15 Squares mod p

Fix a prime p.

Basic question: Given a, how can we determine if $\exists b \in \mathbb{Z}$ such that $a \equiv b^2 \pmod{p}$?

Trivial case if $p|a$, take $b \equiv 0$. So from now on take $(a, p) = 1$.

p=3

x	x^2
1	1
2	1

$1 \equiv d_p$

$2 \not\equiv$

p=5

x	x^2
1	1
2	-1
3	-1
-1=4	1

$1, 4$ as $\mod 5$

$2, 3 \not\equiv$

p=7

x	x^2
1	1
2	4
4	2
5	4
6	1

$1, 2, 4$ as $\mod p$

$3, 5, 6 \not\equiv$

Guess

$$\#\text{ of squares in } (\mathbb{Z}/p)^* = \#\text{ of non-squares in } (\mathbb{Z}/p)^*$$

p odd, $p \not| a$.

Definition: the Legendre symbol of a mod p is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \equiv \text{ and } p \\ -1, & \text{if } a \not\equiv \mod p \end{cases}$$

We say a is a *quadratic residule* mod p if it is a , otherwise a quadratic *non-residue*. (Some would allow a to be divisible by p and set $(\frac{a}{p}) = 0$ if $p|a$.)

Lemma: the guess is on the money.

Proof: Let $S = \{1, 2, \ldots, p-1\}$. We know that S is a set of reps. for $(\frac{\mathbb{Z}}{p})^*$. Put

$$T = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$$

and

$$T^2 = \{b^2 | b \in T\}$$

Claim 1: $\#(T^2 \mod p) = \frac{p-1}{2}$, i.e., if $b, c \in T$, $b \neq c$, then $b^2 \not\equiv c^2 \pmod{p}$. Indeed, if $p^2 \equiv c^2 \pmod{p}$ then $b = \pm c \pmod{p}$. This cannot happen as, $\forall b \in T$, $\exists! b'$ in $S - T$ such that $b' \equiv -b \pmod{p}$, unless $b = c$.

Claim 2: $T^2 \equiv S^2 \pmod p$

Proof: Let $a \in S - T$. Then $\exists! a' \in T$ such that $a' \equiv a \pmod p$. Then $a^2 \equiv (a')^2 \pmod p$. Hence $a^2 \in T^2 \bmod p \Rightarrow$ the equare of any elt. of S is in $T^2 \bmod p$. Hence the claim.

But $\#\{\text{quad res. mod } p = \#S^2 \pmod p$. By claims 1 and 2, there is $\frac{p-1}{2} \Rightarrow \#\{\text{non}\} = p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

Corollary of Lemma: Let p be an odd prime. then

$$\sum_{a \in (\frac{\mathbb{Z}}{p})^*} \left(\frac{a}{p}\right) = 0.$$

Proof:

$$\begin{aligned}\text{LHS} &= \sum_{\text{quad res}} \underbrace{\left(\frac{a}{p}\right)}_{1} + \sum_{\text{quad non-res}} \underbrace{\left(\frac{a}{p}\right)}_{-1} \\ &= 1\#\{\text{quad res.}\} - 1\#\{\text{quad non-res.}\} \\ &= \frac{p-1}{2} - \frac{p-1}{2} = 0.\end{aligned}$$

Lemma: Let a, b be integers prime to p. Then

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

Proof:

Case 1: a, b are both $q, r, m, p.$, i.e. $a \equiv a_1^2$, $b \equiv b^2 \pmod p$ for some a, b. Hence $ab \equiv (a_1 b_1)^2 \pmod p$, and $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}) = 1 \cdot 1$.

Case 2: $(\frac{a}{p}) = 1$, $(\frac{b}{p} = -1$. Suppose $(\frac{ab}{p}) = 1$. Then $\exists c$ such that $ab \equiv c^2$. Since $(\frac{a}{p}) = 1$, $\exists a_1$ such that $a_1^2 \equiv a \ (\div p)$. $\Rightarrow a_1^2 b \equiv c \div p$.

Since $p \not| a_1$, a_1 is invertible mod p, i.e., $\exists a_2$ such that $a_1 a_2 \equiv 1$. Then $a_1^2 a_1^2 \equiv 1$.

$$\Rightarrow b \equiv a_2^2 c^2 \pmod p \Rightarrow \left(\frac{b}{p}\right) = 1.$$

So $(\frac{ab}{p}) = -1$ when $(\frac{a}{p}) = 1$ and $(\frac{b}{p}) = -1$.

Case (iii) $(\frac{a}{p}) = -1$, $(\frac{b}{p}) = 1$ same as (ii).
Case (iv) $(\frac{a}{p}) = (\frac{b}{p}) - 1$ (Try this!)

