Quadratic Congruences in Olympiad Problems
Paul Stoienescu and Tudor-Dimitrie Popescu

In this note, we will present some Olympiad problems which can be solved using quadratic congruence arguments.

1 Definitions and Properties

1.1 The Legendre Symbol

Given a prime number \( p \) and an integer \( a \), Legendre’s symbol \( \left( \frac{a}{b} \right) \) is defined as:

\[
\left( \frac{a}{b} \right) = \begin{cases} 
0 & \text{if } a \text{ is divisible by } p; \\
1 & \text{if } a \text{ is a quadratic residue modulo } p; \\
-1 & \text{otherwise}; 
\end{cases}
\]  

(1)

Property 1: If \( a \equiv b \pmod{p} \) and \( ab \) is not divisible by \( p \), then \( \left( \frac{a}{b} \right) = \left( \frac{b}{a} \right) \).

Property 2: 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 numbers \( p > 2 \).

Property 3: If \( p \neq 2 \), then \( \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} \).

Property 4: If \( p \neq 2 \), then \( \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} \).

Property 5 (Euler’s Criterion): If \( p \nmid a, p \neq 2 \), then \( a^{\frac{p-1}{2}} = \left( \frac{a}{p} \right) \).

Property 6 (Quadratic Reciprocity Law or Gauss’s Law): If \( p, q \) are distinct odd prime numbers, then

\[
\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.
\]

Gauss’s law, combined with the properties of the Legendre symbol, proves that any Legendre symbol can be calculated. This makes it possible to determine whether the quadratic equation \( x^2 \equiv a \pmod{p} \), where \( p \) is an odd prime, has a solution. Moreover, the solution can be found using quadratic residues.

Lemma. Let \( p \) be an odd prime. There are \( \frac{p-1}{2} \) quadratic residues in the set \( \{1, 2, 3, \ldots, p-1\} \).
A quick application: Find \( \left( \frac{30}{211} \right) \).

Solution. We have

\[
\left( \frac{30}{211} \right) = \left( \frac{2}{211} \right) \left( \frac{3}{211} \right) \left( \frac{5}{211} \right).
\]

Since \( 211 \equiv 3 \pmod{8} \), we get \( \left( \frac{2}{211} \right) = -1 \).

For \( \left( \frac{3}{211} \right) \), we apply quadratic reciprocity law to obtain

\[
\left( \frac{3}{211} \right) = \left( \frac{211}{3} \right) (-1)^{105} = \left( \frac{71}{3} \right) = -1.
\]

Finally, we have \( \left( \frac{5}{211} \right) = \left( \frac{211}{5} \right) (-1)^{105-2} = \left( \frac{41}{5} \right) = 1 \).

Combining all of the above, we obtain \( \left( \frac{30}{211} \right) = (-1)(-1)(+1) = 1 \). \( \square \)

1.2 Quadratic Congruences with Composite Moduli

Let \( a \) be an integer and \( b \) an odd number, and let \( b = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n} \) be the factorization of \( b \) into primes. Jacobi's Symbol \( \left( \frac{a}{b} \right) \) is defined as:

\[
\left( \frac{a}{b} \right) = \left( \frac{a}{p_1} \right)^{\alpha_1}\left( \frac{a}{p_2} \right)^{\alpha_2}\ldots\left( \frac{a}{p_n} \right)^{\alpha_n}
\]  \hspace{1cm} (2)

Jacobi's Symbol has almost the same properties as Legendre's with a few changes: it does not have Property 5, while in Properties 3 and 4, \( p \) can be an odd integer and in Property 6, \( p,q \) can be distinct odd integers with no common divisors.

It is easy to see that \( \left( \frac{a}{b} \right) = -1 \) implies that \( a \) is a quadratic nonresidue \( \pmod{p} \).

