Chapter 2 Solutions

An Introduction to Mathematical Thinking: Algebra and Number Systems

William J. Gilbert and Scott A. Vanstone, Prentice Hall, 2005

Solutions prepared by William J. Gilbert and Alejandro Morales

Exercise 2-1:

Find the quotient and remainder when $b = 13$ is divided by $a = 3$.

Solution:

Since $13 = 4 \cdot 3 + 1$, the quotient is 4 and the remainder is 1.

Exercise 2-2:

Find the quotient and remainder when $b = 3$ is divided by $a = 13$.

Solution:

Since $3 = 0 \cdot 13 + 3$ the quotient is 0 and the remainder is 3.

Exercise 2-3:

Find the quotient and remainder when $b = 7$ is divided by $a = 7$.

Solution:

Since $7 = 1 \cdot 7 + 0$ the quotient is 1 and the remainder is 0.

Exercise 2-4:

Find the quotient and remainder when $b = 0$ is divided by $a = 7$.

Solution:

Since $0 = 0 \cdot 7 + 0$, the quotient is 0 and the remainder is 0.

Exercise 2-5:

Find the quotient and remainder when $b = -12$ is divided by $a = 4$.

Solution:

Since $-12 = -3 \cdot 4 + 0$, the quotient is -3 and the remainder is 0.

Exercise 2-6:

Find the quotient and remainder when $b = -10$ is divided by $a = 4$.

Solution:

Since $-10 = -3 \cdot 4 + 2$, the quotient is -3 and the remainder is 2.

Exercise 2-7:

Find the quotient and remainder when $b = -246$ is divided by $a = 11$.

Solution:

Since $-246 = -23 \cdot 11 + 7$, the quotient is -23 and the remainder is 7.

Exercise 2-8:

Find the quotient and remainder when $b = -5$ is divided by $a = 17$.

Solution:

Since $-5 = -1(17) + 12$, the quotient is -1 and the remainder is 12.

Exercise 2-9:

If $3p^2 = q^2$ where $p, q \in \mathbb{Z}$, show that 3 is a common divisor of p and q.

Solution 1:

Since $3|3p^2$, $3|q^2$. By Theorem 2.53 (or Proposition 2.28) $3|q$. Let $q = 3t$, with $t \in \mathbb{Z}$. Then, $3p^2 = 9t^2$. Since $3|3t^2$, $3|p^2$, and so $3|p$.

Solution 2:

Since $3|3p^2$, $3|q^2$. But every prime factor of q appears an even number of times as a factor q^2. Thus $3|q$. Let $q = 3t$, with $t \in \mathbb{Z}$. Then, $3p^2 = 9t^2$. Since $3|3t^2$, $3|p^2$, and so $3|p$.

Exercise 2-10: If $ac \mid bc$ and $c \neq 0$ prove that $a|b$

Solution:

Let $ac \mid bc$. This means there exists $q \in \mathbb{Z}$ such that $bc = q \cdot ac$. Since $c \neq 0$, we can divide by c, and obtain $b = qa$. Hence $a|b$.

Exercise 2-11: Prove that $\gcd(ad, bd) = |d| \cdot \gcd(a, b)$.

Solution:

If $d = 0$, then both sides of the equation are clearly equal to 0.

Suppose $d > 0$ and let $e = \gcd(a, b)$. Then the right side of the equation equals de. We must show that $\gcd(ad, bd) = de$. Since $e \mid a$, then $a = qe$ for some integer q. This tells us that $ad = qde$ and so $de \mid ad$ by definition. Similarly, since $e \mid b$, then $de \mid bd$. Therefore, de is a common divisor of ad and bd.

Since $e = \gcd(a, b)$, by the Extended Euclidean Algorithm, there exist integers x and y so that $ax + by = e$. Multiplying through by d, we obtain $(ad)x + (bd)y = de$. But de is a common divisor of ad and bd, so by the GCD Characterization Theorem, $de = \gcd(ad, bd)$.

If $d < 0$, then set $D = -d = |d|$. Then $\gcd(ad, bd) = \gcd(-ad, -bd) = \gcd(aD, bD) = D \cdot \gcd(a, b) = |d| \ \gcd(a, b)$ from the result for positive D above. This concludes the proof.

Exercise 2-12: Find $\gcd(5280, 3600)$.

Solution:

By the Euclidean Algorithm,

$$\begin{aligned} 5280 &= 1 \cdot 3600 + 1680 \\ 3600 &= 2 \cdot 1680 + 240 \\ 1680 &= 7 \cdot 240 + 0 \ . \end{aligned}$$

As the last nonzero remainder is 240, this is the gcd of 5280 and 3600.

Check: $5280 = 22 \cdot 240$, $3600 = 15 \cdot 240$ and $\gcd(22, 15) = 1$.

Exercise 2-13: Find $\gcd(484, 451)$.

Solution:

By the Euclidean Algorithm,

$$\begin{aligned} 484 &= 1 \cdot 451 + 33 \\ 451 &= 13 \cdot 33 + 22 \\ 33 &= 1 \cdot 22 + 11 \\ 22 &= 2 \cdot 11 + 0 \end{aligned}$$

As the last nonzero remainder is 11, this is the gcd of 484 and 451.

Check: $484 = 11 \cdot 44$, $451 = 11 \cdot 41$ and $\gcd(44, 41) = 1$).

Exercise 2-14: Find $\gcd(616, 427)$.

Solution:

By the Euclidean Algorithm,

$$\begin{aligned} 616 &= 1 \cdot 427 + 189 \\ 427 &= 2 \cdot 189 + 49 \\ 189 &= 3 \cdot 49 + 42 \\ 49 &= 1 \cdot 42 + 7 \\ 42 &= 6 \cdot 7 + 0. \end{aligned}$$

As the last nonzero remainder is 7, this is the gcd of 616 and 427.

Check: $616 = 7 \cdot 88$, $427 = 7 \cdot 61$ and $\gcd(88, 61) = 1$.

Exercise 2-15: Find $\gcd(1137, -419)$.

Solution:

$$\begin{aligned} 1137 &= 2(419) + 299 \\ 419 &= 1(299) + 120 \\ 120 &= 2(120) + 59 \\ 59 &= 29(2) + 1 \\ 2 &= 2(1) + 0 \ . \end{aligned}$$

By the Euclidean Algorithm, $\gcd(1137, -419) = 1$.

Exercise 2-16: Find $\gcd(19201, 3587)$.

Solution: By the Euclidean Algorithm,

$$\begin{aligned} 19201 &= 5(3587) + 1266 \\ 3587 &= 2(1266) + 1055 \\ 1266 &= 1(1055) + 211 \\ 1055 &= 5(211) + 0 \ . \end{aligned}$$

Because 211 is the last nonzero remainder, then $\gcd(19201, 3587) = 211$.

Check: $19201 = 211 \cdot 91$, $3587 = 211 \cdot 17$ and $\gcd(91, 17) = 1$.

Exercise 2-17: Find $\gcd(2^{100}, 100^2)$

Solution:

The prime factorization of 2^{100} is 2^{100}, and of 100^2 is $(2^2 \cdot 5^2) = 2^4 \cdot 5^4$. By Theorem 2.57 the $\gcd(2^{100}, 100^2) = 2^{d_1} \cdot 5^{d_2}$ where $d_1 = \min(100, 4) = 4$ and $d_2 = \min(0, 4) = 0$. Hence, $\gcd(2^{100}, 100^2) = 2^4 = 16$.

Exercise 2-18: Find $\gcd(10!, 3^{10})$.

Solution:

We need only determine the power of 3 in 10!.

$$10! = 10.9.8.7.6.5.4.3.2.1 = 3^4(10.8.7.2.5.4.2.1) \ .$$

Therefore $\gcd(10!, 3^{10}) = 3^4 = 81$.

Exercise 2-19:

If $a = 484$ and $b = 451$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

Use the Extended Euclidean Algorithm.

$484x$	$+451y =$	r	q_i
1	0	484	
0	1	451	
1	−1	33	1
−13	14	22	13
14	−15	11	1
−41	44	0	2

Therefore $484(14) + 451(-15) = 11 = \gcd(484, 451) = 14a - 15b$.

Exercise 2-20:

If $a = 5280$ and $b = 3600$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

Use the Extended Euclidean Algorithm.

$5280x$	$+3600y$	$=\ r$	q_i
1	0	5280	
0	1	3600	
1	−1	1680	1
−2	3	240	2
15	−22	0	7

Therefore $5280(-2) + 3600(3) = 240 = \gcd(5280, 3600) = -2a + 3b$.

Exercise 2-21:

If $a = 17$ and $b = 15$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

Use the Extended Euclidean Algorithm.

$17x$	$+15y$	$= r$	q_i
1	0	17	
0	1	15	
1	−1	2	1
−7	8	1	7
15	−17	0	2

Therefore $17(-7) + 15(8) = 1 = \gcd(17, 15) = -7a + 8b$.

Exercise 2-22:

If $a = 5$ and $b = 13$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

By inspection $5(-5) + 13(2) = 1$, therefore $\gcd(5, 13) = -5a + 2b$.

Exercise 2-23:

If $a = 100$ and $b = -35$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

Use the Extended Euclidean Algorithm.

$100x$	$+35y$	$=\ r$	q_i
1	0	100	
0	1	35	
1	−2	30	2
−1	3	5	1
7	−20	0	6

Therefore $100(-1) - 35(-3) = 5 = \gcd(100, -35) = -a - 3b$.

Exercise 2-24:

If $a = 3953$ and $b = 1829$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution:

Use the Extended Euclidean Algorithm.

$3953x + 1829y =$		r	q_i
1	0	3953	
0	1	1829	
1	−2	295	2
−6	13	59	6
31	−67	0	5

Therefore $3953(-6) + 1829(13) = 59 = \gcd(3953, 1829) = -6a + 13b$.

Exercise 2-25:

If $a = 51$ and $b = 17$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution: Since $51 = 3 \cdot 17$, $\gcd(51, 17) = 17 = b$.

Exercise 2-26:

If $a = 431$ and $b = 0$, write $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.

Solution: Since $\gcd(a, 0) = |a|$, $\gcd(431, 0) = 431 = a$.

Exercise 2-27:

Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$

Solution:

Use the contrapositive proof method to prove each implication, noting that NOT $\gcd(a, c) = \gcd(b, c) = 1$ is equivalent to $\gcd(a, c) \neq 1$ OR $\gcd(b, c) \neq 1$.

First prove:

$$\gcd(ab, c) \neq 1 \implies \gcd(a, c) \neq 1 \text{ OR } \gcd(b, c) \neq 1.$$

If $\gcd(ab, c) \neq 1$ there is a prime p such that $p|ab$ and $p|c$. By Theorem 2.53, either $p|a$ or $p|b$. Hence either ($p|a$ and $p|c$) or ($p|b$ and $p|c$); that is, either $\gcd(a, c) \neq 1$ or $\gcd(b, c) \neq 1$.

Now prove:

$$\gcd(a, c) \neq 1 \text{ OR } \gcd(b, c) \neq 1 \implies \gcd(ab, c) \neq 1.$$

If $\gcd(a, c) \neq 1$ or $\gcd(b, c) \neq 1$, there is a prime p such that ($p|a$ and $p|c$) or ($p|b$ and $p|c$). In either case, $p|ab$ and $p|c$; hence $\gcd(ab, c) \neq 1$.

Exercise 2-28: Prove that any two consecutive integers are coprime.

Solution:

Consider the consecutive integers n and $n+1$. Because $n(-1)+(n+1)(1) = 1$, by Proposition 2.27 (i), $\gcd(n, n+1) = 1$ and the consecutive integers are coprime.

Exercise 2-29: Simplify $\dfrac{95}{646} + \dfrac{40}{391}$.

Solution:

Using the Euclidean Algorithm we can find the $\gcd(95, 646)$ to simplify the fractions.

$$\begin{aligned} 646 &= 6 \cdot 95 + 76 \\ 95 &= 1 \cdot 76 + 19 \\ 76 &= 4 \cdot 19 + 0 \end{aligned}$$

Hence $\gcd(95, 646) = 19$. So, we can simplify $\frac{95}{646}$ into $\frac{5}{34}$. Taking common denominator we get

$$\frac{5}{34} + \frac{40}{391} = \frac{3315}{13294}$$

To simplify the final answer we use again the Euclidean Algorithm to find the $\gcd(3315, 13294)$.

$$\begin{aligned} 13294 &= 4 \cdot 3315 + 34 \\ 3315 &= 17 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Hence $\gcd(3315, 13294) = 17$. Dividing by 17 we get

$$\frac{3315}{13294} = \frac{195}{782}.$$

Check:
Using a calculator: $\frac{95}{646} + \frac{40}{391} \approx 0.147 + 0.1023 \approx 0.2494$ and $\frac{195}{782} \approx 0.2494$.

Exercise 2-30:

Gear A turns at 1 rev/min and is meshed into gear B. If A has 32 teeth and B has 120 teeth, how often will both gears be simultaneously back in their starting positions?

