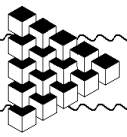
The IMO Compendium Group
Olympiad Training Materials
www.imo.org.yu
www.imocompendium.com



Quadratic Congruences

Dušan Djukić

Contents

1 Quadratic Congruences to Prime Moduli

Definition 1. *Let m, n and a be integers, $m > 1$, $n \geq 1$ and $(a, m) = 1$. We say that a is a residue of n-th degree modulo m if congruence $x^n \equiv a$ (mod m) has an integer solution; else a is a nonresidue of n-th degree.*

Specifically, for $n = 2, 3, 4$ the residues are called quadratic, cubic, biquadratic, respectively. This text is mainly concerned with quadratic residues.

Theorem 1. *Given a prime p and an integer a, the equation $x^2 \equiv a$ has zero, one, or two solutions modulo p.*

Proof. Suppose that the considered congruence has a solution x_1. Then so clearly is $x_2 = -x_1$. There are no other solutions modulo p, because $x^2 \equiv a \equiv x_1^2$ (mod p) implies $x \equiv \pm x_1$. □

As a consequence of the above simple statement we obtain:

Theorem 2. *For every odd positive integer p, among the numbers $1, 2, \ldots, p-1$ there are exactly $\frac{p-1}{2}$ quadratic residues (and as many quadratic nonresidues).* □

Definition 2. *Given a prime number p and an integer a, Legendre's symbol $\left(\frac{a}{p}\right)$ is defined as*

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

Example 1. *Obviously, $\left(\frac{x^2}{p}\right) = 1$ for each prime p and integer x, $p \nmid x$.*

Example 2. *Since 2 is a quadratic residue modulo 7 ($3^2 \equiv 2$), and 3 is not, we have $\left(\frac{2}{7}\right) = 1$ and $\left(\frac{3}{7}\right) = -1$.*

From now on, unless noted otherwise, p is always an odd prime and a an integer. We also denote $p' = \frac{p-1}{2}$.

Clearly, a is a quadratic residue modulo p if and only if so is $a + kp$ for some integer k. Thus we may regard Legendre's symbol as a map from the residue classes modulo p to the set $\{-1, 0, 1\}$.

Fermat's theorem asserts that $a^{p-1} \equiv 1$ (mod p), which implies $a^{p'} \equiv \pm 1$ (mod p). More precisely, the following statement holds:

Theorem 3 (Euler's Criterion). $a^{p'} \equiv \left(\frac{a}{p}\right)$ *(mod p).*

Proof. The statement is trivial for $p \mid a$. From now on we assume that $p \nmid a$.

Let g be a primitive root modulo p. Then the numbers g^i, $i = 0, 1, \ldots, p-2$ form a reduced system of residues modulo p. We observe that $(g^i)^{p'} = g^{ip'} \equiv 1$ if and only if $p-1 \mid ip'$, or equivalently, $2 \mid i$.

On the other hand, g^i is a quadratic residue modulo p if and only if there exists $j \in \{0, 1, \ldots, p-2\}$ such that $(g^j)^2 \equiv g^i \pmod{p}$, which is equivalent to $2j \equiv i \pmod{p-1}$. The last congruence is solvable if and only if $2 \mid i$, that is, exactly when $(g^i)^{p'} \equiv 1 \pmod{p}$. □

The following important properties of Legendre's symbol follow directly from Euler's criterion.

Theorem 4. *Legendre's symbol is multiplicative, i.e.* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *for all integers* a, b *and prime number* $p > 2$. □

Problem 1. *There exists a natural number* $a < \sqrt{p} + 1$ *that is a quadratic nonresidue modulo* p.

Solution. Consider the smallest positive quadratic nonresidue a modulo p and let $b = \left[\frac{p}{a}\right] + 1$. Since $0 < ab - p < a$, $ab - p$ must be a quadratic residue. Therefore

$$1 = \left(\frac{ab-p}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right).$$

Thus b is a quadratic nonresidue and hence $a \leq b < \frac{p}{a} + 1$, which implies the statement.

Theorem 5. *For every prime number* $p > 2$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

In other words, the congruence $x^2 \equiv -1$ modulo a prime p is solvable if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. △

Problem 2. *If* p *is a prime of the form* $4k+1$*, prove that* $x = (p')!$ *is a solution of the congruence* $x^2 + 1 \equiv 0$ *(mod p).*

Solution. Multiplying the congruences $i \equiv -(p-i) \pmod{p}$ for $i = 1, 2, \ldots, p'$ yields $(p')! \equiv (-1)^{p'}(p'+1)\cdots(p-2)(p-1)$. Note that p' is even by the condition of the problem. We now have

$$x^2 = (p')!^2 \equiv (-1)^{p'} p' \cdot (p'+1)\cdots(p-2)(p-1) = (-1)^{p'}(p-1)! \equiv (-1)^{p'+1} = -1 \pmod{p}$$

by Wilson's theorem. △

One can conclude from Problem 1 that every prime factor of number $x^2 + y^2$ (where $x, y \in \mathbb{N}$ are coprime) is either of the form $4k+1$, $k \in \mathbb{N}$, or equal to 2. This conclusion can in fact be generalized.

