1. Modular arithmetic.

A. Ushakov

MA503, September 7

Contents

This course provides an introduction to the theory of public key cryptography and to the mathematical ideas underlying that theory.

- Division with a remainder.
- Division is correctly defined.
- Divisibility.
- Properties of divisibility.
- Greatest common divisor.
- Euclidean algorithm.
- Bezout's identity.
- Integral linear combinations of a and b.
- Prime numbers.
- Properties of prime numbers.
- Prime power factorization.
- Fundamental theorem of arithmetic.
- Linear Diophantine equations. Examples.
- Least common multiple.
- Congruence modulo n. Properties.
- Congruence class.
- Arithmetic of congruences.

Integer numbers

Natural numbers *are numbers used in counting,* $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

The set of **integer numbers** *consists of natural numbers, negative natural numbers and zero*

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

We work with two binary operations on $\mathbb{Z}$:

- addition, $+$
- multiplication, $\cdot$

The set $\mathbb{Z}$ is naturally ordered, for $a, b \in \mathbb{Z}$:

$$a < b \quad \Leftrightarrow \quad b - a \in \mathbb{N}.$$

Properties of integers

Properties of integers, for every $a, b, c \in \mathbb{Z}$	
(1) Associativity of addition	$a + (b + c) = (a + b) + c$
(2) Associativity of multiplication	$a(bc) = (ab)c$;
(3) Commutativity of addition	$a + b = b + a$;
(4) Commutativity of multiplication	$ab = ba$;
(5) Distributivity	$a(b + c) = ab + ac$;
(6) Properties of 0	$0 + a = a$, $0 \cdot a = 0$;
(7) Properties of 1	$1 \cdot a = a$;
(8) Properties of negation	$-(-a) = a$, $a(-b) = -(ab)$, $(-a)(-b) = ab$;
(9) No zero divisors	$ab = 0$ implies $a = 0$ or $b = 0$.

Properties of $\mathbb{N}$	
(10) Induction principle	$P(1) \ \wedge \ \forall i,\ P(i) \rightarrow P(i+1)$ implies $\forall i,\ P(i)$.
(11) Well-ordering principle	Every nonempty subset of $\mathbb{N}$ has the least element.

Based on these axioms we develop divisibility theory for integers.

Division with a remainder

Let $a, b \in \mathbb{Z}$ and $b \neq 0$.

Definition

To **divide a by b** means to find $q, r \in \mathbb{Z}$ such that

$$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < |b|. \tag{1}$$

We call q the **quotient** and r the **remainder** of division.

- Dividing 7 by 3 we get the quotient 2 and the remainder 1 because
$$7 = 3 \cdot 2 + 1 \text{ and } 0 \leq 1 < |3|.$$
- Dividing -7 by 3 we get the quotient -3 and the remainder 2 because
$$-7 = 3 \cdot (-3) + 2 \text{ and } 0 \leq 2 < |3|.$$
(Remember that the remainder must be non-negative!)
- Dividing -7 by -3 we get the quotient 3 and the remainder 2 because
$$-7 = (-3) \cdot 3 + 2 \text{ and } 0 \leq 2 < |-3|.$$
- Division by 0 makes no sense!

Division is possible!

Theorem

For any $a, b \in \mathbb{Z}$ with $b \neq 0$ there exists a unique pair $q, r \in \mathbb{Z}$ such that:

$$a = b \cdot q + r \quad \textit{and} \quad 0 \leq r < b.$$

Proof. Assuming $a \geq 0$ and $b \geq 0$ (other cases are similar).

Existence:

- Define a "set of potential remainders" $S = \{a - qb \mid q \in \mathbb{Z} \text{ and } a - qb \geq 0\} \subseteq \mathbb{N} \cup \{0\}$.
- $a \in S \quad \Rightarrow \quad S \neq \emptyset \quad \Rightarrow \quad S$ contains the least element r.
- $r \in S \quad \Rightarrow \quad r = a - qb$ for some $q \in \mathbb{Z} \quad \Rightarrow \quad a = qb + r$.
- If $r \geq b$, then $r - b = a - (q+1)b \geq 0$ belongs to S and is smaller than r. That contradicts our choice of r.
- Hence, $r < b$ and (q, r) is a required pair. $\square$

Division is possible!

Theorem

For any $a, b \in \mathbb{Z}$ with $b \neq 0$ there exists a unique pair $q, r \in \mathbb{Z}$ such that:

$$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < b.$$

Proof. Assuming $a \geq 0$ and $b \geq 0$ (other cases are similar).

Uniqueness:

- Assume that (q_1, r_1) and (q_2, r_2) satisfy (1).
- On the way to contrary assume that $r_1 \neq r_2$, e.g., $r_1 > r_2$. Then

  $$a = q_1 b + r_1 = q_2 b_2 + r_2.$$

  Hence,

  $$r_1 - r_2 = (q_2 - q_1)b \quad \text{and} \quad 0 < r_1 - r_2 < b,$$

  which is impossible (b does not divide any integer in the set $\{1, \ldots, b-1\}$).
- Thus, $r_1 = r_2$ and $q_1 = q_2$. $\square$

Divisibility

Let $a, b \in \mathbb{Z}$ and $b \neq 0$.

Definition (Divisibility)

We say that b **divides** a and write $b \mid a$ if $a = bq$ for some $q \in \mathbb{Z}$.

