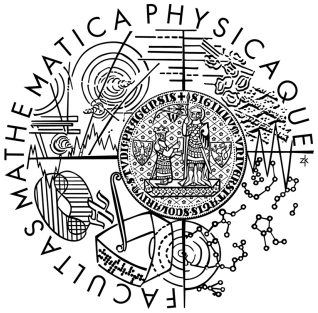
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Veronika Půlpánová

Diofantické rovnice a p-adická čísla

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.

Studijní program: Matematika, Obecná Matematika

2010

Prohlašuji, že jsem svou bakalářskou práci napsala samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne Veronika Půlpánová

Contents

Název práce: Diofantické rovnice a p-adická čísla
Autor: Veronika Půlpánová
Katedra (ústav): Katedra Algebry
Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
e-mail vedoucího: libor.barto@gmail.com

Abstrakt: V předložené práci studujeme využití p-adických čísel pro ověřování existence řešení Diofantických rovnic. Lokálně-globální princip říká, že studiem řešení Diofantických rovnic lokálně v $\mathbb{Q}_p$, tělesech p-adických čísel, můžeme získat informaci o globálním řešení v $\mathbb{Q}$. Hasse-Minkowskiho věta popisuje třídu Diofantických rovnic, na kterých lze Lokálně-globální princip efektivně využít. Detailně studujeme tuto třídu, zúženou na polynomy o třech neznámých. Pro polynom $F(X, Y, Z) = aX^2 + bY^2 + cZ^2$ sestavíme krátký seznam podmínek, které a, b, c musí splňovat, aby existovalo netriviální řešení v $F(X, Y, Z) = 0$ v $\mathbb{Q}$.

Klíčová slova: Diofantické rovnice, Hasse-Minkowskiho věta, Lokálně-globální princip, p-adická čísla

Title: Diophantine equations and p-adic numbers
Author: Veronika Pulpanova
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: libor.barto@gmail.com

Abstract: In the thesis we study the use of p-adic numbers in determining the existence of a solution of Diophantine equations. The Local-global principle says that certain information about the global solution of a Diophantine equation in $\mathbb{Q}$ may be obtained from the study of the local solutions in the completion fields $\mathbb{Q}_p$. The Hasse-Minkowski theorem provides a class of Diophantine equations, where the Local-global principle can be applied in a very effective way. In the further study we restrict this class only to polynomials of three variables. For $F(X, Y, Z) = aX^2 + bY^2 + cZ^2$ we construct a short list of easily checked conditions that determine the existence of a nontrivial solution of $F(X, Y, Z) = 0$ in $\mathbb{Q}$.

Keywords: Diophantine equations, Hasse-Minkowski theorem, Local-global principle, p-adic numbers

Chapter 1

Introduction

The problem of finding a solution in $\mathbb{Z}$ of a polynomial equation with integer coefficient dates back to ancient Greece. These kinds of equations, called Diophantine equations, remained in the interest of many mathematicians during the centuries so that D. Hilbert decided to include them into his famous list of twenty-three mathematical challenges for 20th century [3]. Known as Hilbert's tenth problem it states:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Very importantly, Hilbert's tenth problem marks the beginning of development of computer science, and particularly was decisive for a formalization of the concept of an algorithm that is of an aforementioned "process with finite number of operations" . It was Y. Matiysevich in 1970, who showed that problem of finding solutions of such equations is algorithmically undecidable, that is, no such process can be found [4]. However, there are certain classes of Diophantine equations, where we do know an algorithm that finds all the solutions or says that there are not any (e.g. the class of linear Diophantine equations). There exist many approaches how to solve particular Diophantine equation (e.g. continued fraction method for solving Pell's equation), but these methods usually cannot be generalized in order to solve some larger class of equations. In this thesis we will treat the techniques employed to solve quadratic Diophantine equations and show that these techniques can be effectively used in case of homogenous quadratic homogenous equations in three variables.

One of the useful observations of the theory of Diophantine equations states that a necessary condition for finding a solution of an equation in $\mathbb{Z}$ is the existence

of a solution of the equation modulo p. We call this the *local solution*. However, as it is shown in Chapter 4, the condition is not sufficient and therefore, cannot guarantee the existence of the global solution.

Somehow stronger result can be obtain by looking up solutions modulo p^n for all $n \in \mathbb{N}$, in other words, searching a solution in the field of p-adic integers $\mathbb{Z}_p$, which are discussed in Chapter 2. Although in general again the existence of a solution in $\mathbb{Q}_p$ for all the primes p does not give us a guarantee of a success in finding solution in $\mathbb{Z}$, there is a class of Diophantine equations, i.e. aforementioned homogenous quadratic equations, where this condition proves to be sufficient. This result is know as Hasse–Minkowski theorem, which we deal with towards the end of Chapter 4.

The last chapter is dedicated to applications of the Hasse–Minkowski theorem to a simplified equation and builds a lot simplier way to to determine the existence of a solution.

Chapter 2

p-adic numbers

In this chapter we will define the field of p-adic numbers $\mathbb{Q}_p$ and show some of its basic properties. All the mentioned fields are commutative.

2.1 Basic Notions

We would like to define $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$ with respect to a norm with a special property. Here we provide the definition of a non-Archimedean norm:

Definition 2.1. *Let F be a field. A function $||.|| : F \to \mathbb{R}$ is called a* norm*, if it has the following properties:*

(N1) $||x|| \geq 0$*, with the equality if and only if* $x = 0$*.*

(N2) $\|xy\| = \|x\|\|y\|$*.*

(N3) $\|x + y\| \leq \|x\| + \|y\|$*.*

We say that the distance d is induced by a norm *if* $d(x, y) = \|x - y\|$*.*
A norm is called non-Archimedean *if*

$$\|x + y\| \leq \max(\|x\|, \|y\|)$$

holds for all $x, y \in F$*.*

Obviously, the standard norm on $\mathbb{R}$ does not have this property. We will need the following two properties of non-Archimedean norms.

