = a$, we have that $\gcd(a^2,b) = \gcd(a,b) = 1$. Similarly, if we now apply part (c) with $a = b$, $b = a^2$ and $c = b$, we obtain $\gcd(a^2,b^2) = \gcd(a^2,b) = 1$.

21. Prove that if $d \mid n$, then $2^d - 1 \mid 2^n - 1$. [*Hint:* Employ the identity $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + 1)$.]

Solution Since $d \mid n$, then $n = dk$ for some integer k. It follows that

$$2^n - 1 = \frac{(2^d)^k - 1}{2^d - 1}(2^d - 1) = ((2^d)^{k-1} + \cdots + 1)(2^d - 1).$$

Therefore, $2^d - 1 \mid 2^n - 1$.

2.3 The Euclidean Algorithm

1. Find $\gcd(143,227)$, $\gcd(306,657)$ and $\gcd(272,1479)$.

Solution Let's apply the Euclidean Algorithm:

$$\begin{aligned}
227 &= 1\cdot 143+84\\
143 &= 1\cdot 84+59\\
84 &= 1\cdot 59+25\\
59 &= 2\cdot 25+9\\
25 &= 2\cdot 9+7\\
9 &= 1\cdot 7+2\\
7 &= 3\cdot 2+1\\
2 &= 2\cdot 1+0
\end{aligned}$$

and so $\gcd(143,227)=1$.

$$\begin{aligned}
657 &= 2\cdot 306+45\\
306 &= 6\cdot 45+36\\
45 &= 1\cdot 36+9\\
36 &= 4\cdot 9+0
\end{aligned}$$

and so $\gcd(306,657)=9$.

$$\begin{aligned}
1479 &= 5\cdot 272+119\\
272 &= 2\cdot 119+34\\
119 &= 3\cdot 34+17\\
34 &= 2\cdot 17+0
\end{aligned}$$

and so $\gcd(272,1479)=17$.

2. Use the Euclidean Algorithm to obtain integers x and y satisfying

(a) $\gcd(56,72)=56x+72y$;

(b) $\gcd(24,138)=24x+138y$;

(c) $\gcd(119,272)=119x+272y$;

(d) $\gcd(1769,2378)=1769x+2378y$;

Solution

(a) First, let's apply the Euclidean Algorithm:

$$\begin{aligned}
72 &= 1\cdot 56+16\\
56 &= 3\cdot 16+8\\
16 &= 2\cdot 8+0.
\end{aligned}$$

Now, running these equations backward gives us

$$\begin{aligned} 8 &= 56 - 3 \cdot 16 \\ &= 56 - 3(72 - 56) \\ &= 4 \cdot 56 - 3 \cdot 72. \end{aligned}$$

Thus, $x = 4$ and $y = -3$.

(b) First, let's apply the Euclidean Algorithm:

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Now, running these equations backward gives us

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138 \end{aligned}$$

Thus, $x = 6$ and $y = -1$.

(c) First, let's apply the Euclidean Algorithm:

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0. \end{aligned}$$

Now, running these equations backward gives us

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3(272 - 2 \cdot 119) \\ &= 7 \cdot 119 - 3 \cdot 272 \end{aligned}$$

Thus, $x = 7$ and $y = -3$.

(d) First, let's apply the Euclidean Algorithm:

$$\begin{aligned} 2378 &= 1 \cdot 1769 + 610 \\ 1769 &= 2 \cdot 610 + 549 \\ 610 &= 1 \cdot 549 + 61 \\ 549 &= 9 \cdot 61 + 0. \end{aligned}$$

Now, running these equations backward gives us

$$\begin{aligned} 61 &= 610 - 549 \\ &= 610 - (1769 - 2 \cdot 610) \\ &= 3 \cdot 610 - 1769 \\ &= 3(2378 - 1769) - 1769 \\ &= 3 \cdot 2378 - 4 \cdot 1769. \end{aligned}$$

Thus, $x = -4$ and $y = 3$.

3. Prove that if d is a common divisor of a and b, then $d = \gcd(a, b)$ if and only if $\gcd(a/d, b/d) = 1$. [*Hint:* Use Theorem 2-7.]

Solution Suppose that $d = \gcd(a, b)$ and write $d = ax + by$, then dividing both sides by d gives us $1 = (a/d)x + (b/d)y$. Thus, $\gcd(a/d, b/d) = 1$. Suppose now that $\gcd(a/d, b/d) = 1$, then by multiplying both sides by d, we get

$$\gcd(a, b) = d \gcd(a/d, b/d) = d.$$

4. Assuming that $\gcd(a, b) = 1$, prove the following:

(a) $\gcd(a + b, a - b) = 1$ or 2.

[*Hint:* Let $d = \gcd(a + b, a - b)$ and show that $d \mid 2a$, $d \mid 2b$; thus, that $d \leqslant \gcd(2a, 2b) = 2\gcd(a, b)$.]

(b) $\gcd(2a + b, a + 2b) = 1$ or 3.

(c) $\gcd(a + b, a^2 + b^2) = 1$ or 2.

[*Hint:* $a^2 + b^2 = (a + b)(a - b) + 2b^2$.]

(d) $\gcd(a + b, a^2 - ab + b^2) = 1$ or 3.

[*Hint:* $a^2 - ab + b^2 = (a + b)^2 - 3ab$.]

Solution

(a) Let $d = \gcd(a + b, a - b)$, then $d \mid a + b$ and $d \mid a - b$. It follows that $d \mid (a + b) + (a - b) = 2a$ and $d \mid (a + b) - (a - b) = 2b$. Hence, $d \leqslant \gcd(2a, 2b) = 2\gcd(a, b) = 2$. It follows that $\gcd(a + b, a - b) = d$ is either 1 or 2.

(b) Let $d = \gcd(2a + b, a + 2b)$, then $d \mid 2a + b$ and $d \mid a + 2b$. It follows that $d \mid 2(a + 2b) - (2a + b) = 3b$ and $d \mid 2(2a + b) - (a + 2b) = 3a$. Hence, $d \mid \gcd(3a, 3b) = 3\gcd(a, b) = 3$. Therefore, d is either 1 or 3.

(c) Let $d = \gcd(a + b, a^2 + b^2)$, then $d \mid a + b$ and $d \mid a^2 + b^2$. It follows that $d \mid (a^2 + b^2) - (a + b)(a - b) = 2b^2$ and $d \mid 2(a^2 + b^2) - 2b^2 = 2a^2$. Hence, $d \mid \gcd(2a^2, 2b^2) = 2\gcd(a^2, b^2) = 2$ (Exercise 2.2.20(f)). Therefore, d is either 1 or 2.

(d) Let $d = \gcd(a + b, a^2 - ab + b^2)$ and recall that $\gcd(a, b) = 1 \implies \gcd(a^2, b^2)$. Since $d \mid a + b$ and $d \mid a^2 - ab + b^2$, then $d \mid (a + b)^2 - (a^2 - ab + b^2) = 3ab$. But since $d \mid 3a(a + b)$ and $d \mid 3ab$, we get that $d \mid 3a^2 + 3ab - 3ab = 3a^2$. Similarly, since $d \mid 3b(a + b)$ and $d \mid 3ab$, we get that $d \mid 3ab + 3b^2 - 3ab = 3b^2$. Thus, d divides both $3a^2$ and $3b^2$ and so $d \mid \gcd(3a^2, 3b^2) = 3\gcd(a, b) = 3$. Therefore, $d = 1$ or $d = 3$.

5. For positive integers a, b and $n \geqslant 1$, show that

(a) If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$. [*Hint:* See Problem A°(a), Section 2.2.]

(b) The relation $a^n \mid b^n$ implies that $a \mid b$. [*Hint:* Put $d = \gcd(a, b)$ and write $a = rd$, $b = sd$, where $\gcd(r, s) = 1$. By part (a), $\gcd(r^n, s^n) = 1$. Show that $r = 1$, whence $a = d$.]

Solution

(a) First, let's prove by induction that if $\gcd(c_1, c_2) = 1$, then $\gcd(c_1, c_2^n) = 1$ for all $n \geqslant 1$. When $n = 1$, it holds from our assumption. Suppose now that $\gcd(c_1, c_2^k) = 1$ for some integer $k \geqslant 1$, then using the fact that $\gcd(c_1, c_2) = 1$ and Exercise 2.2.20(a), we get that $\gcd(c_1, c_2^{k+1}) = 1$. Thus, by induction, $\gcd(c_1, c_2^n) = 1$ for all $n \geqslant 1$. Taking $c_1 = a$ and $c_2 = b$, we get that $\gcd(a, b^n) = 1$ for all $n \geqslant 1$. Fixing $n \geqslant 1$ and taking now $c_1 = b^n$ and $c_2 = a$, we get that $\gcd(a^m, b^n) = 1$ for all $m \geqslant 1$. In particular, if we take $m = n$, we get that $\gcd(a^n, b^n) = 1$.

(b) Suppose that $a^n \mid b^n$, then $\gcd(a^n, b^n) = a^n$. Let $d = \gcd(a, b)$, then there exist relatively prime integers r and s such that $a = rd$ and $b = sd$. Since $\gcd(r, s) = 1$, then $\gcd(r^n, s^n) = 1$ by part (a). It follows that from the equations $a^n = r^n d^n$ and $b^n = s^n d^n$, since r^n and s^n are relatively prime, then $d^n = \gcd(a^n, b^n) = a^n = r^n d^n$. By cancelling out the d^n's on both sides we get $r^n = 1$. Since both a and d are positive, then r must be positive as well from the equation $a = rd$. Hence, from $r^n = 1$ we conclude that $r = 1$. Thus, $a = d = \gcd(a, b) \mid b$.

6. Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

Solution Let $d = \gcd(a + b, ab)$, then $d \mid a + b$ and $d \mid ab$. It follows that $d \mid a(a + b) - ab = a^2$. Similarly, $d \mid b(a + b) - ab = b^2$. Thus, $d \mid \gcd(a^2, b^2) = 1$ since it divides both a^2 and b^2.

7. For nonzero integers a and b, verify that the following conditions are equivalent:

$$\text{(a) } a \mid b \qquad \text{(b) } \gcd(a, b) = |a| \qquad \text{(c) } \operatorname{lcm}(a, b) = |b|$$

Solution Suppose that $a \mid b$, then $|a|$ divides both a and b. Since any divisor of a must divide $|a|$, then it follows that $\gcd(a, b) = |a|$.

Suppose that $\gcd(a, b) = |a|$, then the equation $\gcd(a, b) \operatorname{lcm}(a, b) = |a| \cdot |b|$ becomes $\operatorname{lcm}(a, b) = |b|$.

Suppose that $\operatorname{lcm}(a, b) = |b|$, then $|b|$ is a multiple of a. Equivalently, b is a multiple of a which is another way of saying that $a \mid b$.

8. Find $\operatorname{lcm}(143, 227)$, $\operatorname{lcm}(306, 657)$ and $\operatorname{lcm}(272, 1479)$.

Solution For each of these, let's find their greatest common divisor first using the Euclidean Algorithm.

$$\begin{aligned}
227 &= 1 \cdot 143 + 84 \\
143 &= 1 \cdot 84 + 59 \\
84 &= 1 \cdot 59 + 25 \\
59 &= 2 \cdot 25 + 9 \\
25 &= 2 \cdot 9 + 7 \\
9 &= 1 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

which shows that $\gcd(143, 227) = 1$. It follows that

$$\operatorname{lcm}(143, 227) = 143 \cdot 227 = 32461.$$

Let's apply the same procedure to find $\operatorname{lcm}(306, 657)$:

$$\begin{aligned} 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 + 0. \end{aligned}$$

Hence, $\gcd(306, 657) = 9$. It follows that

$$\operatorname{lcm}(306, 657) = \frac{306 \cdot 657}{9} = 306 \cdot 73 = 22338.$$

Let's apply the same procedure to find $\operatorname{lcm}(306, 657)$:

$$\begin{aligned} 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 + 0. \end{aligned}$$

Hence, $\gcd(306, 657) = 9$. It follows that

$$\operatorname{lcm}(306, 657) = \frac{306 \cdot 657}{9} = 306 \cdot 73 = 22338.$$

Let's apply the same procedure to find $\operatorname{lcm}(272, 1479)$:

$$\begin{aligned} 1479 &= 5 \cdot 272 + 119 \\ 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Hence, $\gcd(272, 1479) = 17$. It follows that

$$\operatorname{lcm}(272, 1479) = \frac{272 \cdot 1479}{17} = 16 \cdot 1479 = 23664.$$

9. Prove that the greatest common divisor of two positive integers always divides their least common multiple.

Solution Let a and b be two positive integers, then $\gcd(a, b)$ divides a which in turns divides $\operatorname{lcm}(a, b)$. Hence, by transitivity, $\gcd(a, b) \mid \operatorname{lcm}(a, b)$.

10. Given nonzero integers a and b, establish the following facts concerning $\operatorname{lcm}(a, b)$:

(a) $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.

(b) If $k > 0$, then $\operatorname{lcm}(ka, kb) = k \operatorname{lcm}(a, b)$.

(c) If m is any common multiple of a and b, then $\operatorname{lcm}(a,b) \mid m$.

[*Hint:* Put $t = \operatorname{lcm}(a,b)$ and use the Division Algorithm to write $m = qt + r$, where $0 \leqslant r < t$. Show that r is a common multiple of a and b.]

Solution

(a) Suppose that $\gcd(a,b) = \operatorname{lcm}(a,b)$. Since $\gcd(a,b) \mid a$ and $a \mid \operatorname{lcm}(a,b) = \gcd(a,b)$, then $a = \gcd(a,b)$. Similarly, since $\gcd(a,b) \mid b$ and $b \mid \operatorname{lcm}(a,b) = \gcd(a,b)$, then $\gcd(a,b) = b$. Therefore, $a = \gcd(a,b) = b$. Conversely, if $a = b$, then $\gcd(a,b) = a = b$ and $\operatorname{lcm}(a,b) = a = b$ which shows that $\operatorname{lcm}(a,b) = \gcd(a,b)$.

(b) Let $k > 0$ be an integer, then from the formula of the least common multiple in terms of the greatest common divisor, we obtain:

$$\operatorname{lcm}(ka,kb) = \frac{k^2ab}{\gcd(ka,kb)} = k\frac{ab}{\gcd(a,b)} = k\operatorname{lcm}(a,b).$$

(c) Suppose that m is a common multiple of a and b, then by the Division Algroithm, there exist integers q and r such that $m = q\operatorname{lcm}(a,b) + r$ and $0 \leqslant r < \operatorname{lcm}(a,b)$. Suppose that $r \neq 0$ and notice that $r = m - q\operatorname{lcm}(a,b)$ must be divisible by both a and b since a and b divide both m and $\operatorname{lcm}(a,b)$, it follows that $\operatorname{lcm}(a,b) \leqslant r$ contradicting the fact that $r < \operatorname{lcm}(a,b)$. Thus, $r = 0$ and so $\operatorname{lcm}(a,b) \mid m$.

11. Let a, b, c be integers, no two of which are zero, and $d = \gcd(a,b,c)$. Show that

$$d = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b).$$

Solution Let $d_0 = \gcd(\gcd(a,b),c)$, then $d_0 \mid \gcd(a,b)$ and $d_0 \mid c$. Since $\gcd(a,b)$ divides a and b, then d_0 also divides a and b. It follows that d_0 is a common divisor of a, b and c. To show that it is the greatest, let e be a common divisor of a, b and c, since e divides both a and b, then it must divide $\gcd(a,b)$. Hence, e divides both $\gcd(a,b)$ and c which implies that $e \leqslant \gcd(\gcd(a,b),c)$. Therefore, $d = d_0$. The proofs of the other equalities are strictly the same.

12. Find integers x, y, z satisfying

$$\gcd(198,288,512) = 198x + 288y + 512z.$$

[*Hint:* Put $d = \gcd(198,288)$. Since $\gcd(198,288,512) = \gcd(d,512)$, first find integers u and v for which $\gcd(d,512) = du + 512v$.]

Solution First, let's find $\gcd(198,288)$ using the Euclidean Algorithm:

$$\begin{aligned} 288 &= 1 \cdot 198 + 90 \\ 198 &= 2 \cdot 90 + 18 \\ 90 &= 5 \cdot 18 + 0. \end{aligned}$$

Hence, $\gcd(198, 288) = 18$. Let's use these equations to find the linear combination:

$$\begin{aligned} 18 &= 198 - 2 \cdot 90 \\ &= 198 - 2(288 - 198) \\ &= 3 \cdot 198 - 2 \cdot 288. \end{aligned}$$

Now, let's find $\gcd(198, 228, 512) = \gcd(18, 512)$ using the Euclidean Algorithm:

$$\begin{aligned} 512 &= 28 \cdot 18 + 8 \\ 18 &= 2 \cdot 8 + 2 \\ 8 &= 4 \cdot 2 + 0. \end{aligned}$$

Hence, $\gcd(198, 288, 512) = 1$. Let's use these equations to find the linear combination:

$$\begin{aligned} 2 &= 18 - 2 \cdot 8 \\ &= 18 - 2(512 - 28 \cdot 18) \\ &= 57 \cdot 18 - 2 \cdot 512. \end{aligned}$$

Replacing 18 with the linear combination of 198 and 288 gives us

$$\gcd(198, 288, 512) = 171 \cdot 198 - 114 \cdot 288 - 2 \cdot 512$$

giving us $x = 171$, $y = 114$ and $z = -2$.

2.4 The Diophantine Equation $ax + by = c$

1. Which of the following Diophantine equations cannot be solved ?

(a) $6x + 51y = 22$;

(b) $33x + 14y = 115$;

(c) $14x + 35y = 93$.

Solution

(a) Let's use the Euclidean Algorithm to find $\gcd(6, 51)$:

$$\begin{aligned} 51 &= 4 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Hence, $\gcd(6, 51) = 3$. But 22 is not divisible by 3 so this equation cannot be solved.

(b) Let's use the Euclidean Algorithm to find $\gcd(33, 14)$:

$$\begin{aligned} 33 &= 2 \cdot 14 + 5 \\ 14 &= 2 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Hence, $\gcd(33, 14) = 1$. Since 115 is divisible by 1, then this equation can be solved.

(c) Let's use the Euclidean Algorithm to find $\gcd(14, 35)$:

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

Hence, $\gcd(14, 35) = 7$. But $93 = 13 \cdot 7 + 2$ is not divisible by 7 so this equation cannot be solved.

2. Determine all solutions in the integers of the following Diophantine equations:

(a) $56x + 72y = 40$;

(b) $24x + 138y = 18$;

(c) $221x + 35y = 11$.

Solution

(a) First, let's apply the Euclidean Algorithm to find $\gcd(56, 72)$:

$$\begin{aligned} 72 &= 1 \cdot 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0. \end{aligned}$$

Hence, $\gcd(56, 72) = 8$. Since $40 = 5 \cdot 8$ is divisible by 8, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 8 &= 56 - 3 \cdot 16 \\ &= 56 - 3(72 - 56) \\ &= 4 \cdot 56 - 3 \cdot 72. \end{aligned}$$

Multiplying both sides by 5:

$$20 \cdot 56 - 15 \cdot 72 = 40$$

gives us the solution $x_0 = 20$, $y_0 = -15$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{72}{8}t = 20 + 9t$ and $y = y_0 - \frac{56}{8}t = -15 - 7t$ where t is an integer.

(b) First, let's apply the Euclidean Algorithm to find $\gcd(24, 138)$:

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Hence, $\gcd(24, 138) = 6$. Since 18 is divisible by 6, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138. \end{aligned}$$

Multiplying both sides by 3:

$$18 \cdot 24 - 3 \cdot 138 = 18$$

gives us the solution $x_0 = 18$, $y_0 = -3$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{138}{6}t = 18 + 23t$ and $y = y_0 - \frac{24}{6}t = -3 - 4t$ where t is an integer.

(c) First, let's apply the Euclidean Algorithm to find $\gcd(221, 35)$:

$$\begin{aligned} 221 &= 6 \cdot 35 + 11 \\ 35 &= 3 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Hence, $\gcd(221, 35) = 1$. Since 11 is divisible by 1, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 \\ &= 11 - 5(35 - 3 \cdot 11) \\ &= 16 \cdot 11 - 5 \cdot 35 \\ &= 16(221 - 6 \cdot 35) - 5 \cdot 35 \\ &= 16 \cdot 221 - 101 \cdot 35. \end{aligned}$$

Multiplying both sides by 11:

$$176 \cdot 221 - 1111 \cdot 35 = 11$$

gives us the solution $x_0 = 176$, $y_0 = -1111$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{35}{1}t = 176 + 35t$ and $y = y_0 - \frac{221}{1}t = -1111 - 221t$ where t is an integer.

3. Determine all solutions in the positive integers of the following Diophantine equations:

(a) $18x + 5y = 48$;

(b) $54x + 21y = 906$;

(c) $123x + 360y = 99$;

(d) $158x - 57y = 7$.

Solution

(a) First, let's apply the Euclidean Algorithm to find $\gcd(18, 5)$:

$$\begin{aligned} 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Hence, $\gcd(18, 5) = 1$. Since 48 is divisible by 1, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2(18 - 3 \cdot 5) - 5 \\ &= 2 \cdot 18 - 7 \cdot 5. \end{aligned}$$

Multiplying both sides by 48:

$$96 \cdot 18 - 336 \cdot 5 = 48$$

gives us the solution $x_0 = 96$, $y_0 = -336$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{5}{1}t = 96 + 5t$ and $y = y_0 - \frac{18}{1}t = -336 - 18t$ where t is an integer. To find the positive solutions, it suffices to solve the following inequalities: $x = 96 + 5t > 0$ and $y = -336 - 18t > 0$. This is equivalent to the inequality:

$$-\frac{96}{5} < t < -\frac{336}{18}$$

Since t is an integer, then the only possible value tp have $x, y > 0$ is at $t = -19$.

(b) First, let's apply the Euclidean Algorithm to find $\gcd(54, 21)$:

$$\begin{aligned} 54 &= 2 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Hence, $\gcd(54, 21) = 3$. Since 906 is divisible by 3, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 3 &= 12 - 9 \\ &= 12 - (21 - 12) \\ &= 2 \cdot 12 - 21 \\ &= 2(54 - 2 \cdot 21) - 21 \\ &= 2 \cdot 54 - 5 \cdot 21. \end{aligned}$$

Multiplying both sides by 302:

$$604 \cdot 54 - 1510 \cdot 21 = 906$$

gives us the solution $x_0 = 604$, $y_0 = -1510$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{21}{3}t = 604 + 7t$ and $y = y_0 - \frac{54}{3}t = -1510 - 18t$ where t is an integer. To find the positive solutions, it suffices to solve the following inequalities: $x = 604 + 7t > 0$ and $y = -1510 - 18t > 0$. This is equivalent to the inequality:

$$-\frac{604}{7} < t < -\frac{1510}{18}$$

Since t is an integer, then t must range from -86 to -84 to have $x, y > 0$.

(c) First, let's apply the Euclidean Algorithm to find $\gcd(123, 360)$:

$$\begin{aligned} 360 &= 2 \cdot 123 + 114 \\ 123 &= 1 \cdot 114 + 9 \\ 114 &= 12 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Hence, $\gcd(123, 360) = 3$. Since 99 is divisible by 3, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned} 3 &= 9 - 6 \\ &= 9 - (114 - 12 \cdot 9) \\ &= 13 \cdot 9 - 114 \\ &= 13(123 - 114) - 114 \\ &= 13 \cdot 123 - 14 \cdot 114 \\ &= 13 \cdot 123 - 14(360 - 2 \cdot 123) \\ &= 41 \cdot 123 - 14 \cdot 360. \end{aligned}$$

Multiplying both sides by 33:

$$1353 \cdot 123 - 462 \cdot 360 = 99$$

gives us the solution $x_0 = 1353$, $y_0 = -462$. By Theorem 2-9, we have that the general solution is given by $x = x_0 + \frac{360}{3}t = 1353 + 120t$ and $y = y_0 - \frac{123}{3}t = -462 - 41t$ where t is an integer. To find the positive solutions, it suffices to solve the following inequalities: $x = 1353 + 120t > 0$ and $y = -462 - 41t > 0$. This is equivalent to the inequality:

$$-\frac{1353}{120} < t < -\frac{462}{41}$$

Since t is an integer, then t must be both greater than or equal to -11 and less than or equal to -12. Therefore, this equation has no solutions in the positive integers.

(d) First, let's apply the Euclidean Algorithm to find $\gcd(158, -57) = \gcd(158, 57)$:

$$\begin{aligned}
158 &= 2 \cdot 57 + 44 \\
57 &= 1 \cdot 44 + 13 \\
44 &= 3 \cdot 13 + 5 \\
13 &= 2 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 2 + 0.
\end{aligned}$$

Hence, $\gcd(158, -57) = 1$. Since 7 is divisible by 1, then this equation has integer solutions. First, let's find one solution by reversing the Euclidean Algorithm:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= 2 \cdot 3 - 5 \\
&= 2(13 - 2 \cdot 5) - 5 \\
&= 2 \cdot 13 - 5 \cdot 5 \\
&= 2 \cdot 13 - 5(44 - 3 \cdot 13) \\
&= 17 \cdot 13 - 5 \cdot 44 \\
&= 17(57 - 44) - 5 \cdot 44 \\
&= 17 \cdot 57 - 22 \cdot 44 \\
&= 17 \cdot 57 - 22(158 - 2 \cdot 57) \\
&= 61 \cdot 57 - 22 \cdot 158 \\
&= (-22) \cdot 158 + (-61) \cdot (-57).
\end{aligned}$$

Multiplying both sides by 7:

$$158 \cdot (-154) + (-57) \cdot (-427) = 7$$

gives us the solution $x_0 = -154$, $y_0 = -427$. By Theorem 2-9, we have that the general solution is given by $x = x_0 - \frac{57}{1}t = -154 - 57t$ and $y = y_0 - \frac{158}{1}t = 427 - 158t$ where t is an integer. To find the positive solutions, it suffices to solve the following inequalities: $x = -154 - 57t > 0$ and $y = 427 - 158t > 0$. This is equivalent to the inequality:

$$t < \min\left(-\frac{154}{57}, \frac{427}{158}\right) = -\frac{154}{57} = -\left(2 + \frac{40}{57}\right).$$

Since t is an integer, then t must smaller than or equal to 3 to have $x, y > 0$.

4. If a and b are relatively prime positive integers, prove that the Diophantine equation $ax - by = c$ has infinitely many solutions in the positive integers.
[*Hint:* There exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. For any integer t, which is larger than both $|x_0|/b$ and $|y_0|/a$, $x = x_0 + bt$ and $y = -(y_0 - at)$ are a positive solution of the given equation.]

Solution First, let $b' = -b$, then $d = \gcd(a, b') = \gcd(a, b) = 1$. It follows that the equation $ax + b'y = c$ has a solution since c is divisible by 1. Let x_0 and y_0 be integers such that $ax_0 + b'y_0 = c$, then we know that for all integers t, $x = x_0 + (b'/d)t = x_0 - bt$ and $y = y_0 - (a/d)t = y_0 - at$ are also solutions. If we want x and y to be positive, we need t to satisfy the inequalities $x_0 > bt$ and $y_0 > at$. Equivalently, we need t to be less than $\min(x_0/b, y_0/a)$. Since there are infinitely many such values of t, then there are infinitely many positive solutions to the equation $ax - by = c$.

5.

(a) Prove that the Diophantine equation $ax + by + cz = d$ is solvable in the integers if and only if $\gcd(a, b, c)$ divides d.

(b) Find all solutions in the integers of $15x + 12y + 30z = 24$. [*Hint:* Put $y = 3s - 5t$ and $z = -s + 2t$.]

Solution

(a) First, suppose that there are integers x_0, y_0 and z_0 such that $ax_0 + by_0 + cz_0 = d$, then d must be divisible by $\gcd(a, b, c)$ since $\gcd(a, b, c)$ divides a, b, c, and hence, any of their linear combination, such as d. Conversely, suppose that d is divisible by $\gcd(a, b, c)$ such that $d = s \cdot \gcd(a, b, c)$. Recall from Exercise 2.3.11 that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, hence, there exist integers x' and z_0 such that $\gcd(a, b, c) = \gcd(a, b)x' + cz_0$. Similarly, there exist integers x_0 and y_0 such that $\gcd(a, b) = ax_0 + by_0$ and so it follows that $\gcd(a, b, c) = a(x'x_0) + b(x'y_0) + cz_0$. Thus, we have $d = a(sx'x_0) + b(sx'y_0) + c(sz_0)$. Therefore, the equation $ax + by + cz = d$ is solvable in the integers.

(b) (This solution does not follow the hint.) First, fix $z = t$ and consider the equation $15x + 12y = 24 - 30t$. Since $\gcd(15, 12) = 3\gcd(5, 4) = 3$ divides $24 - 30t = 3(8 - 10t)$, then the equation is solvable in the integers. To find a solution, notice that from $15 - 12 = 3$, we have $(8 - 10t) \cdot 15 - (8 - 10t) \cdot 12 = 24 - 30t$ which gives us the particular solution $x_0 = 8 - 10t$ and $y_0 = -8 + 10t$. It follows that the general solution is given by $x = 8 - 10t + 4s$ and $y =$

$-8+10t-5s$. Therefore, $x = 8-10t+4s$, $y = -8+10t-5s$ and $z = t$ are solutions to the original equation for all integers s and t. We can prove that every solution can be written in this form as follows: suppose that the integers x, y and z satisfy the equation $15x+12y+30z = 24$, then equivalently, x and y satisfy the equation $15x+12y = 24-30z$. Since $x_0 = 8-10z$, $y_0 = -8+10z$ is a particular solution to that equation, then there must be an integer s_0 such that $x = 8-10z+4s_0$ and $y = -8+10z-5s_0$. Thus, if we let $t = z$ and $s = s_0$, then x, y and z are indeed of the form $x = 8-10t+4s$, $y = -8+10t-5s$ and $z = t$. Therefore, these are all the integer solutions to the equation.

6.

(a) A man has \$4.55 in change composed entirely of dimes and quarters. What are the maximum and minimum number of coins that he can have? Is it possible for the numbers of dimes to equal the number of quarters?

(b) The neighborhood theater charges \$1.80 for adult admissions and 75 cents for children. On a particular evening, the total receipts were \$90. Assuming that more adults than children were present, how many people attended?

(c) A certain number of sixes and nines are added to give a sum of 126; if the number of sixes and nines are interchanged, the new sum is 114. How many of each were there originally?

Solution

(a) First, notice that we can think of this problem as being the same as solving the equation $10x+25y = 455$ where x corresponds to the number of dimes, and y corresponds to the number of quarters. Since $\gcd(10,25) = 5\gcd(2,5) = 5$ divides $455 = 5\cdot 91$, then the equation is solvable in the integers. By multiplying the equation $10\cdot(-2)+25 = 5$ by 91, we get the particular solution $x_0 = -182$, $y_0 = 91$. It follows that the general solution is given by $x = -182+5t$, $y = 91-2t$ where t is an integer. Since we want both x and y to be positive, then we want the following inequalities to be satisfied simultaneously: $x = -182+5t > 0$, $y = 91-2t > 0$. Equivalently, t must satisfy $36.4 = \frac{182}{5} < t < \frac{91}{2} = 45.5$. Since t is an integer, then t must range from 37 to 45. The total number of coins can be expressed by $x+y = -182+5t+91-2t = 3t-91$. Since $x+y$ is an increasing function of t, then the maximum number of coins is 44 (at $t = 45$) and the minimum number of coins is 20 (at $t = 37$). For the number of dimes and quarters to be the same, we must have $x = y$ which is equivalent to $-182+5t = 91-2t$. Solving for t, we get $t = 39$. Thus, a possible solution is $x = y = 13$.

(b) First, if we denote the number of adults by x and the number of children by y, then it suffices to solve the equation $180x+75y = 9000$. To do so, notice that $\gcd(180,75) = 15\gcd(12,5) = 15$. From the equation $(-2)\cdot 180+5\cdot 75 = 15$, we get the equation $(-1200)\cdot 180+3000\cdot 75 = 9000$ which gives us the particular solution $x_0 = -1200$ and $y_0 = 3000$. It follows that the general solution is given by $x = -1200+5t$ and $y = 3000-12t$ where t is an integer. Since there are more adults than children, then this translates into $x > y > 0$. In terms of t, then inequality $x > y$ becomes $t > \frac{4200}{17}$, and the inequality

$y > 0$ becomes $\frac{3000}{12} > t$. Hence, t must satisfy $\frac{4200}{17} < t < \frac{3000}{12}$. Since t is an integer, then it ranges from 248 to 250. Since the total number of people is $x + y = -1200 + 5t + 3000 - 12t = 1800 - 7t$, then in total, either 64 (at $t = 248$), 57 (at $t = 249$) or 50 (at $t = 250$) people came.

(c) We need to solve the equation $6x + 9y = 126$ such that $6y + 9x = 114$. Since $\gcd(6, 9) = 3$ and $(-1)\cdot 6+1\cdot 9 = 3$, then $(-42)\cdot 6+42\cdot 9 = 126$ which gives us the particular solution $x_0 = -42$ and $y_0 = 42$. It follows that the general solution is given by $x = -42 + 3t$ and $y = 42 - 2t$ where t is an integer. Now, plugging these values in the second equation gives us $6(42 - 2t) + 9(-42 + 3t) = 114$. This equation can be simplified into $15t = 240$, and so $t = 16$. Therefore, we get $x = 6$ and $y = 10$ which corresponds to six 6s and ten 9s.

7. A farmer purchased one hundred head of livestock for a total cost of \$4000. Prices were as follow: calves, \$120 each; lambs, \$ 50 each; piglets, \$25 each. If the farmer obtained at least one animal of each type how many did he buy ?

Solution If we denote by x the number of calves, by y the number of lambs, and by z the number of piglets, then we need to solve the equation $120x + 50y + 25z = 4000$ where $x, y, z > 0$ and $x + y + z = 100$. Since we can rewrite the previous equation as $z = 100 - x - y$, then it suffices to solve the equation $120x + 50y + 25(100 - x - y) = 4000$. This equation can be simplified into $19x + 5y = 300$. From $19\cdot(-1) + 5\cdot 4 = 1$, we get $19 \cdot (-300) + 5 \cdot 1200 = 300$ which gives us the particular solution $x_0 = -300$, $y_0 = 1200$. It follows that the general solution is given by $x = -300 + 5t$, $y = 1200 - 19t$ where t is an integer. Since we want $x, y, z > 0$, then we need to solve the following inequalities in terms of t: $-300+5t > 0$, $1200-19t > 0$ and $100 > 900-14t$. From these inequalities, we get that t must range from 61 to 63. It follows that we must have one of the three following cases: ($t = 61$) 5 calves, 41 lambs, 54 piglets; ($t = 62$) 10 calves, 22 lambs, 68 piglets; ($t = 63$) 15 calves, 3 lambs, 82 piglets.

8. When Mr. Smith cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of this, Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written. [*Hint:* If x is the number of dollars and y is the number of cents in the check, then $100y + x - 68 = 2(100x + y)$.]

Solution Let x be the number of dollars and y be the number of cents, then the value of the check is given by $x + \frac{1}{100}y$. Thus, we can translate the situation into the equation $y + \frac{1}{100}x - \frac{68}{100} = 2(x + \frac{1}{100}y)$. Multiplying both sides by 100 gives us $100y + x - 68 = 2(100x + y)$. Putting all the terms together gives us the equation $-199x + 98y = 68$. Let's apply the Euclidean Algorithm to find $\gcd(-199, 98) = \gcd(199, 98)$:

$$\begin{aligned} 199 &= 2 \cdot 98 + 3 \\ 98 &= 32 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

From that, we get

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (98 - 32 \cdot 3)\\ &= 33 \cdot 3 - 98\\ &= 33(199 - 2 \cdot 98) - 98\\ &= 33 \cdot 199 - 67 \cdot 98\\ &= (-33) \cdot (-199) + (-67) \cdot 98.\end{aligned}$$

By multiplying both sides by 68, we get

$$(-199) \cdot (-2244) + 98 \cdot (-4556) = 68$$

which gives us the particular solution $x_0 = -2244$, $y_0 = -4556$. It follows that the general solution is given by $x = -2244 + 98t$, $y = -4556 + 199t$ where t is an integer. From the fact that $x, y > 0$, we get the following inequalities for t: $t > \frac{2244}{98}$ and $t > \frac{4556}{199}$. Since t is an integer, then it follows that $t \geqslant 23$. But recall that y represents the number of cents so we also have the inequality $y < 100$. In terms of t, this inequality becomes $t < \frac{4656}{199}$. Since t is an integer, then it means that $t \leqslant 23$. Combining the two inequalities, we get that $t = 23$. Therefore, the value of the check is \$10.21.

9. Solve each of the puzzle-problems below:

(a) Alcuin of York, 775. A hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 buchels, and each child 1/2 bushel. How many men, women, and children are there ?

(b) Mahaviracarya, 850. There were 63 equal piles of plantain fruit put together and 7 single fruits. They were divided evenly among 23 travelers. What is the number of fruits in each pile? [*Hint:* Consider the Diophantine equation $63x + 7 = 23y$].

(c) Yen Kung, 1372. We have an unknown number of coins. If you make 77 strings of them, you are 50 coins short; but if you make 78 strings, it is exact. How many coins are there? [*Hint:* If N is the number of coins, then $N = 77x + 27 = 78y$ for integers x and y.]

(d) Christoff Rudolf, 1526. Find the number of men, women and children in a company of 20 persons if together they pay 20 coins, each man paying 3, each woman 2, and each child 1/2.

(e) Euler, 1770. Divide 100 into two summands such that one is divisible by 7 and the other by 11.

Solution

(a) Let x be the number of men, y be the number of women, and z be the number of child, then we want to solve the equation $3x+2y+\frac{1}{2}z = 100$. Since we know that $x + y + z = 100$, then we can replace z by $100 - x - y$ in the equation to obtain $5x + 3y = 100$. From the equation $5 \cdot (-1) + 3 \cdot 2 = 1$, we get

$5 \cdot (-100) + 3 \cdot 200 = 100$ by multiplying both sides by 100. This gives us the particular solution $x_0 = -100$, $y_0 = 200$. It follows that the general solution is given by $x = -100 + 3t$, $y = 200 - 5t$ where t is an integer. Since we want $x, y, z \geqslant 0$, then we get the following inequalities in terms of t: $t \geqslant \frac{100}{3}$, $t \leqslant \frac{200}{5}$, $t \geqslant 0$. Hence, t must range from 34 to 40. Thus, the possible triplets (x, y, z) are the following: $(2, 30, 68)$, $(5, 25, 70)$, $(8, 20, 72)$, $(11, 15, 74)$, $(14, 10, 76)$, $(17, 5, 78)$, $(20, 0, 80)$.

(b) Let x be the number of fruits in each pile, then we should have $23 \mid 63x + 7$, or $63x + 7 = 23y$ where $x, y \geqslant 1$. This can be rewritten as $63x - 23y = -7$. Let's apply the Euclidean Algorithm to find $\gcd(63, -23) = \gcd(63, 23)$:

$$\begin{aligned}
63 &= 2 \cdot 23 + 17\\
23 &= 1 \cdot 17 + 6\\
17 &= 2 \cdot 6 + 5\\
6 &= 1 \cdot 5 + 1\\
5 &= 5 \cdot 1 + 0.
\end{aligned}$$

Reversing the algorithm gives us $63 \cdot (-4) + (-23) \cdot (-11) = 1$, from which we get $63 \cdot 28 + (-23) \cdot 77 = -7$ by multiplying both sides by -7. Thus, we have the particular solution $x_0 = 28$, $y_0 = 77$. It follows that the general solution is given by $x = 28 - 23t$, $y = 77 - 63t$ where t is an integer. Since we want $x, y \geqslant 1$, then we must have $t \leqslant 1$. Therefore, all the possible values of fruits in each pile are $28 - 23t$ where $t \leqslant 1$.

(c) Let N be the number of coins, then from the statement of part (c), we have that $N = 77x + 27$ and $N = 78y$ for some integers x and y. Moreover, we must have $N > 0$. Thus, we get the equation $77x + 27 = 78y$ which can be rewritten as $77x - 78y = -27$. Since $77 \cdot (-1) + (-78) \cdot (-1) = 1$, then multiplying both sides by -27 gives us $77 \cdot 27 + (-78) \cdot 27 = -27$. Hence, we have the particular solution $x_0 = y_0 = 27$. It follows that the general solution is given by $x = 27 - 78t$, $y = 27 - 77t$ where t is an integer. Since $N > 0$, then $t \leqslant 0$. It follows that a possible value for N is $N = 2106$ which happens when $t = 0$. More generally, the possible values of N are precisely $78(27 - 77t)$ where $t \leqslant 0$.

(d) Let x be the number of men, y be the number of women, and z be the number of children, then we have the two equations $3x + 2y + \frac{1}{2}z = 20$ and $x + y + z = 20$. By multiplying the first equation by 2 on both sides and plugging $z = 20 - x - y$, we obtain $6x + 4y + (20 - x - y) = 40$. After some simplifications, this equation becomes $5x + 3y = 20$. From the equation $5 \cdot (-1) + 3 \cdot 2 = 1$, we get $5 \cdot (-20) + 3 \cdot 40 = 20$ by multiplying both sides by 20. This gives us the particular solution $x_0 = -20$, $y_0 = 40$. It follows that the general solution is given by $x = -20 + 3t$, $y = 40 - 5t$ where t is an integer. Since we want $x, y, z \geqslant 0$, then we get the following inequalities in terms of t: $t \geqslant \frac{20}{3}$, $t \leqslant \frac{40}{5}$, $t \geqslant 0$. Hence, t must be either 7 or 8. Thus, the possible triplets (x, y, z) are the following: $(1, 5, 14)$, $(4, 0, 16)$.

(e) This problem can be simply solved by considering the equation $100 = 7x + 11y$. Since $7 \cdot (-3) + 11 \cdot 2 = 1$, then $7 \cdot (-300) + 11 \cdot 200 = 100$. Hence, we get the particular solution $x_0 = -300$, $y_0 = 200$. It follows that the general solution is given by $x = -300 + 11t$, $y = 200 - 7t$ where t is an integer. If we want $x, y \geqslant 0$, then this is only satisfied when $t = 28$. In that case, we have $x = 8$ and $y = 4$. This gives us the solution $100 = 56 + 44$.

Chapter 3

Primes and Their Distribution

3.1 The Fundamental Theorem of Arithmetic

1. It has been conjectured that there are infinitely many primes of the form n^2-1. Exhibit five such primes.

Solution When $n = 2$, we have $n^2 - 2 = 2$ which is prime. When $n = 3$, we have $n^2 - 2 = 7$ which is prime. When $n = 5$, we have $n^2 - 2 = 23$ which is prime. When $n = 7$, we have $n^2 - 2 = 47$ which is prime. When $n = 9$, we have $n^2 - 2 = 79$ which is prime.

2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either a prime or 1, and $a \geqslant 0$.

Solution Suppose that $25 = p+a^2$, then $25-a^2$ is a prime number for some $a \geqslant 0$. Moreover, $0 \leqslant a \leqslant 5$ since otherwise, $25 - a^2$ is negative. However, when $a = 0$, $25 - a^2 = 25$ is not a prime; when $a = 1$, $25 - a^2 = 24$ is not a prime; when $a = 2$, $25 - a^2 = 21$ is not a prime; when $a = 3$, $25 - a^2 = 16$ is not a prime; when $a = 4$, $25 - a^2 = 9$ is not a prime; when $a = 5$, $25 - a^2 = 0$ is not a prime. Therefore, 25 cannot is not of the form $p + a^2$ contradicting the conjecture.

3. Prove each of the assertions below:

(a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.

(b) Each integer of the form $3n + 2$ has a prime factor of this form.

(c) The only prime of the form n^3-1 is 7. [*Hint:* Write n^3-1 as $(n-1)(n^2+n+1)$.]

(d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.

(e) The only prime of the form $n^2 - 4$ is 5.

Solution

(a) Suppose that $p = 3n + 1$, then n is either of the form $2m$ or $2m + 1$. If $n = 2m + 1$, then $p = 3(2m + 1) + 1 = 2(3m + 2)$ which is impossible. Thus, $p = 6m + 1$.

(b) Consider the integer $k = 3n + 2$. If one of the prime factor is of the form $3m$, then will be automatically of the form $3m$. Suppose that none of the prime factors of k are of the form $3m + 2$, then from the previous observation, it follows that all of its prime factors must be of the form $3m+1$. However, from the fact that

$$(3k_1 + 1)(3k_2 + 1) = 3(3k_1k_2 + k_1 + k_2) + 1,$$

then by induction, we have that k must also be of the form $3m + 1$, a contradiction. Therefore, k must have a prime of the form $3m + 2$.

(c) Suppose that $n^3-1 = (n-1)(n^2+n+1)$ is prime, then either $n-1$ or n^2+n+1 is equal to 1. In the first case, we get that $n = 2$ and so that $n^3 - 1 = 7$ which is indeed a prime. In the second case, we get that $n = 0$ or $n = 1$. If $n = 0$, then $n^3 - 1 = -1$ which is not a prime. Therefore, the only prime of the form $n^3 - 1$ is 7.

(d) Suppose that $3p + 1$ is a perfect square, then $3p + 1 = a^2$. Equivalently, this implies that $3p = (a-1)(a+1)$. Since 3 is a prime number, then either $3 \mid a-1$ or $3 \mid a + 1$. If $3 \mid a - 1$, then $a - 1 = 3k$ and so $3p = 3k(3k + 2)$. In that case, $p = k(k3k + 2)$ which implies that either $k = 1$ or $3k + 2 = 1$. Since $3k + 2 \neq 1$ for any k, then we must have $k = 1$ and hence $p = 5$. Suppose now that $3 \mid a + 1$, then $a + 1 = 3k$ and so $3p = 3k(3k - 2)$. Again, with the same argument as before, it follows that $p = 5$. Therefore, $p = 5$ is the only prime number for which $3p + 1$ is a perfect square.

(e) Suppose that $p = n^2 - 4 = (n - 2)(n + 2)$ is prime, then either $n - 2 = 3$ or $n + 2 = 1$. In the first case, we get that $n = 3$ and hence, $p = 5$ which is indeed prime. In the second case, we get $n = -1$ and hence $p = -3$ which is not a prime. Therefore, the only such prime is $p = 5$.

4. If $p \geqslant 5$ is a prime number, show that $p^2 + 2$ is composite. [*Hint:* p takes one of the forms $6k + 1$ or $6k + 5$.]

Solution Notice that p cannot be of the form $6k$, $6k + 2 = 2(3k + 1)$, $6k + 3 = 3(2k + 1)$ or $6k + 4 = 2(3k + 2)$ because in all of these cases, since $p \geqslant 5$, $k \neq 0$ and so it is composite. If $p = 6k + 1$, then

$$p^2 + 2 = (6k + 1)^2 + 2 = 6^2k^2 + 2 \cdot 6k + 1 + 2 = 3(18k^2 + 4k + 1)$$

which is composite. Similarly, if $p = 6k + 5$, then

$$p^2 + 2 = (6k + 5)^2 + 2 = 6^2k^2 + 2 \cdot 6k + 25 + 2 = 3(18k^2 + 4k + 9)$$

which is composite. Therefore, $p^2 + 2$ is composite for all prime numbers $p \geqslant 5$.

5.

(a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.

(b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?

Solution

(a) Since p is a prime and $p \mid a^n$, then p must divide a. It follows that $p^n \mid a^n$.

(b) We know that $\gcd(a,b) = 1$ implies that $\gcd(a^2,b^2) = 1$ and that $\gcd(ka,kb) = k\gcd(a,b)$. It follows that in this case, $\gcd(\frac{a}{p},\frac{b}{p}) = 1$ and so $\gcd(\frac{a^2}{p^2},\frac{b^2}{p^2}) = 1$ which implies that $\gcd(a^2,b^2) = p^2$.

Similarly, since $\gcd(a,b) = p$, then $a = pk_1$ and $b = pk_2$ where $\gcd(k_1,k_2)$. It follows that $\gcd(k_1^2,k_2) = 1$ (Exercise 2.2.20(f)) and so there exist integers x and y such that $k_1^2x + k_2y = 1$. Multiplying both sides by p gives us that $(pk_1^2)x + k_2(py) = p$ and so $\gcd(pk_1^2,k_2) \mid p$. It follows that $\gcd(pk_1^2,k_2)$ is either 1 or p and so that $\gcd(a^2,b)$ is either p or p^2. It is impossible to lower the number of possibilities because when $a = p$ and $b = p$, we have $\gcd(a^2,b) = p$ and when $a = p$ and $b = p^2$, we have $\gcd(a^2,b) = p^2$. Therefore, p and p^2 are precisely the possible values of $\gcd(a^2,b)$.

For the third value, since $\gcd(a,b) = p$, then $a = pk_1$ and $b = pk_2$ where $\gcd(k_1,k_2)$. It follows that $\gcd(k_1^3,k_2^2) = 1$ (Exercise 2.2.20(f)) and so there exist integers x and y such that $k_1^3x + k_2^2y = 1$. Multiplying both sides by p^2 gives us that $(pk_1^3)x + k_2^2(py) = p$ and so $\gcd(pk_1^3,k_2^2) \mid p$. It follows that $\gcd(pk_1^3,k_2^2)$ is either 1 or p and so that $\gcd(a^3,b^2)$ is either p^2 or p^3. It is impossible to lower the number of possibilities because when $a = p$ and $b = p$, we have $\gcd(a^3,b^2) = p^2$ and when $a = p$ and $b = p^2$, we have $\gcd(a^3,b^2) = p^3$. Therefore, p^2 and p^3 are precisely the possible values of $\gcd(a^3,b^2)$.

6. Establish each of the following statements:

(a) Every integer of the form $n^4 + 4$, with $n > 1$, is composite.

[*Hint:* Write $n^4 + 4$ as a product of two quadratic factors.]

(b) If $n > 4$ is composite, then n divides $(n-1)!$.

(c) Any integer of the form $8^n + 1$, where $n \geqslant 1$, is composite.

[*Hint:* $2^n + 1 \mid 2^{3n} + 1$].

(d) Each integer $n > 11$ can be written as the sum of two composite numbers. [*Hint:* If n is even, say $n = 2k$, then $n - 6 = 2(k-3)$; for n odd, consider the integer $n - 9$.]

Solution

(a) First, notice that $n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$ for all n. Since both factors are strictly bigger than 1 when $n > 1$, then $n^4 + 4$ must be a composite number.

(b) By the Fundamental Theorem of Arithmetic, we know that $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$. If $m > 1$, then we can define the two distinct (by the Fundamental Theorem of Arithmetic) integers $a = p_1^{k_1}$ and $b = p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ such that $a,b > 1$ and $ab = n$. Since these factors are non-trivial, then they must satisfy $a,b \leqslant n-1$. Since they are distinct and less than $n-1$, then we can write

$$(n-1)! = 1 \cdot 2 \cdot \ldots \cdot a \cdot \ldots \cdot b \cdot \ldots \cdot (n-1)$$

which shows that $n = ab \mid (n-1)!$. If $m = 1$, then $n = p^k$. If $k > 2$, then we can let $a = p$, $b = p^{k-1}$ such that $a \neq b$, $a, b < n-1$ and $ab = n$. Hence, with the same argument as above, we can conclude that $n = ab \mid (n-1)!$. If $k \not> 2$, then $k = 2$ since $k = 1$ would imply that n is not composite. Hence, the last case is $n = p^2$. Notice that $p \neq 2$ since otherwise, $n = 4$. Here, let $a = p$ and $b = 2p$ and notice that both numbers are distinct and less than $n - 1$. Hence, we must have that $2n = ab \mid (n-1)!$ and so that $n \mid (n-1)!$. Therefore, in all possible cases, $n \mid (n-1)!$.

(c) If we replace x with 2^n in the relation $x^3 + 1 = (x+1)(x^2 - x + 1)$, we get that $2^n + 1 \mid 2^{3n} + 1 = 8^n + 1$. It follows that $8^n + 1$ is always composite when $n \geqslant 1$.

(d) Let $n > 11$ be an integer. Suppose first that $n = 2k$, then

$$n = (n-6) + 6 = 2(k-3) + 2 \cdot 3.$$

Since both $2(k-3)$ and $2 \cdot 3$ are composite (if $2(k-3) = 0$, then $11 < n = 6$), then n is indeed the sum of two composite numbers. Similarly, if $n = 2k+1$, then

$$n = (n-9) + 9 = 2(k-4) + 3 \cdot 3.$$

Since both $2(k-4)$ and $3 \cdot 3$ are composite (if $2(k-4) = 0$, then $11 < n = 9$), then n is again the sum of two composite numbers. Therefore, it holds for all integers $n > 11$.

7. Find all prime numbers that divide $50!$.

Solution First, notice that every prime number less than 50 must divide $50!$ by the definition of $n!$. Moreover, let p be a prime number dividing $50!$, then p must divide a number less than 50, and hence, p must be less than 50. Therefore, the prime numbers dividing $50!$ are precisely the prime numbers that are less than 50:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

8. If $p \geqslant q \geqslant 5$ and p and q are both primes, prove that $24 \mid p^2 - q^2$.

Solution Since p and q are prime, then both are either of the form $4k + 1$ or $4k + 3$. If $p = 4r + 1$ and $q = 4t + 1$, then $p + q = 4(r + t) + 2 = 2(2(r + t) + 1)$ and $p - q = 4(r - t)$, and so $8 \mid (p + q)(p - q) = p^2 - q^2$. If $p = 4r + 3$ and $q = 4t + 1$, then $p + q = 4(r + t + 1)$ and $p - q = 4(r - t) + 2 = 2(2(r - t) + 1)$, and so $8 \mid (p + q)(p - q) = p^2 - q^2$. The same calculation proves that $8 \mid p^2 - q^2$ when $p = 4r + 1$ and $q = 4t + 3$. Finally, when $p = 4r + 3$ and $q = 4t + 3$, then $p + q = 4(r + t + 1) + 2 = 2(2(r + t + 1) + 1)$ and $p - q = 4(r - t)$, and so $8 \mid p^2 - q^2$. Therefore, in all possible cases, $8 \mid p^2 - q^2$.

Moreover, since p and q are primes, then both are of the form $3k + 1$ or $3k + 2$. If both are of the form $3k + 1$, then $p - q$ is of the form $3k$ and so $3 \mid p^2 - q^2$. If one is of the form $3k + 1$ and the other is of the form $3k + 2$, then $p + q$ is of the form $3k$ and so $3 \mid p^2 - q^2$. If both are of the form $3k + 2$, then $p - q$ is of the form $3k$ and so $3 \mid p^2 - q^2$. Therefore, in all cases, $3 \mid p^2 - q^2$.

From this, we get that both 3 and 8 divide $p^2 - q^2$. Since $\gcd(3, 8) = 1$, then $24 = 3 \cdot 8 \mid p^2 - q^2$.

9.

(a) An unanswered question is whether there are infinitely many primes which are 1 more than a power of 2, such as $5 = 2^2 + 1$. Find two or more of these primes.

(b) A more general conjecture is that there exist infinitely many primes of the form $n^2 + 1$; for example, $257 = 16^2 + 1$. Exhibit five more primes of this type.

Solution

(a) We have $2^0 + 1 = 2$ and $2^1 + 1 = 3$ which are both primes.