Indeed, if \( \left( \frac{a}{b} \right) = -1 \), then by definition \( \left( \frac{a}{p_i} \right) = -1 \) for at least one \( p_i | b \); hence \( a \) is a quadratic nonresidue modulo \( p_i \). The converse is false as we can see in the following example:

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

but 2 is not a quadratic residue modulo 15. As such we have the following.

Theorem. Let \( a \) be an integer and \( b \) be a positive integer, and let \( b = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n} \) be the factorization of \( b \) into 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 \( i = 1, 2, \ldots, n \).
2 Warm-Up Problems

**Problem 1.** Let $a$ and $b$ be positive integers such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares? (IMO 1996.)

**Solution.** Let $15a + 16b = k^2$ and $16a - 15b = l^2$. Then

$$a = \frac{15k^2 + 16l^2}{481}, \quad b = \frac{16k^2 - 15l^2}{481}, \quad k, l \in \mathbb{N}^*.$$ 

Since $481 = 13 \cdot 37$, we have

$$15k^2 + 16l^2 \equiv 0 \pmod{13}, \quad 2k^2 \equiv -3l^2 \pmod{13}, \quad k^2 \equiv 5l^2 \pmod{13}.$$ 

We then obtain $\left(\frac{5}{13}\right) = -1$, which implies that $13|l$ and $13|k$. Note that

$$15k^2 + 16l^2 \equiv 0 \pmod{37}, \quad 32l^2 \equiv -30k^2 \pmod{37}, \quad -5l^2 \equiv -30k^2 \pmod{37}, \quad l^2 \equiv 6k^2 \pmod{37}.$$ 

Combined with the fact that $\left(\frac{6}{37}\right) = -1$, we get that $37|k$ and $37|l$. The least possible value for $l$ is $13 \cdot 37 = 481$. We can take $k = l = 481$ and thus we will get $a = 31 \cdot 481, b = 481$.

**Problem 2.** Prove that $2^n + 1$ has no prime factors of the form $8k + 7$. (Vietnam Team Selection Test 2004.)

**Solution.** Assume that there exists a prime $p$ such that $p|2^n + 1$ and $p \equiv 7 \pmod{8}$.

If $n$ is even, $\left(\frac{-1}{p}\right) = 1$. But

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

since $p \equiv 3 \pmod{4}$, so we have reached a contradiction.

If $n$ is odd, we get that $2^{n+1} \equiv -2 \pmod{p}$, so $-2$ is a quadratic residue modulo $p$, since $n + 1$ is even, so $\left(\frac{-2}{p}\right) = 1$. But

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

which yields a contradiction. 

Copyright © Canadian Mathematical Society, 2017
Problem 3. Let $p$ be a prime number such that $p \equiv 1 \pmod{4}$. Calculate

$$ S = \sum_{k=1}^{\frac{p-1}{2}} \left( \left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \cdot \left\lfloor \frac{k^2}{p} \right\rfloor \right). $$

Solution. Let $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ be the quadratic residues (mod $p$). First, observe that the sum is equivalent to

$$ S = \sum_{i=1}^{\frac{p-1}{2}} 2 \left( \left\lfloor \frac{r_i}{p} \right\rfloor - \left\lfloor \frac{2r_i}{p} \right\rfloor \right). $$

Each term $2\left\{ \frac{r_i}{p} \right\} - \left\{ \frac{2r_i}{p} \right\}$ is $0$ if $r_i \leq \frac{p-1}{2}$, and $1$ if $r_i > \frac{p-1}{2}$. So $S$ is the number of quadratic residues which are greater than $\frac{p-1}{2}$. Since $p \equiv 1 \pmod{4}$, if $r_i$ is a quadratic residue, then so is $p - r_i$, so half of the integers greater than $\frac{p-1}{2}$ are quadratic residues $\Rightarrow S = \frac{p-1}{4}$. □

Problem 4. Let $m, n \geq 3$ be positive odd integers. Prove that $2^m - 1$ doesn’t divide $3^n - 1$.