Theorem 6. *Let* x, y *be coprime integers and* a, b, c *be arbitrary integers. If* p *is an odd prime divisor of number* $ax^2 + bxy + cy^2$ *which doesn't divide* abc*, then*

$$D = b^2 - 4ac$$

is a quadratic residue modulo p.

In particular, if $p \mid x^2 - Dy^2$ *and* $(x, y) = 1$*, then* D *is a quadratic residue (mod* p*).*

Proof. Denote $N = ax^2 + bxy + cy^2$. Since $4aN = (2ax + by)^2 - Dy^2$, we have

$$(2ax + by)^2 \equiv Dy^2 \pmod{p}.$$

Furthermore, y is not divisible by p; otherwise so would be $2ax+by$ and therefore x itself, contradicting the assumption.

There is an integer y_1 such that $yy_1 \equiv 1 \pmod p$. Multiplying the above congruence by y_1^2 gives us $(2axy_1+byy_1)^2 \equiv D(yy_1)^2 \equiv D \pmod p$, implying the statement. □

For an integer a, $p \nmid a$ and $k = 1, 2, \ldots, p'$ there is a unique $r_k \in \{-p', \ldots, -2, -1, 1, 2, \ldots, p'\}$ such that $ka \equiv r_k \pmod p$. Moreover, no two of the r_k's can be equal in absolute value; hence $|r_1|, |r_2|, \ldots, |r_{p'}|$ is in fact a permutation of $\{1, 2, \ldots, p'\}$. Then

$$a^{p'} = \frac{a \cdot 2a \cdot \cdots \cdot p'a}{1 \cdot 2 \cdot \cdots \cdot p'} \equiv \frac{r_1 r_2 \ldots r_{p'}}{1 \cdot 2 \cdot \cdots \cdot p'}.$$

Now, setting $r_k = \epsilon_k |r_k|$ for $k = 1, \ldots, p'$, where $\epsilon_k = \pm 1$, and applying Euler's criterion we obtain:

Theorem 7. $\left(\frac{a}{p}\right) = \epsilon_1 \epsilon_2 \cdots \epsilon_{p'}$. □

Observe that $r_k = -1$ if and only if the remainder of ka upon division by p is greater than p', i.e. if and only if $\left[\frac{2ka}{p}\right] = 2\left[\frac{ka}{p}\right] + 1$. Therefore, $r_k = (-1)^{\left[\frac{2ka}{p}\right]}$. Now Theorem 7 implies the following statement.

Theorem 8 (Gauss' Lemma). $\left(\frac{a}{p}\right) = (-1)^S$, *where* $S = \sum_{k=1}^{p'} \left[\frac{2ka}{p}\right]$. □

Gauss' lemma enables us to easily compute the value of Legendre's symbol $\left(\frac{a}{p}\right)$ for small a or small p. If, for instance, $a = 2$, we have $\left(\frac{2}{p}\right) = (-1)^S$, where $S = \sum_{k=1}^{p'} \left[\frac{4k}{p}\right]$. Exactly $\left[\frac{1}{2}p'\right]$ summands in this sum are equal to 0, while the remaining $p' - \left[\frac{1}{2}p'\right]$ are equal to 1. Therefore $S = p' - \left[\frac{1}{2}p'\right] = \left[\frac{p+1}{4}\right]$, which is even for $p \equiv \pm 1$ and odd for $p \equiv \pm 3 \pmod 8$. We have proven the following

Theorem 9. $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$.

In other words, 2 is a quadratic residue modulo a prime $p > 2$ if and only if $p \equiv \pm 1$ (mod 8).

The following statements can be similarly shown.

Theorem 10. *(a) -2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $p \equiv 3$ (mod 8);*

(b) -3 is a quadratic residue modulo p if and only if $p \equiv 1$ (mod 6);

(c) 3 je quadratic residue modulo p if and only if $p \equiv \pm 1$ (mod 12);

(d) 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1$ (mod 10). □

Problem 3. *Show that there exist infinitely many prime numbers of the form (a) $4k+1$; (b) $10k+9$.*

Solution. (a) Suppose the contrary, that $p_1, p_2, \ldots, p_n$ are all such numbers. Then by Theorem 5, all prime divisors of $N = (2p_1p_2 \cdots p_n)^2 + 1$ are of the form $4k+1$. However, N is not divisible by any of $p_1, p_2, \ldots, p_n$, which is impossible.