Solution:

One revolution of gear A gives 32/120 revs of B so n revolutions of gear A give $\frac{32n}{120}$ revolutions of B. We want the least integer n so that $\frac{32n}{120} = \frac{4n}{15}$ will be an integer. This is $n = 15$. Every 15 revolutions of A (15 minutes) give 4 revolutions of B.

Exercise 2-31:

Find one integer solution, if possible, to the following diophantine equation:

$21x + 35y = 7$

Solution:

By inspection $21(2) + 35(-1) = 7$. Therefore, a solution is $x = 2$ and $y = -1$.

Exercise 2-32:

Find one integer solution, if possible, to the following Diophantine equation.

$14x + 18y = 5$

Solution:

Since the greatest common divisor of 14 and 18 is 2, and $2 \nmid 5$, it follows that the Diophantine equation $14x + 18y = 5$ does not have a solution.

Exercise 2-33:

Find one integer solution, if possible, to the following Diophantine equation.

$x + 14y = 9$

Solution:

By inspection $9 + 14(0) = 9$ so $x_0 = 9$ and $y_0 = 0$ is a solution.

Exercise 2-34:

Find one integer solution, if possible, to the following Diophantine equation.

$11x + 15y = 31$

Solution:

By inspection $11(11) + 15(-8) = 1$. Multiplying by 31 gives

$$11(341) + 15(-248) = 31.$$

So $x_0 = 341$ and $y_0 = -248$ is a particular solution.

Exercise 2-35:

Find one integer solution, if possible, to the following Diophantine equation.

$143x + 253y = 156$

Solution:

By the Euclidean Algorithm

$$\begin{aligned} 253 &= 1 \cdot (143) + 110 \\ 143 &= 1 \cdot (110) + 33 \\ 110 &= 3 \cdot (33) + 11 \\ 33 &= 3 \cdot (11) + 0 \end{aligned}$$

Since $\gcd(253, 143) = 11$ but $11 \nmid 156$, the Diophantine equation does not have a solution.

Exercise 2-36:

Find one integer solution, if possible, to the following Diophantine equation.

$91x + 126y = 203$

Solution:

We use the Extended Euclidean Algorithm to find the gcd$(91, 126)$.

$126y$	$+91x$	$=\ r$	q_i
1	0	126	
0	1	91	
1	−1	35	1
−2	3	21	2
3	−4	14	1
−5	7	7	1
13	−18	0	2

Thus $\gcd(91, 126) = 7$ and $91(7) + 126(-5) = 7$. Since $203 = 7(29)$, then $91(29)(7) + 126(29)(-5) = 203$. $91(203) + 126(-145) = 203$. Therefore, a solution is $x_0 = 203$ and $y_0 = -145$.

Check: $91 \cdot 203 - 126 \cdot 145 = 18473 - 18270 = 203$.

Exercise 2-37: Find all the integer solutions of $7x + 9y = 1$.

Solution:

Since $\gcd(7, 9) = 1$ a solution exists. By inspection $7(-5) + 9(4) = 1$. Therefore, a particular solution is $x = -5$ and $y = 4$. Hence the general solution is

$$\left.\begin{array}{l} x = -5 + 9n \\ y = 4 - 7n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Check: $7(-5 + 9n) + 9(4 - 7n) = -35 + 63n + 36 - 63n = 1$.

Exercise 2-38: Find all the integer solutions of $212x + 37y = 1$.

Solution:

We use the Extended Euclidean algorithm to find gcd$(212, 37)$:

$212x$	$+37y$	$=\ r$	q_i
1	0	212	
0	1	37	
1	−5	27	5
−1	6	10	1
3	−17	7	2
−4	23	3	1
11	−63	1	2
−37	212	0	3

Thus, $\gcd(212, 37) = 1$ and $212(11) + 37(-63) = 1$. Therefore, a particular solution is $x = 11$ and $y = -63$. Hence the general solution is

$$\left.\begin{array}{l} x = 11 + 37n \\ y = -63 - 212n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Check: $212(11 + 37n) + 37(-63 - 212n) = 2332 + 7844n - 2331 - 7844n = 1$.

Exercise 2-39: Find all the integer solutions of $15x - 24y = 9$.

Solution:

Since $\gcd(15, 24) = 3$ and $3|9$ a solution exists. By inspection $15(-1) + -24(-1) = 9$. Therefore, a particular solution is $x = -1$ and $y = -1$. Hence the general solution is

$$\left.\begin{array}{l} x = -1 + 8n \\ y = -1 + 5n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Check: $15(-1 + 8n) - 24(-1 + 5n) = -15 + 120n + 24 - 120n = 9$.

Exercise 2-40: Find all the integer solutions of $16x + 44y = 20$.

Solution:

The equation is equivalent to

$$4x + 11y = 5.$$

Clearly $\gcd(4, 11) = 1$, and a combination of 4 and 11 giving 1 is:

$$4 \cdot 3 + 11(-1) = 1 \ .$$

Multiply the above by 5, we get $x_0 = 15 \ , \ y_0 = -5$ as a particular solution to the original Diophantine equation. Hence the general solution is

$$\left.\begin{array}{l} x = 15 + 11n \\ y = -5 - 4n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Check: $16(15 + 11n) + 44(-5 - 4n) = 240 + 176n - 220 - 176n = 20$.

Exercise 2-41: Find all the integer solutions of $243x + 405y = 123$.

Solution:

We use the Extended Euclidean Algorithm to find the $\gcd(243, 405)$.

$243x +$	$405y =$	r	q_i
1	0	243	
0	1	405	
1	0	243	0
−1	1	162	1
2	−1	81	1
−5	3	0	2

Since $\gcd(243, 405) = 81$, and 81 does not divide 123 ($123 = 1 \cdot 81 + 42$), the Diophantine equation $243x + 405y = 123$ has no integer solution.

Exercise 2-42: Find all the integer solutions of $169x - 65y = 91$.

Solution:

By the Extended Euclidean Algorithm,

$169x$	$+65y =$	r	q_i
1	0	169	
0	1	65	
1	−2	39	2
−1	3	26	1
2	−5	13	1
−5	13	0	2

Therefore, $\gcd(169, -65) = \gcd(169, 65) = 13$ and $169(2) - 65(5) = 13$. Notice that $91 = 13 \cdot 7$, so the Diophantine equation does have a solution. Therefore, a particular solution to $169x - 65y = 91$ is $x = 2 \cdot 7 = 14$, $y = 5 \cdot 7 = 35$. This tells us that the complete integer solution to $169x - 65y = 91$ is

$$\left.\begin{aligned} x &= 14 + \left(\tfrac{-65}{13}\right) n = 14 - 5n \\ y &= 35 - \left(\tfrac{169}{13}\right) n = 35 - 13n \end{aligned}\right\} \text{for all } n \in \mathbb{Z}.$$

Check: $169(14 - 5n) - 65(35 - 13n) = 2366 - 845n - 2275 + 845n = 91$.

Exercise 2-43: Find all the non-negative integer solutions to the diophantine equation $14x + 9y = 1000$

Solution:

Since $\gcd(14, 9) = 1$, a solution exists. By inspection $14(2) + 9(-3) = 1$. Multiplying by 1000 gives $14(2000) + 9(-3000) = 1000$.

Therefore, a particular solution is $x = 2000$ and $y = -3000$. This tells us that the general solution is

$$\left.\begin{aligned} x &= 2000 + 9n \\ y &= -3000 - 14n \end{aligned}\right\} \text{for all } n \in \mathbb{Z}.$$

Since we want non-negative solutions, then $x = 2000 + 9n \geq 0$ or $n \geq -\frac{2000}{9}$ or $n \geq -222$ since n is an integer. Similarly, $y = -3000 - 14n \geq 0$ which yields that $n \leq -\frac{3000}{14}$ or $n \leq -215$. Therefore, n can take the values between -222 and -215. These give eight non-negative solutions

$$(x, y) = (2, 108),\ (11, 94),\ (20, 80),\ (29, 66),\ (38, 52),\ (47, 38),\ (56, 24),\ (65, 10).$$

Check: $14(65) + 9(10) = 910 + 90 = 1000$.

Exercise 2-44:

Find all the **nonnegative** integer solutions of $12x + 57y = 423$.

Solution:

Clearly, $\gcd(12, 57) = 3$ and $3 \mid 423$, so integer solutions exist. To simplify the problem, we can divide through by the gcd to reduce the size of the numbers. This gives us the equation $4x + 19y = 141$. By inspection $4(5) + 19(-1) = 1$. Multiplying by 141 gives $4(705) + 19(-141) = 141$. Thus, the complete solution is

$$\left.\begin{array}{l} x = 705 + 19n \\ y = -141 - 4n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Since we want non-negative solutions, then $x = 705 + 19n \geq 0$ or $n \geq -\frac{705}{19}$ or $n \geq -37$, since n is an integer. Similarly, $y = -141 - 4n \geq 0$ which yields that $n \leq -36$. Therefore, n can take the values -37, -36, which give the non-negative solutions

$$(x, y) = (2, 7),\ (21, 3).$$

Check: $12(21) + 57(3) = 252 + 171 = 423$.

Exercise 2-45: Find all the non-negative integer solutions to the diophantine equation $38x + 34y = 200$.

Solution:

Since $\gcd(34, 38) = 2$ and $2|200$ a solution exists. Dividing the equation by 2 gives and equivalent equation, $19x + 17y = 100$.

We use the Extended Euclidean Algorithm to find a particular solution to the Diophantine equation.

$19x + 17y = r$			q_i
1	0	19	
0	1	17	
1	−1	2	1
−8	9	1	8
17	−19	0	2

We get $19(-8) + 17(9) = 1$. Multiplying by 100 gives $19(-800) + 17(900) = 100$. Therefore, a particular solution is $x = -800$ and $y = 900$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -800 + 17n \\ y = 900 - 19n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want non-negative solutions, $x = -800 + 17n \geq 0$ or $n \geq \frac{800}{17}$ or $n \geq 47.06$. Similarly, $y = 900 - 19n \geq 0$ which yields that $n \leq \frac{900}{19}$ or $n \leq 47.37$. There are no integers between 47.06 and 47.37, so there are no non-negative solutions to the Diophantine equation $38x + 34y = 200$.

Exercise 2-46:

Find all the **nonnegative** integer solutions of $11x - 12y = 13$.

Solution:

Since $\gcd(11, 12) = 1$, and $11(-1) - 12(-1) = 1$, it follows that $x_0 = -13$ and $y_0 = -13$ is a particular solution for $11x - 12y = 13$. Hence the general integer solution is

$$\left.\begin{array}{l} x = -13 - 12n \\ y = -13 - 11n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

For non-negative solutions $-13 - 12n \geq 0$ and $-13 - 11n \geq 0$, which implies that $n \leq -2$ and $n \leq -2$. Thus the complete set of non-negative solutions is

$$\left.\begin{array}{l} x = -13 - 12n \\ y = -13 - 11n \end{array}\right\} \text{ for all integers } n \text{ with } n \leq -2$$

Check: For $n = -2$, $x = 11$, $y = 9$, and $11(11) - 12(9) = 121 - 108 = 13$.

Exercise 2-47:

Can 1000 be expressed as the sum of two positive integers, one of which is divisible by 11 and the other by 17?

Solution:

Solve the Diophantine equation $11x + 17y = 1000$ The $gcd(11, 17) = 1$ so there is a solution to the Diophantine equation. By inspection $11(-3)+17(2) = 1$. Multiplying by 1000 gives $11(-3000) + 17(2000) = 1000$.

Therefore, a particular solution is $x = -3000$ and $y = 2000$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -3000 + 17n \\ y = 2000 - 11n \end{array}\right\} \text{for all } n \in \mathbb{Z}.$$

Since we want positive integers, then $x = -3000 + 17n > 0$ or $n > \frac{3000}{17}$ or $n \geq 177$ since n is an integer. Similarly, $y = 2000 - 11n > 0$ which yields that $n < \frac{2000}{11}$ or $n \leq 181$. Therefore, n can take the values between 177 and 181.

These yields five solutions:

$$\begin{array}{rcrcl} 99 & + & 901 & = & 1000 \\ 286 & + & 714 & = & 1000 \\ 473 & + & 527 & = & 1000 \\ 660 & + & 340 & = & 1000 \\ 847 & + & 153 & = & 1000. \end{array}$$

Exercise 2-48:

Can 120 be expressed as the sum of two positive integers, one of which is divisible by 11 and the other by 17?

Solution:

Solve the Diophantine equation $11x + 17y = 120$
The $\gcd(11, 17) = 1$ so there is a solution to the Diophantine equation. By inspection $11(-3) + 17(2) = 1$. Multiplying by 120 gives $11(-360) + 17(240) = 120$.

Therefore, a particular solution is $x = -360$ and $y = 240$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -360 + 17n \\ y = 240 - 11n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want positive integers, $x = -360 + 17n > 0$ or $n > \frac{360}{17}$ or $n \geq 22$ as n is an integer. Similarly, $y = 240 - 11n > 0$ which yields $n < \frac{240}{11}$ or $n \leq 21$. There is no integer satisfying $n \geq 22$ and $n \leq 21$, so there is no positive solution. Therefore is it not possible to express 120 as the sum of a positive multiple of 11 and a positive multiple of 17.

