

# Introduction Number Theory

# Background

We will use a bit of number theory to construct:

- Key exchange protocols
- Digital signatures
- Public-key encryption

# Notation

From here on:

- $N$  denotes a positive integer.
- $p$  denote a prime.

Notation:  $\mathbb{Z}_N = \{0, 1, \dots, N - 1\}$

Can do addition and multiplication modulo  $N$

# Modular arithmetic

Examples: let  $N = 12$

$$9 + 8 = 5 \quad \text{in } \mathbb{Z}_{12}$$

$$5 \times 7 = \square \quad \text{in } \mathbb{Z}_{12}$$

$$5 - 7 = \square \quad \text{in } \mathbb{Z}_{12}$$

Arithmetic in  $\mathbb{Z}_N$  works as you expect, e.g.  $x \cdot (y+z) = x \cdot y + x \cdot z$  in  $\mathbb{Z}_N$

# Modular arithmetic

Examples: let  $N = 12$

$$9 + 8 = 5 \quad \text{in } \mathbb{Z}_{12}$$

$$5 \times 7 = 11 \quad \text{in } \mathbb{Z}_{12}$$

$$5 - 7 = 10 \quad \text{in } \mathbb{Z}_{12}$$

Arithmetic in  $\mathbb{Z}_N$  works as you expect, e.g.  $x \cdot (y+z) = x \cdot y + x \cdot z$  in  $\mathbb{Z}_N$

# Greatest common divisor

**Def:** For ints.  $x, y$ :  $\text{gcd}(x, y)$  is the greatest common divisor of  $x, y$

Example:  $\text{gcd}(12, 18) = 6$

**Fact:** for all ints.  $x, y$  there exist ints.  $a, b$  such that

$$a \cdot x + b \cdot y = \text{gcd}(x, y)$$

$a, b$  can be found efficiently using the extended Euclid alg.

If  $\text{gcd}(x, y) = 1$  we say that  $x$  and  $y$  are relatively prime

**Example:**  $2 \times 12 - 1 \times 18 = 6$

# Modular inversion

Over the rationals, inverse w.r.t. the multiplication of 2 is  $\frac{1}{2}$ .

What about  $\mathbb{Z}_N$ ?

**Def:** The **inverse** of  $x$  in  $\mathbb{Z}_N$  is an element  $y$  in  $\mathbb{Z}_N$  s.t.  $x \cdot y = 1$   
 $y$  is denoted  $x^{-1}$ .

Example: let  $N$  be an odd integer.

The inverse of 2 in  $\mathbb{Z}_N$  is  $\frac{N+1}{2}$  since  $2 \cdot \frac{N+1}{2} = N + 1 = 1$

# Modular inversion

Which elements have an inverse in  $\mathbb{Z}_N$  ?

**Lemma**:  $x$  in  $\mathbb{Z}_N$  has an inverse if and only if  $\gcd(x, N) = 1$

Proof:

$$\begin{aligned} \gcd(x, N) = 1 &\Rightarrow \exists a, b: a \cdot x + b \cdot N = 1 \Rightarrow a \cdot x = 1 \text{ in } \mathbb{Z}_N \\ &\Rightarrow x^{-1} = a \text{ in } \mathbb{Z}_N \end{aligned}$$

$$\gcd(x, N) > 1 \Rightarrow \forall a: \gcd(a \cdot x, N) > 1 \Rightarrow a \cdot x \neq 1 \text{ in } \mathbb{Z}_N$$

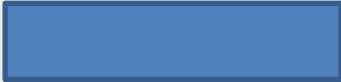


# More notation

**Def:**  $\mathbb{Z}_N^*$  = (set of invertible elements in  $\mathbb{Z}_N$ ) =  
=  $\{ x \in \mathbb{Z}_N : \gcd(x, N) = 1 \}$

Examples:

1. for prime  $p$ ,  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p - 1\}$

2.  $\mathbb{Z}_{12}^* =$  

For  $x$  in  $\mathbb{Z}_N^*$ , can find  $x^{-1}$  using extended Euclid algorithm.

# More notation

**Def:**  $\mathbb{Z}_N^*$  = (set of invertible elements in  $\mathbb{Z}_N$ ) =  
=  $\{ x \in \mathbb{Z}_N : \gcd(x, N) = 1 \}$

Examples:

1. for prime  $p$ ,  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p - 1\}$
2.  $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

For  $x$  in  $\mathbb{Z}_N^*$ , can find  $x^{-1}$  using extended Euclid algorithm.

