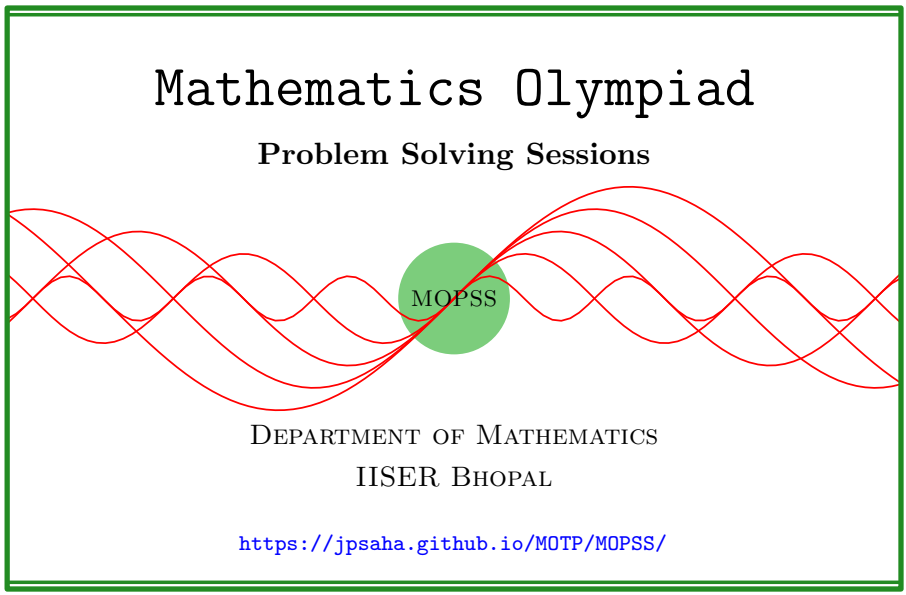
Quadratic reciprocity

MOPSS



Suggested readings

- Evan Chen's advice On reading solutions, available at https://blog.evanchen.cc/2017/03/06/on-reading-solutions/.
- Evan Chen's Advice for writing proofs/Remarks on English, available at https://web.evanchen.cc/handouts/english/english.pdf.
- Notes on proofs by Evan Chen from OTIS Excerpts [**Che25**, Chapter 1].
- Tips for writing up solutions by Edward Barbeau, available at https://www.math.utoronto.ca/barbeau/writingup.pdf.
- Evan Chen discusses why math olympiads are a valuable experience for high schoolers in the post on Lessons from math olympiads, available at https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/.

List of problems and examples

1.1 Exercise . . . 2
1.2 Exercise (Counting squares and non-squares) . . . 2
1.3 Exercise . . . 2
1.4 Exercise . . . 2
1.5 Exercise . . . 3
1.6 Exercise (China TST 2009 P6, AoPS) . . . 3
1.7 Exercise (Belarus TST 2025 P19, AoPS, proposed by V. Kamianetski and Y. Sheshukou) . . . 5

§1 Quadratic reciprocity

In the following, p denotes an odd prime.

For any integer a, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 0 & \text{if } a \text{ is divisible by } p, \\ 1 & \text{if } a \equiv b^2 \pmod{p} \text{ for some integer } b \text{ not divisible by } p, \\ -1 & \text{if } a \not\equiv b^2 \pmod{p} \text{ for any integer } b. \end{cases}$$

Exercise 1.1. Show that the number of solutions of $x^2 \equiv a \bmod p$ is given by

$$1 + \left(\frac{a}{p}\right).$$

Exercise 1.2 (Counting squares and non-squares)**.** Show that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Exercise 1.3. Prove that

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0$$

holds for any integers a, b with $p \nmid a$.

Note that the sums in the above problems are over different sets.

Exercise 1.4. Let a be an integer. Show that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is given by

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right).$$

Exercise 1.5. Let a be an integer. Prove that the number of solutions to $x^2 - y^2 \equiv a \bmod p$ is equal to

$$\begin{cases} p-1 & \text{if } p \nmid a, \\ 2p-1 & \text{if } p \mid a. \end{cases}$$

Corollary 1

Prove that

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p} \right) = \begin{cases} -1 & \text{if } p \nmid a, \\ p-1 & \text{if } p \mid a, \end{cases}$$

$$\sum_{y=0}^{p-1} \left(\frac{a-y^2}{p} \right) = \begin{cases} -\left(\frac{-1}{p}\right) & \text{if } p \nmid a, \\ (p-1)\left(\frac{-1}{p}\right) & \text{if } p \mid a. \end{cases}$$

Lemma 2

Let p be an odd prime. Then for any integer a, the congruence

$$\left(\frac{a}{p} \right) \equiv a^{(p-1)/2} \bmod p$$

holds.

Walkthrough — Count the squares! Does Exercise 1.2 help?

Exercise 1.6 (China TST 2009 P6, AoPS)**.** Determine whether there exists an arithmetic progression consisting of 40 terms and each of whose terms can be written in the form $2^m + 3^n$ or not, where m, n are nonnegative integers.

Here is an argument by AoPS user iceillusion.

Walkthrough —

(a) On the contrary, let us assume that there exists such a progression of length 23.

(b) Put $p = 23$. Note that

$$\left(\frac{2}{p} \right) = \left(\frac{3}{p} \right) = 1, \quad \left(\frac{-1}{p} \right) = -1.$$

It follows that the terms of the progression are nonzero modulo p, and hence at two of those 23 term progression are congruence modulo p. This

shows that their common difference is divisible by p, and hence the 23 terms are congruent to a nonzero residue a modulo p.