Exercise 2-49:

Can 120 be expressed as the sum of two positive integers, one of which is divisible by 14 and the other by 18?

Solution:

Solve the Diophantine equation $14x + 18y = 120$

The $\gcd(14, 18) = 2$ and $2|120$, so there is a solution to the equation. By inspection $14(4) + 18(-3) = 2$. Multiplying by 60 gives $14(240) + 18(-180) = 120$. Therefore, a particular solution is $x = 240$ and $y = -180$, and the general solution is

$$\left.\begin{array}{l} x = 240 + 9n \\ y = -180 - 7n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want positive integers, $x = 240 + 9n > 0$ or $n > -\frac{240}{9}$, or $n \geq -26$, as n is an integer. Similarly, $y = -180 - 7n > 0$ which yields $n < -\frac{180}{7}$ or $n \leq -26$. Therefore, $n = -26$, and the only solution is $x = 6$ and $y = 2$.

Check: $14(6) + 18(2) = 84 + 36 = 120$.

Exercise 2-50:

Find the smallest positive integer x so that $157x$ leaves remainder 10 when divided by 24.

Solution:

Solve the Diophantine equation

$$157x - 24y = 10.$$

Apply the Extended Euclidean Algorithm to 157 and 24:

$157x + 24y = r$			q_i
1	0	157	
0	1	24	
1	−6	13	6
−1	7	11	1
2	−13	2	1
−11	72	1	5
24	−157	0	2

Then $\gcd(24, 157) = 1$ and $157(-11) + 24(72) = 1$. Multiplying the equation by 10 gives the particular solution $x_0 = -110$ and $y_0 = 720$. Therefore the general solution to the Diophantine equation is

$$\left.\begin{array}{l} x = -110 + 24n \\ y = 720 - 157n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Now x is positive if $-110 + 24n > 0$, that is when $n > 4.58$. Hence the smallest positive solution for x occurs when $n = 5$, and $x = 10$.

Check: $1570 = 65 \cdot 24 + 10$.

Exercise 2-51:

The nickel slot of a pay phone will not accept coins. Can a call costing 95 cents be paid for exactly using only dimes and quarters? If so, in how many ways can it be done?

Solution:

Solve the Diophantine equation $10x + 25y = 95$

Where x represents the number of dimes and y the number of quarters. The $\gcd(10, 25) = 5$ and $5|95$, so there is a solution to the equation. Dividing by 5 we obtain the equivalent equation $2x+5y = 19$. By inspection $2(-2)+5(1) = 1$. Multiplying by 19 gives $2(-38) + 5(19) = 19$.

Therefore, a particular solution is $x = -38$ and $y = 19$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -38 + 5n \\ y = 19 - 2n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want a positive solution (to pay 95 cents exactly), $x = -38+5n > 0$ or $n > \frac{38}{5}$, or $n \geq 8$ as n is an integer. Similarly, $y = 19 - 2n > 0$ which yields $n < \frac{19}{2}$ or $n \leq 9$. Therefore, n can take on two values 8 or 9. So the call can be paid in two ways using only dimes and quarters:

$$\begin{array}{lllllllll} \text{for } n & = & 8, & x & = & 2 & \text{and} & y & = & 3 \\ \text{for } n & = & 9, & x & = & 7 & \text{and} & y & = & 1. \end{array}$$

Hence use 2 dimes and 3 quarters, or 7 dimes and 1 quarter.

Exercise 2-52: Convert $(5613)_7$ to base 10.

Solution:

$$\begin{aligned}(5613)_7 &= 5 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7 + 3 \;=\; 1715 + 294 + 7 + 3 \\ &= 2019 \;=\; (2019)_{10}\ .\end{aligned}$$

Exercise 2-53: Convert $(100110111)_2$ to base 10.

Solution:

$$\begin{aligned}(100110111)_2 &= 1 \cdot 2^8 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \\ &= 256 + 32 + 16 + 4 + 2 + 1 \;=\; 311 \;=\; (311)_{10}\ .\end{aligned}$$

Exercise 2-54:

Convert $(9A411)_{12}$ to base 10. Where A is the symbol for ten.

Solution:

$$\begin{aligned}(9A411)_{12} &= 9(12)^4 + 10(12)^3 + 4(12)^2 + 1 \cdot 12 + 1 \\ &= 186624 + 17280 + 576 + 13 \\ &= 204493 \;=\; (204493)_{10}\ .\end{aligned}$$

Exercise 2-55:

How many seconds are there in 4 hours 27 minutes and 13 seconds?

Solution:

The division of the hour and minute into 60 parts indicates that 4 hours 27 minutes and 13 seconds is a number in base 60. If A represents 27 and B represents 13 then:

$$\begin{aligned}(4AB)_{60} &= 4(60)^2 + 27(60) + 13 \\ &= 14400 + 1620 + 13 \\ &= 16033 \text{ seconds.}\end{aligned}$$

Exercise 2-56: Convert 1157 to base 2.

Solution:

We have

$$\begin{aligned} 1157 &= 2 \cdot 578 + \mathbf{1} \\ 578 &= 2 \cdot 289 + \mathbf{0} \\ 289 &= 2 \cdot 144 + \mathbf{1} \\ 144 &= 2 \cdot 72 + \mathbf{0} \\ 72 &= 2 \cdot 36 + \mathbf{0} \\ 36 &= 2 \cdot 18 + \mathbf{0} \\ 18 &= 2 \cdot 9 + \mathbf{0} \\ 9 &= 2 \cdot 4 + \mathbf{1} \\ 4 &= 2 \cdot 2 + \mathbf{0} \\ 2 &= 2 \cdot 1 + \mathbf{0} \\ 1 &= 0 \cdot 2 + \mathbf{1} \end{aligned}$$

and so $1157 = (10010000101)_2$.

Check: $(10010000101)_2 = 2^{10} + 2^7 + 2^2 = 1157$.

Exercise 2-57: Convert 1241 to base 9.

Solution:

By repeated use of the Division Algorithm we obtain

$$\begin{aligned} 1241 &= 137 \cdot 9 + \mathbf{8} \\ 137 &= 15 \cdot 9 + \mathbf{2} \\ 15 &= 1 \cdot 9 + \mathbf{6} \\ 1 &= 0 \cdot 9 + \mathbf{1} \ . \end{aligned}$$

Thus, $1241 = (1628)_9$.

Check: $1 \cdot 9^3 + 6 \cdot 9^2 + 2 \cdot 9 + 8 = 729 + 486 + 18 + 8 = 1241$.

Exercise 2-58: Convert 433 to base 5.

Solution:

$$\begin{aligned} 433 &= 86 \cdot 5 + \mathbf{3} \\ 86 &= 17 \cdot 5 + \mathbf{1} \\ 17 &= 3 \cdot 3 + \mathbf{2} \\ 3 &= 0 \cdot 5 + \mathbf{3}. \end{aligned}$$

Hence $433 = (3213)_5$.

Check: $(3213)_5 = 3(5^3) + 2(5^2) + 1(5) + 3 = 433$.

Exercise 2-59: Convert 30 to base 3.

Solution:

$$\begin{aligned} 30 &= 10 \cdot 3 + \mathbf{0} \\ 10 &= 3 \cdot 3 + \mathbf{1} \\ 3 &= 1 \cdot 3 + \mathbf{0} \\ 1 &= 0 \cdot 3 + \mathbf{1}. \end{aligned}$$

Hence $30 = (1010)_3$.

Check: $(1010)_3 = 1(3^3) + 1(3^1) = 30$.

Exercise 2-60: Convert 5766 to base 12, writing A for ten and B for eleven.

Solution:
By repeated use of the Division Algorithm we obtain

$$\begin{aligned} 5766 &= 480 \cdot 12 + \mathbf{6} \\ 480 &= 40 \cdot 12 + \mathbf{0} \\ 40 &= 3 \cdot 12 + \mathbf{4} \\ 3 &= 0 \cdot 12 + \mathbf{3}\ . \end{aligned}$$

Hence $5766 = (3406)_{12}$.

Check: $(3406)_{12} = 3 \cdot 12^3 + 4 \cdot 12^2 + 6 = 5766$.

Exercise 2-61: Convert 40239 to base 60.

Solution:
By repeated use of the Division Algorithm we obtain

$$\begin{aligned} 40239 &= 670 \cdot 60 + \mathbf{39} \\ 670 &= 11 \cdot 60 + \mathbf{10} \\ 11 &= 0 \cdot 60 + \mathbf{11}. \end{aligned}$$

Letting $A = 10$, $B = 11$ and $X = 39$, the answer is $(BAX)_{60}$.

Check: $(BAX)_{60} = (11) \cdot 60^2 + (10) \cdot 60^1 + 39 = 40239$.

Exercise 2-62: Add and multiply $(1011)_2$ and $(110110)_2$ together in base 2.

Solution:
The only nontrivial part of the base 2 addition and multiplication tables is $(1)_2 + (1)_2 = (10)_2$. Thus

$$\begin{array}{r} (110110)_2 \\ +\ \ (1011)_2 \\ \hline (1000001)_2 \end{array} \qquad\qquad \begin{array}{r} (110110)_2 \\ \times\ \ (1011)_2 \\ \hline (110110)_2 \\ (110110)_2 \\ (000000)_2 \\ (110110)_2 \\ \hline (1001010010)_2 \end{array}$$

Check:

$$\begin{aligned} (110110)_2 &= 2^5 + 2^4 + 2^2 + 2 = 54, \\ (1011)_2 &= 2^3 + 2 + 1 = 11 \\ (1000001)_2 &= 2^6 + 1 = 65 = 54 + 11, \\ (1001010010)_2 &= 2^9 + 2^6 + 2^4 + 2 = 594 = 54 \times 11\ . \end{aligned}$$

Exercise 2-63: Add and multiply $(3130)_4$ and $(103)_4$ together in base 4.

Solution:

Base 4 Addition Table

$+$	$(1)_4$	$(2)_4$	$(3)_4$
$(1)_4$	$(2)_4$	$(3)_4$	$(10)_4$
$(2)_4$	$(3)_4$	$(10)_4$	$(11)_4$
$(3)_4$	$(10)_4$	$(11)_4$	$(12)_4$

Base 4 Multiplication Table

$\cdot$	$(1)_4$	$(2)_4$	$(3)_4$
$(1)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(2)_4$	$(2)_4$	$(10)_4$	$(12)_4$
$(3)_4$	$(3)_4$	$(12)_4$	$(21)_4$

Thus

$$\begin{array}{r} (3130)_4 \\ +\ (103)_4 \\ \hline (3233)_4 \end{array} \qquad \begin{array}{r} (3130)_4 \\ \times\ (103)_4 \\ \hline (22110)_4 \\ +\ (313000)_4 \\ \hline (1001110)_4 \end{array}$$

Check:

$$\begin{aligned} (3130)_4 &= 3(4^3) + 1(4^2) + 3(4^1) = 220 \\ (103)_4 &= 1(4^2) + 3(4^0) = 19 \\ (3233)_4 &= 3(4^3) + 2(4^2) + 3(4^1) + 3(4^0) = 239 = 220 + 19 \\ (1001110)_4 &= 1(4^6) + 1(4^3) + 1(4^2) + 1(4^1) = 4180 = 220 \cdot 19. \end{aligned}$$

Exercise 2-64:

Write out the addition and multiplication tables for base 6 arithmetic, and then multiply $(4512)_6$ by $(343)_6$ in base 6.

Solution:

Base 6 Addition Table

$+$	$(1)_6$	$(2)_6$	$(3)_6$	$(4)_6$	$(5)_6$
$(1)_6$	$(2)_6$	$(3)_6$	$(4)_6$	$(5)_6$	$(10)_6$
$(2)_6$	$(3)_6$	$(4)_6$	$(5)_6$	$(10)_6$	$(11)_6$
$(3)_6$	$(4)_6$	$(5)_6$	$(10)_6$	$(11)_6$	$(12)_6$
$(4)_6$	$(5)_6$	$(10)_6$	$(11)_6$	$(12)_6$	$(13)_6$
$(5)_6$	$(10)_6$	$(11)_6$	$(12)_6$	$(13)_6$	$(14)_6$

Base 6 Multiplication Table

$\cdot$	$(1)_6$	$(2)_6$	$(3)_6$	$(4)_6$	$(5)_6$
$(1)_6$	$(1)_6$	$(2)_6$	$(3)_6$	$(4)_6$	$(5)_6$
$(2)_6$	$(2)_6$	$(4)_6$	$(10)_6$	$(12)_6$	$(14)_6$
$(3)_6$	$(3)_6$	$(10)_6$	$(13)_6$	$(20)_6$	$(23)_6$
$(4)_6$	$(4)_6$	$(12)_6$	$(20)_6$	$(24)_6$	$(32)_6$
$(5)_6$	$(5)_6$	$(14)_6$	$(23)_6$	$(32)_6$	$(41)_6$

Then

$$\begin{array}{r} (4512)_6 \\ \times\ \ (343)_6 \\ \hline (22340)_6 \\ (31252)_6 \\ (22340)_6 \\ \hline (3013300)_6 \end{array} \quad = \text{ Ans.}$$

Check: $(4512)_6 = 4\cdot 6^3+5\cdot 6^2+6+2 = 1052$ and $(343)_6 = 3\cdot 6^2+4\cdot 6+3 = 135$. Now $(3013300)_6 = 3\cdot 6^6 + 1\cdot 6^4 + 3\cdot 6^3 + 3\cdot 6^2 = 142020 = 1052 \times 135$.

