2 *Modular Arithmetic*

Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the modulus. The 12-hour clock—the time convention in which the day is divided into two 12-hour periods—is probably the most familiar example.

The modern approach to modular arithmetic was developed by Carl Friedrich Gauss (1777–1855) in his book *Disquisitiones Arithmeticae* published in 1801.

2.0 Equivalence Relations

What does it mean for two mathematical objects to be the same? One of the foundational concepts in mathematics is that of an equivalence relation on a set.

The history of equivalence in mathematics is surprisingly long and complicated; for example, see Amir Asghari, Equivalence: an attempt at a history of the idea, *Synthese* **196** (2019) 4657–4677.

Let $\mathcal{X}$ be a set. The *cartesian product* $\mathcal{X}\times\mathcal{X}$ consists of all ordered pairs (x, y) of elements $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. A *binary relation* on $\mathcal{X}$ is any subset $\mathcal{R} \subseteq \mathcal{X}\times\mathcal{X}$. One kind of relation is especially interesting.

Definition 2.0.1. An *equivalence relation* on a set $\mathcal{X}$ is a binary relation $\mathcal{R}$ on $\mathcal{X}$ that has the following three properties.

(Reflexive) For any x in $\mathcal{X}$, the pair (x, x) is in $\mathcal{R}$.
(Symmetric) For any (x, y) in $\mathcal{R}$, the pair (y, x) is in $\mathcal{R}$.
(Transitive) For any (x, y) and (y, z) in $\mathcal{R}$, the pair (x, z) is in $\mathcal{R}$.

For any equivalence relation $\mathcal{R}$, we write $(x, y) \in \mathcal{R}$ as $x \sim y$.

Equality of elements is the prototype. In fact, equality is the only relation that is reflexive, symmetric, and antisymmetric.

Remark 2.0.2. Lemma 1.0.1 shows that the relation $\simeq$ on $\mathbb{N} \times \mathbb{N}$, used to define the set $\mathbb{Z}$ of integers, is an equivalence relation.

Problem 2.0.3. For any set $\mathcal{X}$, verify that the subset $\mathcal{R} := \mathcal{X} \times \mathcal{X}$ is an equivalent relation.

The largest equivalence relation.

Solution. Since $\mathcal{R}$ contains all pairs, reflexivity, symmetry, and transitivity follow immediately. □

Problem 2.0.4. For any set $\mathcal{X}$, confirm that the diagonal subset $\mathcal{R} := \{(x, y) \in \mathcal{X} \times \mathcal{X} \mid x = y\}$ is an equivalent relation.

The smallest equivalence relation.

Solution. Since $x = x$ for any $x \in \mathcal{X}$, reflexivity follows. Symmetry and transitivity follow from the same properties for equality. □

Problem 2.0.5. The *parity* relation on the integers is defined, for any two integers m and n, by $m \sim n$ if the difference $m - n$ is divisible by 2. Show that $\sim$ is an equivalence relation.

Solution. Since $m - m = 0$ is divisible by 2, reflexivity follows. When $m - n$ is divisible by 2, there exists an integer j such that $m - n = 2j$. It follows that $n - m = 2(-j)$ and $n - m$ is divisible by 2, so parity is symmetric. When $k - m$ and $m - n$ are divisibile by 2, there are integers i and j such that $k - m = 2i$ and $m - n = 2j$. We obtain $k - n = (k - m) + (m - n) = 2i + 2j = 2(i + j)$, so $k - n$ is divisible by 2 and parity is transitive. □

A binary relation may satisfy any two of the defining properties for an equivalence relation but fail to satisfy the third.

Remark 2.0.6.

- The weak inequality relation $\leqslant$ on integers is not an equivalence relation. It is reflexive and transitive, but not symmetric. For instance, we have $2 \leqslant 3$ and $3 \nleqslant 2$.
- The relation $\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid \gcd(m, n) > 1\}$ is reflexive and symmetric, but not transitive. Indeed, we have $\gcd(2, 6) = 2 > 1$, $\gcd(6, 3) = 3 > 1$, and $\gcd(2, 3) = 1$.
- The empty relation $\varnothing$ on a set $\mathcal{X}$ is vacuously symmetric and transitive. It is not reflexive unless $\mathcal{X} = \varnothing$.

Definition 2.0.7. Let $\sim$ be an equivalence relation on a set $\mathcal{X}$. For any $x \in \mathcal{X}$, the set $[x] := \{w \in \mathcal{X} \mid x \sim w\}$ is the *equivalence class* of x.

