Euler's Criterion: For $a, p \in \mathbb{Z}$ with p prime we have

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

<u>Proof</u>: By P.R.T. $\exists$ some g such that

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, g, g^2, \ldots, g^{p-2}\}$$

First we will show that

$$g^k \text{ square} \iff k \text{ even}.$$

If $k = 2k'$ is even then

$$g^k = g^{2k'} = (g^{k'})^2 \quad \checkmark$$

Conversely, suppose g^k is square, i.e., $g^k = b^2$. But $b = g^\ell$ for some $\ell \in \mathbb{Z}$. It follows that

$$g^k = (g^\ell)^2$$
$$g^k = g^{2\ell}$$
$$1 = g^{2\ell-k} \quad \text{mod } p.$$

Recall: $\text{ord}_p(g) = p-1$.

This implies that

$$p-1 \mid 2\ell-k.$$

But we also have $2 \mid p-1$, hence

$$2 \mid 2\ell-k$$
$$2m = 2\ell-k \quad \text{some } m \in \mathbb{Z}$$
$$k = 2\ell-2m$$
$$k = 2(\ell-m) \text{ even } \checkmark$$

Conclusion: Half the elements are squares: $\underbrace{1, g^2, g^4, \dots, g^{p-3}}_{\frac{p-1}{2} \text{ of these.}}$

Half are not: $\overbrace{g, g^3, g^5, \dots, g^{p-2}}$

Problem: Given a, we know $a = g^k$ for some k, but how do we know if this k is even?

Observe that

$$\left(a^{(p-1)/2}\right)^2 = a^{(p-1)} \underset{\text{Fermat}}{\equiv} 1 \mod p$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a <u>field</u>, this implies that $a^{(p-1)/2} \equiv \pm 1 \mod p$.

If $a = g^k$, I claim that

$$a^{(p-1)/2} \equiv +1 \iff k \text{ even}.$$

Let $k = 2k'$ be even. Then

$$a^{(p-1)/2} = \left(g^{2k'}\right)^{(p-1)/2} = g^{(p-1)k'}$$

$$= \left(g^{p-1}\right)^{k'} = 1^{k'} = +1 \quad \checkmark$$

$$\mod p.$$

Hence $1, g^2, g^4, \dots, g^{p-3}$ are $\underline{\text{all}}$ of the roots of $x^{(p-1)/2} - 1 \bmod p$.

It follows that $a = g^{\text{odd}}$ is NOT a root of $x^{(p-1)/2} - 1$, i.e., $a^{(p-1)/2} \not\equiv +1$

Hence we must have $a^{(p-1)/2} \equiv -1$.

Summary: for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have $a = g^k$ for some $k \in \mathbb{Z}$. Then

a is square mod p

$\Longleftrightarrow$ k is even

$\Longleftrightarrow$ $a^{(p-1)/2} = +1$.

Euler's Criterion

Corollary:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$$

-1 is square mod p

$$\Longleftrightarrow \quad p = 1 \bmod 4$$

-1 is nonsquare mod p

$$\Longleftrightarrow \quad p = 3 \bmod 4.$$

Next Question:

$$\left(\frac{2}{p}\right) = 2^{(p-1)/2} \equiv \; ? \quad \bmod p.$$

To get a better sense of this I will another proof of Euler's criterion that is Less algebraic & more combinatorial.

First: Wilson's Theorem.

For odd prime p,

$$(p-1)! \equiv -1 \bmod p.$$

Proof: $(p-1)! = \prod_{k=1}^{p-1} k$

Now think of each k modulo p.

$$\prod_{k=1}^{p-1} k = 1(-1)\prod_{k\neq\pm1} k$$

$1 \neq -1$
$2 = 0 \bmod p$.

Claim that elements $k \neq \pm 1$ come in pairs $\{k_i, k_i'\}$ $i = 1, 2, \dots, \frac{p-3}{2}$ such that $k_i k_i' = 1 \bmod p$.

