Discrete Mathematics

Supervision 3 – Solutions with Commentary

Marcelo Fiore Ohad Kammar Dima Szamozvancev

3. More on numbers

3.1. Basic exercises

1. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.

> We have that $666 = 2 \cdot 3^2 \cdot 37$ and $330 = 2 \cdot 3 \cdot 5 \cdot 11$. Hence, $\mathrm{CD}(666, 330) = \{1, 2, 3, 2 \cdot 3\} = \{1, 2, 3, 6\}$.
>
> ♪ You may be familiar with this method of computing the common divisors of two numbers using their prime factorisation – this of course relies on the Fundamental Theorem of Arithmetic, introduced later in the course.

2. Find the gcd of 21212121 and 12121212.

> We run Euclid's Algorithm:
>
> $$\begin{aligned}\gcd(21212121, 12121212) &= \gcd(12121212, 9090909)\\ &= \gcd(9090909, 3030303)\\ &= 3030303\end{aligned}$$

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

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

> 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 §1.2.6(a) that $\gcd(m, n) \mid k \cdot m$ and $\gcd(m, n) \mid l \cdot n$; from which it further follows by §1.2.6(b) that $\gcd(m, n) \mid (k \cdot m + l \cdot n)$.
>
> ♪ Like rem, we can treat $\gcd(m, n)$ as a function of two positive integers m and n, or as a symbol for the greatest common divisor of m and n defined using the universal property of gcds. For example, we make use of the fact that $\gcd(m, n)$ is a common divisor of m and n, so we "automatically" get $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$. We will see more examples of this in the upcoming exercises.

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 $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.

> Run the Extended Euclid's Algorithm to find that $\gcd(30, 22) = 2$ and $x \cdot 30 + y \cdot 22 = 2$ for $x = 3$ and $y = -4$. To get a y' between the range $0 \leq y' < 30$, we notice that
>
> $$(x + 11 \cdot l) \cdot 30 + (y - 15 \cdot l) \cdot 22 = 2$$

for all integers l (Slide 219), and find a value l_0 such that $0 \leq y - 15 \cdot l_0 < 30$ setting $x' = x + 11 \cdot l_0$ and $y' = y - 15 \cdot l_0$. The two options are $l_0 = -1$ for $(-8) \cdot 30 + 11 \cdot 22 = 2$, and $l_0 = -2$ for $(-19) \cdot x + 26 \cdot 22 = 2$.

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

(⇒) By Corollary 62 of the notes: if 1 can be expressed as a linear combination of m and n, and $\gcd(m, n)$ must divide any linear combination of m and n, we must have $\gcd(m, n) = 1$.

(⇐) By Theorem 70 of the notes: $\gcd(m, n)$ is a linear combination of m and n.

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 $n \equiv -1 \pmod{p}$.

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 $m \mid n$.

Let m and n be arbitrary positive integers.

(⇒) 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.

(⇐) Assume $m \mid n$.

Here are two arguments.

a) 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 63(3) of the notes) of gcd.

b) By Theorem 61 of the notes, it suffices to prove 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.

♪ It's worth analysing the second approach, as it's quite characteristic of proofs by universal properties: the proof just "pops out" without us having to do a whole lot of work, similar to our use of the Division Theorem in §2.1.3(a).

As mentioned in §3.1.3, there are several equivalent ways of thinking about gcds. One is as a function of two positive integers m and n, computed via Euclid's Algorithm; another

is as a label for a unique number characterised by the universal property of being the greatest common divisor of m and n. The difference may seem insignificant, but that is precisely because of Theorem 61, which states that the value computed by Euclid's Algorithm coincides with the greatest common divisor. The universal property of gcds (which we'll get to shortly) is the *specification* of what it is to be a greatest common divisor; Theorem 61 states that Euclid's Algorithm satisfies the specification. We don't *define* the greatest common divisor of m and n as "the number returned by Euclid's Algorithm"; just as how we don't define a sorted list as "the list returned by the quicksort algorithm" or a lasagna as "the dish you get by following this specific recipe in this specific cookbook". We already know what a gcd/sorted list/lasagna is supposed to be, and we can then ask whether some algorithm computes the gcd or some recipe makes a lasagna, or it doesn't. Of course, what makes a lasagna and what is the *best* lasagna is entirely subjective, while mathematical concepts can be unambiguously characterised using universal properties.

