



52. Austrian Math Olympiads (ÖMO)

Special Math. Olympiad course "Mathematik macht Freu(n)de" – Problem sheet for Jan, 16th, 2021

Procedure

These notes are created by Irfan Glogić. Please send questions and (sketches of) solutions to Problems [via E-Mail](#). We provide hints on Jan, 12th, 2021. Irfan addresses the problems at the [virtual course](#) on Jan, 16th, 2021: 13:15–15:00. You can discuss your solutions there. Afterwards we provide complete solutions to the problems. [Contact us](#), if you want to take part in this course. You are always welcome!

The notes are self-contained, and apart from basic elementary number theory facts no additional knowledge is necessary to follow them. To do the exercises, the ideas that appear beforehand in notes should for the most part suffice. Also, exercises have expository significance, and I strongly advise solving (or at least trying) every one of them in the order they appear. The problems, on the other hand, might in addition require a non-trivial idea/trick/fact (which makes them competition type), and they can be skipped at the first reading. Nonetheless, their placement in notes indicates the (quadratic residue) theory necessary to solve them. Harder problems are indicated with an asterisk.

Quadratic Residues

Irfan Glogić

1 Basic definitions and theorems

Definition 1.1. Let m and a be integers with $m > 1$ and $(m, a) = 1$. We say that a is a *quadratic residue modulo m* if there exists an integer x for which $x^2 \equiv a \pmod{m}$, otherwise a is called a *quadratic non-residue modulo m* .

Theorem 1.2. Let p be an odd prime. Within the reduced set $\{1, 2, \dots, p-1\}$ of residues modulo p , there are exactly $\frac{p-1}{2}$ quadratic residues, and consequently equally many quadratic non-residues.

Proof. Every quadratic residue modulo p is congruent to the square of one of the following numbers

$$-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2},$$

i.e., it is congruent to one of these, $1^2, 2^2, \dots, (\frac{p-1}{2})^2$. It remains to show that these numbers are pairwise incongruent modulo p . This is left as an exercise. \square

Exercise 1.3. Complete the proof of Theorem 1.2.

For an odd prime p we define the function $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \rightarrow \{-1, 0, 1\}$ in the following way

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic non-residue (mod } p), \\ 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue (mod } p). \end{cases} \quad (1.1)$$

The quantity in (1.1) is referred to as *Legendre symbol*.

Theorem 1.4 (Euler's criterion). *For an odd prime p we have that*

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

Proof. First assume $\left(\frac{a}{p}\right) = 1$. Then there exists an integer x_0 for which $x_0^2 \equiv a \pmod{p}$, and by using Fermat's little theorem we see that

$$a^{(p-1)/2} = (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \pmod{p}.$$

Now assume $\left(\frac{a}{p}\right) = -1$. Since $(a, p) = 1$ for every $i \in \{1, 2, \dots, p-1\}$, there exists a unique j from the same set such that $j \neq i$ and $ij \equiv a \pmod{p}$ (this is left as an exercise). Therefore, numbers $1, 2, \dots, p-1$ can be grouped in pairs whose products are congruent to a modulo p . After multiplying all of these pairs we get

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p},$$

and the conclusion follows from Wilson's theorem. \square

Exercise 1.5. Let p be an odd prime and a, b integers not divisible by p . Show that

- i) $a \equiv b \pmod{p}$ implies $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
- ii) $\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ and $\left(\frac{a^2}{p}\right) = 1$.

Problem 1.6. Let p be an odd prime. Prove that there exists a positive integer $a < \sqrt{p} + 1$ which is a quadratic non-residue modulo p .

Euler's criterion applied to $a = -1$ yields $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Therefore, -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$. This observation yields the following lemma.

Lemma 1.7. *Every prime divisor of $n^2 + 1$ is of the form $4k + 1$.*

Exercise 1.8. By using the previous lemma prove that there are infinitely many prime numbers of the form $4k + 1$.

Problem 1.9. Prove that the equation $y^2 = x^3 + 7$ does not have integer solutions. Generalize this statement to an infinite family of Diophantine equations of the form $y^2 = x^3 + c$.

2 Application of primitive roots

Definition 2.1. Let n be a positive integer. An integer g is called a *primitive root modulo n* if every integer relatively prime to n is congruent to a power of g modulo n .

