

1.3 Euclidean Algorithm

How do we efficiently compute greatest common divisors? Division with remainder leads to an algorithm.

1.3.0 Theorem (Euclidean Algorithm for Integers).

Input: Integers m and n .

Output: The greatest common divisor of m and n .

Set $j := \max(|m|, |n|)$;

Set $k := \min(|m|, |n|)$;

While $k \neq 0$ do

Set $r := j \% k$;

Set $j := k$;

Set $k := r$;

Return j .

Proof. We first claim that $\gcd(m, n) = \gcd(n, m \% n)$. Set $q := m // n$ and $r := m \% n$. Division with remainder establishes that $m = qn + r$ and $0 \leq r < |n|$. To prove the claim, it is enough to show that the pairs (m, n) and (n, r) have the same common divisors.

Let e be a common divisor of m and n . There exist integers u and v such that $m = ue$ and $n = ve$. It follows that

$$r = m - qn = ue - qve = (u - qv)e,$$

so e divides r . As e already divides n , we see that e is a common divisor of n and r . Conversely, let d be a common divisor of n and r . There exist integers s and t such that $n = sd$ and $r = td$. It follows that $m = qn + r = qsd + td = (qs + t)d$, so d divides m . As d already divides n , we see that d is a common divisor of m and n .

Each step in the while loop replaces (j, k) with $(k, j \% k)$. Our first claim shows that replacement does not change the greatest common divisor. The algorithm terminates because the sequence of remainders is decreasing and goes to zero in less than n steps. $\square$

1.3.1 Problem. Compute $\gcd(21\,837, 2\,088)$.

Solution. The Euclidean algorithm gives

$$21\,837 = 10(2\,088) + 957,$$

$$2\,088 = 2(957) + 174,$$

$$957 = 5(174) + 87,$$

$$174 = 2(87) + 0.$$

Thus, we deduce that $\gcd(21\,837, 2\,088) = 87$. $\square$

1.3.2 Definition. The integers m and n are *coprime* or *relatively prime* if $\gcd(m, n) = 1$.

1.3.3 Corollary. Let $d, m, n \in \mathbb{Z}$. When $\gcd(d, m) = 1$ and d divides the product $m n$, the number d divides n .

Proof. The Bézout identity shows that there exist $j, k \in \mathbb{Z}$ such that $jd + km = 1$. The properties of integer multiplication give $n =$

In *The Art of Computer Programming*, Donald Knuth asserts that the Euclidean algorithm “is the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day.”

$$\begin{array}{r}
 10 \\
 2088 \overline{) 21837} \\
 \underline{2088} 2 \\
 957 \overline{) 2088} \\
 \underline{1914} 5 \\
 174 \overline{) 957} \\
 \underline{870} 2 \\
 87 \overline{) 174} \\
 \underline{174} \\
 0
 \end{array}$$

From the Bézout identity, we have $\gcd(m, n) = 1$ if and only if 1 is an integer linear combination of m and n .

$(1)n = (jd + km)n = (jn)d + (mn)k$. Since d divides the product mn , there exists $i \in \mathbb{Z}$ such that $mn = id$. It follows that

$$n = (jn)d + (mn)k = (jn)d + (id)k = (jn + ik)d,$$

so d divides n . $\square$

1.3.4 Definition. An integer p is *irreducible* if $p \neq \pm 1$ and the only divisors of p are ± 1 and $\pm p$. A nonzero integer, except for ± 1 , is *reducible* (or *composite*) if it is not irreducible.

The irreducible positive integers less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

We record a simple consequence of irreducibility.

1.3.5 Lemma. Let p be an irreducible integer. For every $m \in \mathbb{Z}$ that is not a multiple of p , we have $\gcd(p, m) = 1$.

Proof. Suppose that d is a common divisor of p and m . We see that $d = \pm 1$ or $d = \pm p$ because d divides p and p is irreducible. Since d also divides m and p is not a divisor of m , we deduce that $d = \pm 1$. As $\gcd(p, m) \geq 0$, we conclude that $d = 1$. $\square$

1.3.6 Definition. An integer p is *prime* if $p \neq \pm 1$, and p dividing the product mn of integers m and n implies that p divides m or n .