Proposition 2.1. *In a field F with a non-Archimedean norm $\|.\|$, all the triangles are isosceles.*

Proof. Let $X, Y, Z \in F$ be a triangle. Without loss of generality, let us assume that

$$\|X - Y\| < \|X - Z\|.$$

Then

$$\|X - Z\| = \|(X - Y) + (Y - Z)\| \leq \max(\|X - Y\|, \|Y - Z\|),$$

$$\text{so } \|X - Z\| \leq \|Y - Z\|.$$

Also

$$\|Y - Z\| = \|(Y - X) + (X - Z)\| \leq \max(\|X - Y\|, \|X - Z\|) = \|X - Z\|.$$

Therefore, we get

$$\|X - Z\| \leq \|Y - Z\| \text{ and } \|Y - Z\| \leq \|X - Z\| \Rightarrow \|X - Z\| = \|Y - Z\|.$$

□

Proposition 2.2. *Let F be a field with a non-Archimedean norm $\|.\|$ and the distance induced by a norm. Let $B(a, r)$ be a ball in F, i.e. $B(a, r) = \{x \in F; \|x - a\| < r\}$. Then all the points of the ball are its center.*

Proof. For any $x, b \in B(a, r)$ we have that

$$\|x - b\| = \|x - a + a - b\| \leq \max(\|x - a\|, \|a - b\|) < r.$$

Hence, for all $x \in B(a, r)$, x is also in $B(b, r)$. Therefore, $B(a, r) \subseteq B(b, r)$.

Analogously, $B(b, r) \subseteq B(a, r)$ and the claim follows.

□

2.2 Norm $|.|_p$

It is time to define some particular non-Archimedean norm.

Definition 2.2. *Let p be a prime. For all $a \in \mathbb{Z}, a \neq 0$, we define $\mathrm{ord}_p a$ as the greatest power of p that divides a. For $a = 0$ we put $\mathrm{ord}_p a = \infty$. For $a \in \mathbb{Q}$, $a = \frac{a_1}{a_2}$, we put $\mathrm{ord}_p a = \mathrm{ord}_p a_1 - \mathrm{ord}_p a_2$.*

Definition 2.3. *Let p be a prime. We define the norm $|.|_p$ on $\mathbb{Q}$*

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0. \end{cases}$$

Proposition 2.3. *$|.|_p$ is a non-Archimedean norm on $\mathbb{Q}$.*

Proof. (N1) If $x = 0$, then $|x|_p = 0$. Let $x \neq 0$, $p \geq 0$, $\text{ord}_p \in \mathbb{Z}$, then

$$|x|_p = p^{-\text{ord}_p x} > 0.$$

(N2) Let $x, y \in \mathbb{Q}$. Since p is a prime, $\text{ord}_p xy = \text{ord}_p x + \text{ord}_p y$. Then

$$|xy|_p = p^{-\text{ord}_p xy} = p^{-\text{ord}_p x - \text{ord}_p y} = p^{-\text{ord}_p x} p^{-\text{ord}_p y} = |x|_p |y|_p.$$

(N3) Let $x, y \in \mathbb{Q}$. If $x = 0$ or $y = 0$ or $x + y = 0$, then the property holds. Let $x, y, x + y \neq 0$. We can write $x = \frac{a}{b}, y = \frac{c}{d}$. We have

$$\text{ord}_p(x + y) = \text{ord}_p \frac{ad + bc}{bd} = \text{ord}_p(ad + bc) - \text{ord}_p b - \text{ord}_p d$$

The greatest power that divides two numbers is at least the minimum of the greatest powers that divide each of the two numbers, i.e.

$$\text{ord}_p(k + l) \geq \min(\text{ord}_p k, \text{ord}_p l).$$

Therefore, we get

$$\text{ord}_p(ad + bc) \geq \min(\text{ord}_p ad, \text{ord}_p bc),$$

$$\text{ord}_p(x + y) = \text{ord}_p \frac{ad + bc}{bd} \geq \min(\text{ord}_p a + \text{ord}_p d, \text{ord}_p b + \text{ord}_p c) - \text{ord}_p b - \text{ord}_p d$$

$$= \min(\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d) = \min(\text{ord}_p x, \text{ord}_p y)$$

$$\text{ord}_p(x + y) \geq \min(\text{ord}_p x, \text{ord}_p y)$$

$$-\text{ord}_p(x + y) \leq \max(-\text{ord}_p x, -\text{ord}_p y)$$

p^α increases with α, so

$$p^{-\text{ord}_p(x+y)} \leq \max(p^{-\text{ord}_p x}, p^{-\text{ord}_p y}),$$

$$\text{i.e. } |x + y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$

We have shown that $|.|_p$ has the property (N3) and that it is non-Archimedean. □

It is possible to show that all the norms on $\mathbb{Q}$ are either equivalent to the standard norm used on $\mathbb{R}$ or to a norm $|.|_p$ for some prime p. The details can be found in Gouvea[2].

2.3 $\mathbb{Q}_p$

The field $\mathbb{Q}$ is not complete with respect to the Archimedean norm. The real numbers $\mathbb{R}$ may be defined as the completion of $\mathbb{Q}$ with respect to an Archimedean norm. The field of p-adic numbers $\mathbb{Q}_p$ is defined similarly.

Definition 2.4. *We define the field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the norm $|.|_p$.*

The field $\mathbb{Q}_p$ has some convenient properties that would not be found in $\mathbb{R}$.

Proposition 2.4. *In $\mathbb{Q}_p$ the series $\sum_{n=0}^{\infty} \beta_n$ is convergent if and only if $\beta_n \to 0$.*

Proof. One implication is clear. To show the reverse implication, we take

$$\left| \sum_{n=0}^{N} \beta_n - \sum_{n=0}^{M} \beta_n \right|_p = | \sum_{n=M+1}^{N} \beta_n |_p \leq \max_{M<n\leq N} |\beta_n|_p \longrightarrow 0.$$

The last inequality holds because the non-Archimedean property can be extended by induction. So $\sum \beta_n$ is a Cauchy sequence. Since $\mathbb{Q}_p$ is complete, $\sum \beta_n$ is convergent.

□

So we have the definition of $\mathbb{Q}_p$, but it is not very clear, what the elements of $\mathbb{Q}_p$ actually are. Obviously, the elements of $\mathbb{Q}$ do belong there, but what else? First we have a closer look at the elements of $\mathbb{Z}_p$, so called p-adic integers, which is a subset of $\mathbb{Q}_p$.

Definition 2.5. *We define the set of* p-adic integers $\mathbb{Z}_p$ *as a subset of $\mathbb{Q}_p$,*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

We can see that $\mathbb{Z}_p \cap \mathbb{Q}$ are exactly such numbers $x \in \mathbb{Q}$ that have the form $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $p \nmid b$.

