Review. (Wilson's theorem) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Corollary 155. n is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Proof. It only remains to show that, if n is not a prime, then $(n-1)! \not\equiv -1 \pmod{n}$.
But this is obvious, if we realize that -1 is invertible modulo n but $(n-1)!$ is not. (Why?!) □

Review. A residue a is invertible modulo n if and only if $\gcd(a,n) = 1$.

Comment. Unfortunately, this criterion is not a good practical primality test. That's because computing the factorial is as much work as trial division by all numbers $2, \ldots, n-1$.

Comment. In fact, can you see why $(n-1)! \equiv 0 \pmod{n}$ if $n > 4$ is not a prime?
If we can write $n = ab$ where $a, b > 1$ and $a \neq b$, then $(n-1)! = \ldots \cdot a \cdot \ldots \cdot b \cdot \ldots \equiv 0 \pmod{n}$. This works (for instance, we can let a be the smallest divisor of n) unless $n = p^2$.
If $n = p^2$, then $(p^2-1)! = \ldots \cdot p \cdot \ldots \cdot (2p) \cdot \ldots \equiv 0 \pmod{p^2}$. Unless $2p > p^2 - 1$, which excludes $p = 2$ ($n = 4$).

17 Euler's criterion for quadratic residues

Example 156. List the first few primes for which 2 (respectively, -1) is a quadratic residue.

Solution.

p	2	3	5	7	11	13	17	19	23
is 2 a quadratic residue mod p?	yes: 0^2	no	no	yes: 3^2	no	no	yes: 6^2	no	yes: 5^2
is -1 a quadratic residue mod p?	yes: 1^2	no	yes: 2^2	no	no	yes: 5^2	yes: 4^2	no	no
$p \pmod 8$	2	3	5	7	3	5	1	3	7

Advanced observations. It turns out that 2 is a quadratic residue modulo an odd prime p if and only if $p \equiv \pm 1 \pmod 8$. Note that every prime (except 2) takes one of the four values $1, 3, 5, 7$ modulo 8.
Similarly, -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1,\ 5 \pmod 8$. Equivalently, $p \equiv 1 \pmod 4$. We will actually prove this second observation below.

Recall. We observed that, for a given odd prime p, half of the values $1, 2, \ldots, p-1$ are squares.
In other words, there is a 50% chance that a random residue is a square modulo a prime p. It therefore is reasonable to expect that a value like 2 or -1 (random residues in the sense that it is unclear whether they are squares modulo p) is a square for "half" of the primes. This is what we are observing.

Advanced comment. We are just scratching the surface of some amazing results in number theory which go under the heading of **quadratic reciprocity**. For instance, suppose p, q are odd primes, at least one of which is $\equiv 1 \pmod 4$. Then, p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p. Check out Chapter 9 in our book for more details.

Theorem 157. (Euler's criterion) Let p be an odd prime and a an invertible residue modulo p. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1$.

Important note. Since $x = a^{(p-1)/2}$ solves $x^2 \equiv 1 \pmod p$ (why?!) it follows that $a^{(p-1)/2} \equiv \pm 1 \pmod p$.

Comment. Our proof below uses the idea from our earlier proof of Wilson's theorem and extends it. It is a nice illustration how proofs can add value far beyond just verifying a claim.

Armin Straub
straub@southalabama.edu

Proof. We proceed similar to our proof of Wilson's theorem. Note that $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ modulo p is the product of all invertible values modulo p. This time, we pair each x in this product with ax^{-1} modulo p, and use $x \cdot (ax^{-1}) \equiv a \pmod{p}$.

Again, we have to be careful about elements that might pair with themselves. Because p is a prime, the congruence $x \equiv ax^{-1} \pmod{p}$ or, equivalently, $x^2 \equiv a \pmod{p}$ either has no solution (if a is not a quadratic residue) or two solutions $x \equiv \pm b \pmod{p}$ (if a is a quadratic residue).

- If a is not a quadratic residue, then we have $(p-1)/2$ pairs and, hence, $(p-1)! \equiv a^{(p-1)/2}$.
- If a is a quadratic residue, then we have $(p-3)/2$ pairs as well as the unpaired residues b and $-b$. Hence, $(p-1)! \equiv a^{(p-3)/2} \cdot b \cdot (-b) \equiv -a^{(p-1)/2}$. [Recall that $b^2 \equiv a$.]

On the other hand, by Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$, so that

$$a^{(p-1)/2} \equiv \begin{cases} -1, & \text{if } a \text{ is not a quadratic residue } (\mathrm{mod}\, p), \\ 1, & \text{if } a \text{ is a quadratic residue } (\mathrm{mod}\, p). \end{cases}$$

□

Alternative proof. If a is a quadratic residue modulo p then, by definition, there is an x such that $x^2 \equiv a \pmod{p}$. By Fermat's little theorem, $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$.