Part (b) is similar to (a), with number $N = 5(2p_1p_2 \cdots p_n)^2 - 1$ being considered instead. △

Problem 4. *Prove that for $n \in \mathbb{N}$ every prime divisor p of number $n^4 - n^2 + 1$ is of the form $12k+1$.*

Solution. We observe that

$$n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2 \quad \text{i} \quad n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2.$$

In view of theorems 5, 6, and 10, the first equality gives us $p \equiv 1 \pmod 4$, whereas the other one gives us $p \equiv \pm 1 \pmod{12}$. These two congruences together yield $p \equiv 1 \pmod{12}$. $\triangle$

Problem 5. *Evaluate*

$$\left[\frac{1}{2003}\right] + \left[\frac{2}{2003}\right] + \left[\frac{2^2}{2003}\right] + \cdots + \left[\frac{2^{2001}}{2003}\right].$$

Solution. Note that 2003 is prime. It follows from Euler's criterion and Theorem 10 that $2^{1001} \equiv \left(\frac{2}{2003}\right) = -1 \pmod{2003}$. Therefore $2003 \mid 2^i(2^{1001} + 1) = 2^{1001+i} + 2^i$; since 2^i and 2^{1001+i} are not multiples of 2003, we conclude that

$$\left[\frac{2^i}{2003}\right] + \left[\frac{2^{1001+i}}{2003}\right] = \frac{2^i + 2^{1001+i}}{2003} - 1.$$

Summing up these equalities for $i = 0, 1, \ldots, 1000$ we obtain that the desired sum equals

$$\frac{1 + 2 + 2^2 + \cdots + 2^{2001}}{2003} - 1001 = \frac{2^{2002} - 1}{2003} - 1001. \ \triangle$$

The theory we have presented so far doesn't really facilitate the job if we need to find out whether, say, 814 is a quadratic residue modulo 2003. That will be done by the following theorem, which makes such a verification possible with the amount of work comparable to that of the Euclidean algorithm.

Theorem 11 (Gauss' Reciprocity Law). *For any different odd primes p and q,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'},$$

where $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$.

Proof. Define $S(p, q) = \sum_{k=1}^{q'} \left[\frac{kp}{q}\right]$. We start by proving the following auxiliary statement.

Lemma 1. $S(p, q) + S(q, p) = p'q'$.

Proof of the Lemma. Given $k \in \mathbb{N}$, we note that $\left[\frac{kp}{q}\right]$ is the number of integer points (k, l) in the coordinate plane with $0 < l < kp/q$, i.e. such that $0 < ql < kp$. It follows that the sum $S(p, q)$ equals the number of integer points (k, l) with $0 < k < p'$ and $0 < ql < kp$. Thus $S(p, q)$ is exactly the number of points with positive integer coordinates in the interior or on the boundary of the rectangle $ABCD$ that lie *below* the line AE, where $A(0, 0)$, $B(p', 0)$, $C(p', q')$, $D(0, q')$, $E(p, q)$.

Analogously, $S(q, p)$ is exactly the number of points with positive integer coordinates in the interior or on the boundary of the rectangle $ABCD$ that lie *above* the line AE. Since there are $p'q'$ integer points in total in this rectangle, none of which is on the line AE, it follows that $S(p, q) + S(q, p) = p'q'$. $\triangledown$

We now return to the proof of the theorem. We have

$$S(p + q, q) - S(p, q) = 1 + 2 + \cdots + p' = \frac{p^2 - 1}{8}.$$

Since Theorem 9 is equivalent to $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, Gauss' lemma gives us

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

hence $\left(\frac{p}{q}\right) = (-1)^{S(p,q)}$. Analogously, $\left(\frac{q}{p}\right) = (-1)^{S(q,p)}$. Multiplying the last two inequalities and using the lemma yields the desired equality. □

Let us now do the example mentioned before the Reciprocity Law.

Example 3. $\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right)\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right) = -\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right)$.

Furthermore, the Reciprocity Law gives us

$$\left(\frac{11}{2003}\right) = -\left(\frac{2003}{11}\right) = \left(\frac{1}{11}\right) = 1 \quad \textit{and} \quad \left(\frac{37}{2003}\right) = \left(\frac{2003}{37}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = -1.$$

Thus $\left(\frac{814}{2003}\right) = 1$*, i.e.* 814 *is a quadratic residue modulo* 2003*.*

Problem 6. *Prove that an integer a is a quadratic residue modulo every prime number if and only if a is a perfect square.*

Solution. Suppose that a is not a square. We may assume w.l.o.g. (why?) that a is square-free.