# Solving modular linear equations

Solve:  $a \cdot x + b = 0$  in  $\mathbb{Z}_N$

Solution:  $x = -b \cdot a^{-1}$  in  $\mathbb{Z}_N$

Find  $a^{-1}$  in  $\mathbb{Z}_N$  using extended Euclid. Run time:  $O(\log^2 N)$

What about modular quadratic equations?

next segments

# Fermat's theorem (1640)

Thm: Let  $p$  be a prime

$$\forall x \in (\mathbb{Z}_p)^* : x^{p-1} = 1 \text{ in } \mathbb{Z}_p$$

Example:  $p=5$ .  $3^4 = 81 = 1$  in  $\mathbb{Z}_5$

Example of application:

$$\text{So: } x \in (\mathbb{Z}_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2} \text{ in } \mathbb{Z}_p$$

another way to compute inverses, but less efficient than Euclid

# Application: generating random primes

Suppose we want to generate a large random prime

say, prime  $p$  of length 1024 bits ( i.e.  $p \approx 2^{1024}$  )

Step 1: choose a random integer  $p \in [ 2^{1024} , 2^{1025}-1 ]$

Step 2: test if  $2^{p-1} = 1$  in  $Z_p$

If so, output  $p$  and stop. If not, goto step 1 .

Simple algorithm (not the best).

**$\Pr[ p \text{ not prime } ] < 2^{-60}$**

# The structure of $(\mathbb{Z}_p)^*$

**Thm** (Euler):  $(\mathbb{Z}_p)^*$  is a **cyclic group**, that is

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

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

Example:  $p=7$ .  $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}_7)^*$

Not every elem. is a generator:  $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

# Order

For  $g \in (\mathbb{Z}_p)^*$  the set  $\{1, g, g^2, g^3, \dots\}$  is called  
the **group generated by  $g$** , denoted  $\langle g \rangle$

Def: the **order** of  $g \in (\mathbb{Z}_p)^*$  is the size of  $\langle g \rangle$

$$\text{ord}_p(g) = |\langle g \rangle| = (\text{smallest } a > 0 \text{ s.t. } g^a = 1 \text{ in } \mathbb{Z}_p)$$

Examples:  $\text{ord}_7(3) = 6$  ;  $\text{ord}_7(2) = 3$  ;  $\text{ord}_7(1) = 1$

Thm (Lagrange):  $\forall g \in (\mathbb{Z}_p)^* : \text{ord}_p(g) \text{ divides } p-1$

# Euler's generalization of Fermat (1736)

**Def:** For an integer  $N$  define  $\varphi(N) = |(Z_N)^*|$  (Euler's  $\varphi$  func.)

Examples:  $\varphi(12) = |\{1,5,7,11\}| = 4$  ;  $\varphi(p) = p-1$

For  $N=p \cdot q$ :  $\varphi(N) = N-p-q+1 = (p-1)(q-1)$

**Thm** (Euler):  $\forall x \in (Z_N)^* : x^{\varphi(N)} = 1$  in  $Z_N$

Example:  $5^{\varphi(12)} = 5^4 = 625 = 1$  in  $Z_{12}$

Generalization of Fermat. Basis of the RSA cryptosystem



# Modular e'th roots

We know how to solve modular linear equations:

$$\mathbf{a \cdot x + b = 0} \quad \text{in } \mathbb{Z}_N \qquad \text{Solution: } \mathbf{x = -b \cdot a^{-1}} \quad \text{in } \mathbb{Z}_N$$

What about higher degree polynomials?

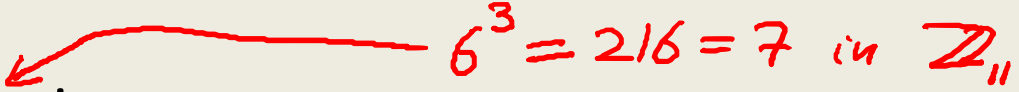
Example: let  $p$  be a prime and  $c \in \mathbb{Z}_p$ . Can we solve:

$$x^2 - c = 0 \quad , \quad y^3 - c = 0 \quad , \quad z^{37} - c = 0 \quad \text{in } \mathbb{Z}_p$$

# Modular e'th roots

Let  $p$  be a prime and  $c \in \mathbb{Z}_p$ .

**Def:**  $x \in \mathbb{Z}_p$  s.t.  $x^e = c$  in  $\mathbb{Z}_p$  is called an **e'th root** of  $c$ .

Examples:  $7^{1/3} = 6$  in  $\mathbb{Z}_{11}$  

$$3^{1/2} = 5 \text{ in } \mathbb{Z}_{11}$$

$2^{1/2}$  does not exist in  $\mathbb{Z}_{11}$

$$1^{1/3} = 1 \text{ in } \mathbb{Z}_{11}$$

# The easy case

When does  $c^{1/e}$  in  $\mathbb{Z}_p$  exist? Can we compute it efficiently?