Proposition 2.5. *$\mathbb{Z}_p$ is a ring.*

Proof. We take $x, y \in \mathbb{Z}_p$. We have $|x|_p, |y|_p \leq 1$. Then

$$\begin{gathered} |x+y|_p \leq \max(|x|_p, |y|_p) \leq 1 \\ |x|_p, |y|_p \leq 1 \text{ so } \operatorname{ord}_p x, \operatorname{ord}_p y \geq 0 \\ \text{we have } 0 \leq \operatorname{ord}_p x + \operatorname{ord}_p y = \operatorname{ord}_p xy \text{ so } |xy|_p \leq 1. \end{gathered}$$

We can see that $|x+y|_p, |xy|_p \leq 1$. Therefore, $\mathbb{Z}_p$ is a ring. □

Proposition 2.6. *Every element of $\mathbb{Z}_p$ can be written uniquely in the form*

$$\alpha = \sum_{n=0}^{\infty} a_n p^n,$$

where $a_n \in \{0, 1, ..., p-1\}$ for all n.

Proof: Based on Cassels[1]. We show that α of the form $\sum_{n=0}^{\infty} a_n p^n$ are in $\mathbb{Z}_p$:

$$|\alpha|_p = \left| \sum_{0}^{\infty} a_n p^n \right|_p \leq \max_{0 \leq n < \infty} (|a_n p^n|_p) = \max_{0 \leq n < \infty} (|p^n|_p) = 1.$$

We take an arbitrary $\alpha \in \mathbb{Z}_p$. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, there exists $b \in \mathbb{Q}$ such that $|b - \alpha|_p < 1$. Obviously, there exists a unique $a_0 \in \{0, ..., p-1\}$ such that $|a_0 - b|_p < 1$. Therefore,

$$\alpha = a_0 + p\alpha_1 \text{ for some } \alpha_1,$$

where $|\alpha_1|_p \leq 1$, i.e. $\alpha_1 \in \mathbb{Z}_p$. By induction, we get the series

$$\alpha = a_0 + a_1 p + a_2 p^2 + ... + a_n p^n + \alpha_{n+1} p^{n+1}$$

where $\alpha_{n+1} \in \mathbb{Z}_p$. We show that $\lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i = \alpha$:

$$|\lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i - \alpha|_p = \lim_{n\to\infty} \left| \sum_{i=0}^{n} a_i p^i - \alpha \right|_p = \lim_{n\to\infty} |\alpha_n p^n|_p \leq \lim_{n\to\infty} p^{-n} = 0.$$

□

Then the elements of $\mathbb{Q}_p$ are the series of a form

$$\alpha = \sum_{n=-n_0}^{\infty} a_n p^n, \ a_n \in \{1, .., p-1\},$$

because for $\alpha \in \mathbb{Q}_p$, we have $|\alpha|_p = p^{n_0}$, for some $n_0 \in \mathbb{Z}$. Hence $\alpha = p^{-n_0}\alpha_1$ for some $\alpha_1 \in \mathbb{Z}_p$ and

$$\alpha = p^{-n_0} \sum_{n=0}^{\infty} a_n p^n = \sum_{n=n_0}^{\infty} a'_n p^n.$$

Note that the p-adic integers could be defined as the formal series $\alpha = \sum_{n=0}^{\infty} a_n p^n$, $a_n \in \{1, ..., p-1\}$. The addition, multiplication and congruences are done rather intuitively. For $\alpha = \sum_{n=0}^{\infty} a_n p^n, \beta = \sum_{n=0}^{\infty} b_n p^n$, we have:

$$\alpha + \beta = \sum_{n=0}^{\infty} (a_n + b_n) p^n$$
$$\alpha \cdot \beta = \sum_{n=0}^{\infty} = \sum_{m=0}^{\infty} a_n b_m p^{n+m}$$
$$\alpha \mod p^n = \sum_{i=0}^{n-1} a_i p^i$$

Note that $\alpha \in \mathbb{Z}_p$ is described uniquely by its reductions modulo p^n for all $n \in \mathbb{N}$.

$$\text{ord}_p \alpha = m, \text{ for the largest } m \in \mathbb{N}, \text{ such that for all } n < m : a_n = 0$$
$$|\alpha|_p = p^{-m}.$$

α is invertible in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$, i.e. $|\alpha|_p = 1$. The set of $\alpha \in \mathbb{Z}_p$, α invertible, is called the p-adic units and it is denoted $\mathbb{Z}_p^\times$.

Proposition 2.7. *The p-adic expansion of a number $\alpha \in \mathbb{Q}_p$ in series of powers of p is finite if and only if α is a positive rational number, such that its denominator is a power of p.*

Proof. Let α be finite series of powers of p, i.e. $\alpha = \sum_{n=-k}^{N} a_n p^n$, with $k \geq 0$.

$$\alpha = a_{-k} p^{-k} + ... + a_0 + a_1 p + ... + a_N p^N$$
$$= \frac{1}{p^k} p^k (a_{-k} p^{-k} + ... + a_0 + a_1 p + ... + a_N p^N) = \frac{1}{p^k} \sum_{n=0}^{N+k} a_n p^n$$

We take $a = \sum_{n=0}^{N+k} a_n p^n$ and $b = p^k$. Then $\alpha = a/b$ where a is a finite sum of integers, which is an integer and b a power of p. This gives us the first implication.

Let $\alpha = \frac{\alpha_1}{p^k}$ with $k \geq 0, \alpha_1 \in \mathbb{Z}$. Since $\alpha_1 \in \mathbb{Z}$ is a finite number, we can write it in a p-ary base, $\alpha = (a_0, ..., a_N)$ with N finite, i.e. $\alpha_1 = \sum_{n=0}^{N} a_n p^n$. Therefore,

$$\alpha = \frac{\alpha_1}{p^k} = \frac{1}{p^k} \sum_{n=0}^{N} a_n p^n = \sum_{n=-k}^{N-k} a_n p^n,$$

which proves the proposition.

□

Chapter 3

Hensel's Lemma

This chapter provides us with a very usefull tool for the work with p-adic numbers and Diophantine equations. We have a Diophantine equation and a prime p and we want to determine, whether there is a solution in $\mathbb{Z}_p$. The Hensel's lemma determines the conditions under which we only need to check the existence of a solution modulo p, which saves us a great deal of effort.

The lemma comes in two versions. The first version is less general than the second, but its conditions are more straightforward to check. If these conditions cannot be satisfied, we can still try to use the second version, which has a wider use.