(b) We have $1^1 + 1 = 2$, $2^2 + 1 = 5$, $4^2 + 1 = 17$, $6^2 + 1 = 37$ and $10^2 + 1 = 101$ which are all primes.

10. If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10. [*Hint:* p takes one of the forms $10k + 1$, $10k + 3$, $10k + 7$ or $10k + 9$.]

Solution Since p is a prime, then it must be of the form $10k + 1$, $10k + 3$, $10k + 7$ or $10k + 9$ since otherwise, it would be composite. If $p = 10k + 1$, then $p^2 - 1 = 10(10k^2 + 2k)$ and so it is divisible by 10. If $p = 10k + 3$, then $p^2 + 1 = 10(10k^2 + 6k + 1)$ and so it is divisible by 10. If $p = 10k + 7$, then $p^2 + 1 = 10(10k^2 + 17k + 5)$ and so it is divisible by 10. If $p = 10k + 9$, then $p^2 - 1 = 10(10k^2 + 18k + 8)$ and so it is divisible by 10. Therefore, it holds for all primes $p \neq 5$.

11. Another unproven conjecture is that there are an infinitude of primes which are 1 less than a power of 2, such as $3 = 2^2 - 1$.

(a) Find four more of these primes.

(b) If $p = 2^k - 1$ is prime, show that k is an odd integer, except when $k = 2$. [*Hint:* $3 \mid 4^n - 1$ for all $n \geqslant 1$.]

Solution

(a) We have that $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ and $2^{13} - 1 = 8191$ are all prime numbers.

(b) Let's prove the contrapositive. Suppose that $k = 2m$ is an even integer not equal to 2, then

$$2^k - 1 = (3 + 1)^m - 1 = 3 \sum_{n=1}^{m} \binom{m}{n} 3^{n-1}$$

is composite since it is divisible by 3 and it is not equal to 3 (the sum is not equal to 1 since $m > 1$).

12. Find the prime factorization of the integers 1234, 10140, and 36000.

Solution Since 1234 is even, then we can write it as $2 \cdot 617$. Since 617 is prime, then the prime factorization is $1234 = 2 \cdot 617$.

Since 10140 is divisible by 10 and $10 = 2 \cdot 5$ where both 2 and 5 are prime, then we can write 10140 as $2 \cdot 5 \cdot 1014$. Since 1014 is even, then we can write it as $2 \cdot 507$. Since 507 is divisible by 3, then we can write it as $3 \cdot 169$. Since 169 is 13^2 where 13 is prime, then we can write $10140 = 2 \cdot 5 \cdot 2 \cdot 3 \cdot 13^2 = 2^2 \cdot 3 \cdot 5 \cdot 13^2$ where all the factors are prime numbers.

For 36000, simply notice that

$$36000 = 36 \cdot 1000 = 6^2 \cdot 10^3 = 2^2 \cdot 3^2 \cdot 2^3 \cdot 5^3 = 2^5 \cdot 3^2 \cdot 5^3.$$

13. If $n > 1$ is an integer not of the form $6k + 3$, prove that $n^2 + 2^n$ is composite. [*Hint:* Show that either 2 or 3 divides $n^2 + 2^n$.]

Solution First, notice that if n is even, then both n^2 and 2^n are even and so is their sum. Thus, $n^2 + 2^n$ in that case. The only cases left are $n = 6k + 1$ and $6k + 5$. But first, let's prove that $3 \mid 2^n + 1$ when n is odd. It follows from the fact that

$$\begin{aligned}
2^n + 1 &= (3-1)^n + 1 \\
&= \sum_{l=0}^{n} \binom{n}{l} (-1)^{n-l} 3^l + 1 \\
&= 3 \sum_{l=1}^{n} \binom{n}{l} (-1)^l 3^{l-1} - 1 + 1 \\
&= 3 \sum_{l=1}^{n} \binom{n}{l} (-1)^l 3^{l-1}.
\end{aligned}$$

Hence, if $n = 6k+1$, then both terms in the sum $n^2 + 2^n = 3(12k^2 + 4k) + (2^n + 1)$ are divisible by 3 since n is odd. Hence, $n^2 + 2^n$ is composite. Similarly, both terms in the sum $n^2 + 2^n = 3(12k^2 + 4k + 4) + (2^n + 1)$ are divisible by 3 and so it is composite.

14. It has been conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways. For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \dots .$$

Express the integer 10 as the difference of two consecutive primes in fifteen ways.

Solution By looking at the tables, we get

$$\begin{aligned}10 &= 149 - 139\\ &= 191 - 181\\ &= 251 - 241\\ &= 293 - 283\\ &= 347 - 337\\ &= 419 - 409\\ &= 431 - 421\\ &= 557 - 547\\ &= 587 - 577\\ &= 641 - 631\\ &= 701 - 691\\ &= 719 - 709\\ &= 797 - 787\\ &= 821 - 811\\ &= 839 - 829.\end{aligned}$$

15. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

Solution First, suppose that a is a square, then $a = n^2$ for some integer. Write $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$, then by the rule of exponents, we get $a = p_1^{2k_1} \cdot ... \cdot p_m^{2k_m}$ and so all the exponents are even in the canonical form of a.

Conversely, suppose that a has the following canonical form: $a = p_1^{2k_1} \cdot ... \cdot p_m^{2k_m}$, then by the rules of exponents, if we let $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$, we get that $a = n^2$ and so a is a square.

16. An integer is said to be *square-free* if it is not divisible by the square of any integer greater than 1. Prove that

(a) an integer $n > 1$ is square-free if and only if n can be factored into a product of disctint primes.

(b) every integer $n > 1$ is the product of a square-free integer and a perfect square. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdot ... \cdot p_s^{k_s}$ is the canonical factorization of n, write $k_i = 2q_i + r_i$ where $r_i = 0$ or 1 according as k_i is even or odd.]

Solution

(a) First, suppose that n is square-free and write it as $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$. Suppose that there is a i between 1 and m such that $k_i > 1$, then we would get that $p_i^2 \mid n$ which contradicts the fact that n is square-free. Thus, $k_i = 1$ for all $1 \leqslant i \leqslant m$ and so $n = p_1 \cdot \cdots \cdot p_m$. Hence, n is a product of distinct primes.

Conversely, suppose that n is a product of distinct primes, then $n = p_1 \cdot \cdots \cdot p_m$. By contradiction, if n is not square-free, then there is an integer $d \neq 1$ such that $d^2 \mid n$. Since $d \neq 1$, then there must be a prime p such that $p \mid d$ and so

$p^2 \mid n = p_1 \cdot \cdots \cdot p_m$. By the property of prime numbers, there is a i such that $p \mid p_i$ but since they are primes, we must have $p = p_i$. Canceling these two one both sides, we get that $p \mid p_1 \ldots p_{i-1} \cdot p_{i+1} \ldots p_m$. Again, by the property of prime numbers, we get that $p = p_k$ for some $k \neq i$. But this implies that $p_i = p_k$ which is impossible since we assumed that the p_l's are distinct. Thus, by contradiction, n is square-free.

(b) Let $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ be an integer. For all k_i, define q_i and r_i as the unique integers such that $k_i = 2q_i + r_i$ where $r_i = 0, 1$ (by the Division Algroithm). Denote by $i_1, \ldots, i_s$ the integers i such that $r_i = 1$, and denote by $j_1, \ldots, j_t$ the integers j such that $r_j = 0$, then we can rewrite n as

$$(p_{i_1} \ldots p_{i_s}) \cdot (p_{i_1}^{q_{i_1}} \ldots p_{i_s}^{q_{i_s}} \cdot p_{j_1}^{q_{j_1}} \ldots p_{j_t}^{q_{j_t}})^2.$$

Hence, if we let $a = p_{i_1} \ldots p_{i_s}$ and $b = p_{i_1}^{q_{i_1}} \ldots p_{i_s}^{q_{i_s}} \cdot p_{j_1}^{q_{j_1}} \ldots p_{j_t}^{q_{j_t}}$, we get that a is square-free using part (a). Therefore, $n = a \cdot b^2$ where a is a square-free integer.

17. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geqslant 0$ and m is an odd integer.

Solution First, write n in its canonical form: $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ where the p_i's are disctint and such that $p_i < p_{i+1}$. If $p_1 \neq 2$, then n cannot be even because otherwise, $2 \mid p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ implies that $2 = p_i$ for some i since 2 and the p_i's are prime, but $i \neq 1$ since $p_1 \neq 2$ and $i > 1$ because we would get $2 < p_1 < p_i = 2$. Thus, n is odd and so we can write $n = 2^0 n$ where n is odd. Suppose now that $p_1 = 2$, then we can let $m = p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$ where $p_2 \neq 2$. As we showed above, m mut be odd and so $n = 2^{k_1} m$ where m is odd and $k_1 \geqslant 0$.

18. Numerical evidences makes it plausible that there are infinitely many primes p such that $p + 50$ is also prime. List fifteen of these primes.

Solution By looking at the tables, we get that the following primes p are such that $p + 50$ is also a prime:

$$3,\ 11,\ 17,\ 23,\ 29,\ 47,\ 53,\ 59,\ 89,\ 101,\ 107,\ 113,\ 131,\ 149,\ 173.$$

3.2 The Sieve of Eratosthenes

1. Determine whether the integer 701 is prime by testing all primes $p \leqslant \sqrt{701}$ as possible divisors. Do the same for the integer 1009.

Solution We know that 701 is between $26^2 = 676$ and $27^2 = 729$, hence, the primes p less than $\sqrt{701}$ are precisely 2, 3, 5, 7, 11, 13, 17, 19 and 23. We can easily see that 701 is not divisible by 2, 3, 5 or 7. When $p = 11$, we have $701 = 11 \cdot 63 + 8$ so 11 doesn't divide 701. When $p = 13$, we have $701 = 13 \cdot 53 + 12$ so 13 doesn't divide 701. When $p = 17$, we have $701 = 17 \cdot 41 + 4$ so 17 doesn't divide 701. When $p = 19$, we have $701 = 19 \cdot 36 + 17$ so 19 doesn't divide 701. Finally, when $p = 23$, we have $701 = 23 \cdot 30 + 11$ so 23 doesn't divide 701. Therefore, 701 is a prime number.

Let's apply the same method to determine if 1009 is a prime number. We know that 1009 is between $31^2 = 961$ and $32^2 = 1024$, hence, the primes p less than $\sqrt{1009}$ are precisely 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29. We can easily see that 1009 is not divisible by 2, 3 and 5. When $p = 7$, we have $1009 = 7 \cdot 144 + 1$ so 7 doesn't divide 1009. When $p = 11$, we have $1009 = 11 \cdot 91 + 8$ so 11 doesn't divide 1009. When $p = 13$, we have $1009 = 13 \cdot 77 + 8$ so 13 doesn't divide 1009. When $p = 17$, we have $1009 = 17 \cdot 59 + 6$ so 17 doesn't divide 1009. When $p = 19$, we have $1009 = 19 \cdot 53 + 2$ so 19 doesn't divide 1009. When $p = 23$, we have $1009 = 23 \cdot 43 + 20$ so 23 doesn't divide 1009. Finally, when $p = 29$, we have $1009 = 29 \cdot 34 + 23$ so 29 doesn't divide 1009. Therefore, 1009 is a prime number.

2. Employing the Sieve of Eratosthenes, obtain all the primes between 100 and 200.

Solution Let's put all the numbers between 1 and 200 in a table and put in red the numbers that are removed as described by the algorithm:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Therefore, the prime numbers that are between 100 and 200 are:

$$101,\ 103,\ 107,\ 109,\ 113,\ 127,\ 131,\ 137,\ 139,\ 149,\ 151,$$

$$157,\ 163,\ 167,\ 173,\ 179,\ 181,\ 191,\ 193,\ 197,\ 199.$$

3. Given that $p \mid n$ for all primes $p \leqslant \sqrt[3]{n}$, show that n is either a prime or the product of two primes. [*Hint:* Assume to the contrary that n contains at least three prime factors.]

Solution Suppose that there are three prime numbers p_1, p_2 and p_3 such that $p_1p_2p_3 \mid n$. From the assumption in the statement of this exercice, we must have $p_1, p_2, p_3 > \sqrt[3]{n}$. Multiplying these three inequalities together gives us $p_1p_2p_3 > n$ which is impossible since $p_1p_2p_3$ divides n. Therefore, n must be factored into at most two primes.

4. Establish the following facts:

(a) $\sqrt{p}$ is irrational for any prime p.

(b) If $a > 0$ and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.

(c) For $n \geqslant 2$, $\sqrt[n]{n}$ is irrational. [*Hint:* Use the fact that $2^n > n$.]

Solution

(a) By contradiction, suppose that there exist integers a and b such that $\sqrt{p} = a/b$. By the Well Ordering Principle, we can assume that a and b are relatively prime. As a consequence, we get that in the canonical factorizations

$$a = p_{i_1}^{k_{i_1}} \dots p_{i_s}^{k_{i_s}} \quad \text{and} \quad b = p_{j_1}^{k_{j_1}} \dots p_{j_t}^{k_{j_t}},$$

none of the p_{i_r}'s are equal to the p_{j_r}'s. Using these canonical factorizations, we can rewrite our previous equation as follows:

$$p \cdot p_{j_1}^{2k_{j_1}} \dots p_{j_t}^{2k_{j_t}} = p_{i_1}^{2k_{i_1}} \dots p_{i_s}^{2k_{i_s}}.$$

From this, we get that $p = p_{i_r}$ for some $1 \leqslant r \leqslant s$. By the uniqueness of the canonical factorization, since there is an even number of p's on the right hand side of the equation, then there must be an even number of p's on the left hand side of the equation. However, none of the p_{j_n}'s are equal to p_{i_r} and hence, there is only one p on the left hand side of the equation. Therefore, by contradiction, $\sqrt{p}$ must be irrational.

(b) Since $\sqrt[n]{a}$ is rational, then there exist positive integers c and d such that $\sqrt[n]{a} = c/d$. By the Well Ordering Principle, we can assume that c and d are relatively prime, and so they have no common divisor. Suppose by contradiction that $d \neq 1$, then there exists a prime number p such that $p \mid d$. If we rewrite the equation $\sqrt[n]{a} = c/d$ as $a \cdot d^n = a^n$, then $p \mid d$ implies that $p \mid a \cdot d^n = c^n$. By properties of prime numbers, it follows that $p \mid c$. But this is impossible because we get that $p \neq 1$ is a common divisor of c and d. Therefore, by contradiction, we must have that $d = 1$ which means that $\sqrt[n]{a}$ is an integer.

(c) By contradiction, suppose that $\sqrt[n]{n}$ is rational, then by part (b), there is an integer k such that $k^n = n$. We have that $k \neq 1$ because otherwise, $n = 1$ which is false. Hence, $k \geqslant 2$ which implies that $n < 2^n \leqslant k^n = n$, a contradiction. Therefore, $\sqrt[n]{n}$ is irrational.

5. Show that any composite three-digit number must have a prime factor less than or equal to 31.

Solution Let n be a three-digit composite number, then it must satisfy $n \leqslant 1000$ and so $\sqrt{n} \leqslant \sqrt{1000}$. Moreover, n must have a prime factor $p \leqslant \sqrt{n} \leqslant \sqrt{1000}$. Since 1000 is between $31^2 = 961$ and $32^2 = 1024$, and p is an integer, then p must be less than or equal to 31.

6. Fill in any missing details in this sketch of a proof of the infinitude of primes: Assume that there are only finitely many primes, say p_1, p_2, ..., p_n. Let A be the product of any r of these primes and put $B = p_1 p_2 \dots p_n / A$. Then each p_k divides either A or B, but not both. Since $A + B > 1$, $A + B$ has a prime divisor different from any of the p_k, a contradiction.

Solution First, let's prove that each p_k divides either A or B but not both. First, since the list p_1, ..., p_n is a list of distinct primes, then $p_i \neq p_j$ whenever $i \neq j$. By construction of A, there are two possibilities, either p_k is in the product of r primes that constitutes A and so $p_k \mid A$, either it is not. In that case, p_k doesn't divide A since otherwise, it would be equal to one of the primes constituing A which is impossible. Hence, since $p_k \mid p_1 \dots p_n = AB$, then $p_k \mid B$ since it doesn't divide A. Therefore, as we saw from these two cases, p_k must divide either A or B.Suppose now that it divides both A and B, then we must have a contradiction because by construction, A is composed of primes distinct than B.

Let's show that each p_k cannot divide $A + B$. By contradiction suppose that $p_k \mid A+B$ and assume without loss of generality that $p_k \mid A$, then $p_k \mid (A+B)-A = B$ which is impossible since p_k cannot divide both.

7. Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.

Solution Suppose that there is a largest prime number p and define the integer $N = p! + 1$. Since $N > 1$, then there must be a prime number q that divides N. But since $q \leqslant p$, then $q \mid p!$ and so $q \mid N - p! = 1$ which is impossible. Therefore, by contradiction, there is no largest prime number.

8. Give another proof of the infinitude of primes by assuming that there are only finitely many primes, say p_1, p_2, ..., p_n, and using the integer

$$N = p_2 p_3 \dots p_n + p_1 p_3 \dots p_n + \cdots + p_1 p_2 \dots p_{n-1}$$

to arrive at a contradiction.

Solution Suppose that there are finitely many primes p_1, p_2, ..., p_n and define the integer

$$N = p_2p_3 \dots p_n + p_1p_3 \dots p_n + \dots + p_1p_2 \dots p_{n-1},$$

then from the fact that $N > 1$, there must be a p_k such that $p_k \mid N$. by construction of N, p_k divides every term of the form $p_1 \dots p_{i-1}p_{i+1} \dots p_n$ except when $i = k$. Hence,

$$p_k \mid N - \sum_{i \neq k} p_1 \dots p_{i-1}p_{i+1} \dots p_n = p_1 \dots p_{k-1}p_{k+1} \dots p_n.$$

It follows that $p_k = p_t$ for some $t \neq k$ which is impossible since the p_j's are distinct. Therefore, by contradiction, there are infinitely many primes.

9.

(a) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$. [*Hint:* If $n! - 1$ is not a prime, then it has a prime divisor p; and $p \neq n$ implies $p \mid n!$, leading to a contradiction.]

(b) For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer greater than n.

Solution

(a) Let $n > 2$ and consider the number $n! - 1$. If it is a prime, then we are done. If it is isn't, then $n! - 1 > 1$ implies that there exist a prime p that divides it. If $p \leqslant n$, then $p \mid n!$ and so $p \mid n! - (n! - 1) = 1$, a contradiction. Therefore, in all cases, there is a prime p satisfying $n < p < n!$.

(b) Let p be a prime number dividing $n! + 1$ where $n > 1$. If $p = 2$, then $p \leqslant n$ and so $p \mid n!$. It follows that $p \mid (n! + 1) - n! = 1$, a contradiction. Therefore, p must be odd. More generally, if $p \leqslant n$, then $p \mid (n! + 1) - n! = 1$ which is again a contradiction. Therefore, p must be odd and greater than n.

10. Let q_n be the smallest prime which is strictly greater than $P_n = p_1p_2 \dots p_n + 1$. It has been conjectured that the difference $(p_1p_2 \dots p_n) - q_n$ is always a prime. Confirm this for the first five values of n.

Solution When $n = 1$, we have $P_1 = p_1 + 1 = 3$ and $q_1 = 5$. Hence, $q_1 - p_1 = 3$ which is a prime number. When $n = 2$, we have $P_2 = p_1p_2 + 1 = 7$ and $q_2 = 11$. Hence, $q_2 - p_1p_2 = 5$ which is a prime number. When $n = 3$, we have $P_3 = p_1p_2p_3 + 1 = 31$ and $q_3 = 37$. Hence, $q_3 - p_1p_2p_3 = 7$ which is a prime number. When $n = 4$, we have $P_4 = p_1p_2p_3p_4 + 1 = 211$ and $q_4 = 223$. Hence, $q_4 - p_1p_2p_3p_4 = 23$ which is a prime number. Finally, when $n = 5$, we have $P_5 = p_1p_2p_3p_4p_5 + 1 = 2311$ and $q_5 = 2333$. Hence, $q_5 - p_1p_2p_3p_4p_5 = 23$ which is a prime number. Therefore, the conjecture holds for $n = 1, 2, 3, 4, 5$.

11. If p_n denotes the nth prime number, put $d_n = p_{n+1} - p_n$. An open question is whether the equation $d_n = d_{n+1}$ has infinitely many solutions; give five solutions.

Solution When $n = 2$, we have $d_2 = p_3 - p_2 = 5 - 3 = 2$, and $d_3 = p_4 - p_3 = 7 - 5 = 2$. Hence, we get $d_2 = d_3$. When $n = 15$, we have $d_{15} = p_{16} - p_{15} = 53 - 47 = 6$, and

$d_{16} = p_{17} - p_{16} = 59 - 53 = 6$. Hence, we get $d_{15} = d_{16}$. When $n = 36$, we have $d_{36} = p_{37} - p_{36} = 157 - 151 = 6$, and $d_{37} = p_{38} - p_{37} = 163 - 157 = 6$. Hence, we get $d_{36} = d_{37}$. When $n = 39$, we have $d_{39} = p_{40} - p_{39} = 173 - 167 = 6$, and $d_{41} = p_{42} - p_{41} = 179 - 173 = 6$. Hence, we get $d_{39} = d_{40}$. When $n = 46$, we have $d_{46} = p_{47} - p_{46} = 211 - 199 = 12$, and $d_{47} = p_{48} - p_{47} = 223 - 211 = 12$. Hence, we get $d_{46} = d_{47}$. Therefore, $n = 2, 15, 36, 39, 46$ are all solutions of the equation $d_n = d_{n+1}$.

12. Assuming that p_n is the nth prime number, establish each of the following statements:

(a) $p_n > 2n - 1$ for $n \geqslant 5$.

(b) None of the integers $P_n = p_1 p_2 \dots p_n + 1$ is a perfect square. [*Hint:* Each P_n is of the form $4k + 3$.]

(c) The sum

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

is never an integer.

Solution

(a) Let $n \geqslant 5$ be an integer and notice that there are $n-1$ odd integers less than $2n-1$. Since prime numbers are all odd except two, then we get that there are at most n prime numbers less than $2n-1$. However, if we add the fact that $2n - 1 \geqslant 9$ and that 9 is not a prime number, we can lower the upper bound and get that there are at most $n-1$ prime numbers less than or equal to $2n-1$. It follows that $p_n > 2n-1$ since otherwise, we would get that there are at least n primes less than $2n-1$.

(b) If we consider the two cases $m = 2k$ and $m = 2k+1$, we get that $m^2 = 4k_0$ or $m^2 = 4k_1 + 1$. Hence, in general, squares are either of the form $4k$ or $4k + 1$. If we let n be an integer, then the integer $P_n = p_1 p_2 \dots p_n + 1$ has the form $4k+3$ because $p_1 = 2$, all the p_i's are odd for $i > 1$ and so $p_2 p_3 \dots p_n = 2k+1$. It follows that $P_n = 2(2k+1)+1 = 4k+3$. Therefore, P_n cannot be a square.

(c) By contradiction, suppose that the sum of fractions is an integer, then equivalently, if we add the fractions together, we get that

$$\frac{p_2 p_3 \dots p_n + p_1 p_3 \dots p_n + \cdots + p_1 p_2 \dots p_{n-1}}{p_1 p_2 \dots p_n}$$

is an integer, and hence that $p_1 p_2 \dots p_n \mid N$ where $N = p_2 p_3 \dots p_n + p_1 p_3 \dots p_n + \cdots + p_1 p_2 \dots p_{n-1}$. It follows that $p_1 \mid N$. But notice that p_1 divides all the terms in the definition of N except the first one, it follows that

$$p_1 \mid N - \sum_{i=2}^{n} p_1 \dots p_{i-1} p_{i+1} \dots p_n = p_2 p_3 \dots p_n.$$

Since p_1 is a prime number, then $p_1 \mid p_i$ for some $i \neq 1$. Since p_i is a prime, then $p_1 = p_i$. But this is a contradiction since the p_j's are distinct. Therefore, the original sum of fractions cannot be an integer.

13.

(a) For the repunits R_n, prove that if $k \mid n$, then $R_k \mid R_n$. [*Hint:* If $n = kr$, consider the identity

$$x^n - 1 = (x^k - 1)(x^{(r-1)k} + x^{(r-2)k} + \cdots + x^k + 1).]$$

(b) Use part (a) to obtain the prime factors of the repunit R_{10}.

Solution

(a) In the identity

$$x^n - 1 = (x^k - 1)(x^{(r-1)k} + x^{(r-2)k} + \cdots + x^k + 1),$$

replace x by 10 and divide both sides by 9 to obtain

$$R_n = R_k(1 + 10^k + 10^{2k} + \cdots + 10^{(r-1)k}).$$

It directly follows that $R_k \mid R_n$.

(b) From part (a), we have that R_{10} is divisible by both $R_2 = 11$ and $R_5 = 41 \cdot 271$. It follows that $R_{10} = 11 \cdot 41 \cdot 271 \cdot 9091$. Since 9091 is a prime number, then we are done.

3.3 The Goldbach Conjecture

1. Verify that the integers 1949 and 1951 are twin primes.

Solution Let's show that both integers are prime numbers by proving that none of the prime less than their square roots are divisors. Since $44^2 < 1949, 1951 < 45^2$, then it suffices to consider the primes that are less than 44: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43. Obviously, both integers are not divisible by 2, 3 and 5.

$$\begin{aligned}
1949 &= 7 \cdot 278 + 1 & 1951 &= 7 \cdot 278 + 3\\
1949 &= 11 \cdot 177 + 2 & 1951 &= 11 \cdot 177 + 4\\
1949 &= 13 \cdot 149 + 12 & 1951 &= 13 \cdot 150 + 1\\
1949 &= 17 \cdot 114 + 11 & 1951 &= 17 \cdot 114 + 13\\
1949 &= 19 \cdot 102 + 11 & 1951 &= 19 \cdot 102 + 13\\
1949 &= 23 \cdot 88 + 17 & 1951 &= 23 \cdot 88 + 19\\
1949 &= 29 \cdot 67 + 3 & 1951 &= 29 \cdot 67 + 5\\
1949 &= 31 \cdot 62 + 27 & 1951 &= 31 \cdot 62 + 29\\
1949 &= 37 \cdot 52 + 25 & 1951 &= 37 \cdot 52 + 27\\
1949 &= 41 \cdot 47 + 22 & 1951 &= 41 \cdot 47 + 24\\
1949 &= 43 \cdot 45 + 14 & 1951 &= 43 \cdot 45 + 16.
\end{aligned}$$

As it can be seen from the previous equations, none of these primes divide the two integers. Therefore, they form a pair of twin primes.

2.

(a) If 1 is added to a product of twin primesn prove that a perfect square is always obtained.

(b) Show that the sum of twin primes p and $p+2$ is divisible by 12, provided that $p > 3$.

Solution

(a) Let p and q be twin primes, then there exists an integer n such that $p = n-1$ and $q = n+1$. It follows that $pq + 1 = (n-1)(n+1) + 1 = (n^2 - 1) + 1 = n^2$ which is a perfect square.

(b) First, since $p > 3$, then p mustbe odd since the only even prime is 2. Moreover, p cannot be of the form $3k$ since $p \neq 3$. Thus, either p is of the form $3k+1$ or of the form $3k+2$. However, $p+2$ is also a prime by our assumption and so if $p = 3k+1$, then $p+2 = 3(k+1)$ which is divisible than 3 and distinct than 3, a contradiction. It follows that $p = 3k+2$. Therefore, $p+1$ is divisible by both 2 and 3 and since $\gcd(2,3) = 1$, then $6 \mid p+1$. It follows that $p + (p+2) = 2(p+1)$ is divisible by 12.

3. Find all pairs of primes p and q satisfying $p - q = 3$.

Solution Notice that if q is even, then $p = q + 3$ is odd, and if q is odd, then $p = q + 3$ is even. It follows that p and q don't have the same parity. But the only even prime is 2 so the only possible pair is $p = 5$ and $q = 2$.

4. Sylvester (1896) rephrased Goldbach's Conjecture so as to read: Every even integer $2n$ greater than 4 is the sum of twin primes, one larger than $n/2$ and the other less than $3n/2$. Verify this version of the conjecture for all even integers between 6 and 76.

Solution

n	$2n$	$n/2$	$3n/2$	twin pair $p \geqslant n/2$	twin pair $q \leqslant 3n/2$	$p+q$
3	6	1.5	4.5	3	3	6
4	8	2	6	3	5	8
5	10	2.5	7.5	5	5	10
6	12	3	9	5	7	12
7	14	3.5	10.5	7	7	14
8	16	4	12	5	11	16
9	18	4.5	13.5	5	13	18
10	20	5	15	7	13	20
11	22	5.5	16.5	11	11	22
12	24	6	18	11	13	24
13	26	6.5	19.5	13	13	26
14	28	7	21	11	17	28
15	30	7.5	22.5	11	19	30
16	32	8	24	13	19	32
17	34	8.5	25.5	31	3	34
18	36	9	27	31	5	36
19	38	9.5	28.5	31	7	38
20	40	10	30	29	11	40
21	42	10.5	31.5	31	11	42
22	44	11	33	31	13	44
23	46	11.5	34.5	41	5	46
24	48	12	36	41	7	48
25	50	12.5	37.5	43	7	50
26	52	13	39	41	11	52
27	54	13.5	40.5	41	13	54
28	56	14	42	43	13	56
29	58	14.5	43.5	41	17	58
30	60	15	45	43	17	60
31	62	15.5	46.5	43	19	62
32	64	16	48	59	5	64
33	66	16.5	49.5	59	7	66
34	68	17	51	61	7	68
35	70	17.5	52.5	41	29	70
36	72	18	54	41	31	72
37	74	18.5	55.5	43	31	74
38	76	19	57	71	5	76

5. In 1752, Goldbach submitted the following conjecture to Euler: Every odd integer can be written in the form $p+2a^2$, where p is either a prime or 1s and $a \geqslant 0$. Show that the integer 5777 refutes this conjecture.

Solution To show that 5777 refutes the conjecture, let's show that $5777 - 2a^2$ is never a prime number. First, notice that if the conjecture is true, then a should be contained in the interval $a = 0$, $a = 53$ since $2 \cdot 53^2 = 5618$ and $2 \cdot 54^2 = 5832$. Hence, we need to show that $5777 - 2a^2$ is not a prime for all $0 \leqslant a \leqslant 53$:

a	$2a^2$	$5777 - 2a^2$	Prime ?	a	$2a^2$	$5777 - 2a^2$	Prime ?
0	0	5777	No	27	1458	4319	No
1	2	5775	No	28	1568	4209	No
2	8	5769	No	29	1682	4095	No
3	18	5759	No	30	1800	3977	No
4	32	5745	No	31	1922	3855	No
5	50	5727	No	32	2048	3729	No
6	72	5705	No	33	2178	3599	No
7	98	5679	No	34	2312	3465	No
8	128	5649	No	35	2450	3327	No
9	162	5615	No	36	2592	3185	No
10	200	5577	No	37	2738	3039	No
11	242	5535	No	38	2888	2889	No
12	288	5489	No	39	3042	2735	No
13	338	5439	No	40	3200	2577	No
14	392	5385	No	41	3362	2415	No
15	450	5327	No	42	3528	2249	No
16	512	5265	No	43	3698	2079	No
17	578	5199	No	44	3872	1905	No
18	648	5129	No	45	4050	1727	No
19	722	5055	No	46	4232	1545	No
20	800	4977	No	47	4418	1359	No
21	882	4895	No	48	4608	1169	No
22	968	4809	No	49	4802	975	No
23	1058	4719	No	50	5000	777	No
24	1152	4625	No	51	5202	575	No
25	1250	4527	No	52	5408	369	No
26	1352	4425	No	53	5618	159	No

Therefore, 5777 refutes the conjecture.

6. Prove that Goldbach's Conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes. [*Hint:* If $2n - 2 = p_1 + p_2$, then $2n = p_1 + p_2 + 2$ and $2n + 1 = p_1 + p_2 + 3$.]

Solution Suppose that Goldbach's Conjecture is true and let $n \geqslant 3$, then there exist two prime numbers p_1 and p_2 such that $2n - 2 = p_1 + p_2$. It follows that $2n = p_1 + p_2 + 2$ and $2n + 1 = p_1 + p_2 + 3$. Therefore, it holds for all integers greater than 5. Conversely, suppose that every integer greater than 5 is the sum of three primes and let $n \geqslant 3$ be an integer, then $2n = p_1 + p_2 + p_3$ for some prime numbers p_1, p_2 and p_3. Since $2n$ is even, then p_1, p_2, p_3 cannot all be odd and so one of them must be even. Without loss of generality, we can assume that p_3 is even and hence, $p_3 = 2$. Thus, $2n - 2 = p_1 + p_2$. This proves Goldbach's Conjecture.

7. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_1 + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.

Solution

$$\begin{array}{rrrr}
7 = 3 + 2 \cdot 2 & 25 = 19 + 2 \cdot 3 & 43 = 37 + 2 \cdot 3 & 61 = 47 + 2 \cdot 7 \\
9 = 5 + 2 \cdot 2 & 27 = 23 + 2 \cdot 2 & 45 = 41 + 2 \cdot 2 & 63 = 59 + 2 \cdot 2 \\
11 = 7 + 2 \cdot 2 & 29 = 23 + 2 \cdot 3 & 47 = 41 + 2 \cdot 3 & 65 = 59 + 2 \cdot 3 \\
13 = 7 + 2 \cdot 3 & 31 = 17 + 2 \cdot 7 & 49 = 43 + 2 \cdot 2 & 67 = 61 + 2 \cdot 3 \\
15 = 11 + 2 \cdot 2 & 33 = 29 + 2 \cdot 2 & 51 = 47 + 2 \cdot 2 & 69 = 59 + 2 \cdot 5 \\
17 = 13 + 2 \cdot 2 & 35 = 31 + 2 \cdot 2 & 53 = 47 + 2 \cdot 3 & 71 = 67 + 2 \cdot 2 \\
19 = 13 + 2 \cdot 3 & 37 = 31 + 2 \cdot 3 & 55 = 41 + 2 \cdot 7 & 73 = 67 + 2 \cdot 3 \\
21 = 17 + 2 \cdot 2 & 39 = 29 + 2 \cdot 5 & 57 = 53 + 2 \cdot 2 & 75 = 71 + 2 \cdot 2 \\
23 = 19 + 2 \cdot 2 & 41 = 37 + 2 \cdot 2 & 59 = 53 + 2 \cdot 3 &
\end{array}$$

Therefore, the conjecture is true for all odd numbers smaller than 75.

8. Given a positive integer n, it can be shown that there exists an even integer a which is representable as the sum of two odd primes in n different ways. Confirm that the integers 60, 78, and 84 can be written as the sum of two primes in six, seven and eight ways, respectively.

Solution Simply notice that

$$60 = 7 + 53 = 13 + 47 = 17 + 43 = 19 + 41 = 23 + 37 = 29 + 31$$
$$78 = 5 + 73 = 7 + 71 = 11 + 67 = 17 + 61 = 19 + 59 = 31 + 47 = 37 + 41$$
$$84 = 5 + 79 = 11 + 73 = 13 + 71 = 17 + 67 = 23 + 61 = 31 + 53 = 37 + 47 = 41 + 43$$

9.

(a) For $n > 3$, show that the integers n, $n + 2$, $n + 4$ cannot all be prime.

(b) Three integers p, $p + 2$, $p + 6$ which are prime are called a *prime-triplet.* Find five sets of prime-triplets.

Solution

(a) Suppose that there is a prime number $n > 3$ such that $n + 2$ and $n + 4$ are also prime. Since n is prime and $n > 3$, then either $n = 3k + 1$ or $n = 3k + 2$. In the first case, we have $n + 2 = 3(k + 1)$ which is a contradiction. Hence, $n = 3k + 2$ but in that case, $n + 4 = 3(k + 2)$ which is again a contradiction. It follows that no such integer n exists.

(b) By looking at the tables, we can find the following prime-triplets: $(5, 7, 11)$, $(11, 13, 17)$, $(17, 19, 23)$, $(41, 43, 47)$ and $(101, 103, 107)$.

10. Establish that the sequence

$$(n+1)!-2,\ (n+1)!-2,\ \ldots,\ (n+1)!-(n+1)$$

produces n consecutive composite integers for $n > 1$.

Solution By construction, the sequence is composed of n consecutive integers. Take now the term $(n+1)!-k$ in the sequence where k is an integer satisfying $2 \leqslant k \leqslant n+1$. Since $k \leqslant n+1$, then $k \mid (n+1)!$ and hence, $k \mid (n+1)!-k$. Since $k \geqslant 2$, then k is a non-trivial factor of $(n+1)!-k$ showing that all the terms of the sequence are composite integers.

11. Find the smallest positive integer n for which the function $f(n) = n^2+n+17$ is composite. Do the same for the functions $g(n) = n^2+21n+1$ and $h(n) = 3n^2+3n+23$.

Solution For the function f, the smallest n is $n = 16$ because $f(16) = 16 \cdot 17 + 17 = 17^2$ which is composite, and because $f(1) = 19$, $f(2) = 23$, $f(3) = 29$, $f(4) = 37$, $f(5) = 47$, $f(6) = 59$, $f(7) = 73$, $f(8) = 89$, $f(9) = 107$, $f(10) = 127$, $f(11) = 149$, $f(12) = 173$, $f(13) = 199$, $f(14) = 227$ and $f(15) = 257$ are all prime numbers.

For the function g, the smallest n is $n = 18$ because $f(18) = 703 = 19 \cdot 37$ which is composite, and because $g(1) = 23$, $g(2) = 47$, $g(3) = 73$, $g(4) = 101$, $g(5) = 131$, $g(6) = 163$, $g(7) = 197$, $g(8) = 233$, $g(9) = 271$, $g(10) = 311$, $g(11) = 353$, $g(12) = 397$, $g(13) = 443$, $g(14) = 491$, $g(15) = 541$, $g(16) = 593$ and $g(17) = 647$ are all prime numbers.

For the function h, the smallest n is $n = 2$ because $h(22) = 1541 = 23 \cdot 67$ which is composite, and because $h(1) = 29$, $h(2) = 41$, $h(3) = 59$, $h(4) = 83$, $h(5) = 113$, $h(6) = 149$, $h(7) = 191$, $h(8) = 239$, $h(9) = 293$, $h(10) = 353$, $h(11) = 419$, $h(12) = 491$, $h(13) = 569$, $h(14) = 653$, $h(15) = 743$, $h(16) = 839$, $h(17) = 941$, $h(18) = 1049$, $h(19) = 1163$, $h(20) = 1283$ and $h(21) = 1409$ are all prime numbers.

12. The following result was conjectured by Bertrand, but first proved by Tchebychef in 1850: For every positive integer $n > 1$, there exists at least one prime p satisfying $n < p < 2n$. Use Bertrand's Conjecture to show that $p_n < 2^n$, where p_n is the nth prime number.

Solution First, define the sequence P_n as $P_1 = 2$, $P_2 = 3$ and P_n as the prime number satisfying $2^{n-1} < P_n < 2^n$ where $n \geqslant 3$. By construction, we have that P_n is a strictly increasing sequence of prime numbers. Hence, since there are at least $n-1$ prime numbers less than P_n, we must have the inequality $p_n \leqslant P_n$. Therefore, by construction, we have $p_n \leqslant P_n < 2^n$ and so $p_n < 2^n$.

13. Apply the same method of proof as in Theorem 3-6 to show that there are infinitely many primes of the form $6n+5$.

Solution Suppose that there are finitely many primes of the form $6n+5$, and denote them by q_1, q_2, ..., q_n. Consider the integer

$$N = 6(q_1q_2\ldots q_n) - 1 = 6(q_1q_2\ldots q_n - 1) + 5$$

Since N is neither even, nor a multiple of 3, then its prime factors are of the form $6n+1$ or $6n+5$. If all prime factors of N are of the form $6n+1$, then the equation

$$(6k+1)(6k'+1) = 6(6kk'+k+k')+1$$

tells us that N must have the form $6n+1$, which is false. Therefore, there must be a prime p of the form $6n+5$. By our assumption, $p = q_i$ for some i and so $p \mid 6(q_1q_2\dots q_n)$. It follows that $p \mid 6(q_1q_2\dots q_n) - N = 1$ which is a contradiction since $p \neq 1$. Therefore, there are infinitely many primes of the form $6n+5$.

14. Find a prime divisor of the integer $N = 4(3\cdot7\cdot11)-1$ of the form $4n+3$. Do the same for $N = 4(3\cdot7\cdot11\cdot15)-1$.

Solution We have that $4(3\cdot7\cdot11)-1 = 923$ is divisble by the prime 71 which is of the form $4n+3$. Since $4(3\cdot7\cdot11\cdot15)-1$ is a prime number (it took me a lot of time to arrive at this conclusion), then it is itself a prime factor of the form $4n+3$.

15. Another unanswered question is whether the exist an infinite number of sets of five consecutive integers of which four are primes. Find five such sets of integers.

Solution The following sets satisfy the property above: $\{3,5,7,9,11\}$, $\{11,13,15,17,19\}$, $\{101,103,105,107,109\}$, $\{191,193,195,197,199\}$ and $\{461,463,465,467,469\}$.

16. Let the sequence of primes, with 1 adjoined, be denoted by $p_0 = 1$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... For each $n \geqslant 1$, it is known that there exists a suitable choice of coefficients $\epsilon_k = \pm 1$ such that

$$p_{2n} = p_{2n-1} + \sum_{k=0}^{2n-2} \epsilon_k p_k, \quad p_{2n+1} = 2p_{2n} + \sum_{k=0}^{2n} \epsilon_k p_k.$$

To illustrate:
$13 = 1+2-3-5+7-11$ and
$17 = 1+2-3-5+7-11+2\cdot13$.
Determine similar expressions for the primes 23, 29, 31, and 37.

Solution We have

$$\begin{aligned}
23 &= -1+2-3-5+7-11+13-17+2\cdot19,\\
29 &= 1+2-3-5+7-11+13-17+19+23,\\
31 &= 1-2+3+5-7+11-13+17-19-23+2\cdot29,\\
37 &= 1-2+3+5-7+11-13-17+19-23+29+31.
\end{aligned}$$

17. In 1848 de Polignac claimed that every odd integer is the sum of a prime and a power of 2. For example, $55 = 47+2^3 = 23+2^5$. Show that the integers 509 and 877 discredit this claim.

Solution To show that 509 is a counterexample, let's show that $509-2^n$ is not a prime for all $n \geqslant 0$. First, notice that if $n \geqslant 9$, $509-2^n < 0$ and so it cannot be a prime number. Thus, we only need to consider the values $n = 0, 1, ..., 8$. When $n = 0$, $509 - 2^n = 508 = 2 \cdot 254$ which is composite. When $n = 1$, $509 - 2^n = 507 = 3 \cdot 169$ which is composite. When $n = 2$, $509 - 2^n = 505 = 5 \cdot 101$ which is composite. When $n = 3$, $509 - 2^n = 501 = 3 \cdot 167$ which is composite. When $n = 4$, $509 - 2^n = 493 = 17 \cdot 29$ which is composite. When $n = 5$, $509 - 2^n = 477 = 3 \cdot 159$ which is composite. When $n = 6$, $509 - 2^n = 445 = 5 \cdot 89$ which is composite. When $n = 7$, $509 - 2^n = 381 = 3 \cdot 127$ which is composite. Finally, when $n = 8$, $509 - 2^n = 253 = 11 \cdot 23$ which is composite. Therefore, 509 cannot be written in the form $p + 2^n$ where p is prime and n is a positive integer.

Similarly, to show that 877 is a counterexample, let's show that $877 - 2^n$ is not a prime for all $n \geqslant 0$. First, notice that if $n \geqslant 10$, $877 - 2^n < 0$ and so it cannot be a prime number. Thus, we only need to consider the values $n = 0, 1, ..., 9$. When $n = 0$, $877 - 2^n = 876 = 2 \cdot 438$ which is composite. When $n = 1$, $877 - 2^n = 875 = 5 \cdot 175$ which is composite. When $n = 2$, $877 - 2^n = 873 = 3 \cdot 291$ which is composite. When $n = 3$, $877 - 2^n = 869 = 11 \cdot 79$ which is composite. When $n = 4$, $877 - 2^n = 861 = 3 \cdot 287$ which is composite. When $n = 5$, $877 - 2^n = 845 = 5 \cdot 169$ which is composite. When $n = 6$, $877 - 2^n = 813 = 3 \cdot 271$ which is composite. When $n = 7$, $877 - 2^n = 749 = 7 \cdot 107$ which is composite. When $n = 8$, $877 - 2^n = 621 = 3 \cdot 207$ which is composite. Finally, when $n = 9$, $877 - 2^n = 365 = 5 \cdot 73$ which is composite. Therefore, 877 cannot be written in the form $p + 2^n$ where p is prime and n is a positive integer.

18.

(a) If p is a prime and $p \nmid b$, prove that in the arithmetic progression

$$a,\ a+b,\ a+2b,\ a+3b,\ \ldots$$

every pth term is divisible by p. [*Hint:* Since $\gcd(p, b) = 1$, there exists integers r and s satisfying $pr + bs = 1$. Put $n_k = kp - as$ for $k = 1, 2, ...$ and show that $p \mid a + n_k b$.]

(b) From part (a), conclude that if b is an odd integer, then every other term in the indicated progression is even.

Solution

(a) Since p doesn't divide b, then $\gcd(p, b) = 1$ and so there exist integers r and s such that $pr + bs = 1$. Hence, if we define the sequence $n_k = kp - as$, then $a + n_k b = a + (kp - as)b = a + bkp - abs = a + bkp - a(1 - pr) = p(bkr)$. It follows that the term $a + n_k b$ is always divisible by p.

(b) If we put $p = 2$ and b be an odd integer, then part (a) tells us that at least one of the even-indexed terms or odd-indexed terms are even.

19. In 1950, it was proven that any integer $n > 9$ can be written as a sum of distinct odd primes. Express the integers 25, 69, 81, and 125 in this fashion.

Solution We have

$$\begin{aligned}25 &= 5+7+13\\ 69 &= 3+5+61,\\ 81 &= 3+5+73,\\ 125 &= 5+7+113.\end{aligned}$$

20. If p and p^2+8 are both prime numbers, prove that p^3+4 is also a prime.

Solution Let p be a prime number such that p^2+8 is also a prime number. Consider the case in which $p = 3k+1$, then $p^2+8 = 3k'+9 = 3(k'+3)$ which is not a prime, hence, p is not of the form $3k+1$. Similarly, if $p = 3k+2$, then $p^2+8 = 3k'+12 = 3(k'+4)$ which is not a prime. Thus, p must be of the form $3k$. But since p is prime, then $p = 3$. Therefore, $p^3+4 = 31$ is indeed a prime number.

21.

(a) For any integer $k > 0$, establish that the arithmetic progression

$$a+b,\ a+2b,\ a+3b,\ \dots,$$

where $\gcd(a,b) = 1$, contains k consecutive terms which are composite. [*Hint:* Put $n = (a+b)(a+2b)\dots(a+kb)$ and consider the k terms

$$a+(n+1)b,\ a+(n+2)b,\ \dots,\ a+(n+k)b.]$$

(b) Find five consecutive composite terms in the arithmetic progression

$$6,\ 11,\ 16,\ 21,\ 26,\ 31,\ 36,\ \dots$$

Solution

(a) Let $n = (a+b)(a+2b)\dots(a+kb)$ and notice that for all $1 \leqslant i \leqslant k$, n is divisible by $a+ib$. It follows that

$$a+(n+i)b = (a+ib)+nb = (a+ib)\left(1+b\frac{n}{a+ib}\right).$$

This proves that the term $a+(n+i)b$ is composite.

(b) Using part (a), we get that 14894891, 14894896, 14894901, 14894906 and 14894911 are five consecutive composite terms of the sequence.

22. Show that 13 is the largest prime that can divide two successive integers of the form n^2+3.

Solution Let p be a prime number such that $p \mid n^2+3$ and $p \mid (n+1)^2+3$, then we can easily derive that $p \mid (n+1)^2+3-n^2-3 = 2n+1$. It follows that $pk = 2n+1$ for some integer k, and so that $n = \frac{pk-1}{2}$. Hence, we rewrite the fact that $p \mid n^2+3$

into the equation $pt = (\frac{pk-1}{2})^2 + 3$ where t is an integer. From this equation, we can derive

$$\begin{aligned} pt = \left(\frac{pk-1}{2}\right)^2 + 3 &\implies 4pt = (pk-1)^2 + 12 \\ &\implies 4pt = p^2k^2 - 2pk + 1 + 12 \\ &\implies p(4t - pk^2 + 2k) = 13 \\ &\implies p \mid 13. \end{aligned}$$

Therefore, $p = 13$ since p and 13 are prime numbers.

23.

(a) The arithmetic mean of the twin primes 5 and 7 is the triangular number 6. Are there any other twin primes with triangular mean?

(b) The arithmetic of the twin primes 3 and 5 is the perfect square 4. Are there any other twin primes with a square mean?

Solution

(a) Suppose that we have a pair of twin primes p and q such that $p = t_n - 1$ and $q = t_n + 1$ for some n, then using the formula for t_n, we get

$$\begin{aligned} p &= \frac{n(n+1)}{2} - 1 \\ &= \frac{n^2 + n - 2}{2} \\ &= \frac{(n-1)(n+2)}{2}. \end{aligned}$$

Since either $n-1$ or $n+2$ is even, then we have $p = (n+2)\frac{n-1}{2}$ or $p = (n-1)\frac{n+2}{2}$. But since p is a prime number, then in the first case, p must be equal to 5 (by solving $\frac{n-1}{2} = 1$) and in the second case, p must be equal to 2. In the second case, $p = 2$ is impossible since it is not a twin prime. Therefore, the only pair of twin primes with an arithmetic mean equal to a triangular number is the pair $p = 5$ and $q = 7$.

(b) Suppose that we have a pair of twin primes p and q such that $p = n^2 - 1$ and $q = n^2 + 1$ for some n, then $p = (n-1)(n+1)$. Since p is a prime, then either $n-1 = 1$ or $n+1 = 1$. In the first case, we get $n = 2$ which implies that $p = 3$. In the second case, we get that $n = 0$ and so that $p = 0$, which is impossible. Therefore, the only twin pair with a square mean is the pair $p = 3$ and $q = 5$.

24. Determine all twin primes p and $q = p + 2$ for which $pq - 2$ is also prime.

Solution First, notice that p cannot be of the form $3k+1$ because this would imply that q is of the form $3k'$ with k', a contradiction since q is prime. Thus, either p is of the form $3k$ (which only happens in the case $p = 3$), or p is of the form $3k + 2$. When $p = 3$, we have $pq - 2 = 3 \cdot 5 - 2 = 13$ which is a prime number. When $p = 3k + 2$, we have

$$pq - 2 = (3k+2)(3k+4) - 2 = 9k^2 + 18k + 6 = 3(3k^2 + 6k + 2)$$

which is composite. Therefore, the only pair that satisfies the condition is the pair $p = 3$ and $q = 5$.

25. Let p_n denote the nth prime. For $n > 3$, show that

$$p_n < p_1 + p_2 + \cdots + p_{n-1}.$$

[*Hint:* Use induction and Bertrand's Conjecture.]

Solution Let's prove it by induction on n. When $n = 4$, we have

$$p_1 + p_2 + p_3 = 2 + 3 + 5 = 10 > 7 = p_4.$$

Hence, the statement holds for $n = 4$. Suppose now that there is an integer $k > 3$ such that

$$p_k < p_1 + p_2 + \cdots + p_{k-1},$$

then equivalently, we have

$$0 < p_1 + p_2 + \cdots + p_{k-1} - p_k.$$

Moreover, by Bertrand's Conjecture, we have that there is a prime p such that $\frac{p_{k+1}-1}{2} < p < p_{k+1} - 1$. Since $p < p_{k+1}$, then we must have $p \leqslant p_k$, then we get that $\frac{p_{k+1}-1}{2} < p_k$ and so that $p_{k+1} - 1 < 2p_k$. Since both $p_{k+1} - 1$ and $2p_k$ are even, then we get that $p_{k+1} < 2p_k$. Finally, using the inequality above, we obtain

$$p_{k+1} < 2p_k < p_1 + p_2 + \cdots + p_{k-1} - p_k + 2p_k < p_1 + p_2 + \cdots + p_k.$$

Therefore, by induction, the statement holds for all $n > 3$.

26. Verify the following:

(a) There exist infinitely many primes ending in 33, such as 233, 433, 733, 1033, ... [*Hint:* Apply Dirichlet's Theorem.]

(b) There exist infinitely many primes which do not belong to any pair of twin primes. [*Hint:* Consider the arithmetic progression $21k + 5$ for $k = 1, 2,$...]

(c) There exists a prime ending in as many consecutive 1's as desired. [*Hint:* To obtain a prime ending in n consecutive 1's, consider the arithmetic progression $10^n k + R_n$ for $k = 1, 2, \ldots$.]

Solution

(a) Since $100 \cdot 1 + 33 \cdot (-3) = 1$, then $\gcd(100, 33) = 1$, and so by Dirichlet's Theorem there exist infinitely many primes of the form $100n + 33$. These primes are precisely the ones ending with 33.

(b) Since $21 \cdot 1 + 5 \cdot (-4) = 1$, then $\gcd(21, 5) = 1$, and so by Dirichlet's Theorem there exist infinitely many primes of the form $21n + 5$. Now, let p be a prime of the form $21n + 5$, then $p + 2 = 21n + 7 = 7(3n + 1)$ which is composite, and similarly, $p - 2 = 21n + 3 = 3(7n + 1)$ which is also composite. Thus, p cannot be a twin primes. Therefore, there are infinitely many primes which do not belong to a pair of twin primes.

(c) Let n be a positive integer, since $10^n \cdot 1 + R_n \cdot (-9) = 1$, then $\gcd(10^n, R_n) = 1$, and so by Dirichlet's Theorem there exist infinitely many primes of the form $10^n k + R_n$. In other words, there are infinitely many primes that end with n 1's. Since this holds for all n, then it follows that there exists a prime ending in as many consecutive 1's as desired.

27. Prove that for every $n \geqslant 2$ there exists a prime p with $p < n < 2p$. [*Hint:* If $n = 2k + 1$, then by Bertrand's Conjecture there exists a prime p such that $k < p < 2k$.]

Solution Let $n \geqslant 2$ be an integer. If n is even, then $n = 2k$ for some non-zero integer k. By Bertrand's Conjecture, we get that $k < p < 2k$ for some prime number p. From the inequality $k < p$, we get $n < 2p$ by multiplying both sides by 2, and from $p < 2k$, we get $p < n$ by definition of k. Thus, we get that $p < n < 2p$. Similarly, if n is odd, then $n = 2k + 1$ for some non-zero integer k. By Bertrand's Conjecture, we get that $k < p < 2k$ for some prime number p. From the inequality $k < p$, we get $n < 2p$ by multiplying both sides by 2, and from $p < 2k < 2k + 1$, we get $p < n$ by definition of k. Thus, we get that $p < n < 2p$. Therefore, it holds for all integers $n \geqslant 2$.

28.

(a) If $n > 1$, show that $n!$ is never a perfect square.

(b) Find the values of $n \geqslant 1$ for which

$$n! + (n+1)! + (n+2)!$$

is a perfect square. [*Hint:* Note that $n! + (n+1)! + (n+2)! = n!(n+2)^2$.]

