CS1231S Chapter 8

Basic number theory

8.1 Divisibility

Definition 8.1.1. Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for "d divides n", and $d \nmid n$ for "d does not divide n". We also say

"n is *divisible* by d" or "n is a *multiple* of d" or "d is a *factor/divisor* of n"

for "d divides n".

Warning 8.1.2. Note that $2 \mid 4$ is a statement, while $2/4$ is a number. Do not confuse $d \mid n$ with $\frac{d}{n}$ or d/n.

Example 8.1.3. (1) $3 \mid 6$ because $6 = 3 \times 2$.

(2) $3 \nmid 7$ because $7 \neq 3k$ for any $k \in \mathbb{Z}$.

Exercise 8.1.4. Let $a, d, n \in \mathbb{Z}$. Show that if $d \mid n$, then $ad \mid an$. ✎ 8a

Lemma 8.1.5. Let $n, d \in \mathbb{Z}$ with $d \neq 0$. Then $d \mid n$ if and only if $n/d \in \mathbb{Z}$.

Proof.
1. ("Only if")
   1.1. Suppose $d \mid n$.
   1.2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
   1.3. Then $n/d = k \in \mathbb{Z}$.
2. ("If")
   2.1. Suppose $n/d \in \mathbb{Z}$.
   2.2. Then $n = dk$, where $k = n/d$.
   2.3. So it follows from the definition of divisibility that $d \mid n$. □

Example 8.1.6. Let $n \in \mathbb{Z}$. Then $1 \mid n$ and $n \mid n$ because $1 \times n = n = n \times 1$.

Example 8.1.7. Let $d \in \mathbb{Z}$. Then $d \mid 0$ because $0 = d \times 0$.

Exercise 8.1.8. Determine which $n \in \mathbb{Z}$ makes $0 \mid n$. ✎ 8b

Lemma 8.1.9. Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$.

Proof.
1. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
2. Then

$$n = (-d)(-k) \quad \text{and} \quad -n = d(-k) \quad \text{and} \quad -n = (-d)k,$$

   where $-k, k \in \mathbb{Z}$.

3. Hence $-d \mid n$ and $d \mid -n$ and $-d \mid -n$ by the definition of divisibility. □

Proposition 8.1.10. Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $n \neq 0$, then $|d| \leqslant |n|$.

Proof. 1. Since $d \mid n$, we know $|d| \mid |n|$ by Lemma 8.1.9.
2. Use this fact to find $k \in \mathbb{Z}$ such that $|n| = |d|k$.
3. Now $n \neq 0$ implies $|n| > 0$ and thus also $|d| > 0$.
4. So $k > 0$ too as $|n| = |d|k$.
5. Since $k \in \mathbb{Z}$, we deduce that $k \geqslant 1$.
6. Hence $|n| = |d|k \geqslant |d| \times 1 = |d|$. □

Example 8.1.11. The only positive divisors of 6 are $1, 2, 3, 6$.

Proposition 8.1.12 (transitivity of divisibility)**.** Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. 1. Assume $a \mid b$ and $b \mid c$.
2. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = b\ell$.
3. Then $c = b\ell = (ak)\ell = a(k\ell)$, where $k\ell \in \mathbb{Z}$.
4. Thus $a \mid c$ by the definition of divisibility. □

Example 8.1.13. Since $3 \mid 6$ and $6 \mid 18$, the transitivity of divisibility tells us $3 \mid 18$.

Lemma 8.1.14 (Closure Lemma (non-standard name))**.** Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

Proof. 1. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $m = dk$ and $n = d\ell$.
2. Then $am + bn = a(dk) + b(d\ell)$ by the choices of k and ℓ;
3. $= d(ak + b\ell)$, where $ak + b\ell \in \mathbb{Z}$.
4. Thus $d \mid am + bn$ by the definition of divisibility. □

Example 8.1.15. Since $3 \mid -6$ and $3 \mid 9$ and $-564 = 100 \times -6 + 4 \times 9$, the Closure Lemma tells us $3 \mid -564$.

Theorem 8.1.16 (Division Theorem)**.** *For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that*

$$n = dq + r \quad \text{and} \quad 0 \leqslant r < d. \tag{$*$}$$

Definition 8.1.17. Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. The unique $q, r \in \mathbb{Z}$ given by the Division Theorem such that $(*)$ holds are called the *quotient* and the *remainder* when n is divided by d, and are denoted $n \,\underline{\mathrm{div}}\, d$ and $n \,\underline{\mathrm{mod}}\, d$ respectively.

Warning 8.1.18. Some programming languages define their $n \,\underline{\mathrm{mod}}\, d$ to have the same sign as n or d. Our $n \,\underline{\mathrm{mod}}\, d$ is *always non-negative.*

Example 8.1.19. (1) $11 \,\underline{\mathrm{div}}\, 5 = 2$ and $11 \,\underline{\mathrm{mod}}\, 5 = 1$ because $11 = 5 \times 2 + 1$ and $0 \leqslant 1 < 5$.

(2) $-16 \,\underline{\mathrm{div}}\, 3 = -6$ and $-16 \,\underline{\mathrm{mod}}\, 3 = 2$ because $-16 = 3 \times -6 + 2$ and $0 \leqslant 2 < 3$.

Proof of the Division Theorem. 1. Let $q = \lfloor n/d \rfloor$ and $r = n - dq$.
2. (Existence)
   2.1. Note that $q, r \in \mathbb{Z}$ and $n = dq + r$.
   2.2. Also $q \leqslant n/d < q + 1$ by the Exercise 6.1.11(1);
   2.3. $\therefore$ $dq \leqslant n < d(q + 1)$ multiplying by d throughout;
   2.4. $\therefore$ $dq - dq \leqslant n - dq < d(q + 1) - dq$ subtracting dq throughout;
   2.5. $\therefore$ $0 \leqslant r < d$ by the definition of r.
3. (Uniqueness)
   3.1. Suppose $q', r' \in \mathbb{Z}$ such that $n = dq' + r'$ and $0 \leqslant r' < d$.

3.2. Then $0 \leqslant n - dq' < d$ by the choice of q' and r';

3.3. $\therefore$ $0 \leqslant \dfrac{n}{d} - q' < 1$ dividing by d throughout;

3.4. $\therefore$ $q' \leqslant \dfrac{n}{d} < q' + 1$ adding q' throughout;

3.5. $\therefore$ $q' = \left\lfloor \dfrac{n}{d} \right\rfloor$ by Exercise 6.1.11(1).

