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

Samy Lahlou

August 31, 2025

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 $n \geq 1$;

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

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

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

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

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 $n \geq 1$.

(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 $n \geq 1$.

(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 $n \geq 1$.

(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 $n \geq 1$.

(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 $n \geq 1$.

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 $n \geq 1$.

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 $n \geq 1$.

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 $n \geq 1$.

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 $n \leq 7$ 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 $n \geq 4$, while $n! > n^3$ for every integer $n \geq 6$.

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

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

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

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

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

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 $n \geq 1$.

8.

(a) Verify that

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

for all $n \geq 1$.

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

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 $n \geq 1$.

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

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

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

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

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

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

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

for all $n \geq 1$.

Solution
Let's prove it by induction on n. When $n = 1$, then $(1+a)^n = 1+a \geq 1+a = 1+na$, 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:

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

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

10. Prove by mathematical induction that

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

for all $n \geq 1$.

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

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

But notice that

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

and so

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

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

1.2 The Binomial Theorem

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

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

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

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 $k \geq 1$, 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 $n \geq 1$.

(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 $n \geq 1$. 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 $n = k \geq 1$, 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 $n \geq 1$.

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

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

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 $n \geq 1$, 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) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \dots$

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

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

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

Solution

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

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

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

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

(c) From the hint, it follows that

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

where the last equality follows from part (a).

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

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

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

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

Thus, using part (a), we get

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

(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 $n \geq 1$:

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

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

(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 $0 \leq r \leq n-1$ 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 $0 \leq r \leq n-1$ 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 $0 \leq r \leq n-1$ 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 $n \geq 1$, 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 $n = k \geq 1$, 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 $n \geq 2$, 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 $\binom{m}{2} + \binom{m+1}{2} = m^2$ for $m \geq 2$, 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 $n = k \geq 2$, 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 $n \geq 2$.

(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 $n \geq 1$, 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 $n = k \geq 1$,

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 $n \geq 1$.

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 $n = k \geq 2$, 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

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

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 $n \geq 1$.

(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

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

Solution

Let $n \geq 1$. 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.):

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

[*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 $n \geq 1$.

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

$$300 = 1+2+3+\cdots+24,$$
$$325 = 1+2+3+\cdots+25,$$
$$351 = 1+2+3+\cdots+26$$

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 $n \geq 1$, 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 $2b \leq r < 3b$.

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 $0 \leq r_0 < b$. This implies that if we let $q = q_0 - 2$ and $r = r_0 + 2b$, then $a = qb + r$ with $2b \leq r < 3b$. To prove that q and r are unique, let q' and r' be integers such $a = q'b + r'$ and $2b \leq r' < 3b$, then equivalently: $a = (q' + 2)b + (r' - 2b)$ where $0 \leq r' - 2b < 3b$. 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 $n \geq 1$, 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

$-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$. [*Hint:* First write $a = q'b + r'$, where $0 \leq r' < |b|$. When $0 \leq r' \leq \frac{1}{2}|b|$, let $r = r'$ and $q = q'$; when $\frac{1}{2}|b| < r' \leq |b|$, 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 $0 \leq r' < |b|$. Consider the two following cases: either $0 \leq r' \leq \frac{1}{2}|b|$ or $\frac{1}{2}|b| < r' < |b|$. In the first case, let $q = q'$ and $r = r'$ to obtain $a = qb + r$ with $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$. 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 $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$.

To prove the uniqueness of q and r, suppose that there exist integers q_0 and r_0 such that $a = q_0b + r_0$ and $-\frac{1}{2}|b| < r_0 \leq \frac{1}{2}|b|$. If $0 \leq r_0 \leq \frac{1}{2}|b| < |b|$, then by uniqueness of q' and r', we get that $q_0 = q'$ and $r_0 = r'$. Moreover, since $0 \leq r' \leq \frac{1}{2}|b|$, 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 $n \geq 1$, 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 $n \geq 1$, 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 $k \geq 1$, 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 $n \geq 1$ 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 $k \geq 1$, 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 $n \geq 1$ 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 $k \geq 1$, 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 $n \geq 1$ 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 $k \geq 1$, 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 $n \geq 1$ 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 $k \geq 2$. 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 $n \geq 1$.

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 $n \geq 0$.
[*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 $d \leq \gcd(2a, 2b) = 2 \gcd(a, b)$.]

