Discrete Mathematics

Exercises 2 – Solutions with Commentary

Marcelo Fiore Ohad Kammar Dima Szamozvancev

2. On numbers

2.1. Basic exercises

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

   a) $i \equiv i \pmod{m}$

   > By §1.2.1(b), every number divides $i - i = 0$, so $m \mid i - i$.

   b) $i \equiv j \pmod{m} \Longrightarrow j \equiv i \pmod{m}$

   > 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) $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m} \Longrightarrow i \equiv k \pmod{m}$

   > Assume $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m}$. Then, $m \mid i - j$ and $m \mid j - k$. Hence, by §1.2.6(a), $m \mid (i - j) + j - k = i - k$ and thus $i \equiv k \pmod{m}$.

   > ♪ When working with congruence, we have three layers of definitions: $i \equiv j \pmod{m}$, defined as $m \mid i - j$, defined as $\exists k \in \mathbb{Z}.\ i - j = k \cdot m$. To prove fundamental properties about congruence (symmetry or transitivity), we usually need to go "down a level" and reason about divisibility. At this level, we may be able to use known properties of divisibility, such as in part (c); other times it may be easier to go further down, and talk about the primitive definition of divisibility, such as in part (b). In the second case we are essentially proving a lemma about divisibility "inline": that $d \mid m$ implies $d \mid -m$. Alternatively, we may notice that this property follows as a direct corollary of §1.2.6(b), with the multiplicative constant $k = -1$. The statement we prove is valid either way, but in some cases writing a quick inline proof may be easier or harder than finding if it is an instance of some existing property.

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

   a) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \Longrightarrow i + k \equiv j + l \pmod{m}$

   > Assume $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m}$. Then, $m \mid i - j$ and $m \mid k - l$. Hence, by §1.2.6(a), $m \mid (i - j) + (k - l) = (i + k) - (j + l)$ and $i + k \equiv j + l \pmod{m}$.

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

   > Assume $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m}$. Then, $m \mid (i - j)$ and $m \mid (k - l)$. By §1.2.6(b),

$m \mid i \cdot (k-l)$ and $m \mid l \cdot (i-j)$; and, by §1.2.6(a), $m \mid i \cdot (k-l) + l \cdot (i-j) = i \cdot k - j \cdot l$. Hence, $i \cdot k \equiv j \cdot l \pmod{m}$.

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

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.

♪ If you're familiar with it, you may be screaming "induction!" – indeed, a formal proof requires the mathematical Principle of Induction, which will be studied later in the course.

♪ These properties of congruence are fairly simple to state and prove, but combined with the previous exercise they form the basis of equational proofs about congruence. They allow us to extend a congruence between two integers into a congruence between two algebraic (polynomial) expressions of arbitrary nesting which differ in those two integers. For example, if we know that $i \equiv j \pmod{m}$, we also know $(3i^2 + 5i - 7)^4 \equiv (3j^2 + 5j - 7)^4 \pmod{m}$ by repeatedly applying the properties proved in this exercise: $i \equiv j \pmod{m}$ implies $i^2 \equiv j^2 \pmod{m}$ implies $3i^2 \equiv 3j^2 \pmod{m}$ and so on. This is really helpful in equational proofs in modular arithmetic, because we can rewrite parts of an expression not only if they are equal, but also when they are merely congruent. We will see examples of this shortly.

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

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

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 that

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

♪ The Division Theorem may seem like a dramatic name for a fairly obvious and unremarkable statement: that numbers can be divided with a remainder. But, in fact, the theorem is quite powerful and allows one to prove properties surprisingly easily. Let's remind ourselves of the full statement:

For every natural number m and positive natural number n, there exists a unique pair of integers q and r such that $0 \leq q$, $0 \leq r < n$, and $m = q \cdot n + r$.

This is a *unique existence* statement, a form very common in mathematics. The associated proof technique relies both on the existence and uniqueness components. To highlight the former, consider the following alternative statement of the Division Theorem:

Given any natural number m and for any choice of positive integer n, we can write m as $m = q \cdot n + r$ where q and r are unique integers satisfying $0 \leq q$ and $0 \leq r < n$.

This form emphasises the fact that if we have a natural number m, we can choose *any* natural number n, and the theorem guarantees that it's possible to write m in terms of n in the specific form $m = q \cdot n + r$ for two unique naturals satisfying $0 \leq q$ and $0 \leq r < n$. In essence, we get immediate "access" to two naturals q and r and two new assumptions about these naturals, as well as their uniqueness proofs.

