UNIVERSITA' DEGLI STUDI DI NAPOLI

"FEDERICO II"

Dipartimento di Matematica e Applicazioni

"Renato Caccioppoli"

Dottorato di Ricerca in
Scienze Matematiche
XXV Ciclo

Legendre's Theorem in $I\Delta_0+\Omega_1$

Michele Bovenzi

Tutor
Ch.mo Prof. Paola D'Aquino

Coordinatore
Ch.mo Prof. Francesco de Giovanni

Legendre's Theorem in $I\Delta_0 + \Omega_1$

Michele Bovenzi

Contents

Acknowledgements

Many people helped me in completing my Ph.D. and I would like to express my sincere gratitude to them.

I am really grateful to my supervisor Professor Paola D'Aquino, for her constant availability to provide help, guidance and teachings during the entire period of my Ph.D. I would also like to thank Professor Angus Macintyre for the enlightening conversations we had.

A special thank goes to my family: even though they couldn't help me about the mathematical aspect of my work (fortunately...), they already help me a lot by always being there for me, and this means very much!

I would also like to thank my girlfriend Antonella, who always incited me into keeping up this career and following my inclinations, which are quite variable from day to day, I admit. And sometimes she helped me with maths too!

I sincerely thank my superiors at the Ministry of Foreign Affairs where I work, Dott.ssa Maria Teresa Di Maio and Ing. Antonio Casaretta, who promptly supported my request of a part-time work and encouraged me to complete my Ph.D.

Finally, I would like to thank all my Friends who made the (little, actually...) spare time I had really joyful.

Introduction

There has been a lot of work in Model Theory on *weak fragments of Peano Arithmetic*. These theories are obtained by *some sort of restrictions* on the usual set of axioms of Peano Arithmetic. One of the central object of research in this area is to determine the *mathematical strength* of such theories. To this end, some classical results of elementary Number Theory have been examined in order to prove their validity in such weak theories.

The weak fragment we are interested in is the theory usually denoted by $I\Delta_0+\Omega_1$: $I\Delta_0$ is the subtheory of Peano Arithmetic in which induction is restricted to $\Delta_0 - formulas$, i.e. formulas where all quantifiers are bounded by terms of the language, and Ω_1 is an axiom stating the totality of the function $x^{log_2 y}$.

Both theories $I\Delta_0$ and $I\Delta_0 + \Omega_1$ are strictly related to complexity theory and many open problems in such theories have complexity-theoretical counterparts. For example it is still open the problem of proving the *MRDP*-theorem (asserting that every Σ_1-formula is equivalent to an existential formula in $I\Delta_0$). This theorem led to the negative solution of Hilbert 10th problem, and if proved in $I\Delta_0$ or $I\Delta_0 + \Omega_1$, it would give a positive solution to the well known open problem $NP \stackrel{?}{=} coNP$.

It is known that the majority of classical results of elementary number theory, such as unboundedness of primes, Lagrange's four squares theorem or quadratic reciprocity law, are provable in $I\Delta_0 + exp$, exp being the axiom asserting the totality of the exponential function 2^x. Moreover, in many cases these results are provable with an *adaptation*, in $I\Delta_0$, of classical number-theoretical arguments in $I\Delta_0 + exp$.

Contrary to the well known mathematical strength of $I\Delta_0 + exp$, very little is known about $I\Delta_0$, or other *intermediate* subtheories of $I\Delta_0 + exp$. For example, all the results mentioned above are not known to be provable in $I\Delta_0$. On the other hand, Woods in [Wo] proved unboundedness of primes in the theory $I\Delta_0 + \Delta_0 PHP$, where $\Delta_0 PHP$ is an axiom scheme expressing a Δ_0-version of the *Pigeonhole Principle*. Actually, in [P-W-W] it is shown that a weaker version of such principle (Δ_0-$WPHP$) is enough to prove unboundedness of primes. Always in [P-W-W] the authors proved that such Δ_0-$WPHP$ is provable in $I\Delta_0 + \Omega_1$. Hence in the theory $I\Delta_0 + \Omega_1$ unboundedness of primes holds.

In this setting we have analyzed a classical theorem due to Legendre, about the existence of non trivial integral solutions of certain quadratic equations in three variables. The proof we have considered follows the lines of the corresponding theorem given in [I-R]. Our contribution has involved a careful analysis of the objects used in the proof. In particular, we have found Δ_0-formula defining all the objects and tools involved in the proof, ensuring their validity in our theory. We have finally obtained estimates on the growth rate of the solution of the considered equations, of polynomial size in $x^{log_2 y}$, hence proving the main theorem in $I\Delta_0 + \Omega_1$.

Chapter 1

Weak fragments of Peano Arithmetic

1.1 Peano Arithmetic and Weak Fragments

Throughout this work we will assume some very basic knowledges of *Logic, Model Theory, Algebra and Number Theory*. The reader may refer, among others, to [Mar], [F-dG], [H-W] and [K] for further details that we shall omit, and for some basic definitions and properties.

We will consider the first-order language $\mathcal{L}$ of arithmetic, consisting of the symbols $+, \cdot, <, 0, 1$. We denote by PA^- the following (finite) set of axioms, that are clearly true for the set $\mathbb{N}$ of natural numbers:

$$
\begin{aligned}
\forall x \forall y \forall z \quad & (x + y) + z = x + (y + z) \\
\forall x \forall y \quad & x + y = y + x \\
\forall x \forall y \forall z \quad & (x \cdot y) \cdot z = x \cdot (y \cdot z) \\
\forall x \forall y \quad & x \cdot y = y \cdot x \\
\forall x \quad & (x + 0 = x) \wedge (x \cdot 0 = 0) \\
\forall x \quad & (x \cdot 1 = x) \\
\forall x \forall y \forall z \quad & (x + y) \cdot z = x \cdot z + y \cdot z
\end{aligned}
$$

$$
\begin{aligned}
\forall x \forall y \forall z \quad & (x < y \wedge y < z) \rightarrow x < z \\
\forall x \quad & \neg(x < x) \\
\forall x \forall y \quad & x < y \vee y < x \vee x = y \\
\forall x \forall y \forall z \quad & x < y \rightarrow (x + z < y + z) \\
\forall x \forall y \forall z \quad & (0 < z \wedge x < y) \rightarrow x \cdot z < y \cdot z \\
\forall x \quad & x = 0 \vee 0 < x \\
0 < 1 \wedge \forall x \quad & 0 < x \rightarrow (1 < x \vee x = 1) \\
\forall x \forall y \quad & x < y \rightarrow \exists z (0 < z \wedge \ x + z = y).
\end{aligned}
$$

The theory of *Peano Arithmetic* (PA) is obtained by adding to the set PA^- the following (infinite) axiom scheme of *mathematical induction*:

$$\forall \bar{y}(\theta(0, \bar{y}) \wedge \forall x \ (\theta(x, \bar{y}) \rightarrow \theta(x + 1, \bar{y})) \rightarrow \forall x \theta(x, \bar{y})),$$

where $\theta(x, \bar{y})$ runs through all formulas of the language $\mathcal{L}$ (here and in what follows we denote by $\bar{y}$ any n-tuple $(y_1, \ldots, y_n)$, for n a positive integer).

The theory PA is appropriate to describe and "talk about" classical number theory, i.e. the arithmetic of natural numbers. In fact, all proofs of classical results in number theory, as in [H-W], can be reproduced in this setting.

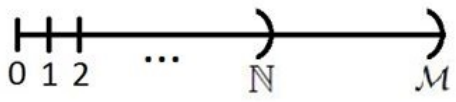
It is clear that $\mathbb{N}$ is a model of PA^- and of PA, and we will refer to it as the *standard model*. Using a simple compactness argument, the existence of models of PA^- different from $\mathbb{N}$ and not isomorphic to it is easily obtained. We will refer to these as the *non-standard* models.

We recall that if $\mathcal{M}, \mathcal{N}$ are $\mathcal{L}$-structures and $\mathcal{N} \subseteq \mathcal{M}$, then we say that $\mathcal{N}$ is an *initial segment* of $\mathcal{M}$, if for all $x \in \mathcal{N}$ and $y \in \mathcal{M}$, if $\mathcal{M} \models y < x$, then $y \in \mathcal{N}$. Moreover, an initial fragment $\mathcal{N}$ of $\mathcal{M}$ is said to be *proper* if $\mathcal{N} \neq \mathcal{M}$.

From the axioms the following property of models of PA^- is easily proved (see also [K]).

Theorem 1.1.1 *Let $\mathcal{M} \models PA^-$. Then there is an embedding of $\mathcal{L}$-structures sending $\mathbb{N}$ onto an initial segment of $\mathcal{M}$.*

Theorem 1.1.1 allows us to identify $\mathbb{N}$ with the smallest initial segment of any model $\mathcal{M}$ of PA^-. Hence we can represent the structure of any model of PA^- as follows,



When $\mathbb{N}$ is a proper initial segment of $\mathcal{M}$, then $\mathbb{N} \ncong \mathcal{M}$. Any element in $\mathcal{M} \setminus \mathbb{N}$ is also called *non-standard*.

There are models of PA^- of any infinite cardinality, which are clearly not isomorphic to $\mathbb{N}$. This is a consequence of the following basic theorem in Model Theory.