In mathematics, the word ‘or’ is not exclusive. The definition allows for the possibility that p may divide both m and n .

1.3.7 Warning. This definition for a prime is unconventional for the set $\mathbb{Z}$ of integers. Most number theory references do *not* include 0 as a prime integer. However, this choice does align with the prevailing terminology in ring theory. Fortunately, this discrepancy does not seem to cause any genuine issues.

2

The next result recovers the standard definition.

1.3.8 Proposition. A nonzero integer is irreducible if and only if it is prime.

Proof. When $p = \pm 1$, the integer p is neither irreducible nor prime, so the assertion holds. We may, thereby, assume that p is an integer other than 0 or ± 1 .

Suppose that the integer p is irreducible. Assume that p divides a product mn of integers and p does not divide m . Lemma 1.3.5 shows that $\gcd(p, m) = 1$ and Corollary 1.3.3 shows that p divides n . Therefore, the integer p is prime.

Conversely, suppose that p is prime. Consider a divisor d of p ; there exists $q \in \mathbb{Z}$ such that $p = qd$. As $(1)p = qd$, the integer p divides the product qd . The definition of a prime implies that p divides q or p divides d . When p divides d , Lemma 1.2.1 establishes that $|d| \leq |p|$ and $|p| \leq |d|$, so $|d| = |p|$ and $d = \pm p$. Similarly, when p divides q , there exists an integer k such that $q = kp$. It follows that $p = qd = kdp$ and $(1 - kd)p = 0$. As $p \neq 0$, we deduce that $1 - kd = 0$. Since $kd = 1$, the integer d divides 1 which implies $d = \pm 1$. We conclude that either $d = \pm p$ or $d = \pm 1$ which shows that p is irreducible. $\square$

2 Modular Arithmetic

Copyright © 2026, Gregory G. Smith
Last Updated: 2026-09-18

Modular arithmetic is a system of arithmetic where numbers “wrap around” when reaching a certain value. The 12-hour clock—the time convention that divides the day into two 12-hour periods—is the most familiar example.

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

2.0 Congruence

How do we regard divisibility as an equivalence relation? The basic notion is remarkably straightforward.

2.0.0 Definition. Fix $\ell \in \mathbb{N}$. The integers m and n are *congruent modulo ℓ* , denoted by $m \equiv n \pmod{\ell}$, if the difference $m - n$ is divisible by ℓ . The number ℓ is the *modulus*.

Congruence modulo 0 is simply equality: the relation $=$.

2.0.1 Lemma. For all $\ell \in \mathbb{N}$, congruence modulo ℓ is an equivalence relation on the set $\mathbb{Z}$ of integers.

Proof. Consider $k, m, n \in \mathbb{Z}$. As $m - m = 0 = (0)\ell$, we have $m \equiv m \pmod{\ell}$ and the congruence relation $\equiv$ is reflexive.

Suppose that $m \equiv n \pmod{\ell}$. Since $m - n$ is divisible by ℓ , there exists $j \in \mathbb{Z}$ such that $m - n = j\ell$. It follows that $n - m = (-j)\ell$, so $n - m$ is also divisible by ℓ . We deduce that $n \equiv m \pmod{\ell}$ and congruence relation $\equiv$ is symmetric.

Suppose that $k \equiv m \pmod{\ell}$ and $m \equiv n \pmod{\ell}$. There exist $i, j \in \mathbb{Z}$ 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 $k \equiv n \pmod{\ell}$ and congruence relation $\equiv$ is transitive. $\square$

2.0.2 Notation. The congruence classes modulo ℓ are

$$\begin{aligned} [m]_\ell &:= \{n \in \mathbb{Z} \mid m \equiv n \pmod{\ell}\} \\ &= \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } m - n = k\ell\} \\ &= \{m + k\ell \mid k \in \mathbb{Z}\}. \end{aligned}$$

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.

