Discrete Mathematics for Part I CST 2016/17
Proofs and Numbers Exercises

WITH ANSWERS

Marcelo Fiore Ohad Kammar

November 10, 2016

1 On proofs

1.1 Basic exercises

Prove or disprove the following statements.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.

   ANSWER. The statement is false. Choose $n = 9$. Then $n = 3 \cdot 3$ isn't prime, yet $2 \cdot n + 13 = 31$ is prime, and we disproved the statement by a counterexample.

2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

   ANSWER. We equivalently prove that if $x^2 + y = 13$ then $y \neq 4$ implies $x \neq 3$.

   Assume that $x^2 + y = 13$. We establish the contrapositive; i.e. if $x = 3$ then $y = 4$. Indeed, assume $x = 3$. Then, $y = 13 - x^2 = 13 - 9 = 4$ as required.

3. For an integer n, n^2 is even if and only if n is even.

   ANSWER. ($\Leftarrow$) We prove the following more general result: The product of an even integer with any integer is an even integer.

   Consider any two integers m, n and assume that m is even. By definition of even integer, $m = 2 \cdot k$ for some integer k. Therefore, $m \cdot n = 2 \cdot l$ for $l = k \cdot n$ and thus, by definition, $m \cdot n$ is an even integer.

   ($\Rightarrow$) We prove the contrapositive; i.e., n odd impliles n^2 odd. Assume n is odd, then by Proposition 8 of the notes, $n \cdot n = n^2$ is odd.

4. For all real numbers x and y there is a real number z such that $x + z = y - z$.

   ANSWER. Consider arbitrary real numbers x, y, and choose $z = \frac{y-x}{2}$. Then, z is a real number satisfying $x + z = x + \frac{y-x}{2} = \frac{y+x}{2} = y + \frac{y-x}{2} = y - z$. Therefore, there exists a real number z satisfying $x + z = y - z$.

5. For all integers x and y there is an integer z such that $x + z = y - z$.

   ANSWER. The statement is false. Indeed, for the integers $x = 0$ and $y = 1$ we will prove that there does not exist an integer z satisfying $x + z = y - z$; i.e., equivalently, such that $z = 1 - z$. Assume to the contrary that such an integer, say z_0, existed. Then, we would have $2 \cdot z_0 = 1$ and hence $z_0 = \frac{1}{2}$; which is absurd as $\frac{1}{2}$ is not an integer. Therefore, there are integers x and y for which there is no integer z such that $x + z = y - z$.

6. The addition of two rational numbers is a rational number.

   ANSWER. We prove the statement.

   Consider any two rational numbers r, s. By definition, there exist some integers a, c and some positive integers b, d such that $r = \frac{a}{b}$ and $s = \frac{c}{d}$. Then, $r+s = \frac{a \cdot d + b \cdot c}{b \cdot d}$ is a quotient of an integer (namely $a \cdot d + b \cdot c$) by a positive integer (namely $b \cdot d$), and hence a rational number.

7. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2 \cdot y/(y+1) = x$.

   ANSWER. We need to show that for every real number x, if $x \neq 2$ then there exists a real number y satisfying: (i) $\frac{2 \cdot y}{y+1} = x$ and (ii) for all real numbers z, if $\frac{2 \cdot z}{z+1} = x$ then $y = z$.

   Here are two arguments.

   - A direct proof relying on the evident scratch work.
     Consider an arbitrary real number x, and assume $x \neq 2$. Then, $y = \frac{x}{2-x}$ is a real number satisfying (i), and if z is any real number satisfying $\frac{2 \cdot z}{z+1} = x$ then $2 \cdot z = z \cdot x + x$. Hence, $(2-x) \cdot z = x$. As $x \neq 2$, $z = \frac{x}{2-x} = y$.
   - A proof by formalising the scratch work.
     Consider an arbitrary real number x, and assume $x \neq 2$. Consider an arbitrary real number y. Then,

     $$\begin{aligned} \tfrac{2 \cdot y}{y+1} = x \quad &\iff \quad 2 \cdot y = y \cdot x + x \\ &\iff \quad (2-x) \cdot y = x \\ &\iff \quad y = \tfrac{x}{2-x} \end{aligned}$$

     Therefore, if we choose $y = \frac{x}{2-x}$ then we have (i), and if we consider an arbitrary z satisfying $\frac{2 \cdot z}{z+1} = x$ then $z = \frac{x}{2-x} = y$, so we also have (ii).

8. For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

   ANSWER. One may prove the contrapositive of the statement; i.e., that if m and n are odd then $m \cdot n$ is odd. But this is nothing but Proposition 8 of the notes.

1.2 Core exercises

1. Characterise those integers d and n such that:

   (a) $0 \mid n$,

   ANSWER. We prove that an integer n satisfies $0 \mid n$ iff $n = 0$.
   $(\Rightarrow)$ Assume $0 \mid n$. By definition, for some integer l, $n = l \cdot 0 = 0$.
   $(\Leftarrow)$ Assume $n = 0$. Then, $n = 0 \cdot 0$ and, by definition, $0 \mid n$.

   (b) $d \mid 0$.

   ANSWER. We prove that $d \mid 0$ for all integers d.
   Indeed, let d be an arbitrary integer. Then, $0 = 0 \cdot d$ and hence $d \mid 0$.

2. Let k, m, n be integers with k positive. Show that:

   $$(k \cdot m) \mid (k \cdot n) \iff m \mid n \quad .$$

   ANSWER. Consider any positive integer k and any two integers m, n.

   $(\Rightarrow)$ Assume $(k \cdot m) \mid (k \cdot n)$. Then, $k \cdot n = l \cdot (k \cdot m)$. As $k > 0$, we can cancel k and deduce $n = l \cdot m$. Hence, $m \mid n$.

   $(\Leftarrow)$ Assume $m \mid n$. Then, $n = a \cdot m$ for some integer a; and multiplying by k, we have $k \cdot n = a \cdot (k \cdot m)$. Hence, $(k \cdot m) \mid (k \cdot n)$. (Btw, note that here we did not require the assumption that k is positive.)

3. Prove or disprove that: For all natural numbers n, $2 \mid 2^n$.

   ANSWER. This is false, as $2 \nmid 2^0$.

4. Prove that for all integers n,

$$30 \mid n \iff \big(2 \mid n \wedge 3 \mid n \wedge 5 \mid n\big) \quad .$$

   ANSWER. ($\Rightarrow$) Assume $30 \mid n$. Then, $n = 30 \cdot a$ for some integer a. Thus, $n = 2 \cdot (15 \cdot a)$ and so $2 \mid n$. Similarly, $n = 3 \cdot (10 \cdot a)$ and therefore $3 \mid n$. And, as $n = 5 \cdot (6 \cdot a)$, we also deduce $5 \mid n$. Therefore $2 \mid n \wedge 3 \mid n \wedge 5 \mid n$.

   ($\Leftarrow$) Assume $2 \mid n \wedge 3 \mid n \wedge 5 \mid n$. As $2 \mid n$ and $3 \mid n$ and $5 \mid n$, we have $n = 2 \cdot a$ and $n = 3 \cdot b$ and $n = 5 \cdot c$ for some integers a, b, c. Moreover, we have:

$$30 \cdot (a + b - 4 \cdot c) = 15 \cdot 2 \cdot a + 10 \cdot 3 \cdot b - 4 \cdot 6 \cdot 5 \cdot c = 15 \cdot n + 10 \cdot n - 24 \cdot n = n$$

   Thus, $n = 30 \cdot k$ for the integer $k = a + b - 4 \cdot c$, as required.

5. Find a counterexample to the statement: For all positive integers k, m, n,

$$\text{if } (m \mid k \wedge n \mid k) \text{ then } (m \cdot n) \mid k \quad .$$

   ANSWER. Choose $k = m = n = 2$. Then, k, m, n are positive integers. As $2 \mid 2$, we have $m \mid k \wedge n \mid k$ yet $(2 \cdot 2) \nmid 2$.

6. Show that for all integers l, m, n,

$$l \mid m \wedge m \mid n \implies l \mid n \quad .$$

   ANSWER. Consider any integers l, m, n, and assume $l \mid m \wedge m \mid k$. As $l \mid m$, $m = a \cdot l$ for some integer a. As $m \mid n$, $n = b \cdot m$ for some integer b. But then: $n = b \cdot m = b \cdot (a \cdot l) = (b \cdot a) \cdot l$ and, as $b \cdot a$ is an integer, we have $l \mid n$.

7. Prove that for all integers d, k, l, m, n,

   (a) $d \mid m \wedge d \mid n \implies d \mid (m + n)$,

   ANSWER. Assume $d \mid m \wedge d \mid n$. As $d \mid m$, $m = a \cdot d$ for some integer a. As $d \mid n$, $n = b \cdot d$ for some integer b. Therefore, $m + n = a \cdot d + b \cdot d = (a + b) \cdot d$. As $a + b$ is an integer, we have $d \mid (m + n)$ as required.

   (b) $d \mid m \implies d \mid k \cdot m$,

   ANSWER. Assume $d \mid m$; i.e., $m = a \cdot d$ for some integer a. Then, $k \cdot m = k \cdot (a \cdot d) = (k \cdot a) \cdot d$. As $k \cdot a$ is an integer, $d \mid (k \cdot m)$.

   (c) $d \mid m \wedge d \mid n \implies d \mid (k \cdot m + l \cdot n)$.

   ANSWER. Assume $d \mid m \wedge d \mid n$. As $d \mid m$, by (7b) above, $d \mid (k \cdot m)$. Analogously, from $d \mid n$ we have $d \mid (l \cdot n)$. Thus, $d \mid (k \cdot m) \wedge d \mid (l \cdot n)$ so that applying (7a) we conclude $d \mid (k \cdot m + l \cdot n)$ as required.

8. Show that for all integers m and n,

$$(\, m \mid n \wedge n \mid m \,) \implies (\, m = n \vee m = -n \,) \quad .$$

ANSWER. Consider any pair of integers m, n, and assume that $m \mid n$ and that $n \mid m$.

If $m = 0$ then, by (1a) above, $n = 0$ and we have $m = n$.