Exercise 2-65:

Subtract $(3321)_4$ from $(10020)_4$ and check your answer by converting to base 10.

Solution: Mimic the algorithm used when subtracting in Base 10.

$$\begin{array}{r} (10020)_4 \\ -\ \ (3321)_4 \\ \hline (33)_4 \end{array}$$

Check:

$$\begin{aligned} (10020)_4 &= 1(4^4) + 2(4^1) = 264 \\ (3321)_4 &= 3(4^3) + 3(4^2) + 2(4^1) + 1(4^0) = 249 \\ (33)_4 &= 3(4^1) + 3(4^0) = 15 = 264 - 249. \end{aligned}$$

Exercise 2-66:

If $a = (342)_8$ and $b = (173)_8$, find $a - b$ without converting to base 10.

Solution:
Mimic the algorithm used when subtracting in Base 10.

$$\begin{array}{r} (342)_8 \\ -\ \ (173)_8 \\ \hline (147)_8 \end{array}$$

Check:

$$\begin{aligned} (342)_8 &= 3(8^2) + 4(8^1) + 2(8^0) = 226 \\ (173)_8 &= 1(8^2) + 7(8^1) + 3(8^0) = 123 \\ (147)_8 &= 1(8^2) + 4(8^1) + 7(8^0) = 103 = 226 - 123 \end{aligned}$$

Exercise 2-67: How many positive divisors does 12 have?

Solution: The prime factorization of 12 is $12 = 2^2 \cdot 3^1$. By Proposition 2.56 the positive divisors of 12 are those integers of the form

$$d = 2^{d_1}3^{d_2} \qquad \text{where} \quad 0 \le d_1 \le 2 \text{ and } 0 \le d_2 \le 1.$$

Thus, d_1 has three possible values $\{0, 1, 2\}$ and d_2 has two possible values $\{0, 1\}$. So 12 has $3 \cdot 2 = 6$ divisors.

Exercise 2-68: How many positive divisors does 6696 have?

Solution:

The prime factorization of 6696 is:

$$6696 = 2^3 \cdot 3^3 \cdot 31.$$

The positive divisors of 6696 are all the numbers of the form $2^{a_1}3^{a_2}, 31^{a_3}$, where

$$\begin{aligned} 0 \le a_1 \le 3 \\ 0 \le a_2 \le 3 \\ 0 \le a_3 \le 1. \end{aligned}$$

There are $(3+1)(3+1)(1+1) = 32$ different possibilities for the ordered triple (a_1, a_2, a_3). So 6696 has 32 positive divisors.

Exercise 2-69:

If we wish to add the fractions $\frac{1}{132} + \frac{4}{9}$, what is the smallest common denominator we could choose?

Solution:

The common denominator of the fractions $\frac{1}{132}$ and $\frac{4}{9}$ is a multiple of 132 and 9. The smallest common denominator is therefore the least common multiple of 132 and 9.

Because $132 = 2^2 \cdot 3 \cdot 11$ and $9 = 2^0 \cdot 3^2 \cdot 11^0$, by Theorem 2.58,

$$\text{lcm}(132, 9) = 3^{a_1} \cdot 2^{a_2} \cdot 11^{a_3},$$

where $a_1 = \max(2, 0) = 2$, $a_2 = \max(1, 2) = 2$, and $a_3 = \max(1, 0) = 1$. Hence $\text{lcm}(132, 9) = 396$.

Exercise 2-70:

Factor the following numbers into prime factors and calculate the greatest common divisor and least common multiple of each pair.

40 and 144.

Solution:

The prime factorizations of 40 and 144 are

$$\begin{aligned} 40 &= 2^3 \cdot 5 = 2^3 \cdot 3^0 \cdot 5^1 \\ 144 &= 2^4 \cdot 3^2 = 2^4 \cdot 3^2 \cdot 5^0. \end{aligned}$$

Therefore

$$\begin{aligned} \gcd(40,144) &= 2^3 \cdot 3^0 \cdot 5^0 &= 8 \\ \operatorname{lcm}(40,144) &= 2^4 \cdot 3^2 \cdot 5^1 &= 720. \end{aligned}$$

Check: $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$, so $40 \cdot 144 = 5760 = 8 \cdot 720$.

Exercise 2-71:

Factor the following numbers into prime factors and calculate the greatest common divisor and least common multiple of each pair.

5280 and 57800.

Solution:

The prime factorizations of 5280 and 57800 are

$$\begin{aligned} 5280 &= 2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 170 \\ 57800 &= 2^3 \cdot 3^0 \cdot 5^2 \cdot 11^0 \cdot 17^2. \end{aligned}$$

Therefore

$$\begin{aligned} \gcd(5280,57800) &= 2^3 \cdot 5 = 40 \\ \operatorname{lcm}(5280,57800) &= 2^5 \cdot 3 \cdot 5^2 \cdot 11 \cdot 17^2 = 7629600. \end{aligned}$$

Check: $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$ so $40 \cdot 7629600 = 305184000 = 57800 \cdot 5280$.

Exercise 2-72: Find $\operatorname{lcm}(12827, 20099)$.

Solution:

We use the Euclidean Algorithm to find the $\gcd(12807, 20099)$:

$$\begin{aligned} 20099 &= 1(12827) + 7272 \\ 12827 &= 1(7272) + 5555 \\ 7272 &= 1(5555) + 1717 \\ 5555 &= 4(1717) + 404 \\ 1717 &= 4(404) + 101 \\ 404 &= 4(101) + 0. \end{aligned}$$

By the Euclidean Algorithm, $\gcd(12827, 20099) = 101$. So, by Theorem 2.59, and long division

$$\operatorname{lcm}(12827, 20099) = (12827 \cdot 20099)/101 = 2552573.$$

Problem 2-73: Prove that $\{ax + by \mid x, y \in \mathbb{Z}\} = \{n \cdot \gcd(a,b) \mid n \in \mathbb{Z}\}$.

Solution:

To show equality of two sets, show that each is a subset of the other.

Let $c \in \{ax + by \mid x, y \in \mathbb{Z}\}$. Then $c = ax + by$ for some $x, y \in \mathbb{Z}$. We know that $\gcd(a, b) \mid a$ and b. Thus $\gcd(a, b) \mid ax + by = c$. This means $c = n \cdot \gcd(a, b)$ for $n \in \mathbb{Z}$. That is $c \in \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}$, and

$$\{ax + by \mid x, y \in \mathbb{Z}\} \subseteq \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}.$$

Now let $c \in \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}$. Thus $c = n \cdot \gcd(a, b)$ for some n. By the Extended Euclidean algorithm there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$. Therefore

$$\begin{aligned} c &= n \cdot \gcd(a, b) = asn + btn \\ &= ax + by \end{aligned}$$

where $x = sn$, and $y = t$. That is $c \in \{ax + by \mid x, y \in \mathbb{Z}\}$, and

$$\{ax + by \mid x, y \in \mathbb{Z}\} \supseteq \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}$$

which proves the result.

Problem 2-74:

Show that $\gcd(ab, c) = \gcd(b, c)$ if $\gcd(a, c) = 1$. Is it true in general that

$$\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)\,?$$

Solution:

Let $d = \gcd(b, c)$. We must show that $d = \gcd(ab, c)$. Since $d \mid b$, then $d \mid ab$. Also, $d \mid c$ since $d = \gcd(b, c)$. Therefore, d is a common divisor of ab and c. By the Extended Euclidean Algorithm, there exist integers u and v such that $au + cv = 1$ (since $\gcd(a, c) = 1$). Hence $abu + cbv = b$. If e is a common divisor of ab and c then $e|b$. Because e is also a common divisor of b and c then $|e| \leq d$. It follows that $d = \gcd(ab, c)$.

In general it is not true that $\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$. For example take $a = b = c = 2$. Then

$$\gcd(ab, c) = 2 \neq 2 \cdot 2 = \gcd(a, c) \cdot \gcd(b, c)$$

so the statement is not true in general.

Problem 2-75:

Show that the Diophantine equation $ax^2 + by^2 = c$ does not have any integer solutions unless $\gcd(a, b)|c$. If $\gcd(a, b)|c$, does the equation always have an integer solution?

Solution:

If $a = b = 0$ then the equation only has solutions if $c = 0$, and then any pair $(x, y) \in \mathbb{Z}$ will work. Otherwise suppose that the equation has a solution x_0 and y_0. Then $ax_0^2 + by_0^2 = c$. Let $d = \gcd(a, b) \neq 0$, so $d|a$ and $d|b$. By Proposition 2.11(ii), $d|ax_0^2 + by_0^2$, so $d|c$.

The converse of this statement is not true, to see this let $a = b = 1$ and $c = 3$. Then $\gcd(1, 1) = 1$, which does divide 3. However, if $x^2 + y^2 = 3$, then $x^2 \leq 3$, so $|x| \leq 1$ and $|y| \leq 1$. None of these integer values give solutions.

Problem 2-76:

For what values of a and b does the Diophantine equation $ax + by = c$ have an infinite number of positive solutions for x and y?

Solution:

In order to have any solutions we must have $\gcd(a, b)|c$. Of course $0x+0y = 0$ has infinitely many positive solutions. If a and b are nonzero, let $d = \gcd(a, b)$, and suppose there is at least one integer solution $x = x_0$, $y = y_0$. The general solution is $x = x_0 + n(b/d)$, $y = y_0 - n(a/d)$. Look at the four cases:

i) If $a > 0$ and $b > 0$, then for n sufficiently large the solutions will have opposite signs. If $-n$ is sufficiently large, the solutions will have opposite signs. Therefore there will only be finitely many solutions.

ii) If $a < 0$ and $b < 0$ then, as above, there will be no solutions.

iii) If $a > 0$ and $b < 0$, then for $-n$ sufficient large, all solutions will be positive so we will have infinitely many positive solutions.

iv) If $a < 0$ and $b < 0$, then for n sufficiently large, all solutions will be positive so we will have infinitely many positive solutions.

Hence there will be a infinite number of positive solutions if $\gcd(a, b)|c$ and a and b have opposite signs, or $a = b = c = 0$.

If a is nonzero, $b = 0$, and a and c have the same sign, then there is one positive solution for x, but an infinite number of positive solutions for y.

Problem 2-77:

For what values of c does $8x+5y = c$ have exactly one strictly positive solution?

Solution:

Let x_0, y_0 be a positive solution to $8x + 5y = c$. The general solution is given by

$$\left.\begin{array}{l} x = x_0 + 5n \\ y = y_0 - 8n \end{array}\right\} \text{ for all } n \in \mathbb{Z} \, .$$

If x_0, y_0 is to be the only positive solution, then $n = 0$ is the only value of n to give a positive solution. Now, if $n = 1$, $x_0 + 5n$ will still be positive, so we must have $y_0 - 8 \leq 0$. Similarly, if $n = -1$, $y_0 - 8n$ will still be positive, so $x_0 - 5 \leq 0$. Hence,

$$c \ \in \ \{8x + 5y \mid 1 \leq x \leq 5, \ 1 \leq y \leq 8\}.$$

This gives the 40 values, $c = 13$, 18, 21, 23, 26, 67, 70, 72, 75, 80 and all c in the range $28 \leq c \leq 65$ except 30, 32, 35, 40, 53, 58, 61 and 63.

Problem 2-78:

An oil company has a contract to deliver 100000 liters of gasoline. Their tankers can carry 2400 liters and they can attach one trailer carrying 2200 liters to each tanker. All the tankers and trailers must be completely full on this contract, otherwise the gas would slosh around too much when going over some rough roads. Find the least number of tankers required to fulfill the contract. Each trailer, if used, must be pulled by a full tanker.

Solution:

Let the number of tankers by x, and the number of trailers be y, where $y \leq x$. From the data given, we want to solve the equation

$$2400x + 2200y = 100\,000.$$

Dividing through by 200, we obtain $12x + 11y = 500$.

Clearly, $\gcd(12, 11) = 1$, so this equation has an integer solution. Now $12(1) + 11(-1) = 1$, so $12(500) + 11(-500) = 500$, and the complete solution is

$$\left.\begin{array}{l} x = 500 + 11n \\ y = -500 - 12n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

We want y to be non-negative, and $x \geq y$. Hence $y = -500 - 12n \geq 0$, and $500 + 11n \geq -500 - 12n$. That is, $n \leq -\frac{500}{12} \approx 41.67$ and $n \geq -\frac{1000}{23} \approx 43.48$. Since n is an integer, $-43 \leq n \leq -42$ and the two possible solutions are

$$(x, y) = (27, 16),\ (38, 4).$$

Therefore the least number of tankers required is 27.