Solution

(a) Let $n > 1$ be an integer and consider the integer $n! > 1$. Let p be the largest prime smaller than n, then $2p$ must be greater than n since otherwise, by Bertrand's Conjecture, there would be a prime q satisfying $p < q < 2p \leqslant n$ contradicting the fact that p is the greatest. It follows that p is the only integer divisible by p that is less than n. It follows that $n! = p^1 \cdot p_1^{r_1} \cdot \cdots \cdot p_k^{r_k}$ where $p_i \neq p$ for all i. This shows that $n!$ is not a square because an integer is a square if and only if every exponent in its canonical form is even (which is not the case for the exponent of p).

(b) When $n = 1$, we have that

$$n! + (n+1)! + (n+2)! = 1 + 2 + 6 = 3^2.$$

Suppose now that $n > 1$, then

$$n! + (n+1)! + (n+2)! = n!(n+2)^2.$$

Since $n!$ is not a square (part a), then it must contain a prime p with an odd exponent in its canonical form. It follows that the exponent of p in the canonical form of $n!(n+2)^2$ is also odd. Therefore, $n! + (n+1)! + (n+2)!$ cannot be a square in that case, and hence, it is only a square when $n = 1$.

Chapter 4

The Theory of Congruences

4.1 Karl Friedrich Gauss

There are no exercises in this section.

4.2 Basic Properties of Congruence

1. Prove each of the following assertions:

(a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.

(c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.

Solution

(a) If $a \equiv b \pmod{n}$, then $n \mid a - b$. Moreover, $m \mid n$ so $m \mid a - b$, and hence, by definition, $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{n}$, then $n \mid a - b$, and hence, $cn \mid c(a - b) = ca - cb$. It follows that $ca \equiv cb \pmod{cn}$.

(c) If $a \equiv b \pmod{n}$, then $a - b = nk$ for some integer k. This equation can be rewritten as $d(a/d - b/d) = d(kn/d)$. Since $d \neq 0$, then we get that $a/d - b/d = kn/d$ and so that by definition, we obtain $a/d \equiv b/d \pmod{n/d}$.

2. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

Solution We have that $1 \not\equiv -1 \pmod{3}$ but $1^2 \equiv (-1)^2 \pmod{3}$.

3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$.

Solution First, recall that if $a \equiv b \pmod{n}$, then there is an integer k such that $a = b + kn$. It follows that any integer linear combination $ax + ny$ of a and n can be written as a linear combination $bx + n(kx + y)$ of b and n. Similarly, any linear combination of b and n can also be written as a linear combination of a and n. It follows that the smallest positive integer that can be written as a linear combination of a and n must be equal to the smallest positive integer that can be written as a linear combination of b and n. In other words, $\gcd(a, n) = \gcd(b, n)$.

4.

(a) Find the remainders when 2^{50} and 41^{65} are divided by 7.

(b) What is the remainder when the sum

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

is divided by 4 ?

Solution

(a) Since $8 \equiv 1 \pmod 7$, then

$$2^{50} \equiv 2^{48} \cdot 4 \equiv 8^{16} \cdot 4 \equiv 1^{16} \cdot 4 \equiv 4 \pmod 7.$$

Hence, 2^{50} has a remainder of 4 after a division by 7. Similarly, since $41 \equiv -1 \pmod 7$, then

$$41^{65} \equiv (-1)^{65} \equiv -1 \equiv 6 \pmod 7.$$

Therefore, 41^{65} has a remainder of 6 after a division by 7.

(b) First, notice that every even number taken to the power of 5 must be divisible by 4. It follows that every even number in the sum is congruent to 0 modulo 4, and hence, can be discarded. The remaining integers 1, 3, 5, ... are alternatively congruent to 1 and -1 modulo 4, and hence, when taken to the power of 5, are still respectively congruent to 1 and -1. It follows that

$$1^5 + 2^5 + \cdots + 99^5 + 100^5 \equiv 1^5 + 3^5 + \cdots + 99^5 \equiv 1 - 1 + \cdots - 1 \equiv 0 \pmod 4.$$

Therefore, the sum has a remainder of 0 after a division by 4.

5. Prove that $53^{103} + 103^{53}$ is divisible by 39, and also that $111^{333} + 333^{111}$ is divisible by 7.

Solution First, notice that $53 \equiv 14 \pmod{39}$ and $103 \equiv -14 \pmod{39}$. Hence, we get that $53^{103} + 103^{53} \equiv 14^{103} + (-14)^{53} \equiv 14^{103} - 14^{53} \pmod{39}$. Now, notice that $14^2 \equiv 196 \equiv 1 \pmod{39}$, and so it follows that

$$53^{103} + 103^{53} \equiv 14^{103} - 14^{53} \equiv 14 \cdot 14^{2 \cdot 51} - 14 \cdot 14^{2 \cdot 26} \equiv 14 - 14 \equiv 0 \pmod{39}.$$

Therefore, $53^{103} + 103^{53}$ is divisible by 39.

Similarly, notice first that $111 \equiv -1 \pmod 7$ and $333 \equiv 4 \pmod 7$. Hence, $111^{333} + 333^{111} \equiv 1 + 4^{111}$. Now, since $4^3 \equiv -1 \pmod 7$, then

$$4^{111} \equiv 4^{3 \cdot 37} \equiv (-1)^{37} \equiv -1 \pmod 7$$

and so it follows that $111^{333} + 333^{111} \equiv 1 + 4^{111} \equiv 1 - 1 \equiv 0 \pmod 7$. Therefore, $111^{333} + 333^{111}$ is divisible by 7.

6. For $n \geqslant 1$, use congruence theory to establish each of the following divisibility statements:

(a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$;

(b) $13 \mid 3^{n+2} + 4^{2n+1}$;

(c) $27 \mid 2^{5n+1} + 5^{n+2}$;

(d) $43 \mid 6^{n+2} + 7^{2n+1}$;

Solution

(a) First, notice that $5^{2n} \equiv 25^n \equiv 4^n \pmod 7$ and

$$2^{5n-2} \equiv 2^{5(n-1)+3} \equiv 8 \cdot (2^5)^{n-1} \equiv 1 \cdot 4^{n-1}.$$

Hence, $5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^n + (-4) \cdot 4^{n-1} \equiv 0 \pmod 7$.

(b) Simply notice that

$$3^{n+2} + 4^{2n+1} \equiv 9 \cdot 3^n + 4 \cdot 3^n \equiv 13 \cdot 3^n \equiv 0 \pmod{13}.$$

(c) Simply notice that

$$2^{5n+1} + 5^{n+2} \equiv 2 \cdot 32^n + 25 \cdot 5^n \equiv 2 \cdot 5^n + 25 \cdot 5^n \equiv 27 \cdot 5^n \equiv 0 \pmod{27}.$$

(d) Simply notice that

$$6^{n+2} + 7^{2n+1} \equiv 36 \cdot 6^n + 7 \cdot 49^n \equiv 36 \cdot 6^n + 7 \cdot 6^n \equiv 43 \cdot 6^n \equiv 0 \pmod{43}.$$

7. For $n \geqslant 1$, show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}.$$

[*Hint:* Notice that $(-13)^2 \equiv -13 + 1 \pmod{181}$; use induction on n.]

Solution Let's prove it by induction. When $n = 1$, we have

$$(-13)^2 \equiv 169 \equiv -12 \equiv -13 + 1 \equiv (-13)^1 + (-13)^0 \pmod{181}.$$

Hence, it holds for $n = 1$. Suppose now that

$$(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181}$$

for some integer $k \geqslant 1$, then multiplying both sides by (-13) gives us

$$(-13)^{(k+1)+1} \equiv (-13)^{k+1} + (-13)^{(k+1)-1} \pmod{181}$$

which shows that the statement holds for $n = k + 1$. Therefore, the proposition holds for all integers $n \geqslant 1$.

8. Prove the assertions below:

(a) If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

(b) For any integer a, $a^3 \equiv 0$, 1, or $6 \pmod 7$.

(c) For any integer a, $a^4 \equiv 0$, or $1 \pmod{5}$.

(d) If the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

Solution

(a) If a is odd, then either $a = 4k+1$ or $a = 4k+3$. In the first case:

$$a^2 \equiv 16k^2 + 8k + 1 \equiv 1 \pmod{8}.$$

In the second case:

$$a^2 \equiv 16k^2 + 8 \cdot 3k + 9 \equiv 1 \pmod{8}.$$

Therefore, $a^2 \equiv 1 \pmod{8}$ for all odd integers a.

(b) Let's work in modulo 7. If $a \equiv 0$, then $a^3 \equiv 0$. If $a \equiv 1$, then $a^3 \equiv 1$. If $a \equiv 2$, then $a^3 \equiv 8 \equiv 1$. If $a \equiv 3$, then $a^3 \equiv 27 \equiv 6$. If $a \equiv 4$, then $a^3 \equiv (-3)^3 \equiv -27 \equiv 1$. If $a \equiv 5$, then $a^3 \equiv (-2)^3 \equiv -8 \equiv 6$. If $a \equiv 6$, then $a^3 \equiv (-1)^3 \equiv -1 \equiv 6$. Therefore, in general, 0, 1 and 6 are the three only possible residues of cubes modulo 7.

(c) Let's work in modulo 5. If $a \equiv 0$, then $a^4 \equiv 0$. If $a \equiv 1$, then $a^4 \equiv 1$. If $a \equiv 2$, then $a^4 \equiv 16 \equiv 1$. If $a \equiv 3$, then $a^4 \equiv (-2)^4 \equiv 1$. If $a \equiv 4$, then $a^4 \equiv (-1)^4 \equiv 1$. Therefore, 0 and 1 are the two only possible residues of a power of 4 modulo 5.

(d) First, notice that an integer a is divisible by 2 or by 3 if and only if its residue modulo 24 is divisible by 2 or by 3. This comes from the fact that 24 is divisible by 2 and 3. Therefore, if an integer is not divisible by 2 and 3, then its possible residues modulo 24 are 0, 1, 5, 7, 11, 13, 17, 19 and 23. Let's now work in modulo 24. If $a \equiv 0$, then $a^2 \equiv 0$. If $a \equiv 1$, then $a^2 \equiv 1$. If $a \equiv 5$, then $a^2 \equiv 25 \equiv 1$. If $a \equiv 7$, then $a^2 \equiv 49 \equiv 1$. If $a \equiv 11$, then $a^2 \equiv 121 \equiv 1$. If $a \equiv 13$, then $a^2 \equiv (-11)^2 \equiv 1$. If $a \equiv 17$, then $a^2 \equiv (-7)^2 \equiv 1$. If $a \equiv 19$, then $a^2 \equiv (-5)^2 \equiv 1$. If $a \equiv 23$, then $a^2 \equiv (-1)^2 \equiv 1$. Therefore, if a is not divisible by 2 and 3, then a^2 must be 0 or 1 modulo 7.

9. If p is a prime satisfying $n < p < 2n$, show that

$$\binom{2n}{n} \equiv 0 \pmod{p}.$$

Solution First, write

$$\binom{2n}{n} = \frac{2n(2n-1) \cdot ... \cdot (n+1)}{n!},$$

then this can be rewritten as

$$2n(2n-1) \cdot ... \cdot (n+1) = \binom{2n}{n} \cdot n!.$$

Since $n < p < 2n$, then p must be one of the factors on the left hand side. It follows that p divides the right hand side. However, since $p > n$, then p cannot divide $n!$, and hence, p must divide $\binom{2n}{n}$. Therefore, $\binom{2n}{n} \equiv 0 \pmod{p}$.

10. If $a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_n$ is also a complete set of residues modulo n. [*Hint:* It suffices to show that the numbers in question are incongruent modulo n.]

Solution It suffices to show that aa_i is incongruent to aa_j modulo n when $i \neq j$. Let $i \neq j$ be two integers between 1 and n, suppose by contradiction that $aa_i \equiv aa_j \pmod{n}$, then by the fact that $\gcd(a, n) = 1$, we get that $a_i \equiv a_j \pmod{n}$. But since a_1, ..., a_n forms a complete set of residues modulo n, then $a_i \equiv a_j \pmod{n}$ implies that $i = j$, a contradiction. Therefore, $aa_i \not\equiv aa_j \pmod{n}$ whenever $i \neq j$. It follows that aa_1, ..., aa_n forms a complete set of residues modulo n.

11. Verify that 0, 1, 2, 2^2, 2^3, . . . , 2^9 form a complete set of residues modulo 11, but 0, 1^2, 2^2, 3^2 . . . , 10^2 do not.

Solution First, we have

$$\begin{aligned}
0 &\equiv 0 \pmod{11} \\
1 &\equiv 1 \pmod{11} \\
2 &\equiv 2 \pmod{11} \\
2^2 &\equiv 4 \pmod{11} \\
2^3 &\equiv 8 \pmod{11} \\
2^4 &\equiv 16 \equiv 5 \pmod{11} \\
2^5 &\equiv 2 \cdot 5 \equiv 10 \pmod{11} \\
2^6 &\equiv 2 \cdot 10 \equiv 20 \equiv 9 \pmod{11} \\
2^7 &\equiv 2 \cdot 9 \equiv 18 \equiv 7 \pmod{11} \\
2^8 &\equiv 2 \cdot 7 \equiv 14 \equiv 3 \pmod{11} \\
2^9 &\equiv 2 \cdot 3 \equiv 6 \pmod{11}
\end{aligned}$$

Since they are all incongruent to each other, then we have that 0, 1, 2, ..., 2^9 forms a complete set of residues modulo 11. However, the first 11 squares do not because $1^1 \equiv 1 \equiv 10^2 \pmod{11}$.

12. Prove the following statements:

(a) If $gcd(a, n) = 1$, then the integers

$$c,\ c + a,\ c + 2a,\ c + 3a,\ \ldots,\ c + (n - 1)a$$

form a complete set of residues modulo n for any c.

(b) Any n consecutive integers form a complete set of residues modulo n. [*Hint:* Use part (a).]

(c) The product of any set of n consecutive integers is divisible by n.

Solution

(a) First, recall that 0, 1, 2, ..., $n-1$ forms a complete set of residues modulo n. This implies that for integers i and j between 0 and $n-1$, $i \equiv j \pmod{n}$ only if $i = j$. Now, let i and j be two integers between 0 and $n-1$ and suppose that $c + ai \equiv c + aj \pmod{n}$, then by subtracting by c on both sides, we get that $ai \equiv aj \pmod{n}$. Now, since $\gcd(a, n) = 1$, then we can "divide" both sides by a to obtain $i \equiv j \pmod{n}$, which in turns implies that $i = j$. Therefore, the integers c, $c + a$, ..., $c + (n-1)a$ are all incongruent and so they form a complete set of residues modulo n.

(b) Notice that any n consecutive integers can be written as c, $c+1$, ..., $c+(n-1)$ where c is the first of the n integers. By taking $a = 1$ in part (a), we immediately get that these n consecutive integers must form a complete set of residues modulo n.

(c) Let a_1, a_2, ..., a_n be a list of n consecutive integers, then by part (b), it is a complete set of residues modulo n. It follows that there is a i between 1 and n such that $a_i \equiv 0 \pmod{n}$. Thus,

$$a_1 a_2 \cdots a_i \cdots a_n \equiv a_1 a_2 \cdots 0 \cdots a_n \equiv 0 \pmod{n}$$

which implies that $n \mid a_1 a_2 \cdots a_n$.

13. Verify that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod{n}$, where the integer $n = \operatorname{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b \pmod{n_1 n_2}$.

Solution If $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then by definition, $a - b$ is a common multiple of n_1 and n_2. Thus, by properties of the least common multiple, we must have that $\operatorname{lcm}(n_1, n_2) \mid a - b$. It follows that $a \equiv b \pmod{n}$ where $n = \operatorname{lcm}(n_1, n_2)$. When n_1 and n_2 are relatively prime, we have $\operatorname{lcm}(n_1, n_2) = n_1 n_2$.

14. Give an example to show that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ need not imply $a^j \equiv b^j \pmod{n}$.

Solution We know that $1^2 \equiv (-1)^2 \pmod{3}$ but $1^5 \not\equiv (-1)^5 \pmod{3}$ even though $2 \equiv 5 \pmod{3}$.

15. Establish that if a is an odd integer, then

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

for any $n \geqslant 1$. [*Hint:* Proceed by induction on n.]

Solution Let's prove it by induction on n. The case $n = 1$ is exactly part (a) of Problem 8 of this section. Suppose now that $a^{2^k} \equiv 1 \pmod{2^{k+2}}$ for some integer $k \geqslant 1$, then $2^{k+2} \mid a^{2^k} - 1$. Now, notice that $a^{2^{k+1}} - 1 = (a^{2^k} - 1)(a^{2^k} + 1)$ is both divisible by 2^{k+2} (from the first factor) and divisible by 2 (from the second factor since $a^{2^k} + 1$ is even). It follows that $2^{k+3} \mid a^{2^{k+1}} - 1$ and so $a^{2^{k+1}} \equiv 1 \pmod{2^{(k+1)+2}}$. Therefore, it holds for all $n \geqslant 1$ by induction.

16. Use the theory of congruences to verify that

$$89 \mid 2^{44} - 1 \qquad \text{and} \qquad 97 \mid 2^{48} - 1.$$

Solution First, notice that $2^{44} = (2^{11})^4 = 2048^4$. Since $2048 \equiv 1 \pmod{89}$, then $2^{44} \equiv 1^4 \equiv 1 \pmod{89}$. It follows that $89 \mid 2^{44} - 1$.

Similarly, notice that $2^{48} = (2^{12})^4 = 4096^4$. Now, we can check that $4096 \equiv 22 \pmod{97}$ and so $2^{48} \equiv 22^4 \pmod{97}$. Moreover, $22^2 = 484$ which can be checked to be congruent to -1 modulo 97. It follows that $2^{48} \equiv 22^4 \equiv (-1)^2 \equiv 1 \pmod{97}$. Therefore, $97 \mid 2^{48} - 1$.

17. Prove that if $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod{n}$.

Solution From the equation $b \equiv d \pmod{n}$, we get $cb \equiv cd \pmod{n}$ by multiplying both sides by c. From $ab \equiv cd \pmod{n}$ and $cb \equiv cd \pmod{n}$, we get $ab \equiv cb \pmod{n}$. Finally, using the fact that $\gcd(b, n) = 1$ lets us conclude that $a \equiv c \pmod{n}$.

18. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$, where the integer $n = \gcd(n_1, n_2)$.

Solution If we let $n = \gcd(n_1, n_2)$, then from the fact that $n \mid n_1, n_2$ and Problem 1.(a) of this section, we get that $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$. By transitivity, it follows that $b \equiv c \pmod{n}$.

4.3 Special Divisibility Tests

1. Prove the following statements:

(a) For any integer a, the units digit of a^2 is 0, 1, 4, 5, 6, or 9.

(b) Any one of the integers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 can occur as the units digit of a^3.

(c) For any integer a, the units digit of a^4 is 0, 1, 5, or 6.

(d) The units digit of a triangular number is 0, 1, 3, 5, 6 or 8.

Solution

(a) It suffices to prove that the only possible residues modulo 10 of a square are 0, 1, 4, 5, 6, or 9. Let's prove it by cases. If $a \equiv 0$, then $a^2 \equiv 0$. If $a \equiv 1$, then $a^2 \equiv 1$. If $a \equiv 2$, then $a^2 \equiv 4$. If $a \equiv 3$, then $a^2 \equiv 9$. If $a \equiv 4$, then $a^2 \equiv 6$. If $a \equiv 5$, then $a^2 \equiv 5$. If a is congruent to 6, 7, 8 or 9, then $-a$ will be congruent to one of the previous cases and so the square are goind to be the same since $(-a)^2 = a^2$. Therefore, from this cases, we get that the possible residues are 0, 1, 4, 5, 6, 9.

(b) It suffices to prove that for all $0 \leqslant i \leqslant 9$, there is an integer a such that $a^3 \equiv i \pmod{10}$. For $i = 0, 1$, simply take $a = i$. For $i = 2$, we have $8^3 \equiv 512 \equiv i$. For $i = 3$, we have $7^3 \equiv 343 \equiv i$. For $i = 4$, we have $4^3 \equiv 64 \equiv i$. For $i = 5$, we have $5^3 \equiv 125 \equiv i$. For $i = 6$, we have $6^3 \equiv 216 \equiv i$. For $i = 7$, we have $3^3 \equiv 27 \equiv i$. For $i = 8$, we have $2^3 \equiv i$. For $i = 9$, we have $9^3 \equiv (-1)^3 \equiv -1 \equiv i$.

(c) Using part (a), it suffices to look at the residues modulo 10 of the squares of 0, 1, 4, 5, 6, 9.

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 4^2 \equiv 6, \qquad 5^2 \equiv 5, \qquad 6^2 \equiv 6, \qquad 9^2 \equiv 1.$$

Therefore, the only possible units of an integer taken to the fourth power are 0, 1, 5 or 6.

(d) Here it is temmpting to simply consider the ten cases of residues modulo 10. However, we never proved that $i \equiv j$ implies $t_i \equiv t_j$. This is nontrivial since this not true in modulo 10. To do this, let's first find the residues of $n(n+1)$ and then deduce the possible residues of triangle numbers. Using the same technique as in part (a) or part (b), we get that the possible residues of $n(n+1)$ are 0, 2 or 6. Now, to find the possible residues of t_n, it suffices to answer the question, what are the numbers such when multiplied by 2, have residue 0, 2, or 6. Again, by cases, we get that these numbers are 0, 1, 3, 5, 6 or 8. Since for each of these numbers it is possible to find a triangular number congruent to it, then this list represents precisely the possible units of a triangular number.

2. Find the last two digits of the number 9^{9^9}. [*Hint:* $9^9 \equiv 9 \pmod{10}$, hence $9^{9^9} = 9^{9+10k}$; now use the fact that $9^{10} \equiv 1 \pmod{100}$.]

Solution First, notice that it suffices to find the residue of 9^{9^9} modulo 100. To do this, let's first find the residue of 9^9 modulo 100:

$$\begin{aligned}
9^9 &\equiv 9^8 \cdot 9 \\
&\equiv (9^2)^4 \cdot 9 \\
&\equiv ((-19)^2)^2 \cdot 9 \\
&\equiv (-39)^2 \cdot 9 \\
&\equiv 21 \cdot 9 \\
&\equiv 89.
\end{aligned}$$

Therefore, we have that $9^9 = 89 + 100n$. This implies that $9^9 = 9 + 10k$ and so we have

$$9^{9^9} = 9^{9+10k} = 9^9 \cdot (9^{10})^k.$$

Since $9^9 \equiv 89 \equiv -11 \pmod{100}$, then $9^{10} \equiv -99 \equiv 1 \pmod{100}$. It follows that

$$9^{9^9} \equiv 89 \cdot 1^k \equiv 89 \pmod{100}.$$

Therefore, the last two digits are 89.

3. Without performing the divisions, determine whether the integers $176, 521, 221$ and $149, 235, 678$ are divisible by 9 or 11.

Solution We simply need to take the (alternating) sum of the digits and examine the resulting numbers. Let's verify if the first number is divisible by 9:

$$1 + 7 + 6 + 5 + 2 + 1 + 2 + 2 + 1 = 27$$

which is divisible by 9. Thus, the first number is divisible by 9. Let's do the same with the second number:

$$1 + 4 + 9 + 2 + 3 + 5 + 6 + 7 + 8 = 45$$

which is again divisible by 9. Thus, even the second number is divisible by 9. Now, let's check the divisibility by 11.

$$1 - 2 + 2 - 1 + 2 - 5 + 6 - 7 + 1 = -3$$

and

$$8 - 7 + 6 - 5 + 3 - 2 + 9 - 4 + 1 = 9.$$

Since none of the results are divisible by 11, then none of the numbers are either.

4.

(a) Obtain the following generalization of Theorem 4-5: If the integer N is represented in the base b by

$$N = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0, \quad 0 \leqslant a_k \leqslant b - 1$$

then $b - 1 \mid N$ if and only if $b - 1 \mid (a_m + \cdots + a_2 + a_1 + a_0)$.

(b) Give criteria for the divisibility the divisibility of N by 3 and 8 which depend on the digits of N when written in base 9.

(c) Is the integer $(447836)_9$ divisible by 3 and 8?

Solution

(a) Consider the polynomial $P(x) = \sum_{k=0}^{m} a_k x^k$. Since $b \equiv 1 \pmod{b-1}$, then

$$\sum_{k=0}^{m} a_k \equiv \sum_{k=0}^{m} a_k b^k \equiv N \pmod{b-1}.$$

Therefore,

$$\begin{aligned} b-1 \mid N &\iff N \equiv 0 \pmod{b-1} \\ &\iff \sum_{k=0}^{m} a_k \equiv 0 \pmod{b-1} \\ &\iff b-1 \mid a_m + \cdots + a_2 + a_1 + a_0 \end{aligned}$$

which is exactly what we wanted to prove.

(b) Using part (a), we get that N is divisible by 8 if and only if the sum of the digits of its base-9 representation is divisible by 8. To find a criteria for the divisibility modulo 3, write $N = \sum_{k=0}^{m} a_k 9_k$, then $N \equiv a_0 \pmod 3$ which shows that N is divisible by 3 if and only if its first digit is divisible by 3 in its base-9 representation.

(c) Since 6 is divisible by 3, then it follows from part (b) that $(447836)_9$ is divisible by 3. Next,

$$4 + 4 + 7 + 8 + 3 + 6 = 32$$

is divisible by 8 and so by part (b), $(447836)_9$ is divisible by 8.

5. Working modulo 9 or 11, find the missing digits in the calculations below:

(a) $51840 \cdot 273581 = 1418243x040$;

(b) $2x99561 = [3(523 + x)]^2$;

(c) $2784x = x \cdot 5569$;

(d) $512 \cdot 1x53125 = 1000000000$.

Solution

(a) If we take this equation modulo 11, we get

$$(0-4+8-1+5)(1-8+5-3+7-2) \equiv 0-4+0-x+3-4+2-8+1-4+1$$

which is the same as $8 \cdot 0 \equiv -13 - x \pmod{11}$. Hence, $x \equiv -13 \equiv 9 \pmod{11}$. But since x is a digit in base 10, then $0 \leqslant x \leqslant 9$ and so $x \equiv 9 \pmod{11}$ implies $x = 9$.

(b) If we take this equation modulo 9, we get

$$2 + x + 9 + 9 + 5 + 6 + 1 \equiv 0 \pmod 9$$

which is equivalent to $x \equiv -5 \equiv 6 \pmod 9$. Since $0 \leqslant x \leqslant 9$, then $x = 6$.

(c) If we take the equation modulo 11, we get

$$x - 4 + 8 - 7 + 2 \equiv x(9 - 6 + 5 - 5) \pmod{11}$$

which is equivalent to $x - 1 \equiv 3x \pmod{11}$. Rearranging the equation gives $2x \equiv 2 \cdot 5 \pmod{11}$. Since $\gcd(2, 11) = 1$, then $x = 5 \pmod{11}$ and so $x = 5$.

(d) If we take the equation modulo 11, we get

$$(2 - 1 + 5)(5 - 2 + 1 - 3 + 5 - x + 1) \equiv -1 \pmod{11}$$

which is equivalent to $6(7-x) \equiv -1 \pmod{11}$. Simplifying the equation gives us $43 \equiv 6x \pmod{11}$ and so $6x \equiv 1 \pmod{11}$. Multiplying by 9 on both sides gives us $x \equiv 54x \equiv 9 \pmod{11}$. Therefore, $x = 9$.

6. Establish the following divisibility criteria:

(a) An integer is divisible by 2 if and only if the sum of its digit is 0, 2, 4, 6, or 8.

(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

(c) An integer is divisible by 4 if and only if the number formed by by its tens and units digits is divisible by 4. [*Hint:* $10^k \equiv 0 \pmod 4$ for $k \geqslant 2$.]

(d) An integer is divisible by 5 if and only if its unit digit is 0 or 5.

Solution

(a) Let N be an arbitrary integer and write it as

$$N = a_m \cdot 10^m + \cdots + a_1 \cdot 10 + a_0$$

where the a_i's satisfy $0 \leqslant a_i \leqslant 9$. Notice that if we take the above equation modulo 2, we get that all the terms become zero except maybe a_0: $N \equiv a_0 \pmod 2$. Hence, we get that the divisibility by 2 of N is equivalent to the divisibility by 2 of a_0. Since $0 \leqslant a_0 \leqslant 9$, then a_0 is only divisible by 2 when $a_0 = 0, 2, 4, 6, 8$. Therefore, N is divisible by 2 if and only if its unit digit is 0, 2, 4, 6 or 8.

(b) Let N be an arbitrary integer and write it as

$$N = a_m \cdot 10^m + \cdots + a_1 \cdot 10 + a_0$$

where the a_i's satisfy $0 \leqslant a_i \leqslant 9$. Notice that if we take the above equation modulo 3, we get that

$$N \equiv a_m + \cdots + a_1 + a_0 \pmod 3$$

since $10 \equiv 1 \pmod 3$. Hence, N is divisible by 3 if and only the sum of its digit is divisible by 3.

(c) Let N be an arbitrary integer and write it as

$$N = a_m \cdot 10^m + \cdots + a_1 \cdot 10 + a_0$$

where the a_i's satisfy $0 \leqslant a_i \leqslant 9$. Notice that if we take the above equation modulo 4, we get that $N \equiv 10a_1 + a_0 \pmod 4$. Since $10a_1 + a_0 = (a_1a_0)_{10}$, then it follows that N is divisible by 4 if and only if $N \equiv 0 \pmod 4$, if and only if $(a_1a_0)_{10} \equiv 0 \pmod 4$, if and only if $(a_1a_0)_{10}$ is divisible by 4.

(d) Let N be an arbitrary integer and write it as

$$N = a_m \cdot 10^m + \cdots + a_1 \cdot 10 + a_0$$

where the a_i's satisfy $0 \leqslant a_i \leqslant 9$. Notice that if we take the above equation modulo 5, we get that all the terms become zero except maybe a_0: $N \equiv a_0 \pmod 5$. Hence, we get that the divisibility by 5 of N is equivalent to the divisibility by 5 of a_0. Since $0 \leqslant a_0 \leqslant 9$, then a_0 is only divisible by 5 when $a_0 = 0, 5$. Therefore, N is divisible by 5 if and only if its unit digit is 0 or 5.

7. For any integer a, show that $a^2 - a + 7$ ends in one of the digits 3, 7, or 9.

Solution It suffices to show that 3, 7 and 9 are the only possible residues of a^2-a+7 modulo 10. Let's work by cases in modulo 10.

- $a \equiv 0 \implies a^2 - a + 7 \equiv 0 - 0 + 7 \equiv 7$;
- $a \equiv 1 \implies a^2 - a + 7 \equiv 1 - 1 + 7 \equiv 7$;
- $a \equiv 2 \implies a^2 - a + 7 \equiv 4 - 2 + 7 \equiv 9$;
- $a \equiv 3 \implies a^2 - a + 7 \equiv 9 - 3 + 7 \equiv 3$;
- $a \equiv 4 \implies a^2 - a + 7 \equiv 16 - 4 + 7 \equiv 9$;
- $a \equiv 5 \implies a^2 - a + 7 \equiv 25 - 5 + 7 \equiv 7$;
- $a \equiv 6 \implies a^2 - a + 7 \equiv 36 - 6 + 7 \equiv 7$;
- $a \equiv 7 \implies a^2 - a + 7 \equiv 49 - 7 + 7 \equiv 9$;
- $a \equiv 8 \implies a^2 - a + 7 \equiv 64 - 8 + 7 \equiv 3$;
- $a \equiv 9 \implies a^2 - a + 7 \equiv 81 - 9 + 7 \equiv 9$;

The proposition now clearly follows.

8. Find the remainder when 4444^{4444} is divided by 9. [*Hint:* Observe that $2^3 \equiv -1 \pmod 9$.]

Solution First, we have that $4444 \equiv 4 + 4 + 4 + 4 \equiv 2^4 \pmod 9$ and so

$$4444^{4444} \equiv (2^{4444})^4 \pmod 9.$$

Now, consider the fact that $4444 = 3 \cdot 1481 + 1$ and use it to get

$$\begin{aligned} 4444^{4444} &\equiv [2^{3\cdot 1481+1}]^4 \\ &\equiv [2 \cdot (2^3)^{1481}]^4 \\ &\equiv [2 \cdot (-1)^{1481}]^4 \\ &\equiv (-2)^4 \\ &\equiv 16 \\ &\equiv 7 \end{aligned}$$

which implies that 7 is the remainder of 4444^{4444} after a division by 9.

9. Prove that no integer whose digits add up to 15 can be a square or a cube. [*Hint:* For any a, $a^3 \equiv 0, 1,$ or $8 \pmod 9$.]

Solution Let's find the possible residues of the squares and the cubes modulo 9.

- $a \equiv 0 \implies a^2 \equiv 0$ and $a^3 \equiv 0$;
- $a \equiv 1 \implies a^2 \equiv 1$ and $a^3 \equiv 1$;
- $a \equiv 2 \implies a^2 \equiv 4$ and $a^3 \equiv 8$;
- $a \equiv 3 \implies a^2 \equiv 0$ and $a^3 \equiv 0$;
- $a \equiv 4 \implies a^2 \equiv 7$ and $a^3 \equiv 1$;
- $a \equiv 5 \implies a^2 \equiv 7$ and $a^3 \equiv 8$;
- $a \equiv 6 \implies a^2 \equiv 0$ and $a^3 \equiv 0$;
- $a \equiv 7 \implies a^2 \equiv 4$ and $a^3 \equiv 1$;
- $a \equiv 8 \implies a^2 \equiv 1$ and $a^3 \equiv 8$;

Let N be an integer such that the sum of its digits is 15, then in other words, $N \equiv 15 \equiv 6 \pmod 9$. Since 6 appears nowhere in the cases above, then N is neither a square or a cube.

10. Assuming that 495 divides $273x49y5$, obtain the digits x and y.

Solution Since 495 divides $273x49y5$, then there is an integer k such that $495k = 273x49y5$. Taking this equation modulo 9 gives us

$$2 + 7 + 3 + x + 4 + 9 + y + 5 \equiv (4 + 9 + 5)k \equiv 0 \pmod 9$$

which can be simplified into $3+x+y \equiv 0 \pmod 9$. Similarly, if we take the equation modulo 11, we get

$$5 - y + 9 - 4 + x - 3 + 7 - 2 \equiv (5 - 9 + 4)k \equiv 0 \pmod{11}$$

which can be simplified into $1 + x \equiv y \pmod{11}$. Since both $1 + x$ and y are between 0 and 10, then this equation becomes $1 + x = y$. Making this substitution into the first equation we found gives us $2x \equiv -4 \pmod 9$. Since $\gcd(2,9) = 1$, then $x \equiv -2 \equiv 7 \pmod 9$. Since $0 \leqslant x \leqslant 9$, then $x = 7$ and so $y = 8$.

11. Determine the last three digits of the number 7^{999}. [*Hint:* $7^{4n} \equiv (1+400)^n \equiv 1 + 400n \pmod{1000}$.]

Solution It suffices to find the residue of 7^{999} modulo 1000. Notice that

$$7^4 \equiv (50-1)^2 \equiv 2500 - 100 + 1 \equiv 1 + 400 \pmod{1000}$$

and so

$$7^{4n} \equiv (1+400)^n \equiv 1 + 400n + 0 + 0 + ... + 0 \equiv 1 + 400n \pmod{1000}.$$

Since $999 = 4 \cdot 249 + 3$, then

$$\begin{aligned} 7^{999} &\equiv 7^3(1 + 400 \cdot 249) \\ &\equiv 343 \cdot (1 + 400 \cdot 9) \\ &\equiv 343 \cdot (1 + 600) \\ &\equiv 343 + 205800 \\ &\equiv 343 + 800 \\ &\equiv 143. \end{aligned}$$

Therefore, the last three digits of 7^{999} are 143.

12. If t_n denotes the nth triangular number, show that $t_{n+2k} \equiv t_n \pmod k$; hence, t_n and t_{n+20} must have the same last digit.

Solution Let n and k be positive integers, then

$$\begin{aligned} t_{n+2k} &\equiv \frac{(n+2k)(n+2k+1)}{2} \\ &\equiv \frac{n(n+2k+1)}{2} + k(n+2k+1) \\ &\equiv \frac{n(n+2k+1)}{2} \\ &\equiv \frac{n(n+1)}{2} + kn \\ &\equiv t_n \pmod k \end{aligned}$$

which proves the statement.

13. For any $n > 1$, prove that there exists a prime with at least n of its digits equal to 0. [*Hint:* Consider the arithmetic progression $10^{n+1}k + 1$ for $k = 1, 2, \ldots$.]

Solution Consider the arithmetic progression $10^{n+1}k + 1$ where $k = 1, 2, \ldots$, since $\gcd(10^{n+1}, 1) = 1$, then by Dirichlet's Theorem there are infinitely many primes numbers of the form $10^{n+1}k + 1$, and so there must be at least ine such prime. Notice now that any number of that form has a unit digit of 1 and the following n

digits equal to 0. Therefore, there exists a prime with at least n of its digits equal to 0.

14. Find the values of $n \leqslant 1$ for which $1! + 2! + 3! + \cdots + n!$ is a perfect square. [*Hint:* Problem 1(a).]

Solution Let's consider the residues of the sequence $1! + 2! + ... + n!$ modulo n. We have that $1! \equiv 1$, $1! + 2! \equiv 3$, $1! + 2! + 3! \equiv 9$, $1! + 2! + 3! + 4! \equiv 3$, and since $n! \equiv 0$ for all $n \geqslant 5$, then $1! + 2! + \cdots + n! \equiv 3$ for all $n \geqslant 5$. Since the possible residues of a square in modulo 10 are 0, 1, 4, 5, 6 or 9, then we know for sure that $1! + 2! + \cdots + n!$ is not a square for $n = 2$ and for all $n \geqslant 4$. Since $1!$ and $1! + 2! + 3!$ are squares, then we have that the sum is a square precisely when $n = 1$ or $n = 3$.

15. Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N. [*Hint:* $10^k \equiv 2^k 5^k \equiv 0 \pmod{2^n}$ for $k \geqslant n$.]

Solution First, suppose that N is made up of more than n digits, otherwise, the statement is trivial. Write N as $a_m 10^m + \cdots + 10a_1 + a_0$ such that $N = (a_m \dots a_1 a_0)_{10}$, then

$$N \equiv a_m 10^m + \cdots + 10a_1 + a_0 \equiv 0 + \cdots + 0 + a_{n-1}10^{n-1} + \cdots + a_0 \pmod{2^n}$$

and so $N \equiv (a_{n-1} \dots a_1 a_0)_{10} \pmod{2^n}$. Therefore, 2^n divides N if and only if 2^n divides $(a_{n-1} \dots a_1 a_0)_{10}$.

16. Let $N = a_m 10^m + \cdots + a_2 10^2 + a_1 10 + a_0$, where $0 \leqslant a_k \leqslant 9$, be the decimal expansion of a positive integer N.

(a) Prove that 7, 11, and 13 all divide N if and only if 7, 11, and 13 divide the integer

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \dots$$

[*Hint:* If n is even, then $10^{3n} \equiv 1$, $10^{3n+1} \equiv 10$, $10^{3n+2} \equiv 100 \pmod{1001}$; $10^{3n} \equiv -1$, $10^{3n+1} \equiv -10$, $10^{3n+2} \equiv -100 \pmod{1001}$.]

(b) Prove that 6 divides N if and only if 6 divides the integer $M = a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$.

Solution

(a) First, notice that

$$10^{3n} \equiv (1000)^n \equiv (-1)^n \pmod{1001}.$$

It follows that the residues of the sequence 1, 10, 10^2, 10^3, 10^4, ... are respectively 1, 10, 100, -1, -10, -100, 1, 10, ... Hence, we get that

$$N \equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + \cdots \equiv M \pmod{1001}.$$

Next, notice that 7, 11, and 13 are all relatively prime so they all divide a number L if and only if their product 1001 divides that same number L. From this, we get that 7, 11, and 13 all divide N, if and only if 1001 divides N, if and only if 1001 divides M, if and only if 7, 11, and 13 all divide M.

(b) First, let's prove by induction that $10^n \equiv 4 \pmod 6$ for all $n \geqslant 1$. For $n = 1$, this is trivial. Suppose now that $10^n \equiv 4 \pmod 6$ for some $n \geqslant 1$, then

$$10^{n+1} \equiv 10^n \cdot 10 \equiv 4 \cdot 4 \equiv 16 \equiv 4 \pmod 6.$$

Therefore, by induction, the proposition holds for all $n \geqslant 1$. From this, we get that $N \equiv M \pmod 6$. Therefore, it follows that N is divisible by 6 if and only if M is divisible by 6.

17. Without performing the divisions, determine whether the integer $1,010,908,899$ is divisible by 7, 11, and 13.

Solution Let $M = 899 - 908 + 10 - 1 = 0$, notice that M is trivially divisible by 7, 11, and 13. Therefore, from the previous exercise, N is divisible by 7, 11, and 13.

18.

(a) Given an integer N, let M be the integer formed by reversing the order of the digits of N (for example, if $N = 6923$, then $M = 3296$). Verify that $N - M$ is divisible by 9.

(b) A *palindrome* is a number that reads the same backwards as forwards (for instance, 373 and 521125 are palindromes). Prove that any palindrome with an even number of digits is divisible by 11.

Solution

(a) Let $N = a_m 10^m + \cdots + a_1 10 + a_0$ and $M = a_0 10^m + \cdots + a_{m-1} 10 + a_m$, then in modulo 9, we have

$$N - M \equiv (a_m + \cdots + a_1 + a_0) - (a_0 + \cdots + a_{m-1} + a_m) \equiv 0 \pmod 9.$$

Therefore, 9 divides $N - M$.

(b) Let $N = a_{2n+1} 10^{2n+1} + \cdots + a_1 10 + a_0$ be a palindrome with an even number of digits, then $a_0 = a_{2n+1}$, $a_1 = a_{2n}$, ..., and so we get

$$N \equiv a_0 - a_1 + \cdots + a_{2n} - a_{2n+1} \equiv 0 \pmod{11}.$$

Therefore, N is divisible by 11.

19. Given a repunit R_n, show that

(a) $9 \mid R_n$ if and only if $9 \mid n$.

(b) $11 \mid R_n$ if and only if n is even.

Solution

(a) Since $R_n \equiv 1 + 1 + ... + 1 \equiv n \pmod 9$, then it directly follows that 9 divides R_n if and only if 9 divides n.

(b) Since

$$R_n \equiv 1 - 1 + 1 - ... \pm 1 \equiv \begin{cases} 0, & \text{if } n \text{ is even} \\ 1, & \text{if } n \text{ is odd} \end{cases} \pmod{11},$$

then 11 divides R_n if and only if n is even.

20. Factor the repunit $R_6 = 111111$ into a product of primes. [*Hint:* Problem 16.]

Solution Using Problem 16 part (a), we get that 111111 is divisible by 7, 11, and 13 because $111 - 111 = 0$. Hence, we get that $R_6 = 7 \cdot 11 \cdot 13 \cdot 111$. Since 111 is divisible by 3, then we can write it as $3 \cdot 37$. Since 37 is prime, then we get that $R_6 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$.

21. Explain why the following curious calculations hold:

$$\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1111 \\
1234 \cdot 9 + 5 &= 11111 \\
12345 \cdot 9 + 6 &= 111111 \\
123456 \cdot 9 + 7 &= 1111111 \\
1234567 \cdot 9 + 8 &= 11111111 \\
12345678 \cdot 9 + 9 &= 111111111 \\
123456789 \cdot 9 + 10 &= 1111111111
\end{aligned}$$

[*Hint:* Show that

$$\begin{aligned}(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \cdots + n)(10 - 1)& \\ + (n+1) = (10^{n+1} - 1)/9.]&\end{aligned}$$

Solution In this exercice, consider that the notation $(a_m \dots a_1 a_0)_{10}$ is just another way of writing

$$a_m 10^m + ... + a_1 10 + a_0$$

with no restrictions on the a_i's. Let's prove it by induction on n. What we want to prove is that for all $n \geqslant 1$, we have the equality $(123 \dots n)_{10} \cdot 9 + (n+1) = R_{n+1}$. When $n = 1$, we have that $1 \cdot 9 + 2 = R_2$ holds by direct calculation. Now, suppose that the equation $(123 \dots n)_{10} \cdot 9 + (n+1) = R_{n+1}$ holds for some $n \geqslant 1$, then multiplying on both sides by 10 and then adding 1 gives us

$$\begin{aligned}
R_{n+2} &= 10[(123 \dots n)_{10} \cdot 9 + (n+1)] + 1 \\
&= 10 \cdot (123 \dots n)_{10} \cdot 9 + 10(n+1) + 1 \\
&= (123 \dots n0)_{10} \cdot 9 + 9(n+1) + (n+1) + 1 \\
&= ((123 \dots n0)_{10} + (n+1)) \cdot 9 + (n+2) \\
&= (123 \dots n(n+1))_{10} \cdot 9 + (n+2)
\end{aligned}$$

which is exactly the proposition for the case $n+2$. Therefore, by induction, it holds for all $n \geqslant 1$.

22. An old and somewhat illegible invoice shows that 72 canned hams were purchased for \$$x67.9y$. Find the missing digits.

Solution First, notice that the price of 1 canned ham must be an integer k divided by 100 (because a price cannot be more detailed than cents) and so we have the equation in the integers $72k = x679y$. Taking this equation modulo 9 gives us $x + 6 + 7 + 9 + y \equiv 0 \pmod 9$ and so $x + y \equiv 5 \pmod 9$. Moreover, since $8 \mid 72$, then $8 \mid x679y$ and so $8 \mid 79y$ by Problem 15. But notice that the only value of y 0 and 9 that makes $79y$ divisible by 8 is 2 so $y = 2$. Hence, we have $x \equiv 5 - 2 \equiv 3 \pmod 9$ so $x = 3$.

23. If 792 divides the integer $13xy45z$, find the digits x, y, and z. [*Hint:* By Problem 15, $8 \mid 45z$.]

Solution First, take the equation $792k = 13xy45z$ modulo 9 to get $1 + 3 + x + y + 4 + 5 + z \equiv 0 \pmod 9$, which can be simplified into $x + y + z \equiv 5 \pmod 9$. Now, since $8 \mid 792$, then $8 \mid 13xy45z$ which implies that $8 \mid 45z$ by Problem 15. But notice that the only integer z between 0 and 9 that makes $45z$ divisible by 8 is $z = 6$. Hence, the previous congruence becomes $x+y \equiv 8 \pmod 9$. Now, take the equation $792k = 13xy456$ modulo 11 to get $6 - 5 + 4 - y + x - 3 + 1 \equiv 0 \pmod{11}$, which can be simplified into $y \equiv 3 + x \pmod{11}$. Let's now compare the two congruences

$$x + y \equiv 8 \pmod 9 \qquad \text{and} \qquad y \equiv 3 + x \pmod{11}$$

and proceed by cases. If $x = 0$, then $y = 3$ by the second congruence but it would not satisfy the first one. If $x = 1$, then $y = 4$ by the second congruence but it would not satisfy the first one. If $x = 2$, then $y = 5$ by the second congruence but it would not satisfy the first one. If $x = 3$, then $y = 6$ by the second congruence but it would not satisfy the first one. If $x = 4$, then $y = 7$ by the second congruence but it would not satisfy the first one. If $x = 5$, then $y = 8$ by the second congruence but it would not satisfy the first one. If $x = 6$, then $y = 9$ by the second congruence but it would not satisfy the first one. If $x = 7$, then $y \equiv 10 \pmod{11}$ which is impossible since $0 \leqslant y \leqslant 9$. If $x = 8$, then $y = 0$ by the second congruence and the first congruence is also satisfied. If $x = 9$, then $y = 1$ by the second congruence but it would not satisfy the first one. The only case that doesn't lead to a contradiction is when $x = 8$ and $y = 0$. Therefore, the digits are $x = 8$, $y = 0$ and $z = 6$.

4.4 Linear Congruences

1. Solve the following linear congruences:

(a) $25x \equiv 15 \pmod{29}$.

(b) $5x \equiv 2 \pmod{26}$.

(c) $6x \equiv 15 \pmod{21}$.

(d) $36x \equiv 8 \pmod{102}$.

(e) $34x \equiv 60 \pmod{98}$.

(f) $140x \equiv 133 \pmod{301}$. [*Hint:* $\gcd(140, 301) = 7$.]

Solution

(a) Let $d = \gcd(25, 29) = 1$, then by Theorem 4-7, there is a unique solution. Since $7 \cdot 25 - 6 \cdot 29 = 1$, then $7 \cdot 25 \equiv 1 \pmod{29}$. Hence, multiplying the original equation by 7 on both sides gives us $x \equiv 7 \cdot 15 \equiv 105 \equiv 18 \pmod{29}$. Therefore, $x = 18$ is the unique solution.

(b) Let $d = \gcd(5, 26) = 1$, then by Theorem 4-7, there is a unique solution. Since $1 \cdot 26 - 5 \cdot 5 = 1$, then $(-5) \cdot 5 \equiv 1 \pmod{26}$. Hence, multiplying the original equation by -5 on both sides gives us $x \equiv (-5) \cdot 2 \equiv -10 \equiv 16 \pmod{26}$. Therefore, $x = 16$ is the unique solution.

(c) Let $d = \gcd(6, 21) = 3$, then by Theorem 4-7, there are three incongruent solutions since $d \mid 15$. To find a special solution, divide the original congruence by 3 to get the equation $2x \equiv 5 \pmod{7}$ and multiply both sides of the congruence by 4 to get $x \equiv 20 \equiv 6 \pmod{7}$. It follows that the solutions of the original equation are $x = 6 + 7t$ for $t = 0, 1, 2$. Therefore, the solutions are precisely $x = 6, 13, 20$.

(d) Let $d = \gcd(36, 102) = 6$. Since 8 is not divisible by d, then the equation has no solutions.

(e) Let $d = \gcd(34, 98) = 2$, then by Theorem 4-7, there are two incongruent solutions since $d \mid 60$. To find a special solution, divide the original congruence by 2 to get the equation $17x \equiv 30 \pmod{49}$ and multiply both sides of the congruence by 23 to get

$$x \equiv 23 \cdot 30 \equiv 690 \equiv 4 \pmod{49}.$$

It follows that the solutions of the original equation are $x = 4 + 49t$ for $t = 0, 1$. Therefore, the solutions are precisely $x = 4$ and $x = 53$.

(f) Let $d = \gcd(140, 301) = 7$, then by Theorem 4-7, there are seven incongruent solutions since $d \mid 133$. To find a special solution, divide the original congruence by 7 to get the equation $20x \equiv 19 \pmod{43}$ and multiply both sides of the congruence by 15 to get $x \equiv 285 \equiv 27 \pmod{43}$. It follows that the solutions of the original equation are $x = 27 + 43t$ for $t = 0, 1, 2, 3, 4, 5, 6$. Therefore, the solutions are precisely $x = 27, 70, 113, 156, 199, 242, 285$.

2. Using congruences, solve the Diophantine equations below:

(a) $4x + 51y = 9$. [*Hint:* $4x \equiv 9 \pmod{51}$ gives $x = 15 + 51t$, while $51y \equiv 9 \pmod{4}$ gives $y = 3 + 4s$. Find the relation between s and t.]

(b) $12x + 25y = 331$.

(c) $5x - 53y = 17$.

Solution

(a) First, take the equation modulo 51 to get the congruence $4x \equiv 9 \pmod{51}$. Since $4 \cdot 13 - 51 = 1$, then mumtiplying the congruence by 13 on both sides gives us $x \equiv 9 \cdot 13 \equiv 117 \equiv 15 \pmod{51}$. Hence, $x = 15 + 51t$. Similarly, we can take the original equation modulo 4 to get the congruence $3y \equiv 1 \pmod{4}$. Multiplying by 3 on both sides gives $x \equiv 3 \pmod{4}$. Thus, $y = 3 + 4s$. Plugging $x = 15 + 51t$ and $y = 3 + 4s$ in the original equation gives us

$$4(15 + 51t) + 51(3 + 4s) = 9$$

which can be simplified into $t + s = -1$ and so $s = -1 - t$. Hence, we have $x = 15 + 51t$ and $s = -1 - 4t$ for an integer t. Let's now prove that any pair of integers of this form is a solution of the equation:

$$4(15 + 51t) + 51(-1 - 4t) = 4 \cdot 15 - 51 = 9$$

for every integer t. Therefore, the solutions are precisely $x = 15 + 51t$ and $y = -1 - 4t$ for all integers t.

(b) First, take the equation modulo 25 to get the congruence $12x \equiv 6 \pmod{25}$. Since $25 - 2 \cdot 12 = 1$, then mumtiplying the congruence by -2 on both sides gives us $x \equiv (-2) \cdot 6 \equiv 13 \pmod{25}$. Hence, $x = 13 + 25t$. Similarly, we can take the original equation modulo 12 to get the congruence $y \equiv 7 \pmod{12}$. Thus, $y = 7 + 12s$. Plugging $x = 13 + 25t$ and $y = 7 + 12s$ in the original equation gives us

$$12(13 + 25t) + 25(7 + 12s) = 331$$

which can be simplified into $t + s = 0$ and so $s = -t$. Hence, we have $x = 13 + 25t$ and $s = 7 - 12t$ for an integer t. Let's now prove that any pair of integers of this form is a solution of the equation:

$$12(13 + 25t) + 25(7 - 12t) = 12 \cdot 13 + 25 \cdot 7 = 331$$

for every integer t. Therefore, the solutions are precisely $x = 13 + 25t$ and $y = 7 - 12t$ for all integers t.

(c) First, take the equation modulo 53 to get the congruence $5x \equiv 17 \pmod{53}$. Since $2 \cdot 53 - 21 \cdot 5 = 1$, then multiplying the congruence by -21 on both sides gives us $x \equiv (-21) \cdot 17 \equiv -39 \equiv 14 \pmod{53}$. Hence, $x = 14 + 53t$. Similarly, we can take the original equation modulo 5 to get the congruence $2y \equiv 2 \pmod{5}$. Multiplying by 3 on both sides gives $x \equiv 1 \pmod{5}$. Thus, $y = 1 + 5s$. Plugging $x = 14 + 53t$ and $y = 1 + 5s$ in the original equation gives us

$$5(14 + 53t) - 53(1 + 5s) = 17$$

which can be simplified into $t - s = 0$ and so $s = t$. Hence, we have $x = 14 + 53t$ and $s = 1 + 5t$ for an integer t. Let's now prove that any pair of integers of this form is a solution of the equation:

$$5(14 + 53t) - 53(1 + 5t) = 5 \cdot 14 - 53 = 17$$

for every integer t. Therefore, the solutions are precisely $x = 14 + 53t$ and $y = 1 + 5t$ for all integers t.

3. Find all solutions of the linear congruence $3x - 7y \equiv 11 \pmod{13}$.

Solution First, fix $y = t$ an rearrange the equation into $3x \equiv 11 + 7t \pmod{13}$. Since $\gcd(3, 13) = 1$, then this equation has precisely one solution. To find it, multiply both sides of the congruence by 9 to get $x \equiv 9(11 + 7t) \pmod{13}$. Hence, we have that the solutions are $x = 9(11 + 7t)$, $y = t$ for all t between 0 and 12.