3.6. Thus $q' = q$.

3.7. By the choice of r', this implies $r' = n - dq' = n - dq = r$. □

Note 8.1.20. The proof above tells us $n \ \underline{\mathrm{div}}\ d = \lfloor n/d \rfloor$.

Definition 8.1.21. (1) An integer is *even* if it is equal to $2k$ for some $k \in \mathbb{Z}$.

(2) An integer is *odd* if it is equal to $2k + 1$ for some $k \in \mathbb{Z}$.

Corollary 8.1.22. Let $n \in \mathbb{Z}$. Then n is either even or odd, but not both.

Proof. 1. Use the Division Theorem to find $q, r \in \mathbb{Z}$ such that $n = 2q + r$ and $0 \leqslant r < 2$.

2. Either $r = 0$ or $r = 1$.
3. So either $n = 2q$ or $n = 2q + 1$.
4. So either n is even or n is odd.
5. n cannot be both even and odd because it is not possible to have $k, k' \in \mathbb{Z}$ such that $2k + 0 = n = 2k' + 1$ by the uniqueness part of the Division Theorem. □

8.2 Prime numbers

Definition 8.2.1. (1) A positive integer is *prime* if it has exactly two positive divisors.

(2) A positive integer is *composite* if it has (strictly) more than two positive divisors.

Remark 8.2.2. (1) 1 is neither prime nor composite because it has exactly one positive divisor.

(2) Every integer $n \geqslant 2$ is either prime or composite.

Example 8.2.3. (1) 7 is prime because its positive divisors are $1, 7$.

(2) 9 is composite because its positive divisors are $1, 3, 9$.

Lemma 8.2.4. An integer n is composite if and only if n has a divisor d such that $1 < d < n$.

Proof. 1. ("If")

1.1. Let d be a divisor of n such that $1 < d < n$.

1.2. Then $1, d, n$ are three (distinct) divisors of n.

1.3. So n is composite.

2. ("Only if")

2.1. Suppose n is composite.

2.2. Then n has a positive divisor, say d, such that $1 \neq d \neq n$.

2.3. Now $d \mid n$ implies $d = |d| \leqslant |n| = n$ by Proposition 8.1.10.

2.4. So $1 < d < n$. □

Lemma 8.2.5 (Prime Divisor Lemma (non-standard name))**.** Let $n \in \mathbb{Z}_{\geqslant 2}$. Then n has a prime divisor.

Proof. 1. Note that n has a positive divisor strictly bigger than 1, say n.

2. Use the Well-Ordering Principle to find the smallest such divisor d of n.
3. We prove that d is prime by contradiction.

3.1. Suppose d is not prime.
3.2. Then d is composite by Remark 8.2.2(2).
3.3. So d has a divisor, say c, such that $1 < c < d$, by Lemma 8.2.4.
3.4. Now $c \mid d$ and $d \mid n$. So $c \mid n$ by the transitivity of divisibility.
3.5. This contradicts the assumption that d is the smallest positive divisor d of n strictly bigger than 1. □

Proposition 8.2.6. *Let n be a composite positive integer. Then n has a prime divisor $p \leqslant \sqrt{n}$.*

Proof. 1. Use Lemma 8.2.4 and the hypothesis that n is composite to find $d \mid n$ such that $1 < d < n$.
2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
3. Case 1: suppose $d \leqslant \sqrt{n}$.
3.1. Use the Prime Divisor Lemma to find a prime $p \mid d$.
3.2. Since $p \mid d$ and $d \mid n$, the transitivity of divisibility implies $p \mid n$.
3.3. As $p \mid d$, we know $p = |p| \leqslant |d| = d \leqslant \sqrt{n}$ by Proposition 8.1.10.
4. Case 2: suppose $d > \sqrt{n}$.
4.1. Note $k = n/d > n/n = 1$ as $d < n$.
4.2. So $k \geqslant 2$ as $k \in \mathbb{Z}$.
4.3. Use the Prime Divisor Lemma to find a prime $p \mid k$.
4.4. Since $p \mid k$ and $k \mid n$, the transitivity of divisibility implies $p \mid n$.
4.5. As $p \mid k$ and $d > \sqrt{n}$, we have $p = |p| \leqslant |k| = k = n/d < n/\sqrt{n} = \sqrt{n}$ by Proposition 8.1.10. □

Example 8.2.7. The primes less than $\sqrt{101}$ are $2, 3, 5, 7$, none of which divides 101. So 101 is prime by Proposition 8.2.6.

Theorem 8.2.8 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. 1. We prove this by contradiction. So suppose the theorem is false.

preparing a new number and creating how it should only be composite

2. Let $p_1, p_2, \ldots, p_k$ be a complete (finite) list of primes.
3. Define $n = p_1 p_2 \ldots p_k + 1$. Note that $n \geqslant 1 + 1 = 2$.
4. Use the Prime Divisor Lemma to find a prime divisor of n say p.
5. Use the hypothesis that $p_1, p_2, \ldots, p_k$ is a complete list of primes to find $i \in \{1, 2, \ldots, k\}$ such that $p = p_i$.
6. As $p_1 p_2 \ldots p_k / p_i \in \mathbb{Z}$, the definition of divisibility tells us that $p_i \mid p_1 p_2 \ldots p_k$.
7. So $p_i \mid (n - p_1 p_2 \ldots p_k)$ by the Closure Lemma, as $p_i \mid n$.
8. Thus $p_i \mid 1$ by the definition of n.
9. Proposition 8.1.10 then implies $2 \leqslant p_i = |p_i| \leqslant |1| = 1$, which is a contradiction. □

since only divides 1, means new number is also prime but supposed to be composite

8.3 Base-b representation

Fix $b \in \mathbb{Z}_{\geqslant 2}$ throughout this section.

Definition 8.3.1. The *base-b representation* of a positive integer n is

$$(a_\ell a_{\ell-1} \ldots a_0)_b$$

where $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$ such that

$$n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0 \quad \text{and} \quad a_\ell \neq 0. \tag{†}$$

The $a_0, a_1, \ldots, a_\ell$ here are called *digits*.

Convention 8.3.2. We identify a positive integer with its base-b representation.

Example 8.3.3. (1) $1231 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 1 \times 10^0 = (1231)_{10}$.