Remark 2.0.8. For parity on $\mathbb{Z}$, the two equivalence classes are $[0] = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ and $[1] = \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\}$.

The integers in the parity class $[0]$ are *even* whereas those in $[1]$ are *odd*.

Proposition 2.0.9. *For any equivalence relation on the set $\mathcal{X}$, the set $\mathcal{P}$ of equivalence classes have the following three properties:*

- *The family $\mathcal{P}$ does not contain the empty set: $\varnothing \notin \mathcal{P}$.*
- *The union of the sets in $\mathcal{P}$ is equal to $\mathcal{X}$: $\bigcup_{\mathcal{A} \in \mathcal{P}} \mathcal{A} = \mathcal{X}$.*
- *The intersection of any two distinct sets in $\mathcal{P}$ is empty: for any two set $\mathcal{A}$ and $\mathcal{B}$ in $\mathcal{B}$, the relation $\mathcal{A} \neq \mathcal{B}$ implies that $\mathcal{A} \cap \mathcal{B} = \varnothing$.*

In other words, the equivalence classes form a partition *of the set X.*

Proof. For any $x \in \mathcal{X}$, reflexivity means $x \sim x$, so $x \in [x]$. Hence, we see that the empty set is not an equivalence class and the union of the equivalence classes equals $\mathcal{X}$. For any elements x and y in $\mathcal{X}$, symmetry shows that $y \in [x]$ implies that $x \in [y]$. For any elements x, y, and z in $\mathcal{X}$, transitivity asserts that $y \in [x]$ and $z \in [y]$ implies that $z \in [x]$. It follows that any two equivalence classes are either equal or disjoint. □

Definition 2.0.10. For any equivalent relation $\sim$ on the set $\mathcal{X}$, the *quotient set*, denoted by $\mathcal{X}/\!\sim$, is the set of equivalence classes. The *canonical map* $\pi \colon \mathcal{X} \to \mathcal{X}/\!\sim$ is defined, for all $x \in \mathcal{X}$, by $\pi(x) = [x]$.

A map $\varphi \colon \mathcal{X} \to \mathcal{Y}$ determines a *well-defined* map $\overline{\varphi} \colon \mathcal{X}/\!\sim \to \mathcal{Y}$ if, for all elements x and y in $\mathcal{X}$, the relation $[x] = [y]$ implies that $\varphi(x) = \varphi(y)$. In other words, the output of φ does not depend on the choice of representatives.

By construction, the canonical map $\pi \colon \mathcal{X} \to \mathcal{X}/\!\sim$ is surjective.

When $\varphi \colon \mathcal{X} \to \mathcal{Y}$ is well-defined, we have $\varphi = \overline{\varphi}\,\pi$. We visualize this property via the commutative diagram:

$$\begin{tikzcd} \mathcal{X} \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathcal{Y} \\ \mathcal{X}/\!\sim \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

Exercises

Problem 2.0.11. Define a binary relation on the set $\mathbb{R}$ of real numbers as follows: for any two real numbers x and y, we have $x \sim y$ if there is an integer k such that $x - y = 2\,k\,\pi$. Verify that this is an equivalence relation. Describe the set of equivalence classes. Are addition and multiplication well-defined on the quotient set $\mathbb{R}/\!\sim$?

2.1 Congruence

How do we generalize the parity relation to divisibility by any non-negative integer? The basic notion is remarkable straightforward.

Definition 2.1.1. Let ℓ be a nonnegative integers. Two integers m and n are *congruent modulo* ℓ, denoted by $m \equiv n \mod \ell$, if the difference $m - n$ is divisible by ℓ. The number ℓ is the *modulus*.

Congruence modulo 0 is simply the relation =.

Lemma 2.1.2. *For any nonnegative integer ℓ, congruence modulo ℓ is an equivalence relation on the set $\mathbb{Z}$ of integers.*

Proof. Let k, m, and n be integers.