It therefore remains to consider the case when a is not a quadratic residue modulo p. A slick argument can be based on the fact that a polynomial of degree k can have at most k roots modulo a prime (we only discussed this for $k=2$). In particular, $x^{(p-1)/2} \equiv 1 \pmod{p}$ can have at most $(p-1)/2$ solutions. But we already know $(p-1)/2$ solutions, namely all quadratic residues modulo p. Hence, if a is not a quadratic residue modulo p, then we cannot have $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Example 158. Use Euler's criterion for quadratic residues to determine whether 5 is a quadratic residue modulo 19. Likewise, is 5 is a quadratic residue modulo 37?

Solution.

- We compute $5^9 \pmod{19}$ using binary exponentiation: $5^2 \equiv 6$, $5^4 \equiv 6^2 \equiv -2$, $5^8 \equiv 4 \pmod{19}$ so that $5^9 \equiv 5 \cdot 4 \equiv 1 \pmod{19}$. Hence, by Euler's criterion, 5 is a quadratic residue modulo 19.
- We compute $5^{18} \pmod{37}$ using binary exponentiation: $5^2 \equiv -12$, $5^4 \equiv 144 \equiv -4$, $5^8 \equiv 16$, $5^{16} \equiv 256 \equiv -3 \pmod{37}$ so that $5^{18} \equiv (-12) \cdot (-3) \equiv -1 \pmod{37}$. Hence, by Euler's criterion, 5 is not a quadratic residue modulo 37.

Corollary 159. Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.

In other words, the quadratic congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof. -1 is a quadratic residue modulo p
$\iff$ $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ [by Euler's criterion]
$\iff$ $(-1)^{(p-1)/2} = 1$
$\iff$ $(p-1)/2$ is even
$\iff$ $p \equiv 1 \pmod{4}$

□

Comment. In the case $p=2$, which we excluded from the discussion, $x^2 \equiv -1 \pmod{2}$ has the solution $x=1$. On the other hand, $x^2 \equiv -1 \pmod{4}$ has no solution.

Advanced comment. If $n = n_1 n_2$ for relatively prime n_1, n_2, then $x^2 \equiv -1 \pmod{n}$ has a solution if and only if both $x^2 \equiv -1 \pmod{n_1}$ and $x^2 \equiv -1 \pmod{n_2}$ has a solution. You are right: this follows immediately from the Chinese remainder theorem.

In general, the quadratic congruence $x^2 \equiv -1 \pmod{n}$ has a solution if and only if the prime factorization $n = 2^{r_0} p_1^{k_1} \cdots p_r^{k_r}$ has the property that $p_i \equiv 1 \pmod{4}$ and $r_0 \in \{0, 1\}$.

Example 160. (extra) Find x such that $x^2 \equiv -1 \pmod{p}$ for $p = 29$ (and for $p = 17$).

Solution. The crucial observation is that, if a is not a quadratic residue modulo p, in which case $a^{(p-1)/2} \equiv -1$ (by Euler's criterion), then $x = a^{(p-1)/4}$ satisfies $x^2 \equiv -1$. Exactly half of the nonzero residues are not quadratic, so every second a will do the trick (and we can just try various a until we find one with $a^{(p-1)/2} \equiv -1 \pmod{p}$).

- $p = 29$: we try $a = 2$ and find $2^{14} \equiv -1$, so that 2 is not a quadratic residue modulo 29.
  Consequently, $x = 2^7 \equiv 12 \pmod{29}$ satisfies $x^2 \equiv -1 \pmod{29}$. (Check it!)

- $p = 17$: we try $a = 2$ and find $2^8 \equiv 1$, so that 2 is a quadratic residue modulo 17.
  We next try $a = 3$ and find $3^8 \equiv -1$, so that 3 is a quadratic residue modulo 17.
  Consequently, $x = 3^4 \equiv -4 \pmod{17}$ satisfies $x^2 \equiv -1 \pmod{17}$. Of course, the simpler $+4$ also works.

Comment. We actually do not know a way of finding a non-quadratic residue that is better than our trial-and-error approach. (We don't even know any (provably) polynomial time algorithm; the trial-and-error method is polynomial time if the Riemann hypothesis is true.)

Advanced comment. Variants of this idea (due to Lagrange, Legendre, Tonelli and others) can be used to compute other "square roots" modulo p. Suppose that, for given quadratic residue a, we want to solve $x^2 \equiv a \pmod{p}$. (In other words, we are interested in the square root of a.)

- If $p \equiv 3 \pmod{4}$, then $x = \pm a^{(p+1)/4}$.
  Why? $x^2 = a^{(p+1)/2} = a^{(p-1)/2} \cdot a \equiv 1 \cdot a \pmod{p}$
  [The reason we need $p \equiv 3 \pmod{4}$ is so that $(p+1)/4$ is an integer.]

- For other primes, one can extend this idea and proceed iteratively. See, for instance, the Tonelli–Shanks algorithm:
  https://en.wikipedia.org/wiki/Tonelli%E2%80%93Shanks_algorithm