- b is a **divisor** (factor) of a;
- a is a **multiple** of b.

Every nontrivial $n \in \mathbb{Z}$ has finitely many divisors.

For instance:

- 6 has divisors $\pm 1, \pm 2, \pm 3, \pm 6$.
- -21 has divisors $\pm 1, \pm 3, \pm 7, \pm 21$.

Divisibility properties-I (can be skipped)

Proposition (Transitivity)

For any $a, b, c \in \mathbb{Z}$ if $a \mid b$ and $b \mid c$, then $a \mid c$;

$$\begin{array}{l} a \mid b \\ b \mid c \end{array} \quad \Rightarrow \quad \begin{array}{l} b = aq_1 \\ c = bq_2 \end{array} \quad \Rightarrow \quad c = a \cdot q_1 q_2 \quad \Rightarrow \quad a \mid c.$$

Proposition

For any $a, b, c, d \in \mathbb{Z}$ if $a \mid b$ and $c \mid d$, then $ac \mid bd$;

$$\begin{array}{l} a \mid b \\ c \mid d \end{array} \quad \Rightarrow \quad \begin{array}{l} b = aq_1 \\ d = cq_2 \end{array} \quad \Rightarrow \quad bd = ac \cdot q_1 q_2 \quad \Rightarrow \quad ac \mid bd.$$

Proposition

If $m \neq 0$, then for any $a, b \in \mathbb{Z}$ $(a \mid b \Leftrightarrow am \mid bm)$;

Proof for $a \mid b \Rightarrow am \mid bm$:

$$a \mid b \quad \Rightarrow \quad b = qa \quad \Rightarrow \quad bm = q \cdot am \quad \Rightarrow \quad am \mid bm$$

Proof for $a \mid b \Leftarrow am \mid bm$: (proving the contropositive statement):

$$\begin{aligned} a \nmid b \quad &\Rightarrow \quad b = qa + r, \text{ s.t. } 0 < r < a \\ &\Rightarrow \quad mb = qam + rm, \text{ s.t. } 0 < rm < am \\ &\Rightarrow \quad am \nmid bm. \end{aligned}$$

Divisibility properties-II

Proposition

For any $a, b \in \mathbb{Z}$ *if* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

Every nontrivial multiple b of a satisfies $|a| \leq |b|$:

$$\ldots, -4a, -3a, -2a, -a, 0, a, 2a, 3a, 4a, \ldots$$

Proposition

Let $c \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{Z}$, *and* $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$. *If* $c \mid a_i$ *for every* $i = 1, \ldots, n$, *then* $c \mid (\alpha_1 a_1 + \ldots + \alpha_n a_n)$.

$$\begin{array}{lcl} c \mid a_1 & & a_1 = q_1 c \\ \ldots & \Rightarrow & \ldots \\ c \mid a_n & & a_n = q_n c \end{array} \Rightarrow \alpha_1 a_1 + \ldots + \alpha_n a_n = \alpha_1 q_1 c + \ldots + \alpha_n q_n c = c(\alpha_1 q_1 + \ldots + \alpha_n q_n)$$

Greatest common divisor

Definition

d is a **common divisor** of a and b if $d \mid a$ and $d \mid b$.

Definition

d is the **greatest common divisor** of a and b if $d \mid a$ and $d \mid b$ and d is the greatest number with this property.

We can find $\gcd(a, b)$ using the definition for small a, b, namely, we can enumerate all divisors of a and b and choose the greatest common divisor.

- $\gcd(2, 3) = 1$,
- $\gcd(8, 12) = 4$,
- $\gcd(-6, 12) = 6$,
- $\gcd(-15, 120, 25) = 5$,
- $\gcd(0, -15, 120, 25) = 5$,
- $\gcd(0, 0)$ is not defined because every nontrivial integer divides 0.
  (In some books $\gcd(0, 0) = 0$!)

For large a, b this approach is inefficient: it requires factorization of a and b which is computationally hard.

Euclidean algorithm

(Euclidean Lemma)

$b = qa + r \quad \Rightarrow \quad \gcd(a, b) = \gcd(a, r).$

d is a common divisor for (a, b) $\quad \Leftrightarrow \quad$ d is a common divisor for $(a, b - qa)$.

(The Euclidean algorithm to compute $\gcd(a, b)$)

Assuming $|b| \geq |a|$

$$
\begin{aligned}
b &= q_1 \cdot a + r_1 & \Rightarrow \quad \gcd(a, b) &= \gcd(a, r_1), & \textit{where } r_1 < |a| \leq |b| \\
a &= q_2 \cdot r_1 + r_2 & &= \gcd(r_2, r_1), & \textit{where } r_2 < r_1 < |a| \\
r_1 &= q_3 \cdot r_2 + r_3 & &= \gcd(r_2, r_3), & \textit{where } r_3 < r_2 < r_1 \\
&\dots & & & \\
r_{k-2} &= q_k \cdot r_{k-1} + r_k = 0 & &= \gcd(r_{k-1}, 0) = r_{k-1}. &
\end{aligned}
$$

For instance,

$$
\begin{aligned}
8 &= 1 \cdot 5 + 3 & \Rightarrow \quad \gcd(8, 5) &= \gcd(3, 5) \\
5 &= 1 \cdot 3 + 2 & &= \gcd(3, 2) \\
3 &= 1 \cdot 2 + 1 & &= \gcd(1, 2) \\
2 &= 2 \cdot 1 + 0 & &= \gcd(1, 0) = 1.
\end{aligned}
$$

The number of steps k is bounded by $\log_2(|a|) + \log_2(|b|)$.

