POLYNOMIAL LEGENDRE'S DIOPHANTINE EQUATIONS

DIMITAR GRANTCHAROV, ALEX KRUTKO, AND MAX KRUTKO

Abstract. In this project we consider polynomial Diophantine equations of Legendre type: $aX^2 + bY^2 + cZ^2 = 0$, where a, b, c, X, Y, Z are polynomials in $\mathbb{Q}[t]$. We find necessary and sufficient conditions for such Legendre's equations to have nontrivial solutions X, Y, Z in the case when all a, b, c have degree at most 1.

1. Introduction

A classical Diophantine equation, is the so-called Legendre's equation:

$$aX^2 + bY^2 + cZ^2 = 0$$

where all a, b, c, X, Y, Z are integer or rational numbers. The equation is named after Adrien Marie Legendre who proved in 1785, [1], that the equation is solvable in integers x, y, z, not all zero, if and only if $-bc$, $-ca$ and $-ab$ are quadratic residues modulo a, b and c, respectively, where a, b, c are nonzero, square-free, pairwise relatively prime integers, not all of the same sign.

In this paper we study Legendre equations in $\mathbb{Q}[t]$, namely equations of the form

$$a(t)X(t)^2 + b(t)Y(t)^2 + c(t)Z(t)^2 = 0$$

where $X(t), Y(t), Z(t)$ are polynomials with rational coefficients in one variable. This problems is interesting on its own but also arises in various mathematical theories, like quantum groups, quadratic fields, and elliptic curves, [2]. Our main theorem is a necessary and sufficient condition for the existence of nontrivial solutions of degree at most 1.

The organization of the paper is as follows. In Section 2 we introduce the classical Legendre equation and its solution. In Section 3 we derive necessary conditions for the polynomial Legendre equation to have a nontrivial solution. Lastly, in Section 4, we sufficient condition for the polynomial Legendre equation to have a nontrivial solution when all a, b, c have degree at most 1.

2. Classical Legendre's Equation

By $\mathbb{Z}$, $\mathbb{Q}$ we will denote the set of integer and rational numbers, respectively. We assume that the reader is familiar with some basic notions and results from number theory, for example, congruences, relatively prime numbers, etc.

Recall that the *classical Legendre's equation* in the integers X, Y, Z is

$$aX^2 + bY^2 + cZ^2 = 0$$

where a, b, c are fixed integers. For convenience, we will assume that a, b, c are relatively prime and square free. Recall that an integer n is *square free* if there is no integer $d > 1$ such that n is divisible by d^2. The following two theorems justify the reason that we may limit our attention to the case when a, b, c are pairwise relative prime and square free. The proof of the theorems is standard, see for example [3] and the references therein.

Theorem 2.1. *Let d be an integer such that d^2 divides a. Then the equation $aX^2+bY^2+cZ^2 = 0$ has a nontrivial solution if and only if $(a/d^2)X^2+bY^2+cZ^2 = 0$ does.*

Theorem 2.2. *Let d be an integer such that d divides a and b. Then the equation $aX^2 + bY^2 + cZ^2 = 0$ has a nontrivial solution if and only if $(a/d)X^2 + (b/d)Y^2 + cZ^2 = 0$ does.*

Recall that an integer u is a *quadratic residue* modulo an integer v, if there is an integer d such that

$$u \equiv d^2 \pmod{v}.$$

Below we state the classical Legendre Theorem.

Theorem 2.3 (Legendre, 1785)**.** *Let a, b, and c be square-free, pairwise relatively prime integers. Then the equation*

$$aX^2 + bY^2 + cZ^2 = 0$$

has a nontrivial solution if and only if not all a, b, c have the same sign, and $-bc$, $-ac$, and $-ab$ are quadratic residues modulo a,b, and c,respectively.

3. Necessary condition for solvability of Polynomial Legendre's equation

3.1. **Divisibility in $\mathbb{Q}[t]$.** By $\mathbb{Q}[t]$ we denote the set of polynomials with rational coefficients. In what follows we assume that all polynomials are with rational coefficients, i.e. in $\mathbb{Q}[t]$. We first introduce some basic divisibility notions in $\mathbb{Q}[t]$.