Check: $2400(27) + 2200(16) = 64\,800 + 35\,200 = 100\,000$.

Problem 2-79:

A trucking company has to move 844 refrigerators. It has two types of trucks it can use, one carries 28 refrigerators and the other 34 refrigerators. If it only sends out full trucks and all the trucks return empty, list the possible ways of moving all the refrigerators.

Solution:

Let x be the number of trucks of the first type, and y be the number of trucks of the second type. The problem asks to solve the Diophantine equation

$$28x + 34y = 844.$$

Using the Extended Euclidean algorithm.

$34y$	$+28x$	$= r$	q_i
1	0	34	
0	1	28	
1	−1	6	1
−4	5	4	4
5	−6	2	1
14	−17	0	2

Since $\gcd(28, 34) = 2$ and $2|844$ an integer solution to the equation exists, and $28(-6) + 34(5) = 2$. Multiplying by 422 gives $28(-2532) + 34(2100) = 844$.

Therefore, a particular solution is $x = -2532$ and $y = 2100$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -2532 + 17n \\ y = 2100 - 14n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want non-negative integer number of trucks, $x = -2532 + 17n \geq 0$ or $n \geq 2532/17 \approx 148.94$; hence $n \geq 149$. Similarly, $y = 2100 - 14n \geq 0$, which yields $n \leq 2100/14 = 150$. Therefore, n can take the values 149 and 150, which yield the solutions

$$\begin{array}{lllllllll} \text{for } n & = & 149, & x & = & 1 & \text{and} & y & = & 24 \\ \text{for } n & = & 150, & x & = & 18 & \text{and} & y & = & 10. \end{array}$$

Thus, the refrigerators can be moved with 1 truck of the first type and 24 of the second type, or 18 of the first type and 10 of the second type.

Problem 2-80:

Show how to measure exactly 2 liters of water from a river using a 27 liter jug and a 16 liter jug. If you could not lift the larger jug when full, but could push it over, could you still measure the 2 liters?

Solution:

Let the 27 ℓ jug be filled x times, while the 16 ℓ jug is filled y times. (If x or y is negative, we treat this as emptying a full jug; and only useful way to empty a jug is after having filled it from the other jug.) We require

$$27x + 16y = 2.$$

Solve this using the Extended Euclidean Algorithm.

$27x + 16y = r$			q_i
1	0	27	
0	1	16	
1	−1	11	1
−1	2	5	1
3	−5	1	2
−16	27	0	5

Hence $x = 3$, $y = -5$ is one solution to $27x + 16y = 1$, and $x = 6$, $y = -10$ is one solution to $27x + 16y = 2$. Therefore fill the large jug from the river, pour it into the small jug until the small jug is full, then empty the small jug onto the ground. Empty the large jug into the small jug, and fill the large jug from the river again. If we repeat this until the large jug has been filled 6 times (162 ℓ of water) and the small jug has been emptied 10 times (160 ℓ of water, all of which has come from the large jug), then there should be 2 liters left in the large jug (assuming we haven't spilt any water!).

If the large jug cannot be lifted when full, then we must try to find a solution to $27x + 16y = 2$ with x negative and y positive. In this case, we can fill the small jug from the river, and empty the large jug by tipping it over.

The general solution of the Linear Diophantine Equation $27x + 16y = 2$ is $(x, y) = (6+16n, -10-27n),\ n \in \mathbb{Z}$. Taking $n = -1$ gives the solution $x = -10$, $y = 17$, that corresponds to filling the small jug 17 times and emptying the large jug 10 times.

Check: $27(-10) + 16(17) = -270 + 272 = 2$.

Problem 2-81:

Let S be the complete solution set of the Diophantine equation $ax + by = d$. Is

$$cS = \{(cx, cy) \mid (x, y) \in S\}$$

the complete solution set of $ax + by = cd$?

Solution:

No, cS is not the complete solution set of $ax + by = cd$.

We are given that S is the complete solution set of the Diophantine equations $ax + by = d$. Hence if a particular solution is (x_0, y_0) and $e = \gcd(a, b)$, then the complete solution is $(x, y) = \{(x_0 + (b/e)t\ ,\ y_0 - (a/e)t)\}\ ,\ t \in \mathbb{Z}$. Now it follows that a particular solution for $ax + by = cd$ is (cx_0, cy_0) and a general solution is $x = cx_0 + (b/e)t\ ,\ y = cy_0 - (a/e)t$. Comparing this with required condition that $cS = \{(cx, cy)\}$, we must have $cx = cx_0 + cbt\ ,\ cy = cy_0 - cat$, and the statements are not the same unless $c = 1$.

Problem 2-82:

Four men and a monkey spend the day gathering coconuts on a tropical island. After they have all gone to sleep at night, one of the men awakens and, not trusting the others, decides to take his share. He divides the coconuts into four equal piles, except for one remaining coconut, which he gives to the monkey. He then hides his share, puts the other piles together and goes back to sleep. Each of the other men awakens during the night and does likewise, and every time there is one coconut left over for the monkey. In the morning all the men awake, divide what's left of the coconuts into four, and again there is one left over that is given to the monkey. Find the minimum number of coconuts that could have been in the original pile.

Solution:

Let m be the minimum number of coconuts. By the Division Algorithm, there exists an integer q_1 such that $m = 4q_1 + 1$. The first man hides q_1 coconuts, and leaves $3q_1$ coconuts, after giving one to the monkey. Similarly, the other 3 men hide q_2, q_3, q_4 coconuts respectively, where $3q_{i-1} = 4q_i + 1$ for $i = 2, 3, 4$. This means that $3q_4$ coconuts remain to be divided in the morning. When that is done, each man takes q_5 more coconuts, where

$$3q_4 = 4q_5 + 1$$

and the monkey receives that last of his 5 coconuts. So we have

$$\begin{aligned} m &= 4q_1 + 1 \\ 3q_1 &= 4q_2 + 1 \\ 3q_2 &= 4q_3 + 1 \\ 3q_3 &= 4q_4 + 1 \\ 3q_4 &= 4q_5 + 1 \end{aligned}$$

Then $q_4 = (4/3)q_5 + 1/3$. Substituting for q_4 in the previous equation gives $q_3 = (4^2/3^2)q_5 + 7/3^2$. Substituting again for q_3 and solving for q_2 gives $q_2 = (4^3/3^3)q_5 + 37/3^3$. Repeating this again gives $q_1 = (4^4/3^4)q_5 + 175/3^4$. Then

$$m \;=\; 4q_1 + 1 \;=\; \frac{4^5}{3^4}q_5 + \frac{175}{3^4} + 1 \;=\; \frac{1024}{81}q_5 + \frac{781}{81}.$$

Hence m and q_1 satisfy the Diophantine Equation

$$81m - 1024q_5 = 781.$$

$1024(-q_5) + 81m =$		r	q_i
1	0	1024	
0	1	81	
1	−12	52	12
−1	13	29	1
2	−25	23	1
−3	38	6	1
11	−139	5	3
−14	177	1	1

By the Extended Euclidean algorithm, $81(177) - 1024(14) = 1$. Multiplying by 781 gives the particular solution $m = 138237$ and $q_5 = 10934$. The general solution to the Diophantine Equation is

$$\left.\begin{aligned} m &= 138237 + 1024n \\ q_5 &= 10934 + 81n \end{aligned}\right\} \text{ for all } n \in \mathbb{Z}.$$

We want the smallest positive value of m, such that $q_5 > 0$ (because in the morning there were still coconuts left). Hence $n > -10934/81 \approx -134.988$; that is $n \geq -134$. The smallest value of m occurs when $n = -134$, with $m = 138237 + 1024(-134) = 1021$ and $q_5 = 10934 + 81(-134) = 80$.

Hence the minimum number of coconuts is 1021.

Check:

$$\begin{aligned} 1021 &= 4(255) + 1 \\ 3(255) = 764 &= 4(191) + 1 \\ 3(191) = 573 &= 4(143) + 1 \\ 3(143) = 429 &= 4(107) + 1 \\ 3(107) = 321 &= 4(80) + 1. \end{aligned}$$

Problem 2-83:

Let a, b, c be nonzero integers. Their *greatest common divisor* $\gcd(a, b, c)$ is the largest positive integer that divides all of them. Prove that

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

Solution:

Note that $g = \gcd(a, b, c)$ is non-negative. Let $d = \gcd(a, \gcd(b, c))$.

By definition, $d|a$ and $d|\gcd(b, c)$. The latter implies that $d|b$ and $d|c$. Thus d is a common divisor of a, b and c, and $d \leq g$.

Now $g|a$, $g|b$, and $g|c$. Because $g|b$ and $g|c$, Proposition 2.29.(iii) implies that $g|\gcd(b, c)$. As $g|a$, g is a common divisor of a and $\gcd(b, c)$, and so $g \leq d$. Hence $\gcd(a, b, c) = g = d = \gcd(a, \gcd(b, c))$.

Problem 2-84:

Prove that the Diophantine equation $ax + by + cz = e$ has a solution if and only if $\gcd(a, b, c)|e$.

Solution:

We follow the outline of the proof of Theorem 2.31 (i). Let $d = \gcd(a, b, c)$.
($\Longrightarrow$) Suppose that there are integers x, y, z for which $ax + by + cz = e$. By definition of gcd $d|a$, $d|b$, and $d|c$. Therefore $d|ax+by$, and again, $d|(ax+by)+cz$, i.e., $d|e$.
($\Longleftarrow$) Suppose that $d|e$, so $e = de_1$ for some e_1 in $\mathbb{Z}$. Let $f = \gcd(b, c)$. By Problem 2-83, $d = \gcd(a, f)$. And by the Extended Euclidean Algorithm, there exist integers x_1 and y_1 such that

$$ax_1 + fy_1 = d$$

By the Extended Euclidean Algorithm again, there exist integers y_2 and z_2 such that

$$by_2 + cz_2 = f.$$

Substituting for f gives

$$ax_1 + by_2y_1 + cz_2y_1 \;=\; d.$$

Multiplying each term by e_1,

$$a(x_1e_1) + b(y_2y_1e_1) \;+\; c(z_2y_1e_1) = de_1 = e.$$

Each product in parenthesis is an integer. So the given Diophantine equation does have an integer solution.

Problem 2-85:

If $\gcd(a, b, c)|e$, describe how to find one solution to the Diophantine equation $ax + by + cz = e$.

Solution:

By Problem 2-83 we know that $\gcd(a,b,c) = \gcd(a, \gcd(b,c))$. Now,

$$by + cz = \gcd(b,c)t \text{ for } t \in \mathbb{Z}.$$

So we have

$$ax + \gcd(b,c)t = e.$$

Because $\gcd(a, \gcd(b,c)) = \gcd(a,b,c) | e$, a solution can be found to this linear Diophantine equation in the two variables x and t. If x_0 and t_0 is a particular solution, we have $ax_0 + \gcd(b,c)t_0 = e$.

We can also find $y_0, z_0 \in \mathbb{Z}$ such that $by_0 + cz_0 = \gcd(b,c)$. Substituting in the previous equation gives

$$ax_0 + by_0t_0 + cz_0t_0 = e$$

Then x_0, y_0t_0 and z_0t_0 will give a solution to the original equation.

Problem 2-86:

Describe how to find all the solutions to the Diophantine equation

$$ax + by + cz = e.$$

Solution:

Every solution can be broken up as in Problem 2- 85, so that the equation is equivalent to the pair of equations

$$\begin{aligned} ax + \gcd(b,c)t &= e \\ by + cz &= \gcd(b,c)t. \end{aligned}$$

There is a solution if and only if $\gcd(a,b,c) | e$ as in Problem 2-84. The procedure consists of finding the general solution of the first equation for x and t. For each t, find the general solution of the second equation for y and z.

If $x = x_0$, $t = t_0$ is one solution to the first equation then the general solution is

$$\left.\begin{aligned} x &= x_0 + \tfrac{d_1}{d}n \\ y &= y_0 - \tfrac{a}{d}n \end{aligned}\right\} \text{ for all } n \in \mathbb{Z}$$

where $d = \gcd(a,b,c) = \gcd(a, \gcd(b,c))$ and $d_1 = \gcd(b,c)$. Then the second equation becomes

$$by + cz = d_1 t = d_1 t_0 - \frac{ad_1}{d}n$$

Treating n as fixed, we find one solution for y and z in the form

$$\begin{aligned} y &= r_1 + r_2 n \\ z &= r_3 + r_4 n \end{aligned}$$

satisfying $br_1 + cr_3 = d_1 t_0$ and $br_2 n + cr_4 n = \frac{ad_1}{d} n$. The general solution to the original equation is then

$$\left.\begin{array}{rcl} x & = & x_0 + \frac{d_1}{d} n \\ y & = & r_1 + r_2 n + \frac{c}{d_1} m \\ z & = & r_3 + r_4 n + \frac{b}{d_1} m \end{array}\right\} \text{ for all } n, m \in \mathbb{Z}$$

Note that there are two independent integer parameters n and m.

Problem 2-87:

Find one integer solution to the Diophantine equation $18x + 14y + 63z = 5$.