It is known that primitive roots modulo odd primes exist. Moreover, for a given primitive root g modulo p , the numbers g, g^2, \dots, g^{p-1} form a reduced system of residues. In particular, $g^{(p-1)/2} \not\equiv 1 \pmod{p}$. Furthermore, since $(g^{(p-1)/2})^2 \equiv g^{p-1} \equiv 1 \pmod{p}$ and the equation $x^2 \equiv 1 \pmod{p}$ has exactly two solutions, namely $x \equiv \pm 1 \pmod{p}$, we obtain the following lemma.

Lemma 2.2. *Let g be a primitive root modulo odd prime p . Then*

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

In other words, primitive roots are quadratic non-residues.

Theorem 2.3. *Let g be a primitive root modulo odd prime p . Then quadratic residues modulo p are given by g^2, g^4, \dots, g^{p-1} , and non-residues are g, g^3, \dots, g^{p-2} .*

Proof. Even powers g^2, g^4, \dots, g^{p-1} are obviously quadratic residues modulo p , and since g is a primitive root, these numbers are all distinct (modulo p). Consequently, the odd powers must be non-residues. A more direct way to obtain this later conclusion is the following. Since g is, according to Lemma 2.2, a quadratic non-residue, then g, g^3, \dots, g^{p-2} , i.e., $g \cdot 1, g \cdot g^2, \dots, g \cdot g^{p-3}$ are, according to Exercise 1.5, non-residues. \square

Now, by using Theorem 2.3 we can come up with a short proof of Euler's criterion.

Proof 2 of Theorem 1.4. If $\left(\frac{a}{p}\right) = 1$ then $a \equiv g^{2k} \pmod{p}$ and therefore $a^{(p-1)/2} \equiv (g^{p-1})^k \equiv 1 \pmod{p}$. If $\left(\frac{a}{p}\right) = -1$ then $a \equiv g^{2k+1} \pmod{p}$ and hence $a^{(p-1)/2} \equiv (g^{p-1})^k \cdot g^{(p-1)/2} \equiv 1 \cdot (-1) \equiv -1 \pmod{p}$. \square

3 Gauss' lemma

Theorem 3.1 (Gauss' lemma). *Let $p = 2n + 1$ be a prime number, $A = \{1, 2, \dots, \frac{p-1}{2}\} = \{a_1, a_2, \dots, a_n\}$, and a an integer not divisible by p . Furthermore, let*

$$a_i a \equiv (-1)^{s(i)} a_{t(i)} \pmod{p}, \quad (3.1)$$

for every $a_i \in A$, where $s(i) \in \{0, 1\}$ and $t(i) \in \{1, 2, \dots, n\}$. Then

$$a^n \equiv \prod_{i=1}^n (-1)^{s(i)} \pmod{p}. \quad (3.2)$$

So, a is a quadratic residue or non-residue depending on whether the number of non-zero exponents $s(i)$ is even or not.

Proof. First, observe that $\{a_{t(i)} : 1 \leq i \leq n\} = A$, i.e., $a_{t(i)}$ are a_i reordered. Indeed, if $a_i a \equiv (-1)^{s(i)} a_{t(i)} \pmod{p}$ and $a_j a \equiv (-1)^{s(j)} a_{t(j)} \pmod{p}$ for $i \neq j$ and $a_{t(i)} = a_{t(j)}$, then we would have $a_i/a_j \equiv (-1)^{s(i)-s(j)} \pmod{p}$, i.e., $a_i \equiv \pm a_j \pmod{p}$ for some choice of signs, but that implies $a_i = a_j$ since $1 \leq a_i, a_j \leq \frac{p-1}{2}$, which contradicts $i \neq j$. By multiplying the n congruences (3.1) we get

$$a^n \cdot \prod_{i=1}^n a_i \equiv \prod_{i=1}^n (-1)^{s(i)} \cdot \prod_{i=1}^n a_{t(i)} \pmod{p}.$$

Finally, since $\prod_{i=1}^n a_i = \prod_{i=1}^n a_{t(i)}$, canceling these factors in the previous congruence yields (3.2). \square

By exploiting Gauss' lemma, we can prove the following result.

