The Legendre and Jacobi Symbols

Nguyen Tran Bach[*] Andrei Tiberiu Pantea[†]

April 30, 2018

In this paper, we present a very often met and useful method used in solving many olympiad number theory problems. This article presents the basic and advanced theory, while also providing some examples (with solutions) and exercises with hints.

Special thanks to Evan Chen for allowing us to use his LaTeXpackage which can be found at web.evanchen.cc and George Adrian Picu for helping us write this article by proposing constructive problems.

Contents

[*]International Computer High School of Bucharest. I can be reached at tactranbach@gmail.com.
[†]International Computer High School of Bucharest. I can be contacted at anditp@gmail.com.

§1 Introduction

§1.1 Quadratic Congruences

Firstly, we need to define the following terms.

Definition 1.1. We call x a **quadratic residue** modulo n if there exists an integer y such that $x \equiv y^2 \pmod{n}$. Otherwise x is called a **quadratic nonresidue** modulo n.

The following theorem shows the exact probability of an integer to be a quadratic residue modulo a prime.

Theorem 1.2

Let p be an odd prime and $A = \{1, 2, 3, ..., p-1\}$. Then, in the set A, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic nonresidues modulo p.

Proof. Consider the set $B = \{1^2, 2^2, 3^2, ..., (p-1)^2\}$. We claim that every quadratic residue modulo p is congruent to at least one element from B. Let n be a quadratic residue modulo p. It is obvious that $(n \bmod p)^2 \in B$, because $(n \bmod p) \in A$, thus our claim is proven.

Moving on, our second claim is that $x^2 \equiv (p-x)^2 \pmod{p}$ $\forall n \in A$ and $\nexists\ a,\ b \in A,\ a+b \neq p$ such that $a^2 \not\equiv b^2 \pmod{p}$. The first one is obvious. To prove the second one, suppose that there exist some numbers $a,\ b \in A$ such that $a+b \neq p$ and $a^2 \not\equiv b^2 \pmod{p}$. Then $p \mid a^2 - b^2 = (a-b)(a+b)$, but $-p < a-b < p \Rightarrow ((a-b)(a+b), p) = 1$, which yields a contradiction.

With both claims proven, the conclusion immediately follows. □

§1.2 Legendre Symbol

Definition 1.3. Let p be an odd prime number and n an integer. The **Legendre Symbol** is a function defined as $\left(\frac{n}{p}\right) = \begin{cases} -1 & \text{if } n \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \text{ divides } n, \\ 1 & \text{if } n \text{ is a quadratic residue modulo } p \text{ and } p \nmid n. \end{cases}$

The following is a table of values of $\left(\frac{k}{n}\right)$ with $n \leq 19$, $k \leq 20$, n odd prime.

n \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1	0	1	−1
5	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0	1	−1	−1	1	0
7	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1	0	1	1	−1	1	−1	−1
11	1	−1	1	1	1	−1	−1	−1	1	−1	0	1	−1	1	1	1	−1	−1	−1	1
13	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1	0	1	−1	1	1	−1	−1	−1
17	1	1	−1	1	−1	−1	−1	1	1	−1	−1	−1	1	−1	1	1	0	1	1	−1
19	1	−1	−1	1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	1	−1	0	1

Consider p an odd prime. Then the following statements are true:

(i) $\left(\frac{n^2}{p}\right) = 1$, $\forall n \in \mathbb{Z}$, $p \nmid n$.

(ii) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $\forall a, b \in \mathbb{Z}$.

(iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

(v) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$

(vi) (Euler's criterion) $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod{p}$, $\forall n \in \mathbb{Z}$.

The properties stated above aren't quite enough for us to be able to compute the Legendre Symbol, but the following theorem will do the trick.

Theorem 1.4 (Law of Quadratic Reciprocity)

Let p and q be some different odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Try to prove this theorem using the following lemma as a practice problem.