Suppose that $a > 0$. Then $a = p_1 p_2 \cdots p_k$ for some primes $p_1, \ldots, p_k$. For every prime number p it holds that

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{k}\left(\frac{p_i}{p}\right) \quad \text{and} \quad \left(\frac{p_i}{p}\right) = (-1)^{p_i' p'}\left(\frac{p}{p_i}\right). \tag{1}$$

If $a = 2$, it is enough to choose $p = 5$. Otherwise a has an odd prime divisor, say p_k. We choose a prime number p such that $p \equiv 1 \pmod 8$, $p \equiv 1 \pmod{p_i}$ for $i = 1, 2, \ldots, k-1$, and $p \equiv a \pmod{p_k}$, where a is an arbitrary quadratic nonresidue modulo p_k. Such prime number p exists according to the Dirichlet theorem on primes in an arithmetic progression. Then it follows from (1) that $p_1, \ldots, p_{k-1}$ are quadratic residues modulo p, but p_k is not. Therefore a is a quadraic nonresidue modulo p.

The proof in the case $a < 0$ is similar and is left to the reader. △

2 Quadratic Congruences to Composite Moduli

Not all moduli are prime, so we do not want to be restricted to prime moduli. The above theory can be generalized to composite moduli, yet losing as little as possible. The following function generalizes Legendre's symbol to a certain extent.

Definition 3. *Let a be an integer and b an odd number, and let $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the factorization of b onto primes. Jakobi'a symbol $\left(\frac{a}{b}\right)$ is defined as*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Since there is no danger of confusion, Jacobi's and Legendre's symbol share the notation.

It is easy to see that $\left(\frac{a}{b}\right) = -1$ implies that a is a quadratic nonresidue modulo b. Indeed, if $\left(\frac{a}{b}\right) = -1$, then by the definition $\left(\frac{a}{p_i}\right) = -1$ for at least one $p_i \mid b$; hence a is a quadratic nonresidue modulo p_i.

However, the converse is *false*, as seen from the following example.

Example 4. *Although*

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1,$$

2 is not a quadratic residue modulo 15, as it is not so modulo 3 and 5.

In fact, the following weaker statement holds.

Theorem 12. *Let a be an integer and b a positive integer, and let $b = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ be the faktorization of b onto primes. Then a is a quadratic residue modulo b if and only if a is a quadratic residue modulo $p_i^{\alpha_i}$ for each $i = 1, 2, \ldots, r$.*

Proof. If a quadratic residue modulo b, it is clearly so modulo each $p_i^{\alpha_i}$, $i = 1, 2, \ldots, r$.

Assume that a is a quadratic residue modulo each $p_i^{\alpha_i}$ and that x_i is an integer such that $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. According to Chinese Remainder Theorem there is an x such that $x \equiv x_i \pmod{p_i^{\alpha_i}}$ for $i = 1, 2, \ldots, r$. Then $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$ for each i, and therefore $x^2 \equiv a \pmod{b}$. □

Theorem 13. *The number of quadratic residues modulo p^n ($n > 0$) is equal to*

$$\left[\frac{2^{n-1}-1}{3}\right] + 2 \text{ for } p = 2, \quad \text{and} \quad \left[\frac{p^{n+1}-1}{2(p+1)}\right] + 1 \text{ for } p > 2.$$

Proof. Let k_n denote the number of quadratic residues modulo p^n.

Let p be odd and $n \geq 2$. Number a is a quadratic residue modulo p^n if and only if either $p \nmid a$ and a is a quadratic residue modulo p, or $p^2 \mid a$ and a/p^2 is a quadratic residue modulo p^{n-2}. It follows that $k_n = k_{n-2} + p'p^{n-1}$.

Let $p = 2$ and $n \geq 3$. Number a is a quadratic residue modulo 2^n if and only if either $a \equiv 1 \pmod 8$ or $4 \mid a$ and $a/4$ is a quadratic residue modulo 2^{n-2}. We obtain $k_n = k_{n-2} + 2^{n-3}$.

Now the statement is shown by simple induction on n. □

Many properties of Legendre's symbols apply for Jacobi's symbols also. Thus the following statements hold can be easily proved by using the definition of Jacobi's symbol and the analogous statements for Legendre's symbols.

Theorem 14. *For all integers a, b and odd numbers c, d the following equalities hold:*

$$\left(\frac{a+bc}{c}\right) = \left(\frac{a}{c}\right), \quad \left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right), \quad \left(\frac{a}{cd}\right) = \left(\frac{a}{c}\right)\left(\frac{a}{d}\right). \ \square$$

Theorem 15. *For every odd integer a,*

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \quad \left(\frac{2}{a}\right) = (-1)^{\left[\frac{a+1}{4}\right]}. \ \square$$

Theorem 16 (The Reciprocity Rule). *For any two coprime odd numbers a, b it holds that*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}. \ \square$$

Problem 7. *Prove that the equation $x^2 = y^3 - 5$ has no integer solutions (x, y).*

Solution. For even y we have $x^2 = y^3 - 5 \equiv 3 \pmod 8$, which is impossible.

Now let y be odd. If $y \equiv 3 \pmod 4$, then $x^2 = y^3 - 5 \equiv 3^3 - 5 \equiv 2 \pmod 4$, impossible again. Hence y must be of the form $4z + 1$, $z \in \mathbb{Z}$. Now the given equation transforms into

$$x^2 + 4 = 64z^3 + 48z^2 + 12z = 4z(16z^2 + 12z + 3).$$

It follows that $x^2 \equiv 4 \pmod{16z^2 + 12z + 3}$.