Theorem 3.1 (Hensel's lemma, First version)**.** *Let $F(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ be a polynomial, where $a_i \in \mathbb{Z}_p$. Suppose, there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$, such that*

$$F(\alpha_1) \equiv 0 \mod p$$

and

$$F'(\alpha_1) \neq 0 \mod p$$

where $F'(X) = a_1 + 2a_2X + ... + na_nX^{n-1}$ is the formal derivative of $F(X)$. Then there exists a p-adic integer $\alpha \in \mathbb{Z}_p$ such that

$$\alpha \equiv \alpha_1 \mod p$$

and

$$F(\alpha) = 0.$$

Proof. (Based on Gouvea[2]). We will construct a sequence $(\alpha_n)_{n\in\mathbb{N}}$ such that $\alpha_n \equiv \alpha_{n+1} \mod p^n$ and

$$F(\alpha_{n+1}) \equiv 0 \mod p^n.$$

The proof goes by induction: for $n = 1$, we have

$$F(\alpha_1) \equiv 0 \mod p.$$

Suppose we have $\alpha_n \in \mathbb{Z}_p$ such that

$$F(\alpha_n) \equiv 0 \mod p^n.$$

Note that from $\alpha_n \equiv \alpha_1$ modulo p, it follows that $F'(\alpha_n) \equiv F'(\alpha_1) \neq 0$ modulo p. We need to find an $\alpha_{n+1} \in \mathbb{Z}_p$ satisfying

$$\alpha_{n+1} \equiv \alpha_n \mod p^n$$

and

$$F(\alpha_{n+1}) \equiv 0 \mod p^{n+1}.$$

We want to find $x \in \{1, ..., p-1\}$, such that $\alpha_{n+1} = \alpha_n + p^n x$ and $F(\alpha_n + p^n x) \equiv 0 \mod p^{n+1}$. Expanding into Taylor serie, we have

$$F(\alpha_n + p^n x) = F(\alpha_n) + F'(\alpha_n)p^n x + \frac{1}{2}F''(\alpha_n)p^{2n}x^2 + ...$$

$$0 \equiv F(\alpha_n + p^n x) \equiv F(\alpha_n) + F'(\alpha_n)p^n x \mod p^{n+1}$$

Since $F(\alpha_n) \equiv 0 \mod p^n$, there exists $y \in \mathbb{Z}$ such that $F(\alpha_n) \equiv yp^n$ modulo p^{n+1}.

$$0 \equiv yp^n + F'(\alpha_n)p^n x \mod p^{n+1}$$

or equivalently,

$$0 \equiv y + F'(\alpha_n)x \mod p.$$

Since $F'(\alpha_n) \neq 0 \mod p$, it is perfectly legal to set

$$x = \frac{y}{F'(\alpha_n)} \mod p.$$

We found $\alpha_{n+1} \in \mathbb{Z}_p$ such that $\alpha_{n+1} \equiv \alpha_n \mod p^n$ and $F(\alpha_{n+1}) \equiv 0 \mod p^{n+1}$.

We found a Cauchy sequence (α_n) in $\mathbb{Q}_p$. Because $\mathbb{Q}_p$ is complete, there exists a limit. We set $\alpha = \lim \alpha_n$. Then $\alpha \equiv \alpha_1 \mod p$ by construction and the continuity gives us $F(\alpha) = 0$. □

Theorem 3.2 (Hensel's lemma, Second version)**.** *Let* $F(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ *be a polynomial, where* $a_i \in \mathbb{Z}_p$*. Suppose, there exists a p-adic integer* $\alpha_1 \in \mathbb{Z}_p$*, such that*

$$|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2$$

where $F'(X) = a_1 + 2a_2X + ... + na_nX^{n-1}$ *is the formal derivative of* $F(X)$*. Then there exists a p-adic integer* $\alpha \in \mathbb{Z}_p$ *such that*

$$\alpha \equiv \alpha_1 \mod p^{\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))}$$

and

$$F(\alpha) = 0.$$

Proof. We will construct a sequence $(\alpha_n)_{n\in\mathbb{N}}$ such that

$$\alpha_n \equiv \alpha_{n+1} \mod p^{n(\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)))}$$

and

$$F(\alpha_{n+1}) \equiv 0 \mod p^{n(\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)))}.$$

The proof goes by induction: for $n = 1$, we have

$$F(\alpha_1) \equiv 0 \mod p^{\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))},$$

because $F(\alpha_1) = p^{\mathrm{ord}_p(F(\alpha_1))}\xi$, where ξ is a p-adic unit and

$$\mathrm{ord}_p(F(\alpha_1)) > \mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)) > 0.$$

Also

$$F'(\alpha_1) \neq 0 \mod p^{\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))},$$

because $F'(\alpha_1) = p^{\mathrm{ord}_p(F'(\alpha_1))}\gamma$, where γ is some p-adic unit and $\mathrm{ord}_p(F'(\alpha_1)) < \mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))$. Note that from $\alpha_n \equiv \alpha_1$ modulo $p^{\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))}$, it follows that $F'(\alpha_n) \equiv F'(\alpha_1) \neq 0$ modulo $p^{\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1))}$. Suppose we have $\alpha_n \in \mathbb{Z}_p$ such that

$$F(\alpha_n) \equiv 0 \mod p^{n(\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)))}.$$

We need to find an α_{n+1} satisfying

$$\alpha_{n+1} \equiv \alpha_n \mod p^{n(\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)))}$$

and

$$F(\alpha_{n+1}) \equiv 0 \mod p^{(n+1)(\mathrm{ord}_p(F(\alpha_1)) - \mathrm{ord}_p(F'(\alpha_1)))}.$$

We want to find $x \in \mathbb{Z}$, such that $\alpha_{n+1} = \alpha_n + p^{n(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}x$ and

$$F(\alpha_n + p^{n(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}x) \equiv 0 \mod p^{n+1}.$$

Expanding into Taylor serie, we have

$$F(\alpha_n+p^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x) = F(\alpha_n)+F'(\alpha_n)p^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x+\frac{F''(\alpha_n)}{2}p^{2n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x^2+...$$

$$0 \equiv F(\alpha_n+p^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x) \equiv F(\alpha_n)+F'(\alpha_n)p^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x \mod p^{(n+1)\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}$$

Since $F(\alpha_n) \equiv 0 \mod p^{n(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}$, there exists $y \in \mathbb{Z}$ such that

$$F(\alpha_n) \equiv yp^{n(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}.$$

$$0 \equiv yp^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)} + F'(\alpha_n)p^{n\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}x \mod p^{(n+1)\left(\mathrm{ord}_p \frac{F(\alpha_1)}{F'(\alpha_1)}\right)}$$

or equivalently,

$$0 \equiv y + F'(\alpha_n)x \mod p^{\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1))}.$$

Since $F'(\alpha_n) \neq 0 \mod p^{\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1))}$, we can set

$$x = \frac{y}{F'(\alpha_n)} \mod p^{\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1))}.$$

We found $\alpha_{n+1} \in \mathbb{Z}_p$ such that $\alpha_{n+1} \equiv \alpha_n \mod p^{n(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}$ and $F(\alpha_{n+1}) \equiv 0 \mod p^{(n+1)(\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1)))}$.