(2) $182 = 2 \times 3^4 + 0 \times 3^3 + 2 \times 3^2 + 0 \times 3^1 + 2 \times 3^0 = (20202)_3$.

Definition 8.3.4. (1) Base-10 representations are called *decimal representations.*

(2) Base-2 representations are called *binary representations.*

(3) Base-8 representations are called *octal representations.*

(4) Base-16 representations are called *hexadecimal representations.*

(5) Base-60 representations are called *sexagesimal representations.*

Convention 8.3.5. In hexadecimal representation, use respectively

$$\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F} \quad \text{for} \quad 10, 11, 12, 13, 14, 15.$$

Example 8.3.6. (1) $(1231)_{10}$ is the decimal representation of 1231.

(2) $(1000011)_2$ is the binary representation of 67 because

$$1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 67.$$

(3) $(117)_8$ is the octal representation of 79 because $1 \times 8^2 + 1 \times 8^1 + 7 \times 8^0 = 79$.

(4) $(4\mathrm{D})_{16}$ is the hexadecimal representation of 77 because $4 \times 16^1 + 13 \times 16^0 = 77$.

Exercise 8.3.7. Calculate by hand the decimal representations of $(10101010)_2$, $(777)_8$, and $(\mathrm{ABC})_{16}$. ✎ 8c

Algorithm 8.3.8 (for finding base-b representations)**.**

```
input $n \in \mathbb{Z}^+$
$q := n$
$\ell := 0$
while $q \neq 0$ do
    $a_\ell := q \,\underline{\mathrm{mod}}\, b$
    $q := q \,\underline{\mathrm{div}}\, b$
    $\ell := \ell + 1$
end do
output $(a_{\ell-1}a_{\ell-2}\dots a_1a_0)_b$
```

Example 8.3.9. $(b, n) = (8, 1511)$

$$\begin{array}{r|llll}
8 & 1511 & & & \\ \cline{2-2}
8 & 188 & — & 7 & \to a_0 \\ \cline{2-2}
8 & 23 & — & 4 & \to a_1 \\ \cline{2-2}
8 & 2 & — & 7 & \to a_2 \\ \cline{2-2}
\multicolumn{1}{r}{} & 0 & — & 2 & \to a_3
\end{array}$$

So $1511 = (2747)_8$.

Example 8.3.10. $(b, n) = (16, 1511)$

$$\begin{array}{r|llll}
16 & 1511 & & & \\ \cline{2-2}
16 & 94 & — & 7 & \to a_0 \\ \cline{2-2}
16 & 5 & — & 14 = \mathrm{E} & \to a_1 \\ \cline{2-2}
\multicolumn{1}{r}{} & 0 & — & 5 & \to a_2
\end{array}$$

So $1511 = (5\mathrm{E}7)_{16}$.

Exercise 8.3.11. Calculate by hand the base-7 representation of 1231. ✎ 8d

Proof that Algorithm 8.3.8 stops. 1. Let q_i be the value of the variable q when the stopping condition $q \neq 0$ of the **while** loop is checked the $(i+1)$th time.

2. Then $n = q_0$ by line 2 in Algorithm 8.3.8;
3. $> q_0 \underline{\operatorname{div}} b$ as $b \geqslant 2$;
4. $= q_1$ by line 6 in Algorithm 8.3.8;
5. $> q_1 \underline{\operatorname{div}} b$ as $b \geqslant 2$;
6. $= q_2$ by line 6 in Algorithm 8.3.8;
7. $> q_2 \underline{\operatorname{div}} b$ as $b \geqslant 2$;
8. $= q_3$ by line 6 in Algorithm 8.3.8;
9. $> \cdots$
10. Since each $q_i \geqslant 0$, the **while** loop can be executed at most n times.
11. In particular, this algorithm stops. □

Note 8.3.12. We implicitly used the Well-Ordering Principle on line 10 of the proof above to deduce that, since

$$\{q_0, q_1, q_2, \dots\}$$

is nonempty, it must have a smallest element.

Proof that Algorithm 8.3.8 is correct. 1. Let q_i be the value of the variable q when the stopping condition $q \neq 0$ of the **while** loop is checked the $(i+1)$th time.

2. Suppose the stopping condition of the **while** loop is checked $\ell + 1$ times in total, where $\ell \in \mathbb{Z}_{\geqslant 0}$.
3. Then $q_{\ell-1} > 0$ and $q_\ell = 0$ by the stopping condition of the **while** loop.
4. Note that $q_i = bq_{i+1} + a_i$ for each $i \in \{0, 1, \dots, \ell - 1\}$ by line 6 in Algorithm 8.3.8.
5. Hence $n = q_0$ by line 2 in Algorithm 8.3.8;
6. $= bq_1 + a_0$ by line 4;
7. $= b(bq_2 + a_1) + a_0$ by line 4;
8. $= b^2 q_2 + a_1 b + a_0$
9. $= b^2(bq_3 + a_2) + a_1 b + a_0$ by line 4;
10. $= b^3 q_3 + a_2 b^2 + a_1 b + a_0$
11. $= \cdots$
12. $= b^\ell q_\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_1 b + a_0$
13. $= a_{\ell-1} b^{\ell-1} + \cdots + a_1 b + a_0$ as $q_\ell = 0$ by line 3.
14. Also $a_{\ell-1} = bq_\ell + a_{\ell-1} = q_{\ell-1} > 0$.
15. So $n = (a_{\ell-1} a_{\ell-2} \dots a_1 a_0)_b$. □

Theorem 8.3.13. For any $n \in \mathbb{Z}^+$, there exist unique $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b-1\}$ such that

$$n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0 \quad \text{and} \quad a_\ell \neq 0.$$

Proof. 1. (Existence) As we already saw, Algorithm 8.3.8 gives a base-b representation of any positive integer.

2. (Uniqueness) We prove this by Strong Mathematical Induction.
   - 2.1. For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".
   - 2.2. (Base step)
     - 2.2.1. Let $c \in \{1, 2, \dots, b-1\}$. Suppose $c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0$ and $a_\ell \neq 0$, where $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b-1\}$.

2.2.2. If we have $i \in \{1, 2, \ldots, \ell\}$ such that $a_i \geqslant 1$, then

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0 \geqslant a_i b^i \geqslant 1 \cdot b^1 = b,$$

which contradicts the choice of c.

