Summarizing:

We can reduce polynomials mod M to polynomial mod m_i $(i \in I)$

By Prime factorization of positive integers,
we have a bijection:

$$\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/n\} \xleftrightarrow[\sim]{\text{CRT}} \prod_{\substack{p \text{ is a} \\ \text{prime divisor} \\ \text{of } n}} \{\text{Roots of } f(T) \text{ in } \mathbb{Z}/p^{\nu_p(n)}\}$$

$$\Big\updownarrow \text{ modular reduction / Hensel lifting}$$

$$\{\text{Roots of } f(T) \text{ in } \mathbb{F}_p\}$$

Q: Solve polynomials in $\mathbb{F}_p$?

- Linear ✓
- Qudratic ?

Quadratic Residues

Defn. Let p be a prime number.

- Say an integer n (or the congruence class $[n]_p$) is a **quadratic residue** (QR) modulo p if $T^2 \equiv n \mod p$ (or equivalently, $T^2 - [n]_p = 0$) has a solution.

Rmk: this property does not dependent on the choice of rep. n.

- Otherwise, we say n (or the congruence class $[n]_p$) is a **quadratic non-residue** (QNR) modulo p

e.g. $p = 7$ $\mathbb{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$x \bmod 7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$x^2 \bmod 7$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{9} = \bar{2}$	$\overline{16} = \bar{2}$	$\overline{25} = \bar{4}$	$\overline{36} = \bar{1}$

Hence, the quadratic residues are

$$\bar{0}, \bar{1}, \bar{4}, \bar{2}$$

and the quadratic non-residues are

$$\bar{3}, \bar{5}, \bar{6}$$

$4 = \underbrace{1}_{\bar{0}} + \underline{3}$
↳ of them $\in \Phi(7)$

$\underline{3}$ all of them $\in \Phi(7)$

nonzero QR = # QNR.

Q: How to determine whether n is a QR mod p effectively?

Rmk: For $p=2$, both $\bar{0}$ and $\bar{1}$ are QR.

Theorem (Euler)

Let p be an odd prime number, and $a \in \Phi(p)$. Then

(i) a is a quadratic residue mod p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

(ii) a is a quadratic non-residue mod p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Rmk: By Fermat Little Theorem, we always have $\varphi(p) = p-1$

$$a^{p-1} \equiv 1 \bmod p.$$

Since p is odd, $\frac{p-1}{2} \in \mathbb{Z}$ and we have

$$a^{\frac{p-1}{2}} \equiv \text{either } 1 \text{ or } -1 \bmod p.$$

↳ is a solution of $T^2 - 1 \pmod p$

Hence, (i) $\Leftrightarrow$ (ii).

Method of Partnership

e.g. Compute $1+2+\cdots+49$. $= 50\cdot 24 + 25 = 1225$.

$$\underbrace{1+\underbrace{2+\cdots+\underbrace{24+25+26}_{50}+\cdots+48}_{50}+49}_{50}$$

e.g. Compute $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \bmod 11$

$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10$$

$\equiv 1\cdot 10 \equiv -1 \bmod 11$.

Theorem (Wilson)

Let p be a prime number. Then

$$(p-1)! \equiv -1 \mod p$$

Proof. Consider $\Phi(p) = \{1, 2, \cdots, p-1\}$.

Partner x and y when $xy \equiv 1 \mod p$.

Note that: any $x \in \Phi(p)$ has a unique mult. inverse in $\Phi(p)$.

Q: Which $x \in \Phi(p)$ is left over? $T^2 - 1 \Rightarrow \pm 1$

A: It is $\Leftrightarrow$ $x^2 \equiv 1 \mod p$ $\Leftrightarrow$ $x =$ either 1 or $p-1$.

If $p > 2$, $(p-1)! =$ the product of all elements in $\Phi(p)$

$$= 1 \cdot (p-1) \cdot \underbrace{(\text{partnered pairs})}_{\equiv 1 \bmod p}$$

$$\equiv -1 \mod p$$

Prop. Let p be an odd prime number.

Then, exactly half (i.e. $\frac{p-1}{2}$) of $\Phi(p)$ are QR, the other half are QNR.

Proof. Consider the map

$$\Phi(p) \xrightarrow{x \longmapsto \text{nat. rep. of } x^2 \text{ mod } p} \Phi(p)$$

Claim: this map is two-to-one. Hence, the # of its image, which are exactly the QRs, is exactly half of $\Phi(p)$.

$\#\Phi(p) : \#QR = 2:1$

Proof of the claim:

For each QR $a \in \Phi(p)$, consider the polynomial $T^2 - \bar{a}$.

Then the preimage of a are exactly the roots of $T^2 - \bar{a}$.
the natural rep. # roots ≤ 2

Since a is a QR, there is $b \in \Phi(p)$ s.t. $b^2 \equiv a \mod p$.

This gives a root $\bar{b}$ of $T^2 - \bar{a}$.