Bezout's identity

Bezout's identity claims that $\gcd(a, b)$ can be expressed as an integral linear combination of a and b.

Theorem (Bezout's identity)

For any $a, b \in \mathbb{Z}$ (not both trivial) $\gcd(a, b) = \alpha a + \beta b$ *for some $\alpha, \beta \in \mathbb{Z}$!*

E.g., for $a = 5, b = 8$ we have $\gcd(5, 8) = 1 = (-3) \cdot 5 + 2 \cdot 8$ and so $\alpha = -3, \beta = 2$.

α, β are not uniquely defined for a, b.

E.g., for $a = 5, b = 8$ we have

$$\begin{aligned} \gcd(5, 8) = 1 &= (-3) \cdot 5 + 2 \cdot 8 && (\alpha = -3, \beta = 2) \\ &= 5 \cdot 5 + (-3) \cdot 8 && (\alpha = 5, \beta = -3) \\ &= 13 \cdot 5 + (-8) \cdot 8 && (\alpha = 13, \beta = -8) \\ &= \text{etc.} \end{aligned}$$

To find α and β one can use computations produced by the Euclidean algorithm.

See worked out examples below.

Bezout's identity: worked out example-I

Example

For $a = 8$ and $b = 5$, using the Euclidean algorithm compute $\gcd(8, 5)$:

$$
\begin{aligned}
8 &= 1 \cdot 5 + 3 & \Rightarrow \quad \gcd(8,5) &= \gcd(3,5) \\
5 &= 1 \cdot 3 + 2 & &= \gcd(3,2) \\
3 &= 1 \cdot 2 + 1 & &= \gcd(1,2) \\
2 &= 2 \cdot 1 + 0 & &= \gcd(1,0) = 1
\end{aligned}
$$

Then, express 1 as an integral linear combination of 5 and 8:

$$
\begin{aligned}
1 &= 1 \cdot 3 - 1 \cdot 2 & &\text{(combination of 2 and 3)} \\
&= 1 \cdot 3 - 1 \cdot (5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3 & &\text{(combination of 3 and 5)} \\
&= (-1) \cdot 5 + 2 \cdot (8 - 1 \cdot 5) = (-3) \cdot 5 + 2 \cdot 8 & &\text{(combination of 5 and 8).}
\end{aligned}
$$

Thus, $\alpha = 2$ and $\beta = -3$.

Be careful when you choose α and β. Remember that

- α is for a,
- β is for b.

Bezout's identity: worked out example-II

Example

For $a = 10$ and $b = 17$, using the Euclidean algorithm compute $\gcd(10, 17)$:

$$\begin{aligned} 17 &= 1 \cdot 10 + 7 & \Rightarrow \quad \gcd(10,17) &= \gcd(10,7) \\ 10 &= 1 \cdot 7 + 3 & &= \gcd(3,7) \\ 7 &= 2 \cdot 3 + 1 & &= \gcd(3,1) \\ 3 &= 3 \cdot 1 + 0 & &= \gcd(0,1) = 1. \end{aligned}$$

Then, express 1 as an integral linear combination of 17 and 10:

$$\begin{aligned} 1 &= 1 \cdot 7 - 2 \cdot 3 & &\text{(combination of 3 and 7)} \\ &= 1 \cdot 7 - 2 \cdot (10 - 1 \cdot 7) = (-2) \cdot 10 + 3 \cdot 7 & &\text{(combination of 7 and 10)} \\ &= (-2) \cdot 10 + 3 \cdot (17 - 1 \cdot 10) = (-5) \cdot 10 + 3 \cdot 17 & &\text{(combination of 10 and 17).} \end{aligned}$$

Thus, $\alpha = -5$ and $\beta = 3$.

Integral linear combinations of a and b

Let $a, b \in \mathbb{Z}$ (not both trivial).

Q. *What numbers can be expressed as integral linear combinations of a, b?*

For instance, if $a = 5$ and $b = 8$, then:

- $0 = 0 \cdot 5 + 0 \cdot 8$
- $1 = -3 \cdot 5 + 2 \cdot 8$
- $-1 = 3 \cdot 5 + -2 \cdot 8$
- $2 = -6 \cdot 5 + 4 \cdot 8$
- $-2 = 6 \cdot 5 + -4 \cdot 8$
- $3 = -1 \cdot 5 + 1 \cdot 8$

Every integer can be expressed as an integral linear combination of 5 and 8!

On the other hand, any integral linear combination of $a = 4$ and $b = 6$ is even. Hence, we cannot express odd numbers as integral linear combinations of 4 and 6!

Integral linear combinations of a and b

Fix $a, b \in \mathbb{Z}$. Let $c \in \mathbb{Z}$.

Theorem (Only multiples of $\gcd(a,b)$ can be expressed as $\alpha a + \beta b$)

$c = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$ $\quad \Leftrightarrow \quad \gcd(a,b) \mid c$.

