Oct15

Wednesday, October 14, 2020 10:52 PM

Warning (TH #7)

N composite.
$1 < a < N$.
<25% chance a not a MR witness for N

$\not\Longrightarrow$

If a not a MR witness $\Rightarrow$ <25% of N being composite.

subtle dependence on probability of a random # being prime.

Quadratic Residues & Quadratic Reciprocity

Underlying problem

Let $a \in \mathbb{Z}$, p prime. How can I tell if a is a square modulo p.

(Cf. HW 2 #8, HW 3 #6, HW5 #9)

Theorem (Euler's Criterion)
p odd prime. $p \nmid a$
a is a square mod p

$$\Longleftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Proof HW 5 9a
Suppose $a \equiv b^2 \mod p$.
Then $a^{\frac{p-1}{2}} = (b^2)^{p-1/2} = b^{p-1} \equiv 1 \mod p$.

In the direction, fix $g \in \mathbb{F}_p^*$ a primitive root.
$a = g^k$ some k.
$a^{\frac{p-1}{2}} = g^{(k/2)(p-1)} = 1 \mod p$.

$\Longrightarrow \underset{p-1}{\underset{\shortparallel}{|g|}}$ divides $\frac{k}{2}(p-1)$

$\Longrightarrow \ell(p-1) = \frac{k}{2}(p-1) \Longrightarrow k = 2\ell.$

$a = g^{2\ell} = (g^{\ell})^2$ & a a square ⊘

Def^n p odd prime. $a \in \mathbb{Z}$ & $p \nmid a$.
a is a quadratic residue mod p if it is a square mod p. (i.e. if $\exists c$ s.t. $a \equiv c^2 \bmod p$)
Else a is a quadratic nonresidue mod p

Prop p odd prime. $a \in \mathbb{Z}$. $p \nmid a$.
$g \in \mathbb{F}_p^*$ a primitive root $g^{k} \equiv a \bmod p$.
The following are equivalent.

① a is a quadratic residue.

② $\exists$ c s.t. $a \equiv c^2 \bmod p$.

→ ③ k is even ⟵ discrete log is even

④ $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Proof

① ⟺ ② Def

② ⟺ ③ HW 2 8d

② ⟺ ④ HW 5 9a

Def^n p odd prime. The Legendre symbol of an integer a is the quantity

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quad res mod } p \\ -1 & a \text{ is a quad non res mod } p \\ 0 & \text{if } p \mid a \end{cases}$$

Rmk Not a FRACTION.

Prop

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof

If $p \mid a \Rightarrow a^{\frac{p-1}{2}} \equiv 0 \mod p$ ✓

Otherwise $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$ HW2 8e

HW5 9a

It is $1 \Leftrightarrow a$ is a square

$\Leftrightarrow \left(\frac{a}{p}\right) = 1$ $\emptyset$

Notice defined a function

$$\begin{aligned} \left(\frac{*}{p}\right) : \mathbb{Z} &\longrightarrow \{-1, 0, 1\} \\ a &\longmapsto \left(\frac{a}{p}\right) \end{aligned}$$

Prop The Legendre Symbol is multiplicative

$$\begin{array}{ccc} \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) & = & \left(\frac{ab}{p}\right) \\ ||| & & ||| \\ a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}} \bmod p & \equiv & (ab)^{\frac{p-1}{2}} \bmod p \end{array}$$

Pf/ $\emptyset$

Slogan

- * (square) · (square) = square
- * (square) · (nonsquare) = nonsquare.
- * (nonsquare) · (nonsquare) = square !!!

Pf/ a, b nonsquares

$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1$

$\hookrightarrow ab$ a square $\emptyset$

Prop $a \equiv b \mod p$

Then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

pf/ Exercise.

Remark

— $\left(\frac{*}{p}\right) : \mathbb{F}_p \longrightarrow \{-1, 0, 1\}$ well defined.

—
$$\begin{tikzcd}
\mathbb{F}_p^* \arrow[r, "\log_g"] \arrow[rr, bend right, "\left(\frac{*}{p}\right)"'] & \mathbb{Z}/p-1\mathbb{Z} \arrow[r, "(-1)^x"] & \{\pm 1\}
\end{tikzcd}$$

Exercise

prove this

Theorem (Quadratic Reciprocity)

p, q odd primes.

① $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$

② $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \underset{\equiv}{1}, 7 \mod 8 \\ -1 & p \equiv 3, 5 \mod 8 \end{cases}$

③ $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \underline{p \equiv 1 \mod 4} \text{ or } \underline{q \equiv 1 \mod 4} \\ -\left(\frac{q}{p}\right) & \underline{p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4} \end{cases}$

$= (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$

Rewrite #3

Suppose $q \equiv 1 \bmod 4$

$x^2 = p \bmod q$ has a solution $\Longleftrightarrow$ $x^2 = q \bmod p$ has a solution.

Question Why should class of p mod q know anything about class of q modulo p.

Example

Is 5 a square modulo 61?

$\rightsquigarrow$ Compute square of every elt mod 61. See if 5 is there.

$\rightsquigarrow$ Find a primitive root of $\mathbb{F}_{61}^*$. Exponentiate until I find 5. See exponent is even or odd.

$\rightsquigarrow$ $5^{p-1/2} = 5^{30} \bmod 61$.

Or use quadratic reciprocity.

Same as asking if 61 is a square mod 5. But $61 \equiv 1 \bmod 5$. yes!!!