Lemma 1.5 (Gauss)

Let p and q be two different odd primes. Define $f_q(p) = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$. Then

$$f_p(q) + f_q(p) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

§1.3 Computational Example

We stated the previous properties, including the **Law of Quadratic Reciprocity**, and now we'll give an example of how to compute the Legendre Symbol for big numbers. We want to calculate $\left(\frac{12345}{331}\right)$.

$$\begin{aligned}
\left(\frac{12345}{331}\right) &= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{823}{331}\right) \\
&= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{161}{331}\right) \\
&= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{7}{331}\right)\left(\frac{23}{331}\right) \\
&= (-1)\left(\frac{331}{3}\right)\left(\frac{331}{5}\right)(-1)\left(\frac{331}{7}\right)(-1)\left(\frac{331}{23}\right) \\
&= \left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{2}{7}\right)\left(\frac{9}{23}\right) \\
&= -\left(\frac{2}{7}\right) = -(-1)^{\frac{7^2-1}{8}} = -1.
\end{aligned}$$

Or a more efficient method:

$$\left(\frac{12345}{331}\right) = \left(\frac{12345 - 37 \cdot 331}{331}\right) = \left(\frac{98}{331}\right) = \left(\frac{2 \cdot 7^2}{331}\right) = \left(\frac{2}{331}\right) = (-1)^{\frac{331^2-1}{8}} = -1.$$

§2 Examples

Now that you know how to compute the Legendre Symbol, we can proceed to solve some problems and lemmas.

Lemma 2.1 (Very Useful)

Let a and b be two integers and p a prime such that $p \mid a^2 + b^2$ and $p \equiv 3 \pmod 4$. Show that $p \mid a$ and $p \mid b$.

Proof. At the base of most number theory problems which can be solved using the Legendre Symbol are the obvious properties **(i)** and **(ii)**. Let's start our proof by assuming that $p \nmid a$, which also means that $p \nmid b$.

$$p \mid a^2 + b^2 \Leftrightarrow a^2 \equiv -b^2 \pmod p \Rightarrow \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) \Leftrightarrow \left(\frac{-1}{p}\right) = 1.$$

According to **(iv)**, we have that $p \equiv 1 \pmod 4$, which yields a contradiction. Thus we can conclude that $p \mid a$ and $p \mid b$. □

Now that you have seen how a problem can be approached with this method, try to solve the next lemma, which is very similar to the first one.

Lemma 2.2 (Very Useful)

Let a and b be two integers and p a prime such that $p \mid a^2 + ab + b^2$ and $p \equiv 2 \pmod 3$. Prove that $p \mid a$ and $p \mid b$.

The next problem is a perfect example of usage of the first two lemmas.

Example 2.3

If n is an integer, then $n^4 - n^2 + 1$ has only nonnegative divisors of the form $12k + 1$.

Proof. Its easy to see that $n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2$ and $n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2$. Bearing in mind the first two exercises, from the first relation we get that $p \equiv 1 \pmod 4$, while from the second one we get that $p \equiv \pm 1 \pmod{12}$. Thus the conclusion follows. □

Example 2.4 (Strengthening of Iran TST 2013)

Prove that there are no positive integers a, b, and c for which $\frac{a^2+b^2+c^2}{3(ab+bc+ca)}$ is an integer.

Proof. Suppose there exist four positive integers a, b, c, and n such that $a^2 + b^2 + c^2 = 3n(ab + bc + ca)$. WLOG[1], consider that $(a, b, c) = 1$. This can be rewritten as

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

[1] Without loss of generality

It is not difficult to see that $3n+2$ has a prime divisor $p \equiv 2 \pmod 3$ such that $2m+1 = v_p(3n+2)$ is[2] odd. Then

$$p^{2m+1} \mid (a+b+c)^2 \Rightarrow p^{2m+2} \mid (a+b+c)^2 \Rightarrow p \mid ab+bc+ca.$$

Substituting $c \equiv -a-b \pmod p$ in the previous relation, we obtain that $p \mid a^2+ab+b^2$. According to **Lemma 2.2**, $p \mid a$ and $p \mid b$, which results in $p \mid c$, but $(a,b,c) = 1$. This yields a contradiction, therefore there are no such numbers. □

The following problem was created by us and it was inspired from a problem from the Romanian Mathematical Olympiad.