Lemma 3.2. Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, that is

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$

Proof. For $p \equiv 1$ or $5 \pmod{8}$ we get that $s(i) = 0$ for $1 \leq i \leq (p-1)/4$ and $s(i) = 1$ for $(p+3)/4 \leq i \leq (p-1)/2$, so $2^{(p-1)/2} \equiv (-1)^{(p-1)/4} \pmod{p}$. Therefore $\left(\frac{2}{p}\right) = 1$ or -1 depending on whether $p \equiv 1$ or $5 \pmod{8}$. Similarly we get that $\left(\frac{2}{p}\right) = 1$ or -1 depending on whether $p \equiv 7$ or $3 \pmod{8}$. \square

Based on Euler's criterion and the previous lemma we have that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p+5)(p-1)}{8}}, \quad (3.3)$$

from which it follows that -2 is a quadratic residue modulo odd prime p if and only if $p \equiv 1$ or $3 \pmod{8}$.

Problem 3.3. Let n be a positive integer. Prove that

- i) if n is odd then all prime divisors of $2^n - 1$ are of the form $8k \pm 1$,
- ii) the number $2^n + 1$ has no prime divisors of the form $8k - 1$.

4 The law of quadratic reciprocity

We now formulate (without proof) a fundamental result which relates Legendre symbols $\left(\frac{p}{q}\right)$ i $\left(\frac{q}{p}\right)$ for odd primes p and q .

Theorem 4.1 (The law of quadratic reciprocity (LQR)). Let p and q be distinct odd prime numbers. Then

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

With this theorem at hand we can easily establish the following result.

Lemma 4.2. For an odd prime $p \neq 3$ we have that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{6}, \\ -1 & \text{if } p \equiv 5 \pmod{6}. \end{cases}$$

Proof. According to Euler's criterion and LQR we have that

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

Furthermore, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ if $p \equiv 1 \pmod{3}$, and $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$ if $p \equiv 2 \pmod{3}$. From this and the fact that every prime greater than 3 is of the form $6k \pm 1$ the lemma follows. \square

Exercise 4.3. For an odd prime p show that

- i) 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$,

ii) 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{10}$.

Exercise 4.4. Use part ii) from the previous exercise to show that there are infinitely many prime numbers of the form $10k + 9$.

Problem 4.5. Let n be a positive integer. Prove that all prime divisors of $n^4 - n^2 + 1$ are of the form $12k + 1$.

Problem 4.6.* Let a be a positive integer which is not a square. Prove that $\left(\frac{a}{p}\right) = -1$ for infinitely many primes p .

5 Additional problems

Problem 5.1. Prove that for every prime p there are integers a, b such that $p \mid a^2 + b^2 + 1$.

Problem 5.2. Prove that for no integer $n > 1$ does $2^n - 1$ divide $3^n - 1$.

Problem 5.3. Let n be a positive integer. Prove that all prime divisors of $n^8 - n^4 + 1$ are of the form $24k + 1$.

Problem 5.4.* Prove that there are no positive integers a, b, c for which $3(ab + bc + ca) \mid a^2 + b^2 + c^2$.

Problem 5.5.* Let m and n be positive integers for which $A = \frac{(m+3)^n + 1}{3^m}$ is also an integer. Prove that A is odd.

Problem 5.6.* Let m and n be positive integers for which $\varphi(5^m - 1) = 5^n - 1$. Prove that m and n are not relatively prime.

Hints to problems

Problem 1.6. Assume contrary, and let $a \geq \sqrt{p} + 1$ be the least non-residue. Then construct a smaller one.

Problem 1.9. Consider $y^2 + 1$, and use Lemma 1.7.

Problem 3.3. i) Find $(\frac{2}{p})$. ii) Find $(\frac{-1}{p})$ or $(\frac{-2}{p})$, depending on the parity of n .

Problem 4.5. Note that $n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2 = (n^2 + 1)^2 - 3n^2$.

Problem 4.6. Use Dirichlet's theorem on primes in arithmetic progressions.

Problem 5.1. Consider $b = na$.

Problem 5.2. Show existence of a prime which divides $2^n - 1$ but not $3^n - 1$.

Problem 5.3. Use Problem 4.5 and the fact that $n^{12} + 1 = (n^4 + 1)(n^8 - n^4 + 1)$.

Problem 5.4. Assume contrary and then exploit the fact that $(a+b+c)^2 = (3n+2)(ab+bc+ca)$.

Problem 5.5. Assume contrary and study m modulo powers of 2.

Problem 5.6. Consider the prime factorization of $5^m - 1$.

Solution to problems

Solutions proposed by Irfan Glogić, edited by the MmF-Team

Problem 1.6. We argue by contradiction. Assume $a \geq \sqrt{p} + 1$ is the least quadratic non-residue. Then define $b := \lfloor \frac{p}{a} \rfloor + 1$. Note that $b < \sqrt{p} + 1$ and therefore b is a quadratic residue. Then by Exercise 1.5 we have that $ab - p$ is a non-residue, but also $0 < ab - p < a$, which is a contradiction with the minimality of a .