However, the value of Jacobi's symbol

$$\left(\frac{-4}{16z^2+12z+3}\right)=\left(\frac{-1}{16z^2+12z+3}\right)$$

equals -1 because $16z^2+12z+3\equiv 3 \pmod 4$. Contradiction. $\triangle$

Problem 8. *Prove that $4kxy-1$ does not divide the number x^m+y^n for any positive integers x, y, k, m, n.*

Solution. Note that $(x^m, y^n, 4kxy-1)=1$. Let us write $m'=[m/2]$ and $n'=[n/2]$. We need to investigate the following cases.

1° $m=2m'$ and $n=2n'$. Then $4kxy-1 \mid (x^{m'})^2+(y^{n'})^2$ by Theorem 6 implies $\left(\frac{-1}{4kxy-1}\right)=1$, which is false.

2° $m=2m'$ and $n=2n'+1$ (the case $m=2m'+1$, $n=2n'$ is analogous). Then $4kxy-1 \mid (x^{m'})^2+y(y^{n'})^2$ and hence $\left(\frac{-y}{4kxy-1}\right)=1$. We claim this to be impossible.

Suppose that y is odd. The Reciprocity Rule gives us

$$\left(\frac{-y}{4kxy-1}\right)=\left(\frac{-1}{4kxy-1}\right)\left(\frac{y}{4kxy-1}\right)=(-1)\cdot(-1)^{\frac{y-1}{2}}\left(\frac{-1}{y}\right)=-1.$$

Now assume that $y=2^t y_1$, where $t\geq 1$ is an integer and $y_1\in\mathbb{N}$. According to Theorem 15, we have $\left(\frac{2}{4kxy-1}\right)=1$, whereas, like in the case of odd y, $\left(\frac{-y_1}{4kxy-1}\right)=\left(\frac{-y_1}{4\cdot 2^t kxy_1-1}\right)=-1$. It follows that

$$\left(\frac{-y}{4kxy-1}\right)=\left(\frac{2}{4kxy-1}\right)^t\left(\frac{-y_1}{4kxy-1}\right)=-1.$$

3° $m=2m'+1$ and $n=2n'+1$. Then $4kxy-1 \mid x(x^{m'})^2+y(y^{n'})^2$, and hence $\left(\frac{-xy}{4kxy-1}\right)=1$. On the other hand,

$$\left(\frac{-xy}{4kxy-1}\right)=\left(\frac{-4xy}{4kxy-1}\right)=\left(\frac{-1}{4kxy-1}\right)=-1,$$

a contradiction.

This finishes the proof. $\triangle$

3 Some Sums of Legendre's symbols

Finding the number of solutions of a certain conguence is often reduced to counting the values of $x\in\{0,1,\ldots,p-1\}$ for which a given polynomial $f(x)$ with integer coefficients is a quadratic residue modulo an odd prime p. The answer is obviously directly connected to the value of the sum

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

In this part we are interested in sums of this type.

For a linear polynomial f, the considered sum is easily evaluated:

Theorem 17. *For arbitrary integers a, b and a prime $p\nmid a$,*

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

Proof. Since $p \nmid a$, the numbers $ax + b$, $x = 0, 1, \ldots, p-1$ form a complete system of residues modulo p. Exactly $\frac{p-1}{2}$ of them are quadratic residues, exactly $\frac{p-1}{2}$ are quadratic nonresidues, and one is divisible by p. It follows that

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p} \right) = \frac{p-1}{2} \cdot 1 + \frac{p-1}{2} \cdot (-1) + 0 = 0. \ \square$$

To evaluate the desired sum for quadratic polynomials f, we shall use the following proposition.

Theorem 18. *Let $f(x)^{p'} = a_0 + a_1 x + \cdots + a_{kp'} x^{kp'}$, where k is the degree of polynomial f. We have*

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \equiv -(a_{p-1} + a_{2(p-1)} + \cdots + a_{k'(p-1)}) \ (\text{mod } p), \quad \text{where } k' = \left[\frac{k}{2} \right].$$

Proof. Define $S_n = \sum_{x=0}^{p-1} x^n$ ($n \in \mathbb{N}$) and $S_0 = p$. It can be shown that $S_n \equiv -1 \pmod p$ for $n > 0$ and $p - 1 \mid n$, and $S_n \equiv 0 \pmod p$ otherwise. Now Euler's Criterion gives us

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \equiv \sum_{x=0}^{p-1} f(x)^{p'} = \sum_{i=0}^{kp'} a_i S_i \equiv -(a_{p-1} + a_{2(p-1)} + \cdots + a_{k'p-1}) \pmod p. \ \square$$

Theorem 19. *For any integers a, b, c and a prime $p \nmid a$, the sum*

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right)$$

equals $-\left(\frac{a}{p}\right)$ if $p \nmid b^2 - 4ac$, and $(p-1)\left(\frac{a}{p}\right)$ if $p \mid b^2 - 4ac$.