We found a Cauchy sequence (α_n) in $\mathbb{Q}_p$. Because $\mathbb{Q}_p$ is complete, there exists a limit. We set $\alpha = \lim \alpha_n$. Then $\alpha \equiv \alpha_1 \mod p^{\mathrm{ord}_p(F(\alpha_1))-\mathrm{ord}_p(F'(\alpha_1))}$ by construction and the continuity gives us $F(\alpha) = 0$. □

Chapter 4

Local and Global

The aim of the thesis is to use the theory of p-adic numbers in search of integer or rational solutions of equations that have integer coeficients.

For an equation to have a solution in $\mathbb{Z}$ or $\mathbb{Q}$, necessarily it needs to have a solution modulo p for all the primes p.

Example 4.1.

$$F(X) = X^3 - 2X + 17$$

does not have a solution modulo 5 *for* $F(X) = 0$*:*

$$F(X) \equiv X^3 + 3X + 2 \mod 5.$$

Trying out the numbers $0, 1, 2, 3, 4$ *shows that we cannot get the* 0*. If there was an* $x_0 \in \mathbb{Z}$ *that* $F(x_0) = 0$*, then necessarily also* $F(x_0)$ *modulo* 5 *would equal zero.*

Then we can move one level higher and try to find a solution that holds modulo p^i for all $i \in \mathbb{N}$ at once.

Here comes an example of a Diophantine equation, where the approach of proving the non-existence of a local solution to reject the existence of a global solution is used.

Example 4.2.

$$F(X, Y, Z) = 3X^2 + 2Y^2 - Z^2 = 0$$

This equation does not have a solution in $\mathbb{Q}_3$*. If there existed a solution* $(x, y, z) \in \mathbb{Q}_3^3$*, then we could multiply it through by a convenient power of 3 to obtain a solution* $(x', y', z') \in \mathbb{Z}_3^3$*, where at least one of* x_1, y_1, z_1 *is not in* $3\mathbb{Z}_3$*. So we have*

$$x' = \sum_{i=0}^{\infty} x_i 3^i,$$

$$y' = \sum_{i=0}^{\infty} y_i 3^i,$$

$$z' = \sum_{i=0}^{\infty} z_i 3^i.$$

We set this into our equation

$$0 = \sum_{n=0}^{\infty} 3^{n+1} \sum_{i=0}^{n} x_i x_{n-i} + \sum_{n=0}^{\infty} 2 \cdot 3^n \sum_{i=0}^{n} y_i y_{n-i} - \sum_{n=0}^{\infty} 3^n \sum_{i=0}^{n} z_i z_{n-i}$$

then we check the equation modulo 3^2*:*

$$0 \equiv 3(x_0+3x_1)^2+2(y_0+3z_1)^2-(z_0+3z_1)^2 \equiv 3x_0^2+3y_0y_1+2y_0^2-z_0^2-6z_0z_1 \mod 9.$$

Since

$$2y_0^2 - z_0^2 \equiv 0 \mod 3,$$

We have $y_0, z_0 = 0$*. Then* $3x_0^2 \equiv 0$ *modulo* 9 *and* $x_0 = 0$*. Then all* x_0, y_0, z_0 *are zero and all* $x', y', z' \in 3\mathbb{Z}_3$*, which is a contradiction with the assumption.*

If an equation has a solution in $\mathbb{Q}$, then necessarily it needs to have a solution in $\mathbb{Q}_p$ for all $2 \leq p \leq \infty$ (here we use the convention $\mathbb{Q}_\infty = \mathbb{R}$). Therefore, given an equation, if we can find such p that there is no solution in $\mathbb{Q}_p$, we know that neither there is one in $\mathbb{Q}$.

In other words, the non-existence of a local solution in some $\mathbb{Q}_p$ yields the non-existence of a global solution (in $\mathbb{Q}$). It would be great, if we could prove the opposite: The existence of a local solution in $\mathbb{Q}_p$ for all p yields the existence of a global solution in $\mathbb{Q}$. Unfortunatelly, we cannot. This statement is not true in general. Here is a counterexample:

Example 4.3.

$$F(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

We will show that this equation has a solution in $\mathbb{Q}_p$ *for all* p*, but does not have a solution in* $\mathbb{Q}$*. We have*

$$F'(X) = 2X((X^2 - 2)(X^2 - 17) + (X^2 - 2)(X^2 - 34) + (X^2 - 17)(X^2 - 34))$$

Let p *be a prime,* $p \neq 2, 17$*. If* 2 *is a square modulo* p*, then there exists* $a \in \{1, ..., p-1\} : a^2 \equiv 2$ *modulo* p*. If* 17 *is a square modulo* p*, then there exists* $a \in \{1, ..., p-1\} : a^2 \equiv 17$ *modulo* p*. If neither* 2 *nor* 17 *is a quadratic residue modulo* p *then necessarily their product* 34 *is, i.e, there exists* $a \in \{1, ..., p-1\} : a^2 \equiv 34$

mod p. *One of these a's does exist and is a non-trivial solution to* $F(X) \equiv 0$ *modulo* p. *Let* $a^2 \equiv 2 \equiv 17$ *modulo* p. *Then either* $p = 3$ *or* $p = 5$, *but neither for* $p = 3$ *nor for* $p = 5$ *is 2 a quadratic residue, so* a^2 *cannot be congruent both with 2 and 17. Also* $a^2 \equiv 2 \equiv 34$ *cannot happen, because 32 is not congruent to zero modulo* $p \neq 2$. *Similarly,* $a^2 \equiv 17 \equiv 34$ *implies 17 is congruent to zero modulo* $p \neq 17$, *which is impossible. We have shown that* a^2 *is congruent to at most one of the numbers 2,17,34. This gives us* $F'(a) \neq 0$ *modulo* p. *We found an* $a \in \{1, ..., p-1\} : F(a) \equiv 0$ *modulo* p *and* $F'(a) \neq 0$ *modulo* p. *The first version of Hensel's Lemma assures us of the existence of a solution in* $\mathbb{Q}_p$.