Lemma 3 (Wilson's Theorem) For any prime p, $(p-1)! \equiv -1 \pmod p$.

Proof: If $p = 2$, both sides $= 1 \pmod 2$, done. So assume p odd. Look at $S = \{1, \ldots, p-1\}$, set of resp. $forall a \in S$, let a' be the unique elt. of S such that $aa' = 1 \pmod p$.

$a = a'$ iff $a^2 = 1 \pmod p$, i.e., iff $a = 1$ or $a = p-1$. So,

$$\forall a \in \{2, \ldots, p-2\} a' \not\supset a \text{ and } a' \in \{2, \ldots, p-1\}.$$

$$\begin{aligned} \Rightarrow (2)(3) \cdot (p-2) &\equiv 1 \pmod p. \\ \Rightarrow (p-1)! &\equiv 1(p-1) \pmod p \\ &\equiv -1 \pmod p. \end{aligned}$$

Proposition (Euler's criterion) Let p be an odd prime, and let $a \in \mathbb{Z}$ with $(a, p) = 1$. Then

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

Recall that the Little Fermat theorem says that

$$a^{p-1} \equiv +1 \pmod p \text{ since } p \not| a;$$

so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.

Corollary of Proposition (Strict multiplicativity)

$$\left(\frac{ap}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \forall a, b \in \mathbb{Z} \text{ with } p \not| ab.$$

Proposition $\Rightarrow$ Corollary 1: By Euler,

$$\begin{aligned} \left(\frac{ab}{p}\right) &= (ab)^{\frac{p-1}{2}} \\ &\equiv \left(a^{\frac{p-1}{2}}\right)\left(b^{\frac{p-1}{2}}\right) \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \end{aligned}$$

Corollary 2 of Proposition: If $p =$ odd prime, -1 is a square mod p iff $p \equiv 1 \pmod 4$.

Proposition⇒Corollary 2: By Euler, $(\frac{-1}{p}) = 1$ iff $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Since p is odd, $p \equiv 1 \pmod 4$ are -1 (mod 4).

$p \equiv 1 \pmod 4$:
$p = 4m + 1$, some $m \in \mathbb{Z}$:

$$\Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{2m} = 1$$

$p \equiv -1 \pmod 4$:
$p = 4m - 1$:

$$(-1)^{\frac{p-1}{2}} = (-1)^{-1} \equiv -1 \pmod p.$$

Proof of proposition: By Fermat, $a^{p-1} \equiv 1 \pmod p$. Since p is odd, $\frac{p-1}{2} \in \mathbb{Z}$ and we can factor:

$$\underbrace{a^{p-1} - 1}_{\equiv 0 \text{ by Fermat}} = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} - 1\right)$$

$$\Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Now suppose a is a square mod p. Then $\exists b$ such that $a \equiv b^2 \pmod p$. So

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p.$$

So:

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

On the other hand, the congruence $X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ has at most $\frac{p-1}{2}$ solutions mod p by Lagrange. We have just proved that, given any quadratic residue a mod p,

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

i.e., a is a solution of

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \text{ (mod } p.$$

By lemma 1, there exists exactly $\frac{p-1}{2}$ quadratic residues mod p. Consequently,

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

has exactly $\frac{p-1}{2}$ solutions, and each of them is a quadratic residue mod p. In other words, if a is a quad. non-residue mod p, then a is not a solution of $X^{\frac{p-1}{2}} \equiv 0 \pmod{p}$.

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

if $a \not\equiv \pmod{p}$.

To summarize, we have the following properties of $(\frac{\cdot}{p})$:

(i) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ *Product formula*

(ii) $(\frac{-1}{p} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$, i.e., -1 is a square $\pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Remark:

Thanks to (i) and the unique factorization in $\mathbb{Z}$, in order to find $(\frac{a}{p})$ for any $a,\ (a,p) = 1$, we need only know

$$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \text{ and } \left(\frac{q}{p}\right), \ q \neq p \text{ an odd prime.}$$

We have already found a formula for $(\frac{-1}{p})$.

As an application of (ii) we will prove the following, special case of Dirichlet's theorem:

Proposition: There are infinitely many primes p which are congruent to 1 modulo 4.

Earlier we proved that there exists infinitely many primes $\equiv 3 \pmod{4}$ in the following way: Suppose there exists a finite number of such primes. List them as $3, p_1, \ldots, p_r$. Consider

$$N = 4p_1 \ldots p_r + 3.$$

Factor N as $q_1, \ldots z_s$, q_j prime for all j. Since N is odd, each q_j is an odd prime. Moreover, since $N \equiv e \pmod{4}$, since q_j must be $\equiv 1$ [3?] $\pmod{4}$. But this q_j cannot be among $\{3, p_1, \ldots, p_r\}$.