Since q and r are uniquely determined by m and n, we can write them as $\mathrm{quo}(m, n)$ and $\mathrm{rem}(m, n)$ as if quo and rem were functions. In reality, they are just shorthands for "the natural q (resp. r) determined from m and n by the Division Theorem". With these, you can succinctly state the Division Theorem as

Any natural number m can be expressed as $m = \mathrm{quo}(m, n) \cdot n + \mathrm{rem}(m, n)$ for any choice of positive integer n, with $\mathrm{quo}(m, n), \mathrm{rem}(m, n) \in \mathbb{N}$ and $\mathrm{rem}(m, n) < n$.

You may well ask "why go through all this when we have the integer division and remainder operators"? Well, we haven't formally defined them yet (and one way to define them formally is precisely via quo and rem!), but even ignoring that, proofs using uniqueness wouldn't really work if we just treated rem and quo as operators. To see how this works, let's expand the solution to the question above.

We are required to show that for all natural numbers k, l and positive integers m, $\mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m)$ – any multiple of m can be cancelled out in a remainder by m. If we think of rem as the remainder operator (e.g. % in Java), this seems obvious – but other than spelling out the details of division as repeated subtraction (the Division Algorithm), it's quite tricky to prove! Instead, as we said above, $\mathrm{rem}(l, m)$ should be treated as "the unique r determined by l and m by the Division Theorem". This is where uniqueness comes in: we know that for any other expansion $l = \mathrm{quo}(l, m) \cdot m + r'$ with $r' < m$, r' *must* be equal to $\mathrm{rem}(l, m)$. Thus, equality of remainders can be derived from showing that they satisfy the same property: that they can appear in the same expansion of l (via m) and are both strictly less than m.

The question is exactly a proof of equality of two remainders: $\mathrm{rem}(k \cdot m + l, m)$ and $\mathrm{rem}(l, m)$. If we show that they appear in two "different" expansions of the same natural number, they must be equal. What expansion would $\mathrm{rem}(l, m)$ appear in? Easy: the Division Theorem tells us that l can always be rewritten in terms of m as

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

Similarly, $\mathrm{rem}(k \cdot m + l, m)$ appears in the expansion

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

All we did is apply the streamlined form of the Division Theorem, expanding both l and $k \cdot m + l$ in terms of m. They can't directly be compared yet, because they are expansions of different naturals. To resolve that, we just add $k \cdot m$ to the first equation and factorise to get:

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

And with that, we are done! How? Well, we have two different expansions of the number $k \cdot m + l$: it's equal both to

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

where both $\mathrm{rem}(k \cdot m + l, m)$ and $\mathrm{rem}(l, m)$ are less than m. But the Division Theorem tells us that there is exactly one such expansion of $k \cdot m + l$ possible, so these two remainders *cannot* be different! That is to say,

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

which was precisely our proof goal.

Such surprising and abrupt conclusions are very much characteristic of proofs by *universal properties*: rather than proving equality directly, we show that both remainders satisfy the universal property (specified by the Division Theorem) of the same number $k \cdot m + l$ and therefore must be equal. We will see a lot of examples of this in the course and the exercises: while many statements can be proved by alternative means, proofs by universal properties are often remarkably compact and elegant, achieving the same goal with only a few clever reasoning steps.

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

Because

$$\begin{aligned} \mathrm{rem}(k + l, m) &= \mathrm{rem}\big(\mathrm{quo}(k, m) \cdot m + \mathrm{rem}(k, m) + l, m\big) && \text{(by DT on } k \text{ with } m\text{)} \\ &= \mathrm{rem}\big(\mathrm{rem}(k, m) + l, m\big) && \text{(by §2.1.3(a))} \end{aligned}$$

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

♪ The previous property of remainders is quite useful, especially in combination with the Division Theorem: since we have a choice of expanding k in terms of any positive integer, we can choose m to then ensure that the term $\mathrm{quo}(k, m) \cdot m$ – being a multiple of m – can be cancelled out.

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

Because

$$\begin{aligned}\operatorname{rem}(k \cdot l, m) &= \operatorname{rem}\big(k \cdot \operatorname{quo}(l, m) \cdot m + k \cdot \operatorname{rem}(l, m), m\big) && \text{(by DT on } l \text{ with } m\text{)}\\ &= \operatorname{rem}\big(k \cdot \operatorname{rem}(l, m), m\big) && \text{(by §2.1.3(a))}\end{aligned}$$

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

♪ Once again, we start by expanding a natural in terms of m, then use part §2.1.3(a) to cancel the whole term. In this case, we choose l: this was guided by the need to end up with a $\operatorname{rem}(l, m)$, which we wouldn't get by expanding k.