Theorem 1.1.2 (Upward Löwenheim-Skolem Theorem) *Let $\mathcal{L}$ be a first-order language of cardinality at most $\lambda \geq \aleph_0$, and let $\mathcal{M}$ be an $\mathcal{L}$-structure. If κ is a cardinal with $\lambda \leq card(\mathcal{M}) \leq \kappa$, then there is a proper elementary extension $\mathcal{N}$ of $\mathcal{M}$ with $card(\mathcal{N}) = \kappa$.*

By restricting the induction scheme to various classes of formulas we obtain subsystems of PA which are usually called *fragments*. All formulas of the language $\mathcal{L}$ can

be arranged in the following classes, of different complexity:

$$\begin{aligned}
E_0 = U_0 = \exists_0 = \forall_0 = &\ \{\phi(\bar{x}) \ : \ \phi \text{ is quantifier-free}\},\\
\exists_{n+1} = &\ \{\exists \bar{y}\ \phi(\bar{x},\bar{y}) \ : \ \phi \in \forall_n\},\\
\forall_{n+1} = &\ \{\forall \bar{y}\ \phi(\bar{x},\bar{y}) \ : \ \phi \in \exists_n\},\\
E_{n+1} = &\ \{\exists \bar{y} \leq t(\bar{x})\ \phi(\bar{x},\bar{y}) \ : \ \phi \in U_n,\ t \text{ a term of } \mathcal{L}\},\\
U_{n+1} = &\ \{\forall \bar{y} \leq t(\bar{x})\ \phi(\bar{x},\bar{y}) \ : \ \phi \in E_n,\ t \text{ a term of } \mathcal{L}\},\\
\Delta_0 = \Sigma_0 = \Pi_0 = &\ \bigcup_{n\in\mathbb{N}} E_n = \bigcup_{n\in\mathbb{N}} U_n,\\
\Sigma_{n+1} = &\ \{\exists \bar{y}\ \phi(\bar{x},\bar{y}) \ : \ \phi \in \Pi_n\},\\
\Pi_{n+1} = &\ \{\forall \bar{y}\ \phi(\bar{x},\bar{y}) \ : \ \phi \in \Sigma_n\}.
\end{aligned}$$

If $\mathcal{C}$ is any of the classes of formulas $\Delta_0, U_n, E_n, \Pi_n, \Sigma_n, \forall_n, \exists_n$, and we restrict induction to be applied only on to $\mathcal{C}$, we get the weak fragment of PA which is denoted by $I\mathcal{C}$. In particular, the *weakest* of these fragments of PA is the theory of IE_0, or *Open Induction* (also denoted by $IOpen$), where induction is only allowed on open formulas (i.e. formulas with no quantifiers).

The systems described above have different mathematical strength as we increase the complexity of formulas we are considering. The relation among these systems is the following:

$$IOpen \subset IE_1 \subseteq IE_2 \subseteq \cdots \subseteq I\Delta_0 \subset I\Sigma_1 \subset I\Sigma_2 \subset \cdots \subset PA.$$

Notice that the symbol $\subset$ in the previous sequence denotes that the inclusion between theories has been proved to be strict, while the symbol $\subseteq$ means that it is still unknown whether the inclusion is strict or not.

We already remarked that the set $\mathbb{N}$ of natural numbers is the standard model of PA^- and all fragments $I\mathcal{C}$. Moreover, there is a very intuitive correspondence between models of PA^- and *discretely ordered rings*, which is the same as between $\mathbb{Z}$ and $\mathbb{N}$. Suppose $\mathcal{M} \models PA^-$ and consider the following relation "$\sim$" on $\mathcal{M}^2$

$$(a,b) \sim (c,d) \Leftrightarrow a + d = b + c.$$

It is easy to verify that this is an equivalence relation, so we can consider $\mathcal{R} = \mathcal{M}^2/\sim$ and denote the equivalence class of (a, b) by $[a, b]$. Then if we define the following operations and relation on $\mathcal{R}$

$$[a, b] + [c, d] = [a + c, b + d],$$

$$[a, b] \cdot [c, d] = [ac + bd, bc + ad],$$

$$[a, b] < [c, d] \Leftrightarrow \ a + d < b + c,$$

and interpret 0 and 1 in $\mathcal{R}$ by $[0, 0]$ and $[1, 0]$ respectively, we obtain a discretely ordered ring. The original structure $\mathcal{M}$ is then embedded in this ring via the map $a \ \mapsto [a, 0]$, sending $\mathcal{M}$ onto the set of non-negative elements of $\mathcal{R}$.

Conversely, if $\mathcal{R}$ is a discretely ordered ring and we denote the subset of non-negative elements of $\mathcal{R}$ by $\mathcal{M}$, then $\mathcal{M}$ is a model of PA^-, from which the original ring $\mathcal{R}$ is again obtained if we repeat the construction described above.

Henceforth in what follows, when no confusion arises, we will make no distinction between a model $\mathcal{M}$ of PA (or of any fragment $I\mathcal{C}$) and its associated ring. When we work with the ring, the axiom scheme of induction is clearly intended to be applied to the non-negative part of the ring.

The main interests in these weaker systems lie mainly in the connection these theories have with complexity theory, where number theory plays a central role. Many open problems in theories such as $I\Delta_0$ or $I\Delta_0 + \Omega_1$ (which will be described later) have complexity-theoretic counterparts.

For example, it is still an open problem if $I\Delta_0$ proves the *MRDP*-theorem. This theorem is due to Matijasevic, Robinson, Davis and Putnam and asserts that every recursively enumerable set is existentially definable. Its proof led to the negative solution of the well known Hilbert's 10th problem. The *MRDP*-theorem can be reformulated in $I\Delta_0$ as follows: for every Σ_1-formula $\theta(\bar{x})$ there are polynomials $p(\bar{x}, \bar{y})$ and $q(\bar{x}, \bar{y})$ such that

$$I\Delta_0 \vdash \ \forall \bar{x} \ \left(\theta(\bar{x}) \leftrightarrow \exists \bar{y} \ p(\bar{x}, \bar{y}) = q(\bar{x}, \bar{y})\right).$$

Wilkie (see [W]) observed that a proof of this theorem in $I\Delta_0$ would give a positive solution to the well known problem $NP \stackrel{?}{=} coNP$. This follows from two considerations.

(1) The set $S = \{(a,b,c) \in \mathbb{N}^3 \ : \ \exists x < c \exists y < c \ (ax^2 + by = c)\}$ is NP-complete (see [M-A]).

(2) If $I\Delta_0 \vdash MRDP$-theorem then $\Delta_0^{\mathbb{N}} = E_1^{\mathbb{N}}$, and this implies $S \in NP \cap co\text{-}NP$.

It is also unknown if $I\Delta_0 + \Omega_1$ proves $MRDP$-theorem and, again, a positive answer would give $NP = coNP$.

1.2 Open Induction

As mentioned in the previous section, the *weakest* fragment of PA is the theory *Open Induction*, denoted as $IOpen$, where induction is only allowed on formulas without quantifiers. Models of this theory have been completely characterized (see [S] and [Ot]) as follows:

Proposition 1.2.1 *Let $\mathcal{M}$ be a discretely ordered ring. Then the following are equivalent.*

(1) *$\mathcal{M}$ is a model of $IOpen$;*

(2) *every quantifier-free definable subset of $\mathcal{M}$ is a union of finitely many intervals in $\mathcal{M}$;*

(3) *for every r in $Q(\mathcal{M})$ (the quotient field of $\mathcal{M}$), there is $a \in \mathcal{M}$ such that $|a - r| < 1$ and $Q(\mathcal{M})$ is dense in $RC(\mathcal{M})$, the real closure of $\mathcal{M}$.*

As a consequence it is possible to define the *integer part* $[\alpha]$ of any $\alpha \in RC(\mathcal{M})$ in the usual way as

$$[\alpha] = z \in \mathcal{M} \Leftrightarrow z \leq \alpha < z + 1.$$

In models of $IOpen$ it is also possible to perform Euclidean division and get, for any $x, y \in \mathcal{M} \models IOpen$, $y \neq 0$, that $x = qy + r$ for some $q, r \in \mathcal{M}$ and $0 \leq r < y$.

Notice that in general models of $IOpen$ lack the Euclidean algorithm for determining a greatest common divisor of any pair of elements of $\mathcal{M}$. This is a consequence of the fact that in Bezout rings the notions of *prime* and *irreducible* elements coincide, and this is not the case in models of $IOpen$, as it is shown in [M-M].

Of course, any model of PA, such as $\mathbb{N}$, is also a model of $IOpen$, but this also admits some "pathological" models. There are models of $IOpen$ where the equation $x^2 = 2y^2$ admits non-trivial solutions (see [S]), hence $IOpen$ does not prove irrationality of $\sqrt{2}$. Moreover, there are models of $IOpen$ where the equation $x^n + y^n = z^n$ admits non-trivial solutions for any natural number n, making Fermat's Last Theorem false in $IOpen$.

1.3 Bounded Induction

The theory we are mainly interested in is the fragment of PA denoted by $I\Delta_0$, where induction is allowed only on Δ_0-formulas, i.e. formulas in which all quantifiers are bounded by terms of the language. Hence a typical Δ_0 statement has the form

$$\forall x < t(x, \bar{a})\ \phi(x, \bar{a}),$$

for a formula $\phi(x, \bar{y})$, a term $t(x, \bar{y})$ of the language $\mathcal{L}$, and a n-tuple of parameters $\bar{a}$. Notice that in the language of arithmetic we are using, terms are actually polynomials.

When working in $I\Delta_0$ care must be taken in expressing properties via Δ_0-formulas, since these are the only formulas we can induct on.
For example, we can express in a Δ_0-way the following property:

$$x \text{ divides } y: \ \delta(x, y) = \exists z \leq y\ (xz = y); \tag{1.1}$$

and by Δ_0-induction we can prove that, for every a, b

$$\exists d \leq a\ \exists x < b\ \exists y < a\ (\delta(d, a) \wedge \delta(d, b) \wedge d = ax + by).$$

This implies that any two elements in any model of $I\Delta_0$ have a greatest common divisor, and thus all models of $I\Delta_0$ are Bezout rings. This is enough to state that the following strict inclusion holds:

$$IOpen \subset I\Delta_0. \tag{1.2}$$

We also remark that in the theory $I\Delta_0$ induction can be used to prove that any non empty set which is Δ_0-definable has a minimum element. This will be used in some proofs later.

One of the few known methods of getting models of bounded induction is by taking particular *initial segments* of a model $\mathcal{M}$.

Theorem 1.3.1 *Let $\mathcal{M} \models I\Delta_0$ and let I be an initial segment of $\mathcal{M}$. If I is closed under $+$ and $\cdot$ then $I \models I\Delta_0$.*

As an example, if $\mathcal{M} \models I\Delta_0$ and $a \in \mathcal{M}$, then the set

$$BP(a) = \{x \in \mathcal{M} \ : \ x < a^n, n \in \mathbb{N}\}$$

is an initial segment closed under sum and multiplication, and so $BP(a) \models I\Delta_0$.

A fundamental result for the theory $I\Delta_0$ is due to Parikh (see [Pa]) and it is stated in the following theorem.