Solution:

By Problem 2-84 we know that the equation has a solution if and only if $\gcd(18, 14, 63)|5$. Now $\gcd(18, 14, 63) = \gcd(18, \gcd(14, 63)) = \gcd(18, 7) = 1$. So the equation has a solution.

Following the approach of Problem 2-85, we first solve the equation

$$18x + 7t = 5$$

By inspection $18(2) + 7(-5) = 1$. Multiplying by 5 gives $18(10) + 7(-25) = 5$. Hence $x_0 = 10$, $t_0 = -25$ is a solution.

Now, we solve the equation $14y + 63z = 7(-25)$. Again by inspection $14(-4) + 63(1) = 7$. Multiplying by -25 gives $14(100) + 63(-25) = 7(-25)$. Hence $y_0 = 100$, $z_0 = -25$ is a solution.

Therefore the values $x = 10$, $y = 100$ and $z = -25$ give one solution to the original equation.

Check: $18(10) + 14(100) + 63(-25) = 180 + 1400 - 1575 = 5$.

Problem 2-88:

Find all the ways that \$1.67 worth of stamps can be put on a parcel, using 6 cents, 10 cents and 15 cents stamps.

Solution:

Let x be the number of 6 cent stamps, y the number of 10 cent stamps and z the number of 15 cent stamps. We have

$$6x + 10y + 15z = 167.$$

We shall first find all the integral solutions to this equation and then determine the nonnegative solutions.

Since $\gcd(10, 15) = 5$, we can write

$$10y + 15z = 5t \quad \text{or} \quad 2y + 3z = t \qquad \text{where} \quad t \in \mathbb{Z}\ .$$

Solving $6x + 5t = 167$ we see that, by inspection, one solution is $x = 2, t = 31$. Hence the general integral solution is

$$x = 2 + 5k, \quad t = 31 - 6k \qquad \text{for } k \in \mathbb{Z}.$$

We now solve $2y+3z = t = 31-6k$. One solution to the equation is $y = 14, z = 1-2k$. The general solution is

$$\left.\begin{array}{l} x = 2+5k \\ y = 14-3l \\ z = 1-2k+2l \end{array}\right\} \text{ for all } k, l \in \mathbb{Z}.$$

Since x, y and z must be nonnegative, we require

$$2+5k \geq 0, \quad 14-3l \geq 0 \quad \text{and} \quad 1-2k+2l \geq 0,$$

that is, $k \geq 0$, $l \leq 4$ and $l \geq k$. That is, $0 \leq k \leq l \leq 4$.

The 15 possible solutions are listed in the following table.

k	0	0	0	0	0	1	1	1	1	2	2	2	3	3	4
l	0	1	2	3	4	1	2	3	4	2	3	4	2	4	4
x	2	2	2	2	2	7	7	7	7	12	12	12	17	17	22
y	14	11	8	5	2	11	8	5	2	8	5	2	5	2	2
z	1	3	5	7	9	1	3	5	7	1	3	5	1	3	1

An alternative way of writing the solutions is

$$x = 2+5k, \quad y = 14-3l, \quad z = 1-2k+2l \quad \text{where } 0 \leq k \leq l \leq 4.$$

Problem 2-89:

Given a balance and weights of 1, 2, 3, 5, and 10 grams, show that any integer gram weight up to 21 grams can be weighed. If the weights were 1, 2, 4, 8 and 16 grams, show that any integer weight up to 31 grams could be weighed.
Solution:

For the first part, weights of 0 to 4 grams can be weighed with no weights or with the weights $1, 2, 3, 3$ and 1,. Including the weight of 5 grams to the first four combinations allows weights 5 to 9. Notice that these combinations do not use the 10 gram weight. So, including it to all the previous combinations will allow weights 10 to 19. The combination $2, 3, 5, 10$ weighs 20 grams, and all the weights together, $1, 2, 3, 5, 10$ weigh 21 grams. So any integer gram weight up to 21 grams can be weighed.

For the second part. By Theorem 2.41 every non-negative integer w has a unique base 2 representation using $0s$ and $1s$. For $w = 31$ its base 2 representation is $(1111)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ with four positions. Then every non-negative integer between 0 and 31 has a base 2 representation of at most four positions.

More formally, any integer w such that $0 \leq w \leq 31$ has a unique base 2 representation

$$(b_3 b_2 b_1 b_0)_2, \quad b_i = 0 \text{ or } 1$$

To weigh w grams with weights of $2^0, 2^1, 2^2, 2^3$ grams you follow this algorithm For $0 \leq i \leq 3$,

If $b_i = 1$ include the 2^i gram weight
If $b_i = 0$ do not include the 2^i gram weight.

This will produce a weight of $b_3 \cdot 2^3 + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0 = (b_3 b_2 b_1 b_0)_2 = w$ grams.

Problem 2-90:

If weights could be put on either side of a balance, show that any integer weight up to 121 grams could be weighed using weights of 1, 3, 9, 27 and 81 grams.

Solution:

Every nonnegative integer w has a base 3 representation using 0, 1, 2. The integer $w = 121$ is represented as $(11111)_3$: it uses five positions. Every w less than 121 also uses at most five positions, exactly five if the representation is filled out with 0's to the left. We convert this to a base 3 representation using 0, 1, -1 in five positions, by the following **Algorithm** (with n in place of 5):

Given: Integer w in standard base 3 representation

$$(a_n a_{n-1} \dots a_1)_3 \leq (1\ 1 \dots 1)_3,$$

Find: w in $(0, 1, -1)$-representation $(b_n b_{n-1} \dots b_1)_3$, using the same n positions. Let c_i denote the *carry* to the i'th position. Start at position $i = 1$. The carry to this initial position is $c_1 = 0$.

$(*)$ (a) If $a_i + c_i$ is 0 or 1, let b_i be that same value, 0 or 1.
If $i = n$ stop : the $(0, 1, -1)$-representation is complete.
Else $i < n$.
Let $c_{i+1} = 0$.

(b) If $a_i + c_i = 2$, let $b_i = -1$ and $c_{i+1} = 1$.

(c) If $a_i + c_i = 3$, let $b_i = 0$ and $c_{i+1} = 1$.

Return to $(*)$ with $i + 1$ in place of i.

Proposition: If an integer w is expressed in standard base 3 representation as an n-digit number which is at most $(1\ 1\ \dots 1)_3$, then its (0, 1, -1)-representation is also an n-digit number.

Proof: If the standard representation has no 2s, this is also its $(0, 1, -1)$-representation. If it has a 2, then somewhere to the left of all 2's is a 0, else $w > (1\ 1\ \dots 1)_3$. In the first such position i, $a_i + c_i = 1$, for which the algorithm gives $c_{i+1} = 0$. The rest of the $(0, 1, -1)$-representation agrees with the standard representation. Altogether, the $(0, 1, -1)$-representation uses the same n positions as the standard representation.

Where to put the weights to balance a given weight w:

1. Put w in the left scale;

2. Put weights corresponding to +1's in the $(0, 1, -1)$-representation in the right scale;

3. Put weights corresponding to -1's in the left scale, i.e., with w.

Example: Take $w = 17$g. Expressed in standard base 3 representation,

$$17 = 1 \cdot 3^2 + 2 \cdot 3 + 2 \cdot 1 \ = \ (1\ 2\ 2)_3.$$

This uses three positions; put 0's to the left to fill out the number to five positions: $(00122)_3$. Convert this to the equivalent $(0, 1, -1)$-number

$$17 = 1 \cdot 3^3 - 1 \cdot 3^2 - 1 \ = \ (0\ 1\ -1\ 0\ -1)_3.$$

This gives the recipe for balance: put w in the left scale, the 27g weight in the right scale, and the 9 and 1 g weights in the left, along with w. The resultant balance verifies that $w = 17$.

Problem 2-91:

If numbers (in their decimal form) are written out in words, such as six hundreds, four tens and three for 643, we require one word for each digit 0, 1, 2, . . . , 9, one word for 10, one word for 10^2, etc. We can name all the integers below 1000 with twelve words. What base would use the least number of words to name all the numbers below 1000? What base would use the least number of words to name all the numbers below 10^6?

Solution:

Let b denote the base. Let us name all numbers less than b^{r+1} using the base b. We require b words for the digits in base b, plus r words for the numbers $b, b^2, \ldots, b^r$, for a total of $b + r$ words. Hence base b can describe numbers up to 10^s using $b + r$ words if $b^{r+1} \geq 10^s$.

Using Theorem 6.84. on logarithms, this happens if

$$r + 1 \ \geq \ \log_b(10^s) \ = \ \frac{\log_{10}(10^s)}{\log_{10} b} \ = \ \frac{s}{\log_{10} b}.$$

Using $\lfloor x \rfloor$, the integral part of x, for each b, the minimum value of r is

$$-\left\lfloor \frac{(-s)}{\log_{10} b} \right\rfloor - 1$$

and the corresponding minimum value of $b + r$ is

$$b - \left\lfloor \frac{-s}{\log_{10} b} \right\rfloor - 1.$$

If we put $s = 3$, for $b \geq 12$ at least 12 words are needed to name the digits $1, 2, \ldots, b-1$, which is not any better than the case for $b = 10$. Now, for $b = 11$, $11^2 = 121 < 1000$, so at least 12 words are needed.

The only cases left are for $b = 2, 3, \ldots 9$. For each of these bases, we use the above formula for $s = 3$. These cases are included in the following table.

b	r	b^r	b^{r+1}	$b + r$
2	9	512	1024	11
3	6	729	2187	9
4	4	256	1024	8
5	4	625	3125	9
6	3	216	1296	9
7	3	343	2401	10
8	3	512	4096	11
9	3	729	6561	12

Thus, the minimum value of this expression is 8 and occurs when $b = 4$. Hence eight words can name all integers below 100 using base 4.

If we put $s = 6$, then a similar table shows that the minimum value of the expression is 13, and occurs when $b = 4$, 5 or 6. Hence thirteen words can name all integers below one million using any of the bases 4, 5 or 6.

Problem 2-92:

Consider the set of all even integers $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$. We can add, subtract and multiply elements of $2\mathbb{Z}$ and the result will always be in $2\mathbb{Z}$, but we cannot always divide. We can define divisibility and factorization in $2\mathbb{Z}$ in a similar way to that in $\mathbb{Z}$. (For example, $2|4$ in $2\mathbb{Z}$, but $2 \not| 6$ even though $6 = 2 \cdot 3$, because $3 \notin 2\mathbb{Z}$.) A prime in $2\mathbb{Z}$ is a positive even integer that cannot be factored into the product of two even integers.

(a) Find all the primes in $2\mathbb{Z}$.

(b) Can every positive element of $2\mathbb{Z}$ be expressed as a product of these primes?

(c) If this factorization into primes can be accomplished, is it unique?

Solution:

(a) The primes in $2\mathbb{Z}$ are $c \in 2\mathbb{Z}$ such that $4 \not| \ c$.

If $4 \not| \ c$ and $a, b \in \mathbb{Z}$ are such that $c = ab$, then either a or $b \notin 2\mathbb{Z}$. Otherwise $a = 2k$ and $b = 2m$ for $k, m \in \mathbb{Z}$. Then $c = ab = (2k) \cdot (2m) = 4km$ which is a contradiction.

This shows that all such c are prime. To rule out any other number, let $c' \in 2\mathbb{Z}$ such that $4|c'$. Then there exists a $n \in \mathbb{Z}$ such that $c = 4n$. For $a = 2$ and $b = 2n$, $a, b \in 2\mathbb{Z}$ and $ab = 4n = c'$. So c' is not a prime in $2\mathbb{Z}$.

(b) Yes, every positive element of $2\mathbb{Z}$ can be expressed as a product of these primes.

To prove this assume that it is not true, and let N be the smallest element of $2\mathbb{Z} > 0$ that cannot be written as a product of primes in $2\mathbb{Z}$. N cannot be itself a prime in $2\mathbb{Z}$ so we can write $N = r \cdot s$ where $0 < r \leq s < N$. By

our hypothesis r and s can be written as a product of primes in $2\mathbb{Z}$. It follows then that $r \cdot s = N$ can be also written as a product of primes in $2\mathbb{Z}$. So, our assumption was wrong.

(c) No, the factorization into these primes is not unique. For example $2, 6, 10, 30$ they are all elements of $2\mathbb{Z}$, and $4 \not| \ 2, 6, 10$ or 30. By part (a) these numbers are primes in $2\mathbb{Z}$. But

$$2 \cdot 6 \cdot 10 = 120, \qquad 2^2 \cdot 30 = 120.$$

Thus 120 does not have a unique factorization in $2\mathbb{Z}$.

Problem 2-93:

Prove that the sum of two consecutive odd primes has at least three prime divisors (not necessarily different).

Solution:

Let p and q be consecutive odd primes, and assume without loss of generality that $p < q$. Since p and q are odd, the sum $p + q$ is even, and so $a = \frac{p+q}{2}$ is an integer.

Since $p < q$, we have

$$\begin{aligned} 2p &< p + q \\ \text{and } \ p + q &< 2q. \end{aligned}$$

Therefore $p < \frac{p+q}{2} < q$.