Now let $p = 2$. *We have that* $F(17) \equiv 0$ *modulo* 2^4, *so* $|F(17)|_p = 2^{-4}$. *We calculate* $F'(17)$:

$$F'(17) = 2 \cdot 17(287 \cdot 272 + 287 \cdot 255 + 272 \cdot 255) \neq 0 \mod 2^2,$$

so $|F'(17)|_p = 2^{-1}$. *We have*

$$|F(17)|_p = 2^{-4} < 2^{-2} = |F'(17)|_p^2.$$

Second version of Hensel's Lemma says that there exists $\alpha \in \mathbb{Z}_p$, $\alpha \equiv 17$ *modulo* $2^{4-1} = 8$, *such that* $F(\alpha) = 0$.

Now let $p = 17$. *We set* $a = 6$. *Then*

$$F(6) = (36-2)(36-17)(36-34) \equiv 0 \mod 17$$

$$F'(6) = 12(36-17)(36-34) \equiv 14 \neq 0 \mod 17$$

Hensel's lemma yields that there is a solution in $\mathbb{Q}_{17}$ *of* $F(X) = 0$.

Let $p = \infty$. *For instance* $x_0 = \sqrt{2} \in \mathbb{R}$ *is a solution.*

We found a solution of $F(X) = 0$ *in* $\mathbb{Q}_p$ *for every prime* p *and also for* $p = \infty$. *However, there is not a solution in* $\mathbb{Q}$, *because none of the numbers* $2, 17, 34$ *is a square in* $\mathbb{Q}$.

The existence of all the local solutions did not serve us in this case. However, there are certain classes of equations, where the existence of all the local solutions is a sufficient condition for an existence of a global solution, as explained in the next section.

4.1 Hasse-Minkowski Theorem

Theorem 4.4 (Hasse-Minkowski)**.** *Let* $F(X_1, X_2, ..., X_n) \in \mathbb{Q}[X_1, X_2, ..., X_n]$ *be a homogeneous polynomial of degree 2 in n variables. The equation*

$$F(X_1, X_2, ..., X_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ *and hence in* $\mathbb{Z}$ *if and only if it has non-trivial solutions in* $\mathbb{Q}_p$ *and hence in* $\mathbb{Z}_p$*, for every prime* $p \leq \infty$*, where* $\mathbb{Q}_\infty = \mathbb{R}$*.*

The proof of the theorem can be found in Serre[5].

The theorem gives us a sufficient condition for the existence of all local solutions to assure us of the existence of a global solution.

Chapter 5

Aplication of Hasse-Minkowski theorem

We have the Hasse–Minkowski theorem that gives us quite good directions on what to do in order to determine the existence of a solution in $\mathbb{Q}$, but when we are standing in front of a particular homogeneous polynomial of degree 2, there is still a lot of work to be done checking the existence of a solution in $\mathbb{Q}_p$ for all the primes p. In this chapter we will restrict the homogeneous polynomial of degree 2 to three variables and we will construct a list of simple conditions to be checked, that will tell us, whether there exists a solution in $\mathbb{Q}$.

We know from Linear Algebra that for a homogeneous polynomial of degree 2 in three variables $F(X,Y,Z) = aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ$, with $a, ..., f \in \mathbb{Z}$ we can find a convenient substitution for X, Y, Z, $X' = uX + vY + wZ$,... such that $F'(X', Y', Z') = a'X'^2 + b'Y'^2 + c'Z'^2$ is diagonal, $a', b', c' \in \mathbb{Q}$. Then we can multiply F' through by the denominators of a', b', c' and we get $F'' = a''X'^2 + b''Y'^2 + c''Z'^2$, where $a'', b'', c'' \in \mathbb{Z}$ and F'' has exactly the same set of solutions like F'. We have shown that determining the existence of a solution of a homogeneous polynomial equation of degree 2 in three variables is equivalent to determining the existence of a solution of $F = aX^2 + bY^2 + cZ^2$.

When does the equation

$$aX^2 + bY^2 + cZ^2 = 0 \tag{5.1}$$

with $a, b, c \in \mathbb{Q}$, have a non-trivial solution in $\mathbb{Q}$?

This is a nice quadratic form, so we are going to try to apply the Hasse-Minkowski theorem. We need to look for solutions in $\mathbb{Q}_p$ for all primes $p, 2 \leq p \leq \infty$.

5.1 $p = \infty$

Let us first have a look at $p = \infty$. We want to determine when does (5.1) have a solution in $\mathbb{Q}_p = \mathbb{R}$. This is obviously if and only if a, b, c do not all have the same signs.

5.2 $p < \infty$

For $p < \infty$ it will be useful to make a few assumptions first.

(i) We can assume that $a, b, c \in \mathbb{Z}$. If not, we could multiply the equation by their denominators.

(ii) We can assume that a, b, c are square-free.

Let's say that $a = a_1 m^2$. Then (x_0, y_0, z_0), the solution of (5.1) corresponds to (mx_0, y_0, z_0), the solution of

$$a_1 X^2 + bY^2 + cZ^2 = 0,$$

where a_1, b, c are square-free. Also, if (mx_0, y_0, z_0) is a solution to $a'X^2 + b'Y^2 + c'Z^2 = 0$, then (x_0, y_0, z_0) is a solution to $a'm^2X^2 + b'Y^2 + c'Z^2 = 0$.

(iii) Without the loss of generality, we can assume that $gcd(a, b, c) = 1$.

If it was not so and $gcd(a, b, c) = k \neq 1$, we could divide the equation by k and all the previous solutions would still hold.

(iv) But we can go further, assuming that a, b, c are pairwise coprime.

If they were not, i.e. $gcd(a, b) = l \neq 1, l \nmid c, l$ is square-free, and there existed a solution (x_0, y_0, z_0) to (5.1), we would get

$$a_1 l x_0^2 + b_1 l y_0^2 + c z_0^2 = 0.$$

We see that l must divide the last term. Since $l \nmid c, l$ must divide z_0^2. Since l is square-free, $l | z_0$. $(x_0, y_0, \frac{z_0}{l})$ is a solution to

$$a_1 X^2 + b_1 Y^2 + clZ^2 = 0.$$

Also, if (x_0, y_0, z_0) is a solution to $aX^2 + bY^2 + clZ^2 = 0$, then $(x_0, y_0, z_0 l)$ is a solution to $alX^2 + blY^2 + cZ^2 = 0$.

If at least one of the numbers a, b, c is equal to zero, say $a = 0$, we have the obvious non-trivial solution $(t, 0, 0)$, $t \in \mathbb{Q}$.

Let me make a little resume of where we are. We have an equation

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

where $a, b, c \in \mathbb{Z}-\{0\}$ are square-free relativelly prime numbers and we are looking for a solution $(x_0, y_0, z_0) \in \mathbb{Q}_p$, for $2 \leq p < \infty$.

