Number Theory

Giulia Mauri

Politecnico di Milano

email: *giulia.mauri@polimi.it*
website: *http://home.deib.polimi.it/gmauri*

April 22, 2015

Overview

Modular Arithmetic

Let n be a positive integer.

Definition

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

Addition and multiplication modulo n behave as expected.

Example

Consider $\mathbb{Z}_6$

$$4 + 5 = 9 \bmod 6 = 3$$
$$4 \times 5 = 20 \bmod 6 = 2$$

Greatest Common Divisor (gcd)

Definition (Greatest Common Divisor (gcd))

For $x, y \in \mathbb{Z}$, $d = \gcd(x, y)$, where d is the largest number that divides both x and y.

Definition (Relatively Prime)

If $\gcd(x, y) = 1$, the x and y are *relatively prime*.

For all $x, y \in \mathbb{Z}$, there exist $a, b \in \mathbb{Z}$ such that:

$$ax + by = \gcd(x, y)$$

a and b can be found efficiently using the Extended Euclid Algorithm (EEA).

Modular Inversion

Definition (Inverse)

The *multiplicative inverse* of $x \in \mathbb{Z}_n$ is $y \in \mathbb{Z}_n$ s.t. $xy \bmod n = 1$. If such y exists, it is indicated as x^{-1}.

Example

In $\mathbb{Z}_7$ the multiplicative inverse of 2 is $2^{-1} = 4$. In fact,
$2 \times 4 = 8 \bmod 7 = 1$.

The multiplicative inverse of $x \in \mathbb{Z}_n$ exist if and only if $\gcd(x, n) = 1$.

Definition

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$$

All the elements of $\mathbb{Z}_n^*$ have a multiplicative inverse, which can be found efficiently using the EEA.

Modular Equations

Solve

$$ax + b = 0 \text{ in } \mathbb{Z}_n$$

Three cases:

- If $\gcd(a, n) = 1$, then
$$x = -ba^{-1}$$
- If $\gcd(a, n) = d > 1$ and $b \bmod d = 0$, then
  1. Consider the new equation
  $$(a/d)x + (b/d) = 0 \text{ in } \mathbb{Z}_{n/d}$$
  2. Find solution $x_0 \in \mathbb{Z}_{n/d}$.
  3. The d solutions to the original equations are
  $$x_0, x_0 + (n/d), x_0 + 2(n/d), \dots, x_0 + (d-1)(n/d) \text{ in } \mathbb{Z}_n$$
- If $\gcd(a, n) = d > 1$ and $b \bmod d > 0$, then there is no solution.

Fermat's Little Theorem

Theorem (Fermat)

Let p be a prime, $\forall x \in \mathbb{Z}_p^*$: $x^{p-1} = 1$ in $\mathbb{Z}_p$.

Example

$$xx^{p-2} \bmod p = 1 \implies x^{-1} = x^{p-2} \text{ in } \mathbb{Z}_p$$

This is another way to compute inverses, but is less efficient than Euclid.

Generating Random Primes

Problem: generate a random prime number with l bits. No fast deterministic algorithm. Standard practice is

1. Generate a random odd integer n with l bits
2. Apply non-deterministic test of primality.

Fermat Primality Test

Input: integer n, candidate prime
Choose $a \leftarrow \mathbb{Z}_n$
if $a^{n-1} \bmod n = 1$ **then**
  return n may be prime
else
  return n is composite
end if

The test is repeated several times to reduce the probability of error.

Group Definition

Definition (Group)

A group is a set G that, together with an operation $\bullet$, must satisfy four requirements:

- *Closure*: for all a, b in G, the result of the operation, $a \bullet b$ is also in G;
- *Associativity*: for all a, b and c in G, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$;
- *Identity element*: there exists an element e in G, such that for every element a in G, the equation $a \bullet e = e \bullet a = a$ holds. Such element e is unique;
- *Inverse element*: for each a in G, there exists an element b in G such that $a \bullet b = b \bullet a = e$, where e is the identity element.

The Group $\mathbb{Z}_p^*$

Let p be a prime, then $\mathbb{Z}_p^*$ is a cyclic group, that is

$$\exists g \in \mathbb{Z}_p^* \text{ such that } \mathbb{Z}_p^* = 1, g, g^2, g^3, \ldots, g^{p-2}$$

g is called a generator of $\mathbb{Z}_p^*$.