- Since $m - m = 0 = (0)\,\ell$, we have $m \equiv m \mod \ell$ and the congruence relation is reflexive.
- Suppose that $m \equiv n \mod \ell$. Since $m - n$ is divisible by ℓ, there exist an integer j such that $m - n = j\,\ell$. We have $n - m = (-j)\,\ell$, so $n - m$ is also divisible by ℓ. We deduce that $n \equiv m \mod \ell$ and congruence relation is symmetric.
- Suppose that $k \equiv m \mod \ell$ and $m \equiv n \mod \ell$. When $k - m$ and $m - n$ are divisible by ℓ, there exists integers i and j such that $k - m = i\,\ell$ and $m - n = j\,\ell$. It follows that
$$k - n = (k - m) + (m - n) = i\,\ell + j\,\ell = (i + j)\ell\,,$$
so $k - n$ is also divisible by ℓ. We conclude that $k \equiv n \mod \ell$ and congruence relation is transitive. □

Notation 2.1.3. For any nonnegative integer ℓ, the congruence classes modulo ℓ are
$$\begin{aligned}[m]_\ell &:= \{n \in \mathbb{Z} \mid m \equiv n \mod \ell\} \\ &= \{m \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } m - n = k\,\ell\} \\ &= \{m + k\,\ell \mid k \in \mathbb{Z}\}\,.\end{aligned}$$
It follows that $[m]_\ell = [n]_\ell$ if and only if $m \equiv n \mod \ell$. For any nonnegative integer ℓ, the set of congruence classes modulo ℓ is denoted by $\mathbb{Z}/\langle \ell \rangle := \mathbb{Z}/\equiv$.

Other popular notations are $\mathbb{Z}/\ell$ and $\mathbb{Z}/\ell\mathbb{Z}$. Although the notation $\mathbb{Z}_\ell$ is unfortunately used by some, it conflicts with the standard notation for another important concept.

Remark 2.1.4. When $\ell = 3$, there are three congruence classes:
$$\begin{aligned}[0]_3 &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = \{0 + 3k \mid k \in \mathbb{Z}\}\,, \\ [1]_3 &= \{\dots, -8, -5, -2, 0, 1, 4, 7, \dots\} = \{1 + 3k \mid k \in \mathbb{Z}\}\,, \\ [2]_3 &= \{\dots, -7, -4, -1, 0, 2, 5, 8, \dots\} = \{2 + 3k \mid k \in \mathbb{Z}\}\,.\end{aligned}$$

Proposition 2.1.5. *Let ℓ be a positive integer. For any integer m, we have $[m]_\ell = [m \,\%\, \ell]_\ell$. Moreover, the set $\mathbb{Z}/\langle \ell \rangle$ consists of exactly the ℓ elements $[0]_\ell, [1]_\ell, [2]_\ell, \dots, [\ell - 1]_\ell$.*

Proof. By division with remainder, there exists integers q and r such that $m = q\,\ell + r$, $0 \leqslant r < \ell$, and $r = m \,\%\, \ell$. Since $m - r = q\,\ell$, we see that $m \equiv r \mod \ell$ or $[m]_\ell = [r]_\ell$.

We claim the that classes $[0]_\ell, [1]_\ell, [2]_\ell, \dots, [\ell - 1]_\ell$ are distinct. Suppose that r and s are integers such that $0 \leqslant r < \ell$, $0 \leqslant s < \ell$, and $[r]_\ell = [s]_\ell$. The inequalities give $0 \leqslant |r-s| < \ell$. The equality implies that $|r-s|$ is divisible by ℓ. Assuming $|r-s| \neq 0$, we would have $\ell \leqslant |r-s| < \ell$ which is a contradiction. Therefore, we deduce that $|r-s| = 0$ and $r = s$.

Lastly, the first part demonstrates that every congruence class equals a listed one. The claim shows that no two of these congruence classes coincide. □

Remark 2.1.6. Given an equivalence relation on a set $\mathcal{X}$, a *system of distinct representatives* or *transversal* is a subset of $\mathcal{X}$ having exactly one element from each equivalence class. Proposition 2.1.5 shows that the subset $\{0, 1, 2, \dots, \ell - 1\} \subset \mathbb{Z}$ is a transversal for congruence modulo ℓ. This is only one of infinitely many viable transversals. Another choice that is more symmetric about 0 is
$$\{-\lfloor (\ell-1)/2 \rfloor, \dots, -1, 0, 1, 2, \dots, \lfloor \ell/2 \rfloor\}.$$

The choice of a transversal produces a *lifting map* $\lambda \colon (\mathcal{X}/\!\sim) \to \mathcal{X}$ defined by $\lambda([x]) := x$. Any lifting map is a one-sided inverse of the canonical map $\pi \colon \mathcal{X} \to \mathcal{X}/\!\sim$ meaning $\pi\,\lambda = \mathrm{id}_{\mathcal{X}/\sim}$.