But since $a = \frac{p+q}{2}$ is an integer lying strictly between p and q, it cannot be prime (because p and q are consecutive primes). Therefore a has at least two prime divisors, say u and v. So $uv|a$, and therefore $2uv|(p + q)$, which shows that $p + q$ has at least three prime divisors.

Problem 2-94:

How many zeros are there at the right end of $100! = 100 \cdot 99 \cdot 98 \cdot 97 \cdots 2 \cdot 1$?
Solution:

If $100! = 1 \cdot 2 \ldots \cdot 100$ has k zeros at its right end of its decimal representation then

$$\begin{aligned} 100! &= 10^k \cdot a \quad \text{where } 10 \not| \ a \\ &= 2^k \cdot 5^k \cdot a. \end{aligned}$$

Let $2^{c_1} \cdot 5^{c_2} \cdot p_3^{c_3} \ldots p_n^{c_n}$ be the prime factorization of a, where c_1 or c_2 could be zero. Then c_1 and c_2 cannot both be nonzero, since $10 \not| \ a$. Therefore if $2^{d_1} \cdot 5^{d_2} \cdot p_3^{d_3} \ldots p_n^{d_n}$ is the prime factorization of 100!, $k = \min(d_1, d_2)$.

Now we can count d_1 and d_2 by counting the number of appearances of $2, 2^2, 2^3, \ldots$ and the appearances of $5, 5^2, 5^3, \ldots$ in the prime factorizations of the numbers $2, 3, \ldots, 99, 100$.

All the multiples of 5 from 1 to a 100 have at least one 5 in their prime factorizations. There are $\lfloor \frac{100}{5} \rfloor$ multiples of 5 from 1 to 100 (where $\lfloor x \rfloor$ is the integer part of x). Similarly, all the multiples of 5^2 from 1 to 100 have at least 5^2 in their prime factorizations. There are $\lfloor \frac{100}{25} \rfloor$ of these. But because the multiples of 5^2 are also multiples of 5, we have already counted one of the 5s, so we only have to count the other. Then the multiples of 5^2 have $\lfloor \frac{100}{25} \rfloor$ additional 5s in their prime factorizations. Finally, because $5^3 = 125 > 100$ there are no multiples of 5^3 from 1 to 100. So

$$\begin{aligned} d_2 &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor \\ &= 20 + 4 \end{aligned}$$

Doing a similar analysis for the number of 2s in the prime factorization of 100!, we get that there are $\lfloor \frac{100}{2} \rfloor = 50$ even numbers from 1 to 100. Hence there are at least that number of 2s in the prime factorization of 100! and so $d_1 > d_2$. Therefore $k = \min(d_1, d_2) = d_2 = 24$, and there are 24 zeros at the right end of the decimal expansion of 100!

Problem 2-95:

Show that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ can never be an integer if $n > 1$.

Solution:

Let $b = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ so that $n!b$ is an integer. Write $n!$ as $a2^l$, where a is odd, and let k be such that $2^k \leq n < 2^{k+1}$. We shall show that 2^{l-k+1} does divide $n!$, but does not divide $n!b$. This will prove that b is not an integer.

If $n > 1$, then $k \geq 1$, and so 2^{l-k+1} does divide $n! = a2^l$.

Now

$$n!b = \left(\frac{n!}{1} + \cdots + \frac{n!}{2^k - 1} + \frac{n!}{2^k + 1} + \cdots + \frac{n!}{n} \right) + \frac{n!}{2^k}.$$

Note that i is not divisible by 2^k, for $i = 1, \ldots, 2^k - 1, 2^k + 1, \ldots, n$. Hence $\frac{n!}{i}$ is divisible by 2^{l-k+1}. However, $\frac{n!}{2^k}$ is not divisible by 2^{l-k+1}. Therefore $n!b$ is not divisible by 2^{l-k+1}, as claimed.

Problem 2-96:

If $\lfloor x \rfloor$ is the greatest integer less than or equal to x (that is, the integer part of x), then for which values of n does $\lfloor \sqrt{n} \rfloor$ divide n?

Solution:

If $n = m^2$ for some integer m, then $\lfloor \sqrt{n} \rfloor = m$, and $\lfloor \sqrt{n} \rfloor$ divides n.

If $m^2 < n < (m+1)^2$ then $m < \sqrt{n} < m + 1$, and necessarily $m = \lfloor \sqrt{n} \rfloor$. We must test when $m = \lfloor \sqrt{n} \rfloor \mid n$ for $n = m^2 + 1, \ldots, m^2 + m, \ldots, m^2 + 2m$, since $(m+1)^2 = m^2 + 2m + 1$. If $m \mid m^2 + q$ then $m \mid q$. Hence $q = m$ or $2m$. Therefore, m divides only $m^2 + m$ and $m^2 + 2m$ in that range.

In summary, $\lfloor \sqrt{n} \rfloor \mid n$ if and only if n is of the form m^2, $m^2 + m$, or $m^2 + 2m$.

	m	1	2	3	4	...
	m^2	1	4	9	16	
n	m^2+m	2	6	12	20	
	m^2+2m	3	8	15	24	

Problem 2-97:

Let a and b be integers greater than 1, and let $e = \text{lcm}(a, b)$. Prove that

$$0 < \frac{1}{a} + \frac{1}{b} - \frac{1}{e} < 1.$$

Solution:
If $d = \gcd(a, b)$, then $ab = de$ by Theorem 2.59, and so $1/e = d/ab$. Hence

$$\frac{1}{a} + \frac{1}{b} - \frac{1}{e} = \frac{b + a - d}{ab}.$$

By the definition of least common divisor, $d \leq a$. Also, since $b > 0$,

$$\frac{b + a - d}{ab} \geq \frac{b + 0}{ab} > 0.$$

Now

$$ab - a - b + d = (a - 1)(b - 1) + d - 1 > 0$$

because $a - 1 > 0$, $b - 1 > 0$, and $d - 1 \geq 0$. Since a and b are positive,

$$\begin{aligned} a + b - d &< ab \\ \frac{b + a - d}{ab} &< 1, \end{aligned}$$

which proves the other inequality.

Problem 2-98:

If a and b are odd positive integers, and the sum of the integers, less than a and greater than b, is 1000, then find a and b.

Solution:

By the formula for the sum of an arithmetic progression, the sum of the integers, $b + 1, b + 2, \ldots, a - 2, a - 1$ is $\frac{(a+b)(a-b-1)}{2}$.

If this sum is 1000 then

$$(a + b)(a - b - 1) = 2000 = 2^4 \cdot 5^3.$$

Furthermore, since a and b are odd, then $a + b$ is even and $a - b - 1$ is odd.

Hence, by the Unique Factorization Theorem, the only possible values for the factors are as follows.

i) $a + b = 2^4, \quad a - b - 1 = 5^3$

ii) $a+b=2^4\cdot 5, \quad a-b-1=5^2$

iii) $a+b=2^4\cdot 5^2, \quad a-b-1=5$

iv) $a+b=2^4\cdot 5^3, \quad a-b-1=1$

Solving the four cases we obtain the solutions:

i) $a=71, \quad b=-55$

ii) $a=53, \quad b=27$

iii) $a=203, \quad b=197$

iv) $a=1001, \quad b=999$

The first case is impossible, so we obtain three possible solutions.

Either $a=53$, $b=27$, or $a=203$, $b=197$ or $a=1001$, $b=999$.

Problem 2-99:

Either prove the following statement about integers, or give a counterexample.

$a^2|b^2$ if and only if $a|b$

Solution: The statement is true.

($\Longleftarrow$) Assume that $a|b$. Then $b=qa$ for some integer q and $b^2=q^2a^2$. Now q^2 is an integer, so $a^2|b^2$.

($\Longrightarrow$) Assume $a^2|b^2$. Find prime factorizations of each of a and b:

$$\begin{aligned} a &= p_1^{c_1}p_2^{c_2}\dots p_n^{c_n} \\ b &= p_1^{d_1}p_2^{d_2}\dots p_n^{d_n}, \end{aligned}$$

where some exponents may be zero. Hence

$$\begin{aligned} a^2 &= p_1^{2c_1}p_2^{2c_2}\dots p_n^{2c_n} \\ b^2 &= p_1^{2d_1}p_2^{2d_2}\dots p_n^{2d_n} \end{aligned}$$

Since $a^2|b^2$, it follows from Theorem 2.56 that $2c_i \le 2d_i$ for each $i=1,\dots n$ Therefore $c_i \le d_i$ for each i, and $a|b$.

Problem 2-100:

Either prove the following statement about integers, or give a counterexample.

$\gcd(a,b)=\gcd(a+b, \mathrm{lcm(a,b)})$

Solution: The statement is true and we shall use a Lemma to prove it. Recall from Theorem 2.59 that $\mathrm{lcm(a,b)} = \mathrm{ab}/\gcd(\mathrm{a,b})$.

Lemma. If $\gcd(a,b)=1$ then $\gcd(a+b,ab)=1$.

Proof. Suppose $\gcd(a+b,ab)\neq 1$ and p is a prime such that $p|a+b$ and $p|ab$. By Theorem 2.53, $p|a$ or $p|b$. If $p|a$, then $p|(a+b)-a$ so $p|b$, which is not possible since $\gcd(a,b)=1$. Similarly p cannot divide b.

This contradiction proves $\gcd(a+b, ab) = 1$. □

Let $d = \gcd(a, b)$. If $d = 0$ then $a = b = 0$ so $\gcd(a, \mathrm{lcm(a, b)}) = 0$ and the result holds.

If $\gcd(a, b) = d = 1$, then the right side reduces to $\gcd(a + b, ab)$ because $\mathrm{lcm(a, b)} = \mathrm{ab}/\gcd(\mathrm{a, b}) = \mathrm{ab}$. The Lemma we have proved shows that the result holds.

Now let $d > 1$. By Proposition 2.27 (ii), $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ and the Lemma implies

$$\gcd\left(\tfrac{a}{d} + \tfrac{b}{d}, \tfrac{a}{d} \cdot \tfrac{b}{d}\right) \;=\; 1.$$

Hence

$$\begin{aligned}
\gcd(a+b, \mathrm{lcm(a, b)}) &= \gcd\left(d \cdot \left(\tfrac{a}{d} + \tfrac{b}{d}\right), \tfrac{ab}{d}\right) \\
&= d \cdot \gcd\left(\tfrac{a}{d} + \tfrac{b}{d}, \tfrac{a}{d} \cdot \tfrac{b}{d}\right) \qquad \text{by Exercise 2-11} \\
&= d \\
&= \gcd(a, b).
\end{aligned}$$

Problem 2-101:

Either prove the following statement about integers, or give a counterexample.

$\mathrm{lcm}(\gcd(a, b), \gcd(a, c)) = \gcd(a, \mathrm{lcm}(b, c))$

Solution: Let

$$\begin{aligned}
a &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n} \\
b &= p_1^{\beta_1} \cdot p_2^{\beta_2} \ldots p_n^{\alpha_n} \\
c &= p_1^{\gamma_1} \cdot p_2^{\gamma_2} \ldots p_n^{\gamma_n}
\end{aligned}$$

where some exponents may be 0. By Theorem 2.58 we know that

$$\begin{aligned}
\gcd(a, b) &= p_1^{e_1} \cdot p_2^{e_2} \ldots p_n^{e_n} \quad \text{where } e_i = \min(\alpha_i, \beta_i) \\
\gcd(a, c) &= p_1^{f_1} \cdot p_2^{f_2} \ldots p_n^{f_n} \quad \text{where } f_i = \min(\alpha_i, \gamma_i)
\end{aligned}$$

for $1 \le i \le n$. And by Theorem 2.58 we also know that

$$\mathrm{lcm}(\gcd(a, b), \gcd(a, c)) = p_1^{g_1} \cdot p_2^{g_2} \ldots p_n^{g_n} \quad \text{where } g_i = \max(e_i, f_i).$$

for $1 \le i \le n$. Similarly,

$$\begin{aligned}
\mathrm{lcm}(b, c) &= p_1^{h_1} \cdot p_2^{h_2} \ldots p_n^{h_n} \text{ where } h_i = \max(\beta_i, \gamma_i) \\
\gcd(a, \mathrm{lcm}(b, c)) &= p_1^{j_1} \cdot p_2^{j_2} \ldots p_n^{j_n} \text{ where } j_i = \min(\alpha_i, \max(\beta_i, \gamma_i))
\end{aligned}$$

for $1 \le i \le n$.

Now for each i we consider two cases.