On the other hand, we have

$p^2 - 2p\cdot b + b^2$

$$(p-b)^2 \equiv b^2 \equiv a \mod p.$$

Since p is odd, $p - b \neq b$. Since $b \in \Phi(p)$, so is $p-b$.
$0 < b \leq p-1$ $0 < p-b \leq p-1$

This gives another root $\overline{p-b}$ of $T^2 - \bar{a}$.

But there are at most two roots of $T^2 - \bar{a}$ since it has degree 2.

Hence, there are no more preimage of a.

Defn. Let p be a prime number, and $a, x, y \in \Phi(p)$.

Say x and y are a-**partners** if

$$xy \equiv a \bmod p.$$

e.g. $p = 7$

$a = 1$ 1   2   3   4   5   6

$a = 2$ 1   2   3   4   5   6

$a = 3$ 1   2   3   4   5   6

Rmk: Every $x \in \Phi(p)$ has an a-partner. Why? $x\,T \equiv a \bmod p$

Theorem (Euler)

Let p be an odd prime number, and $a \in \mathbb{Z}(p)$. Then

(i) a is a quadratic residue mod p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

(ii) a is a quadratic non-residue mod p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Rmk: By Fermat Little Theorem, we always have

$$a^{p-1} \equiv 1 \bmod p.$$

Since p is odd, $\frac{p-1}{2} \in \mathbb{Z}$ and we have

$$a^{\frac{p-1}{2}} \equiv \text{either } 1 \text{ or } -1 \bmod p.$$

Hence, (i) $\Leftrightarrow$ (ii).

Proof: If a is a QR, then there is $x \in \Phi(p)$ s.t. $x^2 \equiv a \bmod p$.

Hence,

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \bmod p \quad (x^2)^{\frac{p-1}{2}}$$

$$\equiv 1 \bmod p. \quad \text{(By Fermat's little theorem)}$$

If a is a QNR, then for every $x \in \Phi(p)$, $x^2 \not\equiv a \bmod p$.

Hence, the a-partner of x is distinct from x.

$xy \equiv a \bmod p$

Then product of elements in $\Phi(p)$

= product of a-partnered pairs

since $\#\Phi(p) = p-1$

Since there are $\frac{p-1}{2}$ such pairs, we have

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \bmod p \quad \text{(By Wilson Theorem)}$$

$\blacksquare$

e.g. Determine wether $a = 3$ is a QR mod $p = 43$

To apply Euler's theorem, we need to compute $a^{\frac{p-1}{2}} \bmod p$.

To do that, we use the "taking square" trick:

$\frac{43-1}{2} = 21$

3^x	mod 43
3^1	3
3^2	9
3^4	$81 \equiv -5$
3^8	25
3^{16}	$625 \equiv -20$

$$
\begin{aligned}
3^{21} &\equiv 3^{16+4+1} \\
&\equiv (-20)\cdot(-5)\cdot 3 \mod 43 \\
&\equiv 300 \mod 43 \\
&\equiv -1 \mod 43
\end{aligned}
$$

Hence 3 is a QNR mod 43

Coro: Let p be an odd prime number,

Then $T^2 + \bar{1} \in \mathbb{F}_p[T]$ is irreducible if and only if

$$p \equiv 3 \mod 4.$$

Proof. $T^2 + \bar{1}$ is irreducible $\Leftrightarrow$ $\underset{a^2}{-1}$ is a QNR

By Euler's theorem, this is equivalent to

$$(-1)^{\frac{p-1}{2}} \equiv -1 \mod p. \qquad (*)$$

But

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ is even}, \\ -1 & \text{if } \frac{p-1}{2} \text{ is odd}. \end{cases}$$

$\frac{p-1}{2} = 2k+1$
$\Rightarrow p = 4k+3 \equiv 3 \mod 4$

Hence, $(*) \Leftrightarrow p \equiv 3 \mod 4$.

Rmark: Suppose p is a prime number and $p \equiv 1 \mod 4$.

How to find a $\bar{x} \in \mathbb{F}_p$ s.t. $\bar{x}^2 + \bar{1} = 0$?

Namely, how to find a "square root of $-1 \mod p$".

Consider

$$\overbrace{A = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (p-2)}^{\text{odd numbers in } \Phi(p)} \quad \frac{p-1}{2} \text{ terms}$$

$$\underbrace{B = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-1)}_{\text{even numbers in } \Phi(p)} \quad \frac{p-1}{2} \text{ terms}$$

Note that

$$\left.\begin{aligned} 2 &\equiv -(p-2) \mod p, \\ 4 &\equiv -(p-4) \mod p, \\ &\cdots \\ p-3 &\equiv -3 \mod p, \\ p-1 &\equiv -1 \mod p. \end{aligned}\right\} \Rightarrow \begin{aligned} B &\equiv (-1)^{\frac{p-1}{2}} A \mod p \\ &\equiv A \mod p \quad (p \equiv 1 \mod 4) \end{aligned}$$

$\pm \bar{A}$ is a "square root of -1 mod p".

On the other hand $AB = (p-1)! \equiv -1 \mod p$. (Wilson theorem)