Problem 1.9. By considering the equation modulo 4, we conclude that x must be odd. In addition, we have that $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4) = (x + 2)[(x^2 - 1)^2 + 3]$, and since the quadratic factor on the right is of the form $4k + 3$, it must have a prime divisor of the same form. But this prime then divides $y^2 + 1$ as well, which is impossible by Lemma 1.7. To generalize, one can take $c = 8a^3 - 1$ for any odd a .

Problem 3.3. i) Let $n = 2m + 1$ and take a prime p which divides $2^n - 1$. Then $1 \equiv 2(2^m)^2 \pmod{p}$, i.e., $2 \equiv (2^{-m})^2 \pmod{p}$, so $(\frac{2}{p}) = 1$ and by Lemma 3.2 the conclusion follows.
ii) Assume the contrary, that there exists a prime $p = 8k - 1$ which divides $2^n + 1$. If n is even then $-1 \equiv (2^{n/2})^2 \pmod{p}$, so $1 = (\frac{-1}{p}) = (-1)^{(p-1)/2} = (-1)^{4k-1} = -1$, a contradiction. If n is odd then $-2 \equiv (2^{(m+1)/2})^2 \pmod{p}$, so $1 = (\frac{-2}{p}) = (-1)^{(p+5)(p-1)/8} = (-1)^{(2k+1)(4k-1)} = -1$, a contradiction.

Problem 4.5. The observation from the hint implies that for every prime divisor p we have

$$\left(\frac{n^2 - 1}{n}\right)^2 \equiv -1 \pmod{p} \quad \text{and} \quad \left(\frac{n^2 + 1}{n}\right)^2 \equiv 3 \pmod{p}.$$

So $(\frac{-1}{p}) = (\frac{3}{p}) = 1$, which, based on Euler's criterion and Exercise 4.3, implies that $p \equiv 1 \pmod{12}$.

Problem 4.6. Without loss of generality we can assume that a is not divisible by a square. If $a = 2$ the claim follows from Lemma 3.2 and the infinitude of primes of the form $8k + 3$. We therefore assume $a > 2$. Then we have the prime factorization $a = 2^\alpha p_1 p_2 \dots p_k$, where $\alpha \in \{0, 1\}$. Furthermore, for every odd prime p we have by LQR that

$$\left(\frac{a}{p}\right) = \left(\frac{2^\alpha}{p}\right) \prod_{i=1}^k \left(\frac{p_i}{p}\right) = \left(\frac{2^\alpha}{p}\right) \prod_{i=1}^k (-1)^{\frac{p_i-1}{2} \frac{p-1}{2}} \left(\frac{p}{p_i}\right). \quad (5.1)$$

Now we prove that there are infinitely many p for which the expression on the right of (5.1) is equal to -1 . By the Chinese remainder theorem there is an integer x for which

$$x \equiv 1 \pmod{8}, \quad x \equiv 1 \pmod{p_i} \text{ for } 1 \leq i \leq k-1, \quad \text{and} \quad x \equiv b \pmod{p_k}$$

where b is an arbitrary quadratic non-residue modulo p_k . Since $(8a, x) = 1$, according to Dirichlet's theorem about primes in arithmetic progressions we conclude that there are infinitely many primes p of the form $p = 8an + x$, for all of which, based on (5.1), we have that $(\frac{a}{p}) = -1$.

Problem 5.1. If $p = 4k + 1$ then $\left(\frac{-1}{p}\right) = 1$, i.e., $-1 \equiv x^2 \pmod{p}$ for some integer x . Then we take $a = x$ and $b = 0$. If $p = 4k + 3$ then the set $\{n^2 + 1 : 0 \leq n \leq \frac{p-1}{2}\}$ consists of $\frac{p+1}{2}$ numbers not divisible by p and pairwise incongruent modulo p . Consequently, this set contains a quadratic non-residue, call it $n_0^2 + 1$. Then $-1 \cdot (n_0^2 + 1)^{-1}$ is a quadratic residue, so there exists integer x for which $x^2 \equiv -(n_0^2 + 1)^{-1} \pmod{p}$, and the claim holds for $a = x$ and $b = n_0x$.