Case 1. If $\min(\alpha_i, \beta_i, \gamma_i) = \alpha_i$, then

$$\begin{aligned} g_i &= \max(e_i, f_i) = \max\big(\min(\alpha_i, \beta_i),\ \min(\alpha_i, \gamma_i)\big) \\ &= \max(\alpha_i, \alpha_i) = \alpha_i, \\ \text{and } j_i &= \min(\alpha_i, \max(\beta_i, \gamma_i)) = \alpha_i. \end{aligned}$$

Case 2. If $\min(\alpha_i, \beta_i, \gamma_i) \neq \alpha_i$, then $\min(\alpha_i, \beta_i, \gamma_i)$ is β_i or γ_i. Because both g_i and j_i are symmetric with respect to β_i and γ_i, without loss of generality we can let $\beta_i = \min(\alpha_i, \beta_i, \gamma_i)$. Then

$$\begin{aligned} g_i &= \max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i)), \\ &= \max(\beta_i, \min(\alpha_i, \gamma_i)) = \min(\alpha_i, \gamma_i), \\ \text{and} \quad j_i &= \min(\alpha_i, \max(\beta_i, \gamma_i)) = \min(\alpha_i, \gamma_i)., \end{aligned}$$

In either case $g_i = j_i$ for each $i = 1, \ldots, n$, so

$$\operatorname{lcm}(\gcd(a,b), \gcd(a,c)) = p_1^{g_1} \cdot p_2^{g_2} \ldots p_n^{g_n} = p_1^{j_1} \cdot p_2^{j_2} \ldots p_n^{j_n} = \gcd(a, \operatorname{lcm}(b,c)).$$

Problem 2-102:

Either prove the following statement about integers, or give a counterexample.

If $\gcd(a, b) = 1$ and $ax + by = c$ has a positive integer solution then so does $ax + by = d$ when $d > c$.

Solution:

We shall show that this statement is false by giving one counterexample.

The Diophantine equation

$$4x + 5y = 9$$

clearly has the positive integer solution $x = 1, y = 1$. Now consider the equation

$$4x + 5y = 11.$$

One integer solution to this is $x = -1, y = 3$ so the general integer solution is

$$\left.\begin{array}{l} x = -1 + 5n \\ y = 3 - 4n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

For positive solutions we require $-1 + 5n > 0$ and $3 - 4n > 0$, that is, $n > 1/5$ and $n < 3/4$. However, there are no integers between $1/5$ and $3/4$ so this equation has no positive solutions.

Problem 2-103:

Write a computer program to test whether a given number is prime. Use your program to find the smallest positive integer n for which the number $n^2 - n + 41$ fails to be prime.

Solution:

A simple and crude method to test whether a given number k is prime is to check if it is divisible by a number between 1 and including $\lfloor\sqrt{k}\rfloor$. By Theorem 2.55, we know that an integer $k > 1$ is either prime or contains a prime factor $\leq \sqrt{k}$, so such a test meets our needs. We include the pseudocode of such a method.

PROCEDURE	CheckIfPrime(k)	
Title	Finds first integer divisor of k or returns 0 if k is prime.	
Argument	k	integer
Variables	isPrime	boolean True or False
	m	$\lfloor\sqrt{k}\rfloor$
	n	integer from 2 to $\lfloor\sqrt{k}\rfloor$

```
BEGIN
    WHILE NOT isPrime AND n = 2 TO m
        IF n | k
            isPrime = False
        END IF
    END WHILE
    IF isPrime
        RETURN 0
    ELSE
        RETURN n
    END IF
END
```

Using a computer program following this pseudocode, the smallest n for which the number $n^2 - n + 41$ is prime is $n = 41$.

Problem 2-104:

Using a computer, test whether $F(4) = 2^{2^4} + 1$ and $F(5) = 2^{2^5} + 1$ are prime.

Solution:

We use the computer program outlined in Problem 2-103.

PROCEDURE	CheckIfPrime(k)	
Title	Finds first integer divisor of k or returns 0 if k is prime.	
Argument	k	integer
Variables	isPrime	boolean True or False
	m	$\lfloor\sqrt{k}\rfloor$
	n	integer from 2 to $\lfloor\sqrt{k}\rfloor$

```
BEGIN
    WHILE NOT isPrime AND n = 2 TO m
        IF n | k
            isPrime = False
        END IF
```

```
    END WHILE
    IF isPrime
        RETURN 0
    ELSE
        RETURN n
    END IF
END
```

This program confirms that $F(4) = 2^{2^4} + 1$ is prime. It also shows that $F(5) = 2^{2^5}$ is not a prime because 641 divides it, confirming Euler's result.

Problem 2-105:

Show that all the integers, $\mathbb{Z}$, both positive and negative, can be represented in the *negative base* -10 using the digits $0, 1, \ldots, 9$ without using a negative prefix. For example, $-1467 = (2673)_{-10}$ and $10 = (190)_{-10}$.

(a) What decimal numbers do $(56)_{-10}$ and $(164)_{-10}$ represent?

(b) Find the negative ten representations of the decimal numbers 1111 and -209.

(c) Try adding and multiplying some numbers in the base negative ten. Then try adding a number to its negative.

Solution:

The Division Algorithm holds even if the divisor is negative. That is, if b is negative, there exist unique integers q and r such that

$$a = qb + r \text{ where } 0 \leq r < |b|.$$

So for any integer x, dividing by $b = -10$ according to this version of the Division Algorithm, we obtain

$$\begin{array}{rcll}
x & = & q_0(-10) + r_0 & \text{where } 0 \leq r_0 < 10 \\
q_0 & = & q_1(-10) + r_1 & \text{where } 0 \leq r_1 < 10 \\
q_1 & = & q_2(-10) + r_2 & \text{where } 0 \leq r_2 < 10 \\
 & \vdots & & \\
q_{i-1} & = & q_i(-10) + r_i & \text{where } 0 \leq r_i < 10 \\
 & \vdots & & \\
q_{n-2} & = & q_{n-1}(-10) + r_{n-1} & \text{where } 0 \leq r_{n-1} < 10 \\
q_{n-1} & = & 0 \cdot (-10) + r_n & \text{where } 0 < r_n < 10.
\end{array}$$

We have to check that this algorithm terminates. Let $x = q_{-1}$. The general step of the algorithm implies that $0 \leq q_{i-1} + 10q_i \leq 9$.

If $0 \leq q_{i-1} < 10$, then the algorithm stops with $q_i = 0$ and $r_i = q_{i-1}$.

If $q_{i-1} \geq 10$, then $q_i < 0$ and $|q_{i-1}| = q_{i-1} \geq 10(-q_i) > |q_i|$.

If $q_{i-1} < 0$, then $q_i > 0$ and $|q_{i-1}| = -q_{i-1} \geq 10(q_i) - 9 \geq q_i = |q_i|$. The equality occurs only if $q_i = 1$ and $q_{i-1} = -1$. In this case the algorithm becomes

$$\begin{aligned} -1 &= 1(-10) + 9 \\ 1 &= 0(-10) + 1 \end{aligned}$$

and so terminates.

Hence $|x| \geq |q_0| \geq |q_1| \geq \cdots$, with at most one equality, and the absolute value of the quotients form a decreasing sequence of nonnegative integers that must eventually reach zero. Using the list of equations we can write

$$x = r_n(-10)^n + r_{n-1}(-10)^{n-1} + \cdots + r_2(-10)^2 + r_1(-10) + r_0,$$

just as we do with positive integers and positive bases. Hence $x \in \mathbb{Z}$ can be represented in the negative base -10 as

$$x = (r_n r_{n-1} \ldots r_1 r_0)_{-10}.$$

where $0 \leq r_i < 10$ for all $0 \leq i \leq n$.

It can be shown that this representation is unique and it can be generalized to any negative base $b \leq -2$ using the digits $0, 1, 2, \ldots, |b| - 1$.

(a) $(56)_{-10} = 5(-10) + 6 = -44$, and $(164)_{-10} = 1(-10)^2 + 6(-10) + 4 = 100 - 60 + 4 = 44$.

(b) Using the algorithm depicted in the proof

$$\begin{aligned} 1111 &= (-111)(-10) + \mathbf{1} \\ -111 &= (12)(-10) + \mathbf{9} \\ 12 &= (-1)(-10) + \mathbf{2} \\ -1 &= 1(-10) + \mathbf{9} \\ 1 &= 0(-10) + \mathbf{1}. \end{aligned} \qquad \begin{aligned} -209 &= 21(-10) + \mathbf{1} \\ 21 &= (-2)(-10) + \mathbf{1} \\ -2 &= (1)(-10) + \mathbf{8} \\ 1 &= 0(-10) + \mathbf{1}. \end{aligned}$$

So $1111 = (19291)_{-10}$ and $-209 = (1811)_{-10}$.

Check: $(19291)_{-10} = 10000 - 9000 + 200 - 90 + 1 = 1111$ and $(1811)_{-10} = -1000 + 800 - 10 + 1 = -209$.

(c) If we add or multiply numbers in the base negative ten, we have to be careful when we carry digits. For example, to add 8 and 4,

$$8 + 4 = 12 = 2 - (1)(-10),$$

so we would carry -1 (which is $(19)_{-10}$).

Bearing this in mind, we add $-1467 = (2673)_{-10}$ and $10 = (190)_{-10}$, and we multiply $1111 = (19291)_{-10}$ with $(190)_{-10}$ to get,

$$\begin{array}{r} (2673)_{-10} \\ +\quad (190)_{-10} \\ \hline (2663)_{-10} \\ \hline \end{array} \qquad \begin{array}{r} (19291)_{-10} \\ \times\quad (190)_{-10} \\ \hline (100190)_{-10} \\ (1929100)_{-10} \\ \hline (29290)_{-10} \\ \hline \end{array}$$

As a check, $(2663)_{-10} = -2000 + 600 - 60 + 3 = -1457 = -1467 + 10$, $(29260)_4 = 20000 - 9000 + 200 - 90 = 11110 = (1111)(10)$.

Finally, we add $44 = (164)_{-10}$ and $-44 = (56)_{-10}$.

$$\begin{array}{r} (164)_{-10} \\ +\quad (56)_{-10} \\ \hline (000)_{-10} \end{array}$$

Adding 4 and 6 in the units column, we have to carry -1. Then adding 6 and 5 and -1 in the next column, we obtain 0 and we have to carry -1. The left column gives 1 plus -1, and we end up with $(0)_{-10}$ as expected.

Problem 2-106:

(a) Find two consecutive primes that differ by at least 10.

(b) Prove that there are arbitrarily large gaps between consecutive primes.

Solution:
(a) The following is the complete list of pairs of consecutive primes which differ by at least 10 and are less than 500:

$$\begin{array}{llllll} (113,127) & (139,149) & (181,191) & (199,211) & (211,223) & (241,251) \\ (283,307) & (317,331) & (337,347) & (409,419) & (421,479) & \end{array}$$

(b) Let n be a positive integer and observe that $i|n!+i$ for $i = 2, \ldots, n$. Then the integers $n!+2, \ldots, n!+n$ are $n-1$ consecutive composite numbers. Since n can be chosen arbitrarily large there are arbitrarily large gaps between consecutive primes.

[If we apply this method with n=10, then it proves that the numbers between $10!+1$ and $10!+11$ are all composite. Using a prime factorization program on the Web, we see that $10!+11$ is prime, but $10!+1 = 11 \times 329891$, is not. In fact, $10!-11 = 3628789$ and $10!+11 = 3628811$ are consecutive primes that differ by 22.]

Problem 2-107:

Let $a < b < c$, where a is a positive integer and b and c are odd primes. Prove that if $a \mid (3b+2c)$ and $a \mid (2b+3c)$, then $a = 1$ or 5. Give examples to show that both these values for a are possible.

Solution:

By Proposition 2.11(ii), $a|2b+3c-3b-2c = c-b$. Again by Proposition 2.11(ii), $a|3b+2x-2(c-b) = 5b$ and $a|2b+3c-2(c-b) = 5c$.

Because 5 and b are primes, the only divisors of $5b$ are $1, 5, b$ and $5b$. Similarly the only divisors of $5c$ are $1, 5, c$ and $5c$. Since a is less than b and c, a is either 1 or 5.

If $a = 1$, any two odd primes b and c will work. If $a = 5$, take $b = 11$ and $c = 31$ so

$$5 \mid 3(11) + 2(31) = 95 \quad \text{and} \quad 5 \mid 2(11) + 3(31) = 115.$$

Problem 2-108:

An integer n is perfect if the sum of its divisors (including itself and 1) is $2n$. Show that if $2^p - 1$ is a prime number, then $n = 2^{p-1}(2^p - 1)$ is perfect.

Solution:

Since $2^p - 1$ is prime, the divisors of n are:

$$1, 2, 2^2, \ldots, 2^{p-1} \text{ and } (2^p - 1), 2(2^p - 1), 2^2(2^p - 1), \ldots, 2^{p-1}(2^p - 1).$$

The sum of the divisors is:

$$\begin{aligned} S &= 1 + 2 + 2^2 + \cdots + 2^{p-1} + \\ &\quad (2^p - 1) + 2(2^p - 1) + 2^2(2^p - 1) + \cdots + 2^{p-1}(2^p - 1) \\ &= (1 + (2^p - 1))[1 + 2 + 2^2 + \cdots + 2^{p-1}]. \end{aligned}$$

The bracketed summation is a geometric series having a common ratio of 2 that sums to

$$(2^p - 1)/(2 - 1) = 2^p - 1.$$

Therefore,

$$S = (1 + (2^p - 1))[2^p - 1] \;=\; 2^p(2^p - 1) \;=\; 2n.$$

Hence $n = 2^{p-1}(2^p - 1)$ is perfect.