Theorem 1.3.2 *Let $\theta(\bar{x}, y)$ be a Δ_0-formula in the language $\mathcal{L}$. If $I\Delta_0 \vdash \forall \bar{x} \exists y \, \theta(\bar{x}, y)$, then $I\Delta_0 \vdash \forall \bar{x} \exists y < t(\bar{x}) \ \theta(\bar{x}, y)$, where $t(\bar{x})$ is a term of $\mathcal{L}$.*

Note that the theorem implies that if a function is Δ_0-definable and provably total in $I\Delta_0$, then the function has polynomial growth.
This is the main limitation of $I\Delta_0$. For example the classical result on the unboundedness of primes is proved using the function $y = \prod_{p \leq x} p$, where p is a prime. This function is expressed by the Δ_0-formula

$$\forall p \leq x \ (Pr(p) \rightarrow (\delta(p, y) \wedge \neg\delta(p^2, x) \wedge \forall p \leq y \ ((Pr(p) \wedge x < p) \rightarrow \neg\delta(p, y)))),$$

where $\delta(x, y)$ is the Δ_0-formula for divisibility (1.1), and $Pr(p)$ is the Δ_0-formula standing for "p is a prime", namely

$$Pr(x) = \forall y \leq x \ (\delta(y, x) \rightarrow (y = 1 \vee y = x)). \tag{1.3}$$

The function $y = \prod_{p \leq x} p$ is of exponential growth, so it is not provably total in $I\Delta_0$. As a consequence, it is still an open problem whether $I\Delta_0$ proves cofinality of primes or not.

If the axiom

$$exp: \ \forall x \exists y \ (y = 2^x)$$

is added to the theory, to guarantee the totality of the exponential function, then in the theory $I\Delta_0 + exp$ cofinality of primes can be proved.

Notice that it is necessary to give a meaning to the function $y = 2^x$ in $I\Delta_0$. This is possible using a Δ_0-formula defining exponentiation, which is due to Paris (see [G-D]) which will be denoted by $E_0(x, y, z)$, where $E_0(x, y, z)$ denotes "$x^y = z$". For any $n \in \mathbb{N}$, $I\Delta_0 \nvdash \forall y \exists z \ E_0(n, y, z)$, hence the function defined by $E_0(x, y, z)$ is not total in $I\Delta_0$. But $I\Delta_0$ proves the following algebraic properties for those elements on which the function is defined.

(i) $\forall x \geq 1 \forall y \forall z_1 \forall z_2 \ (E_0(x, y, z_1) \wedge E_0(x, y, z_2) \rightarrow z_1 = z_2)$

(ii) $\forall x \geq 1 \forall y_1 \forall y_2 \forall z_1 \forall z_2 \ ((E_0(x, y_1, z_1) \wedge E_0(x, y_2, z_2) \rightarrow E_0(x, y_1 + y_2, z_1 z_2))$

(iii) $\forall x \geq 1 \forall y_1 \forall y_2 \forall z_1 \forall z_2 \ ((E_0(x, y_1, z_1) \wedge E_0(z_1, y_2, z_2) \rightarrow E_0(x, y_1 y_2, z_2))$

(iv) $\forall x_1 \geq 1 \forall x_2 \geq 1 \forall y \forall z_1 \forall z_2 \ (E_0(x_1, y, z_1) \wedge E_0(x_2, y, z_2) \wedge z_1 < z_2 \rightarrow x_1 < x_2)$

(v) $\forall x \geq 1 \forall y_1 \forall y_2 \forall z_1 \forall z_2 \ (E_0(x, y_1, z_1) \wedge E_0(x, y_2, z_2) \wedge y_1 < y_2 \rightarrow z_1 < z_2)$.

Moreover, $E_0(x, y, z)$ satisfies the recursion lows for any $x > 1$ on which it is defined, i.e.

(1) $E_0(x, 0, 1)$

(2) $\forall y \forall z\ (E_0(x, y, z) \to E_0(x, y + 1, xz))$

(3) $\forall y \forall z\ (E_0(x, y + 1, z) \to \exists w < z\ (E_0(x, y, w) \wedge z = wx))$.

It can be proved that any other Δ_0-formula satisfying *(1), (2)* and *(3)* is equivalent to $E_0(x, y, z)$ in $I\Delta_0$. Hence Paris' formula gives an invariant meaning to the notion of exponentiation in $I\Delta_0$. So the axiom *exp* stating the totality of exponential function 2^x can actually be expressed as $exp:\ \forall x \exists y\ E_0(2, x, y)$.

The theory $I\Delta_0 + exp$ is strong enough to reproduce cofinality of primes, as well as almost all the results from elementary number theory. In this theory it is usually enough to adapt classical number-theoretical arguments and proofs, so no additional constructive information arise.

On the contrary, many classical results do not hold in the theory $I\Delta_0$. What is available instead is factorization in powers of primes of any element. In order to see this we use some lemmas.

Lemma 1.3.3 *Let A be a bounded and Δ_0-definable subset of $\mathcal{M} \models I\Delta_0$. Then A has a maximum element.*

Proof. Let $\phi(x)$ be the Δ_0 formula defining the set A, and let $\alpha \in \mathcal{M}$ be an upper bound for A.
The set $X = \{y \leq \alpha\ :\ \exists t \leq \alpha\ (\phi(t) \wedge y < t)\}$ is clearly Δ_0-definable, and so is the set $X^c = \mathcal{M} \setminus X = \{y\ :\ y > \alpha\} \cup \{y\ :\ y \leq \alpha \wedge \forall t \leq \alpha(\phi(t) \to y > t)\}$. Let $x_0 = min(X^c)$; then $x_0 - 1 \in X$, hence there is $t \in A$ such that $x_0 - 1 \leq t$. But now necessarily $x_0 - 1 = t$, so $x_0 - 1 = max(A)$. □

Lemma 1.3.4 *Let A be a bounded, Δ_0-definable subset of $\mathcal{M} \models I\Delta_0$. If there is a non-zero $m \in \mathcal{M}$ divisible by all $a \in A$, then there is a non-zero $\mu \in \mathcal{M}$ which is minimal with respect to this property (i.e. if $x \in \mathcal{M}$ is divisible by all elements of A, then μ divides x).*

Proof. Let $\phi(x)$ be the Δ_0-formula defining the set A.
The set $D = \{b \ : \ b \neq 0 \wedge \forall a \leq m \ (\phi(a) \rightarrow \delta(a,b))\}$ is Δ_0-definable and nonempty since $m \in D$ (here $\delta(a,b)$ is the usual Δ_0-formula for divisibility (1.1)).

Let μ be the minimum of D. Now let $x \in \mathcal{M}$ be divisible by all elements of A and not by μ, then we have $x = \mu q + r$ for $q, r \in \mathcal{M}$, with $0 \leq r < \mu$. Hence $r = x - \mu q$ is divisible by all elements of A, and since $\mu = min(D)$, it must be $r = 0$ and so μ divides x. □

The minimal element μ divisible by all elements of A will be called the *least common multiple of* A and it will be denoted by $lcm(A)$.

We also prove, by an easy Δ_0-induction, that every element is divisible by a prime.

Lemma 1.3.5 $I\Delta_0 \vdash \forall x > 1 \ \exists p \leq x \ (Pr(p) \wedge \delta(p,x))$.

Proof. Here $Pr(p)$ is again the Δ_0-statement for primes (1.3).
Let $\psi(x) = \forall y \leq x \ \exists p \leq y \ (Pr(p) \wedge \delta(p,y))$; clearly $I\Delta_0 \vdash \psi(2)$. Suppose $I\Delta_0 \vdash \psi(x)$ and consider $x+1$. If $x+1$ is a prime, then $I\Delta_0 \vdash \psi(x+1)$. If $x+1$ is not a prime, then there is a $1 < y \leq x$ that divides $x+1$. But from $I\Delta_0 \vdash \psi(x)$ we deduce that there is a prime dividing y, and thus dividing $x+1$, hence $I\Delta_0 \vdash \psi(x+1)$. □

We can express that an element is a power of a prime p with the Δ_0-formula

$$Pow_p(x) = Pr(p) \wedge \forall y \leq x \ (\delta(y,x) \rightarrow \delta(p,y)). \tag{1.4}$$

This allows us to identify the greatest power of a prime that divides a given element.

Lemma 1.3.6 $I\Delta_0 \vdash \forall x > 1 \ \forall p \ (Pr(p) \rightarrow \exists! y \leq x \ (Pow_p(y) \wedge \delta(y,x) \wedge \neg\delta(py,x))$

Proof. Let $\mathcal{M} \models I\Delta_0$, $x, p \in \mathcal{M}$, with $x > 1$ and p a prime.
The set $A_p^x = \{y \ : \ Pow_p(y) \wedge \delta(y,x)\}$ of all powers of p dividing x is clearly Δ_0-definable and bounded by x, hence by Lemma 1.3.3 it has a maximum element. □

We can now express that "y is the greatest power of p that divides x" with the Δ_0-formula

$$MPow_p(x,y) = Pow_p(y) \wedge \delta(y,x) \wedge \ \forall z \leq x \ (Pow_p(z) \wedge \delta(z,x)) \rightarrow \delta(z,y) \quad (1.5)$$

For any $x \in \mathcal{M} \models I\Delta_0$ we can consider the Δ_0-definable set

$$A_x = \{y \ : \ \exists p \leq x \ (Pr(p) \wedge MPow_p(x,y))\} \quad (1.6)$$

of all maximum powers of primes dividing x. Since $x \in \mathcal{M}$ is clearly divisible by all elements of A_x, by Lemma 1.3.4 there is the smallest μ divisible by all elements of A_x, which is trivially shown to coincide with x. Hence we have the property of factorization in powers of primes for every element x of a model of $I\Delta_0$ as the $lcm(A_x)$.

What will also be used later is the following $I\Delta_0$-version of the *Chinese Reminder Theorem (CRT)*.

Theorem 1.3.7 *Let A be a bounded, Δ_0-definable subset of $\mathcal{M} \models I\Delta_0$. Let $f, r : A \longrightarrow \mathcal{M}$ be a Δ_0-definable functions such that $(f(a), f(b)) = 1$ for every $a, b \in \mathcal{M}$ and $r(a) < f(a)$ for every $a \in \mathcal{M}$. Suppose there is $w \in \mathcal{M}$ which is divisible by all elements of $f(A)$.*
Then there is $u < \prod_{a \in A} f(a)$ such that $u \equiv r(a)(mod\ f(a))$ for every $a \in A$.

Proof. With $\prod_{a \in A} f(a)$ we mean the $lcm(f(A))$, which exists by Lemma 1.3.4 thanks to the hypothesis that there is $w \in \mathcal{M}$ which is divisible by all elements of $f(A)$.