Example 2.5 (Andrei Tiberiu Pantea, Nguyen Tran Bach)
Let $(a_n)_{n\geq 1}$ be an arithmetic progression of positive integers and $S_n = a_1^2 + a_2^2 + + a_n^2$, $n \in \mathbb{N}^*$. Prove that for all prime numbers $p \geq 5$ such that $p \equiv 5$ or $7 \pmod{12}$, S_p isn't a perfect square.

Proof. First of all, we want to write S_p as simply as possible. Because $p \geq 5$, we have that p is odd. So denote $a_{\frac{p-1}{2}} = a$ and the ratio of the arithmetic progression by r. Now,

$$\begin{aligned} S_p &= (a - \tfrac{p-1}{2}r)^2 + (a - \tfrac{p-3}{2}r)^2 + \cdots + a^2 + \cdots + (a + \tfrac{p-1}{2}r)^2 \\ S_p &= pa^2 + 2(1^2 + 2^2 + \cdots + (\tfrac{p-1}{2})^2)r^2 \\ S_p &= pa^2 + 2\frac{\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot p}{6}r^2 \\ S_p &= pa^2 + \frac{p(p-1)(p+1)}{12}r^2 \end{aligned}$$

So $p \mid S_p$, which means that if S_p is a perfect square, then $p^2 \mid S_p$. This implies that $p \mid a^2 + \frac{(p-1)(p+1)}{r}^2$. But since $(p,12) = 1 \Rightarrow p \mid 12a^2 + (p-1)(p+1)r^2 = 12a^2 + (p^2-1)r^2$. So $p \mid 12a^2 - r^2$, which is equivalent to $12a^2 \equiv r^2 \pmod p$. And this is where the Legendre Symbol comes in handy.

We now know that if S_p is a perfect square, then $\left(\frac{12a^2}{p}\right) = \left(\frac{r^2}{p}\right)$, which is equivalent to $\left(\frac{12}{p}\right) = 1$. From **(iii)**, $1 = \left(\frac{12}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right)$. And now, according to the Law of Quadratic Reciprocity, $1 = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}}$, so $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$.

And it is easy to show that $p = 12k+5$ or $12k+7$ are never solutions to this equation. Moreover, since p is prime, it can only be of the forms $12k+1$, $12k+5$, $12k+7$, or $12k+11$, of which the other two verify the relation. □

§3 What if p isn't prime?

In this section, we'll present a similar method to the one of Legendre Symbol, which allows us to bend the most imposing condition.

§3.1 Jacobi Symbol

Definition 3.1. Let n an integer and k a positive odd number with its prime factorization $k = p_1^{e_1}p_2^{e_2}p_3^{e_3}\dots p_r^{e_r}$. The **Jacobi Symbol** is a function of p and n defined as

$$\left(\frac{n}{k}\right) = \left(\frac{n}{p_1}\right)^{e_1}\left(\frac{n}{p_2}\right)^{e_2}\left(\frac{n}{p_3}\right)^{e_3}\cdots\left(\frac{n}{e_r}\right)^{e_r}.$$

[2] $v_p(n)$ denotes the exponent of p in the prime factorization of n.

As noticed, both the Legendre and Jacobi Symbols use the same notation, but there is no risk of confusion whatsoever. The properties of the Jacobi Symbol, as showed below, are very similar to those of Legendre. For the following statements, consider (a,b) a pair of integers and n, and m two positive odd numbers.

(i) $\left(\frac{a}{b}\right) = 0$ if and only if $(a,b) \neq 1$.

(ii) If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(iii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(iv) $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$

(v) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$

(vi) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$

For the Jacobi Symbol, the Euler's Criterion drops, but the Law of Quadratic Reciprocity still holds.