Universal properties have two parts: the *property* and the *universality*. The former characterises the set of candidates for the concept we are considering; the latter selects a specific candidate which is "better" than all the other ones. In the case of the greatest common divisor of m and n, the property is that of being a common divisor of m and n: the set of candidates that satisfy this property is $\mathrm{CD}(m,n)$. The "best" such candidate that we are looking for is the one which is greater than all the other ones, and since $\mathrm{CD}(m,n)$ is a finite non-empty set of natural numbers, it must have a unique greatest element $\max(\mathrm{CD}(m,n))$. We can denote this element (which depends entirely on m and n) as $\gcd(m,n)$ and call it the greatest common divisor of m and n.

From this description (or, really, definition) of $\gcd(m,n)$ as the greatest element of the set of common divisors, we can directly extract two "axioms": $\gcd(m,n) \in \mathrm{CD}(m,n)$ (since it is a common divisor), and for all $d \in \mathrm{CD}(m,n)$, $d \leq \gcd(m,n)$ (since it is the greatest common divisor). In fact, we can state something stronger: not only are all other common divisors numerically smaller than $\gcd(m,n)$, they also all divide it: $\forall d \in \mathrm{CD}(m,n).\ d \mid \gcd(m,n)$. Expanding these, we universally characterise $\gcd(m,n)$ as the unique natural number g satisfying the properties of being a common divisor and a multiple of all common divisors:

$$① \ g \mid m \wedge g \mid n \qquad ② \ \forall d \in \mathbb{Z}^+.\ (d \mid m \wedge d \mid n) \Longrightarrow d \mid g$$

Using the transitivity of divisibility (§1.2.4), we can combine these into the concise specification of the universal property of greatest common divisors:

$$③ \ \forall d \in \mathbb{Z}^+.\ (d \mid m \wedge d \mid n) \iff d \mid \gcd(m,n)$$

It's easy to show that gcds are unique: if we had two gcds, both would have to satisfy ② and, in particular, they must divide each other; but divisibility (on positive integers) is antisymmetric (§1.2.8), so the two gcds must be equal. Uniqueness in turn gives rise to the following important proof principle:

> To prove that a number $g \in \mathbb{Z}^+$ is equal to $\gcd(m, n)$,
> it is sufficient to show that g satisfies ① and ②.

This is similar to the approach we used with the Division Theorem: to prove that a number r is equal to $\mathrm{rem}(m, n)$, it was sufficient to show that it is less than n and it can appear in an expansion $m = q \cdot k + r$ with $q \in \mathbb{N}$. Adapting this technique to the combined form ③, we get a useful and particularly simple variation:

> To prove that a number d divides $\gcd(m, n)$, it's sufficient to show that $d \mid m$ and $d \mid n$.

This, combined with the antisymmetry of divisibility (on positive integers), allows us to prove equality of gcds, as shown in the example proofs of Lemma 63 in the notes. In essence, the first step in proving something about $\gcd(m, n)$ or $\mathrm{rem}(n, m)$ is "forgetting" about the $\gcd$ or rem and approach the proof via the universal property; it may seem like a very roundabout technique (as opposed to, for example, a direct chain of equalities ending in $\gcd(m, n)$), but it often leads to short and straightforward proofs. However, it's definitely not the case that *all* proofs about gcds have to be done this way, and we'll see more examples later!

To conclude the discussion, let us expand on proof (b) of this exercise, which uses the UP of gcds. To recap, in the ($\Leftarrow$) direction we need to show:

$$\forall m, n \in \mathbb{Z}^+.\ m \mid n \Longrightarrow \gcd(m, n) = m$$

As always, assume $m, n \in \mathbb{Z}^+$ and $m \mid n$. The proof goal $\gcd(m, n) = m$ asks us to show that m is equal to $\gcd(m, n)$; but, by the proof principle above, it is sufficient to show that m satisfies ① and ②. That is,

$$① \ m \mid m \ \wedge \ m \mid n \qquad ② \ \forall d \in \mathbb{Z}^+.\ (d \mid m \ \wedge \ d \mid n) \Longrightarrow d \mid m$$

① holds by reflexivity of $\mid$ and our assumption $m \mid n$; ② is a direct implication. And that's it! The proof (a) wasn't exactly complicated either, but (b) was rightly labelled as "trivial".