(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, $d \leq \gcd(2a, 2b) = 2 \gcd(a, b) = 2$. 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 $n \geq 1$, 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 $n \geq 1$. When $n = 1$, it holds from our assumption. Suppose now that $\gcd(c_1, c_2^k) = 1$ for some integer $k \geq 1$, 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 $n \geq 1$. Taking $c_1 = a$ and $c_2 = b$, we get that $\gcd(a, b^n) = 1$ for all $n \geq 1$. Fixing $n \geq 1$ and taking now $c_1 = b^n$ and $c_2 = a$, we get that $\gcd(a^m, b^n) = 1$ for all $m \geq 1$. 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\text{lcm}(a, b)$. Hence, by transitivity, $\gcd(a, b) \mid \text{lcm}(a, b)$.

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

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

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

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

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

Solution

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

(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:

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

(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 $m = q\,\text{lcm}(a,b) + r$ and $0 \leq r < \text{lcm}(a,b)$. Suppose that $r \neq 0$ and notice that $r = m - q\,\text{lcm}(a,b)$ must be divisible by both a and b since a and b divide both m and $\text{lcm}(a,b)$, it follows that $\text{lcm}(a,b) \leq r$ contradicting the fact that $r < \text{lcm}(a,b)$. Thus, $r = 0$ and so $\text{lcm}(a,b) \mid m$.

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 $e \leq \gcd(\gcd(a,b),c)$. 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 $t \geq 23$. 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 $t \leq 23$. 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 $x, y, z \geq 0$, then we get the following inequalities in terms of t: $t \geq \frac{100}{3}$, $t \leq \frac{200}{5}$, $t \geq 0$. 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 $x, y \geq 1$. 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 $x, y \geq 1$, then we must have $t \leq 1$. Therefore, all the possible values of fruits in each pile are $28 - 23t$ where $t \leq 1$.

(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 $t \leq 0$. 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 $t \leq 0$.

(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 $x, y, z \geq 0$, then we get the following inequalities in terms of t: $t \geq \frac{20}{3}$, $t \leq \frac{40}{5}$, $t \geq 0$. 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 $x, y \geq 0$, 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 $a \geq 0$.

Solution Suppose that $25 = p + a^2$, then $25 - a^2$ is a prime number for some $a \geq 0$. Moreover, $0 \leq a \leq 5$ 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 $p \geq 5$ 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 $p \geq 5$, $k \neq 0$ 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 $p \geq 5$.

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 $k_1^2 x + k_2 y = 1$. 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 $k_1^3 x + k_2^2 y = 1$. 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 $n \geq 1$, 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 $a, b \leq n - 1$. 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 $n \geq 1$.

(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 $p \geq q \geq 5$ 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 $n \geq 1$.]

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 $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, then by the rule of exponents, we get $a = p_1^{2k_1} \cdot \ldots \cdot p_m^{2k_m}$ and so all the exponents are even in the canonical form of a.

Conversely, suppose that a has the following canonical form: $a = p_1^{2k_1} \cdot \ldots \cdot p_m^{2k_m}$, then by the rules of exponents, if we let $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, 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 $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$ 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 $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$. 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 $1 \leq i \leq m$ 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 $p \mid p_1 \dots p_{i-1} \cdot p_{i+1} \dots p_m$. 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 $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$ 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 $i_1, ..., i_s$ the integers i such that $r_i = 1$, and denote by $j_1, ..., j_t$ the integers j such that $r_j = 0$, then we can rewrite n as

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

Hence, if we let $a = p_{i_1} \dots p_{i_s}$ and $b = p_{i_1}^{q_{i_1}} \dots p_{i_s}^{q_{i_s}} \cdot p_{j_1}^{q_{j_1}} \dots p_{j_t}^{q_{j_t}}$, 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 $k \geq 0$ and m is an odd integer.

Solution First, write n in its canonical form: $n = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$ 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, $2 \mid p_1^{k_1} \cdot ... \cdot p_m^{k_m}$ 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 $m = p_2^{k_2} \cdot ... \cdot p_s^{k_s}$ 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 $k_1 \geq 0$.

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 $p \leq \sqrt{701}$ 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 $p \leq \sqrt[3]{n}$, 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 $n \geq 2$, $\sqrt[n]{n}$ 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 $1 \leq r \leq s$. 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, $k \geq 2$ which implies that $n < 2^n \leq k^n = n$, 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 $n \leq 1000$ and so $\sqrt{n} \leq \sqrt{1000}$. Moreover, n must have a prime factor $p \leq \sqrt{n} \leq \sqrt{1000}$. 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 $q \leq p$, 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

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

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 $p \leq n$, 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 $p \leq n$ and so $p \mid n!$. It follows that $p \mid (n! + 1) - n! = 1$, a contradiction. Therefore, p must be odd. More generally, if $p \leq n$, 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 $n \geq 5$.

