Section 8.6: Modular arithmetic

CS1231S Discrete Structures

Wong Tin Lok

National University of Singapore

9 October 2020

Question

Which of the following are true for all $a, b, m, n \in \mathbb{Z}^+$?

1. $((a \underline{\text{mod}}\ n) + (b \underline{\text{mod}}\ n)) \underline{\text{mod}}\ n = (a + b) \underline{\text{mod}}\ n$. ✓ Proposition 8.6.6
2. $((a \underline{\text{mod}}\ m) + (a \underline{\text{mod}}\ n)) \underline{\text{mod}}\ (m + n) = a \underline{\text{mod}}\ (m + n)$. $a = m = n = 1$?
3. $((a \underline{\text{mod}}\ n) \times (b \underline{\text{mod}}\ n)) \underline{\text{mod}}\ n = (a \times b) \underline{\text{mod}}\ n$. ✓ Proposition 8.6.13
4. $((a \underline{\text{mod}}\ m) \times (a \underline{\text{mod}}\ n)) \underline{\text{mod}}\ (m \times n) = a \underline{\text{mod}}\ (m \times n)$. $a = m = n = 2$?

Answer at `https://pollev.com/wtl/`.

Towards a proof of the Fundamental Theorem of Arithmetic

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

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

Algorithm 8.4.8 (Euclidean Algorithm)

Let $m, n \in \mathbb{Z}$ such that $m \geqslant n > 0$. Set

$$r_1 := m \,\underline{\mathrm{mod}}\, n, \quad r_2 := n \,\underline{\mathrm{mod}}\, r_1, \quad r_3 := r_1 \,\underline{\mathrm{mod}}\, r_2, \quad \ldots, \quad r_{k+1} := r_{k-1} \,\underline{\mathrm{mod}}\, r_k,$$

where $r_k \neq 0$ but $r_{k+1} = 0$. Then $\gcd(m, n) = r_k$.

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = ms + nt$.

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 $p \mid n$.

Theorem 8.5.9 (Fundamental Theorem of Arithmetic; Prime Factorization Theorem)

Every integer $n \geqslant 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.

Motivation

+	even	odd
even	even	odd
odd	odd	even

$\times$	even	odd
even	even	even
odd	even	odd

Aim

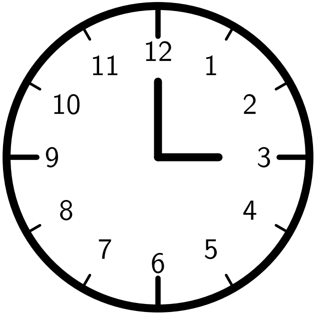
To formalize and generalize

- the arithmetic of the even and the odd; and
- clock arithmetic.

Plan

- congruence
- addition and multiplication
- subtraction and division

Search for "RSA cryptosystem".



We have concluded that the trivial mathematics is, on the whole, useful, and that the real mathematics, on the whole, is not.

G.H. Hardy

Congruence (1/4)

Definition 8.1.1: $d \mid n \quad \Leftrightarrow \quad n = dk$ for some $k \in \mathbb{Z}$.

Definition 8.6.1

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then *a is congruent to b modulo n* if $a \operatorname{\underline{mod}} n = b \operatorname{\underline{mod}} n$. 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 $n \in \mathbb{Z}^+$.

↳ TFAE

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

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

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

$$\begin{array}{ccc} & \text{(ii)} & \\ \Nearrow & & \Searrow \\ \text{(i)} & \Leftarrow & \text{(iii)} \end{array}$$

Example 8.6.3

(1) $5 \equiv 1 \pmod{2}$ because $5 \operatorname{\underline{mod}} 2 = 1 = 1 \operatorname{\underline{mod}} 2$.

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

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

Remark 8.6.4. If we defined $a \operatorname{\underline{mod}} n$ to have the same sign as a for all $a \in \mathbb{Z}$ and all $n \in \mathbb{Z}^+$, then this would fail.

Congruence (2/4)

Definition 8.1.1: $d \mid n \quad \Leftrightarrow \quad n = dk$ for some $k \in \mathbb{Z}$.

Definition 8.6.1

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

Lemma 8.6.2 (alternative definitions of congruence)

$$\begin{tikzcd} & \text{(ii)} \arrow[dr, Rightarrow] & \\ \text{(i)} \arrow[ur, Rightarrow] & & \text{(iii)} \arrow[ll, Rightarrow] \end{tikzcd}$$

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

Proof of (i) $\Rightarrow$ (ii)

1.1. Suppose $a \equiv b \pmod{n}$. By definition, this means $a \,\underline{\text{mod}}\, n = b \,\underline{\text{mod}}\, n$.

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

1.3. Let $p = a \,\underline{\text{div}}\, n$ and $q = b \,\underline{\text{div}}\, n$, 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 $p - q \in \mathbb{Z}$. $\square$

Congruence (3/4)

> Definition 8.1.1: $d \mid n \quad \Leftrightarrow \quad n = dk$ for some $k \in \mathbb{Z}$.

