4.2.1

a) $(231)_2 = 1110\ 0111$

b) $(4532)_2 = 1\ 0001\ 1011\ 0100$

c) $(97644)_2 = 1\ 0111\ 1101\ 0110\ 1100$

4.2.3

a) $(1\ 1111)_2 = 2^5 - 1 = 31$

b) $(10\ 0000\ 0001)_2 = 2^0 + 2^9 = 513$

c) $(1\ 0101\ 0101)_2 = 2^0 + 2^2 + 2^4 + 2^6 + 2^8 = 341$

d) $(110\ 1001\ 0001\ 0000)_2 = 2^4 + 2^8 + 2^11 + 2^13 + 2^14 = 26896$

4.2.5

a) $(572)_8 = 101111010$

b) $(1604)_8 = 11\ 1000\ 0100$

c) $(423)_8 = 1\ 0001\ 0011$

d) $(2417)_8 = 101\ 0000\ 1111$

4.2.7

a) $(80\text{E})_{16} = 1000\ 0000\ 1110$

b) $(135\text{AB})_{16} = 1\ 0011\ 1010\ 1011$

c) $(\text{ABBA})_{16} = 1010\ 1011\ 1011\ 1010$

d) $(\text{DEFACED})_{16} = 1101\ 1110\ 1111\ 1010\ 1100\ 1110\ 1101$

4.2.9

$$(\text{ABCDEF})_{16} = 1010\ 1011\ 1100\ 1101\ 1110\ 1111.$$

4.2.11

$$(1011\ 0111\ 1011)_2 = (B7B)_{16}.$$

4.3.1

a) $21 = 3 \cdot 7 \implies$ not prime

b) 29 is prime

c) 71 is prime

d) 97 is prime

e) $111 = 3 \cdot 37 \implies$ not prime

f) $143 = 11 \cdot 13 \implies$ not prime

4·3·3

a) $88 = 8 \cdot 11 = 2^3 \cdot 11$

b) $126 = 2 \cdot 63 = 2 \cdot 3^2 \cdot 7$

c) $729 = 3 \cdot 243 = 3^2 \cdot 81 = 3^2 \cdot 3^4 = 3^6$

d) $1001 = 11 \cdot 91 = 7 \cdot 11 \cdot 13$

e) $1111 = 11 \cdot 101$

f) $909,090 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$

4·3·5

The prime factorization of 10! is the product of the prime factorizations of the integers ≤ 10. Therefore

$$10! = 2^{(1+2+3+1+1)} \cdot 3^{(1+2+1)} \cdot 5^{(1+1)} \cdot 7 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

4·3·15

Since $30 = 2 \cdot 3 \cdot 5$ its all integers below 30 that do not have any of those as prime factors, hence

$$1, 7, 11, 13, 17, 23.$$

4·3·17

a) Yes they are pairwise relatively prime

b) No since $\gcd(15, 21) = 3 \neq 1$

c) Yes they are pairwise relatively prime

d) Yes they are pairwise relatively prime

4·3·19

We prove via contraposition.

> ***Proof.*** Assume that $n \in \mathbb{Z}^+$ is not prime. Then $\exists a, b \in \mathbb{Z}^+$ such that $ab = n$ and both $a, b > 1$. Note then that
>
> $$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1\right).$$
>
> Since $a > 1$, then $2^a > 2 \implies 2^a - 1 > 1$. Since $b > 1$ the right hand side of the factorization is also guranteed to be larger than 1. Therefore $2^n - 1$ factors into two integers larger than 1, meaning it is must be not prime. ■

4·3·21

a) $\phi(4) = \#\{1, 3\} = 2$

b) $\phi(10) = \#\{1, 3, 7, 9\} = 4$

c) $\phi(13) = \#\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} = 12$

4·3·23

There are p^k candidates to consider. Since p is prime, any number is coprime to it except for the powers of p up to p^k. There are p^{k-1} powers of p less than or equal to p^k meaning

$$\phi\left(p^k\right) = p^k - p^{k-1}.$$

4·3·25

a) $3^5 \cdot 5^3 = 30,375$ b) 1 c) 23^{17}

d) $41 \cdot 43 \cdot 53$ e) 1 f) 1111

4·3·27

a) $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$ b) $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$ c) 23^{31}

d) $41 \cdot 43 \cdot 53$ e) $2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$ f) Undefined

4·3·33

a) Since $18 = 1(12) + 6$ and $12 = 2(6) + 0$, the last non zero remainder is 6 and hence $\gcd(12, 18) = 6$.

b) Using the Euclidean Algorithm:

$$\begin{aligned} 201 &= 1(111) + 90 \\ 111 &= 1(90) + 21 \\ 90 &= 4(21) + 6 \\ 21 &= 3(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