4. Solve each of the following sets of simultaneous congruences:

(a) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$

(b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$

(c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

(d) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$

Solution

(a) Let $n = 3 \cdot 5 \cdot 7 = 105$, $N_1 = n/3 = 35$, $N_2 = n/5 = 21$ and $N_3 = n/7 = 15$. Consider the linear congruences

$$35x \equiv 1 \pmod{3}, \qquad 21x \equiv 1 \pmod{5}, \qquad 15x \equiv 1 \pmod{7}$$

which have the respective solutions $x_1 = 2$, $x_2 = 1$ and $x_3 = 1$. Define the integer $\overline{x} = 52 \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \pmod{n}$. By Theorem 4-8, we have that general solution is given by $x = 52 + 105t$ where t is any integer.

(b) Let $n = 11 \cdot 29 \cdot 31 = 9889$, $N_1 = n/11 = 899$, $N_2 = n/29 = 341$ and $N_3 = n/31 = 319$. Consider the linear congruences

$$899x \equiv 1 \pmod{11}, \qquad 341x \equiv 1 \pmod{29}, \qquad 319x \equiv 1 \pmod{31}$$

which have the respective solutions $x_1 = 7$, $x_2 = 4$ and $x_3 = 7$. Define the integer $\overline{x} = 4944 \equiv 5 \cdot 899 \cdot 7 + 14 \cdot 341 \cdot 4 + 15 \cdot 319 \cdot 7 \pmod{n}$. By Theorem 4-8, we have that general solution is given by $x = 4944 + 9889t$ where t is any integer.

(c) Let $n = 6 \cdot 11 \cdot 17 = 1122$, $N_1 = n/6 = 187$, $N_2 = n/11 = 102$ and $N_3 = n/17 = 66$. Consider the linear congruences

$$187x \equiv 1 \pmod{6}, \qquad 102x \equiv 1 \pmod{11}, \qquad 66x \equiv 1 \pmod{17}$$

which have the respective solutions $x_1 = 1$, $x_2 = 4$ and $x_3 = 8$. Define the integer $\overline{x} = 785 \equiv 5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot 4 + 3 \cdot 66 \cdot 8 \pmod{n}$. By Theorem 4-8, we have that general solution is given by $x = 785 + 1122t$ where t is any integer.

(d) First, let's rewrite and simplify each individual congruences. The congruence $2x \equiv 1 \pmod{5}$ is equivalent to $x \equiv 3 \pmod{5}$ by multiplying by 3 on both sides. Let's solve the congruence $3x \equiv 9 \pmod{6}$ using the methods that we developed in this section. If we let $d = \gcd(3,6) = 3$, then we have that $d \mid 9$ which implies that the congruence has 3 solutions modulo 6. To find these solutions, divide the congruence by d to get the congruence $x \equiv 1 \pmod{2}$. It follows that the solutions are $1, 3, 5$ which correspond precisely to the odd integers. Therefore, the congruence $3x \equiv 9 \pmod{6}$ is precisely equivalent to the congruence $x \equiv 1 \pmod{2}$. Next, multiplying on both sides of the congruence $4x \equiv 1 \pmod{7}$ by 2 shows that it is equivalent to the congruence $x \equiv 2 \pmod{7}$. Finally, multiplying on both sides of the congruence $5x \equiv 9 \pmod{11}$ by 9 shows that it is equivalent to the congruence $x \equiv 4 \pmod{11}$. Therefore, the system becomes

$$x \equiv 3 \pmod{5}, \quad x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Let $n = 5 \cdot 2 \cdot 7 \cdot 11 = 770$, $N_1 = n/5 = 154$, $N_2 = n/2 = 385$, $N_3 = n/7 = 110$ and $N_4 = n/11 = 70$. Consider the linear congruences

$$\begin{aligned} 154x &\equiv 1 \pmod{5}, & 385x &\equiv 1 \pmod{2}, \\ 110x &\equiv 1 \pmod{7}, & 70x &\equiv 1 \pmod{11}, \end{aligned}$$

which have the respective solutions $x_1 = 4$, $x_2 = 1$, $x_3 = 3$ and $x_4 = 3$. Define the integer $\overline{x} = 653 \equiv 3 \cdot 154 \cdot 4 + 1 \cdot 385 \cdot 1 + 2 \cdot 110 \cdot 3 + 4 \cdot 70 \cdot 3 \pmod{n}$. By Theorem 4-8, we have that general solution is given by $x = 653 + 770t$ where t is any integer.

5. Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ by solving the system

$$17x \equiv 3 \pmod{2}, \; 17x \equiv 3 \pmod{3}, \; 17x \equiv 3 \pmod{5}, \; 17x \equiv 3 \pmod{7}.$$

Solution First, let's solve the system of equation. Let's rewrite it as follows:

$$x \equiv 1 \pmod{2}, \quad 2x \equiv 0 \pmod{3}, \quad 2x \equiv 3 \pmod{5}, \quad 3x \equiv 3 \pmod{7}.$$

Next, multiply both sides of the second congruence by 2, multiply both sides of the third congruence by 3 and cancel out the 3's in the last congruence to obtain the system

$$x \equiv 1 \pmod{2}, \quad x \equiv 0 \pmod{3}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 1 \pmod{7}.$$

Let's solve this system using the method developed before. Let $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, $N_1 = n/2 = 105$, $N_2 = n/3 = 70$, $N_3 = n/5 = 42$ and $N_4 = n/7 = 30$. Let's now solve the congruences $N_i x_i = 1 \pmod{n_i}$ where $n_1 = 2$, $n_2 = 3$, $n_3 = 5$ and $n_4 = 7$. We get that $x_1 = 1$, $x_2 = 1$, $x_3 = 3$ and $x_4 = 4$. Now, we can define

$$\overline{x} = 99 \equiv 1 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 + 4 \cdot 42 \cdot 3 + 1 \cdot 30 \cdot 4.$$

By Theorem 4-8, we have that 99 solves the original system of equation. In other words, we have that 2, 3, 5 and 7 divide the quantity $17 \cdot 99 - 3$. Since they are relatively prime, we get that their product also divides this quantity. Therefore, we have that $17 \cdot 99 \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ and so $x = 99$ is the unique solution modulo $2 \cdot 3 \cdot 5 \cdot 7$.

6. Find the smallest integer $a > 2$ such that

$$2 \mid a,\ 3 \mid a+1,\ 4 \mid a+2,\ 5 \mid a+3,\ 6 \mid a+4.$$

Solution First, notice that we can discard the condition that $2 \mid a$ since $4 \mid a+2$ already implies it. Moreover, we rewrite each of these conditions as the following congruences:

$$a \equiv 2 \pmod 3, \quad a \equiv 2 \pmod 4, \quad a \equiv 2 \pmod 5, \quad a \equiv 2 \pmod 6.$$

If we focus on the first three congruences, then by Theorem 4-8, we have that there is a unique solution modulo $3 \cdot 4 \cdot 5 = 60$. Since 2 is clearly a solution, then now have to solve the congruence $a \equiv 2 \pmod 6$ such that $a = 2 + 60t > 2$. When $t = 1$, we have that $a = 62$ satisfies $a \equiv 2 \pmod 6$. Thus, $a = 62$ is indeed the smallest integer $a > 2$ such that the divisibility conditions are satisfied.

7.

(a) Obtain three consecutive integers each having a square factor. [*Hint:* Find an integer a such that $2^2 \mid a$, $3^2 \mid a+1$, $5^2 \mid a+2$.]

(b) Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

Solution

(a) Let's find an integer a such that $2^2 \mid a$, $3^2 \mid a+1$ and $5^2 \mid a+2$. Equivalently, let's solve the system

$$a \equiv 0 \pmod{2^2}, \qquad a \equiv -1 \pmod{3^2}, \qquad a \equiv -2 \pmod{5^2}$$

by applying the method developed in this section. Let $n = 2^2 \cdot 3^2 \cdot 5^2 = 900$, $N_1 = n/2^2 = 225$, $N_2 = n/3^2 = 100$ and $N_3 = n/5^2 = 36$. Next, notice that $x_2 = 1$ and $x_3 = 16$ satisfy the equations $N_2 x_2 \equiv 1 \pmod{3^2}$ and $N_3 x_3 \equiv 1 \pmod{5^2}$ so we can define the integer

$$\overline{x} = 548 \equiv 0 + (-1) \cdot 100 \cdot 1 + (-2) \cdot 36 \cdot 16 \pmod{900}.$$

It follows that the three consecutive integers 548, 549, 550 are respectively divisible by 2^2, 3^2 and 5^2.

(b) Let's find an integer a such that $5^2 \mid a$, $3^3 \mid a+1$ and $2^4 \mid a+2$. Equivalently, let's solve the system

$$a \equiv 0 \pmod{5^2}, \qquad a \equiv -1 \pmod{3^3}, \qquad a \equiv -2 \pmod{2^4}$$

by applying the method developed in this section. Let $n = 5^2 \cdot 3^3 \cdot 2^4 = 10800$, $N_1 = n/5^2 = 432$, $N_2 = n/3^3 = 400$ and $N_3 = n/2^4 = 675$. Next, notice that

$x_2 = 16$ and $x_3 = 11$ satisfy the equations $N_2x_2 \equiv 1 \pmod{3^3}$ and $N_3x_3 \equiv 1 \pmod{2^4}$ so we can define the integer

$$\overline{x} = 350 \equiv 0 + (-1) \cdot 400 \cdot 16 + (-2) \cdot 675 \cdot 11 \pmod{10800}.$$

It follows that the three consecutive integers 350, 351, 352 are respectively divisible by 5^2, 3^3 and 2^4.

8. (Brahmagupta, 7th century A.D.) When eggs in a basket are removed 2,3,4,5,6 at a time there remain respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

Solution First, let's rewrite this problem as a system of congruence. Let x be the number of eggs in the basket, then the first part of the problem states that $x \equiv -1 \pmod{i}$ for all $i = 2, 3, 4, 5, 6$. The second part states that $x \equiv 0 \pmod{7}$. Hence, we have the system

$$x \equiv -1 \pmod{2}, \qquad x \equiv -1 \pmod{3}, \qquad x \equiv -1 \pmod{4},$$

$$x \equiv -1 \pmod{5}, \qquad x \equiv -1 \pmod{6}, \qquad x \equiv 0 \pmod{7}.$$

Notice that the congruences $x \equiv -1 \pmod{2}$ and $x \equiv -1 \pmod{3}$ are equivalent to the fact that 2 and 3 divide $x + 1$. Since they are relatively prime, then $6 \mid x + 1$ and so we get that the congruence $x \equiv -1 \pmod{6}$ is already implied by the others. Hence, we can remove it from the system since it is redundant. Next, from the congruence $x \equiv -1 \pmod{4}$, we directly get that $x \equiv -1 \pmod{2}$ and so this latter congruence can also be removed from the system. Hence, our system is now

$$\begin{aligned} x &\equiv -1 \pmod{3}, & x &\equiv -1 \pmod{4}, \\ x &\equiv -1 \pmod{5}, & x &\equiv 0 \pmod{7}. \end{aligned}$$

Now, notice that 3, 4, and 5 are relatively prime and so by the method we developed in this section, there is a unique solution modulo $3 \cdot 4 \cdot 5 = 60$. Since -1 is clearly a solution, then the previous system is equivalent to

$$x \equiv -1 \pmod{60}, \qquad x \equiv 0 \pmod{7}.$$

Using the first congruence, we get that x must be one of the numbers 59, 119, 179, ... which are of the form $60t - 1$. By looking at these numbers, we see that 59 is not divisible by 7 but 119 is. Therefore, the smallest number of eggs that could have been contained in the basket is 119.

9. The basket-of-eggs problem problem is often phrased in the following form: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, or 6 at a time; but, no eggs remain if they are removed 7 at a time. Find the smallest number of eggs that could have been in the basket.

Solution The solution to this problem will be very similar to the solution to the previous one. First, let's rewrite this problem as a system of congruence. Let x

be the number of eggs in the basket, then the first part of the problem states that $x \equiv 1 \pmod{i}$ for all $i = 2, 3, 4, 5, 6$. The second part states that $x \equiv 0 \pmod{7}$. Hence, we have the system

$$x \equiv 1 \pmod{2}, \qquad x \equiv 1 \pmod{3}, \qquad x \equiv 1 \pmod{4},$$
$$x \equiv 1 \pmod{5}, \qquad x \equiv 1 \pmod{6}, \qquad x \equiv 0 \pmod{7}.$$

Notice that the congruences $x \equiv 1 \pmod{2}$ and $x \equiv 1 \pmod{3}$ are equivalent to the fact that 2 and 3 divide $x - 1$. Since they are relatively prime, then $6 \mid x - 1$ and so we get that the congruence $x \equiv 1 \pmod{6}$ is already implied by the others. Hence, we can remove it from the system since it is redundant. Next, from the congruence $x \equiv 1 \pmod{4}$, we directly get that $x \equiv 1 \pmod{2}$ and so this latter congruence can also be removed from the system. Hence, our system is now

$$\begin{aligned} x &\equiv 1 \pmod{3}, & x &\equiv 1 \pmod{4}, \\ x &\equiv 1 \pmod{5}, & x &\equiv 0 \pmod{7}. \end{aligned}$$

Now, notice that 3, 4, and 5 are relatively prime and so by the method we developed in this section, there is a unique solution modulo $3 \cdot 4 \cdot 5 = 60$. Since 1 is clearly a solution, then the previous system is equivalent to

$$x \equiv 1 \pmod{60}, \qquad x \equiv 0 \pmod{7}.$$

Using the first congruence, we get that x must be one of the numbers 61, 121, 181, 241 ...which are of the form $60t + 1$. By looking at these numbers, we see that 61, 121 and 181 are not divisible by 7 but $241 = 7 \cdot 33$ is. Therefore, the smallest number of eggs that could have been contained in the basket is 241.

10. (Ancient Chinese Problem.) A band of 17 pirates 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 wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen.

Solution First, let's translate this problem into a system of congruences. If we denote by x the number of stolen coins, we get the following system:

$$x \equiv 3 \pmod{17}, \qquad x \equiv 10 \pmod{16}, \qquad x \equiv 0 \pmod{15}.$$

Since 17, 16 and 15 are relatively prime, then we can directly apply the method developed in this section. Let $a_1 = 3$, $a_2 = 10$, $a_3 = 0$, $n_1 = 17$, $n_2 = 16$, $n_3 = 15$, $n = n_1 n_2 n_3 = 4080$, $N_1 = n/n_1 = 240$, $N_2 = n/n_2 = 255$ and $N_3 = n/n_3 = 272$. Let's now solve the congruences $N_i x_i \equiv 1 \pmod{n_i}$ to obtain $x_1 = 9$ and $x_2 = -1$. Now, define

$$\begin{aligned} \overline{x} &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \\ &= 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot (-1) + 0 \\ &= 6480 - 2550 \\ &= 3930, \end{aligned}$$

then by Theorem 4-8, $\overline{x}$ is the unique solution to this system modulo 4080. Since 3930 is the least positive integer of the form $\overline{x}+4080t$, then 3930 is the least number of coins that could have been stolen.

11. Prove that the congruences

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

admit a simultaneous solution if and only if $\gcd(n,m) \mid a-b$; if a solution exists, confirm that it is unique modulo $\operatorname{lcm}(n,m)$.

Solution First, suppose that a solution x exists, then $x = a + kn$ and $x = b + k'm$ for some integers k and k'. It follows that $a + kn = b + k'm$ and so $a - b = -kn + k'm$. Since $\gcd(n,m) \mid -kn + k'm$, then $\gcd(n,m) \mid a-b$. Conversely, if $xn + ym = \gcd(n,m) \mid a-b$, then $a - b = kxn + kym$ for some integer k. If we let $x = a - kxn = b + kym$, then it is clear that $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$. This proves the equivalence.

Suppose now that we have two solutions x and x', then $x \equiv x' \pmod{a}$ and $x \equiv x' \pmod{m}$. Equivalently, we have that n and m divide $x - x'$ and so $\operatorname{lcm}(n,m) \mid x - x'$. Therefore, $x \equiv x' \pmod{\operatorname{lcm}(n,m)}$ which implies that it is unique modulo $\operatorname{lcm}(n,m)$.

12. Use Problem 11 to show that the system

$$x \equiv 5 \pmod{6} \text{ and } x \equiv 7 \pmod{15}$$

does not possess a solution.

Solution Since $\gcd(6,15) = 3$ does not divide $5 - 7 = -2$, then by Problem 11, there is no simultaneous solution to this system of congruences.

13. If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

Solution We have that $x = a+kn$ for some integer k and by the Division Algorithm, we also have that $x = b + 2k'n$ for some integer k'. It follows that $a + kn = b + 2k'n$ and so $b = a + n(k-2k') = a + nk_0$. If we take this equation modulo $2n$, we get that nk_0 is either congruent to 0 or n modulo $2n$ and so $b \equiv a \pmod{2n}$ or $b \equiv a + n \pmod{2n}$. It follows that $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

14. A certain integer between 1 and 1200 leaves the remainders 1, 2, 6 when divided by 9, 11, 13 respectively. What is the integer?

Solution If we translate this problem into a system of congruences, we get that the number, which we will call x, must satisfy

$$x \equiv 1 \pmod{9}, \qquad x \equiv 2 \pmod{11}, \qquad x \equiv 6 \pmod{13}.$$

Since 9, 11, and 13 are all relatively prime, then we can apply Theorem 4-8. Let $n = 9\cdot 11\cdot 13 = 1287$, $N_1 = 11\cdot 13 = 143$, $N_2 = 9\cdot 13 = 117$ and $N_3 = 9\cdot 11 = 99$. Let x_i denote the inverse of N_i modulo 9, 11, and 13 successively, then $x_1 = 8$, $x_2 = -3$

and $x_3 = 5$. Hence, we can define $\overline{x} = 838 \equiv 1 \cdot N_1x_1 + 2 \cdot N_2x_2 + 6 \cdot N_3x_3 \pmod{n}$. By Theorem 4-8, the solutions to the system are precisely $838 + 1287t$ where t is an integer. Since we want $1 \leqslant x \leqslant 1200$, then 838 is the integer we want.

15.

(a) Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12, respectively. (Yih-hing, died 717.)

(b) Find an integer having the remainders 2, 3, 4, 5 when divided by 3, 4, 5, 6, respectively. (Bhaskara, born 1114.)

(c) Find an integer having the remainders 3, 11, 15 when divided by 10, 13, 17, respectively. (Regiomontanus, 1436-1473)

Solution

(a) It suffices to find a simultaneous solution to the congruences

$$\begin{aligned} x &\equiv 1 \pmod{2} \qquad & x &\equiv 2 \pmod{3} \\ x &\equiv 5 \pmod{6} \qquad & x &\equiv 5 \pmod{12} \end{aligned}$$

First, notice that the first two congruences can be rewritten as

$$x \equiv -1 \pmod{2} \qquad x \equiv -1 \pmod{3}.$$

Since 2 and 3 are relatively prime, then applying Theorem 4-8 tells us that there is a unique solution modulo 6. Since -1 is clearly a solution, then these two equations are equivalent to the equation $x \equiv -1 \equiv 5 \pmod{6}$ which was already in our system. Thus, we only need to find a simultaneous solution to the equations

$$x \equiv 5 \pmod{6} \qquad x \equiv 5 \pmod{12}.$$

But now, notice that the second equation implies the first one so the only thing we need to do is to find an integer x such that its residue modulo 12 is 5. If we take $x = 5$, then it clearly satisfies all the conditions.

(b) It suffices to find a simultaneous solution to the congruences

$$\begin{aligned} x &\equiv -1 \pmod{3} \qquad & x &\equiv -1 \pmod{4} \\ x &\equiv -1 \pmod{5} \qquad & x &\equiv -1 \pmod{6}. \end{aligned}$$

From the first and second congruences, we have that both 3 and 4 divide $x+1$ and so 12 divide $x+1$ as well ($\gcd(3,4) = 1$). This clearly implies that $6 \mid x+1$ and hence, $x \equiv -1 \pmod{6}$. It follows that we don't need to consider the last congruence, and so we need to solve the following system:

$$x \equiv -1 \pmod{3}, \qquad x \equiv -1 \pmod{4}, \qquad x \equiv -1 \pmod{5}.$$

Since 3, 4 and 5 are relatively prime, then Theorem 4-8 tells us that there is a unique solution modulo $3 \cdot 4 \cdot 5 = 60$. Since -1 is clearly a solution, then we have that $60t - 1$ represents all possible solutions. Thus, we can take $x = 59$.

(c) We need to solve the following system of congruences:

$$x \equiv 3 \pmod{10}, \qquad x \equiv 11 \pmod{13}, \qquad x \equiv 15 \pmod{17}.$$

Since 10, 13 and 17 are relatively prime, then we can directly apply the method of Theorem 4-8. Let $n = 10{\cdot}13{\cdot}17 = 2210$, $N_1 = n/10 = 221$, $N_2 = n/13 = 170$ and $N_3 = n/17 = 130$. After solving the equations $N_i x_i \equiv 1 \pmod{n_i}$, we get that $x_1 = 1$, $x_2 = 1$ and $x_3 = -3$. From this, we can define the integer $\overline{x} = 1103 \equiv 3 \cdot 221 \cdot 1 + 11 \cdot 170 \cdot 1 + 15 \cdot 130 \cdot (-3) \pmod{n}$. Indeed, we can check that 1103 checks all the conditions.

16. Let t_n denote the nth triangular number. For which values of n does t_n divide $t_1^2 + t_2^2 + \cdots + t_n^2$? [*Hint:* Since $t_1^2 + t_2^2 + \cdots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$, it suffices to determine those n satisfying $3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \cdot 3 \cdot 5}$.]

Solution As the hint tells us, lets find the n's satisfying $3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \cdot 3 \cdot 5}$. By the Chinese Remainder Theorem, it suffices to solve the following system of congruences:

$$\begin{aligned} n^3 + n &\equiv 0 \pmod{2} \\ n + 2 &\equiv 0 \pmod{3} \\ (3n+2)(n^2+1) &\equiv 0 \pmod{5} \end{aligned}$$

which we obtain after simplifications. First, notice that $n^3 + n$ is always even so the first equation can be discarded. The second equation can be replaced by $n \equiv 1 \pmod{3}$ using the rules of congruences. The last equation tells us that 5 divides one of $3n + 2$ or $n^2 + 1$. For the first term, this happens when $n \equiv 1 \pmod{5}$. For the second term, this happens when $n \equiv 2, 3 \pmod{5}$. Thus, the last congruence is equivalent to $n \equiv 1, 2, 3 \pmod{5}$. Hence, our system now becomes

$$\begin{aligned} n &\equiv 1 \pmod{3} \\ n &\equiv 1, 2, 3 \pmod{5} \end{aligned}$$

To solve it, let's solve separatly the three systems where the last equation is $n \equiv 1 \pmod{5}$, $n \equiv 2 \pmod{5}$ and $n \equiv 3 \pmod{5}$ successively. This is not harder than solving just one system because most of the method remains unchanged. Let's apply the method of Theorem 4-8. Let $n = 3 \cdot 5 = 15$, $N_1 = n/3 = 5$, $N_2 = n/5 = 3$. After solving the congruences $N_i x_i \equiv 1 \pmod{n_i}$, we get $x_1 = x_2 = 2$. Hence, the solutions of the system are

$$1 \cdot 5 \cdot 2 + i \cdot 3 \cdot 2 = 10 + 6i$$

up to a multiple of 15 and for $i = 1, 2, 3$. It follows that the solutions are precisely $n \equiv 1, 7, 13 \pmod{15}$.

17. Find the solutions of the system of congruences

$$\begin{aligned} 3x + 4y &\equiv 5 \pmod{13} \\ 2x + 5y &\equiv 7 \pmod{13}. \end{aligned}$$

Solution First, notice that $9 \cdot 3 \equiv 1 \pmod{13}$ and $7 \cdot 2 \equiv 1 \pmod{13}$ so if we multiply both sides of equations 1 and 2 by 9 and 7 respectively, we get the two equations

$$\begin{aligned} x + 10y &\equiv 6 \pmod{13} \\ x + 9y &\equiv 10 \pmod{13}. \end{aligned}$$

If we subtract the first equation by the second one, we get that $y \equiv 9 \pmod{13}$. If we plug this last congruence into the second congruence above, we get that

$$x \equiv 10 - 9 \cdot 9 \equiv 10 - 3 \equiv 7 \pmod{13}.$$

Therefore, the solutions are given by $x \equiv 7 \pmod{13}$, $y \equiv 9 \pmod{13}$.

18. Obtain the two incongruent solutions modulo 210 of the system

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 4x &\equiv 2 \pmod{6} \\ 3x &\equiv 2 \pmod{7}. \end{aligned}$$

Solution By multipliying the first equation by 3, we obtain the equivalent equation $x \equiv 4 \pmod{5}$. Let's solve the second equation. If we divide the congruence by 2, we get the equation $2x \equiv 1 \pmod{3}$ which is equivalent to $x \equiv 2 \pmod{3}$. If we lift this solution modulo 6, we get that the two solutions of the second equation are $x \equiv 2, 5 \pmod{6}$. In the third equation, multiply both sides by 5 to get $x \equiv 3$ (mod 7). Therefore, our system is now

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 2, 5 \pmod{6} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

To solve this system, we need to solve the two independent systems where the second equation changes and merge the solutions. To do this, let's apply Theorem 4-8. Let $n = 5 \cdot 6 \cdot 7 = 210$, $N_1 = n/5 = 42$, $N_2 = n/6 = 35$ and $N_3 = n/7 = 30$. By solving the equations $N_i x_i \equiv 1 \pmod{n_i}$, we get $x_1 = 3$, $x_2 = -1$, $x_3 = 4$. Hence, if we compute

$$4 \cdot 42 \cdot 3 + i \cdot 35(-1) + 3 \cdot 30 \cdot 4 = 864 - 35i \equiv 234 - 35i \pmod{210}$$

and replace i by 2 and 5, we get that the two incongruent solutions modulo 210 are 59 and 164.

Chapter 5

Fermat's Theorem

5.1 Pierre De Fermat

There are no exercises in this section.

5.2 Fermat's Factorization Method

1. Use Fermat's method to factor

(a) 2279;

(b) 10541;

(c) 340663. [*Hint:* The smallest square just exceeding 340663 is 584^2.]

Solution

(a) The smallest square greater than 2279 is $48^2 = 2304$. Thus, we get

$$48^2 - 2279 = 2304 - 2279 = 25 = 5^2$$

which gives us the factorization

$$2279 = 48^2 - 5^2 = (48 - 5)(48 + 5) = 43 \cdot 53.$$

(b) The smallest square greater than 10541 is $103^2 = 10609$. Thus, we get

$$\begin{aligned} 103^2 - 10541 &= 10609 - 10541 = 68, \\ 104^2 - 10541 &= 10816 - 10541 = 275, \\ 105^2 - 10541 &= 11025 - 10541 = 484 = 22^2 \end{aligned}$$

which gives us the factorization

$$10541 = 105^2 - 22^2 = (105 - 22)(105 + 22) = 83 \cdot 127.$$

(c) The smallest square greater than 340663 is $584^2 = 341056$. Thus, we get

$$\begin{aligned}
584^2 - 340663 &= 341056 - 340663 = 393,\\
585^2 - 340663 &= 342225 - 340663 = 1562,\\
586^2 - 340663 &= 343396 - 340663 = 2733,\\
587^2 - 340663 &= 344569 - 340663 = 3906,\\
588^2 - 340663 &= 345744 - 340663 = 5081,\\
589^2 - 340663 &= 346921 - 340663 = 6258,\\
590^2 - 340663 &= 348100 - 340663 = 7437,\\
591^2 - 340663 &= 349281 - 340663 = 8618,\\
592^2 - 340663 &= 350464 - 340663 = 9801 = 99^2
\end{aligned}$$

which gives us the factorization

$$340663 = 592^2 - 99^2 = (592 - 99)(592 + 99) = 493 \cdot 691.$$

2. Prove that a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96. [*Hint:* Since $x^2 \equiv (50+x)^2 \pmod{100}$ and $x^2 \equiv (50-x)^2 \pmod{100}$, it suffices to examine the final digits of x^2 for the 26 values $x = 0, 1, 2, ..., 25$.]

Solution As the hint tells us, since $x^2 \equiv (50+x)^2 \pmod{100}$ and $x^2 \equiv (50-x)^2 \pmod{100}$, it suffices to examine the final digits of x^2 for the 26 values $x = 0, 1, 2, ..., 25$:

$$\begin{aligned}
0^2 &= 0 \equiv 00 \pmod{100} & 13^2 &= 169 \equiv 69 \pmod{100}\\
1^2 &= 1 \equiv 01 \pmod{100} & 14^2 &= 196 \equiv 96 \pmod{100}\\
2^2 &= 4 \equiv 04 \pmod{100} & 15^2 &= 225 \equiv 25 \pmod{100}\\
3^2 &= 9 \equiv 09 \pmod{100} & 16^2 &= 256 \equiv 56 \pmod{100}\\
4^2 &= 16 \equiv 16 \pmod{100} & 17^2 &= 289 \equiv 89 \pmod{100}\\
5^2 &= 25 \equiv 25 \pmod{100} & 18^2 &= 324 \equiv 24 \pmod{100}\\
6^2 &= 36 \equiv 36 \pmod{100} & 19^2 &= 361 \equiv 61 \pmod{100}\\
7^2 &= 49 \equiv 49 \pmod{100} & 20^2 &= 400 \equiv 00 \pmod{100}\\
8^2 &= 64 \equiv 64 \pmod{100} & 21^2 &= 441 \equiv 41 \pmod{100}\\
9^2 &= 81 \equiv 81 \pmod{100} & 22^2 &= 484 \equiv 84 \pmod{100}\\
10^2 &= 100 \equiv 00 \pmod{100} & 23^2 &= 529 \equiv 29 \pmod{100}\\
11^2 &= 121 \equiv 21 \pmod{100} & 24^2 &= 576 \equiv 76 \pmod{100}\\
12^2 &= 144 \equiv 44 \pmod{100} & 25^2 &= 625 \equiv 25 \pmod{100}.
\end{aligned}$$

Therefore, a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.

3. Factor the number $2^{11} - 1$ by Fermat's factorization method.

Solution We have $2^{11} - 1 = 2048 - 1 = 2047$. The smallest square greater than 2047 is $46^2 = 2116$, thus

$$\begin{aligned}
46^2 - 2047 &= 2116 - 2047 = 69,\\
47^2 - 2047 &= 2209 - 2047 = 162,\\
48^2 - 2047 &= 2304 - 2047 = 257,\\
49^2 - 2047 &= 2401 - 2047 = 354,\\
50^2 - 2047 &= 2500 - 2047 = 453,\\
51^2 - 2047 &= 2601 - 2047 = 554,\\
52^2 - 2047 &= 2704 - 2047 = 657,\\
53^2 - 2047 &= 2809 - 2047 = 762,\\
54^2 - 2047 &= 2916 - 2047 = 869,\\
55^2 - 2047 &= 3025 - 2047 = 978,\\
56^2 - 2047 &= 3136 - 2047 = 1089 = 33^2.
\end{aligned}$$

Hence, we get the following factorization:

$$2^{11} - 1 = 56^2 - 33^2 = (56 - 33)(56 + 33) = 23 \cdot 89.$$

4. In 1647, Mersenne noted that when a number can be written as a sum of two relatively prime squares in two distinct ways, it is composite and can be factored as follows: if $n = a^2 + b^2 = c^2 + d^2$, then

$$n = (ac + bd)(ac - bd)/(a + d)(a - d).$$

Use this result to factor the numbers

$$\begin{aligned}
493 &= 18^2 + 13^2 = 22^2 + 3^2,\\
38025 &= 168^2 + 99^2 = 156^2 + 117^2.
\end{aligned}$$

Solution For the first equation, we can take $a = 18$, $b = 13$, $c = 22$ and $d = 3$:

$$493 = \frac{(18 \cdot 22 + 13 \cdot 3)(18 \cdot 22 - 13 \cdot 3)}{(18 + 3)(18 - 3)} = \frac{357 \cdot 435}{21 \cdot 15} = \frac{357}{21} \cdot \frac{435}{15} = 17 \cdot 29.$$

For the first equation, we can take $a = 168$, $b = 99$, $c = 117$ and $d = 156$:

$$\begin{aligned}
38025 &= \frac{(168 \cdot 117 + 99 \cdot 156)(168 \cdot 117 - 99 \cdot 156)}{(168 + 156)(168 - 156)}\\
&= \frac{35100 \cdot 4212}{324 \cdot 12}\\
&= \frac{35100}{12} \cdot \frac{4212}{324}\\
&= 2925 \cdot 13.
\end{aligned}$$

5.3 The Little Theorem

1. Verify that $18^6 \equiv 1 \pmod{7^k}$ for $k = 1, 2, 3$.

Solution When $k = 1$, the congruence $18^6 \equiv 1 \pmod{7^k}$ follows from the little theorem. When $k = 2$, we have

$$18^6 = (18^2)^3 \equiv 30^3 = 900 \cdot 30 \equiv 18 \cdot 30 = 540 \equiv 1 \pmod{7^k}.$$

Finally, when $k = 3$, we have

$$18^6 = (18^2)^3 = 324^3 \equiv (-19)^3 = -361 \cdot 19 \equiv -18 \cdot 19 = -342 \equiv 1 \pmod{7^k}.$$

2.

(a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$. [*Hint:* From Fermat's Theorem $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$.]

(b) If $\gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.

(c) If $\gcd(a, 133) = \gcd(b, 133) = 1$, show that $133 \mid a^{18} - b^{18}$.

Solution

(a) First, since $\gcd(a, 35) = 1$, then $\gcd(a, 5) = \gcd(a, 7) = 1$. Hence, from the little theorem, we have the congruences $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$. Squaring both sides of the first congruence and cubing both sides of the second congruence gives us the two congruences $a^{12} \equiv 1 \pmod 7$ and $a^{12} \equiv 1 \pmod 5$. Since 5 and 7 are relatively prime, then we get that $a^{12} \equiv 1 \pmod{35}$.

(b) First, since $\gcd(a, 42) = 1$, then $\gcd(a, 3) = \gcd(a, 7) = \gcd(a, 2) = 1$. From the fact that $\gcd(a, 3) = \gcd(a, 7) = 1$, and by the little theorem, we get the congruences $a^2 \equiv 1 \pmod 3$ and $a^6 \equiv 1 \pmod 7$. If we cube the first of these congruences, we get $a^6 \equiv 1 \pmod 3$. Hence, we have that both 3 and 7 divide $a^6 - 1$. Now, the equation $\gcd(a, 2) = 1$ asserts that a is odd, it follows that $a \equiv \pm 1, \pm 3 \pmod 8$. When $a \equiv \pm 1 \pmod 8$, then $a^6 \equiv ((\pm 1)^2)^3 \equiv 1 \pmod 8$. When $a \equiv \pm 3 \pmod 8$, then $a^6 \equiv ((\pm 3)^2)^3 \equiv 1 \pmod 8$. Therefore, for all possible a, we have $a^6 \equiv 1 \pmod 8$, and hence, $8 \mid a^6 - 1$. Since 3, 7, and 8 are all relatively prime, then $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.

(c) First, since $\gcd(a, 133) = \gcd(b, 133) = 1$, then $\gcd(a, 19) = \gcd(a, 7) = \gcd(b, 19) = \gcd(b, 7) = 1$ using the fact that $133 = 7 \cdot 19$. Hence, from the little theorem, we have the congruences $a^{18} \equiv 1 \pmod{19}$ and $a^6 \equiv 1 \pmod 7$. Cubing both sides of the second congruence gives us the two congruences $a^{18} \equiv 1 \pmod{19}$ and $a^{18} \equiv 1 \pmod 7$. Since 7 and 19 are relatively prime, then we get that $a^{18} \equiv 1 \pmod{133}$. Since this is also true for b, then both a and b are congruent to 1 modulo 133, when taken to the power of 18. Hence, $a^{18} \equiv b^{18} \pmod{133}$, which is equivalent to $133 \mid a^{18} - b^{18}$.

3. Prove that there exist infinitely many composite numbers n for which $a^{n-1} \equiv a \pmod{n}$. [*Hint:* Take $n = 2p$ where p is an odd prime.]

Solution Let $n = 2p$ where p is an odd prime, and let a be an arbitrary integer. By the little theorem, we have that $a^{p-1} \equiv 1 \pmod{p}$ when a is not divisible by p. In that case, squaring both sides gives us the congruence $a^{2p-2} \equiv 1 \pmod{p}$. Multiplying by a on both sides gives us $a^{n-1} \equiv a \pmod{p}$, which is now true with no restrictions on a. The congruence $a^{n-1} \equiv a \pmod{2}$ is trivial is we check the only cases $a \equiv 0 \pmod{2}$ and $a \equiv 1 \pmod{2}$. Since 2 and p are relatively prime, then $a^{n-1} \equiv a \pmod{n}$. Since there are infinitely many odd primes, then there are infinitely many composite integers n such that $a^{n-1} \equiv a \pmod{n}$ holds for all integers a.

4. Derive each of the following congruences:

(a) $a^{21} \equiv a \pmod{15}$ for all a. [*Hint:* By Fermat's Theorem, $a^5 \equiv a \pmod{5}$.]

(b) $a^7 \equiv a \pmod{42}$ for all a.

(c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.

(d) $a^9 \equiv a \pmod{30}$ for all a.

Solution

(a) By the little theorem, we have that $a^4 \equiv 1 \pmod{5}$ for integers a non-divisible by 5. Taking both sides to the fifth power gives us $a^{20} \equiv 1 \pmod{5}$. Multiplying both sides by a implies that $a^{21} \equiv a \pmod{5}$ for any integers a now. Similarly, by the little theorem, we have that $a^2 \equiv 1 \pmod{3}$ for integers a non-divisible by 3. Taking both sides to the tenth power gives us $a^{20} \equiv 1 \pmod{3}$. Multiplying both sides by a implies that $a^{21} \equiv a \pmod{3}$ for any integers a now. Since 3 and 5 are relatively prime, then it follows that $a^{21} \equiv a \pmod{15}$ for all integers a.

(b) Let a be an integer, then by the little theorem, we have the congruences:

$$\begin{aligned} a^7 &\equiv a \cdot (a^3)^2 \equiv a \cdot a^3 \equiv (a^2)^2 \equiv a \pmod{2}, \\ a^7 &\equiv a \cdot (a^2)^3 \equiv a \cdot a^2 \equiv a^3 \equiv a \pmod{3}, \\ a^7 &\equiv a \pmod{7}. \end{aligned}$$

Since 2, 3, and 7 are relatively prime, then $a^7 \equiv a \pmod{42}$.

(c) Let a be an integer, then by the little theorem, we have the congruences:

$$\begin{aligned} a^{13} &\equiv a \cdot (a^4)^3 \equiv a \cdot a^4 \equiv a^2 \cdot a^3 \equiv a^2 \cdot a \equiv a^3 \equiv a \pmod{3}, \\ a^{13} &\equiv a^6 \cdot a^7 \equiv a^6 \cdot a \equiv a^7 \equiv a \pmod{7}, \\ a^{13} &\equiv a \pmod{13}. \end{aligned}$$

Since 3, 7, and 13 are relatively prime, then $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$.

(d) Let a be an integer, then by the little theorem, we have the congruences:

$$\begin{aligned} &a^9 \equiv a \cdot (a^4)^2 \equiv a \cdot a^4 \equiv a \cdot (a^2)^2 \equiv a \cdot a^2 \equiv a \cdot a \equiv a \pmod{2}, \\ &a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod{3}, \\ &a^9 \equiv a^4 \cdot a^5 \equiv a^4 \cdot a \equiv a^5 \equiv a \pmod{5}. \end{aligned}$$

Since 2, 3, and 5 are relatively prime, then $a^9 \equiv a \pmod{30}$.

5. If $\gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$.

Solution If $\gcd(a, 30) = 1$, then a is not divisible by 2, 3, and 5. Hence, by the little theorem, $a^2 \equiv 1 \pmod{3}$ and $a^4 \equiv 1 \pmod{5}$. Squaring the first congruence gives us $a^4 \equiv 1 \pmod{3}$. Since a is not divisible by 2, then $a \equiv \pm 1 \pmod{4}$ and so $a^4 \equiv 1 \pmod{4}$. Since 3, 4, and 5 are relatively prime, then $a^4 \equiv 1 \pmod{60}$.

6.

(a) Find the units digit of 3^{100} by the use of Fermat's Theorem.

(b) For any integer a, verify that a^5 and a have the same units digit.

Solution

(a) By the little theorem, we have that $3^{100} \equiv 1^{100} \equiv 1 \pmod{2}$ and

$$3^{100} \equiv ((3^4)^5)^5 \equiv (3^4)^5 \equiv 3^4 \equiv 1 \pmod{5}.$$

Since 2 and 5 are relatively prime, then $3^{100} \equiv 1 \pmod{10}$ which implies that the units digit of 3^{100} is 1.

(b) By the little theorem, we have that

$$\begin{aligned} &a^5 \equiv a \cdot (a^2)^2 \equiv a \cdot a^2 \equiv a \cdot a \equiv 1 \pmod{2}, \\ &a^5 \equiv a \pmod{5}. \end{aligned}$$

Since 2 and 5 are relatively prime, then $a^5 \equiv a \pmod{10}$ which implies that a^5 and a have the same units digit.

7. If $7 \nmid a$, prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7. [*Hint:* Apply Fermat's Theorem.]

Solution Since $7 \nmid a$, then by the little theorem, $a^6 \equiv 1 \pmod{7}$, and so $7 \mid a^6 - 1$. But since $a^6 - 1 = (a^3 - 1)(a^3 + 1)$ and 7 is prime, then 7 must divide either $a^3 + 1$ or $a^3 - 1$.

8. The three most recent appearances of Halley's comet were in the years 1835, 1910, and 1986; the next occurence will be in 2061. Prove that

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}.$$

Solution First, notice that $1835 \equiv 1 \pmod 7$, $1986 \equiv -2 \pmod 7$, and $2061 = 6 \cdot 343 + 3$. By the little theorem, we then have

$$\begin{aligned} 1835^{1910} + 1986^{2061} &\equiv 1^{1910} + (-2)^{2061} \\ &\equiv 1 + (-2)^3((-2)^6)^{343} \\ &\equiv 1 + (-8) \cdot 1^{343} \\ &\equiv 1 - 8 \\ &\equiv 0 \pmod 7 \end{aligned}$$

which concludes our proof.

9.

(a) Let p be a prime and $\gcd(a,p) = 1$. Use Fermat's Theorem to verify that $x \equiv a^{p-2}b \pmod p$ is a solution of the linear congruence $ax \equiv b \pmod p$.

(b) By applying part (a), solve the linear congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, and $3x \equiv 17 \pmod{29}$.

Solution

(a) Suppose that $x \equiv a^{p-2}b$ where $\gcd(a,p) = 1$, then by the little theorem:

$$ax \equiv a \cdot a^{p-2}b \equiv a^{p-1}b \equiv 1 \cdot b \equiv b \pmod p.$$

(b) For the equation $2x \equiv 1 \pmod{31}$, part (a) gives us the solution

$$x \equiv 2^{29} = 2^4 \cdot (2^5)^5 = 16 \cdot 32^5 \equiv 16 \cdot 1^5 = 16 \pmod{31}.$$

For the equation $6x \equiv 5 \equiv -6 \pmod{11}$, part (a) gives us the solution

$$x \equiv 6^9 \cdot (-6) = -6^{10} \equiv -3^5 = -3^2 \cdot 3^3 \equiv 2 \cdot 5 = 10 \equiv -1 \pmod{11}.$$

For the equation $3x \equiv 17 \pmod{29}$, part (a) gives us the solution

$$x \equiv 3^{27} \cdot 17 \equiv (-2)^9 \cdot 17 \equiv 2^9 \cdot 12 = 2^{10} \cdot 6 \equiv 3^2 \cdot 2 \cdot 3 \equiv -4 \pmod{29}.$$

10. Assuming that a and b are integers not divisible by the prime p, establish the following:

(a) If $a^p \equiv b^p \pmod p$, then $a \equiv b \pmod p$.

(b) If $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$. [*Hint:* By (a), $a = b = pk$ for some k, so that $a^p - b^p = (b + pk)^p - b^p$; now show that p^2 divides the latter expression.]

Solution

(a) By the little theorem, we have that $a \equiv a^p \equiv b^p \equiv b \pmod p$.

(b) If $a^p \equiv b^p \pmod{p}$, then part (a) tells us that $a \equiv b \pmod{p}$ and so $a = b+pk$ for some integer k. Thus, by the Binomial Theorem, we have that

$$\begin{aligned} a^p - b^p &= (b+kp)^p - b^p \\ &= b^p + \binom{p}{1} b^{p-1}pk + \binom{p}{2} b^{p-2}p^2k^2 + \cdots + (pk)^p - b^p \\ &= \binom{p}{1} b^{p-1}pk + \binom{p}{2} b^{p-2}(pk)^2 + \cdots + (pk)^p. \end{aligned}$$

In the latter expression, every term that contains a fact of $(pk)^n$ is congruent to zero modulo p^2 for $n \geqslant 2$. Hence, we get that

$$a^p - b^p \equiv \binom{p}{1} b^{p-1}pk = p^2b^{p-1}k \equiv 0 \pmod{p^2}.$$

Therefore, $a^p \equiv b^p \pmod{p^2}$.

11. Employ Fermat's Theorem to prove that, if p is an odd prime, then

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

(b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$. [*Hint:* Recall the identity $1 + 2 + 3 + \cdots + (p-1) = p(p-1)/2$.]

Solution

(a) Since every integer between 1 and $p-1$ is not divisible by p, then by the little theorem, we get that

$$1^{p-1}+2^{p-1}+3^{p-1}+\cdots+(p-1)^{p-1} \equiv 1+1+1+\cdots+1 = p-1 \equiv -1 \pmod{p}.$$

(b) By the little theorem, we get that

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 1 + 2 + 3 + \cdots + (p-1) = p\frac{p-1}{2} \pmod{p}.$$

Since p is odd, then $(p-1)/2$ is an integer and so $p(p-1)/2 \equiv 0 \pmod{p}$. Therefore,

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

12. Prove that if p is an odd prime and k is an integer satisfying $1 \leqslant k \leqslant p-1$, then the binomial coefficient

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Solution We know that the binomial coefficient $\binom{p-1}{k}$ can be written as

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-k-1)!} = \frac{(p-1)\ldots(p-k)}{k!}.$$

Hence:

$$k!\binom{p-1}{k} = (p-1)\dots(p-k) \equiv (-1)(-2)\dots(-k) = (-1)^k \cdot k! \pmod p$$

Since p doesn't divide $k!$, then we can cancel out the $k!$ on both sides of the congruence to get

$$\binom{p-1}{k} \equiv (-1)^k \pmod p.$$

13. Assume that p and q are distinct odd primes such that $p-1 \mid q-1$. If $\gcd(a, pq) = 1$, show that $a^{q-1} \equiv 1 \pmod{pq}$.

Solution First, since $\gcd(a, pq) = 1$, then $\gcd(a, p) = \gcd(a, q) = 1$. Hence, by the little theorem, we have that $a^{q-1} \equiv 1 \pmod q$. Similarly, by the little theorem, we have that $a^{p-1} \equiv 1 \pmod p$. Since $p-1 \mid q-1$, then $q-1 = k(p-1)$. Taking both sides of the latter congruence to the kth power gives us $a^{q-1} \equiv 1 \pmod p$. Since p and q are relatively prime, then $a^{q-1} \equiv 1 \pmod{pq}$.

14. If p and q are distinct primes, prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Solution Since p and q are distinct primes, then we can apply the little theorem to get the congruences $p^{q-1} \equiv 1 \pmod q$ and $q^{p-1} \equiv 1 \pmod p$. If we add q^{p-1} on both sides of the first congruence and if we add p^{q-1} on both sides of the second congruence, we get the new congruences $p^{q-1} + q^{p-1} \equiv 1 + q^{p-1} \equiv 1 \pmod q$ and $p^{q-1} + q^{p-1} \equiv p^{q-1} + 1 \equiv 1 \pmod p$. Since p and q are relatively prime, then it follows that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

15. Establish the statements below:

(a) If the number $M_p = 2^p - 1$ is composite, where p is a prime, then M_p is pseudoprime.

(b) Every composite number $F_n = 2^{2^n} + 1$ is a pseudoprime $(n = 0, 1, 2 \dots)$. [*Hint:* By Problem 21, Section 2.2, $2^{n+1} \mid 2^{2^n}$ implies that $2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1$; but $F_n \mid 2^{2^{n+1}} - 1$.]

Solution

(a) Since p is prime, p divides $2^p - 2$ by the little theorem, and hence, by Problem 21, Section 2.2, we have that $M_p = 2^p - 1 \mid 2^{2^p - 2} - 1$. In other words, $M_p \mid 2^{M_p - 1} - 1$. Thus, $M_p \mid 2^{M_p} - 2$ which implies that M_p is a pseudo prime (by assumption, we know that M_p is composite).

(b) Since $n + 1 \leqslant 2^n$, then $2^{n+1} \mid 2^{2^n}$. By Problem 21, Section 2.2, we get that $2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1$. Since $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = F_n(2^{2^n} + 1)$, then $F_n \mid 2^{2^{n+1}} - 1$ and so $F_n \mid 2^{2^{2^n}} - 1$. Multiplying the latter by 2 gives us that $F_n \mid 2^{2^{2^n} + 1} - 2 = 2^{F_n} - 2$. Since F_n is composite, then it follows that F_n is a pseudoprime.

16. Confirm that the following integers are absolute pseudoprimes:

(a) $1105 = 5 \cdot 13 \cdot 17$,

(b) $2821 = 7 \cdot 13 \cdot 31$,

(c) $2465 = 5 \cdot 17 \cdot 29$.

Solution

(a) By the little theorem, we have that if $\gcd(a, 1105) = 1$, then $a^4 \equiv 1 \pmod{5}$, $a^{12} \equiv 1 \pmod{13}$, and $a^{16} \equiv 1 \pmod{17}$. Taking the previous congruences to the 276th, 92th, and 69th power respectively gives us the new congruences $a^{1104} \equiv 1 \pmod{5}$, $a^{1104} \equiv 1 \pmod{13}$, and $a^{1104} \equiv 1 \pmod{17}$. Since 5, 13, and 17 are relatively prime, then $a^{1104} \equiv 1 \pmod{1105}$, and so $a^{1105} \equiv a \pmod{1105}$ for every integer a. Therefore, 1105 is an absolute pseudoprime.

(b) By the little theorem, we have that if $\gcd(a, 2821) = 1$, then $a^6 \equiv 1 \pmod{7}$, $a^{12} \equiv 1 \pmod{13}$, and $a^{30} \equiv 1 \pmod{31}$. Taking the previous congruences to the 470th, 235th, and 94th power respectively gives us the new congruences $a^{2820} \equiv 1 \pmod{7}$, $a^{2820} \equiv 1 \pmod{13}$, and $a^{2820} \equiv 1 \pmod{31}$. Since 7, 13, and 31 are relatively prime, then $a^{2820} \equiv 1 \pmod{2821}$, and so $a^{2821} \equiv a \pmod{2821}$ for every integer a. Therefore, 2821 is an absolute pseudoprime.

(c) By the little theorem, we have that if $\gcd(a, 2465) = 1$, then $a^4 \equiv 1 \pmod{5}$, $a^{16} \equiv 1 \pmod{17}$, and $a^{28} \equiv 1 \pmod{29}$. Taking the previous congruences to the 616th, 154th, and 88th power respectively gives us the new congruences $a^{2464} \equiv 1 \pmod{5}$, $a^{2464} \equiv 1 \pmod{17}$, and $a^{2464} \equiv 1 \pmod{29}$. Since 5, 17, and 29 are relatively prime, then $a^{2464} \equiv 1 \pmod{2465}$, and so $a^{2465} \equiv a \pmod{2464}$ for every integer a. Therefore, 2465 is an absolute pseudoprime.

17. Show that the pseudoprime 341 is not an absolute pseudoprime by showing that $11^{341} \not\equiv 11 \pmod{341}$. [*Hint:* $31 \nmid 11^{341} - 11$.]

Solution Suppose that $11^{341} \equiv 11 \pmod{341}$, then $11^{341} \equiv 11 \pmod{31}$ since $31 \mid 341$. By the little theorem, we have that

$$11^{341} = (11^{11})^{31} \equiv 11^{11} \pmod{31}.$$

Now, since $11^{11} \equiv 11 \cdot 11^{10} \equiv 11 \cdot (-3)^5 \pmod{31}$, then

$$11^{11} \equiv (-33) \cdot 3^4 \equiv (-2) \cdot 81 \equiv (-2) \cdot (-12) = 24 \pmod{31}$$

which implies that $11 \equiv 11^{341} \equiv 24 \pmod{31}$, a contradiction. Therefore, $11^{341} \not\equiv 11 \pmod{341}$ and so 342 is not an absolute pseudoprime.

18.

(a) When $n = 2p$, where p is an odd prime, prove that $a^{n-1} \equiv a \pmod{n}$ for any integer a.

(b) For $n = 195 = 3 \cdot 5 \cdot 13$, verify that $a^{n-2} \equiv a \pmod{n}$ for any integer a.

Solution

(a) By the little theorem, if a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Squaring both sides gives us that $a^{n-2} \equiv 1 \pmod{p}$. Multiplying both sides by a gives us that $a^{n-1} \equiv a \pmod{p}$ for any integer a. Similarly, for any integer a, we have that $a^{n-1} \equiv a \pmod{2}$ by checking the only two cases $a \equiv 0, 1 \pmod{2}$. Since p is odd, then 2 and p are relatively prime, and hence, $a^{n-1} \equiv a \pmod{n}$.

(b) By the little theorem, we have that

$$\begin{aligned} a^{n-2} &= a \cdot (a^{64})^3 \equiv a \cdot a^{64} \equiv a^2 \cdot (a^{21})^3 \equiv a^2 \cdot (a^7)^3 \equiv (a^3)^3 \equiv a \pmod{3}, \\ a^{n-2} &= a^3 (a^{38})^5 \equiv a \cdot a^{40} \equiv a(a^8)^5 \equiv a^4 a^5 \equiv a^5 \equiv a \pmod{5}, \\ a^{n-2} &= a^{11}(a^{14})^{13} \equiv a^{11} \cdot a^{14} = a^{12} \cdot a^{13} \equiv a^{13} \equiv a \pmod{13}. \end{aligned}$$

Since 3, 5, and 13 are relatively prime, then $a^{n-2} \equiv a \pmod{n}$ for all a.

19. Prove that any integer of the form

$$n = (6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime if all the three factors are prime; hence, $1729 = 7 \cdot 13 \cdot 19$ is an absolute pseudoprime.

Solution Let $p_1 = 6k+1$, $p_2 = 12k+1$, and $p_3 = 18k+1$. Let a be an integer not divisible by p_1, then by the little theorem, we have that $a^{6k} \equiv 1 \pmod{p_1}$, which implies that $a^{6kp_2p_3} \equiv 1 \pmod{p_1}$. Since $p_1 \mid p_2p_3 - 1$, then $a^{p_2p_3-1} \equiv 1 \pmod{p_1}$, and hence, $a^{6kp_2p_3+p_2p_3-1} = a^{n-1} \equiv 1 \pmod{p_1}$. Multiplying by a on both sides gives us $a^n \equiv a \pmod{p_1}$. Using the same exact argument with the fact that $p_2 \mid p_1p_3 - 1$ and $p_3 \mid p_1p_2 - 1$ lets us conclude that $a^n \equiv a \pmod{p_2}$ and $a^n \equiv a \pmod{p_3}$. Since the p_i's are distinct, then $a^n \equiv a \pmod{n}$. Therefore, n is an absolute pseudoprime.

