16 Quadratic residues

Definition 149. An integer a is a **quadratic residue** modulo n if $a \equiv x^2 \pmod{n}$ for some x.

Example 150. List all quadratic residues modulo 11.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 \equiv 3$. Hence, the quadratic residues modulo 11 are $0, 1, 3, 4, 5, 9$.

Important comment. Exactly half of the 10 nonzero residues are quadratic. Can you explain why?
[*Hint.* $x^2 \equiv y^2 \pmod{p} \iff (x - y)(x + y) \equiv 0 \pmod{p} \iff x \equiv y$ or $x \equiv -y \pmod{p}$]

Example 151. List all quadratic residues modulo 15.

Solution. We compute all squares modulo 15: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv 10$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$. Hence, the quadratic residues modulo 15 are $0, 1, 4, 6, 9, 10$.

Important comment. Among the $\phi(15) = 8$ invertible residues, the quadratic ones are $1, 4$ (exactly a quarter). Note that 15 is of the form $n = pq$ with p, q distinct primes. Lemma 152 explains why this always happens for such n.

Lemma 152. Let m, n be coprime. Then a is a quadratic residue modulo mn if and only if a is a quadratic residue modulo both m and n.

Proof. a is a quadratic residue modulo mn
$\iff$ $a \equiv x^2 \pmod{mn}$ (for some integer x)
$\iff$ $a \equiv x^2 \pmod{m}$ and $a \equiv x^2 \pmod{n}$ (for some integer x)
$\iff$ a is a quadratic residue modulo both m and n

It is obvious that "$\Longrightarrow$" holds in the final step. To see that "$\Longleftarrow$" also holds is a bit more tricky: if $a \equiv x^2 \pmod{m}$ and $a \equiv y^2 \pmod{n}$, then we can find s, t such that $x - y = sm + tn$ (possible by Bezout because m, n are coprime) or, equivalently, $x - sm = y + tn$. Then, with $X = x - sm$, we have $a \equiv X^2 \pmod{m}$ and $a \equiv X^2 \pmod{n}$. □

Theorem 153. Let p, q, r be distinct odd primes.

- The number of invertible residues modulo n is $\phi(n)$.
- The number of invertible quadratic residues modulo p is $\frac{\phi(p)}{2} = \frac{p-1}{2}$.
- The number of invertible quadratic residues modulo pq is $\frac{\phi(pq)}{4} = \frac{p-1}{2}\frac{q-1}{2}$.
- The number of invertible quadratic residues modulo pqr is $\frac{\phi(pqr)}{8} = \frac{p-1}{2}\frac{q-1}{2}\frac{r-1}{2}$.
- $\ldots$

Armin Straub
straub@southalabama.edu

Proof.

- We already knew that the number of invertible residues modulo n is $\phi(n)$.

- Think about squaring all residues modulo p to make a complete list of all quadratic residues. Let a^2 be one of the nonzero quadratic residues. As we observed earlier, $x^2 \equiv a^2 \pmod{p}$ has exactly 2 solutions, meaning that exactly two residues (namely $\pm a$) square to a^2. Hence, the number of invertible quadratic residues modulo p is half the number of invertible residues modulo p.

  Alternatively. There are $\phi(p)/2$ invertible quadratic residues modulo p and $\phi(q)/2$ invertible quadratic residues modulo q. By the CRT and Lemma 152, it follows that there are $\frac{\phi(p)}{2}\frac{\phi(q)}{2} = \frac{\phi(pq)}{4}$ many invertible quadratic residues modulo pq.

- Again, think about squaring all residues modulo pq to make a complete list of all quadratic residues. Let a^2 be one of the invertible quadratic residues. By the CRT, $x^2 \equiv a^2 \pmod{pq}$ has exactly 4 solutions (why is it important that a is invertible here?!), meaning that exactly four residues square to a^2. Hence, the number of invertible quadratic residues modulo pq is a quarter of the number of invertible residues modulo pq.

- Spell out the situation modulo pqr! □

Comment. Make similar statements when one of the primes is equal to 2.

Example 154. Why do mathematicians confuse Halloween and Christmas?

Because 31 Oct = 25 Dec.

Get it? $(31)_8 = 1 + 3 \cdot 8 = 25$ equals $(25)_{10} = 25$.

Fun borrowed from: https://en.wikipedia.org/wiki/Mathematical_joke

Example 155. (more terrible jokes, parental guidance advised)

There are 10 types of people... those who understand binary, and those who don't.