Theorem 3.2 (Law of Quadratic Reciprocity)
Let $(a,b) \in \mathbb{Z}_+^*$ be a pair of odd coprime numbers. Then $\left(\frac{a}{b}\right)\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

§3.2 Perfect example

Now that you know Jacobi symbol, here is a perfect example so you can get a hang of it and understand that it can simplify some proofs with Legendre Symbol.

Example 3.3 (Romania TST 2008)
Let $m,\ n \geq 3$ be positive odd integers. Prove that $2^m - 1$ doesn't divide $3^n - 1$.

Proof. This is a perfect example showing that Jacobi symbol can sometimes be more useful than Legendre.

Suppose there exist such numbers m and n. Then

$$2^m - 1 \mid 3^n - 1 \Leftrightarrow 3^n \equiv 1 \pmod{2^m - 1} \Rightarrow \left(\frac{3}{2^m-1}\right)^n = \left(\frac{3^n}{2^m-1}\right) = \left(\frac{1}{2^m-1}\right) = 1.$$

Using the Law of Quadratic Reciprocity, we have that

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

$\frac{3-1}{2}\cdot\frac{2^m-2}{2} = 2^{m-1}-1 = \text{odd}$. Therefore we have that $\left(\frac{2^{m-1}-1}{3}\right) = -1$, but $2^{m-1}-1 \equiv 1 \pmod{3}$ which yields a contradiction. □

If you try to approach the problem using Legendre Symbol, you would have to put in a lot of effort. Here is the second solution (provided by AoPS user *freemind*):

Let p be a prime divisor of $2^m - 1$ of the form $4k + 3$. Because $p|3^n - 1$, we have that $d = \text{ord}_3(p)$ is[3] odd. Since $d|p - 1 = 4k + 2$, we have $d|2k + 1$, hence $3^{\frac{p-1}{2}} = \left(\frac{3}{p}\right) = 1$. Then, by the Law of Quadratic Reciprocity, we have $\left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = -1$ hence $\left(\frac{p}{3}\right) = -1$, so $p = 3t + 2$.

Let now p be a prime divisor of $2^m - 1$ of the form $4k + 1$. A reasoning just as above and $\left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = 1$ leads to $\left(\frac{p}{3}\right) = 1$, hence $p = 3t + 1$.

So let M be the multiset of prime divisors p of $2^m - 1$ of the form $4k + 3$, containing each prime with multiplicity equal to its exponent in the prime factorization of $2^m - 1$. Because $2^m - 1 \equiv 3 \pmod 4$, $|M|$ is odd, but M contains precisely all prime divisors p of the form $3t + 2$ of $2^m - 1$. Then considering mod 3, we have $2^m - 1 \equiv 2^{|M|} \equiv 2 \pmod 3$. Contradiction! □

§4 More useful lemmas

Consider the following lemmas.

Lemma 4.1 (Very useful)

Let p be a prime and a, b a pair of integers. If $p \equiv 5$ or $7 \pmod 8$ and $p \mid a^2 + 2b^2$, then $p \mid a$ and $p \mid b$.

Lemma 4.2 (Very useful)

Let p be a prime and a, b a pair of integers. If $p \equiv 3$ or $5 \pmod 8$ and $p \mid a^2 - 2b^2$, then $p \mid a$ and $p \mid b$.

These lemmas are easy to prove using the Legendre Symbol, but they are a huge help, along with **Lemma 2.1**, in solving many Diophantine equations, that have no solutions or just the trivial ones.

§4.1 Diophantine equations

The problems we're about to cover are applications of the previous lemmas. The trick is to factorize a side of the equation so that on the other side we have something like $a^2 + b^2$, $a^2 - 2b^2$, $a^2 + 2b^2$, or $a^2 + ab + b^2$.

Example 4.3

Prove that the equation $x^3 - 6 = y^2$ has no solutions over $\mathbb{Z}^2$.

