Lecture 11
Square Roots, Tonelli's Algorithm, Number of Consecutive Pairs of Squares mod p

Defined the Jacobi Symbol - used to compute Legendre Symbol efficiently (quadratic character)

Eg.

$$
\begin{aligned}
(1729|223) &= (168|223) = (4 \cdot 42|223) = (42|223) \\
&= (2|223)(21|223) = (21|223) = (223|21) = (13|21) \\
&= (21|13) = (8|13) = (2|13) = -1
\end{aligned}
$$

$$(-1|p) = \begin{cases} -1 & \text{if } p \equiv 3 \mod 4 \\ 1 & \text{if } p \equiv 1 \mod 4 \end{cases}$$

$$(2|p) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \mod 8 \\ 1 & \text{if } p \equiv \pm 1 \mod 8 \end{cases}$$

Lemma 43. *If p, q, r are distinct odd primes, and $q \equiv r \mod 4p$, then $(p|q) = (p|r)$.*

Proof. We know $(q|p) = (r|p)$ since $q \equiv r \mod p$. Also, q and r are both either $1 \mod 4$ or both $3 \mod 4$. So

$$
\begin{aligned}
(-1)^{\frac{p-1}{2}\frac{q-1}{2}} &= (-1)^{\frac{p-1}{2}\frac{r-1}{2}} \\
(p|q) &= (q|p)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\
&= (r|p)(-1)^{\frac{p-1}{2}\frac{r-1}{2}} \\
&= (p|r)
\end{aligned}
$$

■

Eg. Characterize the primes p for which 17 is a square mod p. It's clear that 17 is square mod 2. We see that since $17 \equiv 1 \mod 4$, so if $q \equiv r \mod 17$ then $(17|q) = (17|r)$. So we only need to look mod 17 to see when $(17|q) = (q|17) = 1$. Go through mod 17: $\pm 1, \pm 2, \pm 4, \pm 8 \mod 17$ are nonzero square classes, so 17 is a square mod q iff $q = 2, 17$, or $\pm 1, \pm 2, \pm 4, \pm 8 \mod 17$.

If we had asked for 19, we need to look at classes mod $(4 \cdot 19)$, since $19 \not\equiv 1 \mod 4$. (If $q = 1 \mod 4$ then $(19|q) = (q|19)$, so we need q to be a square mod 19. If $q = 3 \mod 4$ then $(19|q) = -(q|19)$, we need q to be not square mod 19)

Euclidean gcd Algorithm - Given $a, b \in \mathbb{Z}$, not both 0, find (a, b)

1. If $a, b < 0$, replace with negative
2. If $a > b$, switch a and b
3. If $a = 0$, return b
4. Since $a > 0$, write $b = aq + r$ with $0 \le r < a$. Replace (a, b) with (r, a) and go to Step 3.

Tonelli's Algorithm - To compute square roots mod p (used to solve $x^2 \equiv a \mod p$). Need a quadratic non-residue mod p, called n. Let g be a primitive root mod p. Now let $p - 1 = 2^s t$, for t odd. We know n is a power of g, say $n \equiv g^k$. Set $c \equiv n^t \equiv g^{kt}$.

Claim: The order of c is exactly 2^s.

Proof.

$$\begin{aligned} c^{2^s} &\equiv (g^{kt})^{2^s} \\ &\equiv (g^{t2^s})^k \\ &\equiv (g^{p-1})^k \\ &\equiv 1 \mod p \end{aligned}$$

So $\operatorname{ord}(c)$ has to divide 2^s, so it's a power of 2. If we can show that $c^{2^{s-1}} \not\equiv 1 \mod p$ then order has to be 2^s.

$$\begin{aligned} c^{2^{s-1}} &\equiv (g^{kt})^{2^{s-1}} \\ &\equiv (g^{t2^{s-1}})^k \\ &\equiv (g^{(p-1)/2})^k \mod p \\ &\equiv (-1)^k \mod p, \text{ since } g \text{ is a primitive root} \end{aligned}$$

Note that k is odd since otherwise $n \equiv g^k$ would be a quadratic residue, so we get $c^{2^{s-1}} \equiv -1 \mod p$, proving claim that $\operatorname{ord}(c) = 2^s$ ■

Lemma 44. *If a, b are coprime to p and have order $2^j \mod p$ (for $j > 0$) then ab has order 2^k for some $k < j$.*

Proof. Since $a^{2^j} \equiv 1 \mod p$, $(a^{2^{j-1}})^2 \equiv 1 \mod p$, we have $a^{2j-1} \equiv \pm 1 \mod p$. So we must have $a^{2^{j-1}} \equiv -1 \mod p$, since $\operatorname{ord}(a) = 2^j$. Similarly $b^{2^{j-1}} \equiv -1 \mod p$. Therefore, $(ab)^{2^{j-1}} \equiv 1 \mod p$, so order has to divide 2^{j-1}, so $k < j$. ■

Proof of Tonelli's Algorithm. First check (by repeated squaring) if $a^{(p-1)/2} \equiv 1 \mod p$. If not, terminate with "false." So assume now on that $a^{(p-1)/2} \equiv 1 \mod p$.

Set $A = a$ and $b = 1$. At each step $a = Ab^2$ ($a \equiv Ab^2 \mod p$) At the end, want $A = 1$, so b is square root of $a \mod p$.