To do algebra in $\mathbb{Z}/\langle \ell \rangle$, we equipe this quotient set with addition and multiplication.

Lemma 2.1.7. *Let ℓ be a nonnegative integer and let j, k, m, and n be integers. When $j \equiv k \mod \ell$ and $m \equiv n \mod \ell$, we have*
$$j + m \equiv k + n \mod \ell \qquad \textit{and} \qquad j\,m \equiv k\,n \mod \ell\,.$$

Proof. Since $j \equiv k \mod \ell$ and $m \equiv n \mod \ell$, there exists integers u and v such that $j - k = u\,\ell$ and $m - n = v\,\ell$. It follows that
$$(j+m) - (k+n) = (j-k) + (m-n) = u\,\ell + v\,\ell = (u+v)\,\ell$$
$$\begin{aligned}(j\,m) - (k\,n) &= (k + u\,\ell)(n + v\,\ell) - (k\,\ell) \\ &= k\,v\,\ell + n\,u\,\ell + u\,v\,\ell^2 = (k\,v + n\,u + u\,v\,\ell)\ell\,.\end{aligned}$$
We conclude that ℓ divides $(j+m) - (k+n)$ and $(j\,m) - (k\,n)$, so $j + m \equiv k + n \mod \ell$ and $j\,m \equiv k\,n \mod \ell$. □

The lemma proves that congruence classes for the addition and the multiplication of integers is independent of the choice of representatives, so the quotient set $\mathbb{Z}/\langle \ell \rangle$ inherits these operations from $\mathbb{Z}$. More formally, we make the following two definitions.

Definition 2.1.8. Let ℓ be a nonnegative integer. For any two elements $[m]_\ell$ and $[n]_\ell$ in $\mathbb{Z}/\langle \ell \rangle$, we define
$$[m]_\ell + [n]_\ell := [m+n]_\ell \qquad \text{and} \qquad [m]_\ell\,[n]_\ell := [m\,n]_\ell\,.$$

Addition and multiplication on the right side are the familiar operations on the set $\mathbb{Z}$ of integers whereas the addition and multiplication on the left side are new operations.

Problem 2.1.9. Simplify 11^3 modulo 13.

Solution. We have
$$11^3 = (11)(11)(11) \equiv (-2)(-2)(-2) \equiv -8 \equiv 5 \mod 13\,.$$ □

Addition is not well-defined for all quotients sets.

Remark 2.1.10. For two integers, 'having the same sign' is an equivalence relation with two classes: $[-1] = \{\dots, -3, -2, -1\}$ and $[1] = \{0, 1, 2, \dots\}$. In this case, addition does depend on the choice of representatives. For instance, we have
$$(-1) + (1) = (-1+1) = 0 \qquad (-4) + (1) = (-4+1) = -3$$
but $[-1] = [-4]$ and $[0] = [1] \neq [-1] = [-3]$.

Exercises

Problem 2.1.11. Let m be an integer. Confirm that

$$m^2 \equiv 0 \text{ or } 1 \mod 3 \qquad \text{and} \qquad m^2 \equiv 0 \text{ or } 4 \mod 5\,.$$

Problem 2.1.12. Let p be a prime integer such that $p \geqslant 5$. Prove that $p^2 + 2$ is reducible (also known as composite).

Problem 2.1.13. Prove that there are infinitely many primes of the form $4\,k + 3$ for some nonnegative integer k.

2.2 Multiplicative Inverses in $\mathbb{Z}/\langle \ell \rangle$

Which properties does the quotient set $\mathbb{Z}/\langle \ell \rangle$ inherit from the set $\mathbb{Z}$ of integers? Although $\mathbb{Z}/\langle \ell \rangle$ acquires many features from the integers, it does have some new traits. We first enumerate the major common attributes.

Theorem 2.2.1. *Let ℓ be a nonnegative integer. For any elements u, v, and w in the quotient set $\mathbb{Z}/\langle \ell \rangle$, we have following eight properties:*

$$\begin{aligned}
(u + v) + w &= u + (v + w) && \text{(associativity of addition)} \\
v + w &= w + v && \text{(commutativity of addition)} \\
v + 0 &= v && \text{(existence of additive identity)} \\
v + (-v) &= 0 && \text{(existence of additive inverses)} \\
u\,(v\,w) &= (u\,v)\,w && \text{(associativity of multiplication)} \\
v\,w &= w\,v && \text{(commutativity of multiplication)} \\
v\,1 &= v && \text{(existence of multiplicative identity)} \\
u\,(v + w) &= u\,v + u\,w && \text{(distributivity)}
\end{aligned}$$