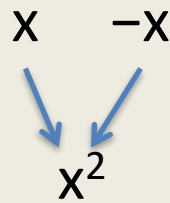
The easy case: suppose  $\gcd(e, p-1) = 1$

Then for all  $c$  in  $(\mathbb{Z}_p)^*$ :  $c^{1/e}$  exists in  $\mathbb{Z}_p$  and is easy to find.

# The case $e=2$ : square roots

If  $p$  is an odd prime then  $\gcd(2, p-1) \neq 1$

**Fact:** in  $\mathbb{Z}_p^*$ ,  $x \rightarrow x^2$  is a 2-to-1 function



**Example:** in  $\mathbb{Z}_{11}^*$ :

1	10	2	9	3	8	4	7	5	6
↙ ↘		↙ ↘		↙ ↘		↙ ↘		↙ ↘	
1		4		9		5		3	

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

$p$  odd prime  $\Rightarrow$  the # of Q.R. in  $\mathbb{Z}_p$  is  $(p-1)/2 + 1$

# Euler's theorem

**Thm:**  $x$  in  $(\mathbb{Z}_p)^*$  is a Q.R.  $\iff x^{(p-1)/2} = 1$  in  $\mathbb{Z}_p$  (p odd prime)

Example:

$$\begin{array}{l} \text{in } \mathbb{Z}_{11} : \quad 1^5, 2^5, 3^5, 4^5, 5^5, 6^5, 7^5, 8^5, 9^5, 10^5 \\ = \quad \quad \quad 1 \quad -1 \quad 1 \quad 1 \quad 1, \quad -1, \quad -1, \quad -1, \quad 1, \quad -1 \end{array}$$

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

**Def:**  $x^{(p-1)/2}$  is called the **Legendre Symbol** of  $x$  over  $p$  (1798)

# Computing square roots mod $p$

Suppose  $p \equiv 3 \pmod{4}$

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

# Solving quadratic equations mod $p$

Solve:  $a \cdot x^2 + b \cdot x + c = 0$  in  $Z_p$

Solution:  $x = (-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}) / 2a$  in  $Z_p$

- Find  $(2a)^{-1}$  in  $Z_p$  using extended Euclid.
- Find square root of  $b^2 - 4 \cdot a \cdot c$  in  $Z_p$  (if one exists)  
using a square root algorithm

# Computing $e$ 'th roots mod $N$ ??

Let  $N$  be a composite number and  $e > 1$

When does  $c^{1/e}$  in  $\mathbb{Z}_N$  exist? Can we compute it efficiently?

Answering these questions requires the factorization of  $N$   
(as far as we know)



# Easy problems

- Given composite  $N$  and  $x$  in  $Z_N$  find  $x^{-1}$  in  $Z_N$
- Given prime  $p$  and polynomial  $f(x)$  in  $Z_p[x]$   
find  $x$  in  $Z_p$  s.t.  $f(x) = 0$  in  $Z_p$  (if one exists)  
Running time is linear in  $\deg(f)$ .

... but many problems are difficult

# Intractable problems with primes

Fix a prime  $p > 2$  and  $g$  in  $(\mathbb{Z}_p)^*$  of order  $q$ .

Consider the function:  $x \mapsto g^x$  in  $\mathbb{Z}_p$

Now, consider the inverse function:

$$\mathbf{Dlog}_g(g^x) = x \quad \text{where } x \text{ in } \{0, \dots, q-2\}$$

Example:

in $\mathbb{Z}_{11}$ :	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$Dlog_2(\cdot)$ :	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

# Intractable problems with composites

Consider the set of integers: (e.g. for  $n=1024$ )

$$\mathbb{Z}_{(2)}(n) := \{ N = p \cdot q \text{ where } p, q \text{ are } n\text{-bit primes} \}$$

**Problem 1**: Factor a random  $N$  in  $\mathbb{Z}_{(2)}(n)$  (e.g. for  $n=1024$ )

**Problem 2**: Given a polynomial  $\mathbf{f}(\mathbf{x})$  where  $\text{degree}(f) > 1$

and a random  $N$  in  $\mathbb{Z}_{(2)}(n)$

find  $x$  in  $\mathbb{Z}_N$  s.t.  $f(x) = 0$  in  $\mathbb{Z}_N$

# The factoring problem

Gauss (1805): *“The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.”*

---

Best known alg. (NFS): run time  $\exp(\tilde{O}(\sqrt[3]{n}))$  for n-bit integer

Current world record: **RSA-768** (232 digits)

- Work: two years on hundreds of machines
- Factoring a 1024-bit integer: about 1000 times harder  
⇒ likely possible this decade