4. Let m be a positive integer.

   a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is:

$$\forall i, j, k \in \mathbb{Z}_m.\ (i +_m j) +_m k = i +_m (j +_m k) \quad \text{and} \quad (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$$

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

$$\begin{aligned}(i +_m j) +_m k &= \big[[i + j]_m + k\big]_m && \text{(by definition of } +_m\text{)}\\ &= \operatorname{rem}\big(\operatorname{rem}(i + j, m) + k, m\big) && \text{(by definition of } [\cdot]_m\text{)}\\ &= \operatorname{rem}\big((i + j) + k, m\big) && \text{(by §2.1.3(b))}\\ &= \operatorname{rem}\big(i + (j + k), m\big) && \text{(by associativity of addition)}\\ &= \operatorname{rem}\big(i + \operatorname{rem}(j + k, m), m\big) && \text{(by §2.1.3(b))}\\ &= \big[i + [j + k]_m\big]_m && \text{(by definition of } [\cdot]_m\text{)}\\ &= i +_m (j +_m k) && \text{(by definition of } +_m\text{)}\end{aligned}$$

Similarly, consider arbitrary i, j, k in $\mathbb{Z}_m$, and calculate as follows:

$$\begin{aligned}(i \cdot_m j) \cdot_m k &= \big[[i \cdot j]_m \cdot k\big]_m && \text{(by definition of } \cdot_m\text{)}\\ &= \operatorname{rem}\big(\operatorname{rem}(i \cdot j, m) \cdot k, m\big) && \text{(by definition of } [\cdot]_m\text{)}\\ &= \operatorname{rem}\big((i \cdot j) \cdot k, m\big) && \text{(by §2.1.3(c))}\\ &= \operatorname{rem}\big(i \cdot (j \cdot k), m\big) && \text{(by associativity of multiplication)}\\ &= \operatorname{rem}\big(i \cdot \operatorname{rem}(j \cdot k, m), m\big) && \text{(by §2.1.3(c))}\\ &= \big[i \cdot [j \cdot k]_m\big]_m && \text{(by definition of } [\cdot]_m\text{)}\\ &= i \cdot_m (j \cdot_m k) && \text{(by definition of } \cdot_m\text{)}\end{aligned}$$

♪ When defining something in terms of an existing construction, its properties will often directly follow from the known properties of the underlying definition. In this case, associativity of $+_m$ relies on the associativity of $+$ in terms of which $+_m$ is defined. However, we needed a lemma about addition and remainders to simplify the expressions until we can directly appeal to the associativity of $+$.

♪ These are examples of *equational proofs*, a very common and useful technique for mathematical reasoning, generalising the algebraic calculations you are familiar with from school. Whenever we need to prove equality or equivalence of two mathematical objects (numbers, sets, functions, etc.), we can build it up as a chain of equalities, each rewriting some part of the expression via some known property, definition, or lemma. There's often a symmetry in the proofs, nicely showcased in this exercise: the first half unwraps several layers of definitions and simplifies the resulting expressions; the second half does the same in reverse. Indeed, it's often helpful to write equational proofs starting from both ends, until they meet in the middle.

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

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

$$l \equiv [l]_m \pmod{m} \text{ for all } l \in \mathbb{Z}$$

one has that

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

♪ This is an example of a *congruence proof*: a weaker form of an equational proof where some of the steps are not strict equalities, but congruences modulo $m \in \mathbb{Z}^+$. Since congruence is a so-called *equivalence relation* (it's reflexive, symmetric, and transitive, all proved in §2.1.1), a chain of congruences establishes a congruence between the endpoints. Reflexivity allows us to strengthen some of the congruences into equalities: in the example above, $k +_m [-k]_m = \big[k + [-k]_m\big]_m$ is a strict equality, since it is the definition of $+_m$. Importantly, all congruences must be modulo the same $m \in \mathbb{Z}^+$, which is denoted at the end of the proof, ranging over the entire chain of congruences.

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.

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 the analogous criterion for multiples of 9 and a similar condition for multiples of 11.

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

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

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

The above follow from the following stronger statements

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

The rule for 3 uses the fact that $10 \equiv 1 \pmod{3}$, which, by the exponentiation property shown in §2.1.2(c), implies $10^l \equiv 1 \pmod{3}$ for all $l \in \mathbb{Z}^+$. This can be applied in every term of the sum (since congruences can be applied within sums and products as shown in §2.1.2, reducing the 10^l coefficients to 1. The technique works the same for divisibility by 9, since $10 \equiv 1 \pmod{9}$; for 11, we notice that $10^{2n} \equiv 1 \pmod{11}$, but $10^{2n+1} \equiv 10 \equiv -1 \pmod{11}$ for all $n \in \mathbb{N}$.