Example

$$p = 5, g = 2 \quad \mathbb{Z}_5^* = \{1, 2, 4, 3\}$$

There exists at least one generator, but not all elements are generators.

Example

$$p = 5, g = 4 \quad \mathbb{Z}_5^* \neq \{1, 4, 1, 4\}$$

Lagrange's Theorem

If g is not a generator, it generates a subgroup of $\mathbb{Z}_p^*$. The size of this subgroup is the order of g.

Definition

$$ord_p(g) = | < g > | = \text{smallest } i \text{ s.t. } g^i = 1 \bmod p$$

Theorem (Lagrange)

$$\forall g \in \mathbb{Z}_p^*, \quad ord_p(g) \ divides \ p - 1$$

Euler's Theorem

Definition (Euler's ϕ)

Let n be a positive integer, then $\phi(n) = |\mathbb{Z}_n^*|$.

Calculating $\phi(n)$ is easy if the factorization of n is known:

$$p \text{ prime}, \ \phi(p) = p - 1$$
$$p, q \text{ distinct primes}, \ \phi(pq) = (p-1)(q-1)$$

Theorem (Euler)

$$\forall x \in \mathbb{Z}_n^*, \quad x^{\phi(n)} \bmod n = 1$$

Quadratic residue

Definition (quadratic residue)

$x \in \mathbb{Z}_p$, is a quadratic residue (Q.R.) if it has a square root in $\mathbb{Z}_p$.

Theorem (Euler's theorem)

$x \in \mathbb{Z}_p^*$, is a Q.R. if and only if $x^{(p-1)/2} = 1 \bmod p$.

Example

in $\mathbb{Z}_{11}$:

$$\begin{aligned} &1^5, 2^5, 3^5, 4^5, 5^5, 6^5, 7^5, 8^5, 9^5, 10^5 \\ =&1, -1, 1, 1, 1, -1, -1, -1, 1, -1 \end{aligned}$$

Note: $x \neq 0 \rightarrow x^{(p-1)/2} = (x^{p-1})^{1/2} = 1^{1/2} \in \{1, -1\}$ in $\mathbb{Z}_p$

Computing square roots mod p

Suppose $p = 3 \pmod 4$.

Lemma

if $c \in \mathbb{Z}_p^*$ is Q.R., then $\sqrt{c} = c^{(p+1)/4}$ in $\mathbb{Z}_p$.

If $p = 1 \pmod 4$ is not possible to find the square root.

EEA

Exercise

The numbers 7 and 23 are relatively prime and therefore there must exists integers a and b such that $7a + 23b = 1$. *Find such a pair* (a, b) *with the smallest possible* $a > 0$. *Given this pair, can you determine the inverse of 7 in* $\mathbb{Z}_{23}$*?*

EEA

Exercise

The numbers 7 and 23 are relatively prime and therefore there must exists integers a and b such that $7a + 23b = 1$. *Find such a pair* (a, b) *with the smallest possible* $a > 0$. *Given this pair, can you determine the inverse of 7 in* $\mathbb{Z}_{23}$*?*

Solution

k	r_k	q_k		s_k	t_k	$r_0 s_k + r_1 t_k$
0	23			1	0	23
1	7	3		0	1	7
2	2	3	$23 = 3 \cdot 7 + 2$	1	-3	2
3	1	2	$7 = 3 \cdot 2 + 1$	-3	10	1
4	0		$2 = 2 \cdot 1 + 0$	7	-23	0

The pair is $(a, b) = (10, -3)$ *and the inverse is* $7^{-1} = 10 \bmod 23$

Modular Equations

Exercise

Solve the equation $3x + 2 = 7$ *in* $\mathbb{Z}_{19}$.

Modular Equations

Exercise

Solve the equation $3x + 2 = 7$ *in* $\mathbb{Z}_{19}$.