The beautiful thing about this characterisation of gcds is that it is an instance of a much more general mathematical notion called a *greatest lower bound* (with the dual *least upper bound* being the least common multiple). These concepts appear all over mathematics and computer science, and you will encounter many examples in this course as well; accordingly, the proof technique described above can be (and will be, and has already been!) applied in several seemingly different contexts. As a teaser, see if you can spot the similarity between statement ③ above, and the pattern for proving a conjunction of two statements P and Q given any set A of assumptions:

$$\forall A.\ \ (A \Rightarrow P) \ \wedge \ (A \Rightarrow Q) \ \iff \ A \Rightarrow (P \ \wedge \ Q)$$

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

$$m \mid k \ \wedge \ n \mid k \iff m \cdot n \mid k$$

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

($\Rightarrow$) Assume that ② $m \mid k$ and ③ $n \mid k$.

It follows from ① that

$$m \cdot i + n \cdot j = 1 \qquad ④$$

for some integers i, j; and it follows from ② and ③ that

$$k = a \cdot m = b \cdot n \qquad ⑤$$

for some natural numbers a, b.

Multiplying ④ by k on both sides and using ⑤, 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 the transitivity of divisibility, we are done.

♪ The ($\Rightarrow$) direction of this proof used another characterisation of $\gcd(m,n)$ as the *least positive linear combination of m and n*. (NB: "Least" here means "lowest", not the superlative of "less positive".) Now that we are more familiar with universal properties, we can decode this description as ① $\gcd(m,n)$ is a linear combination of m and n, and ② $\gcd(m,n)$ divides all linear combinations of m and n:

$$① \ \exists k_0, l_0 \in \mathbb{Z}.\ k_0 \cdot m + l_0 \cdot n = \gcd(m,n) \qquad ② \ \forall k, l \in \mathbb{Z}.\ \gcd(m,n) \mid k \cdot m + l \cdot n$$

This characterisation is especially useful if we are able to express 1 as a linear combination of m and n, since ② means they must be *coprime*, i.e. $\gcd(m,n) = 1$. Another common use of an assumption of coprimality $\gcd(m,n) = 1$ is that multiplication by $\gcd(m,n)$ is a no-op, so we can freely introduce $\gcd(m,n)$ or $k_0 \cdot m + l_0 \cdot n$ for some $k_0, l_0 \in \mathbb{Z}$ into any expression. This is what we make use of in the question when multiplying ④ and ⑤.

3. Prove that for all positive integers a, b, c, if $\gcd(a,c) = 1$ then $\gcd(a \cdot b, c) = \gcd(b,c)$.

Below are three different proofs of the property.

Proof by equational reasoning

For a, b, c positive integers such that $\gcd(a,c) = 1$, we have

$$\begin{aligned}
\gcd(b,c) &= \gcd(\gcd(a,c) \cdot b, c) && \text{(since } \gcd(a,c) = 1\text{)} \\
&= \gcd(\gcd(a \cdot b, c \cdot b), c) && \text{(by linearity)} \\
&= \gcd(a \cdot b, \gcd(c \cdot b, c)) && \text{(by associativity)} \\
&= \gcd(a \cdot b, c) && \text{(by §3.2.1)}
\end{aligned}$$

Proof by universality

Let a, b, c positive integers such that $\gcd(a, c) = 1$. We need to prove that $\gcd(a \cdot b, c) = \gcd(b, c)$, or equivalently, that $\gcd(a \cdot b, c) \mid \gcd(b, c)$ and $\gcd(b, c) \mid \gcd(a \cdot b, c)$. By the universal property of gcds, it is sufficient to show the following two properties:

- $\gcd(a \cdot b, c) \mid b$ and $\gcd(a \cdot b, c) \mid c$. The latter holds since $\gcd(a \cdot b, c)$ is a divisor of c. To establish the former, we note that $b = \gcd(a, c) \cdot b$ (since a and c are coprime), and by distributivity, $\gcd(a \cdot b, c \cdot b)$. Thus, we can show that $\gcd(a \cdot b, c) \mid \gcd(a \cdot b, c \cdot b)$, or equivalently, $\gcd(a \cdot b, c) \mid a \cdot b$ and $\gcd(a \cdot b, c) \mid c \cdot b$, both of which follow from $\gcd(a \cdot b, c)$ being a common divisor of $a \cdot b$ and c.
- $\gcd(b, c) \mid a \cdot b$ and $\gcd(b, c) \mid c$. Both follow from $\gcd(b, c)$ being a divisor of b and c.

Proof using the Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every positive integer is expressible as the product of a unique finite sequence of ordered primes. If two integers are coprime, their unique prime factorisations must be disjoint: that is, there is no prime p that appears in the factorisation of both a and c. For any $b \in \mathbb{Z}^+$, the prime factorisation of $a \cdot b$ will be the product of those of a and b. Therefore the common prime factors of $a \cdot b$ and c must be the common factors of b and c, since there are no common factors of a and c by assumption. Since the greatest common divisor is the product of the common prime factors, we must have $\gcd(a \cdot b, c) = \gcd(b, c)$.

♪ These are three fairly different proofs of the same (relatively simple) theorem: one uses equational reasoning and some properties of gcds, the second makes use of universality, while the third relies on a powerful and general theorem rather than gcd properties. The first is probably the most concise form, but of course it relies on us having established all the required properties of gcds already.

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

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

We have:

$$\begin{aligned} n \cdot i \equiv n \cdot j \pmod{m} &\iff k \cdot m = n(i - j) \\ &\iff k \cdot \frac{m}{\gcd(m, n)} = \frac{n}{\gcd(m, n)} \cdot (i - j) \\ &\iff \frac{m}{\gcd(m, n)} \,\Bigg|\, \frac{n}{\gcd(m, n)} \cdot (i - j) \end{aligned}$$

Now we show that

$$\frac{m}{\gcd(m,n)} \,\Big|\, \frac{n}{\gcd(m,n)} \cdot (i-j) \iff i \equiv j \left(\bmod \frac{m}{\gcd(m,n)}\right)$$

($\Leftarrow$) We have $\frac{m}{\gcd(m,n)} \mid i-j$ by assumption, and from the multiplication property of divisibility (§1.2.6(b)), we have $\frac{m}{\gcd(m,n)} \mid \frac{n}{\gcd(m,n)} \cdot (i-j)$.

($\Rightarrow$) We first establish that $\frac{m}{\gcd(m,n)}$ and $\frac{n}{\gcd(m,n)}$ are coprime using linearity:

$$\gcd(m,n) = \gcd\left(\frac{m \cdot \gcd(m,n)}{\gcd(m,n)}, \frac{n \cdot \gcd(m,n)}{\gcd(m,n)}\right) = \gcd(m,n) \cdot \gcd\left(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right)$$

Since $\gcd(m,n)$ is a positive integer, this equality can only hold if $\gcd\left(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right) = 1$.

This assumption of coprimality can then be used in Euclid's Theorem to conclude

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

as required.

♪ The inspiration for the first "creative" step (dividing both sides by $\gcd(m,n)$) comes from seeing the term $\frac{m}{\gcd(m,n)}$ in the proof goal.

♪ A very useful corollary of this theorem is that we can always divide both sides of a congruence by a positive integer that is coprime with the modulus. Similarly, we can divide both sides of the congruence *and* the modulus with any positive integer that divides all three. The general theorem handles the case "in between", when a positive integer divides both sides of the congruence, but not the modulus.

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 $n = q$.

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

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

$$p = p \cdot \gcd(m,n) = \gcd(p \cdot m, p \cdot n) \qquad ②$$

Now, from ① and the linearity property of gcd, we also have that

$$\gcd(p \cdot m, p \cdot n) = \gcd(p \cdot m, q \cdot m) = \gcd(p,q) \cdot m \qquad ③$$

Finally, since $\gcd(p,q) = 1$, one has $p = m$ from ② and ③.

