Intro. Number Theory

Modular e'th roots

Modular e'th roots

We know how to solve modular **linear** equations:

$a \cdot x + b = 0$ in Z_N Solution: $x = -b \cdot a^{-1}$ in Z_N

What about higher degree polynomials?

Example: let p be a prime and $c \in Z_p$. Can we solve:

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

Modular e'th roots

Let p be a prime and $c \in Z_p$.

Def: $x \in Z_p$ s.t. $x^e = c$ in Z_p is called an **e'th root** of c .

Examples:

$6^3 = 216 = 7$ in $\mathbb{Z}_{11}$

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

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

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

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

The easy case

When does $c^{1/e}$ in Z_p exist? Can we compute it efficiently?

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

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

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

$d \cdot e = 1$ in Z_{p-1} $\Rightarrow \exists k \in \mathbb{Z}: d \cdot e = k \cdot (p-1) + 1 \Rightarrow$

$\Rightarrow (c^d)^e = c^{d \cdot e} = c^{k \cdot (p-1) + 1} = [c^{p-1}]^k \cdot c = c$ in $\mathbb{Z}_p$

The case e=2: square roots

If p is an odd prime then gcd(2, p-1) ≠ 1

$$\begin{tikzcd}[column sep=small] x \arrow[dr] & & -x \arrow[dl] \\ & x^2 & \end{tikzcd}$$

<u>**Fact**</u>: in $\mathbb{Z}_p^*$, $x \longrightarrow x^2$ is a 2-to-1 function

<u>Example</u>: in $\mathbb{Z}_{11}^*$:

$$\begin{tikzcd}[column sep=small] 1 \arrow[dr] & & 10 \arrow[dl] & 2 \arrow[dr] & & 9 \arrow[dl] & 3 \arrow[dr] & & 8 \arrow[dl] & 4 \arrow[dr] & & 7 \arrow[dl] & 5 \arrow[dr] & & 6 \arrow[dl] \\ & 1 & & & 4 & & & 9 & & & 5 & & & 3 & \end{tikzcd}$$

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

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

Euler's theorem

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

Example:

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

Note: $x \neq 0 \Rightarrow x^{(p-1)/2} = \left(x^{p-1}\right)^{1/2} = 1^{1/2} \in \{ 1, -1 \}$ in Z_p

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

Computing square roots mod p

Suppose $p = 3 \pmod 4$

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

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

When $p = 1 \pmod 4$, 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: $x = \left(-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}\right) / 2a$ 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 Z_N** exist? Can we compute it efficiently?

Answering these questions requires the factorization of N

(as far as we know)

End of Segment