Solution. Here we will use Jacobi’s Symbol. Suppose that $2^m - 1$ divides $3^n - 1$. Let $x = 3^{\frac{n-1}{2}}$. We have that $3x^2 \equiv 1 \pmod{2^m - 1}$, so $(3x)^2 \equiv 3 \pmod{2^m - 1}$ and hence $\left( \frac{3}{2^m - 1} \right) = 1$. Using quadratic reciprocity, we get that

$$ 1 = \left( \frac{3}{2^m - 1} \right) = \left( \frac{2^m - 1}{3} \right) (-1)^{\frac{2^m - 2}{2}} \Rightarrow \left( \frac{2^m - 1}{3} \right) = -1, $$

contradiction due to the fact that $2^m - 1 \equiv 1 \pmod{3}$. □

3 Harder Problems

Problem 5. For a positive integer $a$, define a sequence of integers $x_1, x_2, \ldots$ by letting $x_1 = a$ and $x_{n+1} = 2x_n + 1$ for $n \geq 1$. Let $y_n = 2^x_n - 1$. Determine the largest possible $k$ such that, for some positive integer $a$, the numbers $y_1, \ldots, y_k$ are all prime. (2013 Romanian Masters of Mathematics.)

Solution. We will prove that the answer is $2$. Suppose that there exists $a$ such that $k \geq 3$. The numbers $2^a - 1, 2^{2a+1} - 1, 2^{4a+3} - 1$ are primes, so the numbers $a, 2a+1, 4a+3$ are primes (this is because of the fact that if $2^M - 1$ is prime, then $M$ is also a prime; otherwise, if there existed a natural number $d$ such that $d|M$, then $2^d - 1$ would divide $2^M - 1$). Let’s use Euler’s Criterion:

$$ 2^{4a+3-1} \equiv \left( \frac{2}{4a+3} \right) \pmod{4a+3} \Rightarrow 2^{2a+1} \equiv \left( \frac{2}{4a+3} \right) \pmod{4a+3}. $$

Crux Mathematicorum, Vol. 43(8), October 2017
Since $2^{2a+1} - 1$ is prime, then $2^{2a+1} \not\equiv 1 \pmod{4a+3}$, otherwise $2^{2a+1} = 4a + 4$ and that will lead to $a = 1$, false. Hence we have
\[
\left(\frac{2}{4a+3}\right) = -1 \Rightarrow -1 = (-1)^{(4a+2)(4a+4) \over 8} = (-1)^{(2a+1)(a+1)},
\]
which implies that $a + 1$ is odd. But $a$ is prime so $a = 2$. If $a = 2$, we have that $2^{11} - 1 = 23 \cdot 87$ is not prime, contradiction. So we get that the answer is 2 and it is achieved for $a = 2$.

**Problem 6.** Prove that there are infinitely many positive integers $n$ such that $n^2 + 1$ has a prime divisor greater than $2n + \sqrt{2n}$. (IMO 2008.)

**Solution.** Let $p$ be a prime, $p = 8k + 1$. Note that $4^{-1} \equiv 6k + 1 \pmod{p}$. Choose $n = 4k - a$, $0 \leq a < 4k$. Then
\[
\left(\frac{p - 1}{2} - a\right)^2 + 1 \equiv 0 \pmod{p} \iff 4^{-1} + a + a^2 + 1 \equiv 0 \pmod{p},
\]
so
\[a(a + 1) \equiv -6k - 2 \equiv 2k - 1 \pmod{p}.
\]
But $a(a + 1)$ is even and positive, so $a(a + 1) \geq 10k$. We have that
\[(a + 1)^2 > a(a + 1) \geq 10k > p,
\]
so
\[n = \frac{p + 1}{2} - (a + 1) < \frac{p + 1}{2} - \sqrt{p} < \frac{p + 1}{2} - \sqrt{2n},
\]
so $2n + 2\sqrt{2n} - 1 > p$. Note that this result is a bit stronger than the initial inequality.