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

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

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,

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

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,

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

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.

> This is Lemma 26 of the notes.
>
> ♪ The question here refers to the "intuitive" notions of division and remainder, but by recognising their connection to congruence we can refer to the known number-theoretic properties of modular arithmetic.

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

> $\mathrm{rem}(55^2, 79) = 23$, $\mathrm{rem}(23^2, 79) = 55$, $\mathrm{rem}(23 \cdot 55, 79) = 1$, and
>
> $$\begin{aligned} \mathrm{rem}\big((55^2)^{39}, 79\big) &= \mathrm{rem}\big(23 \cdot (23^2)^{19}, 79\big) &&= \mathrm{rem}\big(23 \cdot 55 \cdot (55^2)^9, 79\big) \\ &= \mathrm{rem}\big(23 \cdot (23^2)^4, 79\big) &&= \mathrm{rem}\big(23 \cdot (55^2)^2, 79\big) \\ &= \mathrm{rem}\big(23 \cdot 23^2, 79\big) &&= \mathrm{rem}(23 \cdot 55, 79) \\ &= 1 \end{aligned}$$
>
> Of course, since we know the last one from Fermat's Little Theorem, there was really no need to calculate it!

5. Calculate that $2^{153} \equiv 53 \pmod{153}$. At first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though? *Hint:* Simplify the problem by applying known congruences to subexpressions using the properties in §2.1.2.

> One possible sequence of steps, using the fact that $153 = 2^7 + 25$:
>
> $$\begin{aligned} & 2^{153} = 2^6 \cdot \left(2^7\right)^{21} = 2^6 \cdot 2^7 \cdot \left(2^7\right)^{20} \\ \equiv\ & 2^6 \cdot (-25) \cdot (-25)^{20} = 2^6 \cdot (-25) \cdot \left(25^2\right)^{10} = 2^6 \cdot (-25) \cdot 625^{10} \\ \equiv\ & 2^6 \cdot (-25) \cdot (13^2)^5 = 2^6 \cdot (-25) \cdot 169^5 \\ \equiv\ & (-25) \cdot 2^6 \cdot 16^5 = (-25) \cdot 2^6 \cdot \left(2^4\right)^5 = (-25) \cdot 2^5 \cdot (2^7)^3 \\ \equiv\ & (-25) \cdot 2^5 \cdot (-25) \cdot 25^2 = 2^5 \cdot (25^2)^2 \\ \equiv\ & 2^5 \cdot 13^2 \equiv 2^5 \cdot 16 = 2^2 \cdot 2^7 \equiv 4 \cdot (-25) \\ & \equiv 53 \pmod{153} \end{aligned}$$
>
> This doesn't contradict Fermat's Little Theorem, since $153 = 3^2 \cdot 17$ is composite.
>
> ♪ This may seem like a daunting exercise, but we actually didn't need to do anything more complicated than squaring and addition. The key is being able to make impactful simplifications using congruence: as soon as we have a number greater than 153, we can replace it with the remainder after dividing by 153.

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

- $\mathbb{Z}_3$

$+$	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

♪ Great demonstration of the property that every element of $\mathbb{Z}_p$ has a multiplicative inverse if p is a prime. Algebraically, this makes $\mathbb{Z}_p$ a *field*: a place where you can do division.

7. 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.

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

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

♪ When the question involves prime numbers, you should expect to require properties and theorems specific to primes. In this course – which is only an introduction to number theory – this will quite often be Fermat's Little Theorem.

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

We can proceed by case analysis: 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 $n \equiv 5 \pmod 6$: $n^3 \equiv 5^3 = 125 \equiv 5 \equiv n \pmod 6$.

Of course, this wouldn't really work for larger moduli – see next question. A more elegant solution is proving $6 \mid n^3 - n$, which, by the well-known divisibility rule for 6, follows from showing $3 \mid n^3 - n$ and $2 \mid n^3 - n$. Now,

$$n^3 - n = n \cdot (n^2 - 1) = (n-1) \cdot n \cdot (n+1);$$

but this is a product of three consecutive integers, so at least one of them must be even and one must be divisible by 3. That is, $n^3 - n = 2 \cdot 3 \cdot k$ for some $k \in \mathbb{Z}$, so $n^3 \equiv n \pmod 6$.