Consider henceforth the case $m \neq 0$. As $m \mid n$ and $n \mid m$, there are integers a, b such that $n = a \cdot m$ and $m = b \cdot n$. Thus, $m = b \cdot a \cdot m$ and, as $m \neq 0$, we have $b \cdot a = 1$. Then, since a and b are integers, either $a = b = 1$ or $a = b = -1$ (otherwise, one would have $a \cdot b \geq 2$ or $a \cdot b \leq -2$). Finally, if $a = b = 1$ then $m = n$, and if $a = b = -1$ then $m = -n$. Either way, $m = n$ or $m = -n$ as required.

9. Prove or disprove that: For all positive integers k, m, n,

   if $k \mid (m \cdot n)$ then $k \mid m$ or $k \mid n$.

   ANSWER. We disprove it by means of a counterexample. Choose $m = n = 2$ and $k = 4$. Then $k \mid m \cdot n$, yet neither $k \mid m$ nor $k \mid n$.

10. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the derived statement

$$P^{\#}(m) \;=\; \big(\forall \text{ natural number } k.\ 0 \leq k \leq m \implies P(k)\big)$$

again for m ranging over the natural numbers.

(a) Show that, for all natural numbers ℓ, $P^{\#}(\ell) \implies P(\ell)$.

ANSWER. Let ℓ be a natural number, and assume that

$$P^{\#}(\ell) = \big(\forall \text{ natural number } k.\ 0 \leq k \leq \ell \implies P(k)\big)$$

holds.

Since ℓ is a natural number, it follows by instantiation that

$$0 \leq \ell \leq \ell \implies P(\ell)$$

and, since $0 \leq \ell \leq \ell$ is true, it follows by Modus Ponens that $P(\ell)$ holds as required.

(b) Exhibit a concrete statement $P(m)$ and a specific natural number n for which the statement

$$P(n) \implies P^{\#}(n)$$

does not hold.

ANSWER. Let $P(m) = (m = 1)$ and $n = 1$. Then $P(1) = (1 = 1)$ is true, but $P^{\#}(1)$ is equivalent to $P(0) \wedge P(1) = (0 = 1) \wedge (1 = 1)$ which is false.

(c) Prove the following:

- $P^{\#}(0) \iff P(0)$

  ANSWER. ($\Rightarrow$) Assume $P^{\#}(0)$; that is, for all $0 \leq k \leq 0$, $P(k)$. As $0 \leq 0 \leq 0$, $P(0)$ holds.
  ($\Leftarrow$) Assume $P(0)$. Consider any k, and assume $0 \leq k \leq 0$. Then, $k = 0$ and $P(k)$ holds by assumption.

- $\forall$ natural number $n. \big(P^{\#}(n) \implies P^{\#}(n+1)\big) \iff \big(P^{\#}(n) \implies P(n+1)\big)$

  ANSWER. ($\Rightarrow$) Assume that $\big(P^{\#}(n) \implies P^{\#}(n+1)\big)$, and further assume that $P^{\#}(n)$ holds. Then, it follows that also $P^{\#}(n+1)$ holds; i.e., that

$$\forall \text{ natural number } k.\ 0 \leq k \leq n+1 \implies P(k) \ .$$

  In particular, by instantiation, we have that

$$0 \leq n+1 \leq n+1 \implies P(n+1)$$

and since the antecedent of this implication is true, we deduce that $P(n+1)$ holds, as required. $(\Leftarrow)$ Assume that (i) $\big(P^{\#}(n) \implies P(n+1)\big)$, and further assume that (ii) $P^{\#}(n)$ holds. We need show that $P^{\#}(n+1)$ also holds; i.e., that

$$\forall \text{ natural number } k.\ 0 \leq k \leq n+1 \implies P(k)$$

or, equivalently, that

$$P^{\#}(n) \ \wedge \ P(n+1)$$

hold, which is indeed the case because $P^{\#}(n)$ holds by assumption (ii) and $P(n+1)$ follows by Modus Ponens from assumptions (i) and (ii).

- $\big(\forall \text{ natural number } m.\, P^{\#}(m)\big) \iff \big(\forall \text{ natural number } m.\, P(m)\big)$

  ANSWER. $(\Rightarrow)$ Assume that $\forall$ natural number $m.\, P^{\#}(m)$, and let n be an arbitrary natural number. Then, by assumption, $P^{\#}(n)$ holds; that is

  $$\forall \text{ natural number } k.\ 0 \leq k \leq n \implies P(k) \ .$$

  and, by instantiation, $0 \leq n \leq n \implies P(n)$ so that $P(n)$ holds. Thus, we have shown

  $$\forall \text{ natural number } m.\, P(m) \ .$$

  $(\Leftarrow)$ Assume that (i) $\forall$ natural number $m.\, P(m)$. We need show that for all natural numbers m and k,

  $$0 \leq k \leq m \implies P(k) \ .$$

  To this end, let m and k be arbitrary natural numbers, and assume $0 \leq k \leq m$. Since k is a natural number, we may instantiate assumption (i) with it yielding $P(k)$ as required.

1.3 Optional advanced exercises

1. [Adapted from David Burton]

   (a) A natural number is said to be *triangular* if it is of the form $\sum_{i=0}^{k} i = 0+1+\cdots+k$, for some natural number k. For example, the first three triangular numbers are $t_0 = 0$, $t_1 = 1$, and $t_2 = 3$. Find the next three triangular numbers t_3, t_4, and t_5.

   ANSWER. $t_3 = 6$, $t_4 = 10$, $t_5 = 15$.

   (b) Find a formula for the k-th triangular number t_k.

   ANSWER.

   - Geometric approach.

   $$2 \cdot t_k \ = \ \begin{array}{ccc} \circ & & \\ \circ & \circ & \\ \vdots & & \\ \circ & \cdots & \circ \end{array} \ + \ \begin{array}{ccc} \bullet & \cdots & \bullet \\ & & \\ & \bullet & \vdots \\ & & \bullet \end{array} \ = \ \begin{array}{cccc} \circ & \bullet & \cdots & \bullet \\ \circ & \circ & \bullet & \bullet \\ \vdots & & & \vdots \\ \circ & \cdots & \circ & \bullet \end{array} \ = \ k \cdot (k+1)$$

   - Algebraic approach.
     Note that, on the one hand,

   $$\begin{aligned} \textstyle\sum_{i=0}^{k}(i+1)^2 - \sum_{i=0}^{k} i^2 &= (k+1)^2 + \big(\textstyle\sum_{i=0}^{k-1}(i+1)^2\big) - \big(\textstyle\sum_{i=1}^{k} i^2\big) - 0^2 \\ &= (k+1)^2 \end{aligned}$$

and that, on the other,

$$\begin{aligned}\textstyle\sum_{i=0}^{k}(i+1)^2-\sum_{i=0}^{k}i^2 &= \textstyle\sum_{i=0}^{k}\big((i+1)^2-i^2\big)\\ &= \textstyle\sum_{i=0}^{k}(2\cdot i+1)\\ &= \big(2\cdot\textstyle\sum_{i=0}^{k}i\big)+\sum_{i=0}^{k}1\\ &= 2\cdot t_k+k+1\end{aligned}$$

so that $t_k=\frac{k^2+k}{2}$.

(c) A natural number is said to be *square* if it is of the form k^2 for some natural number k. [Plutarch, circ. 100BC] Show that n is triangular iff $8\cdot n+1$ is square.

ANSWER. ($\Rightarrow$) Assume n is triangular; i.e., $n=t_k$ for some natural number k. By the previous item, $n=\frac{k\cdot(k+1)}{2}$ and one has that $8\cdot n+1=(2\cdot k+1)^2$ is a square number.
($\Leftarrow$) Assume that $8\cdot n+1$ is a square number; i.e., $8\cdot n+1=a^2$ for some natural number a. Then a^2 is odd and, by Proposition 12 of the notes, thus so is a. Therefore, $a=2\cdot k+1$ for some natural number k. Finally, since $8\cdot n+1=a^2=(2\cdot k+1)^2=4\cdot k^2+4\cdot k+1$ one has $n=\frac{k^2+k}{2}=t_k$ as required.

(d) [Nicomachus, circ. 100BC] Show that the sum of every two consecutive triangular numbers is square.

ANSWER. Consider any two consecutive triangular numbers t_k and t_{k+1}. Then, a calculation shows that the sum t_k+t_{k+1} equals $(k+1)^2$ and hence is square.

(e) [Euler, 1775] Show that, for all natural numbers n, if n is triangular, then so are $9\cdot n+1$, $25\cdot n+3$, $49\cdot n+6$, and $81\cdot n+10$.

ANSWER. Consider any natural number n, and assume that n is triangular; i.e., $n=\frac{k\cdot(k+1)}{2}$ for some natural number k. Then, calculate that $9\cdot n+1=t_{3k+1}$, $25\cdot n+3=t_{5\cdot k+2}$, $49\cdot n+6=t_{7\cdot k+3}$, and $81\cdot n+10=\cdots$.

(f) [Jordan, 1991, attributed to Euler] Prove the generalisation: For all n and k natural numbers, there exists a natural number q such that: $(2n+1)^2\,t_k+t_n=t_q$.

ANSWER. Here's a proof by a 2014/15 student (who wished to remain anonymous). Let n and k be arbitrary natural numbers. We know that:

$$t_k=\frac{k(k+1)}{2}\qquad\text{and}\qquad t_n=\frac{n(n+1)}{2}$$

Choose $q=2nk+n+k$, and calculate:

$$\begin{aligned}t_q=\frac{q(q+1)}{2}&=\frac{(2nk+n+k)\cdot(2nk+n+k+1)}{2}\\ &=\frac{4n^2k^2+4n^2k+4nk^2+4nk+k^2+k+n^2+n}{2}\\ &=\frac{(4n^2+4n+1)(k^2+k)+n^2+n}{2}\\ &=(2n+1)^2\cdot\frac{k(k+1)}{2}+\frac{n(n+1)}{2}\\ &=(2n+1)^2\,t_k+t_n\end{aligned}$$

Therefore we are done.

2. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x. (For instance, $P(x)$ could be the predicate "programmer x found a software bug" and Q could be the statement "all the code has to be rewritten".)

Show that the equivalence

$$\Big(\big(\exists x.\, P(x)\big) \implies Q \Big) \iff \Big(\forall x.\, \big(P(x) \implies Q\big) \Big)$$

holds.

ANSWER. ($\Rightarrow$) Assume $\big(\exists x.\, P(x)\big) \implies Q$. We need show $\forall x.\, \big(\, P(x) \implies Q\,\big)$. We do this by considering an arbitrary a and showing that $P(a) \implies Q$, for which in turn we further assume $P(a)$ and finally show Q.

To recap, then, we are in the following situation:

Assumptions	Goal
$\big(\exists x.\, P(x)\big) \implies Q$	Q
for arbitrary a	
$P(a)$	

Then, by the last assumption, $\exists x.\, P(x)$ and from this and the first assumption, by Modus Ponens, we deduce Q as required.

($\Leftarrow$) Assume $\forall x.\, \big(P(x) \implies Q\big)$. We need show $\big(\exists x.\, P(x)\big) \implies Q$. For which we further assume $\exists x.\, P(x)$ and show Q

To recap, then, we are in the following situation:

Assumptions	Goal
$\forall x.\, \big(P(x) \implies Q\big)$	Q
$\exists x.\, P(x)$	

From the second assumption, there is an a for which (i) $P(a)$ holds and, by instantiation from the first assumption, (ii) $P(a) \implies Q$. By Modus Ponens from (ii) and (i), Q follows as required.

2 On numbers

2.1 Basic exercises

1. Let i, j be integers and let m, n be positive integers. Show that:

   (a) $i \equiv i \pmod m$

   ANSWER. Because, by §1.1(1b), every number divides $i - i = 0$.

   (b) $i \equiv j \pmod m \implies j \equiv i \pmod m$

   ANSWER. Assume $i \equiv j \pmod m$. Then $m \mid i - j$; i.e., $i - j = k \cdot m$ for some integer k. Thus, $j - i = (-k) \cdot m$, and as $-k$ is an integer $m \mid j - i$; i.e., $j \equiv i \pmod m$.

   (c) $i \equiv j \pmod m \,\wedge\, j \equiv k \pmod m \implies i \equiv k \pmod m$

   ANSWER. Assume $i \equiv j \pmod m \,\wedge\, j \equiv k \pmod m$. Then, $m \mid i - j$ and $m \mid j - k$. Hence, by §1.1(7a), $m \mid (i - j) + j - k = i - k$ and $i \equiv k \pmod m$.

2. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,

   (a) $i \equiv j \pmod m \,\wedge\, k \equiv l \pmod m \implies i + k \equiv j + l \pmod m$

   ANSWER. Assume $i \equiv j \pmod m \,\wedge\, k \equiv l \pmod m$. Then, $m \mid i - j$ and $m \mid k - l$. Hence, by §1.1(7a), $m \mid (i - j) + (k - l) = (i + j) - (j + l)$ and $i + j \equiv k + l \pmod m$.

(b) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$

ANSWER. Assume $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m}$. Then, $m \mid (i-j)$ and $m \mid (k-l)$. By §1.1(7b), $m \mid i \cdot (k-l)$ and $m \mid l \cdot (i-j)$; and, by §1.1(7a), $m \mid i \cdot (k-l) + l \cdot (i-j) = i \cdot k - j \cdot l$. Hence, $i \cdot k \equiv j \cdot l \pmod{m}$.

(c) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$

ANSWER. For $n = 0$, $i^n \equiv j^n \pmod{m}$ always. Assume now (1) $i \equiv j \pmod{m}$. Then, for $n = 1$, we are done by assumption. For $n = 2$, by the previous item, we have (2) $i^2 \equiv j^2 \pmod{m}$. From (1) and (2), again by the previous item, we have $i^3 \equiv j^3 \pmod{m}$. Iterating this process we get $i^n \equiv j^n \pmod{m}$ for every value of n. (Btw, a formal proof requires the mathematical Principle of Induction, which will be studied later in the course.)

3. Prove that for all natural numbers k, l, and positive integer m,

(a) $\mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m)$

ANSWER. By the Division Theorem,

$$l = \mathrm{quo}(l, m) \cdot m + \mathrm{rem}(l, m)$$

and hence

$$k \cdot m + l = \big(k + \mathrm{quo}(l, m)\big) \cdot m + \mathrm{rem}(l, m)$$

from which it follows by the Division Theorem (explain why!) that

$$\mathrm{quo}(k \cdot m + l, m) = k + \mathrm{quo}(l, m) \quad \text{and} \quad \mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m) \quad .$$

Give another proof using the Division Algorithm.

(b) $\mathrm{rem}(k + l, m) = \mathrm{rem}\big(\mathrm{rem}(k, m) + l, m\big)$, and

ANSWER. Because

$$\begin{aligned} \mathrm{rem}(k + l, m) &= \mathrm{rem}\big(\mathrm{quo}(k, m) \cdot m + \mathrm{rem}(k, m) + l, m\big) \\ &= \mathrm{rem}\big(\mathrm{rem}(k, m) + l, m\big) && \text{, by (3a)} \end{aligned}$$

Note that, as a corollary, $\mathrm{rem}(k + l, m) = \mathrm{rem}\big(\mathrm{rem}(k, m) + \mathrm{rem}(l, m), m\big)$.

(c) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}\big(k \cdot \mathrm{rem}(l, m), m\big)$.

ANSWER. Because

$$\begin{aligned} \mathrm{rem}(k \cdot l, m) &= \mathrm{rem}\big(k \cdot \mathrm{quo}(l, m) \cdot m + k \cdot \mathrm{rem}(l, m), m\big) \\ &= \mathrm{rem}\big(k \cdot \mathrm{rem}(l, m), m\big) && \text{, by (3a)} \end{aligned}$$

Note that, as a corollary, $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}\big(\mathrm{rem}(k, m) \cdot \mathrm{rem}(l, m), m\big)$.

4. Let m be a positive integer.

(a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is, that for all i, j, k in $\mathbb{Z}_m$,

$$(i +_m j) +_m k = i +_m (j +_m k) \quad \text{and} \quad (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k) \quad .$$

ANSWER. Consider arbitrary i, j, k in $\mathbb{Z}_m$, and calculate as follows:

$$\begin{aligned}
(i +_m j) +_m k &= \big[[i+j]_m + k\big]_m && \text{, by definition of } +_m \\
&= \operatorname{rem}\big(\operatorname{rem}(i+j,m)+k,m\big) && \text{, by definition of } [\cdot]_m \\
&= \operatorname{rem}\big((i+j)+k,m\big) && \text{, by §2.1(3b)} \\
&= \operatorname{rem}\big(i+(j+k),m\big) && \\
&= \operatorname{rem}\big(i+\operatorname{rem}(j+k,m),m\big) && \text{, by §2.1(3b)} \\
&= \big[i+[j+k]_m\big]_m && \text{, by definition of } [\cdot]_m \\
&= i +_m (j +_m k) && \text{, by definition of } +_m
\end{aligned}$$

The result for $\cdot_m$ is similar and left as an exercise.

(b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

ANSWER. We need show that $k +_m [-k]_m \equiv 0 \pmod{m}$; and indeed, since

$$l \equiv [l]_m \pmod{m} \text{ for all integers } l \ ,$$

one has that

$$k +_m [-k]_m = \big[k + [-k]_m\big]_m \equiv k + [-k]_m \equiv k + (-k) = 0 \pmod{m} \ .$$

2.2 Core exercises

1. Find an integer i, natural numbers k, l, and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.

   ANSWER. Take $i = 2$, $k = 0$, $l = 3$, and $m = 3$. Then, $k = 0 \equiv 3 = l \pmod{3}$, yet $2^0 = 1 \not\equiv 8 = 2^3 \pmod{3}$.

2. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for analogous criteria for multiples of 9 and for multiples of 11.

   ANSWER. For all natural numbers n and digits $a_1, \ldots, a_n$,

   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv 0 \pmod{3} \iff \big(\sum_{i=0}^{n} a_i\big) \equiv 0 \pmod{3}$
   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv 0 \pmod{9} \iff \big(\sum_{i=0}^{n} a_i\big) \equiv 0 \pmod{9}$
   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv 0 \pmod{11} \iff \big(\sum_{i=0}^{n} (-1)^i \cdot a_i\big) \equiv 0 \pmod{11}$

   The above follow from the following stronger statements

   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv \big(\sum_{i=0}^{n} a_i\big) \pmod{3}$
   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv \big(\sum_{i=0}^{n} a_i\big) \pmod{9}$
   - $\big(\sum_{i=0}^{n} a_i \cdot 10^i\big) \equiv \big(\sum_{i=0}^{n} (-1)^i \cdot a_i\big) \pmod{11}$

   that are easily established from the previous item.

   There are also other proofs. Below is one based on the Binomial Theorem, rather than on the theory of divisibility and/or congruences for the case of divisibility by 11. Please study it and re-adapt it to the cases of divisibility by 3 and by 9.

First we calculate that

$$\begin{array}{rcl} \sum_{i=0}^{n} a_i \cdot 10^i & = & \sum_{i=0}^{n} a_i \cdot (11-1)^i \\ & = & \sum_{i=0}^{n} a_i \cdot \sum_{j=0}^{i} \binom{i}{j} \cdot 11^j \cdot (-1)^{i-j} \\ & = & \sum_{i=0}^{n} a_i \cdot \left[\, (-1)^i + 11 \cdot \sum_{j=1}^{i} \binom{i}{j} \cdot 11^{j-1} \cdot (-1)^{i-j} \,\right] \\ & = & \left(\, \sum_{i=0}^{n} (-1)^i \cdot a_i \,\right) + 11 \cdot \left[\, \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{i} \binom{i}{j} \cdot 11^{j-1} \cdot (-1)^{i-j} \,\right] \end{array}$$

and then argue as follows:

($\Rightarrow$) Assume $11 \mid \left(\, \sum_{i=0}^{n} a_i \cdot 10^i \,\right)$; so that $\sum_{i=0}^{n} a_i \cdot 10^i = 11 \cdot k$ for some integer k. Then,

$$\sum_{i=0}^{n} (-1)^i \cdot a_i \;=\; 11 \cdot \Big(k - \left[\, \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{i} \binom{i}{j} \cdot 11^{j-1} \cdot (-1)^{i-j} \,\right] \Big)$$

showing that $11 \mid \left(\, \sum_{i=0}^{n} (-1)^i \cdot a_i \,\right)$.