2.2.3. This means $a_1 = a_2 = \cdots = a_\ell = 0$, and so $\ell = 0$.

2.2.4. Thus $c = a_0 b^0 = a_0$.

2.2.5. Hence all base-b representations of c must be the same as $(c)_b$.

2.2.6. So $P(c)$ is true.

2.3. (Induction step)

2.3.1. Let $k \in \mathbb{Z}_{\geqslant b-1}$ such that $P(1), P(2), \ldots, P(k)$ are true.

2.3.2. Let $\ell, m \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0 = k + 1 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_0 b^0 \tag{‡}$$

and $a_\ell > 0$ and $d_m > 0$.

2.3.3. The quotients one gets when these are divided by b are equal too, i.e.,

$$a_\ell b^{\ell-1} + a_{\ell-1} b^{\ell-2} + \cdots + a_1 b^0 = (k+1) \underline{\text{div}} b = d_m b^{m-1} + d_{m-1} b^{m-2} + \cdots + d_1 b^0. \tag{§}$$

2.3.4. Note that $1 \leqslant (k+1) \underline{\text{div}}\, b \leqslant (k+k) \underline{\text{div}}\, 2 = k$ because $k + 1 \geqslant b \geqslant 2$.

2.3.5. So $P((k+1) \underline{\text{div}}\, b)$ is true by the induction hypothesis, i.e., $(k+1) \underline{\text{div}}\, b$ has at most one base-b representation.

2.3.6. This implies $\ell = m$ and $a_i = d_i$ for all $i \in \{1, 2, \ldots, \ell\}$ in view of (§).

2.3.7. Substituting these back into (‡) gives

$$\begin{aligned}
&a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_1 b^1 + a_0 b^0 \\
&= d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b^1 + d_0 b^0 \\
&= a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_1 b^1 + d_0 b^0.
\end{aligned}$$

2.3.8. Thus $a_0 = a_0 b^0 = d_0 b^0 = d_0$.

2.3.9. So $P(k+1)$ is true.

2.4. Hence $\forall n \in \mathbb{Z}^+ \;\; P(n)$ is true by Strong MI. □

8.4 Greatest common divisors

Definition 8.4.1. Let $m, n \in \mathbb{Z}$.

(1) A *common divisor* of m and n is divisor of both m and n.

(2) The greatest common divisor of m and n is denoted $\gcd(m, n)$.

Example 8.4.2.

- The positive divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$.
- The positive divisors of 63 are $1, 3, 7, 9, 21, 63$.
- So the positive common divisors of 72 and 63 are $1, 3, 9$.
- So $\gcd(72, 63) = 9$.

Exercise 8.4.3. Let $m, n \in \mathbb{Z}^+$. Show that $m \,\underline{\text{mod}}\, n = 0$ if and only if $\gcd(m, n) = n$. ✎ 8e

Remark 8.4.4. In view of Proposition 8.1.10, for all $m, n \in \mathbb{Z}$, if $m \neq 0$ or $n \neq 0$, then $\gcd(m, n)$ exists and is positive.

Question 8.4.5. $\gcd(0, 0)$ does not exist. Why? (What are the divisors of 0?) ✎ 8f

Exercise 8.4.6. Let $m, p \in \mathbb{Z}^+$. Show that if p is prime, then either $\gcd(m,p) = 1$ or $p \mid m$. (Hint: If $\gcd(m,p) = p$, then $m \,\underline{\mathrm{mod}}\, p = 0$ by Exercise 8.4.3, and so $p \mid m$.) ✎ 8g

Exercise 8.4.7. Let $m, n \in \mathbb{Z}$. Show that the common divisors of m and n are exactly the common divisors of $|m|$ and $|n|$, and hence $\gcd(m,n) = \gcd(|m|,|n|)$. ✎ 8h

Algorithm 8.4.8 (Euclidean Algorithm)**.**

```
input $m, n \in \mathbb{Z}^+$ with $m \geqslant n > 0$
$x := m$
$y := n$
while $y \neq 0$ do
    $r := x \,\underline{\mathrm{mod}}\, y$
    $x := y$
    $y := r$
end do
output $x$
```

$$\begin{array}{ccccc}
x & & y & & r \\
\downarrow & & \downarrow & & \downarrow \\
m & \underline{\mathrm{mod}} & n & = & r_1 \\
n & \underline{\mathrm{mod}} & r_1 & = & r_2 \\
r_1 & \underline{\mathrm{mod}} & r_2 & = & r_3 \\
r_2 & \underline{\mathrm{mod}} & r_3 & = & r_4 \\
 & & & \vdots & \\
r_{k-2} & \underline{\mathrm{mod}} & r_{k-1} & = & r_k \\
r_{k-1} & \underline{\mathrm{mod}} & r_k & = & 0 \\
\hline
\multicolumn{5}{c}{\therefore\ \gcd(m,n) = r_k}
\end{array}$$

Example 8.4.9. To find $\gcd(1076, 414)$:

$$\begin{array}{ccccc}
x & & y & & r \\
\downarrow & & \downarrow & & \downarrow \\
1076 & \underline{\mathrm{mod}} & 414 & = & 248 \\
414 & \underline{\mathrm{mod}} & 248 & = & 166 \\
248 & \underline{\mathrm{mod}} & 166 & = & 82 \\
166 & \underline{\mathrm{mod}} & 82 & = & 2 \\
82 & \underline{\mathrm{mod}} & 2 & = & 0 \\
\hline
\multicolumn{5}{c}{\therefore\ \gcd(1076,414) = 2}
\end{array}$$

Proof that the Euclidean Algorithm stops.

1. Note that each $r_i \geqslant 0$.
2. So

$$\begin{aligned}
n &> m \,\underline{\mathrm{mod}}\, n \\
&= r_1 > n \,\underline{\mathrm{mod}}\, r_1 \\
&= r_2 > r_1 \,\underline{\mathrm{mod}}\, r_2 \\
&= r_3 > r_2 \,\underline{\mathrm{mod}}\, r_3 \\
&\ \vdots
\end{aligned}$$

3. Thus the **while** loop is executed at most n times.
4. In particular, the algorithm stops. □

Note 8.4.10. We implicitly used the Well-Ordering Principle on line 3 of the proof above to deduce that, since

$$\{n, r_1, r_2, r_3, \dots\}$$

is nonempty, it must have a smallest element.