First of all we remark that we can express the congruence "x is equivalent to y modulo z" via the Δ_0-formula:

$$x \equiv y(mod\ z) \ : \ \exists k \leq x \ (x = y + kz). \quad (1.7)$$

Now let $\phi(x)$ be the Δ_0 formula defining the set A, and consider the Δ_0-formula

$$\theta(x,w) = \exists u \leq w \ \left(u < \prod_{a \in A, a \leq x} f(a) \ \wedge \ \forall t \leq x \ (\phi(t) \rightarrow u \equiv r(t)(mod\ f(t))) \right).$$

By Δ_0-induction we show that $\mathcal{M} \models \forall x\ (\phi(x) \to \theta(x, w))$.
Clearly $\mathcal{M} \models (\phi(1) \to \theta(1, w))$ (it is equivalent to state that a solution to one congruence always exists).
Now suppose $\mathcal{M} \models (\phi(x) \to \theta(x, w))$ for an $x \in \mathcal{M}$, and let $u^* < \prod_{a \in A, a \leq x} f(a)$ and $u^* \equiv r(a)(mod\ f(a))$ for all $a \in A$, $a \leq x$. Now, supposing $x + 1 \in A$, the following system of two congruences

$$\begin{cases} u \equiv u^* \left(mod\ \prod_{a \in A, a \leq x} f(a)\right) \\ u \equiv r(x+1)(mod\ f(x+1)) \end{cases} \tag{1.8}$$

has a solution since the moduli are relatively prime by hypothesis (if we put $\alpha = \prod_{a \in A, a \leq x} f(a)$, since $(\alpha, f(x+1)) = 1$ we know that there are $h, k \in \mathcal{M}$ such that $h\alpha + kf(x+1) = 1$; then $u = u^* kf(x+1) + r(x+1)h\alpha$ is a solution to the system (1.8)). Hence $\mathcal{M} \models (\phi(x+1) \to \theta(x+1, w))$. □

We remark that the previous statement is a generalization of the classic CRT where $A = \{m_1, \ldots, m_k\} \subseteq \mathbb{Z}$ is a finite set of pairwise relatively prime moduli, $r_i < m_i$ for all $i = 1, \ldots, k$ and we are looking for integer solutions of the set of congruences

$$\begin{cases} x \equiv r_1(mod\ m_1) \\ \quad \vdots \\ x \equiv r_k(mod\ m_k) \end{cases}.$$

1.4 Pigeonhole principle and Ω_1

Even though the theory $I\Delta_0$ is strong enough to prove factorization of elements as products of primes, there are many other classical number-theoretical results whose provability in $I\Delta_0$ are still open problems. The main obstacle in obtaining results like unboundedness of primes is, as we mentioned before, the lack of functions of

exponential growth rate, such as factorials, since they are not provably total in models of $I\Delta_0$.

An important result is due to Woods (see [Wo]), who proved that in some cases such functions can be avoided and replaced by combinatorial principles such as the *Pigeonhole Principle*. He showed that if we add to the theory $I\Delta_0$ the following Δ_0-version of the pigeonhole principle (Δ_0-PHP)

$$\forall x < z\ \exists y < z\ \theta(x,y) \rightarrow \exists x_1 < z+1\ \exists x_2 < z+1\ (x_1 \neq x_2 \wedge \theta(x_1,y) \wedge \theta(x_2)),$$

where $\theta(x,y)$ runs through all Δ_0-formulas, the resulting theory $I\Delta_0 + \Delta_0$-PHP is strong enough to prove the existence of arbitrarily large primes.

Notice that Δ_0-PHP actually is an axiom scheme, and it basically says that there is no injective Δ_0-function from $z+1$ into z, and we can also use the notation

$$\neg\exists z\ F\ :\ z+1 \rightarrowtail z.$$

What Woods actually proved is then the following.

Theorem 1.4.1 *$I\Delta_0 + \Delta_0$-PHP $\vdash \forall x \exists p\ (Pr(p) \wedge p > x)$.*

Paris, Wilkie and Woods [P-W-W] later improved this result showing that in order to prove unboundedness of primes in $I\Delta_0$ a *weaker* version of the PHP is sufficient. This principle, that will be denoted by Δ_0-WPHP (weak pigeonhole principle), asserts that there is no injective Δ_0-function from $(1+\varepsilon)z$ into z, for every rational number ε such that the integer part of $(1+\varepsilon)z$ is greater than z. This latter result is hence as follows.

Theorem 1.4.2 *$I\Delta_0 + \Delta_0$-WPHP $\vdash \forall x \exists p\ (Pr(p) \wedge p > x)$.*

The weak pigeonhole principle is provable (as it is showed in [P-W-W]) in the theory $I\Delta_0 + \Omega_1$, where Ω_1 is the axiom

$$\forall x \forall y \exists z\ \left(x^{log_2 y} = z\right). \tag{1.9}$$

Notice that the quantity $log_2 y$ here has a Δ_0-meaning, as the following lemma guarantees.

Lemma 1.4.3 *Let $\mathcal{M} \models I\Delta_0$ and let $a, m \in \mathcal{M}$, with $m > 0$, $a > 1$. Then there is a unique $l_0 \in \mathcal{M}$ such that $a^{l_0} \leq m < a^{l_0+1}$.*

Proof. Here we use the Δ_0 we have mentioned before.
The set $A = \{l \in \mathcal{M} \ : \ \exists b \leq m \ E_0(a, l, b)\}$ is clearly Δ_0-definable in $\mathcal{M}$, and it is bounded and non-empty. Hence, by Lemma 1.3.3, it has a maximum element l_0, so it is $a^{l_0} \leq m < a^{l_0+1}$. □

Consider the formula

$$\lambda(x, y, z) = \exists w \leq x \ \left(E_0(y, z, w) \wedge w \leq x \wedge x < wy\right).$$

By the previous lemma for every $a, m \in \mathcal{M}$, with $m > 0$, $a > 1$ there is a unique l_0 such that $\mathcal{M} \models \lambda(m, a, l_0)$; so the formula $\lambda(x, y, z)$ extends the meaning of "z is the (unique) logarithm of x in basis y" to $\mathcal{M}$. So we can express the axiom Ω_1 introduced before as

$$\forall x \forall y \exists z \ (\exists t \leq y \ (\lambda(y, 2, t) \wedge E_0(x, t, z))).$$

The theory $I\Delta_0 + \Omega_1$ has been widely studied and much is known about its number-theoretical strength. We already mentioned that in [P-W-W] cofinality of primes is proved in $I\Delta_0 + \Omega_1$ (which is still an open question in $I\Delta_0$) and the weak version of the pigeon-hole principle Δ_0-WPHP. Notice that, even though function of exponential growth are still "out of range" in $I\Delta_0 + \Omega_1$, the axiom Ω_1 increases the strength of the theory $I\Delta_0$, allowing us to consider functions of growing rate more than polynomial, thanks to the totality of the function $x^{log_2 y}$. Hence we can state that

$$I\Delta_0 \subset I\Delta_0 + \Omega_1. \tag{1.10}$$

Moreover $I\Delta_0 + \Omega_1$ also proves many classical results like Lagrange's four squares theorem (see [B-I]) and basic results about residue fields (see [D-M]).

Anyway the theory $I\Delta_0 + \Omega_1$ is strictly weaker than $I\Delta_0 + exp$: let $\mathcal{M}$ be a model of $I\Delta_0 + \Omega_1$ and $a \in \mathcal{M}$ be non-standard (i.e. $a \in \mathcal{M} \setminus \mathbb{N}$); if we consider the set

$$BL(a) = \left\{ x \in \mathcal{M} \ : \ x < a^{\left(log_2 a\right)^n} \text{ for some } n \in \mathbb{N} \right\}$$

we have that $BL(a) \models I\Delta_0 + \Omega_1$, but $BL(a) \not\models exp$. Thus we have $I\Delta_0 + \Omega_1 \nvdash exp$, and recalling the previous relations (1.2) and (1.10), the following chain of strict inclusions holds for the weak fragments of PA we have described:

$$IOpen \subset I\Delta_0 \subset I\Delta_0 + \Omega_1 \subset I\Delta_0 + exp.$$

Chapter 2

Legendre's theorem

In this chapter we are going to show a proof of Legendre's theorem in the theory $I\Delta_0 + \Omega_1$. In order to do this we will provide all necessary tools and, even though the final proof of the theorem requires the axiom Ω_1, all properties will be stated and proved in the weakest possible fragment of PA that makes them valid, i.e. $I\Delta_0$.

2.1 Legendre's theorem and its equivalent

Legendre's theorem gives a necessary and sufficient condition for the existence of non trivial solution for certain quadratic equations with integer coefficients. The equations considered are of the form

$$ax^2 + by^2 + cz^2 = 0, \tag{2.1}$$

with $a, b, c \in \mathbb{Z} \setminus \{0\}$, *square free*, relatively prime and, clearly, not all of the same sign. For a non trivial solution we mean a solution $(x_0, y_0, z_0) \in \mathbb{Z}$ different from $(0, 0, 0)$.

An integer a is *square free* if no square divides a, or equivalently all primes dividing a appear in with exponent 1 the factorization of a. We remark that this property is Δ_0-definable via the formula:

$$\sigma(x) = \forall y \leq x \ (Pr(y) \rightarrow \neg\delta(y^2, x)),$$

where $\delta(y,x)$ ="*y divides x*" and $Pr(y)$ ="*y is a prime*" are expressed by the Δ_0-formulas (see also 1.1) and (1.2):

$$\delta(y,x) = \exists z \leq x\ (yz = x)$$

$$Pr(y) = \forall x \leq y\ (\delta(x,y) \rightarrow (x = 1 \vee y = x)).$$

We will consider *congruences* in $I\Delta_0$: as for the classical definition on integers we say that a is congruent to b modulo c, with $a, b, c \in \mathcal{M} \models I\Delta_0$, $c \neq 0$, if c divides $b - a$, and this can be expressed by the Δ_0-formula

$$\gamma(a,b,c) = \exists m \leq a\ (a = mc + b). \tag{2.2}$$

We will also denote this fact as $a \equiv b(mod\ c)$. Given any $a, c \in \mathcal{M}$, $c \neq 0$, we can always consider some $b \in \mathcal{M}$ such that $a \equiv b(mod\ c)$ and $|b| \leq c/2$. This follows from the fact that we can find $q, r \in \mathcal{M}$ such that $a = qc + r$, with $0 \leq r < c$, and so we have $a \equiv r \equiv r - c(mod\ c)$, with either r or $r - c \leq c/2$.

