Using Quadratic Reciprocity

Lecture 3

For odd prime p and $a \in \mathbb{Z}$ such that $\left(\frac{a}{p}\right)=1$, want to solve $x^2 \equiv a \bmod p$ not by brute force.

- Tonelli-Shanks algorithm
- Cipolla's algorithm

Focus on 1st one.

Step 1: Write $p-1 = 2^e k$ for $e \geq 1$, k odd

Step 2: Find $b \bmod p$ s.t. $\left(\frac{b}{p}\right)=-1$ by QR.

Rk: GRH $\Rightarrow$ least quad. non-residue is $\leq 2(\log p)^2$.

Rk: If $p \equiv 3 \bmod 4$ then can use $b=-1$.

In fact if $p \equiv 3 \bmod 4$ and $\left(\frac{a}{p}\right)=1$ then an explicit solution to $x^2 \equiv a \bmod p$ is $\boxed{x = a^{(p+1)/4}}$;

it works since $\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a = \left(\frac{a}{p}\right) a = a \pmod p$

Back to step 2: Set $c = b^k \bmod p$. It turns out that $c \bmod p$ has order 2^e [= 2-power in $p-1$].

Step 3 Set $x_1 = a^{\frac{k+1}{2}} \bmod p$, so

$x_1^2 = a^{k+1} = a \cdot a^k = a y_1 \bmod p$ for $y_1 = a^k \pmod p$

Rk: When $p \equiv 3 \bmod 4$, $p-1 = 2k$ so $\frac{k+1}{2} = \frac{\frac{p-1}{2}+1}{2} = \frac{p+1}{4}$,

so $x_1 = a^{\frac{k+1}{2}} = a^{\frac{p+1}{4}} \bmod p$ and $a^k = a^{\frac{p-1}{2}} \equiv 1 (p)$: this recovers the solution to $x^2 \equiv a \bmod p$ for $p \equiv 3 \bmod 4$ seen above

Step 4: Use c in step 2 with order 2^e in order to get new congruences

$x_2^2 = a y_2 \bmod p$, $x_3^2 = a y_3 \bmod p$, ... $x_i^2 = a y_i (p)$

where $y_i \bmod p$ has order dividing 2^{e-i}. Then

$y_e = 1 \bmod p$, so $x_e^2 = y_e a = a \bmod p$.

Ex $p = 1249$ (prime) and $a = 10$: check $\left(\frac{10}{p}\right) = 1$.

Here $p-1 = 1248 = 2^5 \cdot 39 = 2^e \cdot k$.

Need b s.t. $\left(\frac{b}{p}\right) = -1$. Check $\left(\frac{19}{p}\right) = -1$.

Use $b = 19$. Then $c = b^k = 19^{39} \equiv 305 \bmod p$

This c has order $32 = 2^e$.

Set $x_1 = a^{\frac{k+1}{2}} = 10^{20} = 294 \bmod p$.

Write $x_1^2 = 10 y_1 \bmod p \rightarrow y_1 = 650 \ (p)$

and y_1 has order $16 = 2^{e-1}$, as does c^2.

Multiply congruence by c^2:

$$\underbrace{(x_1 c)}_{x_2}^2 = 10 \underbrace{(y_1 c^2)}_{y_2} \bmod p$$

$x_2 = 991$, $y_2 = 911 \rightarrow$ has order 8 in $(\mathbb{Z}/p)^\times$; so does c^4

$$x_2^2 = 10 y_2 \bmod p$$

Multiply congruence by c^4:

$$\underbrace{(x_2 c^2)}_{x_3}^2 = 10 \underbrace{(y_2 c^4)}_{y_3} \bmod p$$

$x_3 = 334$, $y_3 = 664 \rightarrow$ has order 4 in $(\mathbb{Z}/p)^\times$; so does c^8

$$x_3^2 = 10 y_3 \bmod p$$

Multiply congruence by c^8:

$$\underbrace{(x_3 c^4)}_{x_4 = 482}^2 = 10 \underbrace{(y_3 c^8)}_{y_4 = 1} \bmod p$$

$482^2 \equiv 10 \bmod p$: thus we can use $x = 482$ to solve $x^2 = 10 \ (p)$.

What makes this algorithm

① for every b s.t. $\left(\frac{b}{p}\right)=-1$, the number $c := b^k \bmod p$ has order 2^e where $p-1=2^e k$, k odd

② When $x_1 = a^{\frac{k+1}{2}} \bmod p$, we have $x_1^2 = a \cdot y_1 \bmod p$ for $y_1 = a^k \bmod p$ and $y_1^{2^{e-1}} = a^{2^{e-1}k} = a^{\frac{p-1}{2}} \equiv 1 \bmod p$, so $y_1 \bmod p$ has order dividing 2^{e-1} (maybe not equal to 2^{e-1}).

③ $c^2 \bmod p$ has order 2^{e-1} and if $z, w \in (\mathbb{Z}/p\mathbb{Z})^*$ have same 2-power order greater than 1 then zw has smaller 2-power order.

Rk: Changing the b with $\left(\frac{b}{p}\right)=-1$ in the algorithm could lead to the other solution of $x^2 = a \bmod p$.

Ex $p=1249$, $a=10$, $b=19 \rightsquigarrow x = 482 \ (p)$

$p=1249$, $a=10$, $b=23 \rightsquigarrow x = 767 \ (p) = -482 \ (p)$

Note we use one b with $\left(\frac{b}{p}\right)=-1$ in order to solve $x^2 = a \bmod p$ for all a with $\left(\frac{a}{p}\right)=1$: b does not depend on a in the Tonelli-Shanks algorithm.

Question: When $p \equiv 1 \bmod 4$, so the number of b's is $\frac{p-1}{2}$, an even number, do half the b's lead to one soln of $x^2 \equiv a \,(p)$ and half the b's lead to the other solution?

Answer: Letting $b' = -b$, it's not a square mod p since $\left(\frac{b'}{p}\right) = \left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot (-1) = -1$ and $c' = b'^k = (-b)^k = -b^k = -c$ since k is odd.

Let $p \equiv 1 \bmod 4$. Then using b' and c',

$x_1' = a^{\frac{k+1}{2}} = x_1$, $\quad x_1'^2 = a y_1' \Rightarrow x_1^2 = a y_1' = a y_1$

$\Rightarrow y_1' = y_1$.

If y_1 has order 2^{e-1} (like in the example above) then y_1 and $c^2 = c'^2$ have same order, so we multiply $x_1'^2 = a y_1'$ by c'^2:

$$\underbrace{(x_1' c')^2}_{x_2'} \equiv a \underbrace{(y_1' c'^2)}_{y_2' = y_1 c'^2 = y_1 c^2 = y_2}$$

$x_2' = x_1' c' = x_1(-c) = -x_1 c = -x_2$

That sign on $-x_2$ will persist in the rest of the algorithm:
$x_3' = -x_3$, $y_3' = y_3$, ..., $x_i' = -x_i$, $y_i' = y_i$, so $x_e' = -x_e$. Thus we get the other solution to $x^2 \equiv a \bmod p$ by using $-b$ in place of b.

If y_1 has order $< 2^{e-1}$ then it turns out $x_2' = (\text{power of } c^2)\, x_1 = x_2$, $x_i' = x_i$ for $i \geq 2$, and thus $x_e' = x_e$: we get the same solution to $x^2 \equiv a (p)$.