Proof. Suppose that such numbers exist. It is clear that x is odd. Therefore y is also odd and $y^2 + 6 \equiv -1 \pmod 8$. This also means that $x \equiv -1 \pmod 8$. We can rewrite

[3] $\text{ord}_n(a)$ (sometimes written as $\gamma_n(a)$) is the smallest number of the set $\{k \mid a^k \equiv 1 \pmod n,\ k \in \mathbb{N}\}$.

the equation as

$$x^3 - 2^3 = y^2 - 2 \text{ or } (x-2)(x^2+2x+4) = y^2 - 2.$$

Notice that $x-2$ has a prime divisor of the form $8k+3$ or $8k+5$[4]. Using **Lemma 4.2**, we have that this prime divisor also divides y and 1, which yields a contradiction. □

Example 4.4

Prove that the equation $x^3 - 16 = y^2$ has no solutions over $\mathbb{Z}^2$.

Proof. Suppose that such numbers exist. If $x = 2k,\ k \in \mathbb{Z}$, then $8 \mid y^2$, which makes y a multiple of 4. Let $y = 4s$. Furthermore, $16 \mid x^2 + 16 \Rightarrow k = 2l,\ l \in \mathbb{Z}$. Thus we have that $4l^3 - 1 = s^2$, but $s^2 \equiv 0,\ 1,$ or $4 \pmod 8$, which can't happen.

So we have that x and y^2 are odd numbers.

$$y^2 \equiv 1 \pmod 8 \Rightarrow x^3 \equiv 1 \pmod 8 \Rightarrow x \equiv 1 \pmod 8.$$

We rewrite the relation given as

$$x^3 - 2^3 = y^2 + 8 \text{ or } (x-2)(x^2+2x+4) = y^2 + 2 \cdot 2^2.$$

Notice that $x - 2 \equiv -1 \pmod 8$, which proves the existence of a prime $p \mid x-2$ such that $p \equiv 5$ or $7 \pmod 8$[5]. Using **Lemma 4.1**, a contradiction follows immediately. □

[4] If such prime didn't exist, then $x - 2 \equiv \pm 1 \pmod 8$.
[5] If such prime didn't exist, then $x - 2 \equiv 1$ or $3 \pmod 8$.

§5 Practice problems

Now, try it yourself!

Exercise 5.1 (Mathlinks)**.** Prove that for all numbers $1\underbrace{999...9}_{2k+1}$ have only divisors with the last digit 1 or 9.

Exercise 5.2. 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 $p \mid y^2 - y + 25$.

Exercise 5.3 (Gazeta Matematică)**.** Prove that the equation $x_1^p + x_2^p + x_3^p + \cdots + x_n^p + 1 = (x_1 + x_2 + x_3 + \cdots + x_n)^2$ has no integer solutions, where p is a prime such that $p \equiv 2 \pmod 3$.

Exercise 5.4. Let $a > 1$ be an odd integer that isn't a perfect square. Show that there exist two distinct odd primes p and q such that a is a quadratic nonresidue modulo p and also modulo q.

Exercise 5.5. Let a be an integer such that $\exists n \in \mathbb{Z}_+$, $\left(\frac{a}{p}\right) = 1$ $\forall p$ a prime number, $p > n$. Prove that a is a perfect square.

Exercise 5.6. Prove that the equation $x^3 + 11 = y^2$ has no solutions over $\mathbb{Z}^2$.

Exercise 5.7. Prove that the equation $x^3 - 10 = y^2$ has no solutions over $\mathbb{Z}^2$.

Exercise 5.8. The system of equations

$$\begin{cases} x^2 + (p-1)y^2 = z^2, \\ (p-1)x^2 + y^2 = u^2, \end{cases}$$

has no solutions over $\mathbb{Z}^5$, where p is a prime such that $p \equiv 3 \pmod 4$ and none of the numbers above is equal to 0.

Exercise 5.9. Solve the equation $x^3 + 19 = y^2$ over $\mathbb{Z}^2$.

Exercise 5.10. Prove that the equation $x^n - 2^n = x^2 + y^2$ has no solutions over $\mathbb{Z}^3$.

