MEM204-Number Theory

14th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 20/05/2020

University of Crete

Legendre's equation

Introduction

Another natural extension of the Pythagorian triples, are the solutions of the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0.$$

This equation is known as Legendre's equation, in honor of Legendre, who characterized the solvability of this equation in 1795.

As we will later demonstrate with relative examples, the solution of an arbitrary equation of the above form can be reduced to the solution of another equation of the same form, where the numbers a, b, c are pairwise co-prime and square-free (i.e., not divided by any square).

An auxiliary lemma

Lemma

Let $A, B, C \in \mathbb{R}_{>0}$*, such that* $m = ABC \in \mathbb{Z}$*. Then, for every* $u, v, w \in \mathbb{Z}$*, the congruence*

$$ux + vy + wz \equiv 0 \pmod{m}$$

has a solution $(x, y, z) \neq (0, 0, 0)$*, such that* $|x| \leq A$*,* $|y| \leq B$ *and* $|z| \leq C$*.*

Proof of the auxiliary lemma

Take the set

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid 0 \leq x \leq A, 0 \leq y \leq B, 0 \leq z \leq C\}.$$

Then $|S| > ABC = m$, thus, there exist some $(x_1, y_1, z_1) \neq (x_2, y_2, z_2) \in S$, such that

$$ux_1 + vy_1 + wz_1 \equiv ux_2 + vy_2 + wz_2 \pmod{m}.$$

It follows that $(x_1 - x_2, y_1 - y_2, z_1 - z_2)$ is the required solution.

Another auxiliary lemma

Lemma

Let $n_1, n_2 > 1$ be co-prime. If the polynomial $f(x, y, z) = ax^2 + by^2 + cz^2$ $(a, b, c \in \mathbb{Z})$ is factorized into linear factors over $\mathbb{Z}_{n_1}$ and over $\mathbb{Z}_{n_2}$, then it also factors into linear factors over $\mathbb{Z}_{n_1 n_2}$.

Proof of the other auxiliary lemma

We have that

$$f(x,y,z) \equiv (a_1x + b_1y + c_1z)(d_1x + e_1y + f_1z) \pmod{n_1}$$
$$f(x,y,z) \equiv (a_2x + b_2y + c_2z)(d_2x + e_2y + f_2z) \pmod{n_2},$$

for some numbers $a_i, b_i, c_i, d_i, e_i, f_i$ $(i = 1, 2)$. The Chinese Remainder Theorem ensures the existence of some numbers $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$, such that

$$\alpha \equiv a_i \pmod{n_i}, \beta \equiv b_i \pmod{n_i}, \gamma \equiv c_i \pmod{n_i},$$
$$\delta \equiv d_i \pmod{n_i}, \varepsilon \equiv e_i \pmod{n_i}, \zeta \equiv f_i \pmod{n_i},$$

for $i = 1, 2$.

Proof of the other auxiliary lemma

It follows that

$$f(x, y, z) \equiv (\alpha x + \beta y + \gamma z)(\delta x + \varepsilon y + \zeta z) \pmod{n_i},$$

for $i = 1, 2$. Since $(n_1, n_2) = 1$, the above implies

$$f(x, y, z) \equiv (\alpha x + \beta y + \gamma z)(\delta x + \varepsilon y + \zeta z) \pmod{n_1 n_2},$$

as desired.

Next, we move on to our main theorem.

The main theorem

Theorem (Legendre)

Let a, b, c be square-free, pairwise co-prime integers, then the equation

$$f(x, y, z) = ax^2 + by^2 + cz^2 = 0$$

has a solution $(x, y, z) \neq (0, 0, 0)$ if and only if

1. *a, b, c are not all positive or all negative and*
2. *$-ab$, $-bc$ and $-ac$ are quadratic residues modulo $|c|$, $|a|$ and $|b|$ respectively.*

Proof of the main theorem

First, assume that we have a solution $(x, y, z) \neq (0, 0, 0)$. It is not hard to check that we may assume that $\gcd(x, y, z) = 1$.

We will now show that $(x, c) = 1$. If not, then there exists some prime $p \mid x$ and $p \mid c$, hence $p \mid by^2$. Since $(b, c) = 1$, we get

$$p \mid y^2 \overset{p \text{ prime}}{\Longrightarrow} p^2 \mid y^2 \overset{p^2 \mid x^2}{\Longrightarrow} p^2 \mid ax^2 + by^2 \Rightarrow p^2 \mid cz^2.$$

However, since $(x, y, z) = 1$, we get that $(p^2, z^2) = 1$, hence $p^2 \mid c$, a contradiction, since c is square-free. Hence, x is invertible $\pmod{c}$ and let u be its inverse. We now get

$$ax^2 + by^2 \equiv 0 \pmod{|c|} \overset{\cdot bu^2}{\Longrightarrow} (buy)^2 \equiv -ab \pmod{|c|},$$

that is, $-ab$ is a quadratic residue modulo $|c|$.