Since the last non-zero remainder was 3, $\gcd(201, 111) = 3$

c) Using the Euclidean Algorithm:

$$\begin{aligned} 1331 &= 1(1001) + 330 \\ 1001 &= 3(330) + 11 \\ 330 &= 11(33) + 0 \end{aligned}$$

Since the last non-zero remainder was 11, $\gcd(1331, 1001) = 11$

d) Using the Euclidean Algorithm:

$$\begin{aligned} 54321 &= 4(12345) + 4941 \\ 12345 &= 2(4941) + 2463 \\ 4941 &= 2(2463) + 15 \\ 2463 &= 164(15) + 3 \\ 15 &= 5(3) + 0 \end{aligned}$$

Since the last non-zero remainder was 3, $\gcd(12345, 54321) = 3$

e) Using the Euclidean Algorithm:

$$5040 = 5(1000) + 401000 \qquad = 40(25) + 0$$

Since the last non-zero remainder was 40, $\gcd(1000, 5040) = 40$

f) Using the Euclidean Algorithm:

$$\begin{aligned} 9888 &= 1(6060) + 3828 \\ 6060 &= 1(3828) + 2232 \\ 3828 &= 1(2232) + 1596 \\ 2232 &= 1(1596) + 636 \\ 1596 &= 2(636) + 324 \\ 636 &= 1(324) + 312 \\ 324 &= 1(312) + 12 \\ 312 &= 26(12) + 0 \end{aligned}$$

Since the last non-zero remainder was 12, $\gcd(9888, 6060) = 12$

4·3·39

a) $1 = 11 - 10$ b) $1 = 21(21) - 10(44)$ c) $12 = 48 - 36$

d) $1 = 13(55) - 21(34)$ e) $3 = 11(213) - 20(117)$ f) $223 = 0 + 223$

g) $1 = 37(2347) - 706(123)$ h) $2 = 1128(3454) - 835(4666)$

4·4·1

$$15(7) \equiv 105 \equiv 26(4) + 1 \equiv 1 \pmod{24}.$$

4·4·3

$$4(7) \equiv 28 \equiv 3(9) + 1 \equiv 1 \pmod{9}.$$

4·4·5

a) Since $1 = 9 - 2(4)$, we have $-2 \equiv 7 \pmod{9}$ as the inverse of 4

b) Since $1 = 52(19) - 7(141)$, we have 52 as the inverse of 19

c) Since $1 = 34(55) - 21(89)$, we have 34 as the inverse of 55

d) Since $1 = 73(89) - 28(232)$, we have 73 as the inverse of 89

4·4·9

The solution will be $5 \cdot 4^{-1} \equiv 5 \cdot 7 \equiv 35 \equiv 8 \pmod{9}$

4.4.11

a) $x \equiv 67 \pmod{141}$

b) $x \equiv 88 \pmod{89}$

c) $x \equiv 146 \pmod{232}$

4.4.15

Proof. Let $m' = \frac{m}{\gcd(c,m)}$. Since all shared factors between c and m are removed from m, m' is coprime to c. Note that m divides $ac - bc = (a-b)c$ and that m' divides it is as well. Therefore since c and m' are coprime, it follows m' must divides $a - b$. Therefore $a \equiv b \pmod{m'}$. ■

4.4.21

We can construct the solution

$$x = 1(3)(5)(11)(1) + 2(2)(5)(11)(2) + 3(2)(3)(11)(1) + 4(2)(3)(5)(7).$$

Therefore the solutions are all of the form

$$x \equiv 323 \pmod{330}.$$

4.4.37

a) $2^{340} \equiv \left(2^{10}\right)^{34} \equiv \left(2^{11-1}\right)^{34} \equiv 1^{34} \equiv 1 \pmod{11}$

b) $2^{340} \equiv 32^{68} \equiv 1^6 8 \equiv 1 \pmod{31}$

c) $2^{340} \equiv 1 \cdot 1 \equiv 1 \pmod{31 \cdot 11}$ and $31 \cdot 11 = 341$

4.5.15

The check digit is 4

4.5.17

The ISBN is $125967651X$. Note that

$$1(1) + 2(2) + 5(3) + 9(4) + 6(5) + 7(6) + 6(7) + 5(8) + 1(9) + 10(10) = 319 \equiv 0 \pmod{11}.$$

Therefore the ISBN is valid.