Exercise 5.11 (Romania TST 1997)**.** Let p be a prime and a, b, and n integers such that $b \neq 0$ and $p^n = a^2 + 2b^2$. Prove the existence of other two integers x and y for which $p = x^2 + 2y^2$.

Exercise 5.12. Prove that for every odd prime number p, all positive divisors of $\left\lfloor \frac{p+1}{4} \right\rfloor$ are quadratic residues modulo p.

Exercise 5.13 (BMO 1999)**.** Let $p > 2$ be a prime such that $p \equiv -1 \pmod 3$. Consider the set $S = \{y^2 - x^3 - 1 \mid x, y \in \mathbb{Z},\ 0 \leq x, y \leq p-1\}$. Prove that there are at most $p-1$ elements in S which are divisible by p.

Exercise 5.14. Prove that $4kxy - 1$ does not divide the number $x^m + y^n$ for any positive integers x, y, k, m, n.

§6 Hints

Hint 5.1. Just rewrite the number as $\frac{10^{2k+2}-1}{5}$.

Hint 5.2. $4(x^2-x+3)=(2x-1)^2+11$ and $4(y^2-y+25)=(2y-1)^2+99$.

Hint 5.3. Use **Lemma 2.2** and **Fermat's little theorem**.

Hint 5.4. Consider the prime factorization of a.

Hint 5.5. WLOG, consider that n is square-free[6]. Use **Dirichlet's theorem**[7].

Hint 5.6. $x^3+3^3=y^2+4^2$. Use **Lemma 2.1**.

Hint 5.7. $x^3+2^3=y^2+2\cdot 3^2$. Use **Lemma 4.1**.

Hint 5.8. Use **Lemma 2.1**.

Hint 5.9. The only solution is $5^3+19=12^2$. $x^3+3^3=y^2+2\cdot 2^2$. $x^3+1=y^2-2\cdot 3^2$. Use **Lemma 4.1** and **Lemma 4.2**.

Hint 5.10. Consider three cases: x is even, $x\equiv 1 \pmod 4$, and $x\equiv -1 \pmod 4$. Use **Lemma 2.1**.

Hint 5.11. Consider $k=\max(v_p(s),v_p(b))$. It is easy to see that $n-2k\geq 0$ and n is odd. This shows that $n-2k\geq 1$. From here use the Legendre Symbol.

Hint 5.12. If $p=4k+1$, write $p=4hq+1$, q is a prime. Use the **Law of Quadratic Reciprocity**. Same goes for $p=4k+3$.

Hint 5.13. Prove that the function $f:\mathbb{Z}_p\to\mathbb{Z}_p$, $f(x)=x^3$ is injective using **Lemma 2.2**.

Hint 5.14. Investigate three cases: $(m,n)=$ (odd, even), (odd,odd), (even, even). Use the **Law of Quadratic Reciprocity**, **(v)**, **(vi)**, and the following theorem:

Theorem 6.1

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 doesnt divide abc, then $\left(\frac{b^2-4ac}{p}\right)=1$.

§7 References

(1) Wikipedia, *Legendre Symbol*. https://en.wikipedia.org/wiki/Legendre_symbol.

(2) https://artofproblemsolving.com/community/c6h311730p1681256.

(3) Dušan Djukavić, *Quadratic Congruences*. https://web.math.pmf.unizg.hr/nastava/studnatj/quadcong_ddj.pdf.

(4) https://artofproblemsolving.com/community/c6h1208490p5978646.

(5) Laurenţiu Panaitopol, Alexandru Gica. *Probleme de aritmetică şi teoria numerelor. Idei şi metode de rezolvare*, Gil Publishing House.

(6) https://artofproblemsolving.com/community/c6h208565p1148144.

[6] An integer is square-free if there isn't a prime p such that $p^2 \mid n$.

[7] Dirichlet's theorem states that in any arithmetic progression a, $a+b$, $a+2b\ldots$ with $(a,b)=1$, there are infinitely many primes.