**Problem 7.** Suppose that the positive integer $a$ is not a perfect square. Then \(\left(\frac{a}{b}\right) = -1\) for infinitely many primes $p$.

**Solution.** Let us assume that the claim is false. This means that there exists a number $r$ such that for every prime $q > r$, \(\left(\frac{a}{q}\right) = 1\). Because $a$ is not a perfect square, we can write\( a = x^2p_1p_2\ldots p_k\), where $p_1, p_2, \ldots, p_k$ are primes in increasing order. Take a prime $p > r$, $p \equiv 5 \pmod{8}$. We have that
\[
\left(\frac{a}{b}\right) = \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\ldots\left(\frac{p_k}{p}\right).
\]
If $p_i$ is odd, then \(\left(\frac{p_i}{p}\right) = \left(\frac{1}{p}\right)\), by the Quadratic Reciprocity Law.

If $p_1 = 2$, \(\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1\). So
\[
\left(\frac{a}{b}\right) = \left(\frac{p}{p_1}\right)\ldots\left(\frac{p}{p_k}\right) \quad \text{or} \quad \left(\frac{a}{b}\right) = -\left(\frac{p}{p_2}\right)\ldots\left(\frac{p}{p_k}\right).
\]

Copyright © Canadian Mathematical Society, 2017
We can take \( r_2, r_2, \ldots, r_k \) residues \((\text{mod} \ p_2, p_3, \ldots, p_k)\) such that \( \left( \frac{r_2}{p_2} \right) \cdots \left( \frac{r_k}{p_k} \right) \) is 1 or \(-1\) as we wish. By the Chinese Remainder Theorem, there are infinitely many numbers \( t \) with

\[
 t \equiv 5 \pmod{8}, \ t \equiv r_i \pmod{p_i}, \ 2 \leq i \leq k.
\]

Now we look at the progression \( t + 8p_2p_3 \cdots p_k \). By Dirichlet’s Theorem, there are infinitely many primes \( q \) in this sequence and we take \( q > r \). Note that we have \( \left( \frac{a}{q} \right) = 1 \), but as already discussed, we can select \( r_2, r_3, \ldots, r_k \) such that \( \left( \frac{a}{q} \right) = -1 \), a contradiction.

**Problem 8.** Let \( S \) be the set of all rational numbers expressible in the form

\[
\frac{a_1^2 + a_1 - 1)(a_2^2 + a_2 - 1) \cdots (a_n^2 + a_n - 1)}{(b_1^2 + b_1 - 1)(b_2^2 + b_2 - 1) \cdots (b_n^2 + b_n - 1)}
\]

for some positive integers \( n, a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \). Prove that there is an infinite number of primes in \( S \). (2013 Romanian IMO Team Selection Test.)

**Solution.** Clearly, \( S \) is closed under multiplication and division: if \( r \) and \( s \) are in \( S \), so are \( rs \) and \( \frac{r}{s} \). Any prime number which is \( 0, 1 \) or \( 4 \) \((\text{mod} \ 5)\) is in \( S \). Since \( 2^2 + 2 - 1 = 5 \), we know that \( 5 \) is in \( S \). Now we will prove by induction that every prime number which is \( 1 \) or \( 4 \) \((\text{mod} \ 5)\) is in \( S \). Of course, \( 11 = 3^2 + 3 - 1 \) and \( 19 = 4^2 + 4 - 1 \) are in \( S \). Denote \( p_1, p_2, \ldots \) the sequence of primes of this form in increasing order, and suppose that \( p_1, p_2, \ldots, p_{n-1} \) are in \( S \). We will show that \( p_n \) is also in \( S \). Because \( 5 \) is a quadratic residue \((\text{mod} \ p_n)\), there exists a number \( x \) such that

\[
p_n | (2x + 1)^2 - 5 \Rightarrow p_n | x^2 + x - 1
\]

and we can choose \( x \) such that \( 2x + 1 < p_n \). Hence, \( p_n^2 \) does not divide \( x^2 + x - 1 \). Note that any prime which divides \( x^2 + x - 1 \) is \( 0, 1, 4 \) \((\text{mod} \ 5)\) (if \( q \) is a prime such that \( q | x^2 + x - 1 \), then \( q | (2x + 1)^2 - 5 \), so \( 5 \) is a quadratic residue \((\text{mod} \ q)\), so using Gauss’s law we get that \( q \) is \( 0, 1, 4 \) \((\text{mod} \ 5)\)).

