



# Intro. Number Theory

---

## Modular $e^{\text{'th}}$ roots

# 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  $\gcd(e, p-1) = 1$

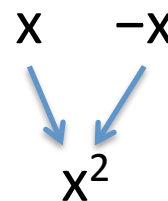
Then for all  $c$  in  $(\mathbb{Z}_p)^*$ :  $c^{1/e}$  exists in  $\mathbb{Z}_p$  and is easy to find.

Proof: let  $d = e^{-1}$  in  $\mathbb{Z}_{p-1}$ . Then  $c^{1/e} = c^d$  in  $\mathbb{Z}_p$

$$\begin{aligned} d \cdot e = 1 \text{ in } \mathbb{Z}_{p-1} &\Rightarrow \exists k \in \mathbb{Z} : d \cdot e = k \cdot (p-1) + 1 \Rightarrow \\ &\Rightarrow (c^d)^e = c^{d \cdot e} = c^{k \cdot (p-1) + 1} = [c^{p-1}]^k \cdot c = c \text{ in } \mathbb{Z}_p \end{aligned}$$

# 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:

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

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  $\mathbb{Z}_p$

Proof:  $\left[ c^{\frac{p+1}{4}} \right]^2 = c^{\frac{p+1}{2}} = \underbrace{c^{\frac{p-1}{2}}}_{=1} \cdot c = c \quad \text{in } \mathbb{Z}_p$

When  $p \equiv 1 \pmod{4}$ , can also be done efficiently, but a bit harder

run time  $\approx O(\log^3 p)$

# 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)

End of Segment