Proof. We have

$$\left(\frac{4a}{p} \right) \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2 - D}{p} \right),$$

where $D = b^2 - 4ac$. Since numbers $ax + b$, $x = 0, 1, \ldots, p-1$ comprise a complete system of residues modulo p, we obtain

$$\left(\frac{a}{p} \right) \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = \sum_{x=0}^{p-1} \left(\frac{x^2 - D}{p} \right) = S.$$

Theorem 18 gives us $S \equiv -1 \pmod p$, which together with $|S| \leq p$ yields $S = -1$ or $S = p - 1$.

Suppose that $S = p - 1$. Then $p - 1$ of the numbers $\left(\frac{x^2 - D}{p}\right)$ are equal to 1, and exactly one, say for $x = x_0$, is equal to 0, i.e. $p \mid x_0^2 - D$. Since this implies $p \mid (-x_0)^2 - D = x_0^2 - p$ also, we must have $x_0 = 0$ and consequently $p \mid D$. Conversely, if $p \mid D$, we have $S = p - 1$; otherwise $S = -1$, which finishes the proof. $\square$

Problem 9. *The number of solutions (x, y) of congruence*

$$x^2 - y^2 = D \ \ (\text{mod } p),$$

where $D \not\equiv 0$ (mod p) is given, equals $p - 1$.

Solution. This is an immediate consequence of the fact that, for fixed x, the number of solutions y of the congruence $y^2 \equiv x^2 - D \pmod p$ equals $\left(\frac{x^2-D}{p}\right) + 1$. $\triangle$

Evaluating the sums of Legendre's symbols for polynomials $f(x)$ of degree greater than 2 is significantly more difficult. In what follows we investigate the case of cubic polynomials f of a certain type.

For an integer a, define

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

Assume that $p \nmid a$. We easily deduce that for each $t \in \mathbb{Z}$,

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

Therefore $|K(a)|$ depends only on whether a is a quadratic residue modulo p or not.

Now we give one non-standard proof of the fact that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

Theorem 20 (Jacobstal's identity). *Let a and b be a quadratic residue and nonresidue modulo a prime number p of the form $4k+1$. Then $|K(a)|$ and $|K(b)|$ are even positive integers that satisfy*

$$\left(\frac{1}{2}|K(a)|\right)^2 + \left(\frac{1}{2}|K(b)|\right)^2 = p.$$

Proof. The previous consideration gives us $p'(K(a)^2 + K(b)^2) = \sum_{n=1}^{p-1} K(n)^2 = \sum_{n=0}^{p-1} K(n)^2$, since $K(0) = 0$. Let us determine $\sum_{n=0}^{p-1} K(n)^2$. For each n we have

$$K(n)^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{xy(x^2+n)(y^2+n)}{p}\right),$$

which implies

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

Note that by the theorem 19, $\sum_{n=0}^{p-1} \left(\frac{(n+x^2)(n+y^2)}{p}\right)$ equals $p-1$ if $x = \pm y$, and -1 otherwise. Upon substituting these values the above equality becomes

$$\sum_{n=0}^{p-1} K(n)^2 = p(2p-2) - \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{xy}{p}\right) = 4pp'.$$

We conclude that $K(a)^2 + K(b)^2 = 4p$. Furthermore, since $K(a)^2 + K(b)^2$ is divisible by 4, both $K(a)$ and $K(b)$ must be even, and the statement follows. $\square$

4 Problems

10. Let p be a prime number. Prove that there exists $x \in \mathbb{Z}$ for which $p \mid x^2 - x + 3$ if and only if there exists $y \in \mathbb{Z}$ for which $p \mid y^2 - y + 25$.

11. Let $p = 4k-1$ be a prime number, $k \in \mathbb{N}$. Show that if a is an integer such that the congruence $x^2 \equiv a \pmod p$ has a solution, then its solutions are given by $x = \pm a^k$.

12. Show that all odd divisors of number $5x^2 + 1$ have an even tens digit.

13. Show that for every prime number p there exist integers a, b such that $a^2 + b^2 + 1$ is a multiple of p.

14. Prove that $\frac{x^2+1}{y^2-5}$ is not an integer for any integers $x, y > 2$.

15. Let $p > 3$ be a prime and let $a, b \in \mathbb{N}$ be such that

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}.$$

Prove that $p^2 \mid a$.

16. Consider $P(x) = x^3 + 14x^2 - 2x + 1$. Show that there exists a natural number n such that for each $x \in \mathbb{Z}$,

$$101 \mid \underbrace{P(P(\ldots P}_{n}(x)\ldots)) - x.$$

17. Determine all $n \in \mathbb{N}$ such that the set $A = \{n, n+1, \ldots, n+1997\}$ can be partitioned into at least two subsets with equal products of elements.