($\Leftarrow$) Assume $11 \mid \left(\, \sum_{i=0}^{n} (-1)^i \cdot a_i \,\right)$; so that $\sum_{i=0}^{n} (-1)^i \cdot a_i = 11 \cdot l$ for some integer l. Then,

$$\sum_{i=0}^{n} a_i \cdot 10^i \;=\; 11 \cdot \Big(l + \left[\, \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{i} \binom{i}{j} \cdot 11^{j-1} \cdot (-1)^{i-j} \,\right] \Big)$$

showing that $11 \mid \sum_{i=0}^{n} a_i \cdot 10^i$.

3. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.

   ANSWER. This is Lemma 26 of the notes.

4. What are $\mathrm{rem}(55^2, 79)$, $\mathrm{rem}(23^2, 79)$, $\mathrm{rem}(23 \cdot 55, 79)$, and $\mathrm{rem}(55^{78}, 79)$?

   ANSWER. $\mathrm{rem}(55^2, 79) = 23$, $\mathrm{rem}(23^2, 79) = 55$, $\mathrm{rem}(23 \cdot 55, 79) = 1$, and

$$\begin{array}{rclcl} \mathrm{rem}\big((55^2)^{39}, 79\big) & = & \mathrm{rem}\big(23 \cdot (23^2)^{19}, 79\big) & = & \mathrm{rem}\big(23 \cdot 55 \cdot (55^2)^{9}, 79\big) \\ & = & \mathrm{rem}\big(23 \cdot (23^2)^{4}, 79\big) & = & \mathrm{rem}\big(23 \cdot (55^2)^{2}, 79\big) \\ & = & \mathrm{rem}\big(23 \cdot 23^2, 79\big) & = & \mathrm{rem}\big(23 \cdot 55, 79\big) \\ & = & 1 & & \end{array}$$

   Of course, since we know the last one from Fermat's Little Theorem, there was really no need to calculate it!

5. Calculate that $2^{153} \equiv 53 \pmod{153}$.

   ANSWER. $2^6 \cdot (2^7)^{21} \equiv 2^6 \cdot (-25) \cdot \big(25^2\big)^{10} \equiv 2^6 \cdot (-25) \cdot (13^2)^5 \equiv (-25) \cdot 2^6 \cdot 16^5 \equiv (-25) \cdot 2^5 \cdot (2^7)^3 \equiv (-25) \cdot 2^5 \cdot (-25) \cdot 25^2 \equiv 2^5 \cdot (25^2)^2 \equiv 2^5 \cdot 13^2 \equiv 2^5 \cdot 16 \equiv 2^2 \cdot 2^7 \equiv 4 \cdot (-25) \equiv 53$.

   (Btw, at first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though?)

   ANSWER. Because 153 is not prime.

6. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$.

   ANSWER.

   - $\mathbb{Z}_3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

	$-(\cdot)$
0	0
1	2
2	1

	$(\cdot)^{-1}$
0	
1	1
2	2

- $\mathbb{Z}_6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

	$-(\cdot)$
0	0
1	5
2	4
3	3
4	2
5	1

	$(\cdot)^{-1}$
0	
1	1
2	
3	
4	
5	5

- $\mathbb{Z}_7$

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	$-(\cdot)$
0	0
1	6
2	5
3	4
4	3
5	2
6	1

	$(\cdot)^{-1}$
0	
1	1
2	4
3	5
4	2
5	3
6	6

7. Prove that $n^3 \equiv n \pmod 6$ for all integers n.

ANSWER. Let n be an arbitrary integer.

Since either $n \equiv 0 \pmod 6$, or $n \equiv 1 \pmod 6$, or $n \equiv 2 \pmod 6$, or $n \equiv 3 \pmod 6$, or $n \equiv 4 \pmod 6$, or $n \equiv 5 \pmod 6$, we check that $n^3 \equiv n \pmod 6$ in each case.

- Case $n \equiv 0 \pmod 6$: $n^3 \equiv 0^3 = 0 \equiv n \pmod 6$.
- Case $n \equiv 1 \pmod 6$: $n^3 \equiv 1^3 = 1 \equiv n \pmod 6$.
- Case $n \equiv 2 \pmod 6$: $n^3 \equiv 2^3 = 8 \equiv 2 \equiv n \pmod 6$.
- Case $n \equiv 3 \pmod 6$: $n^3 \equiv 3^3 = 27 \equiv 3 \equiv n \pmod 6$.
- Case $n \equiv 4 \pmod 5$: $n^3 \equiv 4^3 = 64 \equiv 4 \equiv n \pmod 6$.
- Case $n \equiv 5 \pmod 6$: $n^3 \equiv 5^3 = 125 \equiv 5 \equiv n \pmod 6$.

For a conceptual proof (rather than a calculational one as above), prove and use that

$$\text{for all integers } a, b\text{: } a \equiv b \pmod 6 \iff \big(a \equiv b \pmod 2 \ \wedge\ a \equiv b \pmod 3\big)$$

in conjunction with Fermat's Little Theorem for the primes 2 and 3.

8. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod p$ for all i not multiple of p.

ANSWER. Assume that i and n are positive integers and that p is a prime. Assume further that $n \equiv 1 \pmod{p-1}$; so that $n - 1 = k \cdot (p-1)$ for some *natural number* k. Then, for i not a multiple of p, we have that

$$\begin{array}{rcll} i^n & = & i \cdot (i^{p-1})^k & \\ & \equiv & i \cdot 1^k \pmod p & \text{, by Fermat's Little Theorem} \\ & = & i & \end{array}$$

9. Prove that $n^7 \equiv n \pmod{42}$ for all integers n.

HINT. Study the conceptual answer to §2.3(7) above.

2.3 Optional advanced exercises

1. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$.

ANSWER. Consider an arbitrary integer n.

($\Rightarrow$) Assume there exist natural numbers i and j such that $n = i^2 - j^2$. By Proposition 25 of the notes, we have that

$$\text{either } i^2 \equiv 0 \pmod 4 \text{ or } i^2 \equiv 1 \pmod 4$$

and

$$\text{either } j^2 \equiv 0 \pmod 4 \text{ or } j^2 \equiv 1 \pmod 4$$

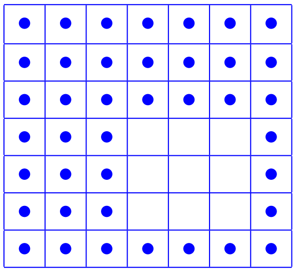
We therefore have four cases:

- $i^2 \equiv 0 \pmod 4$ and $j^2 \equiv 0 \pmod 4$, in which case $n \equiv 0 \pmod 4$;
- $i^2 \equiv 0 \pmod 4$ and $j^2 \equiv 1 \pmod 4$, in which case $n \equiv -1 \equiv 3 \pmod 4$;
- $i^2 \equiv 1 \pmod 4$ and $j^2 \equiv 0 \pmod 4$, in which case $n \equiv 1 \pmod 4$;
- $i^2 \equiv 1 \pmod 4$ and $j^2 \equiv 1 \pmod 4$, in which case $n \equiv 0 \pmod 4$;

Hence, either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$ as required.

($\Leftarrow$) Assume that either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$. We need to find natural numbers i and j such that $n = i^2 - j^2$

Graphically, we want to show that one can distribute any number of balls in a square grid leaving an empty square sub-grid, for instance as follows:



We split our analysis in three cases.

- Case n is zero.
  There are natural numbers $i = j = 0$ such that $n = i^2 - j^2$, and we are done.
- Case n is a non-zero even integer.
  As $\mathrm{rem}(n,4) \;=\; n - \mathrm{quo}(n,4) \cdot 4$, it follows that $\mathrm{rem}(n,4)$ is even and hence necessarily 0. Thus, n is in fact a non-zero multiple of 4; say of the form $4 \cdot k$ for some non-zero integer k. Then,

  $$n \;=\; (k+1)^2 - (k-1)^2 \;=\; (-k-1)^2 - (1-k)^2$$

  and since either

  $$k+1 \text{ and } k-1 \text{ are natural numbers}$$

  or

  $$-k-1 \text{ and } 1-k \text{ are natural numbers}$$

there are natural numbers i, j such that $n = i^2 - j^2$. (Btw, note that this argument slightly generalises that of Proposition 22 of the notes.)

Graphically, we are in the following kind of situation:

●$_2$	●$_2$	●$_2$	●$_2$	●$_2$	●$_2$	●$_2$	●$_3$
●$_1$							●$_3$
●$_1$							●$_3$
●$_1$							●$_3$
●$_1$							●$_3$
●$_1$							●$_3$
●$_1$							●$_3$
●$_1$	●$_4$	●$_4$	●$_4$	●$_4$	●$_4$	●$_4$	●$_4$

- Case n is odd.

  Then $n = 2 \cdot k + 1$ for some integer k, and

$$n \;=\; (k+1)^2 - k^2 \;=\; (-k-1)^2 - (-k)^2 \;\; .$$

  Since either

$$k + 1 \text{ and } k \text{ are natural numbers}$$

  or

$$-k - 1 \text{ and } -k \text{ are natural numbers}$$

  there are natural numbers i, j such that $n = i^2 - j^2$.

  Graphically, we are in the following kind of situation:

●	●$_2$	●$_2$	●$_2$	●$_2$	●$_2$	●$_2$
●$_1$						
●$_1$						
●$_1$						
●$_1$						
●$_1$						
●$_1$						

(Btw, note that the proof is for all integer values of n while the graphical representation only applies to natural numbers.)