Moreover, we will use the fact that if two elements a and b are relatively prime, a is invertible modulo b, and viceversa. Recall that models of $I\Delta_0$ are Bezout rings, so if $(a,b) = 1$ then there are h, k such that $ah + bk = 1$, so $ah \equiv 1(mod\ b)$, and we can identify a^{-1} with h. This is a Δ_0-property since it can be expressed by the Δ_0-formula

$$Inv(a,b) = \exists w \leq b\ \gamma(aw, 1, b), \tag{2.3}$$

where γ is the Δ_0-formula for congruences (2.2).

We will denote the fact that *a is a square modulo b* by $a\mathcal{R}b$. This is Δ_0-definable via:

$$\rho(a,b) = \exists x \leq b/2 \wedge \exists m \leq a(a = x^2 + mb).$$

We now fix a model $\mathcal{M}$ of $I\Delta_0 + \Omega_1$. The statement of Legendre's theorem in $\mathcal{M}$ is as follows.

Theorem 2.1.1 (Legendre) *Let $a, b, c \in \mathcal{M} \setminus \{0\}$ be non-zero, not all of the same sign, square-free and pairwise relatively prime. Then the equation*

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

has a non trivial solution in $\mathcal{M}$ if and only if

(*Leg.1*) $-ab\mathcal{R}c$,

(*Leg.2*) $-bc\mathcal{R}a$,

(*Leg.3*) $-ac\mathcal{R}b$.

Remarks:

1. If a non trivial solution (x_0, y_0, z_0) of (2.1) exists, then we can consider x_0, y_0, z_0 to be pairwise relatively prime (and call such a solution *primitive*). Indeed, suppose p is a prime and p divides x_0 and y_0. Then $p^2|cz_0^2$, and since c is square free, $p|z_0^2$ and so $p|z_0$, so we can factor out p and consider the solution $(x_0/p, y_0/p, z_0/p)$.

2. The necessary condition of Theorem 2.1.1 is easily proved, even in models of $I\Delta_0$:

Proof. ($\Longrightarrow$ of 2.1.1) Let (x_0, y_0, z_0) be a primitive solution of (2.1) in a model $\mathcal{M}$ of $I\Delta_0$. Then

$$ax_0^2 + by_0^2 + cz_0^2 = 0, \tag{2.4}$$

and reducing modulo a we get $-by_0^2 \equiv cz_0^2 (mod\ a)$.
Now if a prime p divides a and y_0, equation (2.4) implies that $p|cz_0^2$. From $(a, c) = 1$ we get that $p \not| c$ and so $p|z_0$. Hence p divides y_0 and z_0, which is a contradiction.

Hence we have $(a, y_0) = 1$, and y_0 is invertible modulo a. So we can write $-b \equiv cz_0^2(y_0^{-1})^2 (mod\ a)$, where y_0^{-1} is given by the formula $Inv(y_0, a)$ (see (2.3)). Hence we can rewrite $-bc \equiv (cz_0y_0^{-1})^2 (mod\ a)$, i.e. $-bc\mathcal{R}a$. In the same way, being the equation (2.1) symmetric for a, b and c, we also get $-ab\mathcal{R}c$ and $-ac\mathcal{R}b$. □

In order to prove Legendre's theorem in any model of $I\Delta_0 + \Omega_1$, we consider the following equivalent *normal form*. Using the same notation as before, the statement is as follows.

Theorem 2.1.2 (Legendre normal form) *Let $a, b \in \mathcal{M} \setminus \{0\}$ be square-free and positive. Then the equation*

$$ax^2 + by^2 = z^2 \tag{2.5}$$

has a non trivial solution in $\mathcal{M}$ if and only if

(Norm.1) $a\mathcal{R}b$,

(Norm.2) $b\mathcal{R}a$,

(Norm.3) $-\frac{ab}{d^2}\mathcal{R}d$, *where* $d = (a, b)$.

Remarks:

1. Using the same arguments as before we can assume that, if a non trivial solution (x_0, y_0, z_0) of the equation (2.5) exists, it is *primitive* (i.e. x_0, y_0, z_0 pairwise relatively coprime).

2. The necessary condition of the Theorem 2.1.2 is proved as follows, in any model of $I\Delta_0$.

Proof. ($\Longrightarrow$ of 2.1.2) Let (x_0, y_0, z_0) be a primitive solution of (2.5) in a model $\mathcal{M}$ of $I\Delta_0$, i.e.

$$ax_0^2 + by_0^2 = z_0^2. \tag{2.6}$$

We have $(a, y_0) = 1$. Indeed, if p is a prime and p divides a and y_0, then $p|z_0^2$, and so$p|z_0$. Then we get $p|(y_0, z_0)$, contradicting the fact that the solution is primitive.

So y_0 is invertible modulo a in $\mathcal{M}$, and we have $by_0^2 \equiv z_0^2 (mod\ a)$, which implies $b \equiv (z_0 y_0^{-1})^2 (mod\ a)$, i.e. $b\mathcal{R}a$.

Similarly, by symmetry of the equation (2.6) on the coefficients a and b, we can show that $a\mathcal{R}b$.

In order to obtain condition *(Norm.3)* of the theorem, we first observe that d is square-free since a, b are. Moreover, if $a = da'$ and $b = db'$, with $(a', b') = 1$, from (2.6) we get

$$d(a'x_0^2 + b'y_0^2) = z_0^2, \tag{2.7}$$

i.e.$d|z_0^2$. Since d is square-free d divides z_0. Let $z_0 = dz_0'$.
From (2.7) we have:

$$a'x_0^2 + b'y_0^2 = z_0^2/d = (dz_0')^2/d = d(z_0')^2 \tag{2.8}$$

which can be rewritten as

$$\frac{a}{d}x_0^2 + \frac{b}{d}y_0^2 = d\left(\frac{z_0}{d}\right)^2. \tag{2.9}$$

Hence $-\frac{a}{d}x_0^2 = \frac{b}{d}y_0^2 - d\left(\frac{z_0}{d}\right)^2 \equiv \frac{b}{d}y_0^2 (mod\ d)$.

We already noticed that $(x_0, b) = 1$, so also $(x_0, d) = 1$, hence x_0 is invertible modulo d. So we have

$$-\frac{a}{d} \equiv \frac{b}{d}y_0^2(x_0^{-1})^2 (mod\ d) \Rightarrow -\frac{a}{d}\frac{b}{d} \equiv \left(\frac{b}{d}y_0x_0^{-1}\right)^2 (mod\ d),$$

that means $-\frac{ab}{d^2}\mathcal{R}d$.$\square$

The next step is to prove the equivalence between the two statements of Legendre's theorem. We will use the following lemma.

Lemma 2.1.3 *Let $a, m, n \in \mathcal{M} \models I\Delta_0$, m, n relatively prime. If $a\mathcal{R}m$ and $a\mathcal{R}n$, then $a\mathcal{R}mn$.*

Proof. From the hypothesis there are $\alpha, \beta \in \mathcal{M}$, $\alpha \leq m/2, \beta \leq n/2$ such that

$$a \equiv \alpha^2 (mod\ m) \text{ and } b \equiv \beta^2 (mod\ n).$$

Consider the system of congruences

$$\begin{cases} x \equiv \alpha (mod\ m) \\ x \equiv \beta (mod\ n) \end{cases}. \tag{2.10}$$

Since $(m, n) = 1$, the system (2.10) has a solution $\gamma \in \mathcal{M}$ by Theorem 1.3.7 (Δ_0-CRT) . Hence, we have

$$\gamma \equiv \alpha (mod\ m) \text{ and } \gamma \equiv \beta (mod\ n).$$

Then we have

$$a \equiv \gamma^2 (mod\ m) \text{ and } a \equiv \gamma^2 (mod\ n),$$

that means that both m, n divide $a - \gamma^2$. Since m, n are relatively prime, we have that mn divides $a - \gamma^2$, that means $a \equiv \gamma^2 (mod\ mn)$, i.e. $a\mathcal{R}mn$.$_\square$

We can now prove the following theorem.

Theorem 2.1.4 *Theorems 2.1.1 and 2.1.2 are equivalent.*

Proof. (2.1.1 $\Longrightarrow$ 2.1.2) To prove this implication we assume Theorem 2.1.1 valid, and we only have to prove the sufficient condition [$\Longleftarrow$] of Theorem 2.1.2, since the other implication has already been shown to be true.

So we consider an equation

$$ax^2 + by^2 = z^2, \tag{2.11}$$

with $a, b \in \mathcal{M} \models I\Delta_0$, a, b square-free and positive, and suppose conditions

(Norm.1) $a\mathcal{R}b$,

(Norm.2) $b\mathcal{R}a$,

(Norm.3) $-\frac{ab}{d^2}\mathcal{R}d$, where $d = (a, b)$

of Ttheorem 2.1.2 hold.

We now consider the equation

$$\frac{a}{d}x^2 + \frac{b}{d}y^2 + (-d)z^2 = 0, \tag{2.12}$$

which can be written as

$$Ax^2 + By^2 + Cz^2 = 0, \tag{2.13}$$

where $A = \frac{a}{d}, B = \frac{b}{d}$ and $C = -d$.

The coefficients A, B, C are square-free and pairwise relatively prime. We have:

$$-AB = -\frac{ab}{d^2}, \text{ and we know that } -\frac{ab}{d^2}\mathcal{R}d \text{ by } (Norm.3),$$

hence we have $-AB\mathcal{R}C$. Moreover,

$$-AC = -\frac{a}{d}(-d) = a, \text{ and we know that } a\mathcal{R}b \text{ by } (\textit{Norm.3}), \text{ so } a\mathcal{R}\frac{b}{d},$$

that means $-AC\mathcal{R}B$. Finally,

$$-BC = -\frac{b}{d}(-d) = b, \text{ and } b\mathcal{R}a \text{ by } (\textit{Norm.2}),$$

which implies $b\mathcal{R}\frac{a}{d}$, that means $-BC\mathcal{R}A$.

So the three conditions of Theorem 2.1.1 hold for the equation (2.12). We can deduce that equation (2.12) has a non trivial solution (x_0, y_0, z_0), i.e.

$$\frac{a}{d}x_0^2 + \frac{b}{d}y_0^2 + (-d)z_0^2 = 0$$

which implies $ax_0^2 + by_0^2 = (dz_0)^2$. Hence the triple (x_0, y_0, dz_0) is a non-trivial solution of (2.11).