[Indeed, for any k, $\exists$ unique $k' =$ "$\frac{1}{k}$" satisfying $kk' = 1 \bmod p$]

It follows that

$$(p-1)! = \prod_{k=1}^{p-1} k = 1(-1)\prod_{k\neq\pm1} k$$

$$= 1(-1)\underbrace{(k_1k_1')}_{1}\underbrace{(k_2k_2')}_{1}\cdots\underbrace{(k_{\frac{p-3}{2}}k_{\frac{p-3}{2}}')}_{1}$$

$$= -1 \bmod p$$

///

The same method gives a new proof of Euler's criterion.

Proof: Consider $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

If a is not square mod p, then elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ break into pairs

$\{k_i, k_i'\}$, $i = 1, 2, \ldots, \frac{p-1}{2}$

such that $k_i k_i' = a \mod p$.

[Indeed, let $k_i' = a/k_i \mod p$.
Since a not square we know that
$k_i \neq k_i'$.]

UNIQUENESS: If $kl = a$
$km = a$

then divide by k:

$$kl = km$$
$$l = m.$$

It follows that

$$-1 \equiv (p-1)! = \prod k$$

$$= (k_1 k_1')(k_2 k_2') \cdots (k_{\frac{p-1}{2}} k_{\frac{p-1}{2}}')$$

$$= \underbrace{a \cdot a \cdot a \cdots a}_{\frac{p-1}{2} \text{ times}}$$

$$= a^{(p-1)/2} \, . \qquad \text{mod } p.$$

On the other hand, if a _is_ a square (say $a = r^2$) then set $(\mathbb{Z}/p\mathbb{Z})^\times$ breaks into two singletons

$\{r\}, \{-r\}$

$$\left(\begin{matrix} r \neq -r \\ 2r \neq 0 \text{ mod } p \end{matrix}\right)$$

Note: a has _at most_ _2_ square roots in the field $\mathbb{Z}/p\mathbb{Z}$

and $\frac{p-3}{2}$ pairs $\{k_i, k_i'\}$, $i = 1, \ldots, \frac{p-3}{2}$

where $k_i k_i' = a$ mod p.

It follows that

$$-1 \equiv (p-1)! = \prod k$$

$$= r(-r)(k_1k_1')(k_2k_2')\cdots(k_{\frac{p-3}{2}}k_{\frac{p-3}{2}}')$$

$$= -r^2 \underbrace{a \cdot a \cdot \cdots a}_{\frac{p-3}{2}}$$

$$= -a \cdot a^{(p-3)/2}$$

$$= -a^{(p-1)/2}$$

$$-1 \equiv -a^{(p-1)/2}$$

$+1 \equiv a^{(p-1)/2}$ as expected ✓

Q.E.D.

Recall that we are heading towards Quadratic Reciprocity.

Recall the statement of QR:

For <u>odd</u> primes p, q we have

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

we also have two "supplements"

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & p = 1 \bmod 4 \\ -1 & p = 3 \bmod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} (-1)^{\frac{p-1}{4}} & p = 1 \bmod 4 \\ (-1)^{\frac{p+1}{4}} & p = 3 \bmod 4 \end{cases}$$

$$= \begin{cases} +1 & p = 1, 7 \bmod 8 \\ -1 & p = 5, 3 \bmod 8 \end{cases}$$

HW Problem: combine QR + $\left(\frac{2}{p}\right)$ to get a formula for $\left(\frac{3}{p}\right)$ of the form

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p = ? \bmod 12 \\ -1 & p = ? \bmod 12 \end{cases}$$

It's possible to get similar formulas for $\left(\frac{4}{p}\right)$, $\left(\frac{5}{p}\right)$, ...

but they look kind of random.

For now, I want to prove the "second supplement"

$$\left(\frac{2}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{4}} & p = 1 \bmod 4 \\ (-1)^{\frac{p+1}{4}} & p = 3 \bmod 4 \end{cases}.$$

Proof By Example:

$p = 1 \bmod 4$, say $p = 13$.