"$\Rightarrow$" Suppose that $c = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. We have

- $\gcd(a,b) \mid a \quad \Rightarrow \quad a = q_1 \gcd(a,b)$.
- $\gcd(a,b) \mid b \quad \Rightarrow \quad b = q_2 \gcd(a,b)$.
- $c = \alpha a + \beta b = \alpha q_1 \gcd(a,b) + \beta q_2 \gcd(a,b) = \gcd(a,b)(\alpha q_1 + \beta q_2)$.
- Therefore, $\gcd(a,b) \mid c$.

"$\Leftarrow$" Suppose that $\gcd(a,b) \mid c$.

- Then $c = q \gcd(a,b) \overset{Bezout}{=} q(\alpha a + \beta b) = q\alpha \cdot a + q\beta \cdot b$
- So, c is an integral linear combination of a and b.

Corollary

$\gcd(a,b)$ is the least positive integer of the form $\alpha a + \beta b$.

Integers of the form $\alpha a + \beta b$ are multiples of $\gcd(a,b)$:

$$\ldots, \quad -2\gcd(a,b), \quad -\gcd(a,b), \quad 0, \quad \gcd(a,b), \quad 2\gcd(a,b), \quad 3\gcd(a,b), \quad \ldots$$

$\gcd(a,b)$ is the least positive number in that list.

Integral linear combinations of a and b

Fix $a, b \in \mathbb{Z}$. Let $c \in \mathbb{Z}$.

Theorem (Only multiples of $\gcd(a,b)$ can be expressed as $\alpha a + \beta b$)

$c = \alpha a + \beta b$ *for some* $\alpha, \beta \in \mathbb{Z} \quad \Leftrightarrow \quad \gcd(a,b) \mid c$.

"$\Rightarrow$" Suppose that $c = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. We have

- $\gcd(a,b) \mid a \quad \Rightarrow \quad a = q_1 \gcd(a,b)$.
- $\gcd(a,b) \mid b \quad \Rightarrow \quad b = q_2 \gcd(a,b)$.
- $c = \alpha a + \beta b = \alpha q_1 \gcd(a,b) + \beta q_2 \gcd(a,b) = \gcd(a,b)(\alpha q_1 + \beta q_2)$.
- Therefore, $\gcd(a,b) \mid c$.

"$\Leftarrow$" Suppose that $\gcd(a,b) \mid c$.

- Then $c = q \gcd(a,b) \stackrel{Bezout}{=} q(\alpha a + \beta b) = \mathrm{q}\alpha \cdot a + \mathrm{q}\beta \cdot b$
- So, c is an integral linear combination of a and b.

Corollary

$\gcd(a,b)$ *is the least positive integer of the form* $\alpha a + \beta b$.

Integers of the form $\alpha a + \beta b$ are multiples of $\gcd(a,b)$:

$$\ldots, \quad -2\gcd(a,b), \quad -\gcd(a,b), \quad 0, \quad \gcd(a,b), \quad 2\gcd(a,b), \quad 3\gcd(a,b), \quad \ldots$$

$\gcd(a,b)$ is the least positive number in that list.

Prime numbers

Definition

An integer $n > 1$ is called **prime** if 1 and n are its only divisors.
If $n > 1$ is not prime, then we say it is **composite**.

Prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

Definition

$a, b \in \mathbb{Z}$ are called **coprime** if $\gcd(a, b) = 1$.

Definition

$a_1, \ldots, a_n$ are **pairwise coprime** if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

For instance,

- $2, 3, 5, 7$ are pairwise coprime.
- $6, 35, 11$ are pairwise coprime.

Theorem

a, b are coprime $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. □

a, b are coprime $\Leftrightarrow$ $1 = \gcd(a, b)$ $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$.

Prime numbers

Definition

An integer $n > 1$ is called **prime** if 1 and n are its only divisors.
If $n > 1$ is not prime, then we say it is **composite**.

Prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

Definition

$a, b \in \mathbb{Z}$ are called **coprime** if $\gcd(a, b) = 1$.

Definition

$a_1, \ldots, a_n$ are **pairwise coprime** if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

For instance,

- $2, 3, 5, 7$ are pairwise coprime.
- $6, 35, 11$ are pairwise coprime.

Theorem

a, b are coprime $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. □

a, b are coprime $\Leftrightarrow$ $1 = \gcd(a, b)$ $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$.

Prime numbers

Definition

An integer $n > 1$ is called **prime** if 1 and n are its only divisors.
If $n > 1$ is not prime, then we say it is **composite**.

Prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.

Definition

$a, b \in \mathbb{Z}$ are called **coprime** if $\gcd(a, b) = 1$.

Definition

$a_1, \ldots, a_n$ are **pairwise coprime** if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

For instance,

- $2, 3, 5, 7$ are pairwise coprime.
- $6, 35, 11$ are pairwise coprime.

Theorem

a, b are coprime $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$. $\square$

a, b are coprime $\Leftrightarrow$ $1 = \gcd(a, b)$ $\Leftrightarrow$ $1 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$.

Properties of prime numbers

Let a, b be coprime and $c \in \mathbb{Z}$.

Proposition

If $a \mid bc$, then $a \mid c$.

$$\begin{aligned} a, b \text{ are coprime} \quad &\Rightarrow \quad 1 = \alpha a + \beta b \quad \text{for some } \alpha, \beta \in \mathbb{Z} \\ &\Rightarrow \quad c = \alpha ac + \beta bc \text{ is divisible by } a. \end{aligned}$$

Lemma

Assume p is prime and $a \in \mathbb{Z}$. Then either $p \mid a$ or a and p are coprime.

$$p \text{ is prime} \quad \Rightarrow \quad \gcd(a, p) = \begin{cases} 1 & \text{if } p \nmid a \quad \Rightarrow \quad a \text{ and } p \text{ are coprime,} \\ p & \text{if } p \mid a \end{cases}$$

Lemma

Assume p is prime and $b, c \in \mathbb{Z}$. If $p \mid bc$, then either $p \mid b$ or $p \mid c$.