Lemma 8.4.11. If $x, y, r \in \mathbb{Z}$ such that $x \,\underline{\mathrm{mod}}\, y = r$, then $\gcd(x,y) = \gcd(y,r)$.

Proof.

1. Let $q = x \,\underline{\mathrm{div}}\, y$.
2. Then $x = yq + r$ by the definition of $\underline{\mathrm{div}}$ and $\underline{\mathrm{mod}}$.
3. If d is a common divisor of x and y, then d is a divisor of r by the Closure Lemma as $r = x - yq = 1 \cdot x + (-q)y$.
4. If d is a common divisor of y and r, then d is a divisor of x by the Closure Lemma as $x = yq + r = qy + 1 \cdot r$.
5. So the common divisors of x and y are the exactly the common divisors of y and r.

6. Hence $\gcd(x, y) = \gcd(y, r)$. □

Proof that the Euclidean Algorithm is correct.

1. If $m \underline{\bmod} n = 0$, then $\gcd(m, n) = n$ by Exercise 8.4.3.
2. Suppose $m \underline{\bmod} n \neq 0$. Let $r_1, r_2, \ldots, r_k$ be as generated in the Euclidean Algorithm, where $k \in \mathbb{Z}^+$.
3. Then Lemma 8.4.11 implies

$$\begin{aligned}
\gcd(m, n) &= \gcd(n, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\;\vdots \\
&= \gcd(r_{k-1}, r_k) \\
&= r_k && \text{by Exercise 8.4.3}
\end{aligned}$$

because $r_{k-1} \underline{\bmod} r_k = 0$. □

8.5 Fundamental Theorem of Arithmetic

Definition 8.5.1. Let $m, n \in \mathbb{Z}$. An *integer linear combination* of m and n is a number of the form $ms + nt$, where $s, t \in \mathbb{Z}$.

Theorem 8.5.2 (Bézout's Lemma)**.** Let $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $\gcd(m, n)$ is an integer linear combination of m and n.

Example 8.5.3. From Example 8.4.9, we know $\gcd(1076, 414) = 2$ because

$$\begin{array}{rcrcrcrclr}
1076 \underline{\bmod} 414 &=& 248 & \dashleftarrow & 248 &=& 1076 &-& 414 \times 2 & (1) \\
414 \underline{\bmod} 248 &=& 166 & \dashleftarrow & 166 &=& 414 &-& 248 \times 1 & (2) \\
248 \underline{\bmod} 166 &=& 82 & \dashleftarrow & 82 &=& 248 &-& 166 \times 1 & (3) \\
166 \underline{\bmod} 82 &=& 2 & \dashleftarrow & 2 &=& 166 &-& 82 \times 2 & (4) \\
82 \underline{\bmod} 2 &=& 0 & & & & & & &
\end{array}$$

Hence

$$\begin{aligned}
\gcd(1076, 414) = 2 &= 166 - 82 \times 2 && \text{by (4);} \\
&= 166 - (248 - 166 \times 1) \times 2 && \text{by (3);} \\
&= 248 \times (-2) + 166 \times 3 \\
&= 248 \times (-2) + (414 - 248 \times 1) \times 3 && \text{by (2);} \\
&= 414 \times 3 + 248 \times (-5) \\
&= 414 \times 3 - (1076 - 414 \times 2) \times 5 && \text{by (1);} \\
&= 1076 \times (-5) + 414 \times 13.
\end{aligned}$$

Remark 8.5.4. Let $m, n \in \mathbb{Z}^+$. If $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = ms + nt$, then by Exercise 8.4.7,

- $\gcd(-m, n) = \gcd(m, n) = ms + nt = (-m)(-s) + nt$;
- $\gcd(m, -n) = \gcd(m, n) = ms + nt = ms + (-n)(-t)$; and
- $\gcd(-m, -n) = \gcd(m, n) = ms + nt = (-m)(-s) + (-n)(-t)$.

Theorem 8.5.5 (Euclid's Lemma)**.** Let $m, n, p \in \mathbb{Z}^+$. If p is prime and $p \mid mn$, then $p \mid m$ or $p \mid n$.

Proof.
1. Suppose p is prime and $p \mid mn$.
2. Suppose $p \nmid m$.

3. Then $\gcd(m, p) = 1$ by Exercise 8.4.6.
4. Apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $1 = \gcd(m, p) = ms + pt$.
5. Multiplying through by n gives $n = nms + npt = s(mn) + (nt)p$.
6. Since $p \mid mn$ by assumption and $p \mid p$, the Closure Lemma implies $p \mid n$. □

Corollary 8.5.6. Let $n, m_0, m_1, \dots, m_n, p \in \mathbb{Z}^+$. If p is prime and $p \mid m_0 m_1 \dots m_n$, then $p \mid m_i$ for some $i \in \{0, 1, \dots, n\}$.

Definition 8.5.7. A *prime factorization* of an integer n is a way of writing n as a product of primes.

Example 8.5.8. (1) A prime factorization of 100 is $2 \times 2 \times 5 \times 5 = 2^2 5^2$.

(2) A prime factorization of 641 is 641.

Theorem 8.5.9 (Fundamental Theorem of Arithmetic, aka Prime Factorization Theorem)**.** Every integer $n \geqslant 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.

Remark 8.5.10. (1) The uniqueness part of the theorem above becomes false if we omit the "nondecreasing order" requirement, because 2×5 and 5×2 are different prime factorizations of 10.

(2) The uniqueness part of the theorem above becomes false if we allowed 1 to be "prime", because then 2×5 and $1 \times 2 \times 5$ would be different "prime factorizations" of 10 in which the "prime factors" are arranged in nondecreasing order.

Proof. 1. (Existence) We show this by Strong Mathematical Induction.