Suppose we tried this for primes $\equiv 1 \pmod 4$. Assume there exists only finitely many such primes $p_1, \ldots, p_m$. Put $N = 4p_1 \ldots p_m + 1$. Factor N as $q_1 \ldots q_s$. Since N is odd, each q_j is an odd prime. But, if s is even, we cannot hope to say that some q_j must be $\equiv 1 \pmod 4$. The method breaks down.

Proof of Proposition: Now we try again using (ii). Again start by assuming there exists only a finite number of primes $\equiv 1 \pmod 4$, say $p_1, \ldots, p_m$. Let $N = 4(p_1 p_2 \ldots p_m)^2 + 1$. Factor N as $q_1 \ldots q_k$, q_j prime for all j. Evidently, each q_j is an odd prime because N is odd.

Claim:

$$\textit{Every } q_j \text{ is } \equiv 1 \pmod 4.$$

Proof of Claim: Pick any odd prime q_j dividing N. Then, since $N = (2p_1 \ldots p_m)^2 + 1$, we get $-1 \equiv b^2 \pmod{q_j}$, where $b = 2p_1 \ldots p_m$. By the criterion (ii), -1 is a square mod q_j iff $q_j \equiv 1 \pmod 4$. Hence the claim.

So q_j is a prime which is $\equiv 1 \pmod 4$, and it cannot be among $\{p_1, \ldots, p_m\}$ because if $p_1 = q_j$ for some i, we will get $1 \equiv 0 \pmod{q_j}$, a contradiction, proving the proposition.

Remark: This proof tells us a way to generate new primes which are $\equiv 1 \pmod 4$ from known ones. Here are some simple examples:

1. Start with 5, and consider $N = 4(5)^2 + 1 = 101$; this is a prime.
2. Start with 13, and consider $N = 4(13)^2 + 1$. Then $N = 677$, also prime.
3. Start with 17. $N = 4(17)^2 + 1 = 1157 = (13)(89)$. Note: 13 and 89 are both $\equiv 1 \pmod 4$.

Next Question: When is 2 a square mod p? To answer this question, Gauss proved a very useful lemma:

Proposition A (Gauss' Lemma) Fix a, prime to p. Let S be a subst of $\mathbb{N}$ such that $S \cup (-S)$ is a set of reps. for $(\mathbb{Z}/p)^*$. Given any $\mathrm{s} \in S$, we can then write $a\mathrm{s} \equiv e_{\mathrm{s}}(a)\mathrm{s}_a \pmod p$, where $\mathrm{s} \in S$ and $e_{\mathrm{s}}(a) \in \{\pm 1\}$. Then

$$\left(\frac{a}{p}\right) = \prod_{\mathrm{s} \in S} e_{\mathrm{s}}(a).$$

Proof: Let s, s$'$ be distinct numbers in S. Then

$$a\mathrm{s} \not\equiv a\mathrm{s}' \pmod p, \text{ i.e., } \mathrm{s}_a \not\equiv \mathrm{s}'_a.$$

Hence the map $S \to S$ given by $\mathrm{s} \to \mathrm{s}_a$ has to be a bijection, i.e., 1-1 and out. (This is also called a pem. or a rearrangement of S.) We get

$$\begin{aligned}
\underbrace{\prod_{\mathrm{s}\in S}(a\mathrm{s})}_{a^{\frac{p-1}{2}}\prod_{\mathrm{s}\in S}\mathrm{s}} &\equiv \prod_{\mathrm{s}\in S} e_{\mathrm{s}}(a)\mathrm{s}_a \pmod p \\
&\equiv \left(\prod_{\mathrm{s}\in S} e_{\mathrm{s}}(a)\right)\left(\prod_{\mathrm{s}\in S}\mathrm{s}_a\right) \pmod p \\
&\equiv \prod_{\mathrm{s}\in S} \mathcal{S} \pmod p
\end{aligned}$$

So $a^{\frac{p-1}{2}}(\prod_{\mathrm{s}\in S}\mathrm{s}) \equiv (\prod_{\mathrm{s}\in S} e_{\mathrm{s}}(a))(\prod_{\mathrm{s}\in S}\mathrm{s}) \pmod p \equiv 0 \bmod p$

