Outline of the square root modulo p algorithm.

$$x^2 \equiv a \pmod p), \quad p-1 = 2^k \cdot m$$

Stage 0: Check that a is QR.

Stage 1: Find b such that $\mathrm{ord}_p(b) = 2^k$

Stage 2: Find $j \in \{0, 1, \dots, 2^{k-1}-1\}$ such that

$$b^{2j} \equiv a^m \pmod p)$$

Stage 3: $x \equiv \pm b^j \cdot a^{-\left(\frac{m-1}{2}\right)} \pmod p)$.

Check: $x^2 \equiv b^{2j} \cdot a^{-(m-1)} \equiv a^{m-(m-1)} \equiv a \pmod p)$.

Example: $x^2 \equiv 2 \pmod{41}$, $40 = 2^3 \cdot 5$

$k = 3$, $m = 5$.

Stage 0: $2^{\frac{41-1}{2}} \equiv 2^{20} \equiv (-9)^4 \equiv (-1)^2 \equiv 1 \pmod{41}$

$\Rightarrow 2$ is QR mod 41.

Stage 1: Look for NR mod 41.

Check 3: $3^{20} \equiv (-1)^5 \equiv -1 \pmod{41} \Rightarrow 3$ is NR.

Take $b \equiv 3^5 \, (3^m) \equiv 38 \equiv -3 \pmod{41}$

Stage 2: Find $j \in \{0, 1, 2, 3\}$ s.t. $(-3)^{2j} \equiv 2^5 \pmod{41}$

$9^0 \equiv 1$, $9^1 \equiv 9$, $9^2 \equiv 40$, $9^3 \equiv 32 \pmod{41}$

$\Rightarrow j = 3$.

Stage 3: $x \equiv \pm (-3)^3 \cdot 2^{-2} \pmod{41} \equiv \pm 27 \cdot 4^{-1} \pmod{41}$

$\equiv \pm \cancel{27} \cdot 10 \equiv \pm 24 \pmod{41}$.

§20.2. The case of $m = p \cdot q$ where p, q are distinct primes.

$x^2 \equiv a \pmod{m}$ is equivalent to $\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q} \end{cases}$

($\Leftarrow$ is by the CRT)

$x^2 \equiv a \pmod{p}$ has $\begin{cases} 2 \text{ solutions if } a \text{ is QR mod } p \\ 1 \text{ solution if } a \equiv 0 \pmod{p} \\ 0 \text{ solutions if } a \text{ is NR} \end{cases}$

The same applies to $x^2 \equiv a \pmod{q}$

We apply CRT to get

$x^2 \equiv a \pmod{m}$ has $\begin{Bmatrix} 2 \\ 1 \\ 0 \end{Bmatrix} \times \begin{Bmatrix} 2 \\ 1 \\ 0 \end{Bmatrix}$ solutions mod m

In total we can have 4, 2, 1 or 0 solutions modulo m.

Examples: (a) $x^2 \equiv 6 \pmod{95}$ $\quad 95 = 5 \cdot 19$

$6 \equiv 1 \equiv 1^2 \pmod{5} \Rightarrow 6$ is QR mod 5

$6 \equiv 25 \equiv 5^2 \pmod{19} \Rightarrow 6$ is QR mod 19

So we have 4 solutions modulo 95:

$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 5 \pmod{19} \end{cases}$ or $\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv -5 \pmod{19} \end{cases}$ or $\begin{cases} x \equiv -1 \pmod{5} \\ x \equiv 5 \pmod{19} \end{cases}$

or $\begin{cases} x \equiv -1 \pmod{5} \\ x \equiv -5 \pmod{19} \end{cases}$

We have: $1 = 4\cdot 5 - 1\cdot 19$

The first system has the solution

$$x \equiv 5\cdot 4\cdot 5 - 1\cdot 1\cdot 19 \equiv 81 \pmod{95}$$

Other solutions are:

$$x \equiv 71 \pmod{95}$$
$$x \equiv 24 \pmod{95}$$
$$x \equiv 14 \pmod{95}$$

1b) $x^2 \equiv 20 \pmod{95}$

$20 \equiv 0 \pmod 5 \Rightarrow x \equiv 0 \pmod 5$

$20 \equiv 1 \equiv 1^2 \pmod{19} \Rightarrow x \equiv \pm 1 \pmod{19}$.

We have two solutions $x \equiv \pm 20 \pmod{95}$.

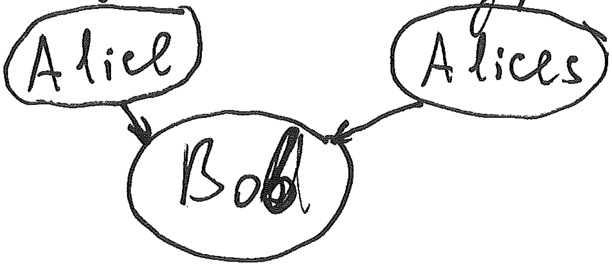
Problem: The method above works well if we know p and q. If we only know m, but not its factorization $m = pq$ then we first need to factorize it.

Q: Can we find a square root mod m without factorizing m?

A: No. It is known that finding a square root mod m is equivalent to factoring m, i.e. it is hard ~~abb~~ and can be used in cryptography

§20.3. Application: Rabin cryptosystem.

Everyone can encrypt a message and only Bob can decrypt it.



Algorithm. **Example.**

Step 1: Bob chooses large primes p, q
Computes $m = p \cdot q$

$p = 7$
$q = 11$
$m = 77$

Step 2: Bob posts m as a public key
Keeps p, q in secret.

Step 3: Alice encodes her message as the sequence of residues mod m: $[t_1, t_2, \dots, t_l]$

$[12]$

Step 4: Alice encrypts the message by replacing $t_i \to t_i^2 \equiv s_i \pmod{m}$

$[67]$

Step 5: Alice sends the encrypted message $[s_1, \dots, s_l]$ to Bob.

Step 6: Bob decrypts the message by solving equations
$t_i^2 \equiv s_i \pmod{m}$.
(He uses p, q).

Example: $t^2 \equiv 67 \pmod{77}$

$t^2 \equiv 4 \equiv 2^2 \pmod 7 \Rightarrow t \equiv \pm 2 \pmod 7$

$t^2 \equiv 1 \equiv 1^2 \pmod{11} \Rightarrow t \equiv \pm 1 \pmod{11}$

Finally, after applying the CRT we get $t \equiv \pm 12$ or $\pm 23 \pmod{77}$.