Also, if \( q | x^2 + x - 1 \), then \( q < p_n \), so \( x^2 + x - 1 \) is a product of primes which are among \( p_1, p_2, \ldots, p_n \). Let \( x^2 + x - 1 = tp_n \), where \( t \) is in \( S \) and so \( p_n \) is in \( S \) (since \( p_n = \frac{x^2 + x - 1}{t} \) and \( \frac{x^2 + x - 1}{t+1} = x^2 + x - 1 \) is in \( S \)). The induction step is complete. □

## 4 Exercises

**Exercise 1.** Let \( p \geq 3 \) be a prime number. Prove that the least quadratic nonresidue \((\text{mod} \ p)\) is less than \( \sqrt{p} + 1 \).

**Exercise 2.** Let \( p \) be a prime number such that \( p \equiv 1 \pmod{4} \). Prove that the equation \( x^p + 2p = p^2 + y^2 \) doesn’t have any solutions in natural numbers.

*Crux Mathematicorum, Vol. 43(8), October 2017*
Exercise 3. Prove that there are only finitely many positive integers $n$ such that
\[
\left(\frac{n}{1} + 1\right)\left(\frac{n}{2} + 2\right)\ldots\left(\frac{n}{n} + n\right)
\]
is an integer. (2016 Danube Mathematical Competition, proposed by Adrian Zahariuc.)

Exercise 4. Let $p$ be a prime of the form $4k + 1$ such that $2^p \equiv 2 \mod p^2$. 
Prove that there is a prime number $q$, divisor of $2^p - 1$, such that $2^q > (6p)^p$.
(Mathematical Reflections.)

Exercise 5. If $m$ is a positive integer, show that $5^m + 3$ has neither a prime divisor
of the form $p = 30k + 11$ nor of the form $p = 30k - 1$. (Mathematical Reflections.)

Exercise 6. Solve the equation $p^2 - pq - q^3 = 1$ in prime numbers. (2013
Tuymaada International Olympiad, Junior League, proposed by A. Golovanov.)

Exercise 7. Solve in natural numbers: $10^n + 89 = x^2$.

Exercise 8. Let $p$ be an odd prime such that $p \equiv 3 \mod 8$. Find all pairs of
integers $(x, y)$ that satisfy $y^2 = x^3 - p^2x$, where $x$ is even.

Exercise 9. Let $a$ be a positive integer such that for each positive integer $n$ the
number $a + n^2$ can be written as a sum of two squares. Prove that $a$ is a square.
(Mathematical Reflections.)

Exercise 10. Let $p = 4k + 3$ be a prime number. Find the number of different
residues $(mod \ p)$ of $(x^2 + y^2)^2$, where $(x, p) = (y, p) = 1$. (2007 Bulgarian IMO
Team Selection Test.)

Exercise 11. Let $p$ be an odd prime congruent to 2 modulo 3. Prove that at
most $p - 1$ members of the set \{ $m^2 - n^3 - 1 \mid 0 < m, \ n < p$ \} are divisible by $p$.
(1999 Balkan Mathematical Olympiad.)

Exercise 12. Let $q$ be an odd prime and $r$ a positive integer such that $q$ does not
divide $r$, $r \equiv 3 \mod 4$ and $\left(\frac{-r}{q}\right) = 1$. Prove that $4qk + r$ does not divide $q^n + 1$
for any $k, n$ positive integers.