Problem 5.2. If n is even then $3 \mid 2^n - 1$ but $3 \nmid 3^n - 1$. Let n be odd. Then $3 \nmid 2^n - 1$ and therefore $2^n - 1$ is of the form $12k \pm 5$, so it must have a prime divisor p of the same form. On the other hand, $p \mid 3(3^n - 1)$ i.e. $(3^{(n+1)/2})^2 \equiv 3 \pmod{p}$, so $\left(\frac{3}{p}\right) = 1$. But, according to Exercise 4.3, this is impossible.

Problem 5.3. Let p be a prime divisor of $n^8 - n^4 + 1$. By Problem 4.5, it follows that $p \equiv 1 \pmod{3}$. It remains to show that $p \equiv 1 \pmod{8}$. Note that $p \mid (n^4 + 1)(n^8 - n^4 + 1) = n^{12} + 1$, i.e., $n^{12} \equiv -1 \pmod{p}$. It follows that $\text{ord}_p n$ divides 24 but not 12, so $\text{ord}_p n \in \{8, 24\}$. Since $\text{ord}_p n \mid p - 1$, in both cases we have that $8 \mid p - 1$, and the claim follows.

Problem 5.4. Assume the contrary, that there are a, b, c and n for which $a^2 + b^2 + c^2 = 3n(ab + bc + ca)$. From this it follows that $(a + b + c)^2 = (3n + 2)(ab + bc + ca)$, and since $3n + 2$ can not be a square, there is a prime $p \equiv 2 \pmod{3}$ which divides all three factors in the last equality. In particular, $p \mid a + b + c$ and $p \mid ab + bc + ca$, from which it follows that $p \mid a^2 + ab + b^2$, and from there $p \mid (2a + b)^2 + 3c^2$. Consequently $\left(\frac{-3}{p}\right) = 1$. Now, according to Lemma 4.2, we have that $p \equiv 1 \pmod{3}$, but this is in contradiction with $p \equiv 2 \pmod{3}$.

Problem 5.5. Assume the contrary, that A is an even number. Then

$$(m + 3)^n + 1 = 6km, \tag{5.2}$$

and therefore m has to be even as well. By considering this equality modulo 3 we conclude that $m = 3l + 2$ and n is odd. Let $m = 2^\alpha m_1$, where m_1 is odd. By considering equality (5.2) modulo 2^α we get that $3^n + 1 \equiv 0 \pmod{2^\alpha}$, which implies $\alpha \leq 2$. Furthermore, we have that $(3^{(n+1)/2})^2 \equiv -3 \pmod{m_1}$, and, according to Lemma 4.2, we conclude that $m_1 = 6m_2 + 1$. From $m = 2^\alpha(6m_2 + 1) = 3l + 2$ and $\alpha \leq 2$ it follows that $\alpha = 1$. Then $m = 12m_2 + 2$, and reducing (5.2) modulo 4 we get $5^n + 1 \equiv 0 \pmod{4}$, which is impossible.

Problem 5.6. Assume the contrary, that $(m, n) = 1$. According to the prime factorization

$$5^m - 1 = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k} \tag{5.3}$$

we have that

$$5^n - 1 = \varphi(5^m - 1) = 2^{\alpha-1} p_1^{\alpha_1-1} \cdots p_k^{\alpha_k-1} (p_1 - 1) \cdots (p_k - 1). \tag{5.4}$$

Since $(5^m - 1, 5^n - 1) = 5^{(m,n)} - 1 = 4$ then from the two displayed equations above we conclude that $\alpha_i = 1$ for all $i = 1, \dots, k$, and $\alpha = 2$. Since $8 \mid 5^m - 1$ for even m , we infer that m is odd, i.e., $m = 2m_1 + 1$. Since $p_i \mid 5 \cdot (5^{m_1})^2 - 1$ for $i = 1, \dots, k$, we see that $\left(\frac{5}{p_i}\right) = 1$, and hence, according to Exercise 4.3, $p_i \equiv \pm 1 \pmod{5}$. Because of (5.4) no $p_i - 1$ is divisible by 5, and therefore $p_i \equiv -1 \pmod{5}$. Now, reducing (5.3) modulo 5 we get $1 = (-1)^k$, i.e., k is even. On the other

hand, reducing (5.4) modulo 5 we get $1 \equiv (-2)^{k+1} \pmod{5}$, implying $k \equiv 3 \pmod{4}$, which is a contradiction with the evenness of k .

References

Unfortunately, the script and the problems are based on former private notes, where no references were noted.