We can show with an analogous argument that $n = q$ as well.

6. Prove that for all positive integers a and b, $\gcd(13 \cdot a + 8 \cdot b, 5 \cdot a + 3 \cdot b) = \gcd(a,b)$.

Calculational proof

For all positive integers a and b, one has

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

Conceptual proof (advanced)

We prove following general statement (see 2018/P8/Q9 exam question):

$$\forall n\in\mathbb{N}.\ \gcd(a\cdot F_{n+3}+b\cdot Fn+2, a\cdot F_{n+1}+b\cdot F_n)=\gcd(a,b)$$

where F_n is the nth Fibonacci number, defined recursively as

$$F_0=0 \qquad F_1=1 \qquad F_{n+2}=F_{n+1}+F_n$$

For $n\in\mathbb{N}$, we prove the following two properties, which, by the universal property of gcds, will imply the required equality.

- Both $\gcd(a,b)\mid(aF_{n+3}+bF_{n+2})$ and $\gcd(a,b)\mid(aF_{n+1}+bF_n)$.

  $\gcd(a,b)$ divides both a and b, so it divides every integer linear combination of them (§1.2.6(c)).

- For all positive integers d,

  $$\text{if } d\mid(aF_{n+3}+bF_{n+2}) \text{ and } d\mid(aF_{n+1}+bF_n) \text{ then } d\mid\gcd(a,b).$$

  Let d be a positive integer such that $d\mid(aF_{n+3}+bF_{n+2})$ and $d\mid(aF_{n+1}+bF_n)$; so that $di=aF_{n+3}+bF_{n+2}$ and $dj=aF_{n+1}+bF_n$ for (positive) integers i and j.

It follows that

$$\begin{aligned} d \cdot (iF_n - jF_{n+2}) &= (F_n \cdot F_{n+3} - F_{n+2} \cdot F_{n+1}) \cdot a \\ &= (F_n \cdot F_{n+2} + F_n \cdot F_{n+1} - F_n \cdot F_{n+1} - F_{n+1} \cdot F_{n+1}) \cdot a \\ &= \left(F_n \cdot F_{n+2} - F_{n+1}^2\right) \cdot a \\ &= (-1)^{n+1} a && \text{(Cassini's Identity)} \end{aligned}$$

so that $d \mid a$; and, analogously,

$$\begin{aligned} d \cdot (iF_{n+1} - jF_{n+3}) &= (F_{n+1} \cdot F_{n+2} - F_{n+3} \cdot F_n) \cdot a \\ &= (F_{n+1} \cdot F_{n+1} + F_n \cdot F_{n+1} - F_n \cdot F_{n+1} - F_n \cdot F_{n+2}) \cdot b \\ &= \left(F_{n+1}^2 - F_n \cdot F_{n+2}\right) \cdot b \\ &= (-1)^n b && \text{(Cassini's Identity)} \end{aligned}$$

so that $d \mid b$. Thus, $d \mid \gcd(a, b)$ as required.

♪ You will learn more about Fibonacci numbers in the next set of exercises.

7. Let n be an integer.

   a) Prove that if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

   This is an instance of Fermat's Little Theorem.

   b) Show that if n is odd, then $n^2 \equiv 1 \pmod 8$.

   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 number greater than 3, then $p^2 - 1$ is divisible by 24.

   Let p be a prime greater than 3. Then, p is an odd integer not divisible by 3 and it follows from part (a) that: ① $3 \mid (p^2 - 1)$. Moreover, as p is odd, we have from part (b) that: ② $8 \mid (p^2 - 1)$.

   Finally, since $\gcd(3, 8) = 1$, by §3.2.2 one has that ① and ② imply $24 \mid (p^2 - 1)$ as required.