We say that $f(x)$ *divides* $g(x)$ in $\mathbb{Q}[t]$ if there is a polynomial $h(t)$ such that $f(t) = g(t)h(t)$ for every t. The notions of congruence modulo a polynomial, square free polynomial, and quadratic residue for polynomials are defined in the same way as for integers. For example, a polynomial $f(t)$ is *square free* if there is a polynomial $g(t)$ in $\mathbb{Q}[t]$ such that $g(t)^2$ divides $f(t)$. Equivalently, $f(t)$ is square free if $f(t)$ has no repeated roots in $\mathbb{C}$.

A *greatest common divisor* $d(t)$ of two polynomials $f(t)$ and $g(t)$, $\gcd(f(t), g(t))$, is a common divisor of $f(t)$ and $g(t)$ of minimal degree. Note that $\gcd(f(t), g(t))$ is not unique. For example $2t$ and $3t$ are greatest common divisors of $7t^2 + 10t$. We say that $f(t)$ and $g(t)$ are *relatively prime* if 1 is a greatest common divisor of $f(t)$ and $g(t)$).

3.2. **Legendre's equation in $\mathbb{Q}[t]$.**

Consider the the equation

$$a(t)X(t)^2 + b(t)Y(t)^2 + c(t)Z(t)^2 = 0 \tag{1}$$

where a, b, c are fixed in $\mathbb{Q}[t]$ and the unknowns X, Y, Z are also in $\mathbb{Q}[t]$. We call this equation the *polynomial Legendre's equation.* Like in the case of the classical Legendre's equation, for convenience, we will assume that a, b, c are pairwise relatively prime and square-free polynomials.

We want to determine conditions for a, b, c such that (1) has *nontrivial solution* (X, Y, Z), namely asolution (X, Y, Z) for which $(X, Y, Z) \neq (0, 0, 0)$. Below we prove a necessary condition for the polynomial Legendre's Equation to have a nontrivial solution.

Theorem 3.1. *Let $a(t), b(t), c(t)$ are square-free, pairwise relatively prime polynomials in $\mathbb{Q}[t]$. If*

$$a(t)X(t)^2 + b(t)Y(t)^2 + c(t)Z(t)^2 = 0$$

has a nontrivial solution, then $-b(t)c(t)$, $-a(t)c(t)$, and $-a(t)b(t)$ are quadratic residues modulo $a(t)$,$b(t)$, and $c(t)$, respectively.

Proof. The proof follows the proof of the classical Legendre theorem. For reader's convenince we outline the steps in the proof.

Assume that X, Y, Z is a nontrivial solution. Assume also that X, Y, Z have no comment factor of positive degree. We first note that $X(t)$ and $c(t)$ are relatively prime. Indeed, if $p(t)$, $\deg p \geq 1$, is irreducible polynomial that divides both $X(t)$ and $c(t)$, then $p(t)$ divides $b(t)Y(t)^2$. Hence, either p is a common factor of b and c, or p is a common factor of X and Y, which is a contradiction. Because $X(t)$ and $c(t)$ are relatively prime, there is a polynomial $W(t)$ such that

$$X(t)W(t) \equiv 1 \pmod{c(t)}.$$

From the equation $a(t)X(t)^2 + b(t)Y(t)^2 + c(t)Z(t)^2 = 0$ we find

$$-a(t)b(t)X(t)^2 \equiv (b(t)Y(t))^2 \pmod{c(t)}$$

Multiplying both sides of the above congruence by $W(t)^2$ we obtain that $-a(t)b(t)$ is a quaddratic residue modulo $c(t)$. Similarly we prove that $-a(t)c(t)$, and $-a(t)b(t)$ are quadratic residues modulo $b(t)$, and $c(t)$, respectively. □

4. Linear Polynomial Legendre Equations

In this section we consider the equation

$$a(t)X(t)^2 + b(t)Y(t)^2 + c(t)Z(t)^2 = 0; \quad \deg a, \deg b, \deg c \leq 1, \tag{2}$$

i.e. a polynomial Legendre equation with all $a(t), b(t), c(t)$ linear polynomials. The following theorem is the main result in this paper.

