Quadratic reciprocity

Math Meet 2026

Introduction

If p is a prime number, we can do arithmetic *modulo* p by replacing numbers with the remainder when they are divided by p. We can always choose a remainder r for which $0 \le r < p$. For example, suppose we work modulo 3. Then since $7 + 4 = 11 = 3 \cdot 3 + 2$, we can write

$$11 \bmod 3 = 2 \tag{1}$$

to indicate that the remainder when dividing 11 by 3 is 2. We can also use the notation

$$x \equiv y \pmod{p} \tag{2}$$

to mean that x and y leave the same remainder when divided by p, or equivalently, that $x - y$ is a multiple of p. So, for instance

$$7 + 4 \equiv 2 \pmod{3} \text{ and } 17 \equiv 52 \pmod{5} \tag{3}$$

It turns out that addition, subtraction, multiplication, and division are well behaved modulo a prime: If $a \equiv b \pmod{p}$ and $c \equiv d \pmod{p}$, then

- $a + c \equiv b + d \pmod{p}$
- $a \cdot c \equiv b \cdot d \pmod{p}$

So, for example,

$$\begin{gathered} 7 + 4 \equiv 1 + 1 \equiv 2 \pmod{3} \\ \text{and} \\ -8 \equiv 0 - 8 \equiv 11 - 8 \equiv 3 \pmod{11} \end{gathered} \tag{4}$$

Division also works. If $c \not\equiv 0 \pmod{p}$, then it has a multiplicative inverse c^{-1}. For example, $3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$, so $3 \equiv 4^{-1} \pmod{p}$.

Questions

1. What is $3 + 5 \cdot 20 \bmod 7$?
2. What is $13^2 \bmod 11$?
3. What is $3^{-1} \bmod 5$? That is, find a number $x \in \{0, 1, 2, 3, 4\}$ that satisfies $3x \equiv 1 \pmod{5}$.

Quadratic residues

Working mod p, an integer a is a *quadratic residue* if it's equivalent to the square of some other number mod p. An integer that isn't a quadratic residue mod p is called a *quadratic non-residue*.

Let's denote the quadratic residues for a given p by $\mathscr{R}_p$ and the non-residues by $\mathscr{N}_p$. Zero and other multiples of p (all of which are equivalent to 0 mod p) are a special case, so we'll leave them out. In symbols, let's define

$$\mathscr{R}_p = \left\{ n \in \mathbb{Z} \;\middle|\; n \equiv x^2 \pmod{p} \text{ has a non-zero solution } x \right\}$$
$$\text{and} \tag{5}$$
$$\mathscr{N}_p = \left\{ n \in \mathbb{Z} \;\middle|\; n \equiv x^2 \pmod{p} \text{ has no solution} \right\}$$

When listing out $\mathscr{R}_p$ and $\mathscr{N}_p$, we'll abbreviate and only list the remainders mod p. For instance, the remainders when $1, 4, 9, 16, 25, 36, \ldots$ are divided by 7 are $1, 2, 4, 2, 2, 4, 1, \ldots$, so

$$\mathscr{R}_7 = \{1, 2, 4\} \pmod{7} \text{ and } \mathscr{N}_7 = \{3, 5, 6\} \pmod{7}. \tag{6}$$

We'll still write things like $18 \in \mathscr{R}_7$ because $18 \equiv 4 \equiv 2^2 \pmod{7}$.

With more number theory, you can prove that if we exclude 0,
- the product of two residues is another residue
- the product of two non-residues is actually a residue
- the product of a residue and a non-residue is a non-residue

So for example,
- $2 \cdot 2 \in \mathscr{R}_7$
- $3 \cdot 5 \in \mathscr{R}_7$
- $2 \cdot 3 \in \mathscr{N}_7$

Questions

4. What is $\mathscr{R}_{11}$?
5. What is $\mathscr{N}_{11}$?

Gauss's favorite theorem: Quadratic reciprocity

Mathematicians Adrien-Marie Legendre and Leonhard Euler conjectured that the status of q as a residue or non-residue mod p is determined by whether p is a residue or non-residue mod q. The exact statement of this *quadratic reciprocity* theorem for distinct odd primes p and q is as follows:
- If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then $p \in \mathscr{R}_q$ if and only if $q \in \mathscr{R}_p$.
- If both $q \equiv 3 \pmod{4}$ and $p \equiv 3 \pmod{4}$, then $p \in \mathscr{R}_q$ if and only if $q \in \mathscr{N}_p$.