1.1. For each $n \in \mathbb{Z}_{\geqslant 2}$, let $P(n)$ be the proposition "n has a prime factorization".
1.2. (Base step)
  1.2.1. 2 is a prime factorization of 2 because 2 is prime.
  1.2.2. So $P(2)$ is true.
1.3. (Induction step)
  1.3.1. Let $k \in \mathbb{Z}_{\geqslant 2}$ such that $P(2), P(3), \dots, P(k)$ are true.
  1.3.2. If $k + 1$ is prime, then $k + 1$ is a prime factorization of $k + 1$.
  1.3.3. So suppose $k + 1$ is not prime. Then $k + 1$ is composite.
  1.3.4. Use Lemma 8.2.4 to find $d \mid k + 1$ such that $1 < d < k + 1$.
  1.3.5. Use the definition of divisibility to find $e \in \mathbb{Z}$ such that $k + 1 = de$.
  1.3.6. Since $d < k + 1 = de$, dividing through by d gives $1 < e$.
  1.3.7. Since $1 < d$, multiplying through by e gives $e < de = k + 1$.
  1.3.8. Combining lines 1.3.6 and 1.3.7 gives $1 < e < k + 1$.
  1.3.9. So both d and e have prime factorizations by the induction hypothesis.
  1.3.10. This implies $k + 1$ has a prime factorization, because $k + 1 = de$.
  1.3.11. So $P(k + 1)$ is true.
1.4. Thus $\forall n \in \mathbb{Z}_{\geqslant 2} \;\; P(n)$ is true by Strong MI.

2. (Uniqueness)

2.1. Suppose $n \in \mathbb{Z}_{\geqslant 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell. \tag{¶}$$

2.2. Now we cancel all the primes that are common to both sides of (¶).
2.3. We know that some primes are left on both sides because otherwise the two prime factorizations in (¶) are the same when arranged in nondecreasing order.
2.4. Let the result of the cancellation in line 2.2 be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}. \tag{‖}$$

2.5. No prime appears on both sides of (‖) since we cancelled out all of them.
2.6. We see from (‖) that $p'_0 \mid q'_0 q'_1 \dots q'_{\ell'}$.
2.7. Use Corollary 8.5.6 to find $i \in \{0, 1, \dots, \ell'\}$ such that $p'_0 \mid q'_i$.
2.8. Since q'_i is prime, its only positive divisors are 1 and q'_i. So $p'_0 = q'_i$ as $p'_0 \neq 1$.
2.9. Line 2.5 and line 2.8 contradict each other. □

8.6 Modular arithmetic

8.6.1 Congruence

Definition 8.6.1. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a *is congruent to* b *modulo* n if $a \underline{\mathrm{mod}}\, n = b \underline{\mathrm{mod}}\, n$. In this case, we write $a \equiv b \pmod{n}$.

Lemma 8.6.2 (alternative definitions of congruence)**.** The following are equivalent for all $a, b \in \mathbb{Z}$ and all $n \in \mathbb{Z}^+$.

(i) $a \equiv b \pmod{n}$.

(ii) $a = nk + b$ for some $k \in \mathbb{Z}$.

(iii) $n \mid (a - b)$.

Example 8.6.3. (1) $5 \equiv 1 \pmod{2}$ because $5 \underline{\mathrm{mod}}\, 2 = 1 = 1 \underline{\mathrm{mod}}\, 2$.

(2) $-2 \equiv 4 \pmod{3}$ because $-2 \underline{\mathrm{mod}}\, 3 = 1 = 4 \underline{\mathrm{mod}}\, 3$.

(3) $-4 \not\equiv 5 \pmod{7}$ because $-4 \underline{\mathrm{mod}}\, 7 = 3 \neq 5 = 5 \underline{\mathrm{mod}}\, 7$.

Remark 8.6.4. If we defined $a \underline{\mathrm{mod}} n$ to have the same sign as a for all $a \in \mathbb{Z}$ and all $n \in \mathbb{Z}^+$, then Example 8.6.3(2) above would fail; cf. Warning 8.1.18.

Proof. 1. ((i) ⇒ (ii))

1.1. Suppose $a \equiv b \pmod{n}$. By the definition of congruence-mod-n, this means $a \underline{\mathrm{mod}}\, n = b \underline{\mathrm{mod}}\, n$.

1.2. Let $r = a \underline{\mathrm{mod}}\, n$, so that $r = b \underline{\mathrm{mod}}\, n$ too.

1.3. Let $p = a \underline{\mathrm{div}}\, n$ and $q = b \underline{\mathrm{div}}\, n$, so that

$$a = np + r \quad \text{and} \quad b = nq + r.$$

1.4. Then $a = a - b + b = (np + r) - (nq + r) + b = n(p - q) + b$, where $p - q \in \mathbb{Z}$.

2. ((ii) ⇒ (iii))

2.1. Let $k \in \mathbb{Z}$ such that $a = nk + b$.

2.2. Then $a - b = nk$, where $k \in \mathbb{Z}$.

2.3. So $n \mid (a - b)$.

3. ((iii) ⇒ (i))

3.1. Suppose $n \mid (a - b)$.

3.2. Let $p = a \underline{\mathrm{div}}\, n$ and $r = a \underline{\mathrm{mod}}\, n$, and $q = b \underline{\mathrm{div}}\, n$ and $s = b \underline{\mathrm{mod}}\, n$.

3.3. Then $a - b = (np + r) - (nq + s) = n(p - q) + (r - s)$.

3.4. As $n \mid (a - b)$ and $n \mid n(p - q)$, the Closure Lemma implies $n \mid (r - s)$.

3.5. So $n \mid |r - s|$ by Lemma 8.1.9.

3.6. We know $0 \leqslant |r - s| < n$ because $0 \leqslant r < n$ and $0 \leqslant s < n$.

3.7. If $r - s \neq 0$, then Proposition 8.1.10 implies $n = |n| \leqslant |r - s| < n$, which is a contradiction. So $r - s = 0$.

3.8. Hence $a \underline{\mathrm{mod}}\, n = r = s = b \underline{\mathrm{mod}}\, n$. This says $a \equiv b \pmod{n}$. □

Lemma 8.6.5. Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

(1) (Reflexivity) $a \equiv a \pmod{n}$.

(2) (Symmetry) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(3) (Transitivity) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. 1. (Reflexivity) Since $a \underline{\mathrm{mod}}\, n = a \underline{\mathrm{mod}}\, n$, we know $a \equiv a \pmod{n}$.

2. (Symmetry) $a \equiv b \pmod{n} \Rightarrow a \,\underline{\mathrm{mod}}\, n = b \,\underline{\mathrm{mod}}\, n$
$\Rightarrow b \,\underline{\mathrm{mod}}\, n = a \,\underline{\mathrm{mod}}\, n \Rightarrow b \equiv a \pmod{n}$.