Theorem 4.1. *Let $a(t) = a_1t+a_0, b(t) = b_1t+b_0, c(t) = c_1t+c_0$, $a_i, b_i, c_i \in \mathbb{Q}$ such that $a(t), b(t), c(t)$ are pairwise relatively rime and a_1, b_1, c_1 are nonzero. Then the equation (2) has nontrivial solutions if and only if the following condition holds.*

- (L1) *The numbers $(c_0a_1 - a_0c_1)(b_0c_1 - c_0b_1)$ and $(b_0c_1 - c_0b_1)(a_0b_1 - b_0a_1)$ are nonzero perfect squares in $\mathbb{Q}$ (hence $(a_0b_1 - b_0a_1)(c_0a_1 - a_0c_1)$ is also a nonzero perfect square in $\mathbb{Q}$).*

If (L1) holds, then one nontrivial solution of (2) is $X(t) = \frac{1}{a_1W_0}$, $Y(t) = \frac{1}{b_1V_0}$, $Z(t) = \frac{1}{c_1U_0}$, where

$$\begin{aligned} U_0^2 &= \frac{(c_0a_1 - a_0c_1)(b_0c_1 - c_0b_1)}{c_1^2} \\ V_0^2 &= \frac{(b_0c_1 - c_0b_1)(a_0b_1 - b_0a_1)}{b_1^2} \\ W_0^2 &= \frac{(a_0b_1 - b_0a_1)(c_0a_1 - a_0c_1)}{a_1^2} \end{aligned}$$

Proof. We first prove the "only if" part. Assume that (2) has a nontrivial solution. Then by Theorem 3.1 we have

$$\begin{aligned} -(a_1t + a_0)(b_1t + b_0) &\equiv U^2 \pmod{c_1t + c_0} \\ -(c_1t + c_0)(a_1t + a_0) &\equiv V^2 \pmod{b_1t + b_0} \\ -(b_1t + b_0)(c_1t + c_0) &\equiv W^2 \pmod{a_1t + a_0} \end{aligned}$$

for some polynomials U, V, W. After substituting t with $-\frac{c_0}{c_1}$, $-\frac{b_0}{b_1}$, $-\frac{a_0}{a_1}$ in the first, second, and third congruence, respectively, we obtain

$$\begin{aligned} a_1b_1\left(\frac{a_0}{a_1} - \frac{c_0}{c_1}\right)\left(\frac{b_0}{b_1} - \frac{c_0}{c_1}\right) &= -U_0^2 \\ a_1c_1\left(\frac{a_0}{a_1} - \frac{b_0}{b_1}\right)\left(\frac{c_0}{c_1} - \frac{b_0}{b_1}\right) &= -V_0^2 \\ b_1c_1\left(\frac{b_0}{b_1} - \frac{a_0}{a_1}\right)\left(\frac{c_0}{c_1} - \frac{a_0}{a_1}\right) &= -W_0^2 \end{aligned}$$

This leads to

$$(c_0a_1 - a_0c_1)(b_0c_1 - c_0b_1) = (c_1U_0)^2 \tag{3}$$

$$(b_0c_1 - c_0b_1)(a_0b_1 - b_0a_1) = (b_1V_0)^2 \tag{4}$$

$$(a_0b_1 - b_0a_1)(c_0a_1 - a_0c_1) = (a_1W_0)^2. \tag{5}$$

The fact that U_0, V_0, W_0 are nonzero follow from the condition that $a(t), b(t), c(t)$ are relatively prime. This completes the proof of the "only if" part.

