## Theorem (CRT)

Let $x$ satisfies a sequence of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad \Big\{ m_1 \mid x - a_1$$

where $a_i \in \mathbb{Z}$, $m_i \in \mathbb{N} \setminus \{0,1\}$
and $\gcd(m_i, m_j) = 1$ if $i \neq j$

—

Then $x$ has a single (unique) solution modulo $M = \prod_{i=1}^{k} m_i$, which is given by the formula:

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{M}, \quad \text{where}$$

$M_i = M/m_i$, $N_i$ is such that:

$$N_i \cdot M_i = 1 \pmod{m_i}$$

$$N_i = M_i^{-1} \pmod{m_i}$$

$m_i \mid M \mid x - \sum_{i=1}^{k} a_i M_i N_0$

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{m_i} = \sum_{j=1}^{i-1} \underbrace{a_j M_j N_j}_{\equiv 0 \pmod{m_i}} + a_i M_i N_i +$$

for $j \neq i$ $\quad m_i \mid M_j$

$$+ \sum_{j=i+1}^{k} \underbrace{a_j M_j N_j}_{\equiv 0 \pmod{m_i}} \pmod{m_i} =$$

$$= a_i \underbrace{M_i N_i}_{=1} \pmod{m_i} \equiv a_i \pmod{m_i}$$

---

So for $p \equiv 3 \pmod 4$

$$a^{-1} \cdot r^2 = a^{-1} \left(a^{\frac{s+1}{2}}\right)^2 = a^{s} = a^{\frac{p-1}{2}} \pmod p$$

$= 1$ because $a$ is QR mod $p$

$p \equiv 3 \pmod 4 \Rightarrow$
$\Rightarrow p-1 =$
$= 4k+3-1$
$= 4k+2 =$
$= 2 \cdot \underbrace{(2k+1)}_{s}$
$t = 1$

so indeed $\operatorname{ord}(a^{-1} r^2) \leq 2^{t-1} = 2^{1-1} = 1$

Let us consider the general case:

So in the general case $r$ can be treated as an initial good approximation of the square root. In fact it is a perfect square root from $a$ in the group $\langle g_1 \rangle$

In $\langle g_2 \rangle$ we need to adjust $r$ to make the relation

$$a^{-1} r^2 \equiv 1 \pmod p$$

satisfied.

To do so we need a generator of the group $\langle g_2 \rangle$, because in $\langle g_1 \rangle$ no adjustment of $r$ is needed (yes, we need to adjust $r$ in $\langle g_2 \rangle$ only, in separation to its value in $\langle g_1 \rangle$).

Let $n$ be any quadratic non-residue mod $p$. Let us choose and fix one.

Set

$$b := n^S \pmod p$$

See that $b$ is a generator of a subgroup $\langle g_2 \rangle$:

1) $n \in \mathbb{F}_p^*$, so $n = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \pmod p$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}_{p-1}$

2) $b \in \langle g_2 \rangle$ because:

$$n^S = \underbrace{g_1^{\alpha_1 \cdot S}}_{\substack{=1 \\ \text{because } \operatorname{ord} g_1 = S}} \cdot g^{\alpha_2 \cdot S} = g_2^{\alpha_2 \cdot S} \pmod p$$

3) $\operatorname{ord} b = 2^t$ because: $\operatorname{ord} b \mid \operatorname{ord} g_2 = 2^t$ and

(**) $b^{2^{t-1}} \pmod p \equiv (n^S)^{2^{t-1}} = n^{2^{t-1} \cdot S} = n^{\frac{p-1}{2}} = -1 \pmod p$

$n$ is QN mod $p$

$\neq 1 \pmod p$

So $\operatorname{ord} b = 2^t$, i.e.: $\langle b \rangle = \langle g_2 \rangle$

So we need to find a correct exponent $j$ such that

$$a^{-1} \cdot (b^j \cdot r)^2 \equiv 1 \pmod p$$

then obviously $b^j \cdot r \pmod p$ will be a square root of $a$ modulo $p$.