- (Case-I) $p \mid b \quad \Rightarrow \quad$ we are done.
- (Case-II) $p \nmid b \quad \Rightarrow \quad p$ and b are coprime $\quad \Rightarrow \quad p \mid c$.

Corollary

Let p be a prime. If $p \mid a_1 \ldots a_n$, then $p \mid a_i$ for some $i = 1, \ldots, n$.

Properties of prime numbers

Let a, b be coprime and $c \in \mathbb{Z}$.

Proposition

If $a \mid bc$, then $a \mid c$.

$$a, b \text{ are coprime} \quad \Rightarrow \quad 1 = \alpha a + \beta b \quad \text{for some } \alpha, \beta \in \mathbb{Z}$$
$$\Rightarrow \quad c = \alpha a c + \beta b c \text{ is divisible by } a.$$

Lemma

Assume p is prime and $a \in \mathbb{Z}$. Then either $p \mid a$ or a and p are coprime.

$$p \text{ is prime} \quad \Rightarrow \quad \gcd(a, p) = \begin{cases} 1 & \text{if } p \nmid a \quad \Rightarrow \quad a \text{ and } p \text{ are coprime,} \\ p & \text{if } p \mid a \end{cases}$$

Lemma

Assume p is prime and $b, c \in \mathbb{Z}$. If $p \mid bc$, then either $p \mid b$ or $p \mid c$.

- (Case-I) $p \mid b \quad \Rightarrow \quad$ we are done.
- (Case-II) $p \nmid b \quad \Rightarrow \quad p$ and b are coprime $\quad \Rightarrow \quad p \mid c$.

Corollary

Let p be a prime. If $p \mid a_1 \dots a_n$, then $p \mid a_i$ for some $i = 1, \dots, n$.

Properties of prime numbers

Let a, b be coprime and $c \in \mathbb{Z}$.

Proposition

If $a \mid bc$, then $a \mid c$.

$$\begin{aligned} a, b \text{ are coprime} \quad &\Rightarrow \quad 1 = \alpha a + \beta b \quad \text{for some } \alpha, \beta \in \mathbb{Z} \\ &\Rightarrow \quad c = \alpha ac + \beta bc \text{ is divisible by } a. \end{aligned}$$

Lemma

Assume p is prime and $a \in \mathbb{Z}$. Then either $p \mid a$ or a and p are coprime.

$$p \text{ is prime} \quad \Rightarrow \quad \gcd(a, p) = \begin{cases} 1 & \text{if } p \nmid a \quad \Rightarrow \quad a \text{ and } p \text{ are coprime,} \\ p & \text{if } p \mid a \end{cases}$$

Lemma

Assume p is prime and $b, c \in \mathbb{Z}$. If $p \mid bc$, then either $p \mid b$ or $p \mid c$.

- (Case-I) $p \mid b \quad \Rightarrow \quad$ we are done.
- (Case-II) $p \nmid b \quad \Rightarrow \quad p$ and b are coprime $\quad \Rightarrow \quad p \mid c$.

Corollary

Let p be a prime. If $p \mid a_1 \dots a_n$, then $p \mid a_i$ for some $i = 1, \dots, n$.

Prime power factorization

Definition

Suppose that $n = p_1^{r_1} \dots p_k^{r_k}$, where p_i are distinct primes and $r_i \in \mathbb{N}$. The product $p_1^{r_1} \dots p_k^{r_k}$ is called the **prime power factorization** of n.

- $\mathrm{PPF}(2) = 2$,
- $\mathrm{PPF}(15) = 3 \cdot 5$,
- $\mathrm{PPF}(28) = 2^2 \cdot 7$,
- $\mathrm{PPF}(960) = 2^6 \cdot 3 \cdot 5$.

Lemma

For any $n > 1$ there exists a prime p such that $p \mid n$.

It is easy to see that the least number greater than 1 dividing n must be prime.

There are infinitely many prime numbers.

Fundamental theorem of arithmetic

Theorem

Each integer $n > 1$ has a prime power factorization (PPF)

$$\mathsf{n} = \mathsf{p}_1^{\mathsf{r}_1} \dots \mathsf{p}_\mathsf{k}^{\mathsf{r}_\mathsf{k}},$$

where p_i are distinct primes and $r_i \in \mathbb{N}$. This factorization is unique up to a permutation of factors.

Proof.

Existence of PPF(n)**.** Sufficient to express n as a product of prime numbers.

- If n is prime, then $\mathrm{PPF}(n) = n$.
- Otherwise, $n = p_1 n_1$, for some prime p_1 and $1 < n_1 < n$. If n_1 is prime, then we are done
- Otherwise, $n = p_1 p_2 n_2$, for some prime p_2 and $1 < n_2 < n_1$. If n_2 is prime, then we are done
- etc.
- Eventually, we express n as a product of prime numbers. □

Fundamental theorem of arithmetic

Theorem

Each integer $n > 1$ has a prime power factorization (PPF)

$$\mathsf{n} = \mathsf{p}_1^{\mathsf{r}_1} \dots \mathsf{p}_\mathsf{k}^{\mathsf{r}_\mathsf{k}},$$

where p_i are distinct primes and $r_i \in \mathbb{N}$. This factorization is unique up to a permutation of factors.