Each step: decrease the power of 2 dividing the order of A. To start with, $A^{(p-1)/2} = A^{2^{s-1}t} \equiv 1 \mod p$. Check if $A^{(p-1)/4} \equiv 1 \mod p$.

If not, then $A^{2^{s-2}t} \equiv -1 \mod p$ (since $(A^{2^{s-2}t})^2 \equiv 1 \mod p$). So powers of 2 dividing $\mathrm{ord}(A)$ is exactly 2^{s-1}. Same as the power of 2 diving $\mathrm{ord}(c^2) = 2^{s-1}$. So set $A = Ac^{-2}$, $b = bc \mod p$. Notice that

$$\begin{aligned}(Ac^{-2})^{2^{s-2}t} &= \frac{A^{2^{s-2}t}}{c^{2^{s-1}t}} \\ &\equiv (-1)(-1)^t \\ &\equiv 1 \mod p\end{aligned}$$

$\mathrm{ord}(Ac^{-2})$ divides $2^{s-2}t$, so power of 2 dividing the order is at most 2^{s-2}, so has decreased by 1.

If yes, (ie., $A^{2^{s-2}t} \equiv 1 \mod p$), do nothing.

Next step: check if $A^{2^{s-3}t} = A^{(p-1)/8} \equiv 1 \mod p$.

If no, (ie., $A^{2^{s-3}t} \equiv -1 \mod p$, set $A := Ac^{-4}$, $b := bc^2$ (c^4 has order 2^{s-2}). $(Ac^{-4})^{2^{s-3}t} \equiv 1$.

If yes, do nothing.

After at most s steps we'll reach the stage when $a \equiv Ab^2 \mod p$ and the power of 2 dividing $\mathrm{ord}(A)$ is 1 - ie., $\mathrm{ord}(A)$ is odd. Now we just compute a square root of A as follows: $\mathrm{ord}(A)$ odd and divides $p - 1 \equiv 2^s t$, so divides t. So $A^t \equiv 1 \mod p$ (t odd). Claim $A^{(t+1)/2}$ is a square root of $A \mod p$.

$$\begin{aligned}(A^{(t+1)/2})^2 &= A^{t+1} \\ &= A^t A \\ &\equiv 1 \cdot A \\ &\equiv A \mod p\end{aligned}$$

So algorithm just returns $bA^{(t+1)/2}$ as $\sqrt{a}$ ■

Eg. If $p \equiv 3 \mod 4$, a is quadratic residue mod p, then a square root of a is $a^{(p+1)/4}$ (square $= a^{(p+1)/2} = a^{(p-1)/2}a \equiv a \mod p$)

Efficient poly-log time assuming we can find a quadratic non-residue n efficiently. A random number is quadratic non-residue with probability $\frac{1}{2}$ so if we run k trials, probability of not getting a quadratic non-residue is $\frac{1}{2}^k$ which is $\frac{1}{p^k}$ if k is $\log p$. So, this is an efficient randomized algorithm. No efficient deterministic algorithm has yet been found. Simplest is to check all primes, expect quadratic non-residue mod p which is less than $c(\log(p))^2 \Rightarrow$ true if assume ERH.

Question: Pairs of squares problem. How many numbers $x \mod p$ such that x and $x+1 \mod p$ are both squares mod p?

Rough heuristic - if x, $x+1$ were independent, roughly $\frac{p}{4}$ solutions.

Define $(0|p) = 0$. Then $\sum_{x \mod p}(x|p) = 0$. Also, number of solutions to $y^2 \equiv x \mod p$ for fixed x is $1+(x|p)$. Also, if $x \not\equiv 0$ then $\frac{1}{2}(1+(x|p))$ is 1 if x is a square, 0 if x is not a square.

So, number of x that $x, x+1$ are squares:

$$\underbrace{1}_{x=0} + \underbrace{\frac{1}{2}\left(1+(-1|p)\right)}_{x=-1} + \sum_{\substack{x \mod p \\ x\neq 0,-1}} \frac{1}{2}\left(1+(x|p)\right)\frac{1}{2}\left(1+(x+1|p)\right)$$

Now

$$\sum_{\substack{x \mod p \\ x\neq 0,-1}} \frac{1}{4}\left(1+(x|p)+(x+1|p)+(x|p)(x+1|p)\right)$$

$$
\begin{aligned}
\frac{1}{4}\sum 1 &= \frac{p-2}{4} \\
\frac{1}{4}\sum (x|p) &= \frac{1}{4}\left(\sum_{\text{all}}(x|p) - (0|p) - (-1|p)\right) \\
&= -\frac{1}{4}(-1|p) \\
\frac{1}{4}\sum (x+1|p) &= \frac{1}{4}\left(\sum_{\text{all}}(x+1|p) - (1|p) - (0|p)\right) \\
&= -\frac{1}{4} \\
\frac{1}{4}\sum (x|p)(x+1|p) &= \frac{1}{4}\sum (x|p)^{-1}(x+1|p) \\
&= \frac{1}{4}\sum \left(\left(\frac{x+1}{x}|p\right)\right) \\
&= \frac{1}{4}\sum_{x\neq 0,-1} \left(\left(1+\frac{1}{x}|p\right)\right) \\
&= \frac{1}{4}\sum_{x\neq 0,-1} (x|p) \\
&= -\frac{1}{4}
\end{aligned}
$$

Add them up to get

$$\frac{p+2+(-1|p)}{4}$$

If we want $x-1, x, x+1$ to all be squares, much more complicated

18.781 Theory of Numbers
Spring 2012