Let $p \neq 2, \infty$ be a prime. We are going to look for a solution $(x_0, y_0, z_0) \in \mathbb{Z}/p\mathbb{Z}$ of the equation

$$aX^2 + bY^2 + cZ^2 \equiv 0, \mod p.$$

One of the solutions would be the trivial one $(0, 0, 0)$. We're going to prove that there is more. From Fermat's Little Theorem it follows that

$$(aX^2 + bY^2 + cZ^2)^{p-1} \equiv \begin{cases} 1 \mod p, \text{ if } (x, y, z) \text{ is not a solution,} \\ 0 \mod p, \text{ if } (x, y, z) \text{ is a solution.} \end{cases}$$

We put N the number of solutions in $\mathbb{Z}/p\mathbb{Z}$. Then

$$N \equiv p^3 - \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \sum_{z=0}^{p-1} (aX^2 + bY^2 + cZ^2)^{p-1} \mod p.$$

The sums may be expanded into

$$N \equiv p^3 - \sum_{x} \sum_{y} \sum_{z} \sum_{i+j+k=p-1} \frac{(p-1)!}{i!j!k!} a^i b^j c^k X^{2i} Y^{2j} Z^{2k}$$

Note that one of the $2i, 2j, 2k$ is always less than $p-1$. We can rewrite N as

$$N \equiv p^3 - \sum_{i+j+k=p-1} \frac{(p-1)!}{i!j!k!} a^i b^j c^k \sum_{x} x^{2i} \sum_{y} y^{2j} \sum_{z} z^{2k}$$

Here we make use of the following lemma.

Lemma 5.1. *For all $n \in 1, ..., p-1$, p prime, we have*

$$\sum_{k=0}^{p-1} k^n \equiv 0 \mod p.$$

Proof. Let a be some generator of the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Then $a^n \neq 1$ modulo p, since $n < p-1$. The map

$$\begin{aligned} \phi : \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ k &\mapsto ak \text{ is bijective.} \end{aligned}$$

Then

$$\sum_{k=0}^{p-1}(ak)^n \equiv \sum_{k=0}^{p-1} k^n$$

and

$$(a^n - 1)\sum_{k=0}^{p-1} k^n \equiv 0 \mod p,$$

which leads to $\sum_{k=0}^{p-1} k^n \equiv 0$ modulo p. □

We see that the inner part of the sum is always congruent to 0 modulo p. Therefore, $N \equiv 0$ modulo p, i.e. $N = kp$, for some $0 \leq k \in \mathbb{Z}$. But we already know that $k \neq 0$, since $(0, 0, 0)$ is a solution. Then, there must exist at least $p-1$ non-trivial solutions to the equation

$$aX^2 + bY^2 + cZ^2 \equiv 0, \mod p.$$

Now it's the time to use Hensel's lemma. Let (x_0, y_0, z_0) be a non-trivial solution to (5.1). Say $x_0 \neq 0$. We take $F(X) = aX^2 + by_0^2 + cz_0^2$. Then

$$F(x_0) \equiv 0 \mod p$$

$$\text{and } F'(x_0) = 2ax_0 \neq 0 \mod p$$

as long as we reject the case $p|a$. Then, according to the First version of Hensel's lemma, there exists such $x_1 \equiv x_0$ modulo p that $F(x_1) = 0$. Then $(x_1, y_0, z_0) \in \mathbb{Q}_p$ is a solution to (5.1).

Now we have to deal with the cases $p|a$ (or b or c) and $p = 2$.

5.3 $p = 2 \nmid a, b, c$

Suppose $p = 2$ and a, b, c are all odd. If (x_0, y_0, z_0) is a solution to our equation, we can assume that they are all in $\mathbb{Z}_p$ and not all of them in $2\mathbb{Z}_p$. If it was not so, we could divide them all by a convenient power of 2 and the result would still be a solution. So

$$aX^2 + bY^2 + cZ^2 \equiv X^2 + Y^2 + Z^2 \equiv 0 \mod 2$$

Since x_0, y_0, z_0 cannot all be $\equiv 0$ modulo 2, we see that two of them, say y_0, z_0 are odd. We know that for $\alpha \in 1 + 2\mathbb{Z}_2$, we have $\alpha^2 \in 1 + 8\mathbb{Z}_2$:

$$\begin{aligned} \alpha &= 1 + 2a_1 + 4a_2 + ... \\ \alpha^2 &= 1 + 4a_1 + 8a_2 + 4a_1^2 + 16a_1a_2 + 16a_2^2 + ... \equiv 1 \mod 8 \end{aligned}$$

We have

$$0 \equiv ax_0^2 + by_0^2 + cz_0^2 \equiv b + c \mod 4.$$

So in order for (x_0, y_0, z_0) to be a solution, necessarily sum of two of a, b, c must be congruent to zero modulo 4.

We will show that this a sufficient condition. We would like to use the Hensel's lemma, but this time it will not be that easy, because the derivative is divisible by two. We will try to fit it to the Second version of the Lemma. We want to find an initial solution (x_0, y_0, z_0), such that

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \mod 8.$$

Let $b + c \equiv 0$ modulo 4. Then either $b + c \equiv 0$ modulo 8 and $(0, 1, 1)$ is a solution modulo 8, or $b + c \equiv 4$ modulo 8 and setting $(x_0, y_0, z_0) = (2, 1, 1)$, we get

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 4a + b + c \equiv 4a + 4 \mod 8.$$

Since a is odd, this is congruent to 0 modulo 8 and we are good. We take $F(Y) = ax_0^2 + bY^2 + cz_0^2$, then $F'(Y) = 2bY$ and

$$|F(y_0)|_2 \leq p^{-3} < p^{-2} = |F'(y_0)|_2^2,$$

because y_0, b are odd. Hensel's Lemma yields that there exists a solution in $\mathbb{Q}_2$. We have that for $p = 2$ and $a, b, c \in \mathbb{Z}$ all odd, there exists a solution $(x_1, y_1, z_1) \in \mathbb{Q}_2$ to (5.1) if and only if the sum of two of a, b, c is congruent to 0 modulo 4.