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

> To show $n^{13} \equiv n \pmod{10}$, by the direct corollary of §3.2.2 it is sufficient to show $n^{13} \equiv n \pmod 2$ and $n^{13} \equiv n \pmod 5$. Both hold by successive applications of Fermat's Little Theorem, repeatedly reducing n^2 or n^5 to n until we reach n. For example:
>
> $$n^{13} = n^5 \cdot n^5 \cdot n^3 \equiv n \cdot n \cdot n^3 = n^5 \equiv n \pmod 5$$

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

> Let l, m, and n be arbitrary positive integers, and assume that $\gcd(l, m \cdot n) = 1$.
>
> By §3.1.5($\Leftarrow$), there exist integers i and j such that $i \cdot l + j \cdot m \cdot n = 1$. Thus, we have that
>
> $$\text{there exist integers } i \text{ and } a \text{ such that } i \cdot l + a \cdot m = 1$$
>
> and
>
> $$\text{there exist integers } i \text{ and } b \text{ such that } i \cdot l + b \cdot n = 1.$$
>
> Therefore, by §3.1.5($\Rightarrow$) one has that $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

10. Solve the following congruences:

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

> By §3.2.4, a solution will satisfy the congruence iff it satisfies ⓣ $7 \cdot x \equiv 1 \pmod{40}$ ($\gcd(40, 11) = 1$ so the modulus does not change). As 7 and 40 are coprime, this amounts to finding the multiplicative inverse of 7 in $\mathbb{Z}_{40}$ (Corollary 75), which is the second coefficient in the expression of 1 as a linear combination of 40 and 7. We run the Extended Euclid's Algorithm to find that $40 \cdot 3 + 7 \cdot (-17) = 1$. Thus, $x_0 = -17$ is a solution to ⓣ, and therefore to $77 \cdot x_0 \equiv 11 \pmod{40}$. To find the general form of solutions, we note that the linear combination of 40 and 7 is not unique (Slide 219), so x can have the general form $x = -17 + 40n \equiv 23 + 40n$ for any integer n.

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

> By §3.2.4, a solution will satisfy the congruence iff it satisfies ⓣ $2 \cdot y \equiv 5 \pmod 9$, that is, $2 \cdot y + 9 \cdot k = 5$ for some $k \in \mathbb{Z}$. Now, since 2 and 9 are coprime, we can express 1 as their linear combination, computing the coefficients using the Extended Euclid's Algorithm: $2 \cdot (-4) + 9 \cdot 1 = 1$. Multiplying both sides by 5 gives us $2 \cdot (-20) + 9 \cdot 5 = 5$, which is a solution to ⓣ with $y_0 = -20$. To generate all the solutions, we note that ⓣ is satisfied by $y_0 + 9n$ for any n, so y can have the general form $y = -20 + 9n \equiv 7 + 9n$ for any integer n.

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

To solve a system of congruences, we find the general form of solutions for the congruences individually, then find the ones that satisfy both.

All solutions to the first congruence are of the form $z_1 = 13 + 21k$ for $k \in \mathbb{Z}$.

Solutions of the congruence $3 \cdot z \equiv 2 \pmod{17}$ satisfy (†) $3 \cdot z + 17 \cdot n = 2$. Since 3 and 17 are coprime, we can express 1 as their linear combination using EEA: $3 \cdot 6 + 17 \cdot (-1) = 1$. Multiplying by 2 on both sides gives a solution to (†), and from there, we get the general form of solutions as $z_2 = 12 + 17l$ for $l \in \mathbb{Z}$.

The solutions for the congruence system will be those which are both of the form z_1 and z_2 simultaneously:

$$13 + 21 \cdot k = 12 + 17 \cdot l$$

Albeit this looks like one equation with two unknowns, we can rearrange it to the form

$$21 \cdot (-k) + 17 \cdot l = 1 \qquad (‡)$$

which we can solve using EEA, since 21 and 17 are coprime:

$$21 \cdot (-4) + 17 \cdot 5 = 1$$

Thus, (‡) has general solutions $k = 4 + 17i$ and $l = 5 + 21j$ for $i, j \in \mathbb{Z}$; at these specific values of k, the general solution $z_1 = 13 + 21 \cdot k$ for the first congruence also satisfies the second congruence (and similarly for z_2). Substituting k into z_1 or l into z_2 gives

$$z = 97 + 357i \qquad \forall i \in \mathbb{Z}.$$

which is the general form of solutions that satisfy the system of congruences.

