17 Quadratic residues

Definition 132. An integer a is a **quadratic residue** modulo n if $a \equiv x^2 \pmod{n}$ for some x.

Example 133. 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 134. 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. Example 135 explains why this always happens for such n.

Example 135. Let m, n be coprime. Show that a is a quadratic residue modulo mn if and only if a is a quadratic residue modulo both m and n.

Solution. 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 $a \equiv X^2 \pmod{n}$.

Corollary. Suppose that p, q are distinct primes. There are $(p-1)/2$ invertible quadratic residues modulo p, and $(q-1)/2$ invertible quadratic residues modulo q. By the CRT and the argument above, it follows that there are $\frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{\phi(p)\phi(q)}{4} = \frac{\phi(pq)}{4}$ many invertible quadratic residues modulo pq.

Suppose p, q are distinct primes.

- Modulo p, there are $\phi(p)$ invertible residues, of which $\frac{\phi(p)}{2}$ are quadratic residues.
- Modulo pq, there are $\phi(pq)$ invertible residues, of which $\frac{\phi(pq)}{4}$ are quadratic residues.

Example 136. 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.

Armin Straub
straub@southalabama.edu

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.

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

Theorem 137. 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 $p \equiv 1 \pmod 4$.

Solution. Let us first see that $p \equiv 1 \pmod 4$ is necessary. Assume $x^2 \equiv -1 \pmod p$. Then, by Fermat's little theorem, $x^{p-1} \equiv 1 \pmod p$. On the other hand, $x^{p-1} = (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$. We therefore need $(-1)^{(p-1)/2} = 1$, which is equivalent to $(p-1)/2$ being even. Which is equivalent to $p \equiv 1 \pmod 4$. (Make sure that's absolutely clear!)

On the other hand, assume that $p \equiv 1 \pmod 4$. Instead of $1, 2, \ldots p-1$, let us use the residues $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$ in Wilson's congruence to get:

$$-1 \equiv (p-1)! \equiv (\pm 1) \cdot (\pm 2) \cdot \ldots \cdot \left(\pm \frac{p-1}{2}\right) = (-1)^{(p-1)/2} \left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 = \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

In the last step, we used $(-1)^{(p-1)/2} = 1$ since $p \equiv 1 \pmod 4$. Hence, $x = \left(\frac{p-1}{2}\right)!$ has the property that $x^2 \equiv -1 \pmod p$.

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.

Examples. Let us check our proof by computing $\left(\frac{p-1}{2}\right)!$ for a few primes p. If $p \equiv 1 \pmod 4$, then (and only then) this is a solution to $x^2 \equiv -1 \pmod p$.

$p = 5$: $x = \left(\frac{p-1}{2}\right)! = 2! = 2$. Indeed, $2^2 \equiv -1 \pmod 5$.

$p = 7$: $x = \left(\frac{p-1}{2}\right)! = 3! = 6$. But $6^2 \equiv 1 \not\equiv -1 \pmod 7$ because $7 \not\equiv 1 \pmod 4$.

$p = 13$: $x = \left(\frac{p-1}{2}\right)! = 720 \equiv 5 \pmod{13}$. Indeed, $5^2 \equiv -1 \pmod{13}$.

Comment. Note that we should not have computed $6! = 720$ in the example modulo 13. Instead, we should have reduced $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ modulo 13 after each multiplication, so as to never work with big numbers.

Advanced comment. Still, this is not a particularly good way of actually computing a square root of -1 modulo p if p is large. A better way rests on the observation that, if a is such that $a^{(p-1)/2} \equiv -1$, then $x = a^{(p-1)/4}$ satisfies $x^2 \equiv -1$. (See Euler's criterion below, why every second a does the trick.)

A more general result. (Euler's criterion) Let p be an odd prime, and $\gcd(a, p) = 1$. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.

Another 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 $r_0 \in \{0, 1\}$.