Proof of the main theorem

Similarly, $-bc$ and $-ac$ are quadratic residues modulo $|a|$ and $|b|$ respectively. Moreover, it is immediate that the existence of a non-trivial solution requires that not all three coefficients have the same sign.

We have now established the right direction of the equivalency and we move on to the left. Assume that the two items of the statement are satisfied. It follows that there exist some r, s such that

$$r^2 \equiv -ab \pmod{|c|} \text{ and } as \equiv 1 \pmod{|c|}.$$

Thus,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + by^2 \equiv as(ax^2 + by^2) \equiv s(a^2x^2 + aby^2) \\ &\equiv s((ax)^2 - (ry)^2) \equiv s(ax - ry)(ax + ry) \pmod{|c|}. \end{aligned}$$

Proof of the main theorem

So, in $\mathbb{Z}_{|c|}$, $ax^2 + by^2 + cz^2$ is factorized into linear factors. Similarly, we can find a facorization of this polynomial into linear factors over $\mathbb{Z}_{|a|}$ and $\mathbb{Z}_{|b|}$ and the second auxiliary lemma implies the existence of some $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$, such that

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\delta x + \varepsilon y + \zeta z) \pmod{|abc|}.$$

Now, apply the first auxiliary lemma, for the congruence

$$\alpha x + \beta y + \gamma z \equiv 0 \pmod{|abc|},$$

for $A = \sqrt{|bc|}$, $B = \sqrt{|ac|}$ and $C = \sqrt{|ab|}$. We get that there exists a solution $(x_0, y_0, z_0) \neq (0, 0, 0)$, with $|x_0| \leq A$, $|y_0| \leq B$ and $|z_0| \leq C$. Also, notice that $A, B, C \notin \mathbb{Z}$, so the above inequalities are, in fact, genuine.

Proof of the main theorem

W.l.o.g. we assume that $a, b > 0$ and $c < 0$. It follows that

$$ax_0^2 + by_0^2 + cz_0^2 < a|bc| + b|ac| = 2|abc|.$$

and

$$ax_0^2 + by_0^2 + cz_0^2 > c|ab| = -|abc|.$$

Given that $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{|abc|}$, the above imply $ax_0^2 + by_0^2 + cz_0^2 = 0$ or $-abc$. In the former case, (x_0, y_0, z_0) is the desired solution.

Proof of the main theorem

In the latter case, we get

$$ax_0^2 + by_0^2 + cz_0^2 = -abc \Rightarrow ax_0^2 + by_0^2 + c(z_0^2 + ab) = 0.$$

This is equivalent to

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 + c(z_0^2 + ab)^2 = 0,$$

where clearly $z_0^2 + ab > 0$. It follows that $(x_0z_0 + by_0, y_0z_0 - ax_0, z_0^2 + ab)$ is the desired solution. This concludes the proof of Legendre's theorem.

An example

Let us now study the existence of a non-trivial solution of the equation

$$9x^2 + 35y^2 - 721z^2 = 0. \tag{1}$$

First, we notice that Legendre's theorem cannot be directly applied to (1), as (i) the coefficients are not square-free and (ii) the coefficients are not pairwise co-prime. However, we can tranform it into one that meets Legendre's theorem criteria.

Namely, we multiply everything by the appearing gcd's (here 7) and gather all the resulting and pre-existing squares and we get the equivalent equation

$$7(3x)^2 + 5(7y)^2 - 103(7z)^2 = 0.$$

An example

We set $X = 3x$, $Y = 7y$ and $Z = 7z$ and get

$$7X^2 + 5Y^2 - 103Z^2 = 0. \tag{2}$$

In the above equation, we can apply Legendre's theorem.

By computing the corresponding Legendre symbols, we can easily check that, in fact, the numbers $-5 \cdot 7$, $103 \cdot 5$ and $103 \cdot 7$ are quadratic residues modulo 103, 7 and 5 respectively, so the existence of an integer solution of (2) is ensured.

Let (u, v, w) be this solution. It follows that $\left(\frac{u}{3}, \frac{v}{7}, \frac{z}{7}\right)$ is a (rational) solution of (1) and that $(7u, 3v, 3z)$ is an integer solution of (1).

Stay safe!