(c) Prove the following.

> **Claim —** For any integer a with $p \nmid a$, the number of pairs (x, y) of nonzero quadratic residues modulo p, satisfying $x + y \equiv a \bmod p$ is equal to
>
> $$= \frac{1}{4}\sum_{y=1}^{p-1}\left(1+\left(\frac{a-y^2}{p}\right)\right) - \frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)$$
> $$= \frac{1}{4}\left(p-1-\left(\frac{-1}{p}\right)-\left(\frac{a}{p}\right)-\left(1+\left(\frac{a}{p}\right)\right)\right)$$
> $$= \frac{1}{4}\left(p-2-\left(\frac{-1}{p}\right)-2\left(\frac{a}{p}\right)\right).$$

(d) Consider the 23 pairs $(2^m, 3^n)$ corresponding to the 23 terms of the progression. Note that these pairs, when reduced modulo p, can take at most

$$\frac{1}{4}\left(p-2-\left(\frac{-1}{p}\right)-2\left(\frac{a}{p}\right)\right) \leq \frac{p-3}{4} = 5$$

values. By the pigeonhole principle, it follows that at least five pairs among these 23 pairs, are congruent to each other modulo p.

(e) Note that the integers $2, 3$ are of order 11 modulo 23. It follows that the pairs of the exponents (m, n), corresponding to these five congruent pairs, are congruent to each other modulo 11.

(f) This produces three suitable positive integers of the form $x + k_1 d, x + k_2 d, x + k_3 d$, with $1 \leq k_1 < k_2 < k_3 \leq 22$.

(g) Obtain a contradiction!

Solution 1. ■

Lemma 3

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. Let $\mathbb{Z}[i]$ denote the set of complex numbers whose real and imaginary parts are integers. For two elements z_1, z_2 of $\mathbb{Z}[i]$, we write

$$z_1 \equiv z_2 \bmod p$$

if the real part and the imaginary part of $z_1 - z_2$ are multiples of p.

The content posted here and at this blog by Evan Chen are quite useful.

Note that

$$(1+i)^p = (1+i)(2i)^{(p-1)/2} = (1+i)i^{(p-1)/2}2^{(p-1)/2}$$

holds, which yields

$$\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1 + i(-1)^{(p-1)/2} \bmod p.$$

This shows that

$$\left(\frac{2}{p}\right) = \begin{cases} (-1)^{(p-1)/4} & \text{if } \frac{p-1}{2} \text{ is even,} \\ (-1)^{(p+1)/4} & \text{if } \frac{p-1}{2} \text{ is odd.} \end{cases}$$

□

Lemma 4 (Quadratic reciprocity)
Let p, ℓ be distinct odd primes. Then the following holds:

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

Exercise 1.7 (Belarus TST 2025 P19, AoPS, proposed by V. Kamianetski and Y. Sheshukou)**.** Find all prime numbers p such that $4p+1$ divides $3^p - 1$.

Walkthrough —

(a) Check that $p = 3$ works.

(b) Assume that $p > 3$ is a prime number such that $4p+1$ divides $3^p - 1$. Show that any prime divisor of $4p+1$ is at least as large as $p+2$. Using this, show that $4p+1$ is a prime number.

(c) Prove that 3 is a quadratic residue modulo $4p+1$.

(d) Use the law of quadratic reciprocity to obtain a contradiction.

Solution 2. Note that $p = 3$ works. It remains to consider the case that $p > 3$, which we assume from now on.

Claim — Let $p > 3$ be a prime number. Assume that $4p+1$ divides $3^p - 1$. Then $4p+1$ is a prime number.

Proof of the Claim. Let q be a prime divisor of $4p+1$. Note that the order of 3 modulo q divides both p and $q-1$. Since q is odd, it follows that the order of 3 modulo q is equal to p. Therefore, p divides $q-1$, which yields

$$q \geq p+1.$$

Since p, q are odd, we obtain $q \geq p+2$. This shows that any prime divisor of $4p+1$ is at least as large as $p+2$. If $4p+1$ is not a prime, then the smallest prime divisor r of $4p+1$ satisfies

$$p+2 \leq r \leq \sqrt{4p+1},$$

which is impossible. Hence $4p+1$ is a prime. □

Let $p > 3$ be a prime number such that $4p+1$ divides $3^p - 1$. Since $4p+1$ is a prime and it divides $3^p - 1$, it follows that 3 is a quadratic residue modulo $4p+1$. Also note that 3 is a nonzero quadratic residue modulo $4p+1$. By the law of quadratic reciprocity, we have that $4p+1$ is a quadratic residue modulo 3. This implies that $4p+1 \equiv 1 \pmod 3$, which is equivalent to $p \equiv 0 \pmod 3$. This contradicts that $p > 3$ is a prime.

Therefore, $p = 3$ is the only prime number such that $4p+1$ divides $3^p - 1$. ■

> **Remark.** Note that if p is a prime and some prime divisor of $4p+1$ is at least as large as $p+2$, then it is not necessary that $4p+1$ is a prime. In fact, for $p = 5$, note that $4p+1$ is composite and it admits $p+2$ as a prime factor.

References

[**Che25**] Evan Chen. *The OTIS Excerpts*. Available at https://web.evanchen.cc/excerpts.html. 2025, pp. vi+289 (cited p. 1)