Proof of ①

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \frac{p-1}{2} \text{ even} \Leftrightarrow p-1 \text{ mult of } 4 \Leftrightarrow p \equiv 1 \bmod 4 \\ -1 & \text{------} \quad p \equiv 3 \bmod 4. \end{cases}$$

$\varnothing$

case 3 $\quad p^{\frac{q-1}{2}}$ & $q^{\frac{p-1}{2}}$ have in common?

Example

Is 17 a square mod 61? NO!

$$\left(\frac{17}{61}\right) \underset{\substack{\uparrow \\ QR}}{=} \left(\frac{61}{17}\right) = \left(\frac{10}{17}\right) = \overset{1}{\cancel{\left(\frac{2}{17}\right)}}\left(\frac{5}{17}\right) \underset{QR}{=} \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Example

Is 31 a square mod 83?

$$* \left(\frac{31}{83}\right) = -\left(\frac{83}{31}\right) = -\left(\frac{21}{31}\right) \overset{?}{\underset{??}{=}} \pm\left(\frac{31}{21}\right) \overset{?}{=} \left(\frac{31}{7}\right)\left(\frac{31}{3}\right) \quad ????$$

Not ~~prime~~

What does this mean?

(Ex 3.64 in [HPS])

can't factor

Lucky for us there is a fancy version w/ composite bases allowed!!

Def^n $a, b \in \mathbb{Z}$. b positive & odd.

Factor b as $b = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$.

Then the Jacobi Symbol is

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}$$

← Legendre

Example

$$\left(\frac{123}{323}\right) = \left(\frac{123}{17\cdot 19}\right) = \overbrace{\left(\frac{123}{17}\right)\left(\frac{123}{19}\right)} = \left(\frac{4}{17}\right)\left(\frac{9}{19}\right) = 1\cdot 1 = 1$$

$$\left(\frac{4}{17}\right) \xleftarrow{} 2^2 \qquad \left(\frac{9}{19}\right) \xleftarrow{} 3^2$$

Remark

a) Values are $\{-1,0,1\}$

b) No longer true that ~~$\left(\frac{a}{b}\right) = a^{\frac{b-1}{2}} \bmod b$~~

e.g. $b=15$, $a=2$

$2^{14} \equiv 4 \bmod 15$ not $\{-1,0,1\}$

c) b is prime then Jacobi $=$ Legendre

d) Unclear whether $\left(\frac{a}{b}\right)=1$ means a is a square mod b. (it doesn't)

Some nice properties remain.

Prop Multiplicativity

1) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$ (b odd & >0)

2) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$ (b_1, b_2 odd & >0)

3) $a_1 \equiv a_2 \bmod b$ (b odd & >0).

$$\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$$

Proof Direct from defn of Jacobi Symbol & apply corresponding Legendre identity.

e.g./ $\left(\frac{a_1 a_2}{pq}\right) = \left(\frac{a_1 a_2}{p}\right)\left(\frac{a_1 a_2}{q}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\left(\frac{a_1}{q}\right)\left(\frac{a_2}{q}\right)$

$= \left(\frac{a_1}{pq}\right)\left(\frac{a_2}{pq}\right)$ $\checkmark$ $\varnothing$

Thm (Quadratic Reciprocity for Jacobi).

$a, b \in \mathbb{Z}$. odd. >0.

$$① \left(\frac{-1}{b}\right) = \begin{cases} 1 & b \equiv 1 \bmod 4 \\ -1 & b \equiv -1 \bmod 4 \end{cases}$$

$$② \left(\frac{2}{b}\right) = \begin{cases} 1 & b \equiv 1, 7 \bmod 8 \\ -1 & b \equiv 3, \underset{\equiv}{5} \bmod 8 \end{cases}$$

$$③ \left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & a \text{ or } b \equiv 1 \bmod 4 \\ -\left(\frac{b}{a}\right) & a \text{ and } b \equiv 3 \bmod 4 \end{cases}$$

Proof Blow up to reduce to the prime case. Do careful bookkeeping.

Example Is 31 a square mod 83 $\underline{\underline{\text{yes}}}$

$$\left(\frac{31}{83}\right) = -\left(\frac{83}{31}\right) = -\left(\frac{21}{31}\right) = -\left(\frac{31}{21}\right)$$

$$= -\left(\frac{10}{21}\right) = -\overset{-1}{\cancel{\left(\frac{2}{21}\right)}}\left(\frac{5}{21}\right)$$

$$= \left(\frac{21}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$\underline{1 = 1^2 \bmod 5}$

Question If $\left(\frac{a}{b}\right) = 1$ does this imply a is a square mod b?

* If b prime ⇒ yes.

Test Case $b = pq$ product of 2 odd primes.

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1$$

2 Cases

① $\left(\frac{a}{p}\right)$ & $\left(\frac{a}{q}\right) = 1$.

a is a square mod p

and a is a square mod q

$$\Big\Updownarrow \text{HW5 9b}$$

a is a square mod pq

yes

② $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$

a not a square mod p.

If $a = c^2 \bmod pq$

$$\Longrightarrow a = c^2 + kpq = c^2 + p(kq)$$
$$\equiv c^2 \bmod p \quad ↯$$

NO!

Rmk Similar argument shows $\left(\frac{a}{b}\right) = -1$ then a not a square mod b.

Find a w/ $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$

Then $\left(\frac{a}{pq}\right) = 1$ but a not a square mod pq.

So... Interesting problem

$b = pq$ be a product of primes

Easy to compute $\left(\frac{a}{pq}\right)$

Hard to tell if a is a square mod pq.

Easy if you know p & q.

↳ Use to build a cryptosystem.