Solution

Since $gcd(3, 19) = 1$, *then* $x = 5 \cdot 3^{-1}$.

k	r_k	q_k		s_k	t_k	$r_0 s_k + r_1 t_k$
0	19			1	0	19
1	3	6		0	1	3
2	1	3	$19 = 6 \cdot 3 + 1$	1	-6	1
3	0		$3 = 3 \cdot 1 + 0$	-3	19	0

Thus, $x = 5 \cdot (-6) = 5 \cdot 13 = 8$

Exercise

How many elements are there in $\mathbb{Z}_{35}^*$*?*

Exercise

How many elements are there in $\mathbb{Z}^*_{35}$*?*

Solution

We compute $\phi(35) = (p-1)(q-1) = (5-1)(7-1) = 24.$

Exercise

How many elements are there in $\mathbb{Z}_{35}^*$*?*

Solution

We compute $\phi(35) = (p-1)(q-1) = (5-1)(7-1) = 24.$

Exercise

What is the order of 2 in $\mathbb{Z}_{17}^*$*?*

Groups

Exercise

How many elements are there in $\mathbb{Z}_{35}^*$?

Solution

We compute $\phi(35) = (p-1)(q-1) = (5-1)(7-1) = 24.$

Exercise

What is the order of 2 in $\mathbb{Z}_{17}^*$?

Solution

$ord_{17}(2) =$ *smallest i s.t.* $2^i = 1 \bmod 17$
Moreover, we know that $17 - 1 = 16 = 2^4$. *Thus the order of 2 should be 2,4,8,16.*
$2^8 = 256 = 1 \quad 2^4 = 16 \quad 2^2 = 4$
The order is $ord_{17}(2) = 8$

Fermat's and Euler's theorem

Exercise

How much is $2^{10001} \bmod 11$*?*
Hint: use Fermat's theorem.

Fermat's and Euler's theorem

Exercise

How much is $2^{10001} \bmod 11$*?*
Hint: use Fermat's theorem.

Solution

We know that $2^{11-1} = 1$*. Thus,* $2^{10001} = 2^{10000} \cdot 2^1 = 1 \cdot 2 = 2$

Fermat's and Euler's theorem

Exercise

How much is $2^{10001} \bmod 11$*?*

Hint: use Fermat's theorem.

Solution

We know that $2^{11-1} = 1$. *Thus,* $2^{10001} = 2^{10000} \cdot 2^1 = 1 \cdot 2 = 2$

Exercise

How much is $2^{245} \bmod 35$*?*

Hint: use Euler's theorem.

Fermat's and Euler's theorem

Exercise

How much is $2^{10001} \bmod 11$*?*
Hint: use Fermat's theorem.

Solution

We know that $2^{11-1} = 1$. *Thus,* $2^{10001} = 2^{10000} \cdot 2^1 = 1 \cdot 2 = 2$

Exercise

How much is $2^{245} \bmod 35$*?*
Hint: use Euler's theorem.

Solution

We know that $2^{24} = 1$. *Thus,* $2^{245} = 2^{240} \cdot 2^5 = 1 \cdot 32 = 32$

Generator

Exercise

Which of the following numbers is a generator of $\mathbb{Z}_{13}^*$?

- *10,* $< 10 >= \{1, 10, 9, 12, 3, 4\}$
- *8,* $< 8 >= \{1, 8, 12, 5\}$
- *7,* $< 7 >= \{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$
- *3,* $< 3 >= \{1, 3, 9\}$
- *2,* $< 2 >= \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$

Generator

Exercise

Which of the following numbers is a generator of $\mathbb{Z}_{13}^*$?

- *10,* $< 10 >= \{1, 10, 9, 12, 3, 4\}$
- *8,* $< 8 >= \{1, 8, 12, 5\}$
- *7,* $< 7 >= \{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$
- *3,* $< 3 >= \{1, 3, 9\}$
- *2,* $< 2 >= \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$

Solution

The group should be composed of 12 elements.
Both 7 and 2 generate the entire group $\mathbb{Z}_{13}^*$.

Solve Equation with quadratic formula

Exercise

Solve the equation $x^2 + 4x + 1 = 0$ *in* $\mathbb{Z}_{23}$ *by using the quadratic formula.*

Solve Equation with quadratic formula

Exercise

Solve the equation $x^2 + 4x + 1 = 0$ *in* $\mathbb{Z}_{23}$ *by using the quadratic formula.*

Solution

$x = (-4 \pm \sqrt{4^2 - 4})/2 \pmod{23} = (-4 \pm \sqrt{12})/2.$
$2^{-1} \pmod{23} = 12$
$23 = 3 \pmod 4$
$12^{(23-1)/2} = 1$, *thus 12 is Q.R.*
Then, $12^{(23+1)/4} = 9$ *is the square root.*
$x = (-4 \pm 9) \cdot 12 \pmod{23} =$ *14 and 5.*