20. Show that $561 \mid 2^{561} - 2$ and $561 \mid 3^{561} - 3$. It is an unanswered question whether there exist infinitely many composite numbers n with the property that $n \mid 2^n - 2$ and $n \mid 3^n - 3$.

Solution First, notice that $561 = 3 \cdot 11 \cdot 17$. Using propoerties of congruences, we have that $2^{561} \equiv (-1)^{561} = -1 \equiv 2 \pmod{3}$. By the little theorem, we have

$$\begin{aligned} 2^{561} &\equiv 2 \cdot (2^{10})^{56} \equiv 2 \cdot 1^{56} = 2 \pmod{11} \\ 2^{561} &\equiv 2 \cdot (2^{16})^{35} \equiv 2 \cdot 1^{35} = 2 \pmod{17}. \end{aligned}$$

Since 3, 11, and 17 are relatively prime, then $2^{561} \equiv 2 \pmod{561}$. Similarly, we have that $3^{561} \equiv 0 \equiv 3 \pmod{3}$, and by the little theorem:

$$\begin{aligned} 3^{561} &\equiv 3 \cdot (3^{10})^{56} \equiv 3 \cdot 1^{56} = 3 \pmod{11} \\ 3^{561} &\equiv 3 \cdot (3^{16})^{35} \equiv 3 \cdot 1^{35} = 3 \pmod{17}. \end{aligned}$$

Since 3, 11, and 17 are relatively prime, then $3^{561} \equiv 3 \pmod{561}$.

5.4 Wilson's Theorem

1.

(a) Find the remainder when 15! is divided by 17.

(b) Find the remainder when 2(26!) is divided by 29. [*Hint:* By Wilson's Theorem, $2(p-3)! \equiv -1 \pmod{p}$ for any odd prime $p > 3$.]

Solution

(a) As we saw in the proof of Wilson's Theorem, $15! = (17-2)! \equiv 1 \pmod{17}$. Therefore, the remainder when 15! is divided by 17 is 1.

(b) As in the previous part, we have that $27! = (29-2)! \equiv 1 \pmod{29}$. Since $27! = 26! \cdot 27 \equiv -2 \cdot 26! \pmod{29}$, then $2(26!) \equiv -1 \pmod{29}$.

2. Determine whether 17 is a prime by deciding whether or not $16! \equiv -1 \pmod{17}$.

Solution Simply notice that

$$\begin{aligned} 16! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \\ &= (1 \cdot 16)(2 \cdot 9)(3 \cdot 6)(4 \cdot 13)(5 \cdot 7)(8 \cdot 15)(10 \cdot 12)(11 \cdot 14) \\ &\equiv (-1) \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \\ &= -1 \pmod{17}. \end{aligned}$$

Therefore, 17 is a prime number.

3. Arrange the integers 2, 3, 4, . . ., 21 in pairs a and b with the property that $ab \equiv 1 \pmod{23}$.

Solution Since $23 + 1 = 24$ can be written as $2 \cdot 12$, $4 \cdot 6$ and $8 \cdot 3$, then this gives the three pairs $(2, 12)$, $(3, 8)$, and $(4, 6)$. Similarly, since $3 \cdot 23 + 1 = 70$ and 70 can be written as $5 \cdot 14$ and $7 \cdot 10$, then we get the pairs $(5, 14)$ and $(7, 10)$. Since $7 \cdot 23 + 1 = 162 = 9 \cdot 18$, then we get the pair $(9, 18)$. Since $9 \cdot 23 + 1 = 208 = 13 \cdot 16$, then we get the pair $(13, 16)$. Since $10 \cdot 23 + 1 = 231 = 11 \cdot 21$, then we get the pair $(11, 21)$. Since $13 \cdot 23 + 1 = 300 = 15 \cdot 20$, then we get the pair $(15, 20)$ and so the last pair is $(17, 19)$. Therefore, the pairs are:

$$(2, 12),\ (3, 8),\ (4, 6),\ (5, 14),\ (7, 10),\ (9, 18),\ (11, 21),\ (13, 16),\ (15, 20),\ (17, 19).$$

4. Show that $18! \equiv -1 \pmod{437}$.

Solution First, notice that $437 = 19 \cdot 57$. By Wilson's Theorem, we have that $18! \equiv -1 \pmod{19}$ and $22! \equiv -1 \pmod{23}$. Since

$$22! = 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \equiv 18!(-4)(-3)(-2)(-1) = 18! \cdot 24 \equiv 18! \pmod{23},$$

then we get that $18! \equiv -1 \pmod{23}$ as well. Since 19 and 23 are relatively prime, we have that $18! \equiv -1 \pmod{437}$.

5.

(a) Prove that any integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.

(b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$.

Solution

(a) Let $n > 1$, then by Wilson's Theorem:

$$\begin{aligned} n \text{ prime} &\iff (n-1)! \equiv -1 \pmod{n} \\ &\iff (n-2)!(n-1) \equiv -1 \pmod{n} \\ &\iff (n-2)!(-1) \equiv -1 \pmod{n} \\ &\iff (n-2)! \equiv 1 \pmod{n}. \end{aligned}$$

(b) Suppose that n is composite, then $n = ab$ with $a, b < n$. If $a \neq b$, then $(n-1)!$ is divisible by ab and hence, $(n-1)! \equiv 0 \pmod{n}$. Suppose now that $n = a^2$, then using the fact that $4 < n$, we get that $2 < a$. Multiplying by a on both sides gives $2a < n$. Since both a and $2a$ are less than n and distinct, then $a \cdot 2a \mid (n-1)!$. It follows that $(n-1)! \equiv 0 \pmod{n}$.

6. Given a prime number p, establish the congruence

$$(p-1)! \equiv p-1 \pmod{1+2+3+\cdots+(p-1)}.$$

Solution By Wilson's Theorem, we have that $p \mid (p-2)! - 1$, and so p divides $2[(p-2)!-1]$. Multiplying by $p-1$ on both sides of this division gives us that $p(p-1) \mid 2[(p-1)! - (p-1)]$. Since either p or $p-1$ is even, then we can divide both sides of the division by 2 to get that $p(p-1)/2 \mid (p-1)! - (p-1)$. Finally, since $p(p-1)/2 = 1+2+3+\cdots+(p-1)$, then

$$(p-1)! \equiv p-1 \pmod{1+2+3+\cdots+(p-1)}.$$

7. If p is prime, prove that

$$p \mid a^p + (p-1)!a \quad \text{and} \quad p \mid (p-1)!a^p + a$$

for any integer a. [*Hint:* By Wilson's Theorem, $a^p + (p-1)!a \equiv a^p - a \pmod{p}$.]

Solution Let a be any integer, then by Fermat's Little Theorem, we have that $a^p \equiv a \pmod{p}$. By Wilson's Theorem, we have that $(p-1)! \equiv -1 \pmod{p}$. Thus, combining these two results, we get that $a^p + (p-1)!a \equiv a^p - a \equiv 0 \pmod{p}$ and $(p-1)!a^p + a \equiv a - a^p \equiv 0 \pmod{p}$. Therefore, p divides $a^p + (p-1)!a$ and $(p-1)!a^p + a$.

8. Find two odd primes $p \leqslant 13$ for which the congruence $(p-1)! \equiv -1 \pmod{p^2}$ holds.

Solution When $p = 5$, we have $p^2 = 25$ and $(p-1)! = 24$. Hence, $(p-1)! \equiv -1 \pmod{p^2}$ holds. Similarly, when $p = 13$, we have $p^2 = 169$. Since $6! = 720 \equiv 44 \pmod{169}$, then $7! \equiv 7 \cdot 44 = 308 \equiv -30 \pmod{169}$. From this, we have that $8! \equiv 8(-30) = -240 \equiv -71 \pmod{169}$. If we continue this process, we get

$$\begin{aligned} 9! &\equiv 9 \cdot (-71) = -639 \equiv 37 \pmod{169}; \\ 10! &\equiv 10 \cdot 37 = 370 \equiv 32 \pmod{169}; \\ 11! &\equiv 11 \cdot 32 = 352 \equiv 14 \pmod{169}; \\ 12! &\equiv 12 \cdot 14 = 168 \equiv -1 \pmod{169}. \end{aligned}$$

Therefore, the desired property holds for $p = 5$ and $p = 13$.

9. Using Wilson's Theorem, prove that

$$1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

for any odd prime p. [*Hint:* Since $k \equiv -(-k) \pmod{p}$, it follows that $2 \cdot 4 \cdot 6 \dots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \dots (p-2) \pmod{p}$.]

Solution Since $1 \equiv -(p-1) \pmod{p}$, $3 \equiv -(p-3)$, ..., $p-2 \equiv -2 \pmod{p}$, then

$$\begin{aligned} 1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 &\equiv 1(-1)(p-2) \cdot 3(-1)(p-3) \cdot \dots (p-2)(-1) \cdot 2 \\ &= (-1)^{(p-1)/2} 1 \cdot 2 \cdot 3 \dots (p-2)(p-1) \\ &= (-1)^{(p-1)/2}(p-1)! \\ &\equiv (-1)^{(p+1)/2} \pmod{p}. \end{aligned}$$

10.

(a) For a prime p of the form $4k+3$, prove that either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \quad \text{or} \quad \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p};$$

hence, $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 \equiv 1 \pmod{p}$.

(b) Use part (a) to show that if $p = 4k+3$ is prime, then the product of all the even integers less than p is congruent modulo p to either 1 or -1. [*Hint:* Fermat's Theorem implies that $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$.]

Solution

(a) In the second part of the proof of Theorem 5-5, it was shown that

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

using Wilson's Theorem. When $p = 4k+3$, we have $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$ so the congruence becomes $-[(p-1)/2]!^2 \equiv -1 \pmod{p}$ which is equivalent to $[(p-1)/2]!^2 \equiv 1 \pmod{p}$. Rearranging, we get that

$$\left[\left(\frac{p-1}{2}\right)! - 1\right]\left[\left(\frac{p-1}{2}\right)! + 1\right] \equiv 0 \pmod{p}.$$

Since p is prime, then we can conclude that either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \text{ or } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}.$$

(b) First, let P be equal to the product of all even integers less than p and notice that

$$\begin{aligned} P &= 2 \cdot 4 \ldots (p-3)(p-1) \\ &= (2 \cdot 1)(2 \cdot 2) \ldots \left(2 \cdot \frac{p-3}{2}\right)\left(2 \cdot \frac{p-1}{2}\right) \\ &= 2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \end{aligned}$$

Using part (a), we get that $P \equiv \pm 2^{(p-1)/2} \pmod{p}$. Next, using Fermat's Little Theorem, we have that $2^{p-1} \equiv 1 \pmod{p}$ which is equivalent to

$$(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Hence, $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Therefore, $P \equiv \pm 1 \pmod{p}$.

11. Apply Theorem 5-5 to find two solutions to the quadratic congruences $x^2 \equiv -1 \pmod{29}$ and $x^2 \equiv -1 \pmod{37}$.

Solution To solve the first congruence, it suffices to find the least positive residue of $[(29-1)/2]! = 14!$ modulo 29. First, since $2 \cdot 3 \cdot 5 \equiv 8 \cdot 11 \equiv 9 \cdot 13 \equiv 1 \pmod{29}$, then

$$14! \equiv 4 \cdot 6 \cdot 7 \cdot 10 \cdot 12 \cdot 14 \pmod{29}.$$

Now, since $6 \cdot 10 \equiv 2 \pmod{29}$, and $4 \cdot 7 \equiv -1 \pmod{29}$, then

$$14! \equiv -2 \cdot 12 \cdot 14 \pmod{29}.$$

Finally, since $-2 \cdot 14 \equiv 1 \pmod{29}$, then $14! \equiv 12 \pmod{29}$. Therefore, a first solution to the quadratic congruence is given by $x \equiv 12 \pmod{29}$. Since $-x = -12 \equiv 17 \pmod{29}$ is also a solution, then the two solutions are $x \equiv 12, 17 \pmod{29}$.

Let's solve the second congruence. It suffices to find the least positive residue of $[(37-1)/2]! = 18!$ modulo 37. Since $2 \cdot 18 \equiv -1 \pmod{37}$, then $3 \cdot 4 \cdot 6 \cdot 18 \equiv (2 \cdot 18)^2 \equiv 1 \pmod{37}$. It follows that

$$18! \equiv 2 \cdot 5 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \pmod{37}.$$

Next, since $5 \cdot 15 \equiv 16 \cdot 7 \equiv 8 \cdot 14 \equiv 1 \pmod{37}$, then

$$18! \equiv 2 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 17 \pmod{37}.$$

Since $10 \cdot 11 \equiv 3 \cdot 12 \equiv -1 \pmod{37}$, then $9 \cdot 10 \cdot 11 \cdot 12 \equiv 3 \pmod{37}$ and so

$$18! \equiv 2 \cdot 3 \cdot 13 \cdot 17 \pmod{37}.$$

Using the fact that $13 \equiv -24 \pmod{37}$ and $17 \equiv -20 \pmod{37}$, we get that

$$\begin{aligned} 18! &\equiv 2 \cdot 3 \cdot 24 \cdot 20 \\ &\equiv 2 \cdot 2 \cdot (3 \cdot 12) \cdot 20 \\ &\equiv -80 \\ &\equiv 31 \pmod{37}. \end{aligned}$$

Therefore, a first solution to the quadratic congruence is given by $x \equiv 31 \pmod{37}$. Since $-x = -31 \equiv 6 \pmod{37}$ is also a solution, then the two solutions are $x \equiv 6, 31 \pmod{37}$.

12. Show that if $p = 4k + 3$ is prime and $a^2 + b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$. [*Hint:* If $a \not\equiv 0 \pmod{p}$, then there exists an integer c such that $ac \equiv 1 \pmod{p}$; use this fact to contradict Theorem 5-5.]

Solution By contradiction, suppose that $a \neq\equiv 0 \pmod{p}$, then there is an integer c such that $ac \equiv 1 \pmod{p}$. Multiplying both sides of the equation by c^2 gives us the new congruence $1 + (cb)^2 \equiv 0 \pmod{p}$ which implies that cb is a solution to the equation $x^2 \equiv -1 \pmod{p}$. By Theorem 5-5, this is impossible so $a \equiv 0 \pmod{p}$. It follows that $b^2 \equiv 0 \pmod{p}$. By primality of p, it follows that $b \equiv 0 \pmod{p}$. Therefore, $a \equiv b \equiv 0 \pmod{p}$.

13. Prove that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$. [*Hint:* Theorem 5-5]

Solution Let p be a prime divisor of $n^2 + 1$, then $n^2 + 1 \equiv 0 \pmod{p}$ and hence, n is a solution to the equation $x^2 + 1 \equiv 0 \pmod{p}$. By Theorem 5-5, it directly follows that p is of the form $4k + 1$.

14. Verify that $4(29!) + 5!$ is divisible by 31.

Solution Using Wilson's Theorem, we have that $29! \equiv 1 \pmod{31}$ which implies that $4(29!) + 5! \equiv 4 + 5! = 124 \equiv 0 \pmod{31}$. Therefore, 31 divides $4(29!) + 5!$.

15. For a prime p and $0 \leqslant k \leqslant p - 1$, show that $k!(p - 1 - k)! \equiv (-1)^{k+1} \pmod{p}$.

Solution First, notice that

$$k!\binom{p-1}{k} = (p-1)\ldots(p-k) \equiv (-1)^k k! \pmod{p}$$

and hence, $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ (since $k! \not\equiv 0 \pmod{p}$). Using Wilson's Theorem, we get that

$$k!(p-k-1)!(-1)^k \equiv k!(p-k-1)!\binom{p-1}{k} \equiv (p-1)! \equiv -1 \pmod{p}.$$

Therefore, $k!(p - 1 - k)! \equiv (-1)^{k+1} \pmod{p}$.

16. If p and q are distinct primes, prove that

$$pq \mid a^{pq} - a^p - a^q + a$$

for any integer a.

Solution Let a be an integer, then by Fermat's Little Theorem, $p \mid a - a^p$. Similarly, if we apply it again to a^q, then $p \mid a^{pq} - a^q$ as well. Thus, $p \mid a^{pq} - a^p - a^q + a$. For the same exact reason, $q \mid a^{pq} - a^p - a^q + a$. Since p and q are relatively prime, then $pq \mid a^{pq} - a^p - a^q + a$.

17. Prove that if p and $p+2$ are a pair of twin prime, then

$$4((p-1)!+1)+p \equiv 0 \pmod{p(p+2)}.$$

Solution First, if we work in modulo p, then using Wilson's Theorem:

$$4((p-1)!+1)+p \equiv 4((p-1)!+1) \equiv 4(-1+1) \equiv 0 \pmod{p}.$$

Next, let's work in modulo $p+2$. Recall that $p \equiv -2 \pmod{p+2}$ and $p! \equiv 1 \pmod{p+2}$ by Wilson's Theorem. It follows that if we let $x = 4((p-1)!+1)+p$, then

$$-2x \equiv px \equiv 4(p!+p)+p^2 \equiv 4(1-2)+(-2)^2 \equiv 0 \pmod{p+2}.$$

It follows that $4((p-1)!+1)+p \equiv 0 \pmod{p+2}$. Since p and $p+2$ are relatively prime, then $4((p-1)!+1)+p \equiv 0 \pmod{p(p+2)}$.

Chapter 6

Number Theoretic Functions

6.1 The Functions τ and σ

1. Let m and n be positive integers and p_1, p_2, ..., p_r be the distinct primes which divide at least one of m or n. Then m and n may be written in the form

$$\begin{aligned} m &= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \quad \text{with } k_i \geqslant 0 \text{ for } i = 1, 2, \dots, r \\ n &= p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}, \quad \text{with } j_i \geqslant 0 \text{ for } i = 1, 2, \dots, r \end{aligned}$$

Prove that

$$\gcd(m, n) = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}, \quad \operatorname{lcm}(m, n) = p_1^{v_1} p_2^{v_2} \dots p_r^{v_r},$$

where $u_i = \min\{k_i, j_i\}$, the smaller of k_i and j_i; and $v_i = \max\{k_i, j_i\}$, the larger of k_i and j_i.

Solution First, if we let $g = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$ with $u_i = \min\{k_i, j_i\}$, then it is clear that g divides both m and n. Let d be a common divisor of m and n, then any prime dividing d msut divide m and n, and hence, it must be equal to one of the p_i's. Thus, $d = p_1^{e_1} ... p_r^{e_r}$ for some non-negative integers e_i. For all i, $p_i^{e_i}$ divides both $p_i^{k_i}$ and $p_i^{j_i}$ so $e_i \leqslant k_i, j_i$. It follows that $e_i \leqslant u_i$, and hence, $p_i^{e_i}$ divides $p_i^{u_i}$. Hence, d divides g. Therefore, g is the greatest common divisor of m and n.

Similarly, let $l = p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$ with $v_i = \max\{k_i, j_i\}$, then it is clear that l and n both divide l. Let c be a common multiple of m and n, then any prime dividing m and n must divide c, hence, $c = p_1^{a_1} ... p_r^{a_r} b$ for some non-negative integers a_i and for an integer b relatively prime to the p_i's. For all i, $p_i^{k_i}$ and $p_i^{j_i}$ both divide $p_i^{a_i}$ so $k_i, j_i \leqslant a_i$. It follows that $v_i \leqslant a_i$, and hence, $p_i^{v_i}$ divides $p_i^{a_i}$. Hence, l divides c. Therefore, l is the least common multiple of m and n.

2. Use the result of Problem 1 to calculate $\gcd(12378, 3054)$ and $\operatorname{lcm}(12378, 3054)$.

Solution Since $12378 = 2^1 \cdot 3^1 \cdot 2063^1$ and $3054 = 2^1 \cdot 3^1 \cdot 509^1$, then $\gcd(12378, 3054) = 2^1 \cdot 3^1 \cdot 509^0 \cdot 2063^0 = 6$ and $\operatorname{lcm}(12378, 3054) = 2^1 \cdot 3^1 \cdot 509^1 \cdot 2063^1 = 6300402$.

3. Deduce from Problem 1 that $\gcd(m, n) \operatorname{lcm}(m, n) = mn$ for positive integers m and n.

Solution Using the notation of Problem 1, we have that for all i, $u_i + v_i = \max\{k_i, j_i\} + \min\{k_i, j_i\} = k_i + j_i$. Hence,

$$\begin{aligned}\gcd(m,n)\operatorname{lcm}(m,n) &= (p_1^{u_1}p_2^{u_2}\dots p_r^{u_r})(p_1^{v_1}p_2^{v_2}\dots p_r^{v_r})\\ &= p_1^{u_1+v_1}p_2^{u_2+v_2}\dots p_r^{u_r+v_r}\\ &= p_1^{k_1+j_1}p_2^{k_2+j_2}\dots p_r^{k_r+j_r}\\ &= (p_1^{k_1}p_2^{k_2}\dots p_r^{k_r})(p_1^{j_1}p_2^{j_2}\dots p_r^{j_r})\\ &= mn\end{aligned}$$

which proves the statement.

4. In the notation of Problem 1, show that $\gcd(m,n) = 1$ if and only if $k_i j_i = 0$ for $i = 1, 2, ..., r$.

Solution Using the notation of Problem 1, we have that $\gcd(m,n) = 1$ if and only if $\min\{k_i, j_i\} = 0$ for all i. But for all i, $\min\{k_i, j_i\} = 0$ if and only if k_i or j_i is zero. Equivalently, for all i, $\min\{k_i, j_i\} = 0$ if and only if $k_i j_i = 0$. Therefore, $\gcd(m,n) = 1$ if and only if $k_i j_i = 0$ for all i.

5.

(a) Verify that $\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3)$ holds for $n = 3655$ and $n = 4503$.

(b) When $n = 14$, 206, and 957, show that $\sigma(n) = \sigma(n+1)$.

Solution

(a) Since $3655 = 5\cdot 17\cdot 43$, $3656 = 2^3\cdot 457$, $3657 = 3\cdot 23\cdot 53$, and $3658 = 2\cdot 31\cdot 59$, then

$$\begin{aligned}\tau(3655) &= (1+1)(1+1)(1+1) = 8,\\ \tau(3656) &= (3+1)(1+1) = 8,\\ \tau(3657) &= (1+1)(1+1)(1+1) = 8,\\ \tau(3658) &= (1+1)(1+1)(1+1) = 8.\end{aligned}$$

Similarly, since $4503 = 3\cdot 19\cdot 79$, $4504 = 2^3\cdot 563$, $4505 = 5\cdot 17\cdot 53$, and $4506 = 2\cdot 3\cdot 751$, then

$$\begin{aligned}\tau(4503) &= (1+1)(1+1)(1+1) = 8,\\ \tau(4504) &= (3+1)(1+1) = 8,\\ \tau(4505) &= (1+1)(1+1)(1+1) = 8,\\ \tau(4503) &= (1+1)(1+1)(1+1) = 8.\end{aligned}$$

(b) Since $14 = 2\cdot 7$, $15 = 3\cdot 5$, $206 = 2\cdot 103$, $207 = 3^2\cdot 23$, $957 = 3\cdot 11\cdot 29$, and $958 = 2\cdot 479$, then

$$\begin{aligned}\sigma(14) &= (1+2)(1+7) = 24 = (1+3)(1+5) = \sigma(15),\\ \sigma(206) &= (1+2)(1+103) = 312 = (1+3+9)(1+23) = \sigma(207),\\ \sigma(957) &= (1+3)(1+11)(1+29) = 1440 = (1+2)(1+479) = \sigma(958).\end{aligned}$$

6. For any integer $n \geqslant 1$, establish the inequality $\tau(n) \leqslant 2\sqrt{n}$. [*Hint:* If $d \mid n$, then one of d or n/d is less than or equal to $\sqrt{n}$.]

Solution Let D be the set of divisors of n, then we can pair each element d of D with another element d' in D such that $dd' = n$. In each pair, one of d or d' must be less than or equal to $\sqrt{n}$. Since there are at most $\sqrt{n}$ divisors of n lesser or equal to n, then there are at most $\sqrt{n}$ pairs (d, d') composing D. Since the number of elements in D, which is equal to $\tau(n)$, is twice (or twice minus 1 when n is a square) the number of pairs (d, d'), then there are at most $2\sqrt{n}$ elements in D. Therefore, $\tau(n) \leqslant 2\sqrt{n}$.

7. Prove that:

(a) $\tau(n)$ is an odd integer if and only if n is a perfect square;

(b) $\sigma(n)$ is an odd integer if and only if n is perfect square or twice a perfect square. [*Hint:* If p is an odd prime, then $1+p+p^2+\cdots+p^k$ is odd only when k is even.]

Solution

(a) Since $\tau(n) = (k_1+1)(k_2+1)\ldots(k_r+1)$, then $\tau(n)$ is odd if and only if $k_i = 2e_i$ for some integer i for all i. Next, $k_i = 2e_i$ for all i if and only if n is a perfect square. Therefore, $\tau(n)$ is odd if and only if n is a perfect square.

(b) If $\sigma(n)$ is odd, then $1 + p_i + \cdots + p_i^{k_i}$ is odd for all i. If p_i is not 2, then k_i must be even. It follows that $k_i = 2e_i$ for some e_i for all i. Thus, $n = 2^{k_0}a^2$ where a is the product of the $p_i^{e_i}$ for all i where p_i is not 2, and where $k_0 \geqslant 0$. If k_0 is even, then n is a square; if k_0 is odd, then $n = 2(2^{(k_0-1)/2}a)^2$ and so n is twice a perfect square.

Conversely, if n is a perfect square or twice a perfect square, then $n = 2^{k_0}a^2$ where a is odd. If we write $a = p_1^{e_1}\ldots p_r^{e_r}$, then $n = 2^{k_0}p_1^{2e_1}\ldots p_r^{2e_r}$ and so $\sigma(n) = (1 + 2 + \cdots + 2^{k_0})\ldots(1 + p_r + \cdots + p_r^{2e_r})$. Clearly, the factor $(1+2+\cdots+2^{k_0})$ is odd. Moreover, for all i, since p_i is odd, then $(1+p_i+\cdots+p_i^{2e_i})$ is odd. Therefore, $\tau(n)$ is odd.

8. Show that $\sum_{d|n} 1/d = \sigma(n)/n$ for every positive integer n.

Solution First, notice that

$$n\sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{n}{d} = \sum_{d|n} d = \sigma(n)$$

because the terms n/d are divisors of n, and n/d ranges over all the divisors of n once when d ranges over all the divisors of n. It follows that $\sum_{d|n} 1/d = \sigma(n)/n$.

9. If n is a square-free integer, prove that $\tau(n) = 2^r$ where r is the number of prime divisors of n.

Solution If n is a square-free integer, then k_i must be equal to 1 for all i because otherwise, n would be divisible by p_i^2, a contradiction. Hence,

$$\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1) = 2\cdot 2\cdots 2 = 2^r.$$

10. Establish the assertions below:

(a) If $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ is the prime factorization of $n>1$, then

$$1 > \frac{n}{\sigma(n)} > \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

(b) For any positive integer n,

$$\sigma(n!)/n! \geqslant 1 + 1/2 + 1/3 + \cdots + 1/n.$$

[*Hint:* See Problem 8.]

(c) If $n>1$ is a composite number, then $\sigma(n) > n+\sqrt{n}$. [*Hint:* Let $d \mid n$, where $1<d<n$, so $1<n/d<n$. If $d\leqslant\sqrt{n}$, then $n/d\geqslant\sqrt{n}$.]

Solution

(a) First, since 1 and n are both distinct divisors of n, then they are part of the sum defining $\sigma(n)$, and hence, $n<n+1\leqslant\sigma(n)$ which implies that $1>n/\sigma(n)$. Moreover, using the product formula for $\sigma(n)$, we get that

$$\begin{aligned}\frac{n}{\sigma(n)} &= \frac{\prod_{i=1}^r p_i^{k_i}}{\prod_{i=1}^r \frac{p_i^{k_i+1}-1}{p_i-1}}\\ &= \prod_{i=1}^r \frac{p_i^{k_i}(p_i-1)}{p_i^{k_i+1}-1}\\ &> \prod_{i=1}^r \frac{p_i^{k_i}(p_i-1)}{p_i^{k_i+1}}\\ &= \prod_{i=1}^r \frac{p_i-1}{p_i}\\ &= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\end{aligned}$$

which completes the proof.

(b) Since $\sigma(n!)/n! = \sum_{d|n!} 1/d$ and all integers between 1 and n divide $n!$, then

$$\frac{\sigma(n!)}{n!} = \sum_{d|n!}\frac{1}{d} \geqslant \sum_{i=1}^n \frac{1}{i} = 1 + 1/2 + 1/3 + \cdots + 1/n.$$

(c) If n is composite, then there is an integer d such that 1, d, and n are divisors of n. We can assume that $d \geqslant \sqrt{n}$ because otherwise, we can replace d by n/d, n/d will be distinct from 1 and n, and will be greater than $\sqrt{n}$. Hence, $\sigma(n) \geqslant 1 + d + n > n + \sqrt{n}$.

11. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$. [*Hint:* Utilize Problem 10(a).]

Solution First, notice that for any prime p, the number $n = p^{k-1}$ will satisfy $\tau(n) = k$. Since there are infinitely many primes, then there are infinitely such numbers n. Next, suppose that $\sigma(n) = k$, then by Problem 10(a), we know that $1 > n\sigma(n)$ which implies that $n < k$. It follows that there must be finitely many n such that $\sigma(n) = k$.

12.

(a) Find the form of all positive integers n satisfying $\tau(n) = 10$. What is the smallest positive integer for which this is true?

(b) Show that there are no positive integers n satisfying $\sigma(n) = 10$. [*Hint:* Note that for $n > 1$, $\sigma(n) > n$.]

Solution

(a) Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $\tau(n) = 10$ implies that $(k_1 + 1) \cdots (k_r + 1) = 10$. Since 10 can be written as a multiplication in only two ways ($1 \cdot 10$ and $2 \cdot 5$), then there are at most two k_i's which are nonzero. Hence, either $k_1 + 1 = 1$ and $k_2 + 1 = 10$, or $k_2 + 1 = 2$ and $k_2 + 1 = 5$. Equivalently, either $n = p^9$, or $n = pq^4$ where p and q are distinct primes. Conversely, every number n of the form p^9 or pq^4 with p and q distinct primes must satisfy $\tau(n) = 10$.

To find the smallest integer n such that $\tau(n) = 10$, consider the two following cases: if n is of the form p^9, then its minimum value is $2^9 = 512$; if n is of the form pq^3, then its minimum value is $3 \cdot 2^3 = 24$. Combining these two observations gives us that $n = 24$.

(b) Let's prove that $\sigma(n) \neq 10$ for all $n \geqslant 1$. First, since $\sigma(n) > n$ for all $n > 1$, then $\sigma(n) > 10$ for all $n \geqslant 10$ and so it suffices to show that $\sigma(n) \neq 10$ for integers between 1 and 9. Since $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$, $\sigma(7) = 8$, $\sigma(8) = 15$, and $\sigma(9) = 13$, then it follows that $\sigma(n) \neq 10$ for all $n \geqslant 1$.

13. Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$. [*Hint:* Choose k such that $\gcd(k, 10) = 1$ and consider the integers $m = 5k$, $n = 4k$.]

Solution First, notice that $\sigma(5^2) = \sigma(4^2)$ because $\sigma(5^2) = (5^3 - 1)/(5 - 1) = 124/4 = 31$ and $\sigma(4^2) = \sigma(2^4) = 2^5 - 1 = 32 - 1 = 31$. Hence, if we take any integer

k relatively prime with 10, then this integer squared will be relatively primes with 5^2 and 4^2. Thus, letting $m = 5k$ and $n = 4k$, we get

$$\sigma(m^2) = \sigma(5^2k^2) = \sigma(5^2)\sigma(k^2) = \sigma(4^2)\sigma(k^2) = \sigma(4^2k^2) = \sigma(n).$$

Finally, since there are infinitely many k's that are relatively prime with 10 (such as all numbers of the form $10t+1$), then there are infinitely many such pairs of m and n.

14. For $k \geqslant 2$, show each of the following:

(a) $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$;

(b) if $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ satisfies the equation $\sigma(n) = 2n$;

(c) if $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.

It is not known if there are any positive integers n for which $\sigma(n) = 2n + 1$.

Solution

(a) Since 2 is a prime number, then using the product formula for σ, we get

$$\sigma(n) = \frac{2^k - 1}{2 - 1} = 2 \cdot 2^{k-1} - 1 = 2n - 1.$$

(b) First, notice that $2^k - 1$ is prime relative to 2^{k-1} since it is odd. Hence, if we assume that $2^k - 1$ is prime, we get that

$$\sigma(n) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)([2^k - 1] + 1) = 2n.$$

(c) Again, since $2^k - 3$ is odd, then it is prime relative to 2^{k-1} giving us

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1})\sigma(2^k - 3)\\ &= (2^k - 1)([2^k - 3] + 1)\\ &= 2^k(2^k - 3) + (2^k - 1) - (2^k - 3) - 1\\ &= 2n + 1.\end{aligned}$$

15. If n and $n + 2$ are a pair of twin primes, establish that $\sigma(n + 2) = \sigma(n) + 2$; this also holds for $n = 434$ and 8575.

Solution First, recall that if p is prime, then $\sigma(p) = p + 1$. It follows that when n and $n + 2$ are a pair of twin primes, then

$$\sigma(n + 2) = n + 2 + 1 = \sigma(n) + 2.$$

The converse doesn't hold because when $n = 434 = 2\cdot 7\cdot 31$, we have $n+2 = 2^2\cdot 109$, and hence:

$$\sigma(n + 2) = 770 = 768 + 2 = \sigma(n) + 2.$$

Similarly, when $n = 8575 = 5^2 \cdot 7^3$, then $n + 2 = 8577 = 3^2 \cdot 953$ and hence:

$$\sigma(n + 2) = 12402 = 12400 + 2 = \sigma(n) + 2.$$

16.

(a) For any integer $n > 1$, prove that there exist integers n_1 and n_2 with $\tau(n_1) + \tau(n_2) = n$.

(b) Prove that Goldbach's Conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\sigma(n_1) + \sigma(n_2) = 2n$.

Solution

(a) Simply notice that for all $n > 1$:

$$\tau(2^{n-2}) + \tau(1) = (n-1) + 1 = n.$$

(b) First, if $2n = 2$, then we can take $n_1 = n_2 = 1$. If $n > 2$, then by Goldbach's Conjecture there exist prime numbers p and q such that $p + q = 2n - 2$. It follows that

$$\tau(p) + \tau(q) = (p+1) + (q+1) = (2n-2) + 2 = 2n.$$

17. For a fixed integer k, show that the function f defined by $f(n) = n^k$ is multiplicative.

Solution Let m and n be two integers relatively prime to each other, then

$$f(mn) = (mn)^k = m^k n^k = f(m)f(n).$$

Therefore, f is multiplicative.

18. Let f and g be multiplicative functions such that $f(p^k) = g(p^k)$ for each prime p and $k \geqslant 1$. Prove that $f = g$.

Solution Let n be an arbitrary integer, then $n = p_1^{k_1} \cdots p_r^{k_r}$ for some primes and integers by the Fundamental Theorem of Arithmetic. Since the integers $p_1^{k_1}$, $p_2^{k_2}$, ..., $p_r^{k_r}$ are pairwise relatively prime, then by multiplicativity of f and g:

$$f(n) = f(p_1^{k_1}) \cdots f(p_r^{k_r}) = g(p_1^{k_1}) \cdots g(p_r^{k_r}) = g(n).$$

Therefore, $f = g$.

19. Prove that if f and g are multiplicative functions, then so is their product fg and quotient f/g (whenever the latter function is defined).

Solution Let m and n be two integers prime relative to each other, then

$$f(mn)g(mn) = f(m)f(n)g(m)g(n) = [f(m)g(m)][f(n)g(n)]$$

and

$$\frac{f(mn)}{g(mn)} = \frac{f(m)f(n)}{g(m)g(n)} = \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)}.$$

Therefore, the functions fg and f/g are multiplicative.

20. Define the function ρ by taking $\rho(1) = 1$ and $\rho(n) = 2^r$, if the prime factorization of $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. For instance, $\rho(8) = 2$ and $\rho(10) = \rho(2^2) = 2^2$.

(a) Deduce that ρ is a multiplicative function.

(b) Find a formula for $F(n) = \sum_{d|n} \rho(d)$ in terms of the prime factorization of n.

Solution There is an error in this exercise. The function ρ is not multiplicative because $\rho(30 \cdot 77) = 5$ while $\rho(30) = 3$ and $\rho(77) = 2$. Hence, $\rho(30 \cdot 77) \neq \rho(30)\rho(77)$ even though $\gcd(30, 77) = 1$. This exercise cannot be done.

21. For any positive integer n, prove that $\sum_{d|n} \tau(n)^3 = (\sum_{d|n} \tau(n))^2$.
[*Hint:* Both sides of the equation in question are multiplicative functions of n, so that it suffices to consider the case $n = p^k$, where p is prime.]

Solution Suppose without loss of generality that $n = p^k$ where p is a prime and k is an integer, then

$$\begin{aligned}
\sum_{d \mid p^k} \tau(d)^3 &= \sum_{i=0}^{k} \tau(p^i)^3 \\
&= \sum_{i=0}^{k} (i+1)^3 \\
&= \left(\sum_{i=0}^{k} (i+1) \right)^2 \\
&= \left(\sum_{i=0}^{k} \tau(p^i) \right)^2 \\
&= \left(\sum_{d \mid p^k} \tau(d) \right)^2 .
\end{aligned}$$

Therefore, for all integers n, we have $\sum_{d|n} \tau(n)^3 = (\sum_{d|n} \tau(n))^2$.

22. Given $n \geqslant 0$, let $\sigma_s(n)$ denote the sum of the sth powers of the positive divisors of n, that is,

$$\sigma_s(n) = \sum_{d \mid n} d^s.$$

Verify the following:

(a) $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.

(b) σ_s is a multiplicative function. [*Hint:* The function f defined by $f(n) = n^s$, is multiplicative.]

(c) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then

$$\sigma_s(n) = \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1} \right) \left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1} \right) \cdots \left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1} \right).$$

Solution

(a) It is clear that when $s = 0$, then the sum of the sth powers of the divisors of n is the same as $\sum_{d|n} 1$, the number of divisors of n. Thus, $\sigma_0(n) = \tau$. Similarly, when $s = 1$, then the sum of the first powers of the divisors of n is simply equal to the sum of the divisors of n. Thus, $\sigma_1 = \sigma$.

(b) If we define the function $f(n) = n^s$, then we can write $\sigma_s(n)$ as $\sum_{d|n} f(d)$. Since f is mutiplicative (Problem 17), then σ_s is multiplicative.

(c) It suffices that the formula holds for the prime powers since the function is multiplicative. Hence, let $n = p^k$, then

$$\sigma_s(n) = \sum_{d \mid p^k} d^s = \sum_{i=0}^{k} p^{is} = \sum_{i=0}^{k} (p^s)^i = \frac{p^{s(i+1)} - 1}{p^s - 1}.$$

23. For any positive integer n, show that

(a) $\sum_{d|n} \sigma(n) = \sum_{d|n} \frac{n}{d}\tau(d)$, and

(b) $\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d)$.

[*Hint:* Since the functions

$$F(n) = \sum_{d|n} \sigma(d) \quad \text{and} \quad G(n) = \sum_{d|n} (n/d)\tau(d)$$

are both multiplicative, it suffices to prove that $F(p^k) = G(p^k)$ for any prime p.]

Solution

(a) Without loss of generality, suppose that $n = p^k$, then

$$\begin{aligned}
\sum_{d \mid n} \sigma(d) &= \sum_{i=0}^{k} \sigma(p^i) \\
&= 1 + (1 + p) + (1 + p + p^2) + \cdots + (1 + \cdots + p^k) \\
&= p^k \cdot 1 + \cdots + p^2(k - 1) + p^1 k + p^0(k + 1) \\
&= \frac{p^k}{p^0}\tau(p^0) + \cdots + \frac{p^k}{p^{k-1}}\tau(p^{k-1}) + \frac{p^k}{p^k}\tau(p^k) \\
&= \sum_{i=0}^{k} \frac{n}{p^i}\tau(p^i) \\
&= \sum_{d \mid n} \frac{n}{d}\tau(d).
\end{aligned}$$

Hence, the equation holds for all integers n.

(b) Similarly, without loss of generality, suppose that $n = p^k$, then

$$\begin{aligned}
\sum_{d \mid n} \frac{n}{d}\sigma(d) &= \sum_{i=0}^{k} p^{k-i}\sigma(p^i) \\
&= p^k \cdot 1 + p^{k-1}(1+p) + \cdots + p^1(1 + \cdots + p^{k-1}) + p^0(1 + \cdots + p^k) \\
&= p^k + (p^k + p^{k-1}) + \cdots + (p^k + \cdots + p) + (p^k + \cdots + 1) \\
&= p^0 \cdot 1 + p^1 \cdot 2 + p^2 \cdot 3 + \cdots + p^{k-1}k + p^k(k+1) \\
&= \sum_{i=0}^{k} p^i \tau(p^i) \\
&= \sum_{d \mid n} d\tau(d).
\end{aligned}$$

Therefore, it holds for all integers n.

6.2 The Möbius Inversion Formula

1.

(a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

(b) For any integer $n \geqslant 3$, show that $\sum_{k=1}^{n} \mu(k!) = 1$.

Solution

(a) We already know that in a list of m consecutive integers, one of them must be divisible by m, it follows that one of n, $n+1$, $n+2$, $n+3$ must be divisible by 4. Since 4 is a square, then it means that one of the four numbers is not square-free. Hence, $\mu(n+i) = 0$ for some $i = 0, 1, 2, 3$. Therefore, the multiplication of $\mu(n+i)$ where i ranges from 0 to 3 must be zero.

(b) Notice that $4 \mid k!$ for all $k \geqslant 4$, so it follows that $\mu(k!) = 0$ for all such k. Hence, for all $n \geqslant 3$:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1) + \mu(2) + \mu(6) + 0 + \cdots + 0 = 1 + (-1) + 1 = 1.$$

2. The *Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geqslant 1 \\ 0, & \text{otherwise} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = -\sum_{d|n} \mu(d) \log d$. [*Hint:* First show that $\sum_{d|n} \Lambda(d) = \log(n)$ and then apply the Möbius Inversion Formula.]

Solution First, let's prove that $\sum_{d|n} \Lambda(d) = \log(n)$. Given an integer $n = p_1^{k_1} \cdots p_r^{k_r}$, we know that divisors of n which are prime powers are precisely p_i^k where $i = 1, ..., r$ and $k = 1, ..., k_i$. It follows that

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{i=1}^{r} \sum_{k=1}^{k_i} \Lambda(p_i^k) \\ &= \sum_{i=1}^{r} \sum_{k=1}^{k_i} \log p_i \\ &= \sum_{i=1}^{r} \log(p_i^{k_i}) \\ &= \log(p_1^{k_1} \cdots p_r^{k_r}) \\ &= \log n. \end{aligned}$$

Therefore, if we apply the Möbius Inversion Formula, we get that

$$\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = \sum_{d|n} \mu(d) \log(n/d).$$

Next, notice that

$$\sum_{d|n} \mu(d) \log(n/d) = \log(n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d.$$

When $n = 1$, the first term on the right hand side is 0 since $\log 1 = 0$. Moreover, when $n > 1$, the first term on the right hand side is zero since $\sum_{d|n} \mu(d) = 0$. Thus, for all $n \geqslant 1$,

$$\sum_{d|n} \mu(d) \log(n/d) = -\sum_{d|n} \mu(d) \log d$$

and therefore:

$$\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = -\sum_{d|n} \mu(d) \log d.$$

3. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. If f is multiplicative, prove that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r)).$$

[*Hint:* By Theorem 6-4, the function F defined by $F(n) = \sum_{d|n} \mu(d) f(d)$ is multiplicative; hence, $F(n)$ is the product of the values $F(p_i^{k_i})$.]

Solution Since both functions μ and f are multiplicative, then so is their product. It follows that the function $F(n) = \sum_{d|n} \mu(d) f(d)$ is multiplicative. Hence, it suffices to prove the desired formula for the case $n = p^k$. In that case,

$$\begin{aligned}
\sum_{d|p^k} \mu(d) f(d) &= \sum_{i=0}^{k} \mu(p^i) f(p^i) \\
&= \mu(1) f(1) + \mu(p) f(p) + \mu(p^2) f(p^2) + \cdots + \mu(p^k) f(p^k) \\
&= 1 \cdot 1 + (-1) f(p) + 0 + \cdots + 0 \\
&= 1 - f(p)
\end{aligned}$$

where we used the fact that $f(1) = 1$. Therefore, the formula holds for all $n > 1$.

4. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, use Problem 3 to establish the following:

(a) $\sum_{d|n} \mu(d) \tau(d) = (-1)^r$;

(b) $\sum_{d|n} \mu(d) \sigma(d) = (-1)^r p_1 p_2 \cdots p_r$;

(c) $\sum_{d|n} \mu(d)/d = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$;

(d) $\sum_{d|n} d\mu(d) = (1-p_1)(1-p_2)\cdots(1-p_r)$.

Solution

(a) $\sum_{d|n} \mu(d)\tau(d) = (1-\tau(p_1))\cdots(1-\tau(p_r)) = (1-2)\cdots(1-2) = (-1)^r$.

(b) $\sum_{d|n} \mu(d)\sigma(d) = (1-\sigma(p_1))\cdots(1-\sigma(p_r)) = (-p_1)\cdots(-p_r) = (-1)^r p_1 p_2 \cdots p_r$.

(c) If we let $f(n) = 1/n$, then f is multiplicative which lets us write

$$\sum_{d|n} \mu(d)/d = \sum_{d|n} \mu(d)f(d) = (1-f(p_1))\cdots(1-f(p_r)) = (1-1/p_1)\cdots(1-1/p_r).$$

(d) If we let $f(n) = n$, then f is multiplicative which lets us write

$$\sum_{d|n} d\mu(d) = \sum_{d|n} \mu(d)f(d) = (1-f(p_1))\cdots(1-f(p_r)) = (1-p_1)\cdots(1-p_r).$$

5. Let $S(n)$ denote the number of square-free divisors of n. Establish that

$$S(n) = \sum_{d|n} |\mu(d)| = 2^r$$

where r is the number of distinct prime divisors of n. [*Hint:* S is a multiplicative function.]

Solution First, notice that for m and n relatively prime, we have $|\mu(mn)| = |\mu(m)\mu(n)| = |\mu(m)| \cdot |\mu(n)|$. Hence, the function $n \mapsto |\mu(n)|$ is multiplicative, and therefore, the function S is also multiplicative. Since

$$S(p^k) = \sum_{d|p^k} |\mu(d)| = |\mu(1)|+|\mu(p)|+|\mu(p^2)|+\cdots+|\mu(p^k)| = 1+|-1|+0+\cdots+0 = 2,$$

then by multiplicativity:

$$S(n) = S(p_1^{k_1})S(p_2^{k_2})\cdots S(p_r^{k_r}) = 2\cdot 2\cdots 2 = 2^r$$

where $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$.

6. Find formulas for $\sum_{d|n} \mu^2(d)/\tau(d)$ and $\sum_{d|n} \mu^2(d)/\sigma(d)$ in terms of the prime factorization of n.

Solution If we let $n = p_1^{k_1}\cdots p_r^{k_r}$, then by Exercise 3, we have

$$\begin{aligned}\sum_{d \,|\, n} \frac{\mu^2(d)}{\tau(d)} &= \left(1 - \frac{\mu(p_1)}{\tau(p_1)}\right)\cdots\left(1 - \frac{\mu(p_r)}{\tau(p_r)}\right)\\ &= \left(1+\frac{1}{2}\right)\cdots\left(1+\frac{1}{2}\right)\\ &= \left(\frac{3}{2}\right)^r.\end{aligned}$$

Similarly:

$$\begin{aligned}\sum_{d \mid n} \frac{\mu^2(d)}{\sigma(d)} &= \left(1 - \frac{\mu(p_1)}{\sigma(p_1)}\right) \cdots \left(1 - \frac{\mu(p_r)}{\sigma(p_r)}\right) \\ &= \left(1 + \frac{1}{p_1+1}\right) \cdots \left(1 + \frac{1}{p_r+1}\right) \\ &= \frac{p_1+2}{p_1+1} \cdots \frac{p_r+2}{p_r+1}.\end{aligned}$$

7. The *Liouville* λ*-function* is defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^{k_1+k_2+\cdots+k_r}$, if the prime factorization of $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. For instance, $\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+1} = (-1)^6 = 1$.

(a) Prove that λ is a multiplicative function.

(b) Given a positive integer n, verify that

$$\sum_{d \mid n} \lambda(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}$$

Solution

(a) Let m and n be integers relatively prime to each other, then the prime factorizations are $m = p_1^{k_1} \cdots p_r^{k_r}$ and $n = q_1^{t_1} \cdots q_s^{t_s}$ where the p_i's are distinct from the q_i's. Hence:

$$\lambda(mn) = (-1)^{k_1+\cdots+k_r+t_1+\cdots+t_s} = (-1)^{k_1+\cdots+k_r}(-1)^{t_1+\cdots+t_s} = \lambda(m)\lambda(n).$$

Therefore, the function is multiplicative.

(b) Since the function $F(n) = \sum_{d|n} \lambda(n)$ is multiplicative, let's first determine its value at powers of primes.

$$\sum_{d \mid p^k} \lambda(d) = \sum_{i=0}^{k} \lambda(p^i) = \sum_{i=0}^{k} (-1)^i = \frac{1+(-1)^k}{2} = \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd} \end{cases}.$$

Therefore, for any integer $n = p_1^{k_1} \cdots p_r^{k_r}$, the sum $\sum_{d|n} \lambda(n)$ will be 1 if and only if all the k_i's are even; otherwise it will be zero. But we know that n is a square if and only if all the k_i's are even; thus:

$$\sum_{d \mid n} \lambda(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}.$$

8. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, establish that $\sum_{d \mid n} \mu(d)\lambda(d) = 2^r$.

Solution Since λ is a multiplicative function, we can apply Exercise 3 to get

$$\begin{aligned}\sum_{d \,\mid\, n} \mu(d)\lambda(d) &= (1-\lambda(p_1))(1-\lambda(p_2))\cdots(1-\lambda(p_r))\\ &= (1-(-1))(1-(-1))\cdots(1-(-1))\\ &= 2\cdot 2\cdots 2\\ &= 2^r.\end{aligned}$$

6.3 The Greatest Integer Function

1. Given integers a and $b > 0$, show that there exists a unique integer r with $0 \leqslant r < b$ satisfying $a = [a/b]b + r$.

Solution First, we have that $a = qb + r$ for some integers q and r. It follows that $a/b = q + r/b$. Since $0 \leqslant r < b$, then $0 \leqslant r/b < 1$. It follows that $[a/b] = q$, and hence, that $a = [a/b]b + r$. Note that this r is unique because otherwise, it would contradict the uniqueness of the pair q, r.

2. Let x and y be real numbers. Prove that the greatest integer function satisfies the following properties:

(a) $[x + n] = [x] + n$ for any integer n.

(b) $[x] + [-x] = 0$ or -1, according as x is an integer or not. [*Hint:* Write $x = [x] + \theta$, with $0 \leqslant \theta < 1$, so that $-x = -[x] - 1 + (1 - \theta)$.]

(c) $[x] + [y] \leqslant [x + y]$ and, when x and y are positive, $[x][y] \leqslant [xy]$.

(d) $[x/n] = [[x]/n]$ for any positive integer n. [*Hint:* Let $x/n = [x/n] + \theta$, where $0 \leqslant \theta < 1$; then $[x] = n[x/n] + [n\theta]$.]

(e) $[nm/k] \geqslant n[m/k]$ for positive integers n, m, k.

(f) $[x] + [y] + [x + y] \leqslant [2x] + [2y]$. [*Hint:* Let $x = [x] + \theta$, $0 \leqslant \theta < 1$, and $y = [y] + \theta'$, $0 \leqslant \theta' < 1$. Consider cases in which neither, one, or both of θ and θ' are greater than or equal to $\frac{1}{2}$.]

Solution

(a) Since we can write $x = [x] + \theta$ for some $0 \leqslant \theta < 1$, then $x + n = k + \theta$ where $k = [x] + n$ is an integer. It follows that $[x + n] = k = [x] + n$.

(b) If x is an integer, then clearly $[x]+[-x] = x+(-x) = 0$. If x is not an integer, then we can write $x = [x]+\theta$ where $0 < \theta < 1$. Hence, $-x = -[x]-1+(1-\theta)$ which implies that $[-x] = -[x]-1$, and thus, that $[x]+[-x] = [x]-[x]-1 = -1$.

(c) Since $[x] \leqslant x$ and $[y] \leqslant y$, then $[x] + [y] \leqslant x + y$. Since $[x] + [y]$ is an integer, then it must be less than or equal to the greatest integer smaller than $x + y$, in other words, $[x] + [y] \leqslant [x + y]$.

Similarly, if x and y are positive, then $[x][y] \leqslant xy$ which implies that $[x][y] \leqslant [xy]$ using the same argument as for the sum.

(d) Since $x/n = [x/n] + \theta$ for some $0 \leqslant \theta < 1$, then $x = n[x/n] + n\theta$, and hence, $[x] = [n[x/n]+n\theta] = n[x/n]+[n\theta]$ by part (a). Dividing both sides by n gives us $[x]/n = [x/n] + [n\theta]/n$. Since $0 \leqslant [n\theta] \leqslant n\theta < n$, then $0 \leqslant [n\theta]/n < 1$, and hence, $[[x]/n] = [x/n]$.

(e) Since $[m/k] \leqslant m/k$, then $n[m/k] \leqslant nm/k$. Since $n[m/k]$ is an integer less than nm/k, then it must be less than or equal to the greatest integer smaller than nm/k. Thus, $n[m/k] \leqslant [nm/k]$.

(f) Let $x = [x] + \theta_1$ and $y = [y] + \theta_2$ where $0 \leqslant \theta_i < 1$. When $\theta_1 + \theta_2 < 1$, we have that $x + y = [x] + [y] + (\theta_1 + \theta_2)$ where $0 \leqslant \theta_1 + \theta_2 < 1$, which implies that $[x + y] = [x] + [y]$. When $1 \leqslant \theta_1 + \theta_2 < 2$, we have that $x + y = [x] + [y] + 1 + \theta$ where $0 \leqslant \theta_1 + \theta_2 - 1 < 1$, and hence, $[x + y] = [x] + [y] + 1$. In both cases, we have that $[x + y] \leqslant [x] + [y]$.

3. Find the highest power of 5 dividing 1000! and the highest power of 7 dividing 2000!.

Solution Using Theorem 6-9, we have that the highest power of 5 dividing 1000! is

$$\left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] = 200 + 40 + 8 + 1 = 249.$$

Similarly, the highest power of 7 dividing 2000! is

$$\left[\frac{2000}{7}\right] + \left[\frac{2000}{7^2}\right] + \left[\frac{2000}{7^3}\right] = 285 + 40 + 5 = 330.$$

4. For an integer $n \geqslant 0$, show that $[n/2] - [-n/2] = n$.

Solution If n is even, then $n = 2k$ which implies that

$$[n/2] - [-n/2] = k - (-k) = 2k = n.$$

If $n = 2k + 1$, then $[n/2] = [k + 1/2] = k$ and $[-n/2] = [-k - 1/2] = -k - 1$. Hence, $[n/2] - [n/2] = k - (-k - 1) = 2k + 1 = n$. Therefore, the formula holds for all n.