Yet another approach is formally establishing the lemma (which can be seen as the generalisation of the divisibility rule of 6):

$$\big(a \equiv b \pmod 2 \wedge a \equiv b \pmod 3\big) \iff a \equiv b \pmod 6$$

In one direction, we have that $a = 2k + b = 3l + b$, so $2k = 3l$ for integers k and l; since $3l$ must be even and 3 is odd, l must itself be even: $l = 2m$ for some $m \in \mathbb{Z}$. Substituting back, we have $a = 3 \cdot 2m + b$, so $a - b = 6m$. In the opposite direction, $a - b = 6k = 2 \cdot 3 \cdot k$, which immediately implies $2 \mid a - b$ and $3 \mid a - b$.

Now, it is sufficient to prove that $n^3 \equiv n \pmod 2$ and $n^3 \equiv n \pmod 3$. The latter is a direct instance of Fermat's Little Theorem for the prime 3; the former holds by the congruence chain $n^3 \equiv n^2 \equiv n \pmod 2$, with both steps using Fermat's Little Theorem $n^2 \equiv n \pmod 2$, multiplied by n in the first step using the product property of §2.1.2.

♪ There are usually many ways of approaching a proof, ranging from "brute force" methods to elegant and concise number-theoretic arguments. It doesn't technically matter what you do as long as the proof is correct – but just like how "working" code doesn't always mean "neat and readable" code, you should strive to make your proofs as streamlined as possible. It's also very useful to practice recognising patterns and realising where some known lemma or property can be applied, since they often end up doing the bulk of the work: you shouldn't need to reprove a specific case of a known, more general statement.

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

An exhaustive case analysis would be impractical in this case. Instead, we adapt our more conceptual solutions above.

First, we use a very similar proof as above for the lemma

$$\big(a \equiv b \pmod 6 \wedge a \equiv b \pmod 7\big) \iff a \equiv b \pmod{42}$$

(notice how the crucial step is $6k = 7l$ implying that $6 \mid l$, because $6 \nmid 7$ – the lemma wouldn't hold for non-coprime numbers (see §1.2.5). Another trick in this case is recognising that $a - b = 7(a-b) - 6(a-b)$, and, since by assumption $a - b = 6k = 7l$, we have $a - b = 7 \cdot 6k - 6 \cdot 7l = 42 \cdot (k - l)$.

Now, $n^7 \equiv n \pmod 7$ holds by Fermat's Little Theorem. To show $n^7 \equiv n \pmod 6$, we can equivalently show $n^7 \equiv n \pmod 2$ and $n^7 \equiv n \pmod 3$; both follow by repeated applications of Fermat's Little Theorem.

2.3. Optional 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 $n \equiv 3 \pmod 4$.

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

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

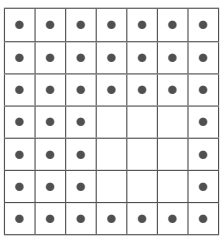
We therefore have four cases:

- $i^2 \equiv 0 \pmod 4$ 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 (as long as it's congruent to 0, 1 or 3 modulo 4) in a square grid leaving an empty square sub-grid, for instance as follows (for $i = 7$, $j = 3$, and $n = 40$):



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 $\mathrm{rem}(n, 4) = n - \mathrm{quo}(n, 4) \cdot 4$ (by the Division Theorem), it follows that $\mathrm{rem}(n, 4)$ is even and since hence it is 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 $n = i^2 - j^2$. (Note that this argument slightly generalises that of Proposition 22 of the notes.)

  Graphically, we are in the following kind of situation:

$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$							$\bullet_3$
$\bullet_1$	$\bullet_4$	$\bullet_4$	$\bullet_4$	$\bullet_4$	$\bullet_4$	$\bullet_4$	$\bullet_4$

- 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:

$\bullet$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$	$\bullet_2$
$\bullet_1$						
$\bullet_1$						
$\bullet_1$						
$\bullet_1$						
$\bullet_1$						
$\bullet_1$						

♪ Graphical proofs are great for intuition: so called "proofs without words" are often as illuminating as they are beautiful. However, they are not (usually) a substitute for a formal proof by logical reasoning, especially if the proposition to be shown is more general than what could be encoded graphically. In this case, the statement is about all *integers* n, while the graphical proof can only work for a *natural number* n.

2. 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?

   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 a square, and that the same holds for binary repunits. Is this the case for every base? *Hint*: Use Lemma 27 of the notes.

   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.

   Incidentally, the calculation above already contains the proof of the property for binary repunits, since they are of the form $n = \sum_{i=0}^{l} 2^i$

   The statement:

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

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