Definition 8.6.1

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

Lemma 8.6.2 (alternative definitions of congruence)

$$\begin{tikzcd} & \text{(ii)} \arrow[dr, Rightarrow] & \\ \text{(i)} \arrow[ur, Rightarrow] & & \text{(iii)} \arrow[ll, Rightarrow] \end{tikzcd}$$

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

Proof of (ii) $\Rightarrow$ (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 $n \mid (a - b)$. $\square$

Congruence (4/4)

Definition 8.1.1: $d \mid n \quad \Leftrightarrow \quad n = dk$ for some $k \in \mathbb{Z}$.

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

$$\begin{array}{ccc} & \text{(ii)} & \\ \Nearrow & & \Searrow \\ \text{(i)} & \Leftarrow & \text{(iii)} \end{array}$$

Proof of (iii) $\Rightarrow$ (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 $a \equiv b \pmod{n}$. □

Prop 8.1.10

$d \mid n \wedge n \neq 0$

$\Rightarrow |d| \leq |n|$

Reflexivity, symmetry, and transitivity

Definition 8.6.1

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

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 $a \underline{\bmod} n = a \underline{\bmod} n$, we know $a \equiv a \pmod{n}$.
2. (Symmetry)
$$\begin{aligned} a \equiv b \pmod{n} \quad &\Rightarrow \quad a \underline{\bmod} n = b \underline{\bmod} n \\ &\Rightarrow \quad b \underline{\bmod} n = a \underline{\bmod} n \quad \Rightarrow \quad b \equiv a \pmod{n}. \end{aligned}$$
3. (Transitivity) 3.1. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

   3.2. Then $a \underline{\bmod} n = b \underline{\bmod} n$ and $b \underline{\bmod} n = c \underline{\bmod} n$.

   3.3. So $a \underline{\bmod} n = c \underline{\bmod} n$.

   3.4. This means $a \equiv c \pmod{n}$. $\square$

Addition

Definition 8.6.1

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then *a is congruent to b modulo n* if $a \underline{\bmod} n = b \underline{\bmod} n$. 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) $n \mid (a - b)$.

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. $\square$

Multiplication

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

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 $ac = (nk + b)(n\ell + d) = n(nk\ell + kd + b\ell) + bd$.
3. This implies $ac \equiv bd \pmod{n}$ by Lemma 8.6.2.

$\square$

Additive inverse

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 $b \equiv -a \pmod{n}$.

Multiplicative inverse (1/3)

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 $n \in \mathbb{Z}^+$.

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 $ac \equiv bd \pmod{n}$.

(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 of (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 $ab' \equiv 1 \pmod{n}$. $\square$

Multiplicative inverse (2/3)

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 $n \in \mathbb{Z}^+$.

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 $ac \equiv bd \pmod{n}$.

(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 of (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. $\square$

Multiplicative inverse (3/3)

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 8.6.13. 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 $ac \equiv bd \pmod{n}$.

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.

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.

Multiplicative inverse — existence (1/2)

Closure Lemma. Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

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 $ab \equiv 1 \pmod{n}$.

Lemma 8.6.2. 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) $n \mid (a - b)$.

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

a and n are *coprime*.

Proof of the "only if" part

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

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

Multiplicative inverse — existence (2/2)

An algorithm for finding multiplicative inverses modulo n.

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 $ab \equiv 1 \pmod{n}$.

Lemma 8.6.2. 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) $n \mid (a - b)$.

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

a and n are *coprime*.

Proof of the "if" part

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. □

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = ms + nt$.

Finding multiplicative inverses

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:

$$\begin{aligned}
12 \operatorname{\underline{mod}} 7 &= 5 & \leftarrow\text{--} \quad 5 &= 12 - 7 \times 1 & (1)\\
7 \operatorname{\underline{mod}} 5 &= 2 & \leftarrow\text{--} \quad 2 &= \ \ 7 - 5 \times 1 & (2)\\
5 \operatorname{\underline{mod}} 2 &= 1 & \leftarrow\text{--} \quad 1 &= \ \ 5 - 2 \times 2 & (3)\\
2 \operatorname{\underline{mod}} 1 &= 0
\end{aligned}$$

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.

Summary

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

What we saw

- congruence modulo n;
- addition, multiplication and subtraction make sense;
- division is not always possible.

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

1. We know -5 is a multiplicative inverse of 7 modulo 12.
2. The solution is $x \equiv -5 \times 2 \pmod{12} = -10$
$$\equiv 2 \pmod{12}.$$

Next: equivalence relations

Theorem 8.6.19

a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.

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 proof of Bézout's Lemma and Theorem 8.6.19.

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

- Note $\quad ax \equiv c \pmod{n} \quad \Leftrightarrow \quad x \equiv bax \equiv bc \pmod{n}$.