5.

(a) Verify that 1000! terminates in 249 zeros.

(b) For what values of n does $n!$ terminate in 37 zeros?

Solution

(a) We already showed that the highest power of 5 dividing 1000! is 249. Since $[x] \leqslant [y]$ when $x \leqslant y$, then it follows from Theorem 6-9 that the highest power of 2 dividing 1000! is higher than 249. It follows that the highest power of 10 dividing 1000! is 249, and equivalently, 1000! ends with 249 zeros.

(b) Using an argument similar to the one used in the previous part, it suffices to find the values of n such that $\sum_{k=1}^{\infty}[n/5^k] = 37$. From this formula, we get that $[n/5] \leqslant 37$, and hence, that $n \leqslant 189$. Since $n = 5^3$ gives $\sum_{k=1}^{\infty}[5^3/5^k] = 31$ which implies that $126 \leqslant n \geqslant 189$. From this range, we get that

$$\sum_{k=1}^{\infty}\left[\frac{n}{5^k}\right] = \left[\frac{n}{5}\right] + \left[\frac{n}{5^2}\right] + \left[\frac{n}{5^3}\right] = \left[\frac{n}{5}\right] + \left[\frac{n}{5^2}\right] + 1.$$

Moreover, the fact that $126 \leqslant n \leqslant 189$ implies that $5 \leqslant [n/5^2] \leqslant 7$. It follows that $[n/5] = 29$, 30, or 31, which implies that $145 \leqslant n \leqslant 160$. Checking the values of $\sum_{k=1}^{\infty}[n/5^k]$ in this range gives us that the possible values of n are $n = 150, 151, 152, 153, 154$.

6. If $n \geqslant 1$ and p is a prime, prove that

(a) $(2n)/(n!)^2$ is an even integer. [*Hint:* Use induction on n.]

(b) The exponent of the highest power of p which divides $(2n)!/(n!)^2$ is

$$\sum_{k=1}^{\infty}([2n/p^k] - 2[n/p^k]).$$

(c) In the prime factorization of $(2n)!/(n!)^2$ the exponent of any prime p such that $n < p < 2n$ is equal to 1.

Solution

(a) Simply notice that

$$\frac{(2n)!}{(n!)^2} = \frac{2n}{n} \cdot \frac{(2n-1)!}{(n-1)! \cdot n!} = 2\binom{2n-1}{n}.$$

Since $\binom{2n-1}{n}$ is an integer, then it follows that $(2n)/(n!)^2$ is an even integer.

(b) The highest exponent of p dividing $(2n)/(n!)^2$ is the highest exponent of p dividing $(2n)!$ minus the highest exponent of p dividing $(n!)^2$. Moreover, the highest exponent of p dividing $(n!)^2$ is simply twice the highest exponent of p dividing $n!$. Putting everything together and using Theorem 6-9 gives us that the highest exponent of p dividing $(2n)/(n!)^2$ is

$$\sum_{k=1}^{\infty}([2n/p^k] - 2[n/p^k]).$$

(c) When $n < p < 2n$, we get that $[2n/p] = 1$ and $[n/p] = 0$; and that $[2n/p^k] = [n/p^k] = 0$ for all $k \geqslant 2$. Hence, using part (b), we get that in the prime factorization of $(2n)!/(n!)^2$ the exponent of p is

$$\sum_{k=1}^{\infty}([2n/p^k] - 2[n/p^k]) = (1 - 2 \cdot 0) + 0 + 0 + \cdots = 1.$$

7. Let the positive integer n be written in terms of powers of the prime p so that $n = a_kp^k + \cdots + a_2p^2 + a_1p + a_0$ where $0 \leqslant a_i < p$. Show that the exponent of the highest power of p appearing in the prime factorization of $n!$ is

$$\frac{n - (a_k + \cdots + a_2 + a_1 + a_0)}{p-1}.$$

Solution Using Theorem 6-9, we have that the highest power of p dividing $n!$ is

$$\begin{aligned}
\sum_{i=1}^{\infty}\left[\frac{a_kp^k+\cdots+a_2p^2+a_1p+a_0}{p^i}\right] &= \sum_{i=1}^{k}(a_kp^{k-i}+\cdots+a_i)\\
&= \sum_{i=1}^{k}\sum_{j=i}^{k}a_jp^{j-i}\\
&= \sum_{j=1}^{k}\sum_{i=1}^{j}a_jp^{j-i}\\
&= \sum_{j=1}^{k}a_jp^j\sum_{i=1}^{j}p^{-i}\\
&= \sum_{j=1}^{k}a_jp^j\cdot\frac{1}{p}\cdot\frac{1-p^{-j}}{1-p^{-1}}\\
&= \frac{1}{p-1}\sum_{j=1}^{k}a_jp^j(1-p^{-j})\\
&= \frac{\sum_{j=1}^{k}a_jp^j-\sum_{j=1}^{k}a_j}{p-1}\\
&= \frac{(n-a_0)-(a_k+\cdots+a_2+a_1)}{p-1}\\
&= \frac{n-(a_k+\cdots+a_2+a_1+a_0)}{p-1}.
\end{aligned}$$

8.

(a) Using Problem 7, show that the exponent of the highest power of p dividing $(p^k-1)!$ is $[p^k-(p-1)k-1]/(p-1)$. [*Hint:* Recall the identity

$$p^k-1=(p-1)(p^{k-1}+\cdots+p^2+p+1).]$$

(b) Determine the highest power of 3 dividing 80! and the highest power of 7 dividing 2400!. [*Hint:* $2400=7^4-1$.]

Solution

(a) Since $p^k-1=(p-1)(p^{k-1}+\cdots+p^2+p+1)$, then it means that we can write p^k-1 as $a_{k-1}p^{k-1}+\cdots+a_1p+a_0$ where $a_i=p-1$ for all i. Hence, using Problem 7, we get that the highest power of p dividing $(p^k-1)!$ is

$$\frac{(p^k-1)-(a_{k-1}+\cdots+a_1+a_0)}{p-1}=\frac{p^k-(p-1)k-1}{p-1}.$$

(b) Since $80=3^4-1$, then part (a) tells us that the exponent of the highest power of 3 dividing 80 is $[80-2\cdot 4]/2=40-4=36$. Similarly, the exponent of the highest power of 7 dividing $2400=7^4-1$ is $[2400-6\cdot 4]/6=400-4=396$.

9. Find an integer $n \geqslant 1$ such that the highest power of 5 contained in $n!$ is 100. [*Hint:* Since the sum of the coefficients of the powers of 5 needed to express n in the base 5 is at least 1, begin by considering the equation $(n-1)/4 = 100$.]

Solution Let $a_0, a_1, ..., a_k$ be the coefficients of the base 5 expression of n, then Problem 7 tells us that n must satisfy the equation $n - (a_k + \cdots + a_1 + a_0) = 400$. If the sum the a_i's is 1, then $n = 401$ which is a contradiction since 401 is not a power of 5. If the sum of the a_i's is 2, then $n = 402 = 3 \cdot 5^2 + 1 \cdot 5^2 + 0 \cdot 5 + 2$ which doesn't satisfy the condition that the sum of the coefficients is 2. Similarly, the sum of the coefficients cannot be 3 or 4 because $403 = 3 \cdot 5^2 + 1 \cdot 5^2 + 0 \cdot 5 + 3$ and $404 = 3 \cdot 5^2 + 1 \cdot 5^2 + 0 \cdot 5 + 4$. Next, if the sum of the coefficients is 5, then $n = 405 = 3 \cdot 5^2 + 1 \cdot 5^2 + 1 \cdot 5 + 0$ which is consistent with the fact that the sum of the coefficients is 5. Indeed, by Problem 7, we have that the highest power of 5 dividing $405! = (3 \cdot 5^2 + 1 \cdot 5^2 + 1 \cdot 5)!$ is

$$\frac{405 - (3+1+1)}{4} = \frac{400}{4} = 100.$$

Therefore, it holds for $n = 405$.

10. Given a positive integer N, show that

(a) $\sum_{n=1}^{N} \mu(n)[N/n] = 1$;

(b) $|\sum_{n=1}^{N} \mu(n)/n| \leqslant 1$.

Solution

(a) Let $F(n) = \sum_{d \mid n} \mu(d)$, then we know that $F(1) = 1$ and $F(n) = 0$ for all $n \geqslant 2$ (Theorem 6-6). Thus, by Theorem 6-11:

$$\sum_{n=1}^{N} \mu(n) \left[\frac{N}{n}\right] = \sum_{n=1}^{N} F(n) = 1.$$

(b) For all $n \leqslant N$, define $\theta_n = N/n - [N/n]$, then $0 \leqslant \theta_n < 1$, and $\theta_1 = 0$. Hence, using part (a):

$$\begin{aligned}\left|\sum_{n=1}^{N} \mu(n)\frac{N}{n}\right| &= \left|\sum_{n=1}^{N} \mu(n)\left(\left[\frac{N}{n}\right] + \theta_n\right)\right| \\ &= \left|\sum_{n=1}^{N} \mu(n)\left[\frac{N}{n}\right] + \sum_{n=1}^{N} \mu(n)\theta_n\right| \\ &= \left|1 + \sum_{n=2}^{N} \mu(n)\theta_n\right| \\ &\leqslant 1 + \sum_{n=2}^{N} |\mu(n)\theta_n| \\ &\leqslant 1 + \sum_{n=2}^{N} 1 \\ &= N.\end{aligned}$$

Thus, we have shown that

$$\left|\sum_{n=1}^{N} \mu(n)\frac{N}{n}\right| \leqslant N.$$

Dividing both sides by N gives us the desired inequality.

11. Illustrate Problem 10 in the case $N = 6$.

Solution

(a)

$$\begin{aligned}
&\sum_{n=1}^{6} \mu(n)\left[\frac{6}{n}\right] \\
&= \mu(1)\left[\frac{6}{1}\right] + \mu(2)\left[\frac{6}{2}\right] + \mu(3)\left[\frac{6}{3}\right] + \mu(4)\left[\frac{6}{4}\right] + \mu(5)\left[\frac{6}{5}\right] + \mu(6)\left[\frac{6}{6}\right] \\
&= 1 \cdot 6 + (-1) \cdot 3 + (-1) \cdot 2 + 0 \cdot 1 + (-1) \cdot 1 + 1 \cdot 1 \\
&= 6 - 3 - 2 - 1 + 1 \\
&= 1.
\end{aligned}$$

(b)

$$\begin{aligned}
\sum_{n=1}^{6} \frac{\mu(n)}{n} &= \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(5)}{5} + \frac{\mu(6)}{6} \\
&= 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{6} \\
&= \frac{2}{15}.
\end{aligned}$$

12. Verify that the formula

$$\sum_{n=1}^{N} \lambda(n)[N/n] = [\sqrt{N}]$$

holds for any positive integer N. [*Hint:* Apply Theorem 6-11 to the multiplicative function $F(n) = \sum_{d \mid n} \lambda(d)$, noting that there are $[\sqrt{N}]$ perfect squares not exceeding n.]

Solution Recall that if we define $F(n) = \sum_{d \mid n} \lambda(d)$, then $F(n)$ is equal to 1 if and only if n is a square, otherwise $F(n) = 0$. Thus, by Theorem 6-11:

$$\sum_{n=1}^{N} \lambda(n)[N/n] = \sum_{n=1}^{N} F(n) = [\sqrt{N}]$$

using the fact that there are $[\sqrt{N}]$ squares between 1 and N.

13. If N is a positive integer, establish that

(a) $N = \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^{N}[2N/n]$;

(b) $\tau(N) = \sum_{n=1}^{N}([N/n] - [(N-1)/n])$.

Solution

(a) Using Corollary 1, we have that

$$\sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^{N} \left[\frac{2N}{n}\right] = \sum_{n=1}^{2N} \left[\frac{2N}{n}\right] - \sum_{n=1}^{N} \left[\frac{2N}{n}\right] = \sum_{n=N+1}^{2N} \left[\frac{2N}{n}\right].$$

Next, we have that for all $N+1 \leqslant n \leqslant 2N$, $[2N/n] = 1$, and hence:

$$\sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^{N} \left[\frac{2N}{n}\right] = \sum_{n=N+1}^{2N} \left[\frac{2N}{n}\right] = \sum_{n=N+1}^{2N} 1 = N.$$

(b) Using Corollary 1:

$$\begin{aligned}\sum_{n=1}^{N} \left(\left[\frac{N}{n}\right] - \left[\frac{N_1}{n}\right]\right) &= \sum_{n=1}^{N} \left[\frac{N}{n}\right] - \sum_{n=1}^{N} \left[\frac{N-1}{n}\right] \\ &= \sum_{n=1}^{N} \tau(n) - \sum_{n=1}^{N-1} \left[\frac{N-1}{n}\right] - \left[\frac{N-1}{N}\right] \\ &= \sum_{n=1}^{N} \tau(n) - \sum_{n=1}^{N-1} \tau(n) - 0 \\ &= \tau(N).\end{aligned}$$

Chapter 7

Euler's Generalization of Fermat's Theorem

7.1 Leonhard Euler

There are no exercices in this section.

7.2 Euler's Phi-Function

1. Calculate $\phi(1001)$, $\phi(5040)$, and $\phi(36,000)$.

Solution Since $1001 = 7 \cdot 11 \cdot 13$, then

$$\phi(1001) = \phi(7)\phi(11)\phi(13) = 6 \cdot 10 \cdot 12 = 720.$$

Since $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, then

$$\phi(5040) = 2^3(2-1) \cdot 3(3-1) \cdot (5-1) \cdot (7-1) = 1152.$$

Since $36,000 = 2^5 \cdot 3^2 \cdot 5^3$, then

$$\phi(36,000) = 2^4(2-1) \cdot 3(3-1) \cdot 5^2(5-1) = 9600.$$

2. Verify that the equality $\phi(n) = \phi(n+1) = \phi(n+2)$ holds when $n = 5186$.

Solution When $n = 5186$, we have $n = 2 \cdot 2593$, $n+1 = 3 \cdot 7 \cdot 13 \cdot 19$, and $n+2 = 2^2 \cdot 1297$. Hence:

$$\begin{aligned}\phi(n) &= (2-1)(2593-1) = 2592\\ \phi(n+1) &= (3-1)(7-1)(13-1)(19-1) = 2592\\ \phi(n+2) &= 2(2-1)(1297-1) = 2592.\end{aligned}$$

3. Show that the integers $m = 3^k \cdot 568$ and $n = 3^k \cdot 638$, where $k \geqslant 0$, satisfy simultaneously

$$\tau(m) = \tau(n),\ \sigma(m) = \sigma(n),\ \phi(m) = \phi(n).$$

Solution Since $m = 2^3 \cdot 3^k \cdot 71$ and $n = 2 \cdot 3^k \cdot 11 \cdot 29$, then

$$\begin{aligned}
\tau(m) &= (3+1)(k+1)(1+1) = (1+1)(k+1)(1+1)(1+1) = \tau(n) \\
\sigma(m) &= (1+2+2^2+2^3)\sigma(3^k)(1+71) = 1080\sigma(3^k) = (1+2)\sigma(3^k)(1+11)(1+29) = \sigma(n) \\
\phi(m) &= 2^2(2-1)\phi(3^k)(71-1) = 280\phi(3^k) = (2-1)\phi(3^k)(11-1)(29-1) = \sigma(n)
\end{aligned}$$

which proves the claim.

4. Establish each of the assertions below:

(a) If n is an odd integer, then $\phi(2n) = \phi(n)$.

(b) If n is an even integer, then $\phi(2n) = 2\phi(n)$.

(c) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.

(d) $\phi(3n) = 2\phi(n)$ if and only if $3 \ \mid n$.

(e) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geqslant 1$. [*Hint:* Write $n = 2^k N$, where N is odd, and use the condition $\phi(n) = n/2$ to show that $N = 1$.]

Solution

(a) If n is odd, then $\gcd(2, n) = 1$, and so it follows that $\phi(2n) = \phi(2)\phi(n) = \phi(n)$.

(b) If n is even, then we can write $n = 2^k m$ where $k \geqslant 1$ and m such that $\gcd(2, m) = 1$. Hence, by multiplicativity:

$$\phi(2n) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m) = 2^k\phi(m) = 2\phi(2^k)\phi(m) = 2\phi(n).$$

(c) Write $n = 3^k m$ where $\gcd(3, m) = 1$. If $3 \mid n$, then $k \geqslant 1$ which implies that $3^k(3-1) = 3 \cdot 3^{k-1}(3-1)$, and hence, that $\phi(3^{k+1})\phi(m) = 3\phi(3^k)\phi(m)$. Equivalently, this means that $\phi(3n) = 3\phi(n)$. Conversely, if $3 \ \mid n$, then $k = 0$, and hence, $\phi(3n) = \phi(3)\phi(n) = 2\phi(n) \neq 3\phi(n)$.

(d) We showed in the previous part that $3 \ \| \ n$ implies that $\phi(3n) = 2\phi(n)$. Conversely, when $3 \mid n$, we know that $\phi(3n) = 3\phi(n)$, and hence, $\phi(3n) \neq 2\phi(n)$.

(e) If $n = 2^k$ for some $k \geqslant 1$, then

$$\phi(n) = \phi(2^k) = 2^{k-1} = n/2.$$

Conversely, suppose that $\phi(n) = n/2$ and write $n = p_1^{k_1} \cdots p_r^{k_r}$, then we can rewrite the equation as

$$n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \frac{n}{2}.$$

Rearranging the equation gives us

$$2(p_1 - 1) \cdots (p_r - 1) = p_1 \cdots p_r.$$

Since the left hand side is even, then one of the primes in the right hand side must be 2, and hence, $p_1 = 2$. The equation becomes

$$(p_2 - 1) \cdots (p_r - 1) = p_2 \cdots p_r.$$

But this equation is impossible (the left hand side is clearly strictly less than the right hand side) when $r \geqslant 2$, if $r = 1$, this equation is simply $1 = 1$. Hence, $r = 1$, and hence, $n = p_1^{k_1} = 2^{k_1}$ for some $k_1 \geqslant 1$.

5. Prove that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $2p-1$ are both odd primes.

Solution Simply notice that

$$\phi(n) = \phi(2)\phi(2p-1) = 2p - 2$$

and

$$\phi(n+2) = \phi(4p) = \phi(4)\phi(p) = 2(p-1).$$

Hence, it follows that $\phi(n) = \phi(n+2)$.

6. Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square. [*Hint:* Consider the integers $n = 2^{k+1}$ for $k = 1, 2, \ldots$.]

Solution Let k be an arbitrary integer and $n = 2^{2k+1}$, then $\phi(n) = 2^{2k} = (2^k)^2$. Since $(2^k)^2 \neq (2^q)^2$ for $k \neq q$, then there are infinitely many n such that $\phi(n)$ is a square since there are infinitely many k's.

7. Verify the following:

(a) For any positive integer n, $\frac{1}{2}\sqrt{n} \leqslant \phi(n) \leqslant n$. [*Hint:* Write $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, so $\phi(n) = 2^{k_0-1} p_1^{k_1-1} \cdots p_r^{k_r-1}(p_1 - 1) \cdots (p_r - 1)$. Now, use the inequalities $p - 1 > \sqrt{p}$ and $k - \frac{1}{2} \geqslant k/2$ to obtain $\phi(n) \geqslant 2^{k_0-1} p_1^{k_1/2} \cdots p_r^{k_r/2}$.]

(b) If the integer $n > 1$ has r distinct prime factors, then $\phi(n) \geqslant n/2^r$.

(c) If $n > 1$ is a composite number, then $\phi(n) \leqslant n - \sqrt{n}$. [*Hint:* Let p be the smallest prime divisor of n, so that $p \leqslant \sqrt{n}$. Then $\phi(n) \leqslant n(1 - 1/p)$.]

Solution

(a) Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = 2^{k_0-1} p_1^{k_1-1} \cdots p_r^{k_r-1}(p_1 - 1) \cdots (p_r - 1)$. Since $(p_i - 1) \geqslant \sqrt{p_i}$, then we get that $\phi(n) \geqslant \frac{1}{2} \cdot 2^{k_0} p_1^{k_1 - \frac{1}{2}} \cdots p_r^{k_r - \frac{1}{2}}$. Next, since $k_0 \geqslant k_0/2$ and $k_i - \frac{1}{2} \geqslant k_i/2$, then $\phi(n) \geqslant \frac{1}{2} 2^{k_0/2} p_1^{k_1/2} \cdots p_r^{k_r} = \frac{1}{2}\sqrt{n}$. Finally, the inequality $\phi(n) \leqslant n$ follows from the definition of ϕ.

(b) Let $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$\frac{n}{\phi(n)} = \frac{n}{n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)} = \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1} \leqslant 2^r$$

which we can rearrange into $\phi(n) \geqslant n/2^r$.

(c) Let p be a prime dividing n, since n is composite, then $p \leqslant \sqrt{n}$, hence, $p\sqrt{n} \leqslant n$. It follows that the numbers p, $2p$, ..., $\lfloor\sqrt{n}\rfloor p$ are all less than n, and not relatively prime to n. There are $\lfloor\sqrt{n}\rfloor$ such numbers. If we let q be a second prime divisor of n (if n is a power of p, then the statement is clear from the formula for $\phi(p^k)$ and the inequality $k - 1 \geqslant k/2$ for $k \geqslant 2$), then we know that q is a number distinct from p, $2p$, ..., $\lfloor\sqrt{n}\rfloor$ that is not relatively prime to n. Hence, we have found $\lfloor\sqrt{n}\rfloor + 1$ numbers less than n which are not relatively prime to it. Therefore, $\phi(n) \leqslant n-(\lfloor\sqrt{n}\rfloor+1) \leqslant n-\sqrt{n}$.

8. Prove that if the integer n has r distinct odd prime factors, then $2^r \mid \phi(n)$.

Solution Write $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ where $k_0 \geqslant 0$ and $k_i \geqslant 1$ for $1 \leqslant i \leqslant r$, then

$$\phi(n) = \phi(2^{k_0}) p_1^{k_1 - 1} \cdots p_r^{k_r - 1} (p_1 - 1) \cdots (p_r - 1).$$

Since all the factors $p_i - 1$ are even, and there are r such factors, then 2^r divides $\phi(n)$.

9. Prove that:

(a) If n and $n + 2$ are a pair of twin primes, then $\phi(n + 2) = \phi(n) + 2$; this also holds for $n = 12$, 14, and 20.

(b) If p and $2p + 1$ are both odd primes, then $n = 4p$ satisfies $\phi(n + 2) = \phi(n) + 2$.

Solution

(a) For any prime p, we have that $\phi(p) = p - 1$. It follows that

$$\phi(n + 2) = n + 1 = (n - 1) + 2 = \phi(n) + 2$$

when both n and $n + 2$ are prime. When $n = 12$:

$$\phi(n + 2) = \phi(2)\phi(7) = 6 = \phi(2^2)\phi(3) + 1 = \phi(n) + 2.$$

When $n = 14$:

$$\phi(n + 2) = \phi(2^4) = 8 = \phi(2)\phi(7) + 2 = \phi(n) + 2.$$

When $n = 20$:

$$\phi(n + 2) = \phi(2)\phi(11) = 10 = \phi(2^2)\phi(5) + 2 = \phi(n) + 2.$$

(b) Suppose that p and $2p+1$ are odd primes, then for $n = 4p$, we have

$$\phi(n+2) = \phi(4p+2) = \phi(2)\phi(2p+1) = 2p$$

and

$$\phi(n) + 2 = \phi(4p) + 2 = \phi(4)\phi(p) + 2 = 2(p-1) + 2 = 2p$$

which proves that $\phi(n+2) = \phi(n) + 1$.

10. If every prime that divides n also divides m, establish that $\phi(nm) = n\phi(m)$; in particular, $\phi(n^2) = n\phi(n)$ for every positive integer n.

Solution Write $n = p_1^{k_1} \cdots p_r^{k_r}$ and $m = p_1^{t_1} \cdots p_r^{t_r} q_1^{s_1} \cdots q_u^{s_u}$, then

$$\begin{aligned}
\phi(nm) &= \phi(p_1^{k_1+t_1} \cdots p_r^{k_r+t_r} q_1^{s_1} \cdots q_u^{s_u}) \\
&= p_1^{k_1+t_1-1}(p_1 - 1) \cdots p_r^{k_r+t_r-1}(p_r - 1)\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= [p_1^{k_1} \cdots p_r^{k_r}] \cdot p_1^{t_1-1}(p_1 - 1) \cdots p_r^{t_r-1}(p_r - 1)\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= n\phi(p_1^{t_1} \cdots p_r^{t_r})\phi(q_1^{s_1} \cdots q_u^{s_u}) \\
&= n\phi(m).
\end{aligned}$$

11.

(a) If $\phi(n) \mid n-1$, prove that n is a square-free integer. [*Hint:* Assume that n has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $k_1 \geqslant 2$. Then $p_1 \mid \phi(n)$, whence $p_1 \mid n-1$, which leads to a contradiction.]

(b) Show that if $n = 2^k$ or $n = 2^k 3^j$, with k and j positive integers, then $\phi(n) \mid n$.

Solution

(a) Let p be a prime divisor of n and let k be the exponent of p in the prime factorization of n, then $\phi(n) = \phi(p^k)\phi(n/p^k) = p^{k-1}(p-1)\phi(n/p^k)$. When $k \geqslant 2$, we have that $p \mid \phi(n)$ using the expression above, but since $\phi(n) \mid n-1$, then $p \mid n-1$. This is impossible because $p \mid n$. Thus, $k = 1$, and hence, n is square-free.

(b) Let $n = 2^k 3^k$ with $k \geqslant 1$. If $j = 0$, then $\phi(n) = 2^{k-1} \mid 2^k = n$. When $j \geqslant 1$, we get $\phi(n) = 2^{k-1} 3^{j-1}(3-1) = 2^k 3^{j-1} \mid 2^k 3^j = n$.

12. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, derive the inequalities

(a) $\sigma(n)\phi(n) \geqslant n^2(1 - 1/p_1^2)(1 - 1/p_2^2) \cdots (1 - 1/p_r^2)$ and

(b) $\tau(n)\phi(n) \geqslant n$. [*Hint:* Show that $\tau(n)\phi(n) \geqslant 2^r \cdot n(1/2)^r$.]

Solution

(a) First, notice that

$$\begin{aligned}\sigma(n) &= (1+\cdots+p_1^{k_1-1}+p_1^{k_1})\cdots(1+\cdots+p_r^{k_r-1}+p_r^{k_r})\\ &\geqslant (p_1^{k_1}+p_1^{k_1-1})\cdots(p_r^{k_r}+p_r^{k_r-1})\\ &= p_1^{k_1}\cdots p_r^{k_r}(1+1/p_1)\cdots(1+1/p_r)\\ &= n(1+1/p_1)\cdots(1+1/p_r).\end{aligned}$$

Multiplying the resulting inequality by

$$\phi(n) = n(1-1/p_1)\cdots(1-1/p_r)$$

gives us

$$\sigma(n)\tau(n) \geqslant n^2(1-1/p_1^2)\cdots(1-1/p_r^2).$$

(b) Since

$$\begin{aligned}\tau(n) &= (k_1+1)(k_2+1)\cdots(k_r+1)\\ &\geqslant \left(1-\frac{1}{p_1}\right)^{-1}\left(1-\frac{1}{p_2}\right)^{-1}\cdots\left(1-\frac{1}{p_r}\right)^{-1}\\ &= \frac{n}{\phi(n)},\end{aligned}$$

then $\tau(n)\phi(n) \geqslant n$.

13. Assuming that $d \mid n$, prove that $\phi(d) \mid \phi(n)$. [*Hint:* Work with the prime factorizations of d and n.]

Solution Let $d = p_1^{k_1}\cdots p_r^{k_r}$ and $n = p_1^{t_1}\cdots p_r^{t_r}q_1^{s_1}\cdots q_u^{s_u}$ with $k_i \leqslant t_i$, then $p_i^{k_i-1} \mid p_i^{t_i-1}$. It follows that $\prod_{i=1}^r p_i^{k_i-1} \mid \prod_{i=1}^r p_i^{t_i-1}$. Using the rules of divisibility, we get that $\phi(d)$, which is equal to $\prod_{i=1}^r p_i^{k_i-1}(p_i-1)$ divides $\prod_{i=1}^r p_i^{t_i-1}(p_i-1)$, which in turns divides $\prod_{i=1}^r p_i^{t_i-1}(p_i-1)\prod_{i=1}^u q_i^{s_i-1}(q_i-1) = \phi(n)$. Therefore, $\phi(d) \mid \phi(n)$.

14. Obtain the following two generalizations of Theorem 7-2:

(a) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(mn)\phi(d)/d,$$

where $d = \gcd(m,n)$.

(b) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(\gcd(m,n))\phi(\operatorname{lcm}(m,n)).$$

Solution

(a) Let $m = p_1^{k_1} \cdots p_r^{k_r} a$ and $n = p_1^{t_1} \cdots p_r^{t_r} b$ where the p_i's are the prime common to m and n, and where a and b are prime relative to the p_i's, then $d = \gcd(m,n)$ is also formed of the primes p_1, ..., p_r. It follows that

$$\begin{aligned}
\phi(mn)\frac{\phi(d)}{d} &= \phi\left(ab\prod_i p_i^{k_i+t_i}\right)\prod_i\left(1-\frac{1}{p_i}\right) \\
&= \phi(a)\phi(b)\prod_i p_i^{k_i+t_i-1}(p_i-1)\prod_i\frac{p_i-1}{p_i} \\
&= \left[\phi(a)\prod_i p_i^{k_i-1}(p_i-1)\right]\left[\phi(b)\prod_i p_i^{t_i-1}(p_i-1)\right] \\
&= \phi(m)\phi(n).
\end{aligned}$$

(b) First, recall that $mn = \gcd(m,n)\operatorname{lcm}(m,n)$. Moreover, since $\gcd(m,n) \mid mn$, then

$$\phi(mn) = \gcd(m,n)\phi\left(\frac{mn}{\gcd(m,n)}\right) = \gcd(m,n)\phi(\operatorname{lcm}(m,n))$$

by Problem 10. Therefore, using part (a):

$$\phi(m)\phi(n) = \phi(mn)\frac{\phi(\gcd(m,n))}{\gcd(m,n)} = \phi(\gcd(m,n))\phi(\operatorname{lcm}(m,n)).$$

15. Prove that:

(a) There are infinitely many integers n for which $\phi(n) = n/3$. [*Hint:* Consider $n = 2^k 3^j$, where k and j are positive integers.]

(b) There are no integers n for which $\phi(n) = n/4$.

Solution

(a) For all positive integers k and j, if we let $n = 2^k 3^j$, then

$$\phi(n) = \phi(2^k)\phi(3^j) = 2^{k-1}3^{j-1}(3-1) = \frac{2^k 3^j}{3} = \frac{n}{3}.$$

Since there infinitely many integers of the form $2^k 3^j$, then there are infinitely many integers n such that $\phi(n) = n/3$.

(b) Suppose that there exists an integer $n = p_1^{k_1} \cdots p_r^{k_r}$ such that $\phi(n) = n/4$, then equivalently:

$$4p_1^{k_1-1}(p_1-1)\cdots p_r^{k_r-1}(p_r-1) = p_1^{k_1}\cdots p_r^{k_r}$$

which we can rewrite as

$$4(p_1-1)\cdots(p_r-1) = p_1\cdots p_r.$$

Since 2 divides the left hand side, then 2 divides $p_1 \cdots p_r$ which implies that $p_i = 2$ for some $1 \leqslant i \leqslant r$. Without loss of generality, we can assume that $p_1 = 2$. If we cancel out p_1 and 2 on both sides, we get the equivalent equation

$$2(p_1 - 1) \cdots (p_r - 1) = p_2 \cdots p_r.$$

Applying the same argument as before ensures that $p_i = 2$ for some $2 \leqslant i \leqslant r$, but it would imply that $p_i = p_1$ with $i \neq 1$. This is impossible because the p_i's are distinct from each other. Therefore, by contradiction, there is no integer n such that $\phi(n) = n/4$.

16. Show that Goldbach's Conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\phi(n_1) + \phi(n_2) = 2n$.

Solution By Goldbach's Conjecture, we know that there exist prime numbers p and q such that $p + q = 2n + 2$. Hence:

$$\phi(p) + \phi(q) = (p - 1) + (q - 1) = 2n + 2 - 2 = 2n.$$

17. Given a positive integer k, show that

(a) there are at most a finite number of integers n for which $\phi(n) = k$;

(b) if the equation $\phi(n) = k$ has a unique solution, say $n = n_0$, then $4 \mid n_0$. [*Hint:* See Problem 4(a) and 4(b).]

A famous conjecture of Carmichael is that the number of solutions of $\phi(n) = k$ cannot be equal to one.

Solution

(a) Since $\phi(n) \geqslant \frac{1}{2}\sqrt{n}$ for all n, then $\phi(n) > k$ for all $n > 4k^2$. Hence, all the solutions of the equation $\phi(n) = k$ must be less than $4k^2$ which implies that there are only finitely many possible solutions.

(b) Write $n_0 = 2^k m$ where m is odd. If $k = 0$, then $\phi(2n_0) = \phi(2)\phi(n_0) = \phi(n_0) = k$, and hence, $2n_0$ is also a solution. This is impossible since $2n_0 \neq n_0$. Similarly, if $k = 1$, then $\phi(m) = \phi(2)\phi(m) = \phi(2m) = \phi(n_0) = k$. Again, this is impossible since $m \neq n_0$. Therefore, $k \geqslant 2$, and hence, $4 \mid n_0$.

18. Find all solutions of $\phi(n) = 16$ and $\phi(n) = 24$. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ satisfies $\phi(n) = k$, then $n = [k/\prod(p_i - 1)] \prod p_i$. Thus, then integers $d_i = p_i - 1$ can be determined by the conditions (1) $d_i \mid k$, (2) $d_i + 1$ is prime and (3) $k/\prod d_i$ contains no prime factor not in $\prod p_i$.]

Solution Write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $\phi(n) = 16$ implies that $\prod p_i^{k_i - 1}(p_i - 1) = 16$. Equivalently, dividing both sides by $\prod(p_i - 1)$ and then multiplying both sides by $\prod p_i$ gives us $n = [16/\prod(p_i - 1)] \prod p_i$. It follows that $p_i - 1$ divide 16 for all i, and hence, $p_i - 1 = 1, 2, 4, 8, 16$. Thus, $p_i = 2, 3, 5, 9, 17$ but $p_i = 9$ is impossible since p_i is prime. Thus, the possible prime factors of n are 2,3, 5, and 17. If n is divisible by 17, then $n = 17^k m$ where m is not divisible by 17, and hence, $\phi(n) = 16$ becomes $17^{k-1} \cdot 16 \cdot \phi(m) = 16$ which implies that $k = 1$ and $m = 1, 2$. Thus, either $n = 17, 34$, or n is only composed of 2, 3, and 5. When n is composed of 2, 3, and 5, then $\prod(p_i - 1) < 16$, and hence, $2 \mid 16/\prod(p_i - 1)$. Since $n = [16/\prod(p_i - 1)]\prod p_i$, then $2 \mid n$ so 2 must be a prime factor of n. If $n = 2^k$, then $\phi(n) = 16$ implies that $n = 32$; if $n = 2^k 3^j$, then $\phi(n) = 16$ implies that $n = 48$; if $n = 2^k 5^t$, then $\phi(n) = 16$ implies that $n = 40$; if $n = 2^k 3^j 5^t$, then $\phi(n) = 16$ implies that $n = 60$. Therefore, the solutions to the equation $\phi(n) = 16$ are $n = 17, 32, 34, 40, 48, 60$.

Next, let's solve the equation $\phi(n) = 24$. As we did in the first part, we have that $n = [24/\prod(p_i - 1)]\prod p_i$. Hence, the prime divisors of n satisfy $p_i - 1 \mid 24$, and hence, p_i must be equal to one of 2, 3, 5, 7, and 13. If $13 \mid n$, then $n = 13^k m$ with $\gcd(13, m) = 1$, and hence, $\phi(n) = 24$ implies that $\phi(m) \cdot 13^{k-1} \cdot 12 = 24$. Thus, $k = 1$ and $\phi(m) = 2$. Hence, m is either 3, 4, or 6. Thus, n can be 39, 52, or 78. Now, if n is not divisible by 13, then n can only be composed of 2, 3, 5, or 7. If n is divisible by 7, then $n = 7^k m$ with $\gcd(7, m) = 1$. In that case, $\phi(n) = 24$ becomes $7^{k-1} \cdot 6\phi(m) = 24$ which implies that $k = 1$ and $\phi(m) = 4$. Thus, $m = 5, 8, 10, 12$ which implies that $n = 35, 56, 70, 84$. Now, if n is not divisible by 7 either, then $n = 3^2 m$ with $\gcd(3, m) = 1$, otherwise, $\phi(n)$ would not be divisible by 3 or would contain too much factors of 3. Hence, we have the following cases: if $n = 2^k 3^2$, then $\phi(n) = 24$ implies that $n = 72$; if $n = 3^2 5^t$, then $\phi(n) = 24$ implies that $n = 45$, if $n = 2^k 3^2 5^t$, then $\phi(n) = 24$ shows that $n = 90$. Therefore, $n = 35, 39, 45, 52, 56, 70, 72, 78, 84, 90$.

19.

(a) Prove that the equation $\phi(n) = 2p$, where p is a prime number and $2p + 1$ is composite, is not solvable.

(b) Prove that there is no solutions to the equation $\phi(n) = 14$, and that 14 is the smallest (positive) even integer with this property.

Solution

(a) Write $n = p_1^{k_1} \cdots p_r^{k_r}$ and suppose that $\phi(n) = 2p$, then

$$p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1) = 2p$$

which implies that n must have at most one odd prime divisor (since p is prime with $2p + 1$ composite, then $p \neq 2$ and so there is only one factor of 2 on both sides of these equations). It follows that n is either a power of 2, a power of an odd prime q, or a number of the form $2^k q^j$ with $k, j \geqslant 1$. Since p is odd, then $2p$ is not a power of 2, and hence, $\phi(n) \neq 2p$. If $n = q^j$, then $q^{j-1}(q - 1) = 2p$. If $q - 1 = 2$, then $q = 3$ and so $3^{j-1} = p$ which implies that $p = q = 3$. But this is impossible since $2p + 1$ is composite while $2 \cdot 3 + 1 = 7$ is prime; hence, $q > 3$. Since $q - 1 \neq 2$, then it must contain at most two prime factors distinct from q (it cannot be a power of two higher than 2 since there is only one factor of 2 on the right hand side of the equation). In that case, since there are only two prime factors on the right hand side, then $q^{j-1} = 1$

and so $q-1=2p$ which implies that $q=2p+1$, a contradiction since $2p+1$ is composite while q is prime; hence, $n \neq q^j$ for some odd prime q. Finally, if $n=2^k q^j$, then $2^{k-1}q^{j-1}(q-1)=2p$. By the same considerations as before, $k=1$ which implies that $q^{j-1}(q-1)=2p$. But this is exactly the same equation as above which lead to a contradiction. Thus, this last case is also impossible. Therefore, the equation $\phi(n)=2p$ has no solutions.

(b) Since $14=2\cdot 7$ and $2\cdot 7+1=15$ is composite, then $\phi(n)=14$ has no solutions. This is the smallest such positive even number because $\phi(n)=12$ has the solution $n=36$, $\phi(n)=10$ has the solution $n=5$, $\phi(n)=8$ has the solution $n=16$, $\phi(n)=6$ has the solution $n=9$, $\phi(n)=4$ has the solution $n=8$, and $\phi(n)=2$ has the solution $n=4$. Therefore, 14 is the smallest positive even number with the property that $\phi(n)=14$ has no solutions.

20. If p is a prime and $k \geqslant 2$, show that $\phi(\phi(p^k))=p^{k-2}\phi((p-1)^2)$.

Solution By the usual rules and by Problem 10, we have

$$\begin{aligned}\phi(\phi(p^k)) &= \phi(p^{k-1}(p-1))\\ &= \phi(p^{k-1})\phi(p-1)\\ &= p^{k-2}(p-1)\phi(p-1)\\ &= p^{k-2}\phi((p-1)^2).\end{aligned}$$

7.3 Euler's Theorem

1. Use Euler's Theorem to establish the following:

(a) For any integer a, $a^{37} \equiv a \pmod{1729}$. [*Hint:* $1729 = 7 \cdot 13 \cdot 19$.]

(b) For any integer a, $a^{13} \equiv a \pmod{2730}$. [*Hint:* $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.]

(c) For any odd integer a, $a^{33} \equiv a \pmod{4080}$. [*Hint:* $4080 = 15 \cdot 16 \cdot 17$.]

Solution

(a) Let a be an integer not divisible by 7, then $a^6 \equiv 1 \pmod 7$ (Euler's Theorem). Taking both sides to the power of 6 gives us $a^{36} \equiv 1 \pmod 7$. Multiplying both sides by a gives us $a^{37} \equiv a \pmod 7$ which now holds for any integer a. Next, let a be an integer not divisible by 13, then $a^{12} \equiv 1 \pmod{13}$ (Euler's Theorem). Taking both sides to the power of 3 gives us $a^{36} \equiv 1 \pmod{13}$. Multiplying both sides by a gives us $a^{37} \equiv a \pmod{13}$ which now holds for any integer a. Finally, if we let a be an integer not divisible by 19, then $a^{18} \equiv 1 \pmod{19}$ (Euler's Theorem). Squaring both sides gives us $a^{36} \equiv 1 \pmod{19}$. Multiplying both sides by a gives us $a^{37} \equiv a \pmod{19}$ which now holds for any integer a. Therefore, for any integer a, we have the three congruences $a^{37} \equiv a \pmod 7$, $a^{37} \equiv a \pmod{13}$, and $a^{37} \equiv a \pmod{19}$. Since 7, 13, and 19 have no common divisor, then $a^{37} \equiv a \pmod{1729}$.

(b) For any odd integer a, we have $a^1 \equiv 1 \pmod 2$. Taking both sides to the power of 12 and multiplying both sides by a gives us $a^{13} \equiv a \pmod 2$ which holds for all integers a. For any integer a not divisible by 3, we have $a^2 \equiv 1 \pmod 3$. Taking both sides to the power of 6 and multiplying both sides by a gives us $a^{13} \equiv a \pmod 3$ which holds for all integers a. For any integer a not divisible by 5, we have $a^4 \equiv 1 \pmod 5$. Taking both sides to the power of 3 and multiplying both sides by a gives us $a^{13} \equiv a \pmod 5$ which holds for all integers a. For any integer a not divisible by 7, we have $a^6 \equiv 1 \pmod 7$. Taking both sides to the power of 2 and multiplying both sides by a gives us $a^{13} \equiv a \pmod 7$ which holds for all integers a. Finally, for any integer a, we have $a^{13} \equiv 1 \pmod{13}$. Therefore, $a^{13} \equiv a \pmod{2730}$.

(c) For any integer a not divisible by 3, we have $a^2 \equiv 1 \pmod 3$. Taking both sides to the power of 16 and multiplying both sides by a gives us $a^{33} \equiv a \pmod 3$ which holds for all integers a. For any integer a not divisible by 5, we have $a^4 \equiv 1 \pmod 5$. Taking both sides to the power of 8 and multiplying both sides by a gives us $a^{33} \equiv a \pmod 5$ which holds for all integers a. For any integer a not divisible by 17, we have $a^{16} \equiv 1 \pmod{17}$. Squaring and multiplying both sides by a gives us $a^{33} \equiv a \pmod{17}$ which holds for all integers a. Finally, using Euler's Theorem, we have that $a^8 \equiv 1 \pmod{16}$ for all even integers a. Taking both sides to the power of 4 and multiplying both sides by a gives us $a^{33} \equiv a \pmod{16}$. Hence, for all even integers a, we have $a^{33} \equiv a \pmod{4080}$.

2. Use Euler's Theorem to confirm that, for any integer $n \geqslant 0$,

$$51 \mid 10^{32n+9} - 7.$$

Solution Since $51 = 3 \cdot 17$, then $\phi(51) = 2 \cdot 16 = 32$. Since $\gcd(10, 51) = 1$, then by Euler's Theorem: $10^{32} \equiv 1 \pmod{51}$. Taking both sides to the power of n gives us $10^{32n} \equiv 1 \pmod{51}$. Since

$$10^9 = 10 \cdot (100)^4 \equiv 10 \cdot (-2)^4 = 160 \equiv 7 \pmod{51},$$

then $10^{32n+9} = 10^{32n} \cdot 10^9 \equiv 7 \pmod{51}$ which is equivalent to

$$51 \mid 10^{32n+9} - 7.$$

3. Prove that $2^{15} - 2^3$ divides $a^{15} - a^3$ for any integer a.
[*Hint:* $2^{15} - 2^3 = 5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$.]

Solution For all integers a not divisible by 5, we have $a^4 \equiv a^{\phi(5)} \equiv 1 \pmod{5}$. Cubing and multiplying both sides by a^3 gives us $a^{15} \equiv a^3 \pmod{5}$ for all integers a. For all integers a not divisible by 7, we have $a^6 \equiv a^{\phi(7)} \equiv 1 \pmod{7}$. Squaring and multiplying both sides by a^3 gives us $a^{15} \equiv a^3 \pmod{7}$ for all integers a. For all integers a not divisible by 2, we have $a^4 \equiv a^{\phi(8)} \equiv 1 \pmod{8}$. Cubing and multiplying both sides by a^3 gives us $a^{15} \equiv a^3 \pmod{8}$ for all integers a. For all integers a not divisible by 3, we have $a^6 \equiv a^{\phi(9)} \equiv 1 \pmod{9}$. Squaring and multiplying both sides by a^3 gives us $a^{15} \equiv a^3 \pmod{9}$ for all integers a. Finally, for all integers a, we have $a^{13} \equiv a \pmod{13}$ so multiplying both sides by a^2 gives us $a^{15} \equiv a^3 \pmod{13}$. Therefore, for all integers a, $a^{15} \equiv a^3 \pmod{2^{15} - 2^3}$ which is equivalent to $2^{15} - 2^3$ divides $a^{15} - a^3$.

4. Show that if $\gcd(a, n) = \gcd(a - 1, n) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}.$$

[*Hint:* Recall that

$$a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1).]$$

Solution Since $\gcd(a, n) = 1$, then $a^{\phi(n)} - 1 \equiv 0 \pmod{n}$. Hence, if we take the equation

$$a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$$

modulo n, then we get that

$$(a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1) \equiv 0 \pmod{n}.$$

Since $\gcd(a-1,n)=1$, then

$$a^{\phi(n)-1}+\cdots+a^2+a+1\equiv 0 \pmod{n}$$

by Corollary 1 of Theorem 4-3.

5. If m and n are relatively prime positive integers, prove that

$$m^{\phi(n)}+n^{\phi(m)}\equiv 1 \pmod{mn}.$$

Solution Since m is prime relative to n, then $m^{\phi(n)}+n^{\phi(m)}\equiv m^{\phi(n)}+0\equiv 1 \pmod{n}$. Similarly, $m^{\phi(n)}+n^{\phi(m)}\equiv 1 \pmod{m}$. Since m and n are relatively prime, then $m^{\phi(n)}+n^{\phi(m)} \pmod{mn}$.

6. Fill any missing details in the following proof of Euler's Theorem: Let p be a prime divisor of n and $\gcd(a,p)=1$. By Fermat's Theorem, $a^{p-1}\equiv 1 \pmod{p}$, so that $a^{p-1}=1+tp$ for some t. Then, $a^{p(p-1)}=(1+tp)^p=1+\binom{p}{1}(tp)+\cdots+(tp)^p\equiv 1 \pmod{p^2}$ and, by induction, $a^{p^{k-1}(p-1)}\equiv 1 \pmod{p^k}$ where $k=1,2,\ldots$. Raise both sides of the congruence to the $\phi(n)/p^{k-1}(p-1)$ power to get $a^{\phi(n)}\equiv 1 \pmod{p^k}$. Thus, $a^{\phi(n)}\equiv 1 \pmod{n}$.

Solution Let's prove more rigorously that $a^{p^{k-1}(p-1)}\equiv 1 \pmod{p^k}$ for all $k\geqslant 1$. The case $k=1$ follows from Fermat's Theorem. Next, if $a^{p^{k-1}(p-1)}\equiv 1 \pmod{p^k}$ for some k, then it means that $a^{p^{k-1}(p-1)}=1+tp^k$ for some integer t. Taking both sides to the power of p gives us $a^{p^k(p-1)}=(1+tp^k)^p$. Using the Binomial Formula, we have that

$$(1+tp^k)^p=1+tp^{k+1}+\sum_{i=2}^{p}\binom{p}{i}t^ip^{ik}.$$

Since $p^{ik}\equiv 0 \pmod{p^{k+1}}$ for all $i\geqslant 2$, we get that $a^{p^k(p-1)}=(1+tp^k)^p\equiv 1 \pmod{p^{k+1}}$. Hence, by indution, $a^{p^{k-1}(p-1)}\equiv 1 \pmod{p^k}$ for all $k\geqslant 1$.

Next, if we let k be such that p^k is the highest power of p dividing n, then $\phi(n)$ is divisible by $p^{k-1}(p-1)$, so $\phi(n)/p^{k-1}(p-1)$ is an integer. From the part proved by induction, we get that $a^{\phi(n)}\equiv 1 \pmod{p^k}$. Finally, if we write $n=p_1^{k_1}\cdots p_r^{k_r}$, then $a^{\phi(n)}\equiv 1 \pmod{p_i^{k_i}}$ for all i. Since $p_1^{k_1}$, ..., $p_r^{k_r}$ are relatively prime, then $a^{\phi(n)}\equiv 1 \pmod{n}$.

7. Find the units digit of 3^{100} by means of Euler's Theorem.

Solution Using Euler's Theorem, we have that $3^4=3^{\phi(10)}\equiv 1 \pmod{10}$ (since $\gcd(3,10)=1$). Hence:

$$3^{100}=(3^4)^{25}\equiv 1^{25}=1 \pmod{10}.$$

8.

(a) If $\gcd(a, n) = 1$, show that the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv ba^{\phi(n)-1} \pmod{n}$.

(b) Use part (a) to solve the congruences $3x \equiv 5 \pmod{26}$, $13x \equiv 2 \pmod{40}$ and $10x \equiv 21 \pmod{49}$.

Solution

(a) If we let $x \equiv ba^{\phi(n)-1}$, then $ax \equiv ba^{\phi(n)} \equiv b \pmod{n}$ by Euler's Theorem. Hence, $x \equiv ba^{\phi(n)-1}$ is the solution of the congruence $ax \equiv b \pmod{n}$ (the solution is unique modulo n).

(b) Using part (a), the solution of the congruence $3x \equiv 5 \pmod{26}$ is

$$x \equiv 5 \cdot 3^{\phi(26)-1} = 5 \cdot 3^{11} = 5 \cdot 3^2 \cdot (3^3)^3 \equiv 5 \cdot 9 \equiv 19 \pmod{26}.$$

The solution of the congruence $13x \equiv 2 \pmod{40}$ is

$$x \equiv 2 \cdot 13^{\phi(40)-1} = 2 \cdot 13^{15} = 2 \cdot 13^3 \cdot (13^4)^3 \equiv 2 \cdot (-3) \cdot 1 \equiv 34 \pmod{40}.$$

The solution of the congruence $10x \equiv 21 \pmod{49}$ is

$$x \equiv 21 \cdot 10^{\phi(49)-1} = 21 \cdot 10 \cdot 100^{20} \equiv 14 \cdot 2^{20} \equiv 14 \cdot (-5)^2 \equiv 7 \pmod{49}.$$

9. Prove that every prime other than 2 or 5 divides infinitely many of the integers 1, 11, 111, 1111, ...

Solution First, notice that the prime number 3 divides infinitely many of these integers because it divides all such integers with a multiple of 3 number of 1's (by the divisibility test). Let p be a prime distinct from 2, 3, and 5, then $10^{k\phi(p)} \equiv 1 \pmod{p}$ for all k, so p divides $10^{k\phi(p)} - 1$. Since 9 divides $10^{k\phi(p)} - 1$ as well, and $\gcd(p, 9) = 1$, then $9p$ divides $10^{k\phi(p)} - 1$. Equivalently, this means that p divides 11...11 whenever the number of 1's is equal to a multiple of $\phi(p)$. Since there are infinitely many such numbers, then p divides infinitely many of the integers 1, 11, 111, 1111, ...

10. For any prime p, establish each of the assertions below:

(a) $\tau(p!) = 2\tau((p-1)!)$;

(b) $\sigma(p!) = (p+1)\sigma((p-1)!)$;

(c) $\phi(p!) = (p-1)\phi((p-1)!)$.

Solution

(a) Since p is prime, then $(p-1)!$ is not divisible by p so it is prime relative to p. It follows that

$$\tau(p!) = \tau(p)\tau((p-1)!) = 2\tau((p-1)!).$$

(b) Since p is prime, then $(p-1)!$ is not divisible by p so it is prime relative to p. It follows that

$$\sigma(p!) = \sigma(p)\sigma((p-1)!) = (p+1)\sigma((p-1)!).$$

(c) Since p is prime, then $(p-1)!$ is not divisible by p so it is prime relative to p. It follows that

$$\phi(p!) = \phi(p)\phi((p-1)!) = (p-1)\phi((p-1)!).$$

11. Given $n \geqslant 1$, a set of $\phi(n)$ integers which are relatively prime to n and which are incongruent modulo n is called a *reduced set of residues modulo n* (that is, a reduced set of residues are those members of a complete set of residues modulo n which are relatively prime to n).

Verify that

(a) the integers $-31, -16, -8, 13, 25, 80$ form a reduced set of residues modulo 9;

(b) the integers $3, 3^2, 3^3, 3^4, 3^5, 3^6$ form a reduced set of residues modulo 14;

(c) the integers $2, 2^2, 2^3, ..., 2^{18}$ form a reduced set of residues modulo 27.

Solution

(a) If we take the residues of the numbers $-31, -16, -8, 13, 25, 80$ modulo 9, we get the numbers $5, 2, 1, 4, 7, 8$. Since all of these numbers are distint, then the original numbers must be noncongruent. Hence, there are $6 = \phi(9)$ noncongruent elements in the list. Moreover, since all the elements in the new list are prime relative to 9, then the same holds for the original list. Therefore, the integers $-31, -16, -8, 13, 25, 80$ form a reduced set of residues modulo 9.

(b) The integers $3, 3^2, 3^3, 3^4, 3^5, 3^6$ are all prime relative to 14 since they share no prime factors. Moreover, if we take the residues of the numbers in this list, we get the new list $3, 9, 13, 11, 5, 1$ where clearly, no two elements are congruent. Hence, there are $6 = \phi(14)$ noncongruent elements in the list. Therefore, the integers $3, 3^2, 3^3, 3^4, 3^5, 3^6$ form a reduced set of residues modulo 14.