2. [Adapted from David Burton]

   A *decimal (respectively binary) repunit* is a natural number whose decimal (respectively binary) representation consists solely of 1's.

   (a) What are the first three decimal repunits? And the first three binary ones?

   ANSWER. The first three decimal repunits are 1, 11, and 111; while the first three binary repunits are 1, 3, and 7.

   (b) Show that no decimal repunit strictly greater than 1 is square, and that the same holds for binary repunits. Is this the case for every base?

ANSWER. Let n be a decimal repunit greater than 1; that is, $n = \sum_{i=0}^{l} 10^i$ for some $l \geq 1$. Then,

$$n \equiv \sum_{i=0}^{l} 2^i \equiv 1 + 2 = 3 \pmod 4$$

and, by Proposition 25 of the notes, we deduce that n is not square.
Btw, the proof for binary repunits is contained in the above. (Why?)
The statement:

> For every base r, there are no r-ary repunits greater than 1.

is false. As a counterexample, take the base $r = 3$ and the 3-ary repunit 4 consisting of two 1's.

3 More on numbers

3.1 Basic exercises

1. Calculate the set CD(666, 330) of common divisors of 666 and 330.

   ANSWER. We have that $666 = 2 \cdot 3^2 \cdot 37$ and $330 = 2 \cdot 3 \cdot 5 \cdot 11$. Hence, $\mathrm{CD}(666, 330) = \{1, 2, 3, 2 \cdot 3\} = \{1, 2, 3, 6\}$.

2. Find the gcd of 21212121 and 12121212.

   HINT. Learn and run Euclid's Algorithm to find that $\gcd(21212121, 12121212) = 3030303$.

3. Prove that for all positive integers m and n, and integers k and l,

$$\gcd(m, n) \mid (k \cdot m + l \cdot n) \ .$$

   ANSWER. Let m, n be positive integers and k, l be integers. As $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$ it follows from §1.1(7a) that $\gcd(m, n) \mid k \cdot m$ and $\gcd(m, n) \mid l \cdot n$; from which it further follows by §1.1(7b) that $\gcd(m, n) \mid (k \cdot m + l \cdot n)$.

4. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \leq y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.

   HINT. Run the Extended Euclid's Algorithm to find that $\gcd(30, 22) = 2$ and $x \cdot 30 + y \cdot 22 = 2$ for $x = \cdots$ and $y = \cdots$.

   Notice also that

$$(x + 11 \cdot l) \cdot 30 + (y - 15 \cdot l) \cdot 22 \ = \ 2$$

   for all integers l, and find a value $l_0 = \cdots$ such that $0 \leq y - 15 \cdot l_0 < 30$ setting $x' = x + 11 \cdot l_0$ and $y' = y - 15 \cdot l_0$.

5. Prove that, for all positive integers m and n, there exist integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m, n) = 1$.

   ANSWER. ($\Leftarrow$) By Theorem 68 of the notes.

   ($\Rightarrow$) By Corollary 61 of the notes

6. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod p$ then either $n \equiv 1 \pmod p$ or $n \equiv -1 \pmod p$.

   ANSWER. Assume $n^2 \equiv 1 \pmod p$. Then p divides $n^2 - 1 = (n - 1) \cdot (n + 1)$. By Euclid's Theorem, $p \mid (n - 1)$ or $p \mid (n + 1)$; that is, either $n \equiv 1 \pmod p$ or $n \equiv -1 \pmod p$.

3.2 Core exercises

1. Prove that for all positive integers m and n,

$$\gcd(m,n) = m \iff m \mid n \ .$$

ANSWER. Let m and n be arbitrary positive integers.

($\Rightarrow$) Assume that $\gcd(m,n) = m$. Then m is the greatest common divisor of both m and n, and in particular a divisor of n.

($\Leftarrow$) Assume $m \mid n$.

Here are two arguments.

(i) We have that $n = k \cdot m$ for some positive integer k, and hence that

$$\gcd(m,n) = \gcd(m, k \cdot m) = m \cdot \gcd(1,k) = m$$

where the second equality is a consequence of the linearity property (Lemma 62(3) of the notes) of gcd.

(ii) By Theorem 60 of the notes, it suffices to prove (explain why!) that

- $m \mid m$ and $m \mid n$, and
- for all positive integers d such that $d \mid m$ and $d \mid n$ it necessarily follows that $d \mid m$;

all of which hold trivially (explain why!).

2. Prove that for all positive integers a, b, c,

$$\gcd(a,c) = 1 \implies \gcd(a \cdot b, c) = \gcd(b,c) \ .$$

HINT. Here is an equational proof sketch: For a, b, c positive integers such that $\gcd(a,c) = 1$, we have

$$\begin{aligned}
\gcd(b,c) &= \gcd\big(\gcd(a,c) \cdot b, c\big) && \text{, by } \ldots \\
&= \gcd\big(\gcd(a \cdot b, c \cdot b), c\big) && \text{, by } \ldots \\
&= \gcd\big(a \cdot b, \gcd(c \cdot b, c)\big) && \text{, by } \ldots \\
&= \gcd(a \cdot b, c) && \text{, by } \ldots
\end{aligned}$$

where you should fill in the gaps explaining each of the steps above.

You should also provide two more proofs of this result, using Theorem 60 of the notes and the Fundamental Theorem of Arithmetic.

3. Prove that for all positive integers m and n, and integers i and j:

$$n \cdot i \equiv n \cdot j \pmod m \iff i \equiv j \ (\text{mod } \frac{m}{\gcd(m,n)})$$

ANSWER. We have:

$$n \cdot i \equiv n \cdot j \pmod m \iff k \cdot m = n(i-j) \iff k \cdot \frac{m}{\gcd(m,n)} = \frac{n}{\gcd(m,n)} \cdot (i-j)$$

$$\iff \frac{m}{\gcd(m,n)} \,\Bigg|\, \frac{n}{\gcd(m,n)} \cdot (i-j)$$

To conclude, we note that

$$\frac{m}{\gcd(m,n)} \;\Big|\; \frac{n}{\gcd(m,n)} \cdot (i-j) \iff i \equiv j \pmod{\frac{m}{\gcd(m,n)}}$$

where ($\Leftarrow$) follows from §1.1(77b), and ($\Rightarrow$) follows from Euclid's Theorem, as by linearity:

$$\gcd(m,n) = \gcd(m,n) \cdot \gcd(\frac{m}{\gcd(m,n)}, \frac{m}{\gcd(m,n)}) \implies 1 = \gcd(\frac{m}{\gcd(m,n)}, \frac{m}{\gcd(m,n)})$$

4. Let m and n be positive integers with $\gcd(m,n) = 1$. Prove that for every natural number k,

$$m \mid k \,\wedge\, n \mid k \iff (m \cdot n) \mid k \quad .$$

ANSWER. Let m and n be arbitrary positive integers, and assume that (i) $\gcd(m,n) = 1$. Further, let k be a natural number.

($\Rightarrow$) Assume that (ii) $m \mid k$ and (iii) $n \mid k$.

It follows from (i) that

$$m \cdot i + n \cdot j = 1 \qquad (\dagger)$$

for some integers i, j; and it follows from (ii) and (iii) that

$$k = a \cdot m = b \cdot n \qquad (\ddagger)$$

for some natural numbers a, b.

Multiplying ($\dagger$) by k on both sides and using ($\ddagger$), we therefore have

$$k \;=\; b \cdot n \cdot m \cdot i + a \cdot m \cdot n \cdot j \;=\; (b \cdot i + a \cdot j) \cdot (m \cdot n)$$

showing that $(m \cdot n) \mid k$.

($\Leftarrow$) Assume that $(m \cdot n) \mid k$. Then, since both $m \mid (m \cdot n)$ and $n \mid (m \cdot n)$, by §1.1(6), we are done.

5. Prove that for all positive integers m, n, p, q such that $\gcd(m,n) = \gcd(p,q) = 1$, if $q \cdot m = p \cdot n$ then $m = p$ and $n = q$.

ANSWER. Let m, n, p, q be positive integers. Assume that $\gcd(m,n) = \gcd(p,q) = 1$ and further that (i) $q \cdot m = p \cdot n$.

Multiplying both sides of the identity $1 = \gcd(m,n)$ by p and using the linearity property of gcd we have that

$$p \;=\; p \cdot \gcd(m,n) \;=\; \gcd(p \cdot m, p \cdot n) \;\; . \qquad (\dagger)$$

Now, from (i) and the linearity property of gcd, we also have that

$$\gcd(p \cdot m, p \cdot n) \;=\; \gcd(p \cdot m, q \cdot m) \;=\; \gcd(p,q) \cdot m \;\; . \qquad (\ddagger)$$

Finally, since $\gcd(p,q) = 1$, one has $p = m$ from ($\dagger$) and ($\ddagger$).

To conclude the proof, give an analogous argument showing that also $n = q$.

6. Prove that for all positive integers a and b,

$$\gcd\big(\,13\cdot a+8\cdot b\,,\,5\cdot a+3\cdot b\,\big)\;=\;\gcd(a,b)\quad.$$

ANSWER. Here's a calculational proof: for all positive integers a and b, one has

$$\begin{aligned}
\gcd\big(\,13\cdot a+8\cdot b\,,\,5\cdot a+3\cdot b\,\big) &= \gcd\big(\,(13\cdot a+8\cdot b)-(5\cdot a+3\cdot b)\,,\,5\cdot a+3\cdot b\,\big)\\
&= \gcd\big(\,8\cdot a+5\cdot b\,,\,5\cdot a+3\cdot b\,\big)\\
&= \gcd\big(\,(8\cdot a+5\cdot b)-(5\cdot a+3\cdot b)\,,\,5\cdot a+3\cdot b\,\big)\\
&= \gcd\big(\,3\cdot a+2\cdot b\,,\,5\cdot a+3\cdot b\,\big)\\
&= \gcd\big(\,3\cdot a+2\cdot b\,,\,(5\cdot a+3\cdot b)-(3\cdot a+2\cdot b)\,\big)\\
&= \gcd\big(\,3\cdot a+2\cdot b\,,\,2\cdot a+b\,\big)\\
&= \gcd\big(\,(3\cdot a+2\cdot b)-(2\cdot a+b)\,,\,2\cdot a+b\,\big)\\
&= \gcd\big(\,a+b\,,\,2\cdot a+b\,\big)\\
&= \gcd\big(\,a+b\,,\,(2\cdot a+b)-(a+b)\,\big)\\
&= \gcd\big(\,a+b\,,\,a\,\big)\\
&= \gcd\big(\,(a+b)-a\,,\,a\,\big)\\
&= \gcd\big(\,b\,,\,a\,\big)\\
&= \gcd\big(\,a\,,\,b\,\big)
\end{aligned}$$

Can you also give a conceptual proof?