(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 $n \geq 5$ 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 $2n - 1 \geq 9$ 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 $p \geq n/2$	twin pair $q \leq 3n/2$	$p+q$
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 $a \geq 0$. 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 $0 \leq a \leq 53$:

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 $n \geq 3$, 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 $n \geq 3$ 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

$$
\begin{array}{llll}
7 = 3 + 2 \cdot 2 & 25 = 19 + 2 \cdot 3 & 43 = 37 + 2 \cdot 3 & 61 = 47 + 2 \cdot 7 \\
9 = 5 + 2 \cdot 2 & 27 = 23 + 2 \cdot 2 & 45 = 41 + 2 \cdot 2 & 63 = 59 + 2 \cdot 2 \\
11 = 7 + 2 \cdot 2 & 29 = 23 + 2 \cdot 3 & 47 = 41 + 2 \cdot 3 & 65 = 59 + 2 \cdot 3 \\
13 = 7 + 2 \cdot 3 & 31 = 17 + 2 \cdot 7 & 49 = 43 + 2 \cdot 2 & 67 = 61 + 2 \cdot 3 \\
15 = 11 + 2 \cdot 2 & 33 = 29 + 2 \cdot 2 & 51 = 47 + 2 \cdot 2 & 69 = 59 + 2 \cdot 5 \\
17 = 13 + 2 \cdot 2 & 35 = 31 + 2 \cdot 2 & 53 = 47 + 2 \cdot 3 & 71 = 67 + 2 \cdot 2 \\
19 = 13 + 2 \cdot 3 & 37 = 31 + 2 \cdot 3 & 55 = 41 + 2 \cdot 7 & 73 = 67 + 2 \cdot 3 \\
21 = 17 + 2 \cdot 2 & 39 = 29 + 2 \cdot 5 & 57 = 53 + 2 \cdot 2 & 75 = 71 + 2 \cdot 2 \\
23 = 19 + 2 \cdot 2 & 41 = 37 + 2 \cdot 2 & 59 = 53 + 2 \cdot 3 &
\end{array}
$$

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 $2 \leq k \leq n+1$. Since $k \leq n+1$, then $k \mid (n+1)!$ and hence, $k \mid (n+1)!-k$. Since $k \geq 2$, 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 $n \geq 3$. 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 $p_n \leq P_n$. Therefore, by construction, we have $p_n \leq P_n < 2^n$ 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 $p \mid 6(q_1q_2\ldots q_n)$. It follows that $p \mid 6(q_1q_2\ldots q_n) - N = 1$ 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 $N = 4(3\cdot 7\cdot 11)-1$ of the form $4n+3$. Do the same for $N = 4(3\cdot 7\cdot 11\cdot 15)-1$.

Solution We have that $4(3\cdot 7\cdot 11)-1 = 923$ is divisble by the prime 71 which is of the form $4n+3$. Since $4(3\cdot 7\cdot 11\cdot 15)-1$ 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 $n \geq 1$, 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
$17 = 1+2-3-5+7-11+2\cdot 13$.
Determine similar expressions for the primes 23, 29, 31, and 37.

Solution We have

$$\begin{aligned}
23 &= -1+2-3-5+7-11+13-17+2\cdot 19,\\
29 &= 1+2-3-5+7-11+13-17+19+23,\\
31 &= 1-2+3+5-7+11-13+17-19-23+2\cdot 29,\\
37 &= 1-2+3+5-7+11-13-17+19-23+29+31.
\end{aligned}$$

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 $n \geq 0$. First, notice that if $n \geq 9$, $509-2^n < 0$ 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 $n \geq 0$. First, notice that if $n \geq 10$, $877 - 2^n < 0$ 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 $p \not| \, b$, 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

$$a + b,\ a + 2b,\ a + 3b,\ \ldots,$$

where $\gcd(a, b) = 1$, contains k consecutive terms which are composite.
[*Hint:* Put $n = (a + b)(a + 2b) \ldots (a + kb)$ and consider the k terms

$$a + (n + 1)b,\ a + (n + 2)b,\ \ldots,\ a + (n + k)b.]$$

(b) Find five consecutive composite terms in the arithmetic progression

$$6,\ 11,\ 16,\ 21,\ 26,\ 31,\ 36,\ \ldots$$

Solution

(a) Let $n = (a + b)(a + 2b) \ldots (a + kb)$ and notice that for all $1 \leq i \leq k$, 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 $p \leq p_k$, 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 $k = 1, 2, ...$]

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 $n \geq 2$ 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 $n \geq 2$ 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 $n \geq 2$.

28.

(a) If $n > 1$, show that $n!$ is never a perfect square.

(b) Find the values of $n \geq 1$ 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 $p < q < 2p \leq n$ 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 $n = 1$.