For the "if" part, first note that

$$\frac{1}{a_1W_0^2} + \frac{1}{b_1V_0^2} + \frac{1}{c_1U_0^2} = 0 \tag{6}$$

Indeed, the above identity can be easily proven by substituting U_0^2, V_0^2, and W_0^2 from (3), (4), (5). As a result we obtain:

$$\frac{(c_0a_1 - a_0c_1)(b_0c_1 - c_0b_1)}{c_1} + \frac{(b_0c_1 - c_0b_1)(a_0b_1 - b_0a_1)}{b_1} + \frac{(a_0b_1 - b_0a_1)(c_0a_1 - a_0c_1)}{a_1} = 0$$

Now we take

$$\begin{aligned} X(t) &= \frac{1}{a_1W_0} \\ Y(t) &= \frac{1}{b_1V_0} \\ Z(t) &= \frac{1}{c_1U_0} \end{aligned}$$

and substitute them in the original equation (2). We have that the degree 1 term of

$$(a_1t + a_0)X(t)^2 + (b_1t + b_0)Y(t)^2 + (c_1t + c_0)Z(t)^2$$

is zero by (6). For the degree 0 term we have:

$$\begin{aligned} a_0\frac{1}{(a_1W_0)^2} + b_0\frac{1}{(b_1V_0)^2} + c_0\frac{1}{(c_1U_0)^2} &= \frac{1}{(a_1W_0)^2} + \frac{1}{b_1(V_0)^2} - c_0\frac{b_1V_0^2 + a_1W_0^2}{c_1a_1b_1W_0^2V_0^2} \\ &= \frac{a_0b_1^2V_0^2 + b_0a_1^2W_0^2}{a_1^2b_1^2W_0^2V_0^2} - c_0\frac{b_1V_0^2 + a_1W_0^2}{c_1a_1b_1W_0^2V_0^2} \\ &= \frac{a_0b_1^2c_1V_0^2 + b_0a_1^2c_1W_0^2 - a_1b_1^2c_0V_0^2 - a_1^2b_1c_0W_0^2}{a_1^2b_1^2c_1W_0^2V_0^2} \\ &= \frac{V_0^2b_1^2(a_0c_1 - a_1c_0) + W_0^2a_1^2(b_0c_1 - b_1c_0)}{a_1^2b_1^2c_1W_0^2V_0^2} \\ &= \frac{-b_1a_1c_1V_0U_0W_0 + b_1a_1c_1V_0W_0U_0}{a_1^2b_1^2c_1W_0^2V_0^2} \\ &= 0. \end{aligned}$$

For the first identitity above we used (6), or more precisely:

$$\frac{1}{c_1U_0^2} = -\frac{1}{a_1W_0^2} + \frac{1}{b_1V_0^2} = -c_0\frac{b_1V_0^2 + a_1W_0^2}{c_1a_1b_1W_0^2V_0^2}.$$

For the fifth identity we used the following. First we observe the identity

$$(c_0a_1 - a_0c_1)(b_0c_1 - c_0b_1)(a_0b_1 - b_0a_1) = a_1b_1c_1U_0V_0W_0$$

which can be obtained by multiplying (3), (4), (5) together. From the latter identity,

$$a_0c_1 - a_1c_0 = -\frac{a_1b_1c_1U_0V_0W_0}{b_1^2V_0^2} = -\frac{a_1c_1U_0W_0}{b_1V_0}$$

Similarly

$$(b_0c_1 - b_1c_0) = \frac{a_1b_1c_1U_0V_0W_0}{a_1^2W_0^2} = \frac{a_1c_1U_0V_0}{a_1W_0}$$

This completes the proof. □

Example 4.2. *One easily checks that $a_1 = b_1 = c_1 = 1$, $a_0 = a$, $b_0 = a - \frac{5}{12}$ and $c_0 = -a + \frac{4}{15}$ satisfy (L1) in Theorem 4.1 for every rational a. This leads to the family of solutions $a(t) = t + a$, $b(t) = t + a - \frac{5}{12}$, $c(t) = -t + \frac{4}{15} - a$ of 2.*

Now we consider the case when one of $a(t), b(t), c(t)$ has degree 0. Since the case when all $a, b, c,$ are of degree 0 is the classical Legendre equation, there are two remaining cases to consider.