It follows that $[m]_\ell = [n]_\ell$ if and only if $m \equiv n \pmod{\ell}$. The set of congruence classes modulo ℓ is denoted by $\mathbb{Z}/\langle\ell\rangle := \mathbb{Z}/\equiv$.

2.0.3 Remark. When $\ell = 3$, there are three congruence classes:

$$\begin{aligned} [0]_3 &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = \{0 + 3k \mid k \in \mathbb{Z}\}, \\ [1]_3 &= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} = \{1 + 3k \mid k \in \mathbb{Z}\}, \\ [2]_3 &= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} = \{2 + 3k \mid k \in \mathbb{Z}\}. \end{aligned}$$

2.0.4 Proposition. Let ℓ be a positive integer. For all $m \in \mathbb{Z}$, we have $[m]_\ell = [m \% \ell]_\ell$. Moreover, the set $\mathbb{Z}/\langle\ell\rangle$ consists of the ℓ elements

$$[0]_\ell, [1]_\ell, [2]_\ell, \dots, [\ell - 1]_\ell.$$

Proof. By division with remainder, there exists $q, r \in \mathbb{Z}$ such that $m = q\ell + r$, $0 \leq r < \ell$, and $r := m \% \ell$. Since $m - r = q\ell$, we see that $m \equiv r \pmod{\ell}$ or $[m]_\ell = [r]_\ell$.

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

The first part shows that every congruence class equals a listed one. The claim shows that no two congruence classes coincide. $\square$

2.0.5 Remark. Given an equivalence relation on a set $\mathcal{X}$, a *complete system of distinct representatives* (or a *transversal*) is a subset of $\mathcal{X}$ having exactly one element from each equivalence class. In particular, Proposition 2.0.4 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 $\{-(\ell - 1)/2, \dots, -1, 0, 1, 2, \dots, \lfloor \ell/2 \rfloor\}$.

The choice of a transversal produces a *lifting map* $\lambda: (\mathcal{X}/\sim) \rightarrow \mathcal{X}$ defined, for all $[x]$ in $\mathcal{X}/\sim$, by $\lambda([x]) := x$. Any lifting map is a one-sided inverse of the canonical map $\pi: \mathcal{X} \rightarrow \mathcal{X}/\sim$ meaning that $\pi \circ \lambda = \text{id}_{\mathcal{X}/\sim}$.

Both $\{0, 1, 2, 3, 4\}$ and $\{-2, -1, 0, 1, 2\}$ are transversals for $\mathbb{Z}/\langle 5 \rangle$.

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

2.0.6 Lemma. Let $\ell \in \mathbb{N}$ and let $j, k, m, n \in \mathbb{Z}$. When $j \equiv k \pmod{\ell}$ and $m \equiv n \pmod{\ell}$, we have

$$j + m \equiv k + n \pmod{\ell} \quad \text{and} \quad jm \equiv kn \pmod{\ell}.$$

Proof. Since $j \equiv k \pmod{\ell}$ and $m \equiv n \pmod{\ell}$, there exists $u, v \in \mathbb{Z}$ such that $j - k = u\ell$ and $m - n = v\ell$. It follows that

$$\begin{aligned} (j + m) - (k + n) &= (j - k) + (m - n) = u\ell + v\ell = (u + v)\ell \\ (jm) - (kn) &= (k + u\ell)(n + v\ell) - (kn) \\ &= kv\ell + nu\ell + uv\ell^2 = (kv + nu + uv\ell)\ell. \end{aligned}$$

We conclude that ℓ divides $(j + m) - (k + n)$ and $(jm) - (kn)$, so $j + m \equiv k + n \pmod{\ell}$ and $jm \equiv kn \pmod{\ell}$. $\square$

The lemma establishes that congruence classes for the addition and the multiplication of integers do not depend on the choice of a representative, so the quotient $\mathbb{Z}/\langle \ell \rangle$ inherits these operations from the set $\mathbb{Z}$. More formally, we make the following definitions.

2.0.7 Definition. Let $\ell \in \mathbb{N}$. For all $[m]_\ell, [n]_\ell \in \mathbb{Z}/\langle \ell \rangle$, we define $[m]_\ell + [n]_\ell := [m + n]_\ell$ and $[m]_\ell [n]_\ell := [mn]_\ell$.