Sketch of proof. All eight properties may be verified by choosing representatives for the congruence classes and utilizing properties of the integers. For example, choose integers k, m, and n such that $u = [k]$, $v = [m]$, and $w = [n]$. The definition of addition on $\mathbb{Z}/\langle \ell \rangle$ and the associativity of addition on $\mathbb{Z}$ gives

$$\begin{aligned}
(u + v) + w &= ([k] + [m]) + [n] \\
&= [k + m] + [n] \\
&= [(k + m) + n] \\
&= [k + (m + n)] \\
&= [k] + [m + n] \\
&= [k] + ([m] + [n]) = u + (v + w)
\end{aligned}$$

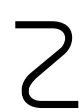
which establishes the associativity of addition on $\mathbb{Z}/\langle \ell \rangle$. □

We overload the symbols 0 and 1. The additive identity in $\mathbb{Z}/\langle \ell \rangle$ is the congruence class containing the integer 0; $0 := [0]_\ell = \{k\,\ell \mid k \in \mathbb{Z}\}$. Similarly, the multiplicative identity is the congruence class containing the integer 1; $1 := [1]_\ell = \{1 + k\,\ell \mid k \in \mathbb{Z}\}$.

Warning 2.2.2. Generally, the multiplicative cancellation law does not hold in $\mathbb{Z}/\langle \ell \rangle$. For instance, we have

$$[2]_6\,[2]_6 = [4]_6 = [10]_6 = [2]_6\,[5]_6\,,$$

but $[2]_6 \neq [5]_6$. Moreover, the product of two nonzero elements may be zero such as $[2]_6\,[3]_6 = [6]_6 = [0]_6$.



Lemma 2.2.3. *Let ℓ be an integer with $\ell > 1$. The congruence class $[m]_\ell$ has a multiplicative inverse in $\mathbb{Z}/\langle \ell \rangle$ if and only if $\gcd(m, \ell) = 1$.*

Proof.

$\Leftarrow$: For some integer j, suppose that $[j]_\ell$ is a multiplicative inverse of the element $[m]_\ell$ in $\mathbb{Z}/\langle \ell \rangle$. Since $[j]_\ell\,[m]_\ell = [j\,m]_\ell = [1]_\ell$, there exists an integer k such that $1 - j\,m = k\,\ell$ or $j\,m + k\,\ell = 1$. Corollary 1.1.8 establishes that $\gcd(m, \ell) = 1$.

$\Rightarrow$: Suppose that $\gcd(m, \ell) = 1$. Theorem 1.1.7 establishes that there are integers j and k such that $j\,m + k\,\ell = 1$. It follows that $[j]_\ell\,[m]_\ell = [j\,m]_\ell = [1 - k\,\ell]_\ell = [1]_\ell$. Since multiplication in $\mathbb{Z}/\langle \ell \rangle$ is commutative, we have $[m]_\ell\,[j]_\ell = [1]_\ell$. We conclude that $[j]_\ell$ is the multiplicative inverse of $[m]_\ell$. □

Problem 2.2.4. Find the last base-ten digit of 7^{99}.

Solution. Since

$$\begin{aligned} 7^2 &= 49 \equiv 9 \mod 10\,, \\ 7^3 &= 7^2(7) \equiv 9(7) \equiv 63 \equiv 3 \mod 10\,, \text{ and} \\ 7^4 &= 7^3(7) \equiv 3(7) \equiv 21 \equiv 1 \mod 10\,, \end{aligned}$$

and $99 = 24(4) + 3$, we have

$$7^{99} = 7^{24(4)+3} \equiv (7^4)^{24}(7^3) \equiv 1^{24}(3) \equiv 3 \mod 10\,,$$

so the last base-ten digit of 7^{99} is 3. □

Theorem 2.2.5. *For any $\ell \in \mathbb{Z}$ with $\ell > 1$, the following are equivalent:*

(a) *The integer ℓ is prime.*

(b) *For any two elements u and v in $\mathbb{Z}/\langle \ell \rangle$, having $u\,v = 0$ implies that $u = 0$ or $v = 0$.*

(c) *Any nonzero element u in $\mathbb{Z}/\langle \ell \rangle$ has a multiplicative inverse.*

Proof.