(2.1.2 $\Longrightarrow$ 2.1.1) As before, to prove this implication we assume Theorem 2.1.2 valid, and we prove the sufficient condition [$\Longleftarrow$] of Theorem 2.1.1.

Consider the equation

$$ax^2 + by^2 + cz^2 = 0, \tag{2.14}$$

with $a, b, c \in \mathcal{M} \models I\Delta_0$, a, b, c square-free, pairwise relatively prime and not all of the same sign. W.l.o.g. we can assume $a, b > 0$ and $c < 0$, and suppose the conditions

(*Leg.1*) $-ab\mathcal{R}c$,

(*Leg.2*) $-bc\mathcal{R}a$,

(*Leg.3*) $-ac\mathcal{R}b$

of Theorem 2.1.1 hold.

If we multiply both sides of (2.14) by $-c$ we obtain the equation

$$(-ac)x^2 + (-bc)y^2 = (cz)^2, \tag{2.15}$$

which can be written as

$$Ax^2 + By^2 = Z^2, \tag{2.16}$$

where $A = -ac, B = -bc$ and $Z = cz$.

Here the coefficients A and B are square-free (since a, b, c are pairwise relatively prime) and positive.

From (*Leg.3*) we have $A\mathcal{R}b$, and also $A\mathcal{R}c$ since $c|A$, and since $(b, c) = 1$ we can apply Lemma 2.1.3 to obtain that $A\mathcal{R}B$. In the same way we can prove that $B\mathcal{R}A$.

Finally, notice that $(A, B) = (ac, bc) = c$, and

$$-\frac{AB}{c^2} = 1\frac{-(ac)(-bc)}{c^2} = -ab, \text{ and we know that } -ab\mathcal{R}c \text{ from (}Leg.1\text{)},$$

hence we have $-\frac{AB}{c^2}\mathcal{R}c$. We can conclude that all conditions of Theorem 2.1.2 hold for the equation (2.16), so it has a non trivial solution (x_0, y_0, Z_0), for which $Z_0 = cz_0$, for some $z_0 \in \mathcal{M}$, and

$$(-ac)x_0^2 + (-bc)y_0^2 = (cz_0)^2 \iff c(-ax_0^2 - by_0^2) = c^2z_0^2 \iff ax_0^2 + by_0^2 = cz_0^2,$$

hence (x_0, y_0, z_0) is a non-trivial solution of (2.14).□

2.2 Proof of the theorem in $I\Delta_0 + \Omega_1$

In this section we are going to prove Legendre's theorem in the theory $I\Delta_0 + \Omega_1$ by proving its equivalent normal form. The proof follows the main ideas of that in [I-R]. We will pay close attention in adapting all the arguments in $I\Delta_0 + \Omega_1$.

We start from the following lemmas which imply a crucial result that will be used in the main proof.

Lemma 2.2.1 *If $p \in \mathcal{M} \models I\Delta_0$ is a prime and -1 is a square modulo p (i.e. $-1\mathcal{R}p$), then there is $k \in \mathcal{M}$, with $k < p$, such that $kp = 1 + a^2$, for $a \leq \frac{p-1}{2}$.*

Proof. Let $a \in \mathcal{M}$, $a \leq \frac{p-1}{2}$ be such that $-1 \equiv a^2 (mod\ p)$. This means that there is $k \in \mathcal{M}$ such that

$$kp = a^2 + 1 \leq \left(\frac{p-1}{2}\right)^2 + 1.$$

We can prove that $\left(\frac{p-1}{2}\right)^2 + 1 < p^2$. Indeed, if not, we would get $p^2 + 2p - 3 \leq 0$, which implies $-3 \leq p \leq 1$, a contradiction.

Hence we have $kp < p^2$, with $k < p$, and $kp = 1 + a^2$. □

Lemma 2.2.2 *Let $p \in \mathcal{M} \models I\Delta_0$ be a prime. If there is $k \in \mathcal{M}$, with $k < p$ such that kp is the sum of two squares, then p itself is the sum of two squares.*

Proof. It is clear that $2 = 1 + 1$ is a sum of two squares, so we can assume $p \neq 2$.

The set $S(p) = \{m \in \mathcal{M} : m < p$ and mp is the sum of two squares $\}$, is Δ_0-definable via the formula $\sigma(x) = \exists y < p\ \exists z < p\ (xp = y^2 + z^2)$, and it is clearly bounded by p and, by hypothesis, not empty. By Δ_0-induction $S(p)$ has a minimum element, and we now show that it is 1.

Let $h \in \mathcal{M}$ be the minimum of $S(p)$, and let $, a, b < p$ be such that $hp = a^2 + b^2$. Suppose that $h > 1$, and we show that we can find a $h' \in S(p)$ with $h' < h$. We will distinguish two cases.

- *case h is even*: then a and b must be both even or both odd.

If a, b are both even we can write

$$hp = 4\left(\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2\right),$$

hence 4 divides h and we have

$$\frac{h}{4}p = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2.$$

So there is $h' = h/4 < h$ and $h'p$ is the sum of two squares.

If a, b are both odd we can write

$$\frac{h}{2}p = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2,$$

so again we get $h'p$ as a sum of two squares, with $h' = h/2 < h$.

- *case h is odd*: let $a \equiv \alpha (mod\ h)$ and $b \equiv \beta (mod\ h)$, with $\alpha, \beta < \frac{h}{2}$. Then

$$hp = a^2 + b^2 \equiv \alpha^2 + \beta^2 \equiv 0 (mod\ h),$$

hence there is $j \in \mathcal{M}$ such that

$$\alpha^2 + \beta^2 = jh, \tag{2.17}$$

and $j < h$ since $\alpha^2 + \beta^2 < (h/2)^2 + (h/2)^2 = h^2/2 < h^2$.
Now from $a^2 + b^2 = kp$ and (2.17) we obtain

$$\left(a^2 + b^2\right)\left(\alpha^2 + \beta^2\right) = jh^2p. \tag{2.18}$$

Since

$$\left(a^2 + b^2\right)\left(\alpha^2 + \beta^2\right) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2,$$

and $a\alpha + b\beta \equiv \alpha^2 + \beta^2 \equiv 0(mod\ h)$, we have that h divides $a\alpha + b\beta$ and, similarly, h divides $a\beta - b\alpha$.
Henceforth, from (2.18) we obtain

$$\left(\frac{a\alpha + b\beta}{h}\right)^2 + \left(\frac{a\beta - b\alpha}{h}\right)^2 = jp,$$

so we have jp as a sum of two squares and $j < h$. □

It is now easy to deduce the following property.

Proposition 2.2.3 *Let $\mathcal{M} \models I\Delta_0$ and let $p \in \mathcal{M}$ be a prime. If -1 is a square modulo p, then p is the sum of two squares.*

Proof. It is sufficient to observe that if -1 is a square modulo p, then by Lemma 2.2.1 there are $k, a \in \mathcal{M}$, $k, a < p$, such that $kp = 1 + a^2$, which is clearly a sum of two squares. The statement then follows straightforward from Lemma 2.2.2.□

We now use the previous result to reproduce a property of the integers in models of $I\Delta_0 + \Omega_1$, that will be used later in the proof of Legendre's theorem.

Proposition 2.2.4 *Let $\mathcal{M} \models I\Delta_0$ and $b \in \mathcal{M}$. If -1 is a square modulo b, then b is the sum of two squares.*

Proof. If -1 is a square modulo b, then -1 is a square modulo every prime p dividing b. Proposition 2.2.3 implies that every prime dividing b is the sum of two squares.

It is easy to verify that the product of sums of two squares is still a sum of two squares (e.g. $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$). We can iterate this argument to the product of all primes dividing b, which is of logarithmic length with respect to b (roughly $log_2\ b$), where all the partial products are bounded by b itself. □

Remarks:

On most texts on classic number theory the previous properties are proved using tools such as the (full) Pigeonhole Principle, which we have not available even in $I\Delta_0+\Omega_1$, or *Legendre's symbol* $\left(\frac{a}{p}\right)$ (see [H-W]) and the property that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}(mod\ p)$, which is not known to be valid in $I\Delta_0$. The arguments showed above is thus an adaptation of classical results to our context.

We can now go through the proof of theorem 2.1.2 in the theory $I\Delta_0+\Omega_1$. In the first part we show how to get a solution of the considered equation, and in the second part we formalize its existence in $I\Delta_0+\Omega_1$. Here we restate the theorem.

Theorem 2.2.5 (Legendre normal form) *Let $\mathcal{M} \models I\Delta_0+\Omega_1$ and let $a, b \in \mathcal{M}$ be square-free and positive. Then the equation*

$$ax^2 + by^2 = z^2 \tag{2.19}$$

has a non trivial solution in $\mathcal{M}$ if and only if

(Norm.1) $a\mathcal{R}b$,

(Norm.2) $b\mathcal{R}a$,

(Norm.3) $-\frac{ab}{d^2}\mathcal{R}d$, *where* $d = (a, b)$.

Proof. As noticed in the remarks following the statement of 2.1.2, we only have to prove that the properties (*Norm.1-3*) imply that the equation (2.19) has a non-trivial solution. Consider such an equation and suppose conditions (*Norm.1-3*) hold for $a, b \in \mathcal{M}$, a, b square-free and positive. There are some trivial cases:

- Case $a = 1$: then (2.19) becomes $x^2+by^2 = z^2$ and the triple $(1, 0, 1)$ is a non-trivial solution;
- Case $b = 1$: as before, being $(0, 1, 1)$ a non-trivial solution for $ax^2 + y^2 = z^2$;
- Case $a = b$: then (2.19) becomes $b(x^2 + y^2) = z^2$, and the condition (*Norm.3*) says that $-\frac{b^2}{b^2}\mathcal{R}b$, i.e. $-1\mathcal{R}b$; now, by proposition 2.2.4 we know that there are $r, s \in \mathcal{M}$ such that $b = r^2 + s^s$, and the triple (r, s, b) represents a non-trivial solution of the equation.

Notice that in all these trivial cases the solution (x_0, y_0, z_0) is such that $x_0, y_0, z_0 \leq a$.