♪ This question shows the usefulness of the characterisation of gcds via linear combinations: it allows us to solve one equation with two unknowns, as long as the RHS is a multiple of the gcd of the coefficients (so if the coefficients are coprime, the RHS can be any positive integer). Solving a congruence $ax \equiv b \pmod{m}$ amounts to characterising the integer solutions of the equation $ax - my = b$ (known as a linear Diophantine equation), which exist only if $\gcd(a, m) \mid b$.

If a congruence $ax \equiv b \pmod{m}$ has one solution x_0 (i.e. if $\gcd(a, m) \mid b$), it has an infinite number of solutions of the form $x = x_0 + pk$ for $k \in \mathbb{Z}$, all separated by a "period" p. In some cases (such as part (a)), the period coincides with the modulus, so all possible solutions can be derived from a single integer $x_0 \in \mathbb{Z}_m$. In other cases (such as part (b)) the solutions may be more "frequent" due to the period being a fraction of the modulus: $m = dp$. Then, the solutions $x_0 + pk$ can be split into d classes, all with the period m, but different initial values $x_0, x_1, \ldots x_{d-1} \in \mathbb{Z}_m$. One such class $\{\ldots, x - 2m, x - m, x, x + m, x + 2m, \ldots\}$ is often called the *congruence class of x modulo m* (denoted $\overline{x}_m$ or sometimes $[x]_m$, although this

course uses the latter notation to refer to the least positive element of $\overline{x}_m$ in $\mathbb{Z}_m$), so in essence, an infinite number of integer solutions to a congruence can be characterised by a finite number of congruence classes. With this interpretation, part (a) had only one solution $\overline{23}_{40}$, while part (b) had six:

$$\overline{7}_{54} \quad \overline{16}_{54} \quad \overline{25}_{54} \quad \overline{34}_{54} \quad \overline{43}_{54} \quad \overline{52}_{54}$$

By considering a solution to be a congruence class modulo m, we can show that a congruence $ax \equiv b \pmod{m}$ has exactly $\gcd(a, m)$ solutions if $\gcd(a, m) \mid b$, and 0 otherwise. Of course, the $d = \gcd(a, m)$ congruence classes modulo m can be combined into one congruence class modulo m/d – the two representations are equivalent, but one may be more useful in some contexts than the other. As an example, compare the phrases "every 8 hours starting at 1am" and "every day at 1am, 9am, and 5pm", and how we must use the latter form to refer to events repeating regularly several times a week because 7 prime.

Since integer solutions of a congruence are not unique, we can ask which solutions of one congruence also satisfy another – that is, solve a *system of congruences*. These are quite different from the systems of equations you are familiar with, which involve n unknowns and n independent equations, and the solution is found by expressing one variable in terms of the others and performing substitutions. Congruence systems involve only one unknown, and the individual congruences are independent constraints on this one unknown. Rather than trying to combine the congruences via substitution, we solve each of them independently, getting sets of congruence classes for each individual congruence. Then, the task is finding the common elements of the congruence classes (their intersection), which therefore must satisfy the whole system of congruences simultaneously. If the individual solutions have the form $x + pk$ and $y + ql$, the congruence classes $\overline{x}_p$ and $\overline{y}_p$ will intersect when $x + pk = y + ql$; this now becomes another linear Diophantine equation of the form $pk - ql = y - x$ that can be solved if $\gcd(p, q) \mid y - x$. The resulting integer values for k and l tell us the number of periods one needs to offset x and y by until they coincide, and since all solutions are uniformly periodic, k and l will themselves be periodic congruence classes. The general expressions can then be substituted back into either $x + pk$ or $y + ql$ to find an initial value and a larger period for the solutions that satisfy both parts of the congruence system.