(a) $\Rightarrow$ (c): Suppose that ℓ is a prime integer. Choose an integer m such that $u = [m]_\ell$. As $m \neq 0$, we have $[m]_\ell \neq [0]_\ell$ and p does not divide m. Hence, Lemma 1.2.6 shows that $\gcd(\ell, m) = 1$ and Theorem 1.1.7 establishes that there are integers j and k such that $j\,m + k\,\ell = 1$. Since $[k\,\ell]_\ell = [0]_\ell$, we deduce that $[1]_\ell = [j\,m + k\,\ell]_\ell = [j\,m]_\ell\,[m]_\ell + [k\,\ell]_\ell = [j]_\ell\,[m]_\ell$. Since multiplication in $\mathbb{Z}/\langle \ell \rangle$ is commutative, we see that $[j]_\ell$ is the multiplicative inverse of $u = [m]_\ell$.

(c) $\Rightarrow$ (b): Suppose that every nonzero element in $\mathbb{Z}/\langle \ell \rangle$ has a multiplicative inverse. Consider two elements u and v in $\mathbb{Z}/\langle \ell \rangle$, such that $u\,v = 0$. When $u \neq 0$, the element u has a multiplicative inverse w. It follows that $v = 1\,v = (w\,u)\,v = w\,(u\,v) = w\,0 = 0$. We deduce that $u = 0$ or $v = 0$.

(b) $\Rightarrow$ (a): Suppose that $u\,v = 0$ implies that $u = 0$ or $v = 0$. Choose integers m and n such that $u = [m]_\ell$ and $v = [n]_\ell$. We obtain $[0]_\ell = 0 = u\,v = [m]_\ell\,[n]_\ell = [m\,n]_\ell$, so ℓ divides $m\,n$. Our supposition ensures that $[m]_\ell = 0$ or $[n]_\ell = 0$, which means that ℓ divides m or ℓ divides n. From Definition 1.2.7, we conclude that ℓ is prime. □

Problem 2.2.6. Simplify $9^{2023} \mod 7$.

Solution. Since $9 \equiv 2 \mod 7$ and $2^3 \equiv 1 \mod 7$, we obtain

$$9^{2023} \equiv 2^{2023} \equiv 2^{674(3)+1} \equiv (1)^{674}\, 2^1 \equiv 2 \mod 7\,. \qquad \square$$

Problem 2.2.7. Determine the last two base-ten digits of 3^{400}.

Solution. Since

$$\begin{aligned} &3^2 \equiv 9 \mod 10 && 3^8 \equiv (3^4)^2 \equiv 81^2 \equiv 61 \mod 100 \\ &3^3 \equiv 27 \equiv 7 \mod 10 && 3^{12} \equiv 3^8(3^4) \equiv (61)(81) \equiv 41 \mod 100 \\ &3^4 \equiv 3^3(3) \equiv 7(3) \equiv 1 \mod 10 && 3^{16} \equiv 3^{12}(3^4) \equiv (41)(81) \equiv 21 \mod 100 \\ & && 3^{20} \equiv 3^{14}(3^4) \equiv (21)(81) \equiv 1 \mod 100 \end{aligned}$$

we obtain $3^{400} \equiv 3^{20(20)} \equiv (3^{20})^{20} \equiv 1^{20} \equiv 1 \mod 100$, so the last base-ten digit of 3^{400} are 01. $\square$

Exercises

Problem 2.2.8. Consider the integer $m = \sum_{j=0}^{k} d_j\, 10^j$ where k is a nonnegative integer and $0 \leqslant d_j \leqslant 9$ for all $0 \leqslant j \leqslant k$.

(i) Show that 2 divides m if and only if 2 divides d_0.

(ii) Show that 3 divides m if and only if 3 divides $\sum_{j=0}^{k} d_j$.

(iii) Show that 4 divides m if and only if 4 divides $10\, d_1 + a_0$.

(iv) Show that 5 divides m if and only if 5 divides d_0.

(v) Show that 7 divides m if and only if 7 divides

$$\sum_{j=1}^{k} d_j\, 10^{j-1} - 2\, d_0\,.$$

(vi) Show that 9 divides m if and only if 9 divides $\sum_{j=0}^{k} d_j$.

(vii) Show that 11 divides m if and only if 11 divides

$$\sum_{j=0}^{k} (-1)^j\, d_j\,.$$

(viii) Show that 13 divides m if and only if 13 divides

$$\sum_{j=1}^{k} d_i\, 10^{j-1} + 4\, d_0\,.$$