4.1. The case $\deg(c) = \deg(b) = 0, \deg(a) = 1$.

Theorem 4.3. *Let $a(t) = a_1t + a_0, b(t) = b_0, c(t) = c_0$ where $a_1, b_0,$ and c_0 is nonzero. Then the equation (2) has a nontrivial solution if and only if and only if the following condition holds.*

(L2) $-c_0b_0 = n^2$ *for some nonzero* $n \in \mathbb{Q}$.

If the above conditions hold then one nontrivial solution of (2) is $X = 0, Y = n, Z = b_0$

Proof. For the "only if" part, we use Theorem 3.1 and obtain

$$-c(t)b(t) \equiv q(t)^2 (\operatorname{mod} a(t))$$

for some polynomial $q(t)$ in $\mathbb{Q}[t]$. Hence $-c_0b_0 = \left(q(-\frac{a_0}{a_1})\right)^2$. Then $n = q(-\frac{a_0}{a_1})$ is the needed rational number in (L2).

For the "if" part, we directly verify:

$$(a_1t + a_0)0^2 + b_0n^2 + c_0b_0^2 = b_0n^2 - b_0n^2 = 0$$

This completes the proof. □

4.2. The case $\deg(a) = 0, \deg(b) = \deg(c) = 1$.

Theorem 4.4. *Let $a(t) = a_0, b(t) = b_1t + b_0, c(t) = c_1t + c_0$ where $b(t), c(t)$ are relatively prime and a_0, b_1, c_1 are nonzero. Then the equation (2) has a nontrivial solution if and only if the following condition holds.*

(L3) $-a_0\left(c_0 - \frac{c_1}{b_1}b_0\right) = U_0^2$ *and* $-a_0\left(b_0 - \frac{b_1}{c_1}c_0\right) = V_0^2$ *for some* $U_0, V_0 \in \mathbb{Q}$.

If the condition (L3) holds then one nontrivial solution of (2) is $X = U_0V_0$, $Y = U_0, Z = V_0$.

Proof. For the "only if" part, we use Theorem 3.1 and obtain

$$-a_0(c_1t + c_0) \equiv q(t)^2 \ (\operatorname{mod} (b_1t + b_0))$$

$$-a_0(b_1t+b_0)\equiv r(t)^2 \ (\mathrm{mod}\,(c_1t+c_0)),$$

for some $q(t)$ and $r(t)\in\mathbb{Q}[t]$. After substituting t with $-\frac{b_0}{b_1}$ and $-\frac{c_0}{c_1}$, we obtain:

$$-a_0\left(c_0-\frac{c_1}{b_1}b_0\right)=q\left(-\frac{b_0}{b_1}\right)^2$$
$$-a_0\left(b_0-\frac{b_1}{c_1}c_0\right)=r\left(-\frac{c_0}{c_1}\right)^2$$

Let $U_0 := q\left(-\frac{b_0}{b_1}\right)$ and $V_0 := r\left(-\frac{c_0}{c_1}\right)$. The fact that U_0 and V_0 are nonzero follows from the condition that $b(t)$ and $c(t)$ are relatively prime. In this way we establish the necessity of condition (L3).

For the "if" part, we need to verify that $X=U_0V_0, Y=U_0, Z=V_0$ is a solution of (2). If we set $\Delta=b_1c_0-c_1b_0$ we easily obtain

$$\begin{aligned}a_0X^2+(b_1t+b_0)Y^2+(c_1t+c_0)Z^2 &= a_0\frac{\Delta^2}{b_1c_1}+(b_1t+b_0)\left(-\frac{a_0\Delta}{b_1}\right)+(c_1t+c_0)\left(\frac{a_0\Delta}{c_1}\right)\\ &= 0.\end{aligned}$$

□

References

[1] L. Dickson, *History of the Theory of Numbers. Vol.II: Diophantine Analysis*, Chelsea Publishing, 1971, 422.

[2] P. Samet, An equation in gaussian integers, *The American Mathematical monthly* **59** (1952), 448–452

[3] J.-P. Serre, A course in arithmetic, *Graduate Texts in Mathematics*, **7**, Springer, 1973.