(c) The integers $2, 2^2, 2^3, ..., 2^{18}$ are all prime relative to 27 since they share no prime factors. Moreover, if we take the residues of the numbers in this list, we get the new list $2, 4, 8, 16, 5, 10, 20, 13, 26, 25, 23, 19, 11, 22, 17, 7, 14, 1$ where clearly, no two elements are congruent. Hence, there are $18 = \phi(27)$ noncongruent elements in the list. Therefore, the integers $2, 2^2, 2^3, ..., 2^{18}$ form a reduced set of residues modulo 14.

12. If p is an odd prime, show that the integers

$$-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2}$$

form a reduced set of residues modulo p.

Solution Using Problem 12(b) from section 4.3, we have that the integers

$$-\frac{p-1}{2}, ..., -2, -1, 0, 1, 2, ..., \frac{p-1}{2}$$

form a complete set of residues modulo n. But since 0 is the only element which is not prime relative to p, then it follows that by removing 0 from these integers, we get the following reduced set of residues modulo p:

$$-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2}$$

7.4 Some Properties of the Phi-Function

1. For a positive integer n, prove that

$$\sum_{d \mid n} (-1)^{n/d}\phi(d) = \begin{cases} 0 \text{ if } n \text{ is even} \\ -n \text{ if } n \text{ is odd} \end{cases}$$

[*Hint:* If $n = 2^k N$, where N is odd, then $\sum_{d|n}(-1)^{n/d}\phi(d) = \sum_{d|2^{k-1}N}\phi(d) - \sum_{d|N}\phi(2^k d)$.]

Solution First, let n be an even number and write it as $2^k N$ where $k \geqslant 1$ and N is odd, then the divisors of n are precisely the numbers of the form $2^i d$ where $0 \leqslant i \leqslant k$ and d is a divisor of N. Hence:

$$\sum_{d \mid n} (-1)^{n/d}\phi(d) = \sum_{i=0}^{k}\sum_{d \mid N} (-1)^{n/2^i d}\phi(2^i d).$$

When $i \neq k$, $n/2^i d = 2^{k-i}(N/d)$ is an even number, and when $i = k$, it is odd, so we get

$$\begin{aligned}\sum_{d \mid n} (-1)^{n/d}\phi(d) &= \sum_{i=0}^{k-1}\sum_{d \mid N} (-1)^{n/2^i d}\phi(2^i d) + \sum_{d \mid N} (-1)^{n/2^k d}\phi(2^k d) \\ &= \sum_{i=0}^{k-1}\sum_{d \mid N} \phi(2^i)\phi(d) - \sum_{d \mid N} \phi(2^k)\phi(d) \\ &= \sum_{i=0}^{k-1}\phi(2^i)\sum_{d \mid N}\phi(d) - \phi(2^k)\sum_{d \mid N}\phi(d).\end{aligned}$$

Using Theorem 7-6:

$$\begin{aligned}\sum_{d \mid n} (-1)^{n/d}\phi(d) &= \sum_{i=0}^{k-1}\phi(2^i)N - \phi(2^k)N \\ &= N\left[\sum_{i=0}^{k-1}\phi(2^i) - 2^{k-1}\right] \\ &= N(2^{k-1} - 2^{k-1}) \\ &= 0.\end{aligned}$$

When n is odd, then for all divisors d of n, we have that n/d is odd as well. Thus, using Theorem 7-6:

$$\sum_{d \mid n} (-1)^{n/d}\phi(d) = -\sum_{d \mid n}\phi(d) = -n.$$

Therefore:

$$\sum_{d \mid n} (-1)^{n/d}\phi(d) = \begin{cases} 0 \text{ if } n \text{ is even} \\ -n \text{ if } n \text{ is odd} \end{cases}.$$

2. Confirm that $\sum_{d|36} \phi(d) = 36$ and $\sum_{d|36}(-1)^{36/d}\phi(d) = 0$.

Solution We have

$$\begin{aligned}\sum_{d \mid 36} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(9) + \phi(12) + \phi(18) + \phi(36)\\ &= 1 + 1 + 2 + 2 + 2 + 6 + 4 + 6 + 12\\ &= 36\end{aligned}$$

and

$$\begin{aligned}\sum_{d \mid 36} (-1)^{36/d}\phi(d) &= (-1)^{36}\phi(1) + (-1)^{18}\phi(2) + (-1)^{12}\phi(3) + (-1)^{9}\phi(4) + (-1)^{6}\phi(6)\\ &\quad + (-1)^{4}\phi(9) + (-1)^{3}\phi(12) + (-1)^{2}\phi(18) + (-1)^{1}\phi(36)\\ &= 1 + 1 + 2 - 2 + 2 + 6 - 4 + 6 - 12\\ &= 0.\end{aligned}$$

3. For a positive integer n, prove that $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$.
[*Hint:* See the hint in Problem 1.]

Solution Let $F(n) = \sum_{d|n} \mu^2(d)/\phi(d)$ and $G(n) = n/\phi(n)$. Since both are multiplicative functions, then to prove that $F = G$, it suffices to show that $F(p^k) = G(p^k)$ for all prime p and $k \geqslant 1$. Let p be a prime and $k \geqslant 1$, then

$$\begin{aligned}F(p^k) &= \sum_{d|p^k} \frac{\mu^2(d)}{\phi(d)}\\ &= \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + \frac{\mu^2(p^2)}{\phi(p^2)} \cdots + \frac{\mu^2(p^k)}{\phi(p^k)}\\ &= \frac{1}{1} + \frac{1}{p-1} + 0 \cdots + 0\\ &= \frac{p}{p-1}\\ &= \frac{p^k}{p^{k-1}(p-1)}\\ &= \frac{p^k}{\phi(p^k)}\\ &= G(p^k).\end{aligned}$$

Therefore, $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(n)$.

4. Use Problem 3, Section 6-2, to give a different proof of the fact that

$$n \sum_{d \mid n} \mu(d)/d = \phi(n).$$

Solution Using Problem 3 of Section 6-2, we have that

$$\sum_{d \mid n} \mu(d)/d = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

where $n = p_1^{k_1} \cdots p_r^{k_r}$. Hence,

$$n \sum_{d \mid n} \mu(d)/d = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

By Theorem 7-3, it follows that

$$n \sum_{d \mid n} \mu(d)/d = \phi(n).$$

5. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, establish the following:

(a) $\sum_{d \mid n} \mu(d)\phi(d) = (2 - p_1)(2 - p_2) \cdots (2 - p_r)$

(b) $$\sum_{d \mid n} d\phi(d) = \left(\frac{p_1^{2k_1+1} + 1}{p_1 + 1}\right) \left(\frac{p_2^{2k_2+1} + 1}{p_2 + 1}\right) \cdots \left(\frac{p_r^{2k_r+1} + 1}{p_r + 1}\right)$$

(c) $$\sum_{d \mid n} \phi(d)/d = \left(1 + \frac{k_1(p_1 - 1)}{p_1}\right) \left(1 + \frac{k_2(p_2 - 1)}{p_2}\right) \cdots \left(1 + \frac{k_r(p_r - 1)}{p_r}\right)$$

[*Hint:* For part (a), use Problem 3, Section 6-2.]

Solution

(a) Using Problem 3, Section 6-2:

$$\begin{aligned}\sum_{d \mid n} \mu(d)\phi(d) &= (1 - \phi(p_1))(1 - \phi(p_2)) \cdots (1 - \phi(p_r)) \\ &= (2 - p_1)(2 - p_2) \cdots (2 - p_r).\end{aligned}$$

(b) Since the function $n\phi(n)$ is multiplicative, it suffices to prove it for $n = p^k$

where p is prime and $k \geqslant 1$:

$$\begin{aligned}
\sum_{d \mid n} d\phi(d) &= \sum_{i=0}^{k} p^i \phi(p^i) \\
&= 1 + \sum_{i=1}^{k} p^i \cdot p^{i-1}(p-1) \\
&= 1 + \frac{p-1}{p} \sum_{i=1}^{k} (p^2)^i \\
&= 1 + \frac{p-1}{p} \cdot \frac{p^2(p^{2k}-1)}{p^2-1} \\
&= 1 + \frac{p(p^{2k}-1)}{p+1} \\
&= \frac{p^{2k+1}+1}{p+1}.
\end{aligned}$$

(c) Since the function $n\phi(n)$ is multiplicative, it suffices to prove it for $n = p^k$ where p is prime and $k \geqslant 1$:

$$\begin{aligned}
\sum_{d \mid n} \phi(d)/d &= \sum_{i=0}^{k} \phi(p^i)/p^i \\
&= 1 + \sum_{i=0}^{k} p^{i-1}(p-1)/p^i \\
&= 1 + \sum_{i=0}^{k} (p-1)/p \\
&= 1 + \frac{k(p-1)}{p}.
\end{aligned}$$

6. Verify the formula $\sum_{d=1}^{n} \phi(d)[n/d] = n(n+1)/2$ for any positive integer n. [*Hint:* This is a direct application of Theorem 6-11 and 7-6.]

Solution Since $\sum_{d|n} \phi(d) = n$, then Theorem 6-11 tells us that

$$\sum_{d=1}^{n} \phi(d)[n/d] = \sum_{d=1}^{n} d = \frac{n(n+1)}{2}.$$

7. If n is a square-free integer, prove that $\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k$ for all integers $k \geqslant 2$.

Solution First, notice that $\sigma(n^{k-1})$ is a multiplicative function since given two relatively prime integers a and b, we have that a^{k-1} and b^{k-1} are relatively prime as well so $\sigma((ab)^{k-1}) = \sigma(a^{k-1} \cdot b^{k-1}) = \sigma(a^{k-1})\sigma(b^{k-1})$. Hence, $\sigma(n^{k-1})\phi(n)$ is a multiplicative function, so it follows that $\sum_{d|n} \sigma(d^{k-1})\phi(d)$ is multiplicative. Thus, it suffices to prove the desired formula in the special case $n = p$ for some prime p:

$$\begin{aligned}\sum_{d \mid n} \sigma(d^{k-1})\phi(d) &= \sigma(1^{k-1})\phi(1) + \sigma(p^{k-1})\phi(p) \\ &= 1 \cdot 1 + \frac{p^k - 1}{p - 1}(p - 1) \\ &= 1 + p^k - 1 \\ &= p^k.\end{aligned}$$

8. For a square-free integer $n > 1$, show that $\tau(n^2) = n$ if and only if $n = 3$.

Solution Let $n = p_1 p_2 \cdots p_r$ be a square-free integer such that $\tau(n^2) = n$, then equivalently, this implies that $\tau(p_1^2)\tau(p_2^2) \cdots \tau(p_r^2) = n$. But since $\tau(p^2) = 3$ for all prime p, the previous equation becomes $3^r = n$. Since n is square-free, then r must be equal to 1, and hence, $n = 3$. Conversely, when $n = 3$, we have

$$\tau(3^2) = \tau(9) = 3.$$

9. Prove that $3 \mid \sigma(3n + 2)$ and $4 \mid \sigma(4n + 3)$ for any positive integer n.

Solution Let $3n+2 = p_1^{k_1} \cdots p_r^{k_r}$ be an integer. Notice that p_i cannot be of the form $3k$ because otherwise, $3n+2$ would be of the form $3k$ which is impossible. Hence, p_i is either of the form $3k+1$ or $3k+2$. If all primes are of the form $3k+1$, then $3n+2$ will be of the form $3k+1$ as well (a product of numbers of the form $3k+1$ is of the form $3k+1$), a contradiction. Hence, there must be a prime p_i of the form $3k+2$. Now, suppose that k_i is even whenever p_i is of the form $3k+2$, then $p_i^{k_i}$ will be of the form $3k+1$ (it suffices to look at $p_i^{k_i}$ modulo 3), in that case, $p_i^{k_i}$ will be of the form $3k+1$ for all i, and hence, $3n+2$ will be of the form $3k+1$, a contradiction. Thus, there is a i such that p_i is of the form $3k+2$ and k_i is odd. It follows that

$$\begin{aligned}\sigma(3n+2) &= \sigma(p_i^{k_i})\sigma(N) \\ &= (1 + p_i + \cdots + p_i^{k_i})\sigma(N) \\ &\equiv (1 - 1 + \cdots + (-1)^{k_i})\sigma(N) \\ &= 0 \pmod 3\end{aligned}$$

where $N = (3n+2)/p_i^{k_i}$. Therefore, $3 \mid \sigma(3n+2)$.

Let $4n + 3 = p_1^{k_1} \cdots p_r^{k_r}$ be an integer. Notice that p_i cannot be of the form $4k$ or $4k+2$ because otherwise, $4n+3$ would be of the form $4k$ or $4k+2$ which is impossible. Hence, p_i is either of the form $4k+1$ or $4k+3$. If all primes are of the form $4k+1$, then $4n+3$ will be of the form $4k+1$ as well (a product of numbers of the form $4k+1$ is of the form $4k+1$), a contradiction. Hence, there must be a prime p_i of the form $4k+3$. Now, suppose that k_i is even whenever p_i is of the form $4k+3$, then $p_i^{k_i}$ will be of the form $4k+1$ (it suffices to look at $p_i^{k_i}$ modulo 4), in that case, $p_i^{k_i}$ will be of the form $4k+1$ for all i, and hence, $4n+3$ will be of the form $4k+1$, a contradiction. Thus, there is a i such that p_i is of the form $4k+3$ and k_i is odd. It follows that

$$\begin{aligned}\sigma(4n+3) &= \sigma(p_i^{k_i})\sigma(N)\\ &= (1+p_i+\cdots+p_i^{k_i})\sigma(N)\\ &\equiv (1-1+\cdots+(-1)^{k_i})\sigma(N)\\ &= 0 \pmod 4\end{aligned}$$

where $N=(4n+3)/p_i^{k_i}$. Therefore, $4 \mid \sigma(4n+3)$.

10.

(a) Given $k>0$, establish that there exists a sequence of k consecutive integers $n+1$, $n+2$, ..., $n+k$ satisfying

$$\mu(n+1)=\mu(n+2)=\cdots=\mu(n+k)=0.$$

[*Hint:* Consider the system of linear congruences

$$x \equiv -1 \pmod 4,\ x \equiv -2 \pmod 9,\ \ldots,$$
$$x \equiv -k \pmod{p_k^2}$$

where p_k is the kth prime.]

(b) Find four consecutive integers for which $\mu(n)=0$.

Solution

(a) Let $k>0$ be an integer, and consider the system of congruences

$$\begin{aligned}x &\equiv -1 \pmod 4,\\ x &\equiv -2 \pmod 9,\\ &\vdots\\ x &\equiv -k \pmod{p_k^2}\end{aligned}$$

where p_k is the kth prime. Since 2^2, 9^2, ..., p_k^2 are relatively prime, then the system of congruences has a solution by the Chinese Remainder Theorem. Hence, if we let n be a solution of the system, then $2^2 \mid n+1$, $3^2 \mid n+2$, ..., $k^2 \mid n+k$. It follows that

$$\mu(n+1)=\mu(n+2)=\cdots=\mu(n+k)=0.$$

(b) Let's solve the following system of congruences:

$$\begin{aligned}x &\equiv -1 \pmod 4,\\ x &\equiv -2 \pmod 9,\\ x &\equiv -3 \pmod{25},\\ x &\equiv -4 \pmod{49}.\end{aligned}$$

To do so, we first need to find integers a, b, c, and d such that

$$\begin{aligned} 9\cdot 25\cdot 49a &\equiv 1 \pmod{4}\\ 4\cdot 25\cdot 49b &\equiv 1 \pmod{9}\\ 4\cdot 9\cdot 49c &\equiv 1 \pmod{25}\\ 4\cdot 9\cdot 25d &\equiv 1 \pmod{49}. \end{aligned}$$

If we simplify the equations, we get

$$\begin{aligned} a &\equiv 1 \pmod{4}\\ 4b &\equiv 1 \pmod{9}\\ 14c &\equiv 1 \pmod{25}\\ 18d &\equiv 1 \pmod{49}. \end{aligned}$$

Using the Euclidean Algorithm, we get that $a \equiv 1 \pmod{4}$, $b \equiv 7 \pmod{9}$, $c \equiv 9$ (mod 2)5, and $d \equiv 30 \pmod{49}$. Hence, we can take $a = 1$, $b = -2$, $c = 9$, and $d = -19$. Next, we define the integer x up to a multiple of $4 \cdot 9 \cdot 25 \cdot 49 = 44100$ as follows:

$$\begin{aligned} x &= -9\cdot 25\cdot 49a - 2\cdot 4\cdot 25\cdot 49b - 3\cdot 4\cdot 9\cdot 49c - 4\cdot 4\cdot 9\cdot 25d\\ &= -11025 + 19600 - 47628 + 68400\\ &= 29347. \end{aligned}$$

By construction, x is a solution of the system of congruences we started with (can be verified directly). Hence, 4 divides $x+1$, 9 divides $x+2$, 25 divides $x+3$, and 49 divides $x+4$. Therefore,

$$\mu(29348) = \mu(29349) = \mu(29350) = \mu(29351) = 0.$$

11. Prove the statements below:

(a) An integer n is prime if and only if $\sigma(n) + \phi(n) = n\tau(n)$.
[*Hint:* First derive the relation $\sum_{d|n} \sigma(d)\phi(n/d) = n\tau(n)$.]

(b) An integer n is prime if and only if $\phi(n) \mid n-1$ and also $n+1 \mid \sigma(n)$. [*Hint:* See Problem 11(a), Section 7-2.]

Solution

(a) First, it is clear that the equation doesn't hold for $n = 1$. Now, since $\sigma(n) = 1 + S + n$ where S is the sum of the nontrivial proper divisors of n, then we can can write the equation $\sigma(n) + \phi(n) = n\tau(n)$ as

$$1 + S + n + \phi(n) = n\tau(n).$$

If we subtract by n on both sides, we get

$$(1 + \phi(n)) + S = n(\tau(n) - 1) = n + ... + n.$$

Notice that S represents a sum of $\tau(n)-2$ terms so if we add the term $[1+\phi(n)]$, then there are as many terms on the LHS than on the RHS. If n is not prime, then there is a nontrivial proper divisor d of n. It follows that the sum S is nonempty, and every term in S is strictly smaller than n. Since $(1+\phi(n)) \leqslant n$, then comparing term by term gives us

$$(1+\phi(n)) + S < n + ... + n = n(\tau(n)-1),$$

a contradiction. Therefore, n must be prime.

Conversely, if n is prime, then

$$\sigma(n) + \phi(n) = (n+1) + (n-1) = 2n = n\tau(n).$$

(b) Despite all my efforts, I was not able to solve this exercise. I used Problem 11(a) to deduce that n is square-free. Then, I used this information to write $\sigma(n)$ as the product of (p_i+1) where n is the product of the p_i's. Then, I tried to find an upperbound for $\sigma(n)$ in terms of n, for example, $\sigma(n) \leqslant 2n$ or $\sigma(n) \leqslant 3n$. However, using the fact that $\sum 1/p = \infty$, we get that

$$\frac{\sigma(n)}{n} = \prod_i \left(1 + \frac{1}{p_i}\right)$$

can be arbitrarily large. Similarly, every other ideas turned out to be false. This exercice has been removed from the next editions of this book, maybe because the proof that the author had in mind was false, and the actual proof (if the statement is true) is much harder. Hopefully, this is the only time this happens.

12. For $n > 2$, establish the inequality $\phi(n^2) + \phi((n+1)^2) \leqslant 2n^2$.

Solution First, using Problem 10, Section 7-2, we can write

$$\phi(n^2) + \phi((n+1)^2) = n\phi(n) + (n+1)\phi(n+1).$$

One of n, $n+1$ is even. If n is even, then at least half of the integers less than n are no prime relative to n so $\phi(n) \leqslant n/2$. We cannot say much for $n+1$ but at least we know that there are at most n numbers less than $n+1$ that are prime relative to $n+1$ since we don't count $n+1$. Hence:

$$\phi(n^2) + \phi((n+1)^2) \leqslant n\left(\frac{n}{2}\right) + (n+1)n = \frac{3}{2}n^2 + n.$$

Since $n > 2$, then $n \leqslant n^2/2$ which implies that $3n^2/2 + n \leqslant 2n^2$. Therefore,

$$\phi(n^2) + \phi((n+1)^2) \leqslant 2n^2.$$

Next, suppose that $n+1$ is even, then $\phi(n+1) \leqslant (n+1)/2$ and $\phi(n) \leqslant n-1$. Hence:

$$\begin{aligned}\phi(n^2) + \phi((n+1)^2) &= n\phi(n) + (n+1)\phi(n+1) \\ &\leqslant n(n-1) + n\left(\frac{n+1}{2}\right) \\ &= \frac{3n^2}{2} - \frac{n}{2} \\ &\leqslant 2n^2.\end{aligned}$$

Therefore, the inequality holds for all $n > 2$.

13. Given an integer n, prove that there exists at least one k for which $n \mid \phi(k)$.

Solution When $n = 1$, every k works. If $n > 1$, write $n = p_1^{k_1} \cdots p_r^{k_r}$ and let $k = p_1^{k_1+1} \cdots p_r^{k_r+1}$, then

$$\phi(k) = p^{k_1}(p_1 - 1) \cdots p_r^{k_r}(p_r - 1) = n(p_1 - 1) \cdots (p_r - 1).$$

Hence, $n \mid \phi(k)$.

14. Show that if n is a product of two twin primes, say $n = p(p + 2)$, then $\phi(n)\sigma(n) = (n + 1)(n - 3)$.

Solution If $n = p(p + 2)$ where p and $p + 2$ are prime, then

$$\begin{aligned}\phi(n)\sigma(n) &= \phi(p)\phi(p+2)\sigma(p)\sigma(p+2)\\ &= (p-1)(p+1)(p+1)(p+3)\\ &= (p+1)^2(p-1)(p+3)\\ &= (p^2+2p+1)(p^2+2p-3)\\ &= (p(p+2)+1)(p(p+2)-3)\\ &= (n+1)(n-3).\end{aligned}$$

15. Prove that $\sum_{d\ |n} \sigma(d)\phi(n/d) = n\tau(n)$.

Solution We can write

$$\sum_{d|n} \sigma(d)\phi\left(\frac{n}{d}\right) = \sum_{d|n}\sum_{t|d} t\phi\left(\frac{n}{d}\right).$$

Since the set of pairs (d, t) satisfying $d \mid n$ and $t \mid d$ is the same as the set of pairs (d, t) such that $t \mid n$ and $t \mid d$ where $d \mid n$, then we can invert the two sums to get

$$\sum_{d|n}\sum_{t|d} t\phi\left(\frac{n}{d}\right) = \sum_{t|n}\sum_{t|d} t\phi\left(\frac{n}{d}\right) = \sum_{t|n} t\left(\sum_{t|d}\phi\left(\frac{n}{d}\right)\right)$$

where, for a fixed t, the second sum runs over all d which are divisors of n and divisible by t. Let's look at the sum $\sum_{t|d}\phi\left(\frac{n}{d}\right)$ in more details. Notice that whenever d is multiple of t and divisor of n, then n/d divides n/t. Moreover, every divisor of n/t can be written as n/d where d is a multiple of t that divides n. Therefore, we can rewrite the sum $\sum_{t|d}\phi\left(\frac{n}{d}\right)$ more simply as $\sum_{d|\frac{n}{t}}\phi(d)$. Therefore, putting everything together and using Theorem 7-6:

$$\sum_{d|n} \sigma(d)\phi\left(\frac{n}{d}\right) = \sum_{t|n} t\left(\sum_{d|\frac{n}{t}}\phi(d)\right) = \sum_{t|n} t\left(\frac{n}{t}\right) = \sum_{d|n} n = n\tau(n).$$

16. If $a_1, a_2, ..., a_{\phi(n)}$ is a reduced set of residues modulo n, show that $a_1 + a_2 + ... + a_{\phi(n)} \equiv 0 \pmod{n}$.

Solution If $a_1, a_2, ..., a_{\phi(n)}$ is a reduced set of residues modulo n, then a_i is prime relative to n for all i. Since a_i up to any multiple multiple of n is prime relative to n, then the least positive residue of n is prime relative to n for all i. Since the a_i's are noncongruent relative to n, then their least positive residues are noncongruent relative to n. This means that the least positive resiudes of $a_1, a_2, ..., a_{\phi(n)}$ is a list $b_1, ..., b_{\phi(n)}$ of $\phi(n)$ integers (since they are noncongruent) between 1 and n that are relatively prime to n. But since there are precisely $\phi(n)$ integers between 1 and n that are relatively prime to n (by definition of $\phi(n)$), then $b_1, ..., b_{\phi(n)}$ of $\phi(n)$ is precisely the list of integers between 1 and n that are relatively prime to n. Therefore:

$$a_1 + a_2 + ... + a_{\phi(n)} \equiv \sum_{\gcd(k,n)=1} k = \frac{1}{2} n\phi(n) \pmod{n}.$$

Since $n > 2$, then $\phi(n)$ is even, and hence,

$$\frac{1}{2} n\phi(n) = n \cdot \frac{\phi(n)}{2}$$

is an integer multiple of n. It direcly follows that

$$a_1 + a_2 + ... + a_{\phi(n)} \equiv 0 \pmod{n}.$$

7.5 An Application to Cryptography

1. Encrypt the message *RETURN HOME* using the Caesar cipher.

Solution The Caesar cipher is defined by the rule $C \equiv P + 3 \pmod{26}$. Hence, the encrypted message is *UHWXUQ KRPH*.

2. If the Ceasar cipher produced *KDSSB ELUWKGDB*, what is the plaintext message ?

Solution The equation $C \equiv P + 3 \pmod{26}$ is equivalent to $P \equiv C - 3 \pmod{26}$ so it suffices to replace every letter by the letter which is three positions before in the alphabet. Hence, we get that the plaintext message is *HAPPY BIRTHDAY*.

3.

(a) A linear cipher is defined by the congruence $C \equiv aP+b \pmod{26}$, where a and b are integers with $\gcd(a, 26) = 1$. Show that the corresponding decrypting congruence is $P \equiv a'(C - b) \pmod{26}$, where the integer a' satisfies $aa' \equiv 1 \pmod{26}$.

(b) Using the linear cipher $C \equiv 5P+11 \pmod{26}$, encrypt the message *NUMBER THEORY IS EASY*.

(c) Decrypt the message *TZSVIW JQBVMIJ HL MVOOVI*, which was produced using the linear cipher $C \equiv 3P + 7 \pmod{26}$.

Solution

(a) The decypting congruence must be a congruence where P is expressed in terms of C. If we let a' be the integer such that $aa' \equiv 1 \pmod{26}$ (which must exist since $\gcd(a, 26) = 1$), then multiplying both sides of the congruence $C \equiv aP+b \pmod{26}$ by a' gives us $a'C \equiv P + a' \pmod{26}$. Subtracting both sides by $a'b$ gives us $P \equiv a'(C - b) \pmod{26}$.

(b) Using this linear cipher, the alphabet becomes

$$PUZEJOTYDINSXCHMRWBGLQVAFK.$$

Hence, the message *NUMBER THEORY IS EASY* becomes *CLXUJW GYJHWF DB JPBF*.

(c) From the linear cipher $C \equiv 3P+7 \pmod{26}$ we get the decrypting congruence $P \equiv 9C-11 \pmod{26}$. Hence, the decrypted message is *MODERN ALGEBRA IS BETTER*.

4. If $n = pq = 274279$ and $\phi(n) = 272376$, find the primes p and q.

[*Hint:* Note that

$$\begin{aligned}p+q &= n-\phi(n)+1,\\ p-q &= [(p+q)^2-4n]^{1/2}.]\end{aligned}$$

Solution Since $\phi(n)=(p-1)(q-1)=n-(p+q)+1$, then

$$p+q=n-\phi(n)+1=1904.$$

Similarly, since

$$(p-q)^2=(p+q)^2-4pq=(p+q)^2-4n,$$

then

$$p-q=\sqrt{1904^2-4\cdot 274279}=2\sqrt{632025}=1590.$$

Solving the system of equations

$$\begin{cases}p+q &= 1904\\ p-q &= 1590\end{cases}$$

gives us $p=1747$ and $q=157$.

5. When the RSA algorithm is based on the key $(n,k)=(3233,37)$, what is the recovery exponent for the cryptosystem?

Solution Since $n=53\cdot 61$, then $\phi(n)=52\cdot 60=3120$. The recovery exponent satisfies $37j\equiv 1 \pmod{3120}$. Using the Euclidean Algorithm, we get that $j=253$.

6. Encrypt the message *GOLD MEDAL* using the RSA algorithm with key $(n,k)=(2419,3)$.

Solution First, we convert the message into the following blocks of integers:

071 512 040 013 050 401 12.

Next, we need to raise each of these integers to the power of k, and reduce to the least positive residue modulo n:

$$\begin{aligned}71^3 &\equiv 71\cdot 203\equiv 2318 \pmod{2419}\\ 512^3 &\equiv 512\cdot 892\equiv 1932 \pmod{2419}\\ 40^3 &\equiv 40\cdot 1600\equiv 1106 \pmod{2419}\end{aligned}$$

[Starting from now, I will use a calculator to finish this exercice and the next two exercices. It takes too much time.]

$$\begin{aligned}13^3 &\equiv 2197 \pmod{2419}\\ 50^3 &\equiv 1631 \pmod{2419}\\ 401^3 &\equiv 337 \pmod{2419}\\ 12^3 &\equiv 1728 \pmod{2419}.\end{aligned}$$

Therefore, the ciphertext is

$$2318 \quad 1932 \quad 1106 \quad 2197 \quad 1631 \quad 0337 \quad 1728.$$

7. The ciphertext message produced by the RSA algorithm with key $(n, k) = (1643, 223)$ is

$$1451 \quad 0103 \quad 1263 \quad 0560 \quad 0127 \quad 0897.$$

Determine the original plaintext message. [*Hint:* The recovery exponent is $j = 7$.]

Solution Since $1643 = 31 \cdot 53$, then $\phi(n) = 30 \cdot 52 = 1560$. By the Euclidean Algorithm, we get that j must be 7. Thus, we need to raise each block of integers to the 7th power and reduce to the least positive residue modulo 1643:

$$\begin{aligned} 1451^7 &\equiv 180 \pmod{1643} \\ 103^7 &\equiv 516 \pmod{1643} \\ 1263^7 &\equiv 122 \pmod{1643} \\ 560^7 &\equiv 500 \pmod{1643} \\ 127^7 &\equiv 141 \pmod{1643} \\ 897^7 &\equiv 523 \pmod{1643}. \end{aligned}$$

Hence, the integer associated to the plaintext message is

$$180516122500141523$$

which implies that the plaintext message is

$$\textit{REPLY} \quad \textit{NOW}$$

8. Decrypt the ciphertext

$$1037 \quad 0431 \quad 0629 \quad 0690 \quad 0204 \quad 2267 \quad 0595$$

that was encrypted using the RSA algorithm with key $(n, k) = (2419, 211)$. [*Hint:* The recovery exponent is 11.]

Solution Since $2419 = 41 \cdot 59$, then $\phi(n) = 40 \cdot 58 = 2320$. By the Euclidean Algorithm, we get that j must be 11. Thus, we need to raise each block of integers to the 11th power and reduce to the least positive residue modulo 2419:

$$\begin{aligned} 1037^{11} &\equiv 190 \pmod{2419} \\ 431^{11} &\equiv 512 \pmod{2419} \\ 629^{11} &\equiv 120 \pmod{2419} \\ 690^{11} &\equiv 19 \pmod{2419} \\ 204^{11} &\equiv 81 \pmod{2419} \\ 2267^{11} &\equiv 518 \pmod{2419} \\ 595^{11} &\equiv 20 \pmod{2419} \end{aligned}$$

Hence, the integer associated to the plaintext message is

$$1905121200190815182\,0$$

which implies that the plaintext message is

$$SELL\ \ SHORT$$

Chapter 8

Primitive Roots and Indices

8.1 The Order of an Integer Modulo n

1. Find the order of the integers 2, 3, and 5: (a) modulo 17, (b) modulo 19, and (c) modulo 23.

Solution

(a) In modulo 17, the order of an integer must be a divisor of 16, so it must be one of 1, 2, 4, 8, or 16. Therefore, it suffices to check only the latter powers except 16. Since

$$2^1 \equiv 2 \not\equiv 1 \pmod{17}, \quad 2^2 \equiv 4 \not\equiv 1 \pmod{17},$$

$$2^4 \equiv 16 \not\equiv 1 \pmod{17}, \quad 2^8 \equiv 1 \pmod{17},$$

then the order of 2 is 8 with respect to the modulus 17. Since

$$3^1 \equiv 3 \not\equiv 1 \pmod{17}, \quad 3^2 \equiv 9 \not\equiv 1 \pmod{17},$$

$$3^4 \equiv 13 \not\equiv 1 \pmod{17}, \quad 3^8 \equiv 16 \not\equiv 1 \pmod{17},$$

then the order of 3 is 16 with respect to the modulus 17. Since

$$5^1 \equiv 5 \not\equiv 1 \pmod{17}, \quad 5^2 \equiv 8 \not\equiv 1 \pmod{17},$$

$$5^4 \equiv 13 \not\equiv 1 \pmod{17}, \quad 5^8 \equiv 16 \not\equiv 1 \pmod{17},$$

then the order of 5 is 16 with respect to the modulus 17.

(b) In modulo 19, the order of an integer must be a divisor of 18, so it must be one of 1, 2, 9, or 18. Therefore, it suffices to check only the latter powers except 18. Since

$$2^1 \equiv 2 \not\equiv 1 \pmod{19}, \quad 2^2 \equiv 4 \not\equiv 1 \pmod{19}, \quad 2^9 \equiv 18 \not\equiv 1 \pmod{19},$$

then the order of 2 is 18 with respect to the modulus 19. Since

$$3^1 \equiv 2 \not\equiv 1 \pmod{19}, \quad 3^2 \equiv 9 \not\equiv 1 \pmod{19}, \quad 3^9 \equiv 18 \not\equiv 1 \pmod{19},$$

then the order of 3 is 18 with respect to the modulus 19. Since

$$5^1 \equiv 5 \not\equiv 1 \pmod{19}, \quad 5^2 \equiv 6 \not\equiv 1 \pmod{19}, \quad 5^9 \equiv 1 \pmod{19},$$

then the order of 5 is 9 with respect to the modulus 19.

(c) In modulo 23, the order of an integer must be a divisor of 22, so it must be one of 1, 2, 11, or 22. Therefore, it suffices to check only the latter powers except 22. Since

$$2^1 \equiv 2 \not\equiv 1 \pmod{23}, \quad 2^2 \equiv 4 \not\equiv 1 \pmod{23}, \quad 2^{11} \equiv 1 \pmod{23},$$

then the order of 2 is 11 with respect to the modulus 23. Since

$$3^1 \equiv 3 \not\equiv 1 \pmod{23}, \quad 3^2 \equiv 9 \not\equiv 1 \pmod{23}, \quad 3^{11} \equiv 1 \pmod{23},$$

then the order of 3 is 11 with respect to the modulus 23. Since

$$5^1 \equiv 5 \not\equiv 1 \pmod{23}, \quad 5^2 \equiv 2 \not\equiv 1 \pmod{23}, \quad 5^{11} \equiv 2 \not\equiv 1 \pmod{23},$$

then the order of 5 is 22 with respect to the modulus 23.

2. Establish each of the statements below:

(a) If a has order hk modulo n, then a^h has order k modulo n.

(b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.

(c) If a has order $n-1$ modulo n, then n is prime.

Solution

(a) Since $a^{hk} \equiv 1 \pmod{n}$, then $(a^h)^k \equiv 1 \pmod{n}$. Hence, the order d of a^h divides k, and so $d \leqslant k$. On the other hand, if d is the order of a^h, then $a^{hd} \equiv 1 \pmod{n}$. It follows that $hk \leqslant hd$, and hence, $k \leqslant d$. Therefore, we must have $d = k$, or in another words, that the order of a^h is k.

(b) Using part (a), a^k must have order 2. If we let b be an arbitrary element of order 2, then b satisfies the congruence $(b-1)(b+1) \equiv 0 \pmod{p}$. Since p is an odd prime, then $1 \not\equiv -1$ and hence, $b \equiv 1$ or $b \equiv -1$. Since 1 don't have order 2 modulo p, then $b \equiv -1$. Therefore, letting $b = a^k$ gives us that $a^k \equiv -1 \pmod{p}$.

(c) Since teh order of a divides $\phi(n)$, then $n - 1 \leqslant \phi(n)$. On the other hand, $\phi(n) \leqslant n-1$ by looking at the definition of $\phi(n)$. Therefore, $\phi(n) = n-1$, and hence, n is prime.

3. Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$. [*Hint:* The integer 2 has order n modulo $2^n - 1$.]

Solution First, notice that $2^n \equiv 1 \pmod{2^n - 1}$, and $2^k \not\equiv 1 \pmod{2^n - 1}$ for all $1 \leqslant k < n$ because $2^k - 1 < 2^n - 1$. Thus, the order of 2 is n modulo $2^n - 1$. Therefore, n divides $\phi(2^n - 1)$.

4. Assume that the order of a modulo n is h and the order of b modulo n is k. Show that the order of ab modulo n divides hk; in particular, if $\gcd(h,k) = 1$, then

ab has order hk.

Solution Since $a^h \equiv b^k \equiv 1 \pmod{n}$, then

$$(ab)^{hk} = (a^h)^k(b^k)^h \equiv 1 \pmod{n}.$$

Therefore, the order of ab modulo n divides hk. In particular, suppose that $\gcd(h,k) = 1$, then the order d of ab divides hk. By Theorem 8-3, the order of $(ab)^h$ is $d/\gcd(d,h)$. But since $(ab)^h \equiv b^h$, then the corollary of Theorem 8-3 implies that the order of $(ab)^h$ is k. Thus, $d/\gcd(d,h) = k$ which implies that k divides d. In the exact same way, we can prove that h divides d. Since $\gcd(h,k) = 1$, hk divides d so $d = hk$. Therefore, the order ab is hk.

5. Given that a has order 3 modulo p, where p is an odd prime, show that $a+1$ must have order 6 modulo p. [*Hint:* From $a^2 + a + 1 \equiv 0 \pmod{p}$, it follows that $(a+1)^2 \equiv a \pmod{p}$ and $(a+1)^3 \equiv -1 \pmod{p}$.]

Solution Since a has order 3, then $a^3 - 1 \equiv 0 \pmod{p}$. Equivalently, $(a-1)(a^2 + a + 1) \equiv 0 \pmod{p}$. Since p is an odd prime and $a \not\equiv 1 \pmod{p}$, then $a^2 + a \equiv -1 \pmod{p}$. It follows that

$$(a+1)^3 = a^3 + 3(a^2 + a) + 1 \equiv 2 - 3 = -1 \pmod{p}.$$

Hence, $(a+1)^6 \equiv 1 \pmod{p}$, so the order of $a+1$ must be a divisor of 6, in other words, the order of $a+1$ is 1, 2, 3, or 6. If it was 1, then $a+1 \equiv 1 \pmod{p}$ implying that $a \equiv 0 \pmod{p}$. But this is impossible since $a^3 \equiv 1 \pmod{p}$. The order cannot be 2 because

$$(a+1)^2 = (a^2 + a) + (a+1) \equiv a \not\equiv 1 \pmod{p}.$$

Finally, the order of $a+1$ cannot be 3 because $(a+1)^3 \equiv -1 \not\equiv 1 \pmod{p}$. Therefore, the order of $a+1$ must be 6.

6. Verify the following assertions:

(a) The odd prime divisors of the integer $n^2 + 1$ are of the form $4k+1$. [*Hint:* $n^2 \equiv -1 \pmod{p}$, where p is an odd prime, implies that $4 \mid \phi(p)$ by Theorem 8-1.]

(b) The odd prime divisors of the integer $n^4 + 1$ are of the form $8k+1$.

(c) The odd prime divisors of the integer $n^2 + n + 1$ which are different from 3 are of the form $6k+1$.

Solution

(a) Let p be an odd prime divisor of the integer $n^2 + 1$, then $n^2 \equiv -1 \pmod{p}$. It follows that $n^4 \equiv 1 \pmod{p}$ so the order of n must be either 1, 2, or 4. Clearly, the order of n is not 2 since $n^2 \equiv -1 \not\equiv 1 \pmod{p}$ (p is an odd prime) and the order of n cannot be 1 because it would imply that $n^2 \equiv 1 \pmod{p}$ which is false. Thus, the order of n must be 4. Hence, $4 \mid \phi(p) = p - 1$ which implies that p is of the form $4k+1$.

(b) Let p be an odd prime divisor of the integer $n^4 + 1$, then $n^4 \equiv -1 \pmod{p}$. It follows that $n^8 \equiv 1 \pmod{p}$ so the order of n must be either 1, 2, 4, or 8. Clearly, the order of n is not 4 since $n^4 \equiv -1 \not\equiv 1 \pmod{p}$ (p is an odd prime) and the order of n cannot be 1 or 2 because it would imply that $n^4 \equiv 1 \pmod{p}$ which is false. Thus, the order of n must be 8. Hence, $8 \mid \phi(p) = p-1$ which implies that p is of the form $8k + 1$.

(c) Let p be a prime different from 2 and 3 dividing n^2+n+1, then $n^2+n+1 \equiv 0 \pmod{p}$. It follows that

$$n^3 - 1 = (n-1)(n^2+n+1) \equiv 0 \pmod{p}$$

so the order of n is either 1 or 3. The order of n cannot be 1 because otherwise, $n \equiv 1 \pmod{p}$, and hence, $0 \equiv n^2 + n + 1 \equiv 3 \pmod{p}$ which is impossible since p is not 3. Thus, the order of n is 3, impliying that $3 \mid \phi(p) = p-1$. Since p is odd, then $2 \mid p-1$. Thus, $6 \mid p-1$ which implies that p is of the form $6k+1$.

7. Establish that there are infinitely many primes of each of the forms $4k + 1$, $6k + 1$, and $8k + 1$. [*Hint:* Assume that there are only finitely many primes of the form $4k+1$; call them $p_1, p_2, ..., p_r$. Consider the integer $(2p_1p_2\cdots p_r)^2 + 1$ and apply the previous problem.]

Solution Suppose that there are finitely many primes $p_1, ..., p_m$ of the form $4k+1$, and define the integer $n = 2p_1 \cdots p_m$, then n^2+1 is an odd number. Let p be a prime dividing $n^2 + 1$, then this number is odd, and hence, by the previous problem, p is of the form $4k + 1$. Thus, $p = p_i$ for some i. But in that case, p divides $2p_1 \cdots p_m$, so p divides n^2 which implies that p divides 1, a contradiction. Therefore, there are infinitely many primes of the form $4k + 1$. Proving that there are infinitely many primes of the form $8k + 1$ is the same because $n^4 + 1$ is also odd in that case, and hence, any prime divisor of $n^4 + 1$ is a prime of the form $8k + 1$ which cannot be in the original list.

For the case $6k+1$, the proof is the same. It suffices to notice that if $p_1, ..., p_m$ is the list of all primes of the form $6k+1$, then when n is defined as twice the product of all the p_i's, then

$$n^2 + n + 1 \equiv 2^2 + 2 + 1 = 1 \pmod{6},$$

which implies that any prime divisor of $n^2 + n + 1$ must be an odd prime distinct from 3. From this, the same proof as above shows that this prime must be of the form $6k + 1$, and distinct from the p_i's.

8.

(a) Prove that if p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k. [*Hint:* Since $a^p \equiv 1 \pmod{q}$, the order of a modulo q is either 1 or p; in the latter case, $p \mid \phi(q)$.]

(b) Use part (a) to show that if p is an odd prime, then the prime divisors of $2^p - 1$ are of the form $2kp + 1$.

(c) Find the smallest prime divisor of the integers $2^{17}-1$ and $2^{29}-1$.

Solution

(a) Since $q \mid a^p - 1$, then $a^p \equiv 1 \pmod{q}$. It follows that the order of a modulo q is a divisor of p. Hence, the order of a modulo q is either 1 or p. If the order of a is 1, then $a \equiv 1 \pmod{p}$, and hence, $q \mid a-1$. Otherwise, the order of a is p, which implies that p divides $\phi(q) = q-1$. Since q is odd, then $2 \mid q-1$. Since p is odd, then $\gcd(2,p)=1$, and hence, $2p \mid q-1$. Equivalently, $q = 2kp+1$ for some integer k.

(b) Let q be a prime divisor of $2^p - 1$, then q is odd since $2^p - 1$ is clearly not even. By part (a), either $q \mid 2-1 = 1$ or $q = 2kp+1$ for some integer k. Since $q \neq 1$, then the only possibility is that $q = 2kp+1$ for some integer k.

(c) By part (b), the prime divisors of $2^{17}-1 = 131071$ must be of the form $34k+1$ where k is an integer. Let's find the smallest divisor of $2^{17}-1$ by iterating over $k \geqslant 1$:

- $34 \cdot 1 + 1 = 35$: not a prime.
- $34 \cdot 2 + 1 = 69$: not a prime.
- $34 \cdot 3 + 1 = 103$: a prime. By computing the remainder of 131071 when divided by 103, we get 55 which shows that 103 is not a divisor of $2^{17}-1$.
- $34 \cdot 4 + 1 = 137$: a prime. By computing the remainder of 131071 when divided by 137, we get 99 which shows that 137 is not a divisor of $2^{17}-1$.
- $34 \cdot 5 + 1 = 171$: not a prime.
- $34 \cdot 6 + 1 = 205$: not a prime.
- $34 \cdot 7 + 1 = 239$: a prime. By computing the remainder of 131071 when divided by 239, we get 99 which shows that 239 is not a divisor of $2^{17}-1$.
- $34 \cdot 8 + 1 = 273$: not a prime.
- $34 \cdot 9 + 1 = 307$: a prime. By computing the remainder of 131071 when divided by 307, we get 289 which shows that 307 is not a divisor of $2^{17}-1$.
- $34 \cdot 10 + 1 = 341$: not a prime.

Since $362 \leqslant \sqrt{2^{17}-1} \leqslant 363$ and the next number is $34 \cdot 11 + 1 = 375 > 363$, then we are done checking for primes dividing $2^{17}-1$, and hence, we can conclude that $2^{17}-1$ is prime.

By part (b), the prime divisors of $2^{29}-1 = 536,870,911$ must be of the form $58k+1$ where k is an integer. Let's find the smallest divisor of $2^{29}-1$ by iterating over $k \geqslant 1$:

- $58 \cdot 1 + 1 = 59$: a prime. By computing the remainder of 536,870,911 when divided by 59, we get 57 which shows that 59 is not a divisor of $2^{29}-1$.
- $58 \cdot 2 + 1 = 117$: not a prime.
- $58 \cdot 3 + 1 = 175$: not a prime.

- $58 \cdot 4 + 1 = 233$: a prime. By computing the remainder of 536,870,911 when divided by 233, we get 0 which shows that 59 is a divisor of $2^{29} - 1$.

Therefore, 233 is the smallest prime divisor of $2^{29} - 1$.

9. Prove that there are infinitely many primes of the form $2kp + 1$, where p is an odd prime. [*Hint:* Assume that there are finitely many primes of the form $2kp + 1$, call them $q_1, q_2, ..., q_r$, and consider the integer $(q_1 q_2 \cdots q_r)^p - 1$.]

Solution Suppose that $q_1, ..., q_n$ forms the complete (finite) list of primes of the form $2kp + 1$. If we let $a = q_1 \cdots q_n$, then a and a^p are of the form $2kp + 1$ as well (a product of elemnents of the form $mk + 1$ is also of that form). It follows that the integer $a^p - 1$ is of the form $2kp$, and hence, it is not a power of 2. Thus, the integer $a^p - 1$ must have an odd prime divisor q. By the previous Problem, we must have $q \mid a - 1$ or $q = 2kp + 1$. The first case implies that $q \mid q_1 \cdots q_n - 1$.

Unfortunately, I was not able to prove that the statement $q \mid a - 1$ leads to a contradiction. I don't see any other way of solving this exercice, especially since the hint of the exercise tells us to go this way. I will not spend more time on this exercise because it was removed from the following editions of this book.

10.

(a) Verify that 2 is a primitive root of 19, but not 17.

(b) Show that 15 has no primitive roots by calculating the orders of 2, 4, 7, 8, 11, 13, and 14 modulo 15.

Solution

(a) It suffices to show that the order of 2 modulo 19 is 18. Since the order of a number is necessarily a divisor of $\phi(19) = 18$, it suffices to verify that the order of 2 modulo 19 is not 1, 2, 3, 6, and 9:

$$\begin{aligned} 2^1 &\equiv 2 \not\equiv 1 \pmod{19}, \\ 2^2 &\equiv 4 \not\equiv 1 \pmod{19}, \\ 2^3 &\equiv 8 \not\equiv 1 \pmod{19}, \\ 2^6 &\equiv 7 \not\equiv 1 \pmod{19}, \\ 2^9 &\equiv 18 \not\equiv 1 \pmod{19}. \end{aligned}$$

Therefore, 2 is a primitive root of 19. However, 2 is not a primitive root of 17 because the order of 2 modulo 17 is 8 (Problem 1 part (a)) and not 16.

(b) The integers which are prime relative to and less than 15 are 2, 4, 7, 8, 11, 13, and 14. To find the order of an integer, it suffices to raise this integer to the 2nd and 4th power because the order must be a divisor of $\phi(15) = 8$ and we know that none of these integers have order 1.

(a) Since $2^2 \equiv 4 \not\equiv 1 \pmod{15}$, and $2^4 \equiv 1 \pmod{15}$, then 2 is not a primitive root since the order of 2 modulo 15 is 4, not 8.

(b) Since $4^2 \equiv 1 \pmod{15}$, then 4 is not a primitive root since the order of 4 modulo 15 is 2, not 8.

(c) Since $7^2 \equiv 4 \not\equiv 1 \pmod{15}$, and $7^4 \equiv 1 \pmod{15}$, then 7 is not a primitive root since the order of 7 modulo 15 is 4, not 8.

(d) Since $8^2 \equiv 4 \not\equiv 1 \pmod{15}$, and $8^4 \equiv 1 \pmod{15}$, then 8 is not a primitive root since the order of 8 modulo 15 is 4, not 8.

(e) Since $11^2 \equiv 1 \pmod{15}$, then 11 is not a primitive root since the order of 11 modulo 15 is 2, not 8.

(f) Since $13^2 \equiv 4 \not\equiv 1 \pmod{15}$, and $13^4 \equiv 1 \pmod{15}$, then 13 is not a primitive root since the order of 13 modulo 15 is 4, not 8.

(g) Since $14^2 \equiv 1 \pmod{15}$, then 14 is not a primitive root since the order of 14 modulo 15 is 2, not 8.

11. Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

Solution The integer r^k is a primitive root of n if and only if r^k has order $\phi(n)$. By the theorems of this section, the order of r^k is equal to the order of r divided by the greatest common divisor of the order of r and k. But since r is a primitive root, then its order is $\phi(n)$, hence, the order of r^k is $\phi(n)/\gcd(k, \phi(n))$. Thus, the first statement is equivalent to the equation $\phi(n) = \phi(n)/\gcd(k, \phi(n))$. But clearly, this is equivalent to $\gcd(k, \phi(n)) = 1$.

12.

(a) Find two primitive roots of 10.

(b) Use the information that 3 is a primitive root of 17 to obtain the eight primitive roots of 17.

Solution

(a) The primitive roots of 10 are the elements of order $\phi(10) = 4$. Since

$$3^1 \equiv 3 \not\equiv 1 \pmod{10}, \quad 3^2 \equiv 9 \not\equiv 1 \pmod{10}, \quad 3^4 \equiv 1 \pmod{10},$$

then 3 is a primitive root of 10. The other primitive root of 10 is $3^3 \equiv 7 \pmod{10}$ since $\gcd(3, \phi(10)) = 1$ (previous Problem).

(b) The integers which are prime relative and less than $\phi(17) = 16$ are 1, 3, 5, 7, 9, 11, 13, and 15. Hence, since Problem 11, the eight primitive roots of 17 are

$$\begin{aligned}
3^1 &\equiv 3 \pmod{17},\\
3^3 &\equiv 10 \pmod{17},\\
3^5 &\equiv 5 \pmod{17},\\
3^7 &\equiv 11 \pmod{17},\\
3^9 &\equiv 14 \pmod{17},\\
3^{11} &\equiv 7 \pmod{17},\\
3^{13} &\equiv 12 \pmod{17},\\
3^{15} &\equiv 6 \pmod{17}.
\end{aligned}$$

13.

(a) Prove that if p and $q > 3$ are odd primes and $q \mid R_p$, then $q = 2kp + 1$ for some integer k.

(b) Find the smallest prime divisors of the repunits $R_5 = 11111$ and $R_7 = 1111111$.

Solution

(a) Since $R_p = (10^p - 1)/9$, then $q \mid R_p$ implies that $q \mid 10^p - 1$. By Problem 8 part (a), this implies that $q \mid 9$ or that $q = 2kp + 1$ for some p. Since $q \neq 3$, then q cannot divide 9. Thus, we must have $q = 2kp + 1$ for some integer k.

(b) The prime divisors of R_5 must be of the form $10k+1$ by part (a). Let's iterate over $k \geqslant 1$ to find the smallest divisor of R_5.

- $10 \cdot 1 + 1 = 11$ is prime number but it is not a divisor of R_5 using the divisibility rule by 11.
- $10 \cdot 2 + 1 = 21$ is not a prime number.
- $10 \cdot 3 + 1 = 31$ is a prime number but the residue of R_5 after dividing by 31 is 13, so 31 is not a divisor of R_5.
- $10 \cdot 4 + 1 = 41$ is a prime number and the residue of R_5 after dividing by 41 is 0, so 41 is a divisor of R_5.

The prime divisors of R_7 must be of the form $14k+1$ by part (a). Let's iterate over $k \geqslant 1$ to find the smallest divisor of R_7.

- $14 \cdot 1 + 1 = 15$ is not a prime number.
- $14 \cdot 2 + 1 = 29$ is a prime number but the residue of R_7 after dividing by 29 is 5, so 29 is not a divisor of R_7.
- $14 \cdot 3 + 1 = 43$ is a prime number but the residue of R_7 after dividing by 43 is 34, so 43 is not a divisor of R_7.
- $14 \cdot 4 + 1 = 57$ is not a prime number.
- $14 \cdot 5 + 1 = 71$ is a prime number but the residue of R_7 after dividing by 71 is 12, so 71 is not a divisor of R_7.

- $14 \cdot 6 + 1 = 85$ is not a prime number.
- $14 \cdot 7 + 1 = 99$ is not a prime number.
- $14 \cdot 8 + 1 = 113$ is a prime number but the residue of R_7 after dividing by 113 is 95, so 113 is not a divisor of R_7.
- $14 \cdot 9 + 1 = 127$ is a prime number but the residue of R_7 after dividing by 127 is 115, so 127 is not a divisor of R_7.
- $14 \cdot 10 + 1 = 141$ is not a prime number.
- $14 \cdot 11 + 1 = 155$ is not a prime number.
- $14 \cdot 12 + 1 = 169$ is not a prime number.
- $14 \cdot 13 + 1 = 183$ is not a prime number.
- $14 \cdot 14 + 1 = 197$ is a prime number but the residue of R_7 after dividing by 197 is 31, so 197 is not a divisor of R_7.
- $14 \cdot 15 + 1 = 211$ is a prime number but the residue of R_7 after dividing by 211 is 196, so 211 is not a divisor of R_7.
- $14 \cdot 16 + 1 = 225$ is not a prime number.
- $14 \cdot 17 + 1 = 239$ is a prime number and the residue of R_7 after dividing by 239 is 0, so 239 is a divisor of R_7.

