## 15 Quadratic residues

**Definition 146.** An integer $a$ is a **quadratic residue** modulo $n$ if $a \equiv x^2 \pmod{n}$ for some $x$.

**Example 147.** 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 148.** 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 149 explains why this always happens for such $n$.

**Lemma 149.** 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 150.** 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 $\frac{\phi(pqr)}{8} = \frac{p-1}{2}\frac{q-1}{2}\frac{r-1}{2}$.
- ...

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 149, 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, $x^2 \equiv a^2 \pmod{p}$ 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 151.** 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 152. (more terrible jokes, parental guidance advised)**

*There is I0 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 I0 types of people... those who understand hexadecimal, F the rest...*

## 16 Wilson's theorem

**Example 153.** 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 is 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 154. (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, $2^{-1}\equiv 4$, $3^{-1}\equiv 5$.