7. (a) Prove that if an integer n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.

   HINT. This is an instance of Fermat's Little Theorem. A calculational proof can be give as in §2.3(7).

   (b) Show that if an integer n is odd, then $n^2 \equiv 1 \pmod{8}$

   ANSWER. Let n be an odd integer, and thereby let k be an integer such that $n = 2\cdot k+1$. We consider two cases.

   - Case k is even.
     Then, $k = 2\cdot l$ for some integer l, and $n^2 = 8\cdot l\cdot(2\cdot l+1) \equiv 1 \pmod{8}$.
   - Case k is odd.
     Then, $k = 2\cdot l+1$ for some integer l, and $n^2 = 8\cdot(2\cdot l+1)\cdot(l+2)+1 \equiv 1 \pmod{8}$.

   Either way $n^2 \equiv 1 \pmod{8}$, as required.

   (c) Conclude that if p is a prime greater than 3, then p^2-1 is divisible by 24.

   ANSWER. Let p be a prime greater than 3. Then, p is an odd integer not divisible by 3 and it follows from the first item above that: (i) $3 \mid (p^2-1)$. Moreover, as p is odd, we have from the second item above that: (ii) $8 \mid (p^2-1)$.
   Finally, since $\gcd(3,8)=1$, by §3.1(4), one has that (i) and (ii) imply $24 \mid (p^2-1)$ as required.

8. Prove that $n^{13} \equiv n \pmod{10}$ for all integers n.

   HINT. Study the conceptual answer to §2.3(7) above.

9. Prove that for all positive integers l, m, and n, if $\gcd(l, m\cdot n) = 1$ then $\gcd(l,m)=1$ and $\gcd(l,n)=1$.

   ANSWER. Let l, m, and n be arbitrary positive integers, and assume that $\gcd(l, m\cdot n)=1$.
   By §3.3(5($\Leftarrow$)), there exist integers i and j such that $i\cdot l + j\cdot m\cdot n = 1$. Thus, we have that

there exist integers i and a such that $i \cdot l + a \cdot m = 1$

and

there exist integers i and b such that $i \cdot l + b \cdot n = 1$.

Therefore, by §3.3(5($\Rightarrow$)), one has that $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

10. Solve the following congruences:

   (a) $77 \cdot x \equiv 11 \pmod{40}$

   HINT. Run the Extended Euclid's Algorithm on the pair $(7, 40)$ to compute integers i and j such that $7 \cdot i + 40 \cdot j = 1$. Notice then that i is a solution because $11 = 77 \cdot i + 40 \cdot 11 \cdot j \equiv 77 \cdot i$ (mod 4)0. Prove that, in fact, all solutions are of the form $i + 40 \cdot k$ for k ranging over the integers.

   (b) $12 \cdot y \equiv 30 \pmod{54}$

   HINT. Run the Extended Euclid's Algorithm on the pair $(2, 9)$ to compute integers i and j such that $2 \cdot i + 9 \cdot j = 1$. Notice then that $5 \cdot i$ is a solution because $30 = 12 \cdot (5 \cdot i) + 54 \cdot 5 \cdot j \equiv 12 \cdot (5 \cdot i) \pmod{54}$. Prove that, in fact, all solutions are of the form $5 \cdot i + \frac{54}{\gcd(12,54)} \cdot k$ for k ranging over the integers.

   (c) $\begin{cases} z \equiv 13 \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

   HINT. As before, all solutions of the first congruence are of the form

$$13 + 21 \cdot k$$

   for k ranging over the integers, and all solutions of the second congruence are of the form

$$2 \cdot i_0 + 17 \cdot l$$

   for l ranging over the integers and where i_0 is such that $3 \cdot i_0 + 17 \cdot j_0 = 1$ for some integer j_0 both of which you should compute by running the Extended Euclid's Algorithm on the pair $(3, 17)$. With this information, to solve the congruence system, we need find integer values for k and l such that

$$13 + 21 \cdot k \;=\; 2 \cdot i_0 + 17 \cdot l \;\; .$$

   To do this, run the Extended Euclid's Algorithm on the pair $(21, 17)$ to compute integers k_0 and l_0 such that

$$21 \cdot k_0 + 17 \cdot l_0 = 1 \;\; .$$

   Then,

$$21 \cdot \big(k_0 \cdot (2 \cdot i_0 - 13)\big) + 17 \cdot \big(l_0 \cdot (2 \cdot i_0 - 13)\big) \;=\; 2 \cdot i_0 - 13$$

   and one can take as solution of the congruence system:

$$13 + 21 \cdot \big(k_0 \cdot (2 \cdot i_0 - 13)\big) \;=\; 2 \cdot i_0 + 17 \cdot \big(l_0 \cdot (13 - 2 \cdot i_0)\big) \;\; .$$

11. What is the multiplicative inverse of: (i) 2 in $\mathbb{Z}_7$, (ii) 7 in $\mathbb{Z}_{40}$, and (iii) 13 in $\mathbb{Z}_{23}$?

   HINT. Apply Corollary 73 of the notes.

12. Prove that $[22^{12001}]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$.

   ANSWER. Because $\gcd(22^{12001}, 175) = \gcd(2^{12001} \cdot 11^{12001}, 5^2 \cdot 7) = 1$ using the following remark:

> For every pair of positive integers m and n, we have that $[n]_m$ has a multiplicative inverse in $\mathbb{Z}_m$ iff $\gcd(m,n)=1$.

the proof of which follows.

($\Rightarrow$) Let m and n be arbitrary positive integers, and assume that $[n]_m$ has a multiplicative inverse in $\mathbb{Z}_m$, say l. Then,

$$n\cdot l \;\equiv\; [n\cdot l]_m \;=\; [n]_m \cdot_m l \;=\; 1 \pmod{m}$$

and thus there exists an integer k such that $n\cdot l + m\cdot k = 1$. Thus, from §3.3(5($\Rightarrow$)), $\gcd(m,n)=1$.

($\Leftarrow$) By Corollary 73(2) of the notes.

3.3 Optional advanced exercises

1. (a) Let a and b be natural numbers such that $a^2 \mid b(b+a)$. Prove that $a \mid b$.

ANSWER. If either a or b are 0 the result is straightforward. Consider thus the case in which both a and b are positive integers, and assume that $a^2 \mid b(b+a)$.
Then, for $a_0 = \frac{a}{\gcd(a,b)}$ and $b_0 = \frac{b}{\gcd(a,b)}$, we have that $a_0 \mid b_0(b_0+a_0)$ and, since $\gcd(a_0,b_0)=1$, that $a_0 \mid (b_0+a_0)$ so that $a_0 \mid b_0$ and thus $a_0 = \gcd(a_0,b_0) = 1$. Therefore, $\gcd(a,b)=a$ and we are done.

(b) [49th Putnam, 1988] Prove the converse to §1.3(1f): For all natural numbers n and s, if there exists a natural number q such that:

$$(2n+1)^2 s + t_n = t_q$$

then there exists a natural number k such that $s = t_k$.

ANSWER. Suggested by a 2014/15 student (who wished to remain anonymous).
Assume $(2n+1)^2 s + t_n = t_q$. Then, $t_n \equiv t_q \big(\text{mod } (2n+1)^2\big)$; so that $n(n+1) \equiv q(q+1) \big(\text{mod } (2n+1)^2\big)$ and hence $(q-n)(q-n+2n+1) \equiv 0 \big(\text{mod } (2n+1)^2\big)$.
Therefore $(2n+1)^2 \mid (q-n)(q-n+2n+1)$, and it follows from the previous item that $(2n+1) \mid (q-n)$.
As $t_q \geq t_n$, we have that $q \geq n$, and therefore that $k = \frac{q-n}{2n+1}$ is a natural number. By assumption and the solution to §1.3(1f), we then have:

$$(2n+1)^2\, s + t_n = t_q = (2n+1)^2\, t_k + t_n$$

and so that $s = t_k$, as required.

2. Show the correctness of the following algorithm

```
fun gcd0( m , n )
  = if m = n then m
    else
      let
        val p = min(m,n) ; val q = max(m,n)
      in
        gcd0( p , q - p )
      end
```

for computing the gcd of two positive integers.

ANSWER. The partial correctness of the algorithm follows from Corollary 57(2) of the notes. To establish the termination of `gcd0` on a pair of positive integers (m,n) we consider and analyse the computations arising from the call `gcd0`(m,n). We consider three cases:

- Case $m = n$.

  The computation of `gcd0`(m, n) reduces in one step to m, and therefore terminates.

- Case $m \neq n$.

  The computation of `gcd0`(m, n) reduces in one step to that of `gcd0`$(p, q-p)$, where $p = \min(m, n)$ and $q = \max(m, n)$. Thus, the passage of computing `gcd0`(m, n) by means of computing `gcd0`$(p, q-p)$ maintains the invariant of having both components of the pair being positive integers; but, crucially, strictly decreases the sum of the pairs in each recursive call (as $m + n > \max(m, n) = p + (q - p)$ because both m and n are positive). As this process cannot go on for ever (explain why!), the recursive calls must eventually stop and the overall computation terminate (in fact, in a number of steps necessarily less that or equal the sum of the input pair).

Btw, the formalisation of arguments such as the above requires induction; and, to make the point here, we proceed to show that

> For all natural numbers $l \geq 2$, we have that for all positive integers m, n, if $m + n \leq l$ then `gcd0`(m, n) terminates.

by the Principle of Induction.