Cancelling $(\prod_{\mathrm{s}\in S}\mathcal{S})$, which is invertible mod p from each side, get

$$a^{\frac{p-1}{2}} \equiv \prod_{\mathcal{S}\in S} e_{\mathcal{S}}(0)$$

Done because

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

Remark: people very often take S to be the "canonical" half set of reps for $(\mathbb{Z}/p)^*$, namely $S = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Formulation (II) of Gauss' Lemma: Let $S = \{1, 2, \ldots, \frac{p-1}{2}\}$. For each $j \in S$, find the smallest positive residue $\bar{a}_j$ of a_j mod p. This is well defined, and

$$\bar{a}_j \in \{1, 2, \ldots, p-1\}.$$

Let

$$k = \#\{j \in S | \bar{a}_j \notin S\}.$$

Then Gauss' Lemma says

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Corollary of Gauss' lemma:

$$\left(\frac{2}{p}\right) = (-1)^{n(p)},$$

$n(p)$ is the number of integers s such that

$$\frac{p-1}{4} < \mathrm{s} < \frac{p-1}{2}.$$

Explicitly,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p = \pm 1 \pmod 8 \\ -1, & \text{if } p = \pm 5 \pmod 8 \end{cases}$$

Proof. Apply Gauss' lemma to $S = \{1, 2, \ldots, \frac{p-1}{2}\}$ with $a = 2$. Then

$$e_{\mathrm{s}}(2) = \begin{cases} 1, & \text{if } 2\mathrm{s} \le \frac{p-1}{2} \\ -1, & \text{otherwise} \end{cases}$$

Since $(\frac{2}{p} = \prod_{\mathrm{s}\in S} e_{\mathrm{s}}(a) \pmod p)$, $(\frac{2}{p}) = (-1)^{n(p)}$. The rest follows.

Definition: If $x \in \mathbb{R}$, its integral part $[x]$ is the largest integer $\le x$.

Proposition (Formulation III of Gauss' Lemma) Let p odd prime, and $a \in \mathbb{Z}$ with $p \not| a$. Then

$$\left(\frac{a}{p}\right) = (-1)^t, \text{ where } t = \sum_{j=1}^{(p-1)/2} [\frac{ja}{p}].$$

Proof: For every $j \in \{1, 2, \ldots, \frac{p-1}{2}\}$ it is easy to see that

$$a_j = q_j p + \bar{a}_j, \text{ with } 0 < \bar{a}_j < p.$$

Easy exercise:

$$q_j = \left[\frac{a_j}{p}\right].$$

So $\bar{a}_j = a_j - [\frac{a_j}{p}]$.

Summing over all the j's from 1 to $\frac{p-1}{2}$, we get

$$\sum_{j=1}^{\frac{p-1}{2}} a_j = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{a_j}{p}\right] p + \sum_{i-1}^{k} r_i + \sum_{i=1}^{k'} \ell_i, \tag{1}$$

where $k' = \frac{p-1}{2} - k$, $\{r_i\}$ = residues $\bar{a}_j$ *not* in S, $\{\ell_i\}$ = residues in S.

Also

$$\sum_{j=1}^{\frac{(p-1)}{2}} j = \sum_{i=1}^{k}(p - r_i) - \sum_{i=1}^{k} \ell_i. \tag{2}$$

Subtracting equation (2) from equation (1), we get

$$\begin{aligned}(a-1)\sum_{j=1}^{\frac{(p-1)}{2}} &= p\left(\sum_{j=1}\left[\frac{ja}{p}\right] - k\right) + 2\sum_{i=1}^{k} r, \\ &= \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = \frac{p^2-1}{8}\end{aligned}$$

Thus

$$\underbrace{(a-1)}_{\text{even since } a \text{ is odd}} \left(\frac{p^2-1}{8}\right) = \sum_{j=1}^{\frac{(p^2-1}{2}} \left[\frac{ja}{p}\right] - k \pmod 2$$

Consequently, k has the same parity as

$$\sum_{j=1}^{\frac{(p-1)}{2}} \left[\frac{ja}{p}\right].$$

Review: p prime, $a \in \mathbb{Z}$, $p \not| a$:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \equiv \mod p \\ -1, & a \not\equiv \mod p \end{cases}$$

(Some also define $\frac{a}{p}$ for all $\mathbb{Z}$ by setting $(\frac{a}{p}) = 0$ if $p|a$.)

$p = 2$: Everything is a square mod p. So assume p odd from now on. One has the multiplicativity property

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{*}$$

This follows from Euler's result that

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

Note: Since p is odd, if $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod p$, for some a, b prime to p, then $(\frac{a}{b}) = (\frac{b}{p})$. $(*)$ reduces finding $(\frac{a}{p})$ to the three cases

(i) $a = -1$

(ii) $a = 2$

(iii) $a = q$, an odd prime $\neq p$

We have already proved

(i)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

(ii)

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 5 \pmod 8 \end{cases}$$

(iii) q: odd prime $\neq p$.

$$\left(\frac{q}{p}\right) = ?$$