Of course, you knew that. How about:

There are II types of people... those who understand Roman numerals, and those who don't.

It's not getting any better:

There are 10 types of people... those who understand hexadecimal, F the rest...

17 Wilson's theorem

Example 156. What can you say about factors of $n! + 1$? Is $n! + 1$ composite infinitely often? Is it prime infinitely often?

Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12
$n!+1$	2	3	7	5^2	11^2	$7 \cdot 103$	71^2	$61 \cdot 661$	$19 \cdot 71 \cdot 269$	$11 \cdot 329,891$	$39,916,801$	$13^2 \cdot 2,834,329$

- Every factor $m \geqslant 2$ of $n! + 1$ has to be bigger than n. That's because, if $m \leqslant n$, then $n! + 1 \equiv 1 \pmod{m}$.

  Comment. In other words, the number $n! + 1$ has the property that all its prime factors are bigger than n. This observation provides us with another proof that there are infinitely many primes (see below).

- By Wilson's theorem (which we discuss below), if p is a prime, then p divides $(p-1)! + 1$. Hence, $n! + 1$ is composite whenever $n + 1$ is prime (so that $n = p - 1$ for some prime p).

- It is not known whether $n! + 1$ is prime infinitely often. $n! + 1$ is prime for $n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, \ldots$. Only 21 such "factorial primes" are currently known, the largest being $n = 150209$.

  https://en.wikipedia.org/wiki/Factorial_prime

  For comparison, the largest known prime is $2^{82,589,933} - 1$ (a Mersenne prime; possibly the 51st). It has a bit over 24.8 million (decimal) digits.

Another proof of Euclid's theorem. In order to show that there are infinitely many primes, it is sufficient to observe that there doesn't exist a largest prime number. Indeed, as noted above, the number $n! + 1$ has the property that all its prime factors are bigger than n, so that arbitrarily large primes exist.

The data in the above table suggests that, if p is a prime, then p divides $(p-1)! + 1$.

Apparently, this was guessed by John Wilson, a student of Waring who mentions this in his 1770 algebra book. Neither of these two could prove it at the time (and were pessimistic about it); Lagrange proved it in 1771.

The first few cases. As in the table above:

If $p = 2$, then $(p-1)! + 1 = 2$ is divisible by 2.

If $p = 3$, then $(p-1)! + 1 = 3$ is divisible by 3.

If $p = 5$, then $(p-1)! + 1 = 25$ is divisible by 5.

[If $p = 6$, then $(p-1)! + 1 = 121$ is not divisible by 6.]

If $p = 7$, then $(p-1)! + 1 = 721$ is divisible by 7.

Theorem 157. (Wilson) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. We can check the case $p = 2$ directly (as we did in the previous example).

Note that $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ modulo p is the product of all invertible values modulo p. Our main idea is to pair each x in this product with its inverse x^{-1} modulo p (different elements have different inverses), and to use $x \cdot x^{-1} \equiv 1 \pmod{p}$ so that those terms cancel unless $x \equiv x^{-1}$.

Because p is a prime, the congruence $x \equiv x^{-1} \pmod{p}$ or, equivalently, $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv \pm 1 \pmod{p}$. Hence, $(p-1)! \equiv 1 \cdot (-1) = -1 \pmod{p}$ because the contribution of any other value x is cancelled by $x^{-1} \pmod{p}$. □

For instance. Go through the proof for $p = 7$. In that case, $2^{-1} \equiv 4$, $3^{-1} \equiv 5$.

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

Corollary 158. 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 a good primality test in practice. 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 $p = 2$ $(n = 4)$.

18 Euler's criterion for quadratic residues

Example 159. 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 quadratic residues.
In other words, there is a 50% chance that a random residue (modulo a prime p!) is a quadratic residue. 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 quadratic residues) is a quadratic residue 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 160. (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 $a^{(p-1)/2} \equiv 1 \pmod{p}$.

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 $a x^{-1}$ modulo p [note how $a x^{-1}$ gets paired with $a(a x^{-1})^{-1} \equiv x$], and use $x\cdot(a x^{-1}) \equiv a \pmod{p}$.

Again, we have to be careful about elements that might pair with themselves. Because p is a prime, the congruence $x \equiv a x^{-1} \pmod{p}$ 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

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

□

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 161. 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 162. 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 163. (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 not 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