3. (Transitivity)
    3.1. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.
    3.2. Then $a \,\underline{\mathrm{mod}}\, n = b \,\underline{\mathrm{mod}}\, n$ and $b \,\underline{\mathrm{mod}}\, n = c \,\underline{\mathrm{mod}}\, n$.
    3.3. So $a \,\underline{\mathrm{mod}}\, n = c \,\underline{\mathrm{mod}}\, n$.
    3.4. This means $a \equiv c \pmod{n}$. □

8.6.2 Addition

Proposition 8.6.6. Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a + c \equiv b + d \pmod{n}$.

Proof. 1. Use Lemma 8.6.2(ii) to find $k, \ell \in \mathbb{Z}$ such that $a = nk + b$ and $c = n\ell + d$.
2. Then $a + c = (nk + b) + (n\ell + d) = n(k + \ell) + (b + d)$, where $k + \ell \in \mathbb{Z}$.
3. This implies $a + c \equiv b + d \pmod{n}$ by Lemma 8.6.2. □

Note 8.6.7. $\forall x \in \mathbb{Z}\ \ x + 0 \equiv x \pmod{n}$ for all $n \in \mathbb{Z}^+$.

Definition 8.6.8. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. The integer b is an *additive inverse of a modulo n* if $a + b \equiv 0 \pmod{n}$.

Example 8.6.9. (1) 1 is an additive inverse of 3 mod 4 as $3 + 1 = 4 \equiv 0 \pmod{4}$.

(2) -3 is an additive inverse of 3 mod 4 as $3 + (-3) = 0 \equiv 0 \pmod{4}$.

Proposition 8.6.10. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

(1) $-a$ is an additive inverse of a modulo n.

(2) b is an additive inverse of a modulo n if and only if $b \equiv -a \pmod{n}$.

Proof. (1) $a + (-a) = 0 \equiv 0 \pmod{n}$ by the reflexivity of congruence.

(2) 1. ("Only if") If b be an additive inverse of a modulo n, then

1.1. $a + b \equiv 0 \pmod{n}$ as b is an additive inverse of a;
1.2. $\equiv a + (-a) \pmod{n}$ as $-a$ is an additive inverse of a;
1.3. $\therefore\ -a + a + b \equiv -a + a + (-a) \pmod{n}$ by Proposition 8.6.6;
1.4. $\therefore\ b \equiv -a \pmod{n}$.

2. ("If") If $b \equiv -a \pmod{n}$, then b is an additive inverse of a modulo n because

2.1. $a + b \equiv a + (-a) \pmod{n}$ by Proposition 8.6.6;
2.2. $= 0$. □

Corollary 8.6.11. Let $n \in \mathbb{Z}^+$. If $a, b, c \in \mathbb{Z}$ such that $b + a \equiv c + a \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof. 1. If $b + a \equiv c + a \pmod{n}$, then

1.1. $b = b + a + (-a)$
1.2. $\equiv c + a + (-a) \pmod{n}$ by Proposition 8.6.6;
1.3. $= c$. □

Corollary 8.6.12. Let $a, b, x \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then $x + a \equiv b \pmod{n}$ if and only if $x \equiv b - a \pmod{n}$.

Proof. 1. ("Only if") If $x + a \equiv b \pmod{n}$, then

1.1.	$x = x + a + (-a)$	
1.2.	$\equiv b + (-a) \pmod{n}$	by Proposition 8.6.6;
1.3.	$= b - a$.	

2. ("If") If $x \equiv b - a \pmod{n}$, then

2.1.	$x + a \equiv b - a + a \pmod{n}$	by Proposition 8.6.6;
2.2.	$= b$.	□

8.6.3 Multiplication

Proposition 8.6.13. Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $ac \equiv bd \pmod{n}$.

Proof. 1. Use Lemma 8.6.2(ii) to find $k, \ell \in \mathbb{Z}$ such that $a = nk + b$ and $c = n\ell + d$.
2. Then $ac = (nk + b)(n\ell + d) = n(nk\ell + kd + b\ell) + bd$, where $nk\ell + kd + b\ell \in \mathbb{Z}$.
3. This implies $ac \equiv bd \pmod{n}$ by Lemma 8.6.2. □

Note 8.6.14. $\forall x \in \mathbb{Z}\ \ x1 \equiv x \pmod{n}$ for all $n \in \mathbb{Z}^+$.

Definition 8.6.15. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. A *multiplicative inverse of a modulo n* is an integer b such that $ab \equiv 1 \pmod{n}$.

Proposition 8.6.16. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.

(1) Let b, b' be multiplicative inverses of a. Then $b \equiv b' \pmod{n}$.

(2) Let b be a multiplicative inverse of a and $b' \in \mathbb{Z}$ such that $b \equiv b' \pmod{n}$. Then b' is also a multiplicative inverse of a.

Proof. (1)

1.	$ab \equiv 1 \pmod{n}$	as b is a multiplicative inverse of a;
2.	$\equiv ab' \pmod{n}$	as b' is a multiplicative inverse of a;
3. $\therefore$	$b'ab \equiv b'ab' \pmod{n}$	by Proposition 8.6.13;
4. $\therefore$	$b \equiv b' \pmod{n}$	by Proposition 8.6.13, as $ab' \equiv 1 \pmod{n}$.

(2)

1.	$ab' \equiv ab \pmod{n}$	by Proposition 8.6.13, as $b \equiv b' \pmod{n}$;
2.	$\equiv 1 \pmod{n}$	as b is a multiplicative inverse of a. □

Example 8.6.17. (1) 5 is a multiplicative inverse of 5 modulo 6 because $5 \times 5 = 25 \equiv 1 \pmod{6}$.

(2) 11 is a multiplicative inverse of 5 modulo 6 because $5 \times 11 = 55 \equiv 1 \pmod{6}$.

(3) 2 does not have a multiplicative inverse modulo 6.

Definition 8.6.18. Two integers a, n are *coprime* if $\gcd(a, n) = 1$.

Theorem 8.6.19. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a has a multiplicative inverse modulo n if and only if a and n are coprime.

Proof. 1. ("Only if")
1.1. Let b be a multiplicative inverse of a modulo n.
1.2. Then $ab \equiv 1 \pmod{n}$ by the definition of multiplicative inverses.
1.3. Use Lemma 8.6.2(ii) to find $k \in \mathbb{Z}$ such that $ab = nk + 1$.
1.4. Let $d = \gcd(a, n)$. Note that $d \geqslant 1$, and $d \mid a$ and $d \mid n$.
1.5. Then the Closure Lemma implies $d \mid ba + (-k)n = 1$.