That is, if at least one of p and q is of the form $4k + 1$, then their statuses as residues are symmetric. If both are of the form $4k + 3$, then their statuses as residues are opposites.

A few other special cases:
- $-1 \in \mathscr{R}_p$ if and only if $p \equiv 1 \pmod{4}$
- $2 \in \mathscr{R}_p$ if and only if $p \equiv \pm 1 \pmod{8}$

This result was first proved by Gauss. It was his favorite theorem. He published six proofs and had unpublished notes for two more.

Legendre used a useful shorthand:

$$\left(\!\left(\frac{x}{p}\right)\!\right) = \begin{cases} 1 & \text{if } x \in \mathscr{R}_p \\ -1 & \text{if } x \in \mathscr{N}_p \\ 0 & \text{if } x \equiv 0 \pmod{p} \end{cases} \tag{7}$$

Then the product properties of quadratic residues can be expressed concisely as

$$\left(\!\!\left(\frac{ab}{p}\right)\!\!\right) = \left(\!\!\left(\frac{a}{p}\right)\!\!\right) \cdot \left(\!\!\left(\frac{b}{p}\right)\!\!\right) \tag{8}$$

and the quadratic reciprocity theorem *for distinct odd primes* can be expressed as

$$\left(\!\!\left(\frac{q}{p}\right)\!\!\right) \cdot \left(\!\!\left(\frac{p}{q}\right)\!\!\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{9}$$

For the cases of $q \equiv -1$ and $q \equiv 2 \pmod{p}$,

$$\left(\!\!\left(\frac{-1}{p}\right)\!\!\right) = (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \left(\!\!\left(\frac{2}{p}\right)\!\!\right) = (-1)^{\frac{p^2-1}{8}}. \tag{10}$$

For example, since $29 \equiv 1 \pmod{7}$ and $1 \in \mathscr{R}_7$,

$$\left(\!\!\left(\frac{29}{7}\right)\!\!\right) = \left(\!\!\left(\frac{1}{7}\right)\!\!\right) = 1. \tag{11}$$

But since $-2 \equiv 5 \pmod{7}$ and $5 \in \mathscr{N}_7$,

$$\left(\!\!\left(\frac{-2}{7}\right)\!\!\right) = \left(\!\!\left(\frac{5}{7}\right)\!\!\right) = -1. \tag{12}$$

Also, $7 \equiv 3 \pmod{4}$ and $6 \equiv -1 \pmod{7}$, so

$$\left(\!\!\left(\frac{6}{7}\right)\!\!\right) = \left(\!\!\left(\frac{-1}{7}\right)\!\!\right) = (-1)^{\frac{7-1}{2}} = (-1)^3 = -1. \tag{13}$$

Finally, $7 \equiv -1 \pmod{8}$ and $9 \equiv 2 \pmod{7}$, so

$$\left(\!\!\left(\frac{9}{7}\right)\!\!\right) = \left(\!\!\left(\frac{2}{7}\right)\!\!\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = 1. \tag{14}$$

The quadratic reciprocity theorem allow us to determine pretty quickly whether any integer is a quadratic residue or non-residue modulo any prime. For example, is 60 a quadratic residue mod 127?

$$\begin{aligned}
\left(\frac{60}{127}\right) &= \left(\frac{2^2 \cdot 3 \cdot 5}{127}\right) \\
&= \left(\frac{2^2}{127}\right) \cdot \left(\frac{3}{127}\right) \cdot \left(\frac{5}{127}\right) \\
&= 1 \cdot -\left(\frac{127}{3}\right) \cdot \left(\frac{127}{5}\right) \qquad (15) \\
&= -\left(\frac{1}{3}\right) \cdot \left(\frac{2}{5}\right) \\
&= -1 \cdot -1 \\
&= 1
\end{aligned}$$

So yes it is! It turns out that $21^2 \equiv 60 \pmod{127}$.

Unfortunately, the quadratic reciprocity theorem is an *existential* result. It only lets you know whether any given n is in $\mathscr{R}_p$ or $\mathscr{N}_p$. If it's in $\mathscr{R}_p$, you know that a solution to $x^2 \equiv n \pmod{p}$ exists, but you'll have to use some other means to find it.

Questions

6. Is 38 a quadratic residue mod 61?
7. Is 39 a quadratic residue mod 61?
8. Is 40 a quadratic residue mod 61?
9. Is 50 a quadratic residue mod 127?
10. Is 51 a quadratic residue mod 127?
11. Is -52 a quadratic residue mod 127?