Base case: We need show that for all positive integers m, n, if $m + n \leq 2$ then `gcd0`(m, n) terminates. To this end, we let m and n be arbitrary positive integers, and assume that $m + n \leq 2$. Then, $m = n = 1$ and `gcd0`(m, n) terminates.

Inductive step: Let l be an arbitrary natural number greater than or equal 2, and assume the Induction Hypothesis

(IH) For all positive integers m, n, if $m + n \leq l$ then `gcd0`(m, n) terminates.

We need show that for all positive integers m, n, if $m+n \leq l+1$ then `gcd0`(m, n) terminates. To this end, we let a, b be arbitrary positive integers, assume that $a + b \leq l + 1$, and proceed to prove that `gcd0`(a, b) terminates.

We consider three cases.

- If $a = b$, then `gcd0`(a, b) terminates.
- If $a < b$, then `gcd0`$(a, b) =$ `gcd0`$(a, b - a)$. Moreover, by the Inductive Hypothesis (IH), we have that

  $$\text{if } a + (b - a) \leq l \text{ then } \texttt{gcd0}(a, b - a) \text{ terminates} \ ,$$

  and since

  $$a + (b - a) \ = \ b \ \leq \ l + 1 - a \ \leq \ l$$

  it follows that `gcd0`$(a, b - a)$ terminates and therefore that so does `gcd0`(a, b).

- If $b < a$, then `gcd0`$(a, b) =$ `gcd0`$(b, a - b)$. Moreover, by the Inductive Hypothesis (IH), we have that

  $$\text{if } b + (a - b) \leq l \text{ then } \texttt{gcd0}(b, a - b) \text{ terminates} \ ,$$

  and since

  $$b + (a - b) \ = \ a \ \leq \ l + 1 - b \ \leq \ l$$

  it follows that `gcd0`$(b, a - b)$ terminates and therefore that so does `gcd0`(a, b).

4 On induction

4.1 Basic exercises

1. Prove that for all natural numbers $n \geq 3$, if n distinct points on a circle are joined in consecutive order by straight lines, then the interior angles of the resulting polygon add up to $180 \cdot (n-2)$ degrees.

2. Prove that, for any positive integer n, a $2^n \times 2^n$ square grid with any one square removed can be tiled with L-shaped pieces consisting of 3 squares.

4.2 Core exercises

1. Establish the following:

   (a) For all positive integers m and n,

$$(2^n - 1) \cdot \textstyle\sum_{i=0}^{m-1} \; 2^{i \cdot n} = 2^{m \cdot n} - 1 \quad .$$

ANSWER. The first thing to note is that an inductive proof is not really necessary. Indeed, for arbitrary positive integers m and n, one can calculate that

$$\begin{aligned}(2^n - 1) \cdot \textstyle\sum_{i=0}^{m-1} 2^{i \cdot n} &= \textstyle\sum_{i=0}^{m-1} 2^{(i+1) \cdot n} - \sum_{i=0}^{m-1} 2^{i \cdot n} \\ &= \textstyle\sum_{i=1}^{m-1} 2^{i \cdot n} + 2^{((m-1)+1) \cdot n} - 2^{0 \cdot n} - \sum_{i=1}^{m-1} 2^{i \cdot n} \\ &= 2^{m \cdot n} - 1\end{aligned}$$

However, as it is very instructive, two inductive proofs follow. Note the different, though subtle, ways in which the inductive hypothesis is used in each proof.

For the *first proof*, we show

$$\forall \, m \geq 1 \text{ in } \mathbb{N}. \, P(m)$$

for $P(m)$ the statement

$$\forall \, n \geq 1 \text{ in } \mathbb{N}. \; (2^n - 1) \cdot \sum_{i=0}^{m-1} \; 2^{i \cdot n} \; = \; 2^{m \cdot n} - 1$$

by the Principle of Induction.

Base case: The statement $P(1)$ amounts to

$$\forall \, n \geq 1 \text{ in } \mathbb{N}. \; (2^n - 1) \cdot 2^{0 \cdot n} \; = \; 2^{1 \cdot n} - 1$$

which is vacuously true.

Inductive step: Let k be an arbitrary positive integer, and assume that the Inductive Hypothesis $P(k)$ holds for it; i.e., that

$$(\mathrm{IH}_1) \qquad \forall \, n \geq 1 \text{ in } \mathbb{N}. \; (2^n - 1) \cdot \textstyle\sum_{i=0}^{k-1} \; 2^{i \cdot n} \; = \; 2^{k \cdot n} - 1 \; .$$

We need show that $P(k+1)$ follows; i.e., that

$$\forall \, n \geq 1 \text{ in } \mathbb{N}. \; (2^n - 1) \cdot \sum_{i=0}^{(k+1)-1} \; 2^{i \cdot n} \; = \; 2^{(k+1) \cdot n} - 1 \; .$$

To this end, we let l be an arbitrary positive integer and proceed to show that

$$(2^l - 1) \cdot \textstyle\sum_{i=0}^{k} \; 2^{i \cdot l} \; = \; 2^{(k+1) \cdot l} - 1 \; . \qquad (\dagger)$$

Indeed, instantiating the (IH_1), we have that

$$(2^l - 1) \cdot \textstyle\sum_{i=0}^{k-1} \; 2^{i \cdot l} \;=\; 2^{k \cdot l} - 1 \qquad (\star)$$

and so that

$$\begin{array}{rcll} (2^l - 1) \cdot \sum_{i=0}^{k} 2^{i \cdot l} & = & \big(\, (2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} \,\big) + (2^l - 1) \cdot 2^{k \cdot l} & \\ & = & 2^{k \cdot l} - 1 + (2^l - 1) \cdot 2^{k \cdot l} & \text{, by } (\star) \\ & = & 2^{(k+1) \cdot l} - 1 & \end{array}$$

establishing (†) as required.

For the *second proof*, to show

$$\forall\, n \geq 1 \text{ in } \mathbb{N}.\, \forall\, m \geq 1 \text{ in } \mathbb{N}.\; (2^n - 1) \cdot \sum_{i=0}^{m-1} \; 2^{i \cdot n} \;=\; 2^{m \cdot n} - 1$$

we let l be an arbitrary positive integer and prove

$$\forall\, m \geq 1 \text{ in } \mathbb{N}.\, Q(l, m)$$

for $Q(l, m)$ the statement

$$(2^l - 1) \cdot \sum_{i=0}^{m-1} \; 2^{i \cdot l} \;=\; 2^{m \cdot l} - 1$$

by the Principle of Induction.

Base case: The statement $Q(l, 1)$ amounts to

$$(2^l - 1) \cdot 2^{0 \cdot l} \;=\; 2^{1 \cdot l} - 1$$

which is vacuously true.

Inductive step: Let k be an arbitrary positive integer, and assume that the Inductive Hypothesis $Q(l, k)$ holds for it; i.e., that

$$(\mathrm{IH}_2) \qquad (2^l - 1) \cdot \textstyle\sum_{i=0}^{k-1} \; 2^{i \cdot l} \;=\; 2^{k \cdot l} - 1 \;\;.$$

We need show that $Q(l, k+1)$ follows; i.e., that

$$(2^l - 1) \cdot \textstyle\sum_{i=0}^{(k+1)-1} \; 2^{i \cdot l} \;=\; 2^{(k+1) \cdot l} - 1 \;\;. \qquad (\ddagger)$$

Indeed,

$$\begin{array}{rcll} (2^l - 1) \cdot \sum_{i=0}^{k} 2^{i \cdot l} & = & \big(\, (2^l - 1) \cdot \sum_{i=0}^{k-1} 2^{i \cdot l} \,\big) + (2^l - 1) \cdot 2^{k \cdot l} & \\ & = & 2^{k \cdot l} - 1 + (2^l - 1) \cdot 2^{k \cdot l} & \text{, by } (\mathrm{IH}_2) \\ & = & 2^{(k+1) \cdot l} - 1 & \end{array}$$

establishing (‡) as required.

(b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.

ANSWER. Let k be an arbitrary positive integer. We consider two cases: (i) $k = 1$, and (ii) $k \geq 2$.

(i) The statement holds because $2^1 - 1 = 1$ is not prime.

(ii) Assume that $k \geq 2$ is not prime. Hence, it is of the form $m \cdot n$ for natural numbers m, n greater than or equal 2. It follows from the previous item that $2^k - 1 = 2^{m \cdot n} - 1 = (2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n}$; and, since $2^n - 1 \geq 2^2 - 1 = 3$ and $\sum_{i=0}^{m-1} 2^{i \cdot n} \geq 1 + 4 = 5$, we have that $2^k - 1$ has a non-trivial decomposition. Hence it is not prime.

2. Prove that

$$\forall n \in \mathbb{N}.\ \forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x \quad .$$

ANSWER. We prove $\forall n \in \mathbb{N}. P(n)$ for $P(n)$ the statement

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x$$

by the Principle of Induction.

Base case: The statement $P(0)$ reduces to

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies 1 \geq 1$$

and holds vacuously.

Inductive step: Let k be an arbitrary natural number, and assume $P(k)$; i.e., assume the Inductive Hypothesis

$$\text{(IH)} \qquad \forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^k \geq 1 + k \cdot x \quad .$$

We need show that $P(k+1)$ also holds; i.e., that

$$\forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^{k+1} \geq 1 + (k+1) \cdot x$$

To this end, we let y be an arbitrary real number, assume further that

$$y \geq -1 \quad , \tag{$\star$}$$

and proceed to show that

$$(1+y)^{k+1} \geq 1 + (k+1) \cdot y \quad . \tag{$\dagger$}$$

From (IH), by instantiation and Modus Ponens using ($\star$), one concludes that

$$(1+y)^k \geq 1 + k \cdot y$$

and from this, since by ($\star$) we have $1 + y \geq 0$, it follows that

$$(1+y)^{k+1} \;=\; (1+y)^k \cdot (1+y) \;\geq\; (1+k \cdot y) \cdot (1+y) \;=\; 1 + (k+1) \cdot y + k \cdot y^2$$

Thus, from the fact that $k \cdot y^2 \geq 0$, ($\dagger$) holds.