Proof.

Uniqueness. Sufficient to prove that equal products of prime numbers

$$p_1 \dots p_s = q_1 \dots q_t$$

have the same factors (up to a permutation).

- p_1 is prime and divides $q_1 \dots q_t$, hence it divides some q_i (wma $i = 1$). But q_1 is prime, which means that $p_1 = q_1$. Remove p_1 and q_1 from LHS and RHS to get $p_2 \dots p_s = q_2 \dots q_t$.
- p_2 is prime and divides $q_2 \dots q_t$, Arguing as before $p_2 = q_j$ for some j (wma $j = 2$).
- Continue the same way and see that the factors on the left and on the right are the same. □

Linear Diophantine equations

A **Diophantine equation** is an equation where only integer solutions are allowed. An equation $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are fixed integers and x, y are unknowns is called a **linear Diophantine equation**.

Theorem

Let $d = \gcd(a, b)$. A Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ in which case there are infinitely many solutions described as follows:

$$\begin{cases} x = x_0 + \frac{b}{d} n, \\ y = y_0 - \frac{a}{d} n, \end{cases} \qquad n \in \mathbb{Z},$$

where (x_0, y_0) is a particular solution.

For instance, later we will find a general solution for the equation $10x + 16y = 4$:

$$\begin{cases} x = -6 + 8n, \\ y = 4 - 5n, \end{cases}$$

Each value of n defines x and y, e.g.

- $n = -1 \quad \Rightarrow \quad x = -14, \ y = 9$
- $n = 0 \quad \Rightarrow \quad x = -6, \ y = 4$
- $n = 1 \quad \Rightarrow \quad x = 2, \ y = -1$
- $n = 2 \quad \Rightarrow \quad x = 10, \ y = -6$

So, the formula for x, y is a **parametrization** of the set of solutions using a **parameter** n.

Linear Diophantine equations: proof

Theorem

Let $d = \gcd(a, b)$. A Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ in which case there are infinitely many solutions described as follows:

$$\begin{cases} x = x_0 + \frac{b}{d}n, \\ y = y_0 - \frac{a}{d}n, \end{cases} \qquad n \in \mathbb{Z},$$

where (x_0, y_0) is a particular solution.

The pairs (x, y) defined above are solutions because

$$ax_0 + by_0 = c \quad \Rightarrow \quad a\big(x_0 + \tfrac{b}{d}n\big) + b\big(y_0 - \tfrac{a}{d}n\big) = c.$$

Conversely, if (x, y) is a solution, then

$$\begin{aligned} ax + by = c \quad &\Rightarrow \quad a(x - x_0) + b(y - y_0) = 0 \\ &\Rightarrow \quad a(x - x_0) = b(y_0 - y) \\ &\Rightarrow \quad \tfrac{a}{d}(x - x_0) = \tfrac{b}{d}(y_0 - y) \qquad\qquad \text{where } \gcd(\tfrac{a}{d}, \tfrac{b}{d}) = 1 \\ &\Rightarrow \quad \tfrac{b}{d} \mid x - x_0 \quad \Rightarrow \quad x = x_0 + \tfrac{b}{d}n \\ &\Rightarrow \quad y = y_0 - \tfrac{a}{d}n. \end{aligned}$$

Linear Diophantine equations: examples

1. Find a general solution for the linear Diophantine equation $10x + 16y = 4$.

- Use Euclidean algorithm to find $\gcd(10, 16) = 2$.
- (Bezout identity) $-3 \cdot 10 + 2 \cdot 16 = 2$.
- Multiply coefficients by 2 to get $-6 \cdot 10 + 4 \cdot 16 = 4$.
- That gives a particular solution $x_0 = -6$, $y_0 = 4$.
- Finally, form a general solution

$$\begin{cases} x = -6 + \frac{16}{2}n, \\ y = 4 - \frac{10}{2}n, \end{cases} \quad \text{which is} \quad \begin{cases} x = -6 + 8n, \\ y = 4 - 5n, \end{cases}$$

2. Find a general solution for the linear Diophantine equation $x \cdot 19 + y \cdot 53 = -3$.

- Use Euclidean algorithm to find $\gcd(19, 53) = 1$.
- (Bezout identity) $-39 \cdot 19 + 14 \cdot 53 = 1$.
- Multiply coefficients by -3 to get $117 \cdot 19 - 42 \cdot 53 = -3$.
- That gives a particular solution $x_0 = 117$, $y_0 = -42$.
- Finally, form a general solution

$$\begin{cases} x = 117 + 53n \\ y = -42 - 19n \end{cases}$$

Least common multiple

Definition

The **least common multiple** for a and b denoted by $\mathrm{lcm}(a,b)$ is the least positive integer m such that

$$a \mid m \text{ and } b \mid m.$$

Let $a = p_1^{a_1} \dots p_m^{a_m}$ and $b = p_1^{b_1} \dots p_m^{b_m}$, where $p_1, \dots, p_m$ are distinct primes and $a_1, \dots, a_m, b_1, \dots, b_m$ are non-negative integers. Then

$$\begin{aligned} ab &= p_1^{a_1+b_1} \dots p_m^{a_m+b_m} \\ \gcd(a,b) &= p_1^{\min(a_1,b_1)} \dots p_m^{\min(a_m,b_m)} \\ \mathrm{lcm}(a,b) &= p_1^{\max(a_1,b_1)} \dots p_m^{\max(a_m,b_m)}. \end{aligned}$$

Since $a + b = \min(a,b) + \max(a,b)$ for any $a, b \in \mathbb{Z}$, the following theorem holds.