Consider $12!$ working mod 13.

$$12! = \underbrace{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10}_{p-1 \text{ factors}} \cdot 11$$

$$= \underbrace{(1 \cdot 3 \cdot 5)}_{\frac{p-1}{4}} \underbrace{(7 \cdot 9 \cdot 11)}_{\frac{p-1}{4}} \underbrace{(2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12)}_{\frac{p-1}{2}}$$

$$= (\underline{1\cdot 3\cdot 5})(7\cdot 9\cdot 11)(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)\,2^{\frac{p-1}{2}}.$$

We really want
8, 10, 12

We multiply each of
1, 3, 5 by -1

$$= (-1)^{\frac{p-1}{4}}\,2^{\frac{p-1}{2}}\underbrace{\underset{12\cdot 10\cdot 8}{\left((-\cancel{1})(-\cancel{3})(-\cancel{5})\right)}(7\cdot 9\cdot 11)(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)}_{12!}$$

Summary: Working mod p we have

$$\cancel{(p-1)!} = (-1)^{\frac{p-1}{4}}\,2^{\frac{p-1}{2}}\,\cancel{(p-1)!}$$

$$(-1)^{\frac{p-1}{4}} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \quad \text{mod } p.$$

Euler's Criterion.

Other case: $p = 3$ mod 4, say $p = 11$.

Consider $10!$ mod 11.

$$10! = \underbrace{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10}_{p-1 \text{ factors}}$$

$$= \underbrace{(1\cdot 3\cdot 5)}_{\frac{p+1}{4}}\ \underbrace{(7\cdot 9)}_{\frac{p-3}{4}}\ \underbrace{(2\cdot 4\cdot 6\cdot 8\cdot 10)}_{\frac{p-1}{2} \text{ evens.}}$$

$$= (-1)^{\frac{p+1}{4}} \left((\overset{10}{\cancel{-1}})(\overset{8}{\cancel{-3}})(\overset{6}{\cancel{-5}})\right)(7\cdot 9)$$

$$\cdot\,(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)\, 2^{\frac{p-1}{2}}$$

$$= (-1)^{\frac{p+1}{4}}\, 2^{\frac{p-1}{2}}\, 10!$$

In general,

$$\cancel{(p-1)!} = (-1)^{\frac{p+1}{4}}\, 2^{\frac{p-1}{2}}\, \cancel{(p-1)!}$$

$$(-1)^{\frac{p+1}{4}} = 2^{\frac{(p-1)}{2}} \equiv \left(\frac{2}{p}\right) \qquad ✓$$

Euler's Criterion.

QED.

The attempt to generalize tricks like these led Euler to the discovery of QR, but he couldn't prove it.

First proof due to Gauss, and it was very complicated. Today we have 100s of proofs to choose from, but all of them involve some tricks.

For now, an application of $\left(\frac{2}{p}\right)$.

Theorem: $\exists\ \infty$ many primes $= 7 \bmod 8$.

<u>Proof</u>: Let $p_1, p_2, \dots, p_k = 7 \bmod 8$.

Define $N := (p_1 p_2 \cdots p_k)^2 - 2 > 1$.

Observe $2 \nmid N$ & $p_i \nmid N$ $\forall i$.

Let $p \mid N$ be any prime divisor.

Note $2 \equiv \underbrace{(p_1 \cdots p_k)^2}_{\text{square}} \bmod p$.

$\Rightarrow$ $p \equiv 1$ or $7 \bmod 8$.

But if all prime factors of N are $\equiv 1 \bmod 8$ then $N \equiv 1 \bmod 8$.

But $N = (7 \cdot 7 \cdots 7)^2 - 2$

$$\equiv 1 - 2 \equiv -1 \mod 8$$

$\Rightarrow$ N has some prime factor $\equiv 7 \bmod 8$, which is not in the list.

☺

For more like this, see Keith Conrad's note on "Square patterns and infinitude of primes."