2.0.8 Problem. Simplify 11^3 modulo 13.

Solution. We have $11^3 \equiv (-2)^3 \equiv -8 \equiv 5 \pmod{13}$. $\square$

Addition is not well-defined for all quotient sets.

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

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.

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

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

2.1.0 Theorem. *Let $\ell \in \mathbb{N}$. For all $u, v, w \in \mathbb{Z}/\langle \ell \rangle$, we have:*

(associativity of addition)	$(u + v) + w = u + (v + w),$
(commutativity of addition)	$v + w = w + v,$
(existence of additive identity)	$v + 0 = v,$
(existence of additive inverses)	$v + (-v) = 0,$
(distributivity)	$u(v + w) = uv + uw,$
(associativity of multiplication)	$u(vw) = (uv)w,$
(commutativity of multiplication)	$vw = wv,$
(existence of multiplicative identity)	$v1 = v.$

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

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

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

2.1.1 Warning. Generally, the multiplicative cancellation law does not hold in the quotient $\mathbb{Z}/\langle \ell \rangle$; $[2]_6 [2]_6 = [4]_6 = [10]_6 = [2]_6 [5]_6$, but $[2]_6 \neq [5]_6$. Moreover, the product of nonzero elements may be zero such as $[2]_6 [3]_6 = [6]_6 = [0]_6$.

2

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

Proof. Consider $j \in \mathbb{Z}$ such that its congruence class $[j]_\ell$ in $\mathbb{Z}/\langle \ell \rangle$ is a multiplicative inverse of $[m]_\ell$. As $[j]_\ell [m]_\ell = [jm]_\ell = [1]_\ell$, there exists $k \in \mathbb{Z}$ such that $1 - jm = k\ell$ or $jm + k\ell = 1$. The Bézout identity establishes that $\gcd(m, \ell) = 1$.

Suppose that $\gcd(m, \ell) = 1$. The Bézout identity shows that there exist $j, k \in \mathbb{Z}$ such that $jm + k\ell = 1$. It follows that

$$[j]_\ell [m]_\ell = [jm]_\ell = [1 - k\ell]_\ell = [1]_\ell.$$

Multiplication in $\mathbb{Z}/\langle \ell \rangle$ is commutative, so $[m]_\ell [j]_\ell = [1]_\ell$. We conclude that $[j]_\ell$ is the multiplicative inverse of $[m]_\ell$. $\square$

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

Solution. Since $7^2 = 49 \equiv 9 \pmod{10}$,

$$7^3 = 7^2(7) \equiv 9(7) \equiv 63 \equiv 3 \pmod{10}, \text{ and}$$

$$7^4 = 7^3(7) \equiv 3(7) \equiv 21 \equiv 1 \pmod{10},$$

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

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

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

2.1.4 Theorem. For any positive $\ell \in \mathbb{Z}$, the following are equivalent:

- a. The integer ℓ is prime.
- b. For all $u, v \in \mathbb{Z}/\langle \ell \rangle$, $uv = 0$ implies that $u = 0$ or $v = 0$.
- c. Any nonzero $u \in \mathbb{Z}/\langle \ell \rangle$ has a multiplicative inverse.

Proof.

a $\Rightarrow$ c: Suppose that ℓ is a prime. Choose $m \in \mathbb{Z}$ such that $u = [m]_\ell$.

By hypothesis, we have $u = [m]_\ell \neq [0]_\ell$ and ℓ does not divide m .