4.5.21

a) The code cannot be recovered

b) $Q = 5$

c) $Q = 7$

d) $Q = 8$

5.1.3

a) $P(1)$ is the statement that $1^2 = \frac{1(1+1)(2(1)+1)}{6}$

b) $P(1)$ is true since $1^2 = 1 = \frac{6}{6} = \frac{1(2)(3)}{6} = \frac{1(1+1)(2(1)+1)}{6}$

c) $P(k)$, that is $1^2 + 2^2 + \ldots + (k-1)^2 + k^2 = \frac{k(k+1)(2k+1)}{6}$

d) $P(k) \to P(k+1)$

e)

> ***Proof.*** Consider the sum
>
> $$1^2 + 2^2 + \ldots + (k-1)^2 + k^2 + (k+1)^2.$$
>
> By the inductive hypothesis
>
> $$1^2 + 2^2 + \ldots + (k-1)^2 + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2.$$
>
> Since
>
> $$\begin{aligned}\frac{k(k+1)(2k+1)}{6} + (k+1)^2 &= \frac{2k^3+3k^2+k}{6} + \frac{k^2+2k+1}{6} \\ &= \frac{2k^3+4k^2+3k+1}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}\end{aligned}$$
>
> we have what we sought to show. ■

f) $P(1)$ is true and $P(k) \to P(k+1)$ meaning by the principal of mathematical induction $P(n)$ is true for all $n \in \mathbb{Z}^+$

5.1.7

> ***Proof.*** Proceed with induction. Consider the base case $n = 1$. Note that
>
> $$3 = \frac{3(4)}{4} = \frac{3(5^1 - 1)}{4}.$$
>
> Therefore the base case is established. Let $n \in \mathbb{Z}^+$ and assume that
>
> $$3 + 3 \cdot 5 + 3 \cdot 5^2 + \ldots + 3 \cdot 5^n = \frac{3\left(5^{n+1} - 1\right)}{4}.$$
>
> Note that
>
> $$3 + 3 \cdot 5 + 3 \cdot 5^2 + \ldots + 3 \cdot 5^n + 3 \cdot 5^{n+1} = \frac{3\left(5^{n+1} - 1\right)}{4} + 3 \cdot 5^{n+1}$$

by the inductive hypothesis. Therefore

$$\begin{aligned}\frac{3\left(5^{n+1}-1\right)}{4}+3\cdot 5^{n+1} &= \frac{3\left(5^{n+1}-1\right)+3\cdot 4\cdot 5^{n+1}}{4}\\ &= \frac{3\left(5^{n+1}-1\right)+3\cdot (5-1)\cdot 5^{n+1}}{4}\\ &= \frac{3\left(5^{n+1}-1\right)+3\cdot (5^{n+2}-5^{n+1})}{4}\\ &= \frac{3\left(5^{n+2}-1\right)}{4}\end{aligned}$$

hence we have

$$3+3\cdot 5+3\cdot 5^2+\ldots+3\cdot 5^n+3\cdot 5^{n+1}=\frac{3\left(5^{n+2}-1\right)}{4}$$

which was to be shown. Hence the statement holds for all $n\in\mathbb{Z}^+$. ■

5.1.15

Proof. Proceed with induction. Consider the base case $n = 1$. Note that

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

Therefore the base case holds. Let $n \in \mathbb{Z}^+$ and assume that

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

By the inductive hypothesis

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

We have

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

Therefore

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

which was to be shown. Therefore the original statement is true for all $n \in \mathbb{Z}^+$. ■

5.1.23

The integers for which the statement holds are $n \geq 4$.

Proof. Proceed with induction. Consider the base case $n = 4$. Note that

$$2(4) + 3 = 8 + 3 = 11 \leq 16 = 2^4.$$

Therefore the base case holds. Let $n \in \mathbb{Z}^+$ with $n \geq 4$ and assume that

$$2n + 3 \leq 2^n.$$

Note that

$$2(n+1) + 3 = 2n + 5 \leq 4n + 6.$$

Therefore by the inductive hypotheis

$$2^{n+1} = 2 \cdot 2^n \geq 2(2n+3) = 4n + 6 \geq 2(n+1) + 3$$

which was to be shown. Therefore the original statement holds for all integers $n \geq 4$. ■

5.2.37

Proof. Assume that $a = dq + r = dq' + r'$ where $0 \leq r, r' < d$. Note that

$$dq + r = dq' + r' \implies d(q - q') = r - r'.$$

Therefore d divides $r - r'$. However $-d < r - r' < d$ meaning $r - r' = 0 \implies r = r'$. This means as well that $q = q'$. Hence the original solution was unique. ■

5.2.41

Proof. Assume towards contradiction that the well ordering principle is false. Then we can find a set $\varnothing \neq S \subset \mathbb{Z}^+$ such that there is no least element. We can then define the statement

$$P(n) \coloneqq i \notin S, 0 \leq i \leq n.$$

$P(0)$ is true since if $0 \in S$, 0 must be a least element which is assumed not possible. It also follows that $P(n) \to P(n+1)$ because otherwise we would have $n+1$ as a least elements of S. Therefore by induction we have that $P(n)$ is true for all $n \in \mathbb{Z}^+$. However, this means no $n \in \mathbb{Z}^+$ is in S and hence $S = \varnothing$, a contradiction. ■