Theorem

$ab = \gcd(a,b)\,\mathrm{lcm}(a,b).$

One can use the formula above to efficiently compute $\mathrm{lcm}(a,b)$. For instance,

$$\mathrm{lcm}(60,45) = \frac{60 \cdot 45}{\gcd(60,45)}.$$

That reduces computing lcm to Euclidean algorithm.

A binary relation on $\mathbb{Z}$: congruence modulo n

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$.

Definition

a is congruent to b modulo n if a and b give the same remainder when divided by n.

(Notation for congruence)

- $a \equiv b \mod n$.
- $a \equiv_n b$.

For instance:

- $-4 \equiv_3 2 \equiv_3 8$ because when we divide -4, 2, or 8 by 3 we get the same remainder 2;
- $-1 \equiv_4 3 \equiv_4 11$. because when we divide -1, 3, or 11 by 4 we get the same remainder 3.

Congruences: properties

Proposition

$a \equiv_n b \quad \Leftrightarrow \quad n \mid (b-a).$

$$\begin{aligned} a \equiv_n b \quad &\Rightarrow \quad a = q_1 n + r \text{ and } b = q_2 n + r \text{ for some } q_1, q_2, r \in \mathbb{Z} \\ &\Rightarrow \quad b - a = n(q_2 - q_1) \quad \Rightarrow \quad n \mid b - a. \\ a \not\equiv_n b \quad &\Rightarrow \quad a = q_1 n + r_1 \text{ and } b = q_2 n + r_2 \text{ for some } q_1, q_2, r_1 < r_2 \in \mathbb{Z} \\ &\Rightarrow \quad b - a = n(q_2 - q_1) + (r_2 - r_1) \quad \Rightarrow \quad n \nmid b - a. \end{aligned}$$

Proposition

$\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

(R) $a \equiv_n a$ because $n \mid (a-a)$.

(S) $a \equiv_n b \;\Rightarrow\; n \mid (b-a) \;\Rightarrow\; n \mid (a-b) \;\Rightarrow\; b \equiv_n a.$

(T) $\begin{matrix} a \equiv_n b \\ b \equiv_n c \end{matrix} \;\Rightarrow\; \begin{matrix} n \mid b-a \\ n \mid c-b \end{matrix} \;\Rightarrow\; n \mid (b-a)+(c-b) = c-a \;\Rightarrow\; a \equiv_n c.$

Definition

Denote by $[a]_n$ the equivalence class of a, called the **congruence class** of a modulo n.

Congruence class modulo n

By definition,

$$\begin{aligned}[a]_n = \{b \in \mathbb{Z} \mid b \equiv_n a\} &= \{\, b \in \mathbb{Z} \mid n \mid b - a \,\} \\ &= \{\, b \in \mathbb{Z} \mid b - a = qn \text{ for some } q \in \mathbb{Z} \,\} \\ &= \{\, b \in \mathbb{Z} \mid b = a + qn \text{ for some } q \in \mathbb{Z} \,\} \\ &= \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\},\end{aligned}$$

which is the set of all numbers b that give the same remainder as a when divided by n.

Proposition

There are exactly n distinct congruence classes modulo n:

$$[0]_n, [1]_n, \dots, [n-1]_n.$$

Proof.

There are exactly n remainders of division by n: $0, 1, 2, \dots, n-1$. □

By definition, $[a]_n$ is the set on numbers that are the same as a modulo n. So, we can think that $[a]_n$ is a **number modulo n**.

Definition

$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.

Congruence classes

For instance, there are exactly 5 classes modulo 5:

- $[0]_5 = \{\dots, -10, -5, 0, 5, 10, \dots\} = [5]_5 = [10]_5 = \dots$
- $[1]_5 = \{\dots, -9, -4, 1, 6, 11, \dots\} = [6]_5 = [11]_5 = \dots$
- $[2]_5 = \{\dots, -8, -3, 2, 7, 12, \dots\} = [7]_5 = [12]_5 = \dots;$
- $[3]_5 = \{\dots, -7, -2, 3, 8, 13, \dots\} = [8]_5 = [13]_5 = \dots;$
- $[4]_5 = \{\dots, -6, -1, 4, 9, 14, \dots\} = [9]_5 = [14]_5 = \dots.$

Proposition

The least non-negative number in $[a]_n$ is the remainder of division of a by n.

$[a]_n \in \mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ and so $[a]_n = [r]_n$ for some $0 \le r < n$ which must be the remainder of division of a by n.

Arithmetic of congruences

Define binary operations $+$ *and* $\cdot$ *on* $\mathbb{Z}_n$ *as follows:*

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab].$$

For instance,

$$[2]_6 + [5]_6 = [7]_6 \qquad [3]_6 \cdot [5]_6 = [15]_6$$
$$[4]_6 + [-7]_6 = [-3]_6 \qquad [4]_6 \cdot [-7]_6 = [-28]_6.$$

Q. *What can go wrong with our definition of* $+$ *and* $\cdot$*?*

- $+, \cdot$ are operations on congruence classes from $\mathbb{Z}_n$.
- But, $+$ and $\cdot$ are defined using representatives of classes.