Of ~~course~~ course $j < \operatorname{ord} b = 2^t$

otherwise $j = j' + 2^t \cdot q$

for some $q \in \mathbb{Z}$ and $j' < 2^t$

$$b^j = b^{j' + 2^t \cdot q} = b^{j'} \cdot \underbrace{(b^{2^t})}_{=1}{}^q = b^{j'} \pmod p$$

$$j \equiv j' \pmod{\underset{\operatorname{ord} b}{\underbrace{2^t}}}$$

Note that $(**)$ is satisfied

$$b^{2^{t-1}} \pmod p = -1 \pmod p$$

so is sufficient to determine

$$j = \sum_{k=0}^{t-2} 2^k \cdot j_k \quad \text{for } j_k \in \{0, 1\}$$

Extending $j$ to $2^{t-1}$ would result in multiplying by $b^{2^{t-1}} \pmod p$, that is in changing the sign of the square root.

Let us start with establishing $j_0$:

Calculate

$$(3*) \quad (a^{-1} r^2)^{2^{t-2}} \pmod p$$

Since the square of the value above equals $1$, we see that the value itself is in $\{1, -1\}$.

So if (3*) equals $-1$ then we set $j_0=1$ else we set $j_0=0$

As a result we get:

$$\left(a^{-1}\left(b^{j_0} r\right)^2\right)^{2^{t-2}} = \left(b^{j_0}\right)^{2^{t-1}} \cdot \left(a^{-1}\cdot r^2\right)^{2^{t-2}} \pmod p$$

$$= \left(b^{2^{t-1}}\right)^{j_0} \left(a^{-1}\cdot r^2\right)^{2^{t-2}} = (-1)^{j_0} \left(a^{-1} r^2\right)^{2^{t-2}} \equiv$$

$$\equiv 1 \pmod p$$

$$\equiv 1\cdot 1$$

$$\equiv (-1)\cdot(-1)$$

Now suppose that $j_0, j_1, \dots, j_{\gamma-1}$ has been determined, for consecutive $\gamma = 1, 2, \dots, t-2$

Consequently, for each such $\gamma$ in the sequence the condition:

$$\left(a^{-1}\left(b^{\sum_{k=0}^{\gamma-1} 2^k j_k} \cdot r\right)^2\right)^{2^{t-\gamma-1}} \equiv 1 \pmod p$$

is satisfied. So calculate:

$$\left(a^{-1}\left(\left(b^{\sum_{k=0}^{\gamma-1} 2^k \cdot j_k}\right)\cdot r\right)^2\right)^{2^{t-\gamma-2}} \mod p$$

and since the square of the value above is 1, the value itself belongs to $\{-1, 1\}$. Thus if it equals $-1$ we set $j_\gamma = 1$, else we set $j_\gamma = 0$.

As a result:

$$\left(a^{-1}\cdot\left(\left(b^{\sum_{k=0}^{\gamma} 2^k j_k}\right)\cdot r\right)^2\right)^{2^{t-\gamma-2}} \equiv$$

$$\left(b^{2^\gamma \cdot j_\gamma}\right)^{2^{t-\gamma-1}} \cdot \left(a^{-1}\left(\left(b^{\sum_{k=0}^{\gamma-1} 2^k \cdot j_k}\right)\cdot r\right)^2\right)^{2^{t-\gamma-2}} =$$

$$= \underbrace{\left(b^{2^{t-1}}\right)^{j_\gamma}}_{=(-1)^{j_\gamma}} \cdot \left(a^{-1}\left(\left(b^{\sum_{k=0}^{\gamma-1} 2^k \cdot j_k}\right)\cdot r\right)^2\right)^{2^{t-\gamma-2}} =$$

$$= \left\{ \begin{array}{l} = (-1)\cdot(-1) \\ \text{or} \\ = 1\cdot 1 \end{array} \right\} = 1 \pmod p$$

See that that the computations above can be accelerated:

- exponentiation to power $2^{t-\gamma-2}$ is achieved by repeated squaring
- so during that exponentiation we can actually stop on the power $2^i$ yielding the result $-1$.

It may happen that $i = t-\gamma-2$, but sometimes it happens that $i < t-\gamma-2$. Set $\gamma' := t-i-2$ and set the bits $j_\gamma, \dots, j_{\gamma'-1}$ to $0$ and $j_{\gamma'}$ to $1$.

## Projective coordinates:

In affine equation:

$$(1) \quad y^2 = x^3 + ax + b$$

substitute $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + a\left(\frac{X}{Z}\right) + b \quad / \cdot Z^3$$

$$(2) \quad Y^2 Z = X^3 + aXZ^2 + bZ^3$$

The equation (2) is homogeneous: the cumulative exponent of each component on each side is the same (=3 in our case)

Formula (2) is called projective equation of the curve $E_{a,b}(K)$.