We can now consider $a, b > 1$ and, $a \neq b$; without loss of generality we suppose $b < a$. The argument is as follows: from the starting equation (2.19) we build another equation

$$Ax^2 + by^2 = z^2, \tag{2.20}$$

with $0 < A < a$ and satisfying the appropriate conditions (*Norm.1-3*), such that if (2.20) has a non-trivial solution, we obtain a non-trivial solution of (2.19) from it. By applying repeatedly this argument, possibly switching the role of the coefficients a and b at some point, we eventually get to one of the trivial cases $a = 1$, $b = 1$ or $a = b$, that admit a non-trivial solution, and going backward from that we obtain a non-trivial solution to (2.19). We have to formalize this argument by Δ_0 induction.

For the equation $ax^2 + by^2 = z^2$ we know from (*Norm.2*) that there is $\beta \leq a/2$ such that $b \equiv \beta^2 (mod\ a)$, hence there is $k \leq a$ such that $\beta^2 - b = ka$. If we factor out the squares in k we can write

$$\beta^2 - b = h^2 Aa, \tag{2.21}$$

with A square-free. This is the coefficient we use in equation (2.20) we are going to work with.

Now

$$0 \leq \beta^2 = h^2Aa + b < h^2Aa + a = a(h^2A + 1) \Rightarrow h^2A + 1 > 0 \Rightarrow A > -\frac{1}{h^2} \geq -1,$$

hence $A \geq 0$. On the other hand, if $A = 0$ then $b = \beta^2$, a contradiction since b is square-free. We have then proved that $A > 0$.

Moreover, from (2.21) we also get

$$aA \leq aAh^2 < \beta^2 \leq \frac{a^2}{4},$$

that means

$$A < \frac{a}{4}. \tag{2.22}$$

This inequality will turn out to be very important later.

Now if $d = (a, b)$ then $a = da_1,\ b = db_1$, with $(a_1, b_1) = 1$.

If a prime p divides both a_1 and d, then p^2 divides a, and since a is square-free we have $(a_1, d) = 1$, and the same argument shows $(b_1, d) = 1$.

From (2.21) we get

$$\beta^2 = h^2Aa + b = h^2Aa_1d + b_1d = d(h^2Aa_1 + b_1),$$

hence d divides β^2, and since d is square-free, we have $d|\beta$. Llet $\beta = d\beta_1$, then $\beta^2 = d^2\beta_1^2$ and we have $d^2\beta_1^2 = d(h^2Aa_1 + b_1)$, hence

$$d\beta_1^2 = h^2Aa_1 + b_1. \tag{2.23}$$

Now, if any prime p divides both d and h, from (2.23) it follows that p divides b_1, and hence p divides both b_1 and d, a contradiction since they are relatively prime. So necessarily $(d, h) = 1$. From (2.23) we obtain

$$h^2Aa_1 \equiv -b_1 (mod\ d) \ \text{ which implies } \ h^2Aa_1^2 \equiv -b_1a_1 (mod\ d),$$

and since $(a_1, d) = (h, d) = 1$, both h and a_1 are invertible modulo d. So we have

$$A \equiv -a_1b_1 \left(h^{-1}a_1^{-1}\right)^2 (mod\ d).$$

Now, since $-a_1b_1 = -\frac{ab}{d^2}$, condition (*Norm.3*) tells us that $-a_1b_1$ is a square modulo d, and so we get

$$A\mathcal{R}d. \tag{2.24}$$

Notice that if there is a prime p which divides both h and b, then from (2.21) we get that p divides β an then p^2 divides b, and this is a contradiction since b is square-free. Hence $(h, b) = 1$. Since b_1 divides b, also $(h, b_1) = 1$. Then from (2.21) the following implication holds

$$h^2Aa \equiv \beta^2 (mod\ b_1) \Rightarrow A \equiv \beta^2 \left(h^{-1}\right)^2 a^{-1} (mod\ b_1).$$

From (*Norm.1*) states that $a\mathcal{R}b$ it follows that $a\mathcal{R}b_1$, and so

$$A\mathcal{R}b_1. \tag{2.25}$$

Now from (2.24), (2.25) and Lemma 2.1.3 we get

$$A\mathcal{R}b. \tag{2.26}$$

Moreover, from (2.21) we know that $b \equiv \beta^2 (mod\ A)$, that means

$$b\mathcal{R}A. \tag{2.27}$$

If $r = (A, b)$, then it is left to show that $-\frac{Ab}{r^2}\mathcal{R}r$.
Let $A = A_2r, b = b_2r$, with $(A_2, b_2) = 1$. We have $(r, A_2) = (r, b_2) = 1$ since A, b are square-free. From (2.21) we obtain

$$\beta^2 = b_2r + h^2A_2ra = r(b_2 + h^2A_2a). \tag{2.28}$$

So r divides β^2, and since r is square-free, we have $r|\beta$. Let $\beta = \beta_2r$, from (2.28) we get the following implications

$$r\beta_2^2 = b_2 + h^2A_2a \Rightarrow h^2A_2a \equiv -b_2 (mod\ r) \Rightarrow -A_2b_2h^2a \equiv b_2^2 (mod\ r). \tag{2.29}$$

Now using the same arguments as before we can show that $(a, r) = (h, r) = 1$, so both a, h are invertible modulo r, and we obtain

$$-A_2b_2 \equiv b_2^2 \left(h^{-1}\right)^2 a^{-1} (mod\ r).$$

Recalling that $a\mathcal{R}b$ and $r|b$, we have that $a\mathcal{R}r$, and since $-A_2b_2 = -\frac{Ab}{r^2}$, the previous congruences imply that

$$-\frac{Ab}{r^2}\mathcal{R}r. \tag{2.30}$$

We have then obtained the equation (2.20) $Ax^2 + by^2 = z^2$, with $0 < A < a/4$, A square-free and (by (2.26), (2.27) and (2.30)) satisfying the conditions

(*Norm.1)* $A\mathcal{R}b$,

(*Norm.2)* $b\mathcal{R}A$,

(*Norm.3)* $-\frac{Ab}{r^2}\mathcal{R}r$, where $r = (A, b)$.

The single reduction we have made can easily be formalized in $I\Delta_0$, since it is based only on congruences and the quantifiers are obviously bounded by the initial coefficients a and b.

Now suppose (x_0, y_0, z_0) is a non-trivial solution of (2.20), hence

$$Ax_0^2 = z_0^2 - by_0^2 \tag{2.31}$$

By multiplying (2.31) by (2.21) we have

$$A^2x_0^2h^2a = (z_0^2 - by_0^2)(\beta^2 - b) = z_0^2\beta^2 - bz_0^2 - by_0^2\beta^2 + b^2y_0^2;$$

if we now add and subtract the quantity $2z_0\beta by_0$ we have

$$A^2x_0^2h^2a = (z_0^2\beta^2+b^2y_0^2+2z_0\beta by_0)-b(z_0^2+y_0^2\beta^2+2z_0\beta by_0) = (z_0\beta+by_0)^2-b(z_0+y_0\beta)^2,$$

and so

$$a(Ax_0h)^2 + b(z_0 + y_0\beta)^2 = (z_0\beta + by_0)^2,$$

which states that the triple

$$(Ax_0h,\ z_0 + y_0\beta,\ z_0\beta + by_0)$$

is a non-trivial solution of equation (2.19).

We now need to estimate the growth rate of the solution of equation (2.19) in terms of that of (2.20).
First of all, notice that if $Ax_0^2 + by_0^2 = z_0^2$, then clearly $x_0, y_0 \leq z_0$ (remember that both A and b are positive).
Then, as already showed, the components of the solution of (2.19) are

- $Ax_0h \leq x_o\frac{a}{4}$ (since $Ah < \frac{a}{4}$)
- $z_0 + y_0\beta \leq z_0 + z_0\beta = z_0\left(1 + \frac{a}{2}\right)$ (since $\beta \leq \frac{a}{2}$)
- $z_0\beta + by_0 \leq z_0\frac{a}{2} + az_0 = z_0\left(\frac{3}{2}a\right)$

and since we are assuming $a > 1$ we can conclude that all the components of the new solution are $\leq z_0\left(\frac{3}{2}a\right)$.

We now have to iterate this procedure and formalize it in $I\Delta_0 + \Omega_1$. We start with the given equation

$$E_0 : \ ax^2 + by^2 = z^2, \tag{2.32}$$

where a, b are square-free, $a > b$ and

$$a\mathcal{R}b, \ b\mathcal{R}a, \ -\frac{ab}{d^2}\mathcal{R}d, \text{ where } d = (a, b),$$

and we build a sequence of equations, for $i > 0$

$$E_i : \ A_ix^2 + B_iy^2 = z^2, \tag{2.33}$$

where every A_i, B_i are defined by recursion as follows (where $A_0 = a, B_0 = b$)

$$\bullet \ \beta_i^2 - B_i = h_i^2A_iA_{i-1}, \ B_i = B_{i-1} \tag{2.34}$$

with $A_ih_i < \frac{A_{i-1}}{4}, \ \beta_i \leq \frac{A_{i-1}}{2}$, if at step $i-1$ we have $A_{i-1} > B_{i-1}$, or

$$\bullet \ \alpha_i^2 - A_i = h_i^2B_iB_{i-1}, \ A_i = A_{i-1} \tag{2.35}$$

with $B_ih_i < \frac{B_{i-1}}{4}, \ \alpha_i \leq \frac{B_{i-1}}{2}$, if at step $i-1$ we have $A_{i-1} < B_{i-1}$.

For every equation E_i the following congruence conditions hold.

$$A_i \mathcal{R} B_i,\ B_i \mathcal{R} A_i,\ -\frac{A_i B_i}{r_i^2} \mathcal{R} r_i,\ \text{where } r_i = (A_i, B_i).$$

Moreover, if (x_i, y_i, z_i) is a non-trivial solution of equation E_i, then a non-trivial solution of E_{i-i} is either

$$\bullet\ (A_i x_i h_i,\ z_i + y_i \beta_i,\ z_i \beta_i + B_{i-1} y_i) \tag{2.36}$$

or

$$\bullet\ (z_i + y_i \alpha_i,\ B_i x_i h_i,\ z_i \alpha_i + A_{i-1} y_i) \tag{2.37}$$

according to $A_{i-1} > B_{i-1}$ or $A_{i-1} < B_{i-1}$, respectively.