Now, imagine the following situation:

- $[a_1] = [a_2]$,
- $[b_1] = [b_2]$,
- but $[a_1] + [b_1] \neq [a_2] + [b_2]$,

i.e., **sums of equal classes are different**. In that case we would say that $+$ is **not well-defined**.

Arithmetic of congruences: well-definedness

$+$ *is well-defined on* $\mathbb{Z}_n$.

Indeed, for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ we have

$$\begin{array}{c} [a_1] = [a_2] \\ [b_1] = [b_2] \end{array} \Rightarrow \begin{array}{c} n \mid (a_2 - a_1) \\ n \mid (b_2 - b_1) \end{array} \Rightarrow n \mid (a_2 - a_1) + (b_2 - b_1) = (a_2 + b_2) - (a_1 + b_1)$$

$$\Rightarrow [a_1 + b_1] = [a_2 + b_2].$$

$\cdot$ *is well-defined on* $\mathbb{Z}_n$.

Indeed, for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ we have

$$\begin{array}{c} [a_1] = [a_2] \\ [b_1] = [b_2] \end{array} \Rightarrow \begin{array}{c} n \mid (a_2 - a_1) \\ n \mid (b_2 - b_1) \end{array} \Rightarrow n \mid a_2(b_2 - b_1) + b_1(a_2 - a_1) = a_2 b_2 - a_1 b_1$$

$$\Rightarrow [a_1 b_1] = [a_2 b_2].$$

Arithmetic of congruences: properties

For every $[a], [b], [c] \in \mathbb{Z}_n$

Properties of $+_n$	
$[0]$ *is the trivial element*	$[0] + [a] = [a] + [0] = [a]$
$[-a]$ *is the inverse of* $[a]$	$[a] + [-a] = [-a] + [a] = [0]$
$+_n$ *is associative*	$([a] + [b]) + [c] = [a] + ([b] + [c])$
$+_n$ *is commutative*	$[a] + [b] = [b] + [a]$

Properties of $\cdot_n$	
$[1]$ *is the unity*	$[1] \cdot [a] = [a] \cdot [1] = [a]$
$\cdot_n$ *is associative*	$([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$
$\cdot_n$ *is commutative*	$[a] \cdot [b] = [b] \cdot [a]$
distributivity	$[a]([b] + [c]) = [a][b] + [a][c]$

Proofs are very straightforward. For instance,

$[0]$ is the trivial element: $[0] + [a] = [a] + [0] = [a]$

$$[0] + [a] = [0 + a] = [a] = [a + 0] = [a] + [0] = [a + 0]$$

$[-a]$ is the inverse of $[a]$: $[a] + [-a] = [-a] + [a] = [0]$

$$[-a] + [a] = [-a + a] = [0] = [a - a] = [a] + [-a] = [a + a]$$

$+_n$ is associative: $([a] + [b]) + [c] = [a] + ([b] + [c])$

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$$

Examples: Working with numbers modulo n

We can use congruences to compute remainders of division. For instance

Compute $r = (34 \cdot 17) \ \% \ 29$

- We can compute the product $34 \cdot 17$ and then divide by 29.
- But, to avoid long multiplication we can consider the congruence class $[34 \cdot 17]_{29}$

$$\begin{aligned}
[34 \cdot 17] &= [34] \cdot [17] \\
&= [5] \cdot [-12] \\
&= [-60] \\
&= [27].
\end{aligned}$$

Hence, $r = 27$. (Recall that r is the least non-negative number in $[34 \cdot 17]_{29}$)

Remark. We can do the same computations without classes:

$$\begin{aligned}
34 \cdot 17 &\equiv 5 \cdot (-12) \\
&\equiv -60 \\
&\equiv 27.
\end{aligned}$$

That replaces $=$ with $\equiv$.

Examples: Working with numbers modulo n

Compute 2^{100} % 7.

The modulus is small. We can compute several powers of 2 modulo 7 until we get 1

$$2^1 \equiv_7 2, \quad 2^2 \equiv_7 4, \quad 2^3 \equiv_7 1.$$

But then

$$\begin{aligned} 2^{100} &= (2^3)^{33} \cdot 2 && \text{(exponentiation properties)} \\ &\equiv 1^{33} \cdot 2 = 2 && \text{(replacing } 2^3 \text{ with 1)} \end{aligned}$$

Hence, 2 is the remainder of division of 2^{100} by 7.

Prove that $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$ *for every* $n \in \mathbb{N}$.

We can show that $5^{2n} + 3 \cdot 2^{5n-2} \equiv_7 0$ directly as follows:

$$\begin{aligned} 5^{2n} + 3 \cdot 2^{5n-2} &= 25^n + 3 \cdot 8 \cdot 2^{5n-5} \\ &\equiv_7 4^n + 3 \cdot 2^{5(n-1)} \\ &= 4 \cdot 4^{n-1} + 3 \cdot 32^{n-1} \\ &= 4 \cdot 4^{n-1} + 3 \cdot 4^{n-1} = 7 \cdot 4^{n-1} \equiv_7 0. \end{aligned}$$

(One can also solve this problem using induction.)