18. (a) Prove that for no $x, y \in \mathbb{N}$ is $4xy - x - y$ a square;
    (b) Prove that for no $x, y, z \in \mathbb{N}$ is $4xyz - x - y$ a square.

19. If $n \in \mathbb{N}$, show that all prime divisors of $n^8 - n^4 + 1$ are of the form $24k + 1$, $k \in \mathbb{N}$.

20. Suppose that m, n are positive integers such that $\varphi(5^m - 1) = 5^n - 1$. Prove that $(m, n) > 1$.

21. Prove that there are no positive integers a, b, c for which

$$\frac{a^2 + b^2 + c^2}{3(ab + bc + ca)}$$

is an integer.

22. Prove that, for all $a \in \mathbb{Z}$, the number of solutions (x, y, z) of the congruence

$$x^2 + y^2 + z^2 \equiv 2axyz \pmod{p}$$

equals $\left(p + (-1)^{p'}\right)^2$.

5 Solutions

10. The statement is trivial for $p \leq 3$, so we can assume that $p \geq 5$.

Since $p \mid x^2 - x + 3$ is equivalent to $p \mid 4(x^2 - x + 3) = (2x-1)^2 + 11$, integer x exists if and only if -11 is a quadratic residue modulo p. Likewise, since $4(y^2 - y + 25) = (2y-1)^2 + 99$, y exists if and only if -99 is a quadratic residue modulo p. Now the statement of the problem follows from

$$\left(\frac{-11}{p}\right) = \left(\frac{-11 \cdot 3^2}{p}\right) = \left(\frac{-99}{p}\right).$$

11. According to Euler's criterion, the existence of a solution of $x^2 \equiv a \pmod{p}$ implies $a^{2k-1} \equiv 1 \pmod{p}$. Hence for $x = a^k$ we have $x^2 \equiv a^{2k} \equiv a \pmod{p}$.

12. If $p \mid 5x^2+1$, then $\left(\frac{-5}{p}\right) = 1$. The Reciprocity rule gives us

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$

It is easy to verify that the last expression has the value 1 if and only if p is congruent to $1, 3, 7$ or 9 modulo 20.

13. Clearly, $p \mid a^2+b^2+1$ if and only if $a^2 \equiv -b^2-1 \pmod p$.

Both sets $\{a^2 \mid a \in \mathbb{Z}\}$ and $\{-b^2-1 \mid b \in \mathbb{Z}\}$ modulo p are of cardinality exactly $\frac{p+1}{2}$, so they have an element in common, i.e. there are $a, b \in \mathbb{Z}$ with a^2 and $-b^2-1$ being equal modulo p.

14. If y is even, y^2-5 is of the form $4k+3$, $k \in \mathbb{Z}$ and thus cannot divide x^2+1 for $x \in \mathbb{Z}$. If y is odd, then y^2-5 is divisible by 4, while x^2+1 is never a multiple of 4.

15. It suffices to show that $\frac{2(p-1)!a}{b} = \sum_{i=1}^{p-1} \frac{2(p-1)!}{i}$ is divisible by p^2. To start with,

$$\frac{2(p-1)!a}{b} = \sum_{i=1}^{p-1}\left(\frac{(p-1)!}{i} + \frac{(p-1)!}{p-i}\right) = \sum_{i=1}^{p-1}\frac{p(p-1)!}{i(p-i)}.$$

Therefore, $p \mid a$. Moreover, if for $i \in \{1, 2, \ldots, p-1\}$ i' denotes the inverse of i modulo p, we have

$$\frac{2(p-1)!a}{pb} = \sum_{i=1}^{p-1}\frac{(p-1)!}{i(p-i)} \equiv \sum_{i=1}^{p-1} i'^2(p-1)! \equiv 0 \pmod p.$$

It follows that $p^2 \mid 2(p-1)!a$.

16. All congruences in the solution will be modulo 101.

It is clear that $P(x) \equiv P(y)$ for integers x, y with $x \equiv y$.

We claim that the converse holds: $P(x) \not\equiv P(y)$ if $x \not\equiv y$. We have

$$\frac{4[P(x)-P(y)]}{x-y} = 4(x^2+xy+y^2+14x+14y-2) \equiv (2x+y+14)^2 + 3(y-29)^2.$$

Since -3 is not a quadratic residue modulo 101, the left hand side is not divisible by 101 unless if $2x+y+14 \equiv y-29 \equiv 0$, i.e. $x \equiv y \equiv 29$. This justifies our claim.

We now return to the problem. The above statement implies that $P(0), P(1), \ldots, P(100)$ is a permutation of $0, 1, \ldots, 100$ modulo 101. We conclude that for each $x \in \{0, 1, \ldots, 100\}$ there is an n_x such that $P(P(\ldots P(x)\ldots)) \equiv x$ (with P applied n_x times).