1.6. So $1 \leqslant d = |d| \leqslant |1| = 1$ by Proposition 8.1.10.

1.7. Hence $\gcd(a, n) = d = 1$.

2. ("If")

2.1. Suppose $\gcd(a, n) = 1$.

2.2. Use Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $1 = \gcd(a, n) = as + nt$.

2.3. Then $as = 1 - nt = n(-t) + 1$, where $-t \in \mathbb{Z}$.

2.4. So $as \equiv 1 \pmod{n}$ by Lemma 8.6.2.

2.5. This says s is a multiplicative inverse of a modulo n. □

Note 8.6.20. The proof above actually gives an algorithm for finding multiplicative inverses modulo n.

Example 8.6.21. Find a multiplicative inverse of 7 modulo 12.

Solution. Apply the Euclidean Algorithm:

$$\begin{array}{rcrl}
12 \ \underline{\text{mod}}\ 7 = 5 & \dashleftarrow & 5 = 12 - 7 \times 1 & (1) \\
7 \ \underline{\text{mod}}\ 5 = 2 & \dashleftarrow & 2 = \ \ 7 - 5 \times 1 & (2) \\
5 \ \underline{\text{mod}}\ 2 = 1 & \dashleftarrow & 1 = \ \ 5 - 2 \times 2 & (3) \\
2 \ \underline{\text{mod}}\ 1 = 0 & & &
\end{array}$$

Hence
$$\begin{aligned}
\gcd(12, 7) = 1 &= 5 - 2 \times 2 && \text{by (3);} \\
&= 5 - (7 - 5 \times 1) \times 2 && \text{by (2);} \\
&= 7 \times (-2) + 5 \times 3 && \\
&= 7 \times (-2) + (12 - 7 \times 1) \times 3 && \text{by (1);} \\
&= 12 \times 3 + 7 \times (-5) && \\
&\equiv 7 \times (-5) \pmod{12}. &&
\end{aligned}$$

Hence -5 is a multiplicative inverse of 7 modulo 12. In view of Proposition 8.6.16(2), this implies $7, 19, 31, \ldots$ are all multiplicative inverses of 7 modulo 12.

Corollary 8.6.22. Let $n \in \mathbb{Z}^+$. If $a, c, d \in \mathbb{Z}$ such that $ca \equiv da \pmod{n}$ and $\gcd(a, n) = 1$, then $c \equiv d \pmod{n}$.

Proof. 1. Use Theorem 8.6.19 to find a multiplicative inverse b of a modulo n.

2. Then $c = c \cdot 1$

3. $\equiv (ca)b \pmod{n}$ as b is a multiplicative inverse of a modulo n;

4. $\equiv (da)b \pmod{n}$ as $ca \equiv da \pmod{n}$;

5. $\equiv d \cdot 1 \pmod{n}$ as b is a multiplicative inverse of a modulo n;

6. $= d$. □

Corollary 8.6.23. Let $n \in \mathbb{Z}^+$. Suppose $a, b, c \in \mathbb{Z}$, where b is a multiplicative inverse of a modulo n. Then
$$ax \equiv c \pmod{n} \quad \Leftrightarrow \quad x \equiv bc \pmod{n}.$$

Proof. 1. ($\Rightarrow$) If $ax \equiv c \pmod{n}$, then

1.1. $x = 1 \cdot x$

1.2. $\equiv (ab)x \pmod{n}$ as b is a multiplicative inverse of a modulo n;

1.3. $= b(ax)$

1.4. $\equiv bc \pmod{n}$ as $ax \equiv c \pmod{n}$.

2. ($\Leftarrow$) If $x \equiv bc \pmod{n}$, then

2.1. $ax \equiv a(bc) \pmod{n}$ by Proposition 8.6.13, as $x \equiv bc \pmod{n}$;

2.2. $\equiv 1 \cdot c \pmod{n}$ as b is a multiplicative inverse of a modulo n;

2.3. $= c$. □

To solve the equation $ax \equiv c \pmod{n}$**, where** $\gcd(a, n) = 1$**.** (1) Find a multiplicative inverse b of a modulo n.

- This can be done either by trial and error, or by using the Euclidean Algorithm as in the proofs of Bézout's Lemma and Theorem 8.6.19.

(2) The solution is $x \equiv bc \pmod{n}$.

Example 8.6.24. To solve $7x \equiv 2 \pmod{12}$:

(1) We know from Example 8.6.21 that -5 is a multiplicative inverse of 7 modulo 12.

(2) The solution is

$$\begin{aligned} x &\equiv -5 \times 2 \pmod{12} \\ &= -10 \\ &\equiv 2 \pmod{12}. \end{aligned}$$

Example 8.6.25. Solve $26x \equiv 9 \pmod{35}$.

Solution. Apply the Euclidean Algorithm:

$$\begin{array}{rcl} 35 \,\underline{\text{mod}}\, 26 = 9 & \dashleftarrow & 9 = 35 - 26 \times 1 \qquad (1) \\ 26 \,\underline{\text{mod}}\, 9 = 8 & \dashleftarrow & 8 = 26 - 9 \times 2 \qquad (2) \\ 9 \,\underline{\text{mod}}\, 8 = 1 & \dashleftarrow & 1 = 9 - 8 \times 1 \qquad (3) \\ 8 \,\underline{\text{mod}}\, 1 = 0 & & \end{array}$$

Hence

$$\begin{aligned} \gcd(35, 26) = 1 &= 9 - 8 \times 1 && \text{by } (3); \\ &= 9 - (26 - 9 \times 2) \times 1 && \text{by } (2); \\ &= 26 \times (-1) + 9 \times 3 \\ &= 26 \times (-1) + (35 - 26 \times 1) \times 3 && \text{by } (1); \\ &= 35 \times 3 + 26 \times (-4) \\ &\equiv 26 \times (-4) \pmod{35}. \end{aligned}$$

Hence -4 is a multiplicative inverse of 26 modulo 35. Thus the solution to the congruence equation is

$$\begin{aligned} x &\equiv -4 \times 9 \pmod{35} \\ &= -36 \\ &\equiv 34 \pmod{35}. \end{aligned}$$