We remark that:

(i) the growth factor from a solution of the equation E_i to that of E_{i-1} is always bounded by $\frac{3}{2}A_{i-1} \leq \frac{3}{2}a$ when $A_{i-1} > B_{i-1}$, and by $\frac{3}{2}B_{i-1} \leq \frac{3}{2}b$ when $A_{i-1} < B_{i-1}$;

(ii) when "descending" through the sequence, the coefficients of equation E_i and those of equation E_{i-1} are related as follows:

$$A_i < \frac{A_{i-1}}{4} \leq \frac{a}{4} \text{ or } B_i < \frac{B_{i-1}}{4} \leq \frac{b}{4}.$$

Hence the length of the sequence of E_i's is at most $log_4 a + log_4 b$.

(iii) the sequence of equations will eventually stop with one of the trivial cases where one of the coefficients is 1 or they are equal. In these cases non trivial solutions exist, namely $(1, 0, 1)$ or $(0, 1, 1)$ or (r_i, s_i, B_i), where $B_i = r_i^2 + s_i^2$.

Let l be the length of the sequence. For the final solution of equation E_l we can clearly state that $x_l, y_l, z_l \leq b$ (where b is the coefficient of the initial equation (2.19)). From remarks *(i)* and *(ii)* we can derive that all the components of the non-trivial solution (x_0, y_0, z_0) of E_0, and so of (2.19), are bounded as follows

$$x_0, y_0, z_0 \leq b \left(\frac{3}{2}a\right)^{log_4 a} \left(\frac{3}{2}b\right)^{log_4 b}. \tag{2.38}$$

It is only left to formalize the recursion we have constructed in $I\Delta_0 + \Omega_1$. For the sake of clarity we will recall here all the Δ_0-formulas we need:

- x divides y: $\delta(x,y) = \exists z \leq y\ (xz = y)$
- x is a prime: $Pr(x) = \forall y \leq x\ (\delta(y,x) \rightarrow (y = 1 \vee y = x))$
- z is the *g.c.d.* of x and y:

$$\gamma(x,y,z) = \delta(z,x) \wedge \delta(z,y) \wedge \forall t \leq x\ (\delta(t,x) \wedge \delta(t,y)) \rightarrow \delta(t,z)$$

- x is square-free: $\sigma(x) = \forall y \leq x\ (Pr(y) \rightarrow \neg\delta(y^2,x))$
- x is a square modulo y: $\rho(x,y) = \exists z \leq x \wedge \exists r \leq y/2\ (x = r^2 + zy)$.

We can now express all conditions of the theorem with a Δ_0-formula:

$$\begin{aligned}\Theta(a,b) = 0 \leq a \wedge 0 \leq b \wedge \sigma(a) \wedge \sigma(b) \wedge \rho(a,b) \wedge \rho(b,a) \wedge \\ \wedge \forall d \leq a\ \left(\gamma(a,b,d) \rightarrow \rho\left(-\frac{ab}{d^2}, d\right)\right).\end{aligned} \tag{2.39}$$

We now make induction on the formula

$$\Lambda(t) = \forall a \leq t\ \forall b \leq t\ \ (ab \leq t \wedge b \leq a \wedge \Theta(a,b)) \longrightarrow$$

$$\exists x,y,z \leq b \left(\frac{3}{2}a\right)^{log_4 a} \left(\frac{3}{2}b\right)^{log_4 b}\ \neg(x = 0 \wedge y = 0 \wedge z = 0) \wedge (ax^2 + by^2 = z^2), \tag{2.40}$$

which is a Δ_0 formula that uses boundaries which are allowed by the axiom Ω_1.

For $t = 1$ the formula is true since in this case $a = b = 1$ and the equation $x^2 + y^2 = z^2$ has non-trivial solutions, for example $(1,0,1)$, which clearly satisfy $x,y,z \leq 1 \cdot \left(\frac{3}{2} \cdot 1\right)^{log_4 1} \left(\frac{3}{2} \cdot 1\right)^{log_4 1} = 1$.

Now suppose $\mathcal{M} \models \Lambda(t)$, with $t \in \mathcal{M}$, $t > 1$, and consider $t' = t + 1$

Let $a, b \in \mathcal{M}$, $a, b \leq t'$; and $ab = t'$ (if $ab < t' \Rightarrow ab \leq t$ and we already know $\Lambda(t)$ is true).

W.l.o.g. we can assume $b < a$, and hence apply the first step of the reduction and obtain the equation $Ax^2 + by^2 = z^2$, with $A < a/4$ and $\mathcal{M} \models \Theta(A,b)$.

Now $Ab < t'$, hence $Ab \leq t$, so by inductive hypothesis ($\mathcal{M} \models \Lambda(t)$), this equation admits a non-trivial solution (x_1, y_1, z_1) in $\mathcal{M}$, such that

$$x_1, y_1, z_1 \leq b \left(\frac{3}{2}A\right)^{log_4 A} \left(\frac{3}{2}b\right)^{log_4 b}.$$

From this we showed how we can get a non-trivial solution (x_0, y_0, z_0) of the equation $ax^2 + by^2 = z^2$, and by the previous observations we made we can state that

$$x_0, y_0, z_0 \leq b \left(\frac{3}{2}A\right)^{log_4 A} \left(\frac{3}{2}b\right)^{log_4 b} \left(\frac{3}{2}a\right) \leq b \left(\frac{3}{2}a\right)^{log_4 A+1} \left(\frac{3}{2}b\right)^{log_4 b}.$$

Since $A < a/4$, we have $log_4 A \leq log_4 a - 1$, and we can conclude that

$$x_0, y_0, z_0 \leq b \left(\frac{3}{2}a\right)^{log_4 a} \left(\frac{3}{2}b\right)^{log_4 b}.$$

Hence we have that $\mathcal{M} \models \Lambda(t')$, and this concludes the proof. □

Concluding remarks:

We have adapted a proof of Legendre's theorem suggested in [I-R]. Cassels in [C] obtained a linear bound of the solution in terms of the initial coefficients. Unfortunately the proof uses tools of geometry of numbers which seem to rely on the (full) pigeonhole principle, which is not known to be provable in $I\Delta_0 + \Omega_1$. Hence a possible further development in this subject could be to search for an alternative proof with no use of PHP, in order to obtain Cassels' result in $I\Delta_0 + \Omega_1$.

Bibliography

[B-I] Berarducci A. and Intrigila B., *Combinatorial principles in elementary number theory*, Annals of Pure and Applied Logic, vol. 55 (1991), pp. 35-50.

[C] Cassels J.W.S., *Rational Quadratic Forms*, Academic Press, 1978.

[D] D'Aquino P., *Pell equations and exponentiation in fragments of arithmetic*, Annals of Pure and Applied Logic, vol. 77 (1996), pp.1-34.

[D2] D'Aquino P., *Weak fragments of Peano Arithmetic*, in The Notre Dame Lectures, edited by P. Cholak, Association for Symbolic Logic, Lecture Notes in Logic, 18 (2005), pp. 149-185

[D3] D'Aquino P., *Local behaviour of Chebyshev teorem in models of* $I\Delta_0$, Journal of Symbolic Logic 57 (1) (1992), pp.12-27

[D-M] D'Aquino P. and A. Macintyre, *Non standard finite fields over* $I\Delta_0 + \Omega_1$, in Israel Journal of Mathematics 117, (2000), pp. 311-333.

[D-M2] D'Aquino P. and A. Macintyre, *Primes in Models of* $I\Delta_0 + \Omega_1$*: Density in Henselizations*, in New Studies in Weak Arithmetics, edited by P. Cegielski, C.Cornaros, C. Dimitracopoulos, CSLI Publications, Lecture Notes Number 211, pp. 85-91.

[D-M3] D'Aquino P. and A. Macintyre, *Quotient Fields of a Model of* $I\Delta_0 + \Omega_1$, Mathematical Logic Quarterly 47 (2001) 3, pp. 305-314.

[F-dG] Franciosi S., de Giovanni F., *Elementi di Algebra*, Aracne ed., 1995.

[G-D] Gaifman H., Dimitracopulos C., *Fragments of Peano's arithmetic and the MRDP theorem*, Logic and Algorithmic (Zurich, 1980), Univ. Genve, Geneva, 1982, pp. 187-206.

[H-P] Hajek P. and Pudlak P., *Metamathematics of first-order arithmetic*, Springer-Verlag, Berlin, 1998, second printing.

[H-W] Hardy G.H. and Wright E.M., *An Introduction to the Theory of Numbers*, (5th ed.) Oxford University Press, 1980.

[I-R] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, second edition, Springer, 1990.

[K] Kaye R., *Models of Peano Arithmetic*, Oxford University Press, Oxford, 1991.

[L] Lagarias J.C., *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, in Transactions of American Mathematical Society vol. 260, N. 2 (1980), pp. 485-508.

[M-M] Macintyre A., Marker D., *Primes and their residue rings in models of open induction*, Annals of Pure and Applied Logic, vol. 43 (1989), no. 1, pp 57-77.

[M-A] Manders K. L., Adleman L., *NP-complete decision problems for binary quadratics*, Journal of Computer and System Sciences, vol. 16 (1978), no. 2, pp. 168-184.

[Mar] Marker D., *Model Theory: an Introduction*, Springer-Verlag, 2002

[Ot] Otero M., *Models of open induction*, Ph.D. Thesis, Oxford University, 1991.

[Pa] Parikh R., *Existence and feasibility in arithmetic*, Journal of Symbolic Logic, vol. 36 (1976), no. 3, pp 494-508.

[P-W-W] Paris J., Wilkie A. and Woods A., *Provability of the Pigeonhole Principle and the existence of infinitely many primes*, Journal of Symbolic Logic 53, no. 4, (1988), pp 1235-1244.

[R] Rose H.E., *A Course in Number Theory*, 2nd ed. Oxford University Press, 1995.

[S] Shepherdson C.J., *A non-standard model for a free variable fragment of number theory*, Bull. Acad. Polon. Sci. Sr. Sci. Math. Astronom. Phys., vol. 12 (1964), pp. 79-86.

[W] Wilkie A., *Applications of complexity theory to Σ_0-definability problems in arithmetic*, in Pacholski et al. eds., Model theory, Algebra and Arithmetic, Proc. Karpacz, Poland 1979. Lecture Notes in Mathematics vol. 834, Springer 1980, pp. pp.363-369.

[W-P] Wilkie A. and Paris J., *On the scheme of induction for bounded arithmetic formulas*, Annals of Pure and Applied Logic 35 (1987), pp. 261-302

[Wo] Woods A., *Some problems in logic and number theory and their connections*, Ph.D. thesis, Manchester University, 1981.