Any common multiple of the numbers $n_0, n_1, \ldots, n_{100}$ is clearly a desired n.

17. Suppose that A can be partitioned into k subsets $A_1, \ldots, A_k$, each with the same product of elements m. Since at least one and at most two elements of A are divisible by the prime 1997, we have $1997 \mid m$ and hence $k = 2$. Furthermore, since the number of elements divisible by the prime 1999 is at most one, we have $1999 \nmid m$; hence no elements of A is divisible by 1999, i.e. the elements of A are congruent to $1, 2, 3, \ldots, 1998$ modulo 1999. Then $m^2 \equiv 1 \cdot 2 \cdot 3 \cdots 1998 \equiv -1 \pmod{1999}$, which is impossible because -1 is a quadratic nonresidue modulo $1999 = 4 \cdot 499 + 3$.

18. Part (a) is a special case of (b).

(b) Suppose $x, y, z, t \in \mathbb{N}$ are such that $4xyz - x - y = t^2$. Multiplying this equation by $4z$ we obtain

$$(4xz-1)(4yz-1) = 4zt^2 + 1.$$

Therefore, $-4z$ is a quadratic residue modulo $4xz-1$. However, it was proved in problem 8 that the value of Legendre's symbol $\left(\frac{-z}{4xz-1}\right)$ is -1 for all x, z, yielding a contradiction.

19. Consider an arbitrary prime divisor p of $n^8 - n^4 + 1$. It follows from problem 4 that p is congruent to 1 or 13 (mod 24). Furthermore, since

$$n^8 - n^4 + 1 = (n^4 + n^2 + 1) - 2(n^3 + n)^2,$$

2 is a quadratic residue modulo p, excluding the possibility $p \equiv \pm 13 \pmod{24}$.

20. Suppose that $(m, n) = 1$. Let

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

be the factorization of $5^m - 1$ onto primes, where $p_i > 2$ za $i = 1, \ldots, k$. By the condition of the problem,

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

Obviously, $2^\alpha \mid 5^n - 1$. On the other hand, it follows from $(5^m - 1, 5^n - 1) = 5^1 - 1 = 4$ that $\alpha_i = 1$ for each $i = 1, \ldots, k$ and $\alpha = 2$. Since $2^3 \mid 5^x - 1$ for every even x, m must be odd: $m = 2m' + 1$ for some $m' \in \mathbb{N}_0$.

Since $p_i \mid 5 \cdot (5^{m'})^2 - 1$ for $i = 1, \ldots, k$, 5 is a quadratic residue modulo p_i, and consequently $p_i \equiv \pm 1 \pmod 5$. However, (2) implies that none of $p_i - 1$ is divisible by 5. We thus obtain that $p_i \equiv -1 \pmod 5$ for all i.

Reduction of equality (1) modulo 5 yields $(-1)^k = 1$. Thus k is even. On the other hand, equality (2) modulo 5 yields $(-2)^{k+1} \equiv 1 \pmod 5$, and therefore $k \equiv 3 \pmod 4$, contradicting the previous conclusion.

Remark. Most probably, m and n do not even exist.

21. Suppose that a, b, c, n are positive integers such that $a^2 + b^2 + c^2 = 3n(ab + bc + ca)$. This equality can be rewritten as

$$(a + b + c)^2 = (3n + 2)(ab + bc + ca).$$

Choose a prime number $p \equiv 2 \pmod 3$ which divides $3n + 2$ with an odd exponent, i.e. such that $p^{2i-1} \mid 3n + 2$ and $p^{2i} \nmid 3n + 2$ for some $i \in \mathbb{N}$ (such p must exist). Then $p^i \mid a + b + c$ and therefore $p \mid ab + bc + ca$. Substituting $c \equiv -a - b \pmod p$ in the previous relation we obtain

$$p \mid a^2 + ab + b^2 \quad \Rightarrow \quad p \mid (2a + b)^2 + 3b^2.$$

It follows that $\left(\frac{-3}{p}\right) = 1$, which is false because $p \equiv 2 \pmod 3$.

22. The given congruence is equivalent to

$$(z - axy)^2 \equiv (a^2x^2 - 1)y^2 - x^2 \pmod p. \tag{1}$$

For any fixed $x, y \in \{0, \ldots, p-1\}$, the number of solutions z of (1) equals

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

Therefore the total number of solutions of (1) equals

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

According to theorem 19, $\sum_{y=0}^{p-1}\left(\frac{(a^2x^2-1)y^2-x^2}{p}\right)$ is equal to $-\left(\frac{a^2x^2-1}{p}\right)$ if $ax \not\equiv \pm 1 \pmod p$, and to $p\left(\frac{-1}{p}\right)$ if $ax \equiv \pm 1 \pmod p$. Therefore

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