Lemma 1.3.5 shows that $\gcd(\ell, m) = 1$ and Bézout identity shows that there exist $j, k \in \mathbb{Z}$ such that $jm + k\ell = 1$. As $[k\ell]_\ell = [0]_\ell$, we have $[1]_\ell = [jm]_\ell + [k\ell]_\ell = [j]_\ell [m]_\ell$. As 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 the quotient $\mathbb{Z}/\langle \ell \rangle$ has a multiplicative inverse. Consider elements u and v in $\mathbb{Z}/\langle \ell \rangle$, such that $uv = 0$. When $u \neq 0$, the element u has a multiplicative inverse w . It follows that $v = 1v = (wu)v = w(uv) = w0 = 0$. We deduce that $u = 0$ or $v = 0$.

b $\Rightarrow$ a: Suppose that the equation $uv = 0$ implies that $u = 0$ or $v = 0$. Choose $m, n \in \mathbb{Z}$ such that $u = [m]_\ell$ and $v = [n]_\ell$. It follows that $[0]_\ell = 0 = uv = [m]_\ell [n]_\ell = [mn]_\ell$, so ℓ divides mn . Our supposition ensures that $[m]_\ell = 0$ or $[n]_\ell = 0$, which means that ℓ divides m or ℓ divides n . From Definition 1.3.6, we conclude that ℓ is prime. $\square$

2.1.5 Problem. Simplify $9^{2026} \pmod{7}$.

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

$$9^{2026} \equiv 2^{2026} \equiv 2^{675(3)+1} \equiv (1)^{675} 2^1 \equiv 2 \pmod{7}. \quad \square$$

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

Solution. Since $3^2 \equiv 9 \pmod{10}$, $3^3 \equiv 27 \equiv 7 \pmod{10}$, and

$$3^4 \equiv 3^3(3) \equiv 7(3) \equiv 1 \pmod{10}$$

$$3^8 \equiv (3^4)^2 \equiv 1^2 \equiv 1 \pmod{100}$$

$$3^{12} \equiv 3^8(3^4) \equiv (1)(1) \equiv 1 \pmod{100}$$

$$3^{16} \equiv 3^{12}(3^4) \equiv (1)(1) \equiv 1 \pmod{100}$$

$$3^{20} \equiv 3^{16}(3^4) \equiv (1)(1) \equiv 1 \pmod{100}$$

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

2.3 Exercises

2.3.1 Problem. Determine which of the following statements are true. If a statement is false, provide a counterexample and, if possible, salvage it by modifying the statement so that it becomes true.

- i. Integers are congruent modulo ℓ if and only if they have the same remainder upon division by ℓ .
- ii. Let $\ell \in \mathbb{Z}$ be positive. Congruence modulo ℓ partitions the set $\mathbb{Z}$ into exactly ℓ equivalence classes.
- iii. If $km \equiv kn \pmod{\ell}$, then $m \equiv n \pmod{\ell}$.
- iv. If $m \equiv n \pmod{\ell}$ then $m^k \equiv n^k \pmod{\ell}$ for all $k \in \mathbb{N}$.
- v. If $m \equiv n \pmod{k}$ and $m \equiv n \pmod{\ell}$, then $m \equiv n \pmod{k\ell}$.
- vi. An integer m has a multiplicative inverse modulo ℓ if and only if $\gcd(m, \ell) = 1$.
- vii. If m has a multiplicative inverse modulo ℓ , then that inverse is unique modulo ℓ .
- viii. If $m^{\phi(\ell)} \equiv 1 \pmod{\ell}$ for all $m \in \mathbb{Z}$ with $\gcd(m, \ell) = 1$, then ℓ is prime.
- ix. If $\phi(m)$ is prime, then m must be a power of 2.
- x. If p is a positive prime integer, then $(p-2)! \equiv 1 \pmod{p}$.

2.3.2 Problem. Let $m \in \mathbb{Z}$. Confirm that $m^2 \equiv 0$ or $1 \pmod{3}$ and $m^2 \equiv 0$ or $4 \pmod{5}$.

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

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

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

- 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 $10d_1 + d_0$.
- 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

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

- 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

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

2.3.6 Problem. Demonstrate that the equation $x^6 + y^{12} = 703$ has no integer solutions.

2.3.7 Problem. Let ℓ be a reducible integer such that $\ell > 4$. Verify that $(\ell-1)! \equiv 0 \pmod{\ell}$.

2.3.8 Problem. Let p be a positive prime integer having the form $p = 2k + 1$ for some integer k . Prove that $(k!)^2 \equiv (-1)^{k+1} \pmod{p}$.