8.2 Primitive Roots for Primes

1. If p is an odd prime, prove that

(a) the only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p-1$;

(b) the congruence $x^{p-2}+\cdots+x^2+x+1 \equiv 0 \pmod{p}$ has exactly $p-2$ incongruent solutions and they are the integers 2, 3, ..., $p-1$.

Solution

(a) Let x be a solution of the congruence $x^2 \equiv 1 \pmod{p}$, then equivalently, $(x+1)(x-1) \equiv 0 \pmod{p}$. Since p is prime, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Taking one representative for each gives us that $x = 1$ and $x = p-1$ are the only two incongruent solutions of the congruence.

(b) Since the congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ incongruent solutions, namely 1, 2, ..., $p-1$, then the following equivalent congruence has the same solutions:

$$(x-1)(x^{p-2}+\cdots+x^2+x+1) \equiv 0 \pmod{p}.$$

Let x be an integer not congruent to 0 or 1 modulo p, then x satisfies the congruence above. Since it is a product, then either $x \equiv 1 \pmod{p}$ or x is a solution of the congruence

$$x^{p-2}+\cdots+x^2+x+1 \equiv 0 \pmod{p}.$$

But since x is assumed to be not congruent to 1, then x is necessarily a solution to the latter congruence. Moreover, we clearly have that when x is congruent to 0 or 1, x is not a solution to the latter congruence. Therefore, the incongruent solutions of the congruence

$$x^{p-2}+\cdots+x^2+x+1 \equiv 0 \pmod{p}$$

are 2, 3, ..., $p-1$.

2. Verify that each of the congruences $x^2 \equiv 1 \pmod{15}$, $x^2 \equiv -1 \pmod{65}$ and $x^2 \equiv -2 \pmod{33}$ has four incongruent solutions; hence, Lagrange's Theorem need not hold if the modulus is a composite number.

Solution The congruence $x^2 \equiv 1 \pmod{15}$ is equivalent to the problem of finding the integers x such that $(x-1)(x+1)$ is a multiple of 15. A product ab is a multiple of 15 if one of the following condition holds: a is a multiple of 15, b is a multiple of 15, a is a multiple of 3 and b is a multiple of 5, or a is a multiple of 5 and b is a multiple of 15. To find a solution in the first case, it suffices to find an x such that $x+1$ is a multiple of 15, we find that $x = 14$ is the only solution between 0 and 14. To find a solution in the second case, it suffices to find an x such that $x-1$ is a multiple of 15, we find that $x = 1$ is the only solution between 0 and 14. For the third case, we need to find an x such that $x-1$ is a multiple of 3 and $x+1$ is a multiple of 5, we find that $x = 4$ is the only solution between 0 and 14. Finally, for the fourth case, we need to find an x such that $x - 1$ is a multiple of 5 and $x + 1$ is a multiple of 3, we find that $x = 11$ is the only solution between 0 and 14. Therefore, there are four incongruent solutions: 1, 4, 11, 14.

If we rewrite the second equation as $(x - 8)(x + 8) \equiv 0 \pmod{65}$ and use the same method as before, we get that there are four incongruent solutions: 8, 18, 47, 57.

Similarly, if we rewrite the third equation as $(x - 8)(x + 8) \equiv 0 \pmod{33}$ and use the same method as before, we get that there are four incongruent solutions: 8, 14, 19, 25.

3. Determine all the primitive roots of the primes $p = 11$, 19, and 23, expressing each as a power of some one of the roots.

Solution To find a primitive root of 11, we start by checking if 2 is a primitive root. Since $2^5 \equiv -1 \pmod{11}$, then 2 has order 10 modulo 11 which means that 2 is a primitive root. It follows that the other primitive roots are $2^3 \equiv 8 \pmod{1}1$, $2^7 \equiv 7 \pmod{11}$ and $2^9 \equiv 6 \pmod{11}$.

To find a primitive root of 19, we start by checking if 2 is a primitive root. Since $2^9 \equiv -1 \pmod{11}$, then 2 has order 18 modulo 19 which means that 2 is a primitive root. It follows that the other primitive roots are $2^5 \equiv 13 \pmod{19}$, $2^7 \equiv 14 \pmod{19}$, $2^{11} \equiv 15 \pmod{19}$, $2^{13} \equiv 3 \pmod{19}$, and $2^{17} \equiv 10 \pmod{19}$.

To find a primitive root of 23, we start by checking if 2 is a primitive root. Since $2^{11} \equiv 1 \pmod{23}$, then 2 is not a primitive root of 23. Similarly, $3^{11} \equiv 1 \pmod{23}$, so 3 is not a primitive root of 23. However, since $5^{11} \equiv -1 \pmod{23}$, then 5 is a primitive root of 23. It follows that the otehr primitive roots of 23 are $5^3 \equiv 10 \pmod{23}$, $5^5 \equiv 20 \pmod{23}$, $5^7 \equiv 17 \pmod{23}$, $5^9 \equiv 11 \pmod{23}$, $5^{13} \equiv 21 \pmod{23}$, $5^{15} \equiv 19 \pmod{23}$, $5^{17} \equiv 15 \pmod{23}$, $5^{19} \equiv 7 \pmod{23}$, and $5^{21} \equiv 14 \pmod{23}$.

4. Given that 3 is a primitive root of 43, find

(a) all positive integers less than 43 having order 6 modulo 43;

(b) all positive integers less than 43 having order 21 modulo 43.

Solution

(a) Since 3 is a primitive root of 43, then the integers having order 6 modulo 43 are precisely the integers of the form 3^k where k satisfies $\phi(43)/\gcd(k, \phi(43)) = 6$, or equivalently, where k satisfies $\gcd(k, 42) = 7$. These integers are precisely 7 and 35. Hence, the positive integers less than 43 having order 6 modulo 43 are $3^7 \equiv 37 \pmod{43}$ and $3^{35} \equiv 7 \pmod{43}$.

(b) Since 3 is a primitive root of 43, then the integers having order 21 modulo 43 are precisely the integers of the form 3^k where k satisfies $\phi(43)/\gcd(k, \phi(43)) = 21$, or equivalently, where k satisfies $\gcd(k, 42) = 2$. These integers are precisely 2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, and 40. Hence, the positive integers less than 43 having order 21 modulo 43 are

$$\begin{aligned}
3^2 &\equiv 9 \pmod{43}; & 3^{22} &\equiv 40 \pmod{43};\\
3^4 &\equiv 38 \pmod{43}; & 3^{26} &\equiv 15 \pmod{43};\\
3^8 &\equiv 25 \pmod{43}; & 3^{32} &\equiv 13 \pmod{43};\\
3^{10} &\equiv 10 \pmod{43}; & 3^{34} &\equiv 31 \pmod{43};\\
3^{16} &\equiv 23 \pmod{43}; & 3^{38} &\equiv 17 \pmod{43};\\
3^{20} &\equiv 14 \pmod{43}; & 3^{40} &\equiv 24 \pmod{43}.
\end{aligned}$$

5. Find all positive integers less than 61 having order 4 modulo 61.

Solution First, let's find a primitive root of 61. Since $2^{30} \equiv -1 \pmod{61}$, then 2 is a primitive root of 61. It follows that the integers less than 61 having order 4 modulo 61 are precisely the integers of the form 2^k where k satisfies $\phi(61)/\gcd(k, \phi(61)) = 4$, equivalently, where k satisfies $\gcd(k, 60) = 15$. These integers k are precisely the integers 15 and 45. Therefore, positive integers less than 61 having order 4 modulo 61 are $2^{15} \equiv 11 \pmod{61}$ and $2^{45} \equiv 50 \pmod{61}$.

6. Assuming that r is a primitive root of the odd prime p, establish the following facts:

(a) The congruence $r^{(p-1)/2} \equiv -1 \pmod{p}$ holds.

(b) If r' is any other primitive root of p, then rr' is not a primitive root of p. [*Hint:* By part (a), $(rr')^{(p-1)/2} \equiv 1 \pmod{p}$.]

(c) If the integer r' is such that $rr' \equiv 1 \pmod{p}$, then r' is a primitive root of p.

Solution

(a) Since $r^{p-1} \equiv 1 \pmod{p}$, then $(r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1) \equiv 0 \pmod{p}$. Since p is prime, then $r^{(p-1)/2} \equiv 1 \pmod{p}$ or $r^{(p-1)/2} \equiv -1 \pmod{p}$. The first case cannot hold because it would contradict the fact that r has order $p-1$. Therefore, $r^{(p-1)/2} \equiv -1 \pmod{p}$.

(b) By part (a), $r^{(p-1)/2} \equiv -1 \pmod{p}$ and $(r')^{(p-1)/2} \equiv -1 \pmod{p}$. Multiplying the two equations gives us $(rr')^{(p-1)/2} \equiv 1 \pmod{p}$ which shows that rr' is not a primitive root.

(c) Let r' be an integer such that $rr' \equiv 1 \pmod{p}$, then for all $1 \leqslant k < p-1$, we have $r^k(r')^k \equiv 1 \pmod{p}$. If $(r')^k \equiv 1 \pmod{p}$, then $r^k \equiv 1 \pmod{p}$, a contradiction. Therefore, $r^k \not\equiv 1 \pmod{p}$ for all $1 \leqslant k < p-1$, so r' is a primitive root.

7. For a prime $p > 3$, prove that the primitive roots of p occur in pairs r, r' where $rr' \equiv 1 \pmod{p}$. [*Hint:* If r is a primitive root of p, consider the integer $r' = r^{p-2}$.]

Solution Let r be a primitive root of p, then by Problem 6 part (c), we have that the integer r' satisfying $rr' \equiv 1 \pmod{p}$ is also a primitive root of p. Next, this integer r' is necessarily not congruent to r because otherwise, we could rewrite the previous equation as $r^2 \equiv r^{p-1} \pmod{p}$ and conclude that $r^{p-3} \equiv 1 \pmod{p}$, which is impossible since $p > 3$. Therefore, the primitive roots occur in pairs (r, r').

8. Let r be a primitive root of the odd prime p. Prove that

(a) if $p \equiv 1 \pmod{4}$, then $-r$ is also a primitive root of p;

(b) if $p \equiv 3 \pmod{4}$, then $-r$ has order $(p-1)/2$ modulo p.

Solution

(a) Since $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is an even number. It follows that $(-r)^{(p-1)/2} = r^{(p-1)/2} \not\equiv 1 \pmod{p}$. Therefore, $-r$ is a primitive root of p.

(b) Since $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is an odd number. It follows that $(-r)^{(p-1)/2} = -r^{(p-1)/2} \equiv 1 \pmod{p}$. Hence, $-r$ has an order equal to a divisor $(p-1)/2$. Since $(p-1)/2$ is odd, then its divisors must be odd as well. Thus, if we let d be the order of $-r$, then $(-r)^d \equiv d \pmod{p}$, which is equivalent to $r^d \equiv -1 \pmod{p}$. It follows that $d = (p-1)/2$, and therefore, that $-r$ has order $(p-1)/2$ modulo p.

9. Give a different proof of Theorem 5-5 by showing that if r is a primitive root of the prime $p \equiv 1 \pmod{4}$, then $r^{(p-1)/4}$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$.

Solution Define the integer $x = r^{(p-1)/4}$, then $x^4 \equiv 1 \pmod{p}$, and hence, $x^2 - 1 \equiv 0$ or $x^2 + 1 \pmod{0} \pmod{p}$. The first case implies that $r^{(p-1)/2} = x^2 \equiv 1 \pmod{p}$, which contradicts the fact that r is a primitive root. Thus, the second case must hold, and hence, $x^2 + 1 \equiv 0 \pmod{p}$. Conversely, if there is an integer x such that $x^2 + 1 \equiv 0 \pmod{p}$, then x has order 4. But the order of x must divide $p - 1$ so $p \equiv 1 \pmod{p}$, proving Theorem 5-5.

10. Use the fact that each prime p has a primitive root to give a different proof of Wilson's Theorem. [*Hint:* If p has a primitive root r, then by Theorem 8-4, $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$.]

Solution Let r be a primitive root of p, then the integers $r^1, ..., r^{p-1}$ are congruent to the integers $1, ..., (p-1)$ in a different order. It follows that $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$. Since $1 + 2 + \cdots + (p-1) = (p-1)p/2$, then when p is odd, we have that

$$(p-1)! \equiv (r^p)^{(p-1)/2} \equiv r^{(p-1)/2} \equiv 1 \pmod{p}.$$

Since the case when p is even is trivial, this concludes the proof of Wilson's Theorem.

11. If p is a prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent modulo p to $(-1)^{\phi(p-1)}$. [*Hint:* If f is a primitive root of p, then then the integer r^k is a primitive root of p provided that $\gcd(k, p-1) = 1$; now use Theorem 7-7.]

Solution When $p > 3$, we know that the primitive roots occur in pairs (r, r') where $rr' \equiv 1 \pmod{p}$ (Problem 7). Thus, if we group the primitive roots in such pairs in the product of all primitive roots of p, then the result will be equal to 1 modulo p. Since $p > 3$ in that case, then $\phi(p-1)$ is even, and hence, $(-1)^{\phi(p-1)} = 1 =$ the product of all primitive roots of p modulo p. When $p = 2$, the only primitive root is 1 and $(-1)^{\phi(2-1)} \equiv 1 \pmod{p}$ so the statement holds. Finally, when $p = 3$, the only primitive root is -1 and $(-1)^{\phi(3-1)} = (-1)^1 = -1$. Therefore, the statement is true for all primes.

12. For an odd prime p verify that the sum

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} \text{ if } (p-1) \nmid n \\ -1 \pmod{p} \text{ if } (p-1) \mid n \end{cases}$$

[*Hint:* If $(p-1) \nmid n$, and r is a primitive root of p, then the sum is congruent modulo p to

$$1 + r^n + r^{2n} + \cdots + r^{(p-2)n} \equiv \frac{r^{(p-1)n} - 1}{r^n - 1}.]$$

Solution Let r be a primitive root of p, then

$$1^n + 2^n + \cdots + (p-1)^n \equiv (r^n)^0 + (r^n)^1 + \cdots + (r^n)^{p-2} \pmod{p}.$$

Using the formula for geometric series, we get that

$$(r^n - 1)(1^n + 2^n + \cdots + (p-1)^n) \equiv (r^n)^{p-1} - 1 \pmod{p}.$$

By Fermat's Little Theorem:

$$(r^n - 1)(1^n + 2^n + \cdots + (p-1)^n) \equiv 0 \pmod{p}.$$

When n is not a multiple of $p-1$, we have that r^n is not congruent to 1 modulo p, and hecne, the above equation becomes

$$1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}.$$

Next, if n is a multiple of $p-1$, then $r^n \equiv 1 \pmod{p}$, giving us

$$1^n + 2^n + \cdots + (p-1)^n \equiv 1^0 + 1^1 + \cdots + 1^{p-2} = p - 1 \equiv -1 \pmod{p}.$$

Therefore:

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} \text{ if } (p-1) \nmid n \\ -1 \pmod{p} \text{ if } (p-1) \mid n \end{cases}$$

8.3 Composite Numbers Having Primitive Roots

1.

(a) Find the four primitive roots of 26 and the eight primitive roots of 25.

(b) Determine all the primitive roots of 3^2, 3^3 and 3^4.

Solution

(a) First, let's find one primitive root of 26. Since $26 = 2p$ where p is an odd prime, then it suffices to find an odd primitive root of p. Since 11 is a primitive root of 13, then it is also a primitive root of 26. The other primitive roots of 26 are

$$11^5 \equiv 7 \pmod{26}, \qquad 11^7 \equiv 15 \pmod{26}, \qquad 11^{11} \equiv 19 \pmod{26}.$$

Therefore, the four primitive roots of 26 are 7, 11, 15, and 19.

Similarly, 25 is of the form p^2 where $p = 5$ is an odd prime. Hence, to find the primitive roots of 25, we first need to find a primitive root of 5 and deduce from it a primitive root of 25. Since 2 is a primitive root of 5, let's determine if it is also a primitive root of 25. Since $2^4 \equiv 16 \not\equiv 1 \pmod{25}$, then 2 is a primitive root of 25. Hence, the other primitive roots of 25 are

$$2^3 \equiv 8 \pmod{25}, \qquad 2^7 \equiv 3 \pmod{25}, \qquad 2^9 \equiv 12 \pmod{25},$$
$$2^{11} \equiv 23 \pmod{25}, \qquad 2^{13} \equiv 17 \pmod{25}, \qquad 2^{17} \equiv 22 \pmod{25}$$
$$2^{19} \equiv 13 \pmod{25}.$$

Therefore, the eight primitive roots of 25 are 2, 3, 8, 12, 13, 17, 22, and 23.

(b) The only primitive root of 3 is 2. Notice that $2^2 \not\equiv 1 \pmod{3^2}$ so 2 is also a primitive root of 3^2. It follows that 2 is a primitive root for all powers of 3. Therefore, the two primitive roots of 3^2 are

$$2^1 \equiv 2, \qquad 2^5 \equiv 5.$$

The six primitive roots of 3^3 are

$$2^1 \equiv 2, \quad 2^5 \equiv 5, \quad 2^7 \equiv 20, \quad 2^{11} \equiv 23, \quad 2^{13} \equiv 11, \quad 2^{17} \equiv 14.$$

Finally, the eighteen primitive roots of 3^4 are

$$\begin{array}{cccccc} 2^1 \equiv 2, & 2^5 \equiv 32, & 2^7 \equiv 47, & 2^{11} \equiv 23, & 2^{13} \equiv 11, & 2^{17} \equiv 14, \\ 2^{19} \equiv 56, & 2^{23} \equiv 5, & 2^{25} \equiv 20, & 2^{29} \equiv 77, & 2^{31} \equiv 65, & 2^{35} \equiv 68, \\ 2^{37} \equiv 29, & 2^{41} \equiv 59, & 2^{43} \equiv 74, & 2^{47} \equiv 50, & 2^{49} \equiv 38, & 2^{53} \equiv 41. \end{array}$$

2. For an odd prime p, establish the following facts:

(a) There are as many primitive roots of $2p^n$ as of p^n.

(b) Any primitive root r of p^n is also a primitive root of p. [*Hint:* Let r have order k modulo p. Show that $r^{pk} \equiv 1 \pmod{p^2}$, ..., $r^{p^{n-1}k} \equiv 1 \pmod{p^n}$, hence, $\phi(p^n) \mid p^{n-1}k$.]

(c) A primitive root of p^2 is also a primitive root of p^n for $n \geqslant 2$.

Solution

(a) By Theorem 8-10, both p^n and $2p^n$ have at least one primitive root. Hence, p^n has $\phi(\phi(p^n)) = \phi(p^{n-1}(p-1))$ primitive roots, and $2p^n$ has $\phi(\phi(2p^n)) = \phi(p^{n-1}(p-1))$ primitive roots. Therefore, they have the same number of primitive roots.

(b) Let r be a primitive root of p^n, and let k be the order of r modulo p, then $r^k \equiv 1 \pmod{p}$ and $k \mid p-1$. It follows that $r^k \equiv 1 + ap \pmod{p^2}$, which implies that

$$r^{pk} \equiv (1+ap)^p \equiv 1 \pmod{p^2}.$$

Similarly, if the congruence $r^{p^{m-1}k} \equiv 1 \pmod{p^m}$ for some $m \geqslant 1$, then

$$r^{p^m k} \equiv (1+bp^m)^p \equiv 1 \pmod{p^{m+1}}$$

which proves that the congruence $r^{p^{m-1}k} \equiv 1 \pmod{p^m}$ holds for all $m \geqslant 1$ by induction. In particular, we have the congruence, $r^{p^{n-1}k} \equiv 1 \pmod{p^n}$. But since r is a primitive root of p^n, then $\phi(p^n) = p^{n-1}(p-1) \mid p^{n-1}k$. This division is equivalent to $p-1 \mid k$. Thus, $k = p-1$, and therefore, r is a primitive root of p.

Another way to solve this exercise would be to notice that the residues of the powers of r modulo p^n span all the numbers prime relative to p modulo p^n. If we reduce everything modulo p, we get that the residues of r modulo p span all the numbers between 1 and $p-1$. Thus, r must be a primitive root of p.

(c) By Theorem 8-9, any primitive root of p satisfying $r^{p-1} \not\equiv 1 \pmod{p^2}$ is a primitive root of p^k for all $k \geqslant 1$. Let r be a primitive root of p^2, then by part (b), r is a primitive root of p. Moreover, since r is a primitive root of p^2, then we must have $r^{p-1} \not\equiv 1 \pmod{p^2}$ (since $p-1 < \phi(p^2) = p(p-1)$). Therefore, the primitive root r of p^2 must be a primitive root for p^n for all $n \geqslant 2$.

3. If r is a primitive root of p^2, p being an odd prime, show that the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ are precisely the integers r^p, r^{2p}, ..., $r^{(p-1)p}$.

Solution Since r is a primitive root of p^2, then every solution of the congruence is of the form r^k for some $1 \leqslant p(p-1)$. Hence, if we have a solution $x = r^k$, then equivalently, $r^{k(p-1)} \equiv 1 \pmod{p^2}$. It follows that $\phi(p^2) = p(p-1) \mid k(p-1)$, and hence, that $p \mid k$. Conversely, if $p \mid k$, then $x = r^k$ is a solution of the congruence. Therefore, the solutions of the congruence are precisely r^p, r^{2p}, ..., $r^{(p-1)p}$.

4.

(a) Prove that 3 is a primitive root of all the integers of the form 7^k and $2 \cdot 7^k$.

(b) Find a primitive root root for any integer of the form 17^k.

Solution

(a) First, 3 is a primitive root of 7, and $3^6 \equiv 43 \not\equiv 1 \pmod{7^2}$ so 3 is a primitive root of all the numbers of the form 7^k. Moreover, 3 is odd so it is also a primitive root of all the numbers of the form $2 \cdot 7^k$.

(b) We know that 3 is a primitive root of 17. Moreover, $3^{16} \equiv 171 \not\equiv 1 \pmod{17^2}$ so 3 is also a primitive root of 17^2. Therefore, 3 is a primitive for all numbers of the form 17^k.

5. Obtain all the primitive roots of 41 and 82.

Solution The integer 41 is a prime number. We know that 6 is a primitive root of 41, so the 15 other primitive roots of 41 are

$$\begin{array}{ccccc} 6^3 \equiv 11, & 6^7 \equiv 29, & 6^9 \equiv 19, & 6^{11} \equiv 28, & 6^{13} \equiv 24, \\ 6^{17} \equiv 26, & 6^{19} \equiv 34, & 6^{21} \equiv 35, & 6^{23} \equiv 30, & 6^{27} \equiv 12, \\ 6^{29} \equiv 22, & 6^{31} \equiv 13, & 6^{33} \equiv 17, & 6^{37} \equiv 15, & 6^{39} \equiv 7. \end{array}$$

To find the primitive roots of $82 = 2 \cdot 41$, it suffices to use the take the list of primitive roots of 41 and replace each even primitive root r of 41 with $r + 41$. It follows that the primitive roots of 82 are:

$$7,\ 11,\ 13,\ 15,\ 17,\ 19,\ 29,\ 35,\ 47,\ 53,\ 63,\ 65,\ 67,\ 69,\ 71,\ 75.$$

6.

(a) Prove that a primitive root r of p^k, where p is an odd prime, is a primitive root of $2p^k$ if and only if r is an odd integer.

(b) Confirm that 3, 3^3, 3^5, and 3^9 are primitive roots of $578 = 2 \cdot 17^2$, but that 3^7 and 3^{11} are not.

Solution

(a) Let r be a primitive root of p^k where p is an odd prime. If r is a primitive root of $2p^k$, then r must be prime relative to $2p^k$, and hence, r must be even. Conversely, if r is an odd integer, then r is prime relative to $2p^k$. Let d be the order of r modulo $2p^k$, then $r^d \equiv 1 \pmod{p^k}$, and so $\phi(2p^k) = \phi(p^k) \mid d$, but also $d \mid \phi(2p^k)$. Thus, $d = \phi(2p^k)$, and therefore, r is a primitive root of $2p^k$.

(b) **[There is an error in the statement of this exercise. 3^7 and 3^{11} need to be replaced by 3^4 and 3^{17}. This was changed in the more recent editions of this textbook.]** We already showed that 3 is a primitive root of 17^2 in problem 4 part (b). It follows that 3 is a primitive root of $2 \cdot 17^2$.

Hence, the primitive roots of $2 \cdot 17^2$ are precisely of the form 3^k where k is prime relative to $\phi(2 \cdot 17^2) = 2^4 \cdot 17$. Since 1, 3, 5, 9 and prime relative to $2^4 \cdot 17$, then 3, 3^3, 3^5, and 3^9 are primitive roots of $2 \cdot 17^2$, and since 4 and 17 are not prime relative to $2^4 \cdot 17$, then 3^4 and 3^{17} are not primitive roots of $2 \cdot 17^2$.

7. Assume that r is a primitive root of the odd prime p and $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$. Show that $r+tp$ is a primitive root of p^k for each $k \geqslant 1$.

Solution First, notice that $r + tp \equiv r \pmod p$, so $r+tp$ is a primitive root of p. Since $(r+tp)^2 \not\equiv 1 \pmod{p^2}$, then it must also be a primitive root of p^2, and hence, be a primitive root of all powers of p.

8. If $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, define the *universal exponent* $\lambda(n)$ of n by

$$\lambda(n) = \operatorname{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$$

where $\lambda(2) = 1$, $\lambda(2^2) = 2$, and $\lambda(2^k) = 2^{k-2}$ for $k \geqslant 3$. Prove the following statements concerning the universal exponent:

(a) For $n = 2, 4, p^k, 2p^k$, where p is an odd prime, $\lambda(n) = \phi(n)$.

(b) If $\gcd(a, 2^k) = 1$, then $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$. [*Hint:* For $k \geqslant 3$, use induction on k and the fact that $\lambda(2^{k+1}) = 2\lambda(2^k)$.]

(c) If $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod n$. [*Hint:* For each prime power p^k occurring in n, $a^{\lambda(n)} \equiv 1 \pmod{p^k}$.]

Solution

(a) The cases $n = 2, 4, p^k$ follow directly from the definition of $\lambda(n)$. When $n = 2p^k$, we have

$$\lambda(n) = \operatorname{lcm}(\lambda(2), \phi(p^k)) = \operatorname{lcm}(1, \phi(p^k)) = \phi(p^k) = \phi(2p^k).$$

(b) If $\gcd(a, 2^k) = 1$, then a is odd. When $k = 1$, $a^{\lambda(2^k)} \equiv 1 \pmod 2$. When $k = 2$, $a^{\lambda(2^k)} = a^2 \equiv 1 \pmod{2^k}$. When $k \geqslant 3$, it suffices to follow the proof of Theorem 8-7.

(c) If we write $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and take an integer a prime relative to n, then $a^{\lambda(2^{k_0})} \equiv 1 \pmod{2^{k_0}}$, which implies that $a^{\lambda(n)} \equiv 1 \pmod{2^{k_0}}$ since $\lambda(n)$ is a multiple of $\lambda(2^{k_0})$. Similarly, we have $a^{\phi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}$ by Euler's Theorem, from which it follows that $a^{\lambda(n)} \equiv 1 \pmod{p_i^{k_i}}$ since $\lambda(n)$ is a multiple of $\phi(p_i^{k_i})$. From these congruences, we get that $a^{\lambda(n)} \equiv 1 \pmod n$.

9. Verify that, for $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $\lambda(5040) = 12$ and $\phi(5040) = 1152$.

Solution We have

$$\lambda(5040) = \operatorname{lcm}(\lambda(2^4), \phi(3^2), \phi(5), \phi(7)) = \operatorname{lcm}(4, 6, 4, 6) = 12$$

and

$$\phi(5040) = \phi(2^4)\phi(3^2)\phi(5)\phi(7) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152.$$

10. Use Problem 8 to show that if $n \neq 2, 4, p^k, 2p^k$, where p is an odd prime, then n has no primitive root. [*Hint:* Except for the cases 2, 4, p^k, $2p^k$, we have $\lambda(n) \mid \frac{1}{2}\phi(n)$; hence, $a^{\phi(n)/2} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.]

Solution Let n be a natural number such that $n \neq 2, 4, p^k, 2p^k$, let's show that n has no primitive root. If $n = 2^{k_0}p_1^{k_1} \cdots p_r^{k_r}$ with $k_0 \geqslant 3$, then

$$\lambda(n) = \operatorname{lcm}(2^{k_0-2}, \phi(p_1^{k_1}), ..., \phi(p_r^{k_r})) \mid \frac{1}{2}\phi(2^{k_0})\phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = \frac{1}{2}\phi(n).$$

Hence, for all $\gcd(a, n) = 1$, we have $a^{\phi(n)/2} \equiv 1 \pmod{n}$, and thus, n has no primitive root. If $k_0 = 2$, the constraints on n force r to be greater than 1. Since $\phi(p_1^{k_1})$ is even, then $\phi(p_1^{k_1} \cdots p_r^{k_r})$ is a common multiple of $\lambda(2^2)$, $\phi(p_1^{k_1})$, ..., $\phi(p_r^{k_r})$. Hence:

$$\lambda(n) = \operatorname{lcm}(\lambda(2^2), \phi(p_1^{k_1}), ..., \phi(p_r^{k_r})) \mid \phi(p_1^{k_1} \cdots p_r^{k_r}) = \frac{1}{2}\phi(n).$$

Again, this implies that n has no primitive root. Next, if $k_0 = 1$, then the constraints on n forces $r \geqslant 2$. From this, we get that $2 \mid \gcd_i(\phi(p_i^{k_i}))$. Thus, for all $\gcd(a, n) = 1$, we have

$$\lambda(n) = \operatorname{lcm}(1, \phi(p_1^{k_1}), ..., \phi(p_r^{k_r})) = \frac{\phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})}{\gcd_i(\phi(p_i^{k_i}))} \mid \frac{1}{2}\phi(p_1^{k_1} \cdots p_r^{k_r}) = \frac{1}{2}\phi(n).$$

Again, this implies that n has no primitive root. The proof of the case $k_0 = 0$ is the same as the proof of the case $k_0 = 1$. This concludes the proof.

11.

(a) Prove that if $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv ba^{\lambda(n)-1} \pmod{n}$.

(b) Use part (a) to solve the congruences $13x \equiv 2 \pmod{40}$ and $3x \equiv 13 \pmod{77}$.

Solution

(a) If $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$. If we let $x \equiv ba^{\lambda(n)-1} \pmod{n}$, we get

$$ax \equiv ba^{\lambda(n)} \equiv 1 \pmod{n}.$$

Therefore, $x \equiv ba^{\lambda(n)-1} \pmod{n}$ is a solution of the congruence $ax \equiv b \pmod{n}$.

(b) Since

$$\lambda(40) = \operatorname{lcm}(\lambda(2^3), \phi(5)) = \operatorname{lcm}(2, 4) = 4,$$

then the solution to the congruence $13x \equiv 2 \pmod{40}$ is

$$x \equiv 2 \cdot 13^3 \equiv 2 \cdot 37 \equiv 34 \pmod{40}.$$

Similarly, since

$$\lambda(77) = \text{lcm}(\phi(7), \phi(11)) = \text{lcm}(6, 10) = 30,$$

then the solution to the congruence $3x \equiv 13 \pmod{77}$ is

$$x \equiv 13 \cdot 3^{29} \equiv 13 \cdot 26 \equiv 30 \pmod{77}.$$

8.4 The Theory of Indices

1. Find the index of 5 relative to each of the primitive roots of 13.

Solution First, recall that 2 is a primitive root of 13. Since

$$\begin{aligned} 2^1 &\equiv 2 \pmod{13}, & 2^2 &\equiv 4 \pmod{13}, & 2^3 &\equiv 8 \pmod{13},\\ 2^4 &\equiv 3 \pmod{13}, & 2^5 &\equiv 6 \pmod{13}, & 2^6 &\equiv 12 \pmod{13},\\ 2^7 &\equiv 11 \pmod{13}, & 2^8 &\equiv 9 \pmod{13}, & 2^9 &\equiv 5 \pmod{13},\\ 2^{10} &\equiv 10 \pmod{13}, & 2^{11} &\equiv 7 \pmod{13}, & 2^{12} &\equiv 1 \pmod{13}, \end{aligned}$$

it follows that the index of 5 relative to 2 is 9, and that the other primitive roots of 13 are 6, 7, and 11. To find the index of 5 relative to 6, we need to solve the equation

$$6^k \equiv 5 \pmod{13}$$

which we can rewrite as

$$2^{5k} \equiv 2^9 \pmod{13}$$

from which it follows that

$$5k \equiv 9 \pmod{12}.$$

Multiplying by 5 on both sides gives us $k \equiv 9 \pmod{12}$. Hence, the index of 5 relative to 6 is 9 as well. Using the same method, finding the index of 5 relative to 7 is equivalent to solving the congruence $11k \equiv 9 \pmod{12}$. Since this is equivalent to $k \equiv 3 \pmod{12}$, then the index of 5 relative to 7 is 3. Finally, since solving the congruence $7k \equiv 9 \pmod{12}$ gives us $k \equiv 3 \pmod{12}$, then the index of 5 relative to 11 is 3.

2. Using a table of indices for a primitive root of 11, solve the congruences

(a) $7x^3 \equiv 3 \pmod{11}$

(b) $3x^4 \equiv 5 \pmod{11}$

(c) $x^8 \equiv 10 \pmod{11}$

Solution First, let's construct a table for a primitive root of 11. Since 2 is a primitive root, then

$$\begin{aligned} 2^1 &\equiv 2 \pmod{11}, & 2^2 &\equiv 4 \pmod{11}, & 2^3 &\equiv 8 \pmod{11},\\ 2^4 &\equiv 5 \pmod{11}, & 2^5 &\equiv 10 \pmod{11}, & 2^6 &\equiv 9 \pmod{11},\\ 2^7 &\equiv 7 \pmod{11}, & 2^8 &\equiv 3 \pmod{11}, & 2^9 &\equiv 6 \pmod{11}, \end{aligned}$$

and so we get the following table:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$	10	1	8	2	4	9	7	3	6	5

(a) The congruence $7x^3 \equiv 3 \pmod{11}$ is equivalent to the congruence

$$\operatorname{ind}_2 7 + 3 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{10}.$$

Using the table, we get that this is equivalent to the congruence

$$3 \operatorname{ind}_2 x \equiv 1 \pmod{10}.$$

Multiplying both sides by 7 gives us $\operatorname{ind}_2 x \equiv 7 \pmod{10}$. Finally, using the table one last time gives us $x \equiv 7 \pmod{11}$.

(b) The congruence $3x^4 \equiv 5 \pmod{11}$ is equivalent to the congruence

$$\operatorname{ind}_2 3 + 4 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 5 \pmod{10}.$$

Using the table, we get that this is equivalent to the congruence

$$4 \operatorname{ind}_2 x \equiv -4 \pmod{10}$$

which is, in turn, equivalent to $2 \operatorname{ind}_2 x \equiv -2 \pmod 5$. Solving gives us $\operatorname{ind}_2 x \equiv -1 \equiv 4 \pmod 5$, and hence, $\operatorname{ind}_2 x \equiv 4, 9 \pmod{10}$. Therefore, $x \equiv 5, 6 \pmod{11}$.

(c) The congruence $x^8 \equiv 10 \pmod{11}$ is equivalent to the congruence

$$8 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 10 \equiv 5 \pmod{10}.$$

However, this congruence has no solution since 5 is not divisible by $2 = \gcd(8, 10)$.

3. The following is a table of indices for the prime 17 relative to the primitive root 3:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

With the aid of this table, solve the congruences

(a) $x^{12} \equiv 13 \pmod{17}$

(b) $8x^5 \equiv 10 \pmod{17}$

(c) $9x^8 \equiv 8 \pmod{17}$

(d) $7^x \equiv 7 \pmod{17}$

Solution

(a) The congruence $x^{12} \equiv 13 \pmod{17}$ is equivalent to

$$12 \operatorname{ind}_3 x \equiv \operatorname{ind}_3 13 \equiv 4 \pmod{16}.$$

Dividing the congruence by 4 gives us

$$3 \operatorname{ind}_3 x \equiv 1 \pmod 4.$$

Multiplying both sides by 3 gives us $\operatorname{ind}_3 x \equiv 3 \pmod 4$. Hence, $\operatorname{ind}_3 x \equiv 3, 7, 11, 15 \pmod{16}$ which implies that $x \equiv 6, 7, 10, 11 \pmod{17}$.

(b) The congruence $8x^5 \equiv 10 \pmod{17}$ is equivalent to

$$5\,\mathrm{ind}_3\,x \equiv \mathrm{ind}_3\,10 - \mathrm{ind}_3\,8 \equiv -7 \pmod{16}.$$

Multiplying both sides by -3 gives us $\mathrm{ind}_3\,x \equiv 5 \pmod{16}$. Hence, $x \equiv 5 \pmod{17}$.

(c) The congruence $9x^8 \equiv 8 \pmod{17}$ is equivalent to

$$8\,\mathrm{ind}_3\,x \equiv \mathrm{ind}_3\,8 - \mathrm{ind}_3\,9 \equiv 8 \pmod{16}.$$

Dividing the congruence by 8 gives us

$$\mathrm{ind}_3\,x \equiv 1 \pmod{2}.$$

Hence, $\mathrm{ind}_3\,x \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$ which implies that

$$x \equiv 3, 5, 6, 7, 10, 12, 11, 14 \pmod{17}.$$

(d) The congruence $7^x \equiv 7 \pmod{17}$ is equivalent to

$$x\,\mathrm{ind}_3\,7 \equiv \mathrm{ind}_3\,7 \pmod{16},$$

which is equivalent to $11x \equiv 11 \pmod{16}$. Therefore, $x \equiv 1 \pmod{16}$.

4. Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17. [*Hint:* Use the theory of indices.]

Solution First, let $x \equiv 3^{24} \cdot 5^{13} \pmod{17}$, then

$$\mathrm{ind}_3\,x \equiv 24\,\mathrm{ind}_3\,3 + 13\,\mathrm{ind}_3\,5 \pmod{16}.$$

Using the table of indices from the previous exercise, we get that

$$\mathrm{ind}_3\,x \equiv 24 \cdot 1 + 13 \cdot 5 = 24 + 65 \equiv 9 \pmod{16}.$$

It follows that $x \equiv 14 \pmod{17}$. Therefore, $x = 14$.

5. If r and r' are both primitive roots of the odd prime p, show that for $\gcd(a, p) = 1$

$$\mathrm{ind}_{r'}\,a \equiv (\mathrm{ind}_r\,a)(\mathrm{ind}_{r'}\,r) \pmod{p-1}.$$

This corresponds to the rule for changing the base of logarithms.

Solution By the definition of the index, we have the equation $a \equiv r^{\mathrm{ind}_r\,a} \pmod{p}$. Taking the index relative to r' on both sides gives us

$$\mathrm{ind}_{r'}\,a \equiv \mathrm{ind}_{r'}(r^{\mathrm{ind}_r\,a}) \equiv (\mathrm{ind}_r\,a)(\mathrm{ind}_{r'}\,r) \pmod{p-1}$$

which is the desired equation.

6.

(a) Construct a table of indices for the prime 17 with respect to the primitive root 5. [*Hint:* By the previous problem, $\operatorname{ind}_5 a \equiv 13 \operatorname{ind}_3 a \pmod{16}$.]

(b) Using the table in part (a), solve the congruences in Problem 3.

Solution

(a) By the previous problem, we have that

$$\operatorname{ind}_5 a \equiv (\operatorname{ind}_3 a)(\operatorname{ind}_5 3) = 13 \operatorname{ind}_3 a \pmod{16}.$$

Hence, it suffices to multiply each entry in the second row of the table in Problem 3 by 13 and reduce modulo 16. This gives us

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_5 a$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

(b) (i) The congruence $x^{12} \equiv 13 \pmod{17}$ is equivalent to

$$12 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 13 \equiv 4 \pmod{16}.$$

Dividing the congruence by 4 gives us

$$3 \operatorname{ind}_5 x \equiv 1 \pmod{4}.$$

Multiplying both sides by 3 gives us $\operatorname{ind}_5 x \equiv 3 \pmod{4}$. Hence, $\operatorname{ind}_5 x \equiv 3, 7, 11, 15 \pmod{16}$ which implies that $x \equiv 6, 7, 10, 11 \pmod{17}$.

(ii) The congruence $8x^5 \equiv 10 \pmod{17}$ is equivalent to

$$5 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 10 - \operatorname{ind}_5 8 \equiv 5 \pmod{16}.$$

This is equivalent to $\operatorname{ind}_5 x \equiv 1 \pmod{16}$. Hence, $x \equiv 5 \pmod{17}$.

(iii) The congruence $9x^8 \equiv 8 \pmod{17}$ is equivalent to

$$8 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 8 - \operatorname{ind}_5 9 \equiv -8 \pmod{16}.$$

Dividing the congruence by 8 gives us

$$\operatorname{ind}_5 x \equiv -1 \equiv 1 \pmod{2}.$$

Hence, $\operatorname{ind}_5 x \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$ which implies that

$$x \equiv 3, 5, 6, 7, 10, 12, 11, 14 \pmod{17}.$$

(vi) The congruence $7^x \equiv 7 \pmod{17}$ is equivalent to

$$x \operatorname{ind}_5 7 \equiv \operatorname{ind}_5 7 \pmod{16},$$

which is equivalent to $15x \equiv 15 \pmod{16}$. Therefore, $x \equiv 1 \pmod{16}$.

7. If r is a primitive root of the odd prime p, verify that

$$\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1) = \frac{1}{2}(p-1).$$

Solution Since $-1 \equiv p-1 \pmod{p}$, then $\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1)$. Moreover, by Problem 6(a) in Section 8.2, we have that $r^{(p-1)/2} \equiv -1 \pmod{p}$. It follows that $(p-1)/2$ is the least positive integer k such that $r^k \equiv -1 \pmod{p}$. Therefore,

$$\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1) = \frac{1}{2}(p-1).$$

8.

(a) Determine the integers a $(1 \leqslant a \leqslant 12)$ such that the congruence $ax^4 \equiv b \pmod{13}$ has a solution for $b = 2$, 5, and 6.

(b) Determine the integers a $(1 \leqslant a \leqslant p-1)$ such that the congruence $x^4 \equiv a \pmod{p}$ has a solution for $p = 7$, 11, and 13.

Solution

(a) Since 2 is a primitive root of 13, we get the equivalent congruence

$$4 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 b - \operatorname{ind}_2 a \equiv 1 - \operatorname{ind}_2 a \pmod{12}.$$

This equivalent congruence is solvable if and only if $4 = \gcd(4,12)$ divides $\operatorname{ind}_2 b - \operatorname{ind}_2 a$.

When $b = 2$, $\operatorname{ind}_2 b = 1$ so we get the condition $4 \mid 1 - \operatorname{ind}_2 a$ which is equivalent to $\operatorname{ind}_2 a \equiv 1 \pmod{4}$. Since $1 \leqslant \operatorname{ind}_2 a \leqslant 12$, then the possible values of $\operatorname{ind}_2 a$ are 1, 5, and 9. Using the table of indices in Example 8-4, we get that the possible values of a are $a \equiv 2, 5, 6 \pmod{13}$.

When $b = 5$, $\operatorname{ind}_2 b = 9$ so we get the condition $4 \mid 9 - \operatorname{ind}_2 a$ which is again equivalent to $\operatorname{ind}_2 a \equiv 1 \pmod{4}$. Thus, the possible values of a are $a \equiv 2, 5, 6 \pmod{13}$.

Finally, when $b = 6$, $\operatorname{ind}_2 b = 5$ so we get the condition $4 \mid 5 - \operatorname{ind}_2 a$ which is again equivalent to $\operatorname{ind}_2 a \equiv 1 \pmod{4}$. Thus, the possible values of a are $a \equiv 2, 5, 6 \pmod{13}$.

(b) Let r be a primitive root of p, then we get the equivalent congruence

$$4 \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{p-1}.$$

Hence, a is a solution if and only if $\gcd(4, p-1)$ divides $\operatorname{ind}_2 a$.

When $p = 7$, we can take the primitive root $r = 3$ and construct the following table of indices:

a	1	2	3	4	5	6
$\operatorname{ind}_3 a$	6	2	1	4	5	3

Since a is a solution if and only if $2 = \gcd(4,6) \mid \operatorname{ind}_3 a$, then we know that $\operatorname{ind}_3 a = 2,4,6$. Hence, using the table, the solutions are $a \equiv 1,2,4 \pmod 7$.

When $p = 11$, we can take the primitive root $r = 2$ and use the table of indices constructed in Problem 2. Since a is a solution if and only if $2 = \gcd(4,10) \mid \operatorname{ind}_2 a$, then we know that $\operatorname{ind}_2 a = 2,4,6,8,10$. Hence, using the table, the solutions are $a \equiv 1,3,4,5,9 \pmod{11}$.

Finally, when $p = 13$, we can take the primitive root $r = 2$ and use the table of indices given in Example 8-4. Since a is a solution if and only if $4 = \gcd(4,12) \mid \operatorname{ind}_2 a$, then we know that $\operatorname{ind}_2 a = 4,8,12$. Hence, using the table, the solutions are $a \equiv 1,3,9 \pmod{13}$.

9. Employ the corollary to Theorem 8-12 to establish that if p is an odd prime, then

(a) $x^2 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 4$;

(b) $x^4 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 8$.

Solution

(a) By the corollary to Theorem 8-12 (which we can apply since p is prime and $\gcd(-1,p) = 1$), the congruence

$$x^2 \equiv -1 \pmod p$$

is solvable if and only if $(-1)^{(p-1)/d} \equiv 1 \pmod p$ where $d = \gcd(2, p-1)$. Since p is odd, then $d = 2$. Moreover, the congruence $(-1)^{(p-1)/2} \equiv 1 \pmod p$ holds if and only if $(-1)^{(p-1)/2} = 1$. Thus, the original congruence is solvable if and only if $(p-1)/2$ is even, or in other words, if and only if $(p-1)/2 = 2k$ for some integer k. Equivalently, this means that $p = 4k+1$, or that $p \equiv 1 \pmod 4$.

(b) By the corollary to Theorem 8-12 (which we can apply since p is prime and $\gcd(-1,p) = 1$), the congruence

$$x^4 \equiv -1 \pmod p$$

is solvable if and only if $(-1)^{(p-1)/d} \equiv 1 \pmod p$ where $d = \gcd(4, p-1)$. As before, the congruence $(-1)^{(p-1)/d} \equiv 1 \pmod p$ is equivalent to the equation $(-1)^{(p-1)/d} = 1$, which is equivalent to $(p-1)/d$ being even, which is in turn equivalent to $p = 2dk+1$ for some integer k. But notice that p is odd so $d = 2$ or $d = 4$. Hence, $p = 2dk+1$ implies that $d = 4$ because otherwise, we would get $d = 2$ and so $p = 4k+1$, contradicting the fact that $d = \gcd(4, p-1) = 4$. Thus, the condition $p = 2dk+1$ is equivalent to $p = 8k+1$ since $d = 4$. Therefore, the original equation is equivalent to the condition $p \equiv 1 \pmod 8$.

10. Given the congruence $x^3 \equiv a \pmod p$, where $p \geqslant 5$ is a prime number and $\gcd(a,p) = 1$, prove that

(a) if $p \equiv 1 \pmod 6$, then the congruence has either no solutions or three incongruent solutions modulo p;

(b) if $p \equiv 5 \pmod 6$, then the congruence has a unique solution modulo p.

Solution

(a) Suppose that $p = 6k + 1$, then $d = \gcd(3, p-1) = 3$. Thus, by Theorem 8-12, the congruence either has no solutions, or has 3 incongruent solutions modulo p.

(b) Suppose that $p = 6k + 5$, then $d = \gcd(3, p-1) = 1$. Hence, by Theorem 8-12, it is solvable if and only if $a^{p-1} \equiv 1 \pmod p$ holds. But we know that it holds by Fermat's Little Theorem. Therefore, the congruence is solvable, and it has a unique solution modulo p since $d = 1$.

11. Show that the congruence $x^3 \equiv 3 \pmod{19}$ has no solutions, while $x^3 \equiv 11 \pmod{19}$ has three incongruent solutions.

Solution By Theorem 8-12, the congruence $x^3 \equiv 3 \pmod{19}$ is solvable if and only if the equation $3^6 \equiv 1 \pmod{19}$ holds. However,

$$3^6 \equiv 9^3 \equiv 9 \cdot 81 \equiv 9 \cdot 5 \equiv 7 \not\equiv 1 \pmod{19}.$$

Therefore, the congruence has no solutions. Similarly, the congruence $x^3 \equiv 11 \pmod{19}$ is solvable if and only if the equation $11^6 \equiv 1 \pmod{19}$ holds. Since,

$$11^6 \equiv 8^6 \equiv 7^3 \equiv 7 \cdot 11 \equiv 1 \pmod{19},$$

then the congruence has three distinct solutions ($\gcd(3, 19-1) = 3$).

12. Determine whether the two congruences $x^5 \equiv 13 \pmod{23}$ and $x^7 \equiv 15 \pmod{29}$ are solvable.

Solution By the corollary to Theorem 8-12, the congruence $x^5 \equiv 13 \pmod{23}$ is solvable if and only if the congruence $13^{22} \equiv 1 \pmod{23}$ holds. But we know that it holds by Fermat's Little Theorem. Thus, the congruence is solvable. Similarly, by the corollary to Theorem 8-12, the congruence $x^7 \equiv 15 \pmod{29}$ is solvable if and only if the congruence $15^4 \equiv 1 \pmod{29}$ holds. However,

$$15^2 = 225^2 \equiv 7^2 \equiv 20 \pmod{29}.$$

Therefore, the second congruence is not solvable.

13. If p is a prime and $\gcd(k, p-1) = 1$, prove that the integers

$$1^k,\ 2^k,\ 3^k,\ \ldots,\ (p-1)^k$$

form a reduced set of residues modulo p.

Solution First, let r be a primitive root of p and consider the integers

$$\operatorname{ind}_r 1,\ \operatorname{ind}_r 2,\ \ldots,\ \operatorname{ind}_r(p-1).$$

By the properties of indices, we know that they are congruent modulo $p-1$ to the integers $1, 2, ..., p-1$ but in a different order. It follows that the integers

$$k \operatorname{ind}_r 1,\ k \operatorname{ind}_r 2,\ \ldots,\ k \operatorname{ind}_r(p-1)$$

are also congruent to the integers $1, 2, ..., p-1$ but in a different order (Problem 12, Section 4.2). By properties of indices, the list above is the same as the list

$$\operatorname{ind}_r 1^k,\ \operatorname{ind}_r 2^k,\ \ldots,\ \operatorname{ind}_r(p-1)^k$$

so the same holds for that list. Finally, taking r to the power of each of these elements gives us that the elements

$$1^k,\ 2^k,\ 3^k,\ \ldots,\ (p-1)^k$$

are congruent to the elements $1, ..., p-1$ modulo p. Therefore, the integers $1^k, 2^k, ...,$ $(p-1)^k$ forms a reduced set of residues modulo p.

14. Let r be a primitive root of the odd prime p and let $d = \gcd(k, p-1)$. Prove that the values of a for which the congruence $x^k \equiv a \pmod p$ is solvable are r^d, r^{2d}, $\ldots$, $r^{[(p-1)/d]d}$.

Solution The congruence $x^k \equiv a \pmod p$ is equivalent to the congruence

$$k \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{p-1}.$$

If we write $a \equiv r^m \pmod p$ with $1 \leqslant m \leqslant p-1$, then the congruence becomes

$$k \operatorname{ind}_r x \equiv m \pmod{p-1}.$$

This congruence is solvable if and only if $d \mid m$. Hence, the possible values of m are $1, 2, \ldots, (p-1)/d$ which implies that the a's for which the congruence $x^k \equiv a$ $\pmod p$ is solvable are r^d, r^{2d}, $\ldots$, $r^{[(p-1)/d]d}$.

15. If r is a primitive root of the odd prime p, show that $\operatorname{ind}_r(p-a) \equiv \operatorname{ind}_r a + (p-1)/2 \pmod{p-1}$; hence, only one half of an index table need be calculated in order to complete the table.

Solution Using the rules of indices and Problem 7, simply notice that

$$\operatorname{ind}_r(p-a) = \operatorname{ind}_r(-a) \equiv \operatorname{ind}_r(-1) + \operatorname{ind}_r a \equiv \operatorname{ind}_r a + \frac{p-1}{2} \pmod{p-1}.$$

16.

(a) Let r be a primitive root of the odd prime p. Establish that the exponential congruence

$$a^x \equiv b \pmod{p}$$

has a solution if and only if $d \mid \operatorname{ind}_r b$, where the integer $d = \gcd(\operatorname{ind}_r a, p-1)$; in this case, there are d incongruent solutions modulo p.

(b) Solve the exponential congruences $4^x \equiv 13 \pmod{17}$ and $5^x \equiv 4 \pmod{19}$.

Solution

(a) **[There was an error in the statement of this question. The "...solutions modulo p." should be replaced with "...solutions modulo $p-1$.". This error was corrected in the latter editions of this book.]** The congruence $a^x \equiv b \pmod{p}$ is equivalent to the congruence $x \operatorname{ind}_r a \equiv \operatorname{ind}_r b \pmod{p-1}$ which is solvable if and only if $d = \gcd(\operatorname{ind}_r a, p-1)$ divides $\operatorname{ind}_r b$. In that case, the latter congruence has d incongruent solutions modulo $p-1$ (Theorem 4-7).

(b) Using the primitive root $r = 3$ for the prime 17 and the table of indices given in Problem 3, we get that the congruence $4^x \equiv 13 \pmod{17}$ is equivalent to the congruence $12x \equiv 4 \pmod{16}$. Dividing the congruence by 4 gives us the equivalent congruence $3x \equiv 1 \pmod{4}$, and hence, $x \equiv 3 \pmod{4}$. Therefore, the solutions of the congruence $4^x \equiv 13 \pmod{17}$ are $x \equiv 3 \pmod{4}$, or $x \equiv 3, 7, 11, 15 \pmod{16}$.

Similarly, the congruence $5^x \equiv 4 \pmod{19}$ is equivalent to the congruence $x \operatorname{ind}_2 5 \equiv \operatorname{ind}_2 4 \pmod{18}$ using the fact that 2 is a primitive root of 19. Since $2^2 \equiv 4 \pmod{19}$ and $2^{16} \equiv 5 \pmod{19}$, then the original congruence is equivalent to $16x \equiv 2 \pmod{18}$. Dividing the congruence by 2 gives us the equivalent congruence $8x \equiv 1 \pmod{9}$, and hence, $x \equiv -1 \pmod{9}$. Therefore, the solutions of the original congruence are $x \equiv -1 \pmod{9}$, or $x \equiv 8, 17 \pmod{18}$.

17. For which values of b is the exponential congruence $9^x \equiv b \pmod{13}$ solvable?

Solution Using the table given in Example 8-4, the exponential congruence $9^x \equiv b \pmod{13}$ is equivalent to the linear congruence $8x \equiv \operatorname{ind}_2 b \pmod{12}$, which is solvable if and only if $4 = \gcd(8, 12)$ divides $\operatorname{ind}_2 b$. Hence, $\operatorname{ind}_2 b = 4, 8, 12$, and therefore, the exponential congruence is solvable if and only if $b \equiv 1, 3, 9 \pmod{13}$.