As a simple example, consider the congruence classes $\overline{1}_2$, $\overline{2}_3$ and $\overline{2}_4$. The classes $\overline{1}_2$ and $\overline{2}_3$ will intersect whenever $1 + 2n = 2 + 3k$, and the linear Diophantine equation $2n - 3k = 1$ has solutions $n = 3m + 2$ and $k = 2m + 1$. What this means is that every 3rd ● starting from the second one (using 0-indexed counting) will coincide with every 2nd ■ starting from the first one, as can be seen below at step 5 (when $m = 0$) and 11 (when $m = 1$). To figure out what "every 3rd ● starting from the second one" means on the resolution of the integers, we substitute the solution for n back into $1 + 2n$, which combines the periods of "there is a solution at every 3rd circle" and "there is a circle every 2 steps" into "there is a solution every 6 steps" and similarly for the offset. Thus, the intersection of $\overline{1}_2$ and $\overline{2}_3$

will be $\overline{5}_6$. We can do a similar procedure to find the intersection of $\overline{2}_3$ and $\overline{2}_4$ to be $\overline{2}_{12}$. However, $\overline{1}_2$ and $\overline{2}_4$ will never intersect, since the Diophantine equation $2n - 4l = 1$ has no solutions – $\gcd(2,4) = 2 \nmid 1$. Congruence systems often arise from the interaction of periodic events: examples are scheduling, polyrhythms, predator-prey life cycles, etc.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$1+2n$	●		●		●		●		●		●		●	
$2+3k$		■			■			■			■			■
$2+4l$		▲				▲				▲				▲

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

We apply Corollary 75 of the notes, which states that if $\gcd(m,n) = 1$, the multiplicative inverse of $[n]_m$ is $[\mathrm{lc}_2(m,n)]_m$, where $\mathrm{lc}_2(m,n)$ is the second coefficient of the expression of 1 as a linear combination of m and n using EEC. With this, we get that:

a) $1 \cdot 7 + (-3) \cdot 2 = 1$, so $2^{-1} \equiv 4 \pmod 7$
b) $3 \cdot 40 + (-17) \cdot 7 = 1$, so $7^{-1} \equiv 23 \pmod{40}$
c) $4 \cdot 23 + (-7) \cdot 13 = 1$, so $13^{-1} \equiv 16 \pmod{23}$

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

We first establish the following lemma:

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

($\Rightarrow$) 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 §3.1.5($\Rightarrow$), $\gcd(m,n) = 1$.

($\Leftarrow$) By Corollary 75(2) of the notes.

Now, $\gcd(22^{12001}, 175) = \gcd(2^{12001} \cdot 11^{12001}, 5^2 \cdot 7)$, and since the two numbers have no prime factors in common, they must be coprime. By the above lemma, $\gcd(22^{12001}, 175) = 1$ implies that $\left[22^{12001}\right]_{175}$ has a multiplicative inverse, as required.

3.3. Optional exercises

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

Hint: For positive a and b, consider $a_0 = \frac{a}{\gcd(a,b)}$ and $b_0 = \frac{b}{\gcd(a,b)}$ so that $\gcd(a_0, b_0) = 1$, and show that $a^2 \mid b(b+a)$ implies $a_0 = 1$.

> 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.

2. Prove the converse of §1.3.1(f): For all natural numbers n and s, if there exists a natural number q such that $(2n+1)^2 \cdot s + t_n = t_q$, then s is a triangular number. (49th Putnam, 1988)

   Hint: Recall that if ⓣ $q = 2nk + n + k$ then $(2n+1)^2\, t_k + t_n = t_q$. Solving for k in ⓣ, we get that $k = \frac{q-n}{2n+1}$; so it would be enough to show that the fraction $\frac{q-n}{2n+1}$ is a natural number.

> Suggested by a 2014/15 student (who wished to remain anonymous).
>
> Assume $(2n+1)^2 s + t_n = t_q$. Then, $t_n \equiv t_q \pmod{(2n+1)^2}$; so that $n(n+1) \equiv q(q+1) \pmod{(2n+1)^2}$ and hence $(q-n)(q-n+2n+1) \equiv 0 \pmod{(2n+1)^2}$.
>
> 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 §1.3.1(f), 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.

3. Informally justify the correctness of the following alternative algorithm for computing the gcd of two positive integers:

```
let rec gcd0(m, n) = if m = n then m
                                else let p = min m n
                                     and q = max m n
                                      in gcd0(p, q - p)
```

> The partial correctness of the algorithm follows from Corollary 58(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 two 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 compon-

ents 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 forever (the sum is of two strictly positive integers but decreases at every step, so the lowest it can go is $1 + 1 = 2$, at which point $m = n$), 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).

♪ We can use induction to make this argument formal; see §4.3.1.