3. Recall that the Fibonacci numbers F_n for n ranging over the natural numbers are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

   (a) Prove Cassini's Identity: For all natural numbers n,

   $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^{n+1} \quad .$$

   ANSWER. We prove

   $$\forall n \in \mathbb{N}.\, F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^{n+1}$$

   by the Principle of Induction.

   Base case: We have that

   $$F_0 \cdot F_2 = {F_1}^2 + (-1)^1$$

   because $F_0 = 0$ and $F_1 = 1$.

   Inductive step: For an arbitrary natural number n, assume the Induction Hypothesis

(IH) $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^{n+1} \quad .$$

We need show that
$$F_{n+1} \cdot F_{(n+1)+2} = {F_{(n+1)+1}}^2 + (-1)^{(n+1)+1} \quad ;$$
i.e., that
$$F_{n+1} \cdot F_{n+3} = {F_{n+2}}^2 + (-1)^n \quad ,$$
for which one calculates as follows:

$$\begin{array}{lll} F_{n+1} \cdot F_{n+3} & & \\ \quad = & {F_{n+1}}^2 + F_{n+1} \cdot F_{n+2} & \text{, by definition of Fibonacci numbers} \\ \quad = & F_n \cdot F_{n+2} - (-1)^{n+1} + F_{n+1} \cdot F_{n+2} & \text{, by (IH)} \\ \quad = & {F_{n+2}}^2 + (-1)^n & \text{, by definition of Fibonacci numbers} \end{array}$$

(b) Prove that for all natural numbers k and n,
$$F_{n+k+1} = F_{k+1} \cdot F_{n+1} + F_k \cdot F_n \quad .$$

ANSWER. We prove that
$$\forall k \in \mathbb{N}.\, P(k)$$
for $P(k)$ the statement
$$\forall n \in \mathbb{N}.\ F_{n+k+1} \ = \ F_{k+1} \cdot F_{n+1} + F_k \cdot F_n$$
by the Principle of Induction.

Base case: We need show that
$$\forall n \in \mathbb{N}.\ F_{n+1} \ = \ F_1 \cdot F_{n+1} + F_0 \cdot F_n$$
which holds because $F_1 = 1$ and $F_0 = 0$.

Inductive step: For an arbitrary natural number k, assume the Induction Hypothesis

(IH) $$\forall n \in \mathbb{N}.\ F_{n+k+1} \ = \ F_{k+1} \cdot F_{n+1} + F_k \cdot F_n$$

We need show that
$$\forall n \in \mathbb{N}.\ F_{n+(k+1)+1} \ = \ F_{(k+1)+1} \cdot F_{n+1} + F_{k+1} \cdot F_n \quad ;$$
i.e., that
$$\forall n \in \mathbb{N}.\ F_{n+k+2} \ = \ F_{k+2} \cdot F_{n+1} + F_{k+1} \cdot F_n \quad . \qquad (\star)$$
To this end, we let m be an arbitrary natural number and proceed to show the equivalent identity:
$$F_{(m+1)+k+1} \ = \ F_{k+2} \cdot F_{m+1} + F_{k+1} \cdot F_m \quad . \qquad (\dagger)$$
Indeed, instantiating the universally-quantified Induction Hypothesis (IH) for the natural number $m+1$, one has that
$$F_{(m+1)+k+1} = F_{k+1} \cdot F_{(m+1)+1} + F_k \cdot F_{m+1} \quad ,$$
from which one further calculates as follows:

$$\begin{array}{lll} F_{k+1} \cdot F_{(m+1)+1} + F_k \cdot F_{m+1} & & \\ \quad = & F_{k+1} \cdot F_m + F_{k+1} \cdot F_{m+1} + F_k \cdot F_{m+1} & \text{, by definition of Fibonacci numbers} \\ \quad = & F_{k+1} \cdot F_m + F_{k+2} \cdot F_{m+1} & \text{, by definition of Fibonacci numbers} \end{array}$$

to conclude (†).

(Btw, one could have also shown ($\star$) by the Principle of Induction; thereby having an inductive proof within an inductive proof. Sometimes this is indeed necessary.)

(c) Deduce that $F_n \mid F_{l \cdot n}$ for all natural numbers n and l.

HINT. Consider first the cases when either l or n are zero. As for positive n, consider the following scratch work that relies on the previous item:

- $F_{2 \cdot n} = F_{n+(n-1)+1} = F_{n+1} \cdot F_n + F_n \cdot F_{n-1} = F_n \cdot (F_{n+1} + F_{n-1})$
- $$\begin{aligned} F_{3 \cdot n} &= F_{2 \cdot n+(n-1)+1} \\ &= F_{2 \cdot n+1} \cdot F_n + F_{2 \cdot n} \cdot F_{n-1} \\ &= F_{2 \cdot n+1} \cdot F_n + \big(F_n \cdot (F_{n+1} + F_{n-1})\big) \cdot F_{n-1} \\ &= F_n \cdot \big(F_{2 \cdot n+1} + \big(F_{n+1} + F_{n-1}\big) \cdot F_{n-1}\,\big) \end{aligned}$$

Proceed now to give a formal proof by the Principle of Induction.

(d) Prove that $\texttt{gcd}(F_{n+2}, F_{n+1})$ terminates with output 1 in n steps for all positive numbers n.

HINT. Consider the following scratch work

$$\texttt{gcd}(F_{n+2}, F_{n+1}) = \texttt{gcd}(F_{n+1}, F_n) = \cdots = \texttt{gcd}(F_3, F_2) = 1$$

and give a formal proof by the Principle of Induction.

(e) Deduce also that,

(i) for positive integers $n < m$, $\gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$

and hence that,

(ii) for all positive integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

HINT. Firstly, we prove the following statement equivalent to (i):

For all positive integers n and natural numbers k,

$$\gcd(F_{n+k+1}, F_n) = \gcd(F_{k+1}, F_n) \ .$$

Indeed, let n be a positive integer and k a natural number. Then,

$$\begin{aligned} \gcd(F_{n+k+1}, F_n) &= \gcd(F_{n+1} \cdot F_{k+1} + F_n \cdot F_k, F_n) && \text{, by } \ldots \\ &= \gcd(F_{n+1} \cdot F_{k+1}, F_n) && \text{, by } \ldots \\ &= \gcd(F_{k+1}, F_n) && \text{, by } \ldots \end{aligned}$$

where you should fill in the gaps explaining each of the steps above.

Secondly, we prove the following statement from which (ii) follows:

for all positive integers l, $P(l)$

where $P(l)$ is the statement:

for all positive integers m, n,
if $\texttt{gcd0}(n, m)$ terminates in l steps then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

The proof is by the Principle of Induction.

Base case: Let m, n be arbitrary positive integers. Assume that $\texttt{gcd0}(m, n)$ terminates in 1 step. Then $m = n$ and $\gcd(F_m, F_n) = F_m = F_{\gcd(m,n)}$.

Inductive step: Let l be an arbitrary positive integers, and assume the Induction Hypothesis $P(l)$. Further, let m, n be arbitrary positive integers, and assume that $\texttt{gcd0}(m, n)$ terminates in $l + 1$ steps. Then, for $p = \min(m, n)$ and $q = \max(m, n)$, $\texttt{gcd0}(m, n) = \texttt{gcd0}(p, q - p)$ and $\texttt{gcd0}(p, q - p)$ terminates in l steps. Thus, by the Induction Hypothesis, we have that $\gcd(F_{q-p}, F_p) = F_{\gcd(q-p,p)}$. Finally, since by the previous item, $\gcd(F_m, F_n) = \gcd(F_q, F_p) = \gcd(F_{q-p}, F_p)$ and $F_{\gcd(q-p,p)} = F_{\gcd(q,p)} = F_{\gcd(m,n)}$ we are done.

(f) Show that for all positive integers m and n, $(F_m \cdot F_n) \mid F_{m \cdot n}$ if $\gcd(m, n) = 1$.

HINT. Use §4.1(3e-*ii*), §4.1(3c), and §3.1(4).

(g) Conjecture and prove theorems concerning the sums

(*i*) $\sum_{i=0}^{n} F_{2 \cdot i}$, and

(*ii*) $\sum_{i=0}^{n} F_{2 \cdot i+1}$

for n any natural number.

HINT. Consult `wikipedia.org/wiki/Fibonacci_number`.

4.3 Optional advanced exercises

1. Recall the `gcd0` function from §3.3(2). Prove that

> For all natural numbers $l \geq 2$, we have that for all positive integers m, n, if $m + n = l$ then `gcd0`(m, n) terminates.

by the Principle of Strong Induction from basis 2.

HINT. Study §3.3(2).

2. The set of *(univariate) polynomials* (over the rationals) on a variable x is defined as that of arithmetic expressions equal to those of the form $\sum_{i=0}^{n} a_i \cdot x^i$, for some $n \in \mathbb{N}$ and some $a_1, \ldots, a_n \in \mathbb{Q}$.

(a) Show that if $p(x)$ and $q(x)$ are polynomials then so are $p(x) + q(x)$ and $p(x) \cdot q(x)$.

(b) Deduce as a corollary that, for all $a, b \in \mathbb{Q}$, the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials $p(x)$ and $q(x)$ is a polynomial.

(c) Show that there exists a polynomial $p_2(x)$ such that $p_2(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + \cdots + n^2$ for every $n \in \mathbb{N}$.[1]
Hint: Note that for every $n \in \mathbb{N}$,

$$(n+1)^3 \quad = \quad \sum_{i=0}^{n} (i+1)^3 - \sum_{i=0}^{n} i^3 \ . \qquad (\dagger)$$

(d) Show that, for every $k \in \mathbb{N}$, there exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n} i^k = 0^k + 1^k + \cdots + n^k$.
Hint: Generalise

$$(n+1)^2 \quad = \quad \sum_{i=0}^{n} (i+1)^2 - \sum_{i=0}^{n} i^2$$

and (†) above.

[1] Chapter 2.5 of *Concrete Mathematics: A Foundation for Computer Science* by R.L. Graham, D.E. Knuth, and O. Patashnik looks at this in great detail.