5.4 $2 = p|a$

Suppose now that $p = 2$ and p divides one of a, b, c, say $p|a$, i.e. $a = 2a_1$. As a is square-free and a, b, c are pairwise coprime, a_1, b, c are all odd. Let (x_0, y_0, z_0) be a solution to (5.1). Again, we may suppose that $x_0, y_0, z_0 \in \mathbb{Z}_2$ are not all in $2\mathbb{Z}_2$. If

$$x_0 \in 1 + 2\mathbb{Z}_2 \;\Rightarrow\; x_0^2 \in 1 + 8\mathbb{Z}_2$$

then y_0, z_0 must be either both in $2\mathbb{Z}_2$ or both in $1 + 2\mathbb{Z}_2$, otherwise the equation would not have a solution modulo 2. If $y_0, z_0 \in 2\mathbb{Z}_2$, then $y_0^2, z_0^2 \in 4\mathbb{Z}_2$, so

$$0 \equiv 2a_1x_0^2 + by_0^2 + cz_0^2 \equiv 2a_1 + 4(b + c) \mod 8,$$

which cannot be true, so y_0, z_0 are both in $1 + 2\mathbb{Z}_2$ and

$$0 \equiv 2a_1x_0^2 + by_0^2 + cz_0^2 \equiv 2a_1 + b + c \mod 8,$$

therefore, $a + b + c \equiv 0$ modulo 8.

If $x_0 \notin 1 + 2\mathbb{Z}_2$, we have

$$x_0 \in 2\mathbb{Z}_2 \ \Rightarrow \ x_0^2 \in 4\mathbb{Z}_2.$$

Then necessarily both $y_0, z_0 \in 1 + 2\mathbb{Z}_2$.So

$$0 \equiv 2a_1x_0^2 + by_0^2 + cz_0^2 \equiv b + c \mod 8.$$

We conclude that in order for (x_0, y_0, z_0) to be a solution, either sum of two or sum of three of a, b, c must be congruent to zero modulo 8.

Again, we will make this a sufficient condition for a solution to exist. Again, we need to find a solution of

$$2a_1x_0^2 + by_0^2 + cz_0^2 \equiv 0 \mod 8,$$

If $a + b + c \equiv 0$ modulo 8, then $(1, 1, 1)$ is a solution. If $b + c \equiv 0$ modulo 8, then $(0, 1, 1)$ is a solution. We found a non-trivial solution to an equation $2a_1x_0^2 + by_0^2 + cz_0^2 \equiv 0$ modulo 8. We take $F(Y) = ax_0^2 + bY^2 + cz_0^2$. Then

$$|F(1)|_2 \leq 2^{-3} < 2^{-2} = |F'(1)|_2^2.$$

The Second version of Hensel's lemma assures us that there is a solution $x_1, y_1, z_1 \in \mathbb{Q}_2$ to (5.1). The necessary condition is sufficient.

5.5 $p|a$

Suppose that $p \neq 2$ and $a = pa_1$, a, b, c are pairwise relatively prime, (x_0, y_0, z_0) is a non-trivial solution to

$$aX^2 + bY^2 + cZ^2 \equiv 0 \mod p, \text{ so}$$

$$pa_1x_0^2 + by_0^2 + cz_0^2 \equiv by_0^2 + cz_0^2 \equiv 0 \mod p$$

If $p \nmid y_0$, then $b + c\frac{z_0^2}{y_0^2} \equiv 0$ modulo p. It follows that there exists such $r \in \{1, ...p-1\}$ that $b + cr^2 \equiv 0$ modulo p. If $y_0 = kp$, for some $k \in \mathbb{Z}$, then $by_0^2 + cz_0^2 \equiv cz_0^2 \equiv 0$ modulo p and then necessarily $p|c$ and $p|b$, we set $r = 1$ and $b + c \equiv 0$ modulo p. (If $p|z_0$, we would have $p|x_0$ and the solution would be trivial.)

Sufficiency of this condition follows. If $b + cr^2 \equiv 0$ modulo p, then $(0, 1, r)$ is a solution to $aX^2 + bY^2 + cZ^2 \equiv 0$ modulo p. We put

$$F(Y) = bY^2 + cr^2$$

We have $F \equiv 0$ modulo p and $F'(1) = 2b \neq 0$ modulo p. According to the first version of Hensel's Lemma, there exists a $y_1 \in \mathbb{Q}_p$ such that $F(y_1) = 0$ and $(0, y_1, r)$ is a non-trivial solution to (5.1) in $\mathbb{Q}_p$.

5.6 Conclusion

It's time to put all the information collected together and state the conditions, when (5.1) has a non-trivial solution in $\mathbb{Q}_p$ for every p, hence from Hasse-Minkowski theorem, there is a non-trivial solution in $\mathbb{Q}$.

Proposition 5.2. *Let a, b, c be pairwise relatively prime integers that are square-free. Then the equation*

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

has a solution in $\mathbb{Q}$ if and only if all of the following is satisfied:

(1) Not all a, b, c have the same sign.

(2) If $2 \nmid abc$, then either $a + b$ or $b + c$ or $a + c$ is divisible by 4.

(3) If $2|a$, then either $b + c$ or $a + b + c$ is divisible by 8. (Similarly, if $2|b, c$.)

(4) For all odd primes, such that $p|a$, there exists $r \in \{1, ...p - 1\}$, such that $b + cr^2 \equiv 0 \mod p$. (Similarly, if $p|b, c$.)

Checking these four conditions is obviously way more simple than checking the existence of a solution in $\mathbb{Q}_p$ for all the primes p.

Example 5.3.

$$F(X, Y, Z) = 5X^2 + 7Y^2 - 13Z^2$$

Does the equation have a solution for $F(X, Y, Z) = 0$ *in* $\mathbb{Q}$*? We need to check that all the conditions of the proposition are satisfied. Obviously (1) and (3) are. Then a+b=5+7=12 is divisible by 4, which satisfies (2). We need to check (4) for* $p = 5, 7, 13$.

$$\begin{aligned} 7 - 3r^2 &\equiv 0 \mod 5 \text{ for } r = 2, \\ 5 - 13r^2 &\equiv 0 \mod 7 \text{ for } r = 3, \\ 5 + 7r^2 &\equiv 0 \mod 13 \text{ for } r = 4, \end{aligned}$$

According to the proposition, there exists a solution to this equation in $\mathbb{Q}$.

As we can see, the proposition really *did* save us a lot of work.

Bibliography

[1] J. W. S. Cassels: *Lectures on Elliptic Curves*, Cambridge University Press, 1991, Chapter 2, 11.

[2] F. Q. Gouvêa: *p-adic Numbers, An Introduction*, Springer-Verlag, 1993.

[3] S. B. Cooper: *Computability Theory*, Chapman and Hall/CRC, 2004, p. 98.

[4] Y. V. Matiysevic: *Hilbert's tenth problem*, Massachusetts Institute of Technology, 1993, p. xix.

[5] J.-P. Serre: *A Course in Arithmetic* , Springer-Verlag, Berlin, 1973.