

Algebraic Number Theory – Lecture 1

Martin Klazar

October 2, 2026

Abstract

We survey results in Chapters 1 and 2 of Mordell's book [3].

We denote by $\mathbb{N} = \{1, 2, \dots\}$ the set of natural numbers, by $\mathbb{N}_0 = \{0, 1, \dots\}$ the set of nonnegative integers, and by $\mathbb{Z}$ the ordered integral domain of integers; $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z}$. By $\mathbb{Q}$ we denote the ordered field of fractions (rational numbers), $\mathbb{R}$ is the complete ordered field of real numbers, and $\mathbb{C}$ is the algebraically closed field of complex numbers; $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Chapter 1 (pp. 1–2)

Introduction

We begin by interpreting, formalizing, correcting, and making precise the initial claims in the chapter. They are reductions between various Diophantine problems. “Obvious” in proofs below means that no proof is given in [3]; often the proof is labeled as such in [3].

Proposition 1 *Let $f \in \mathbb{Q}[x_1, \dots, x_n]$, $n \in \mathbb{N}$, be any polynomial, let $d \in \mathbb{N}$, let $X \subset \mathbb{Q}^n$, and let $g(\bar{x}) := d \cdot f(\bar{x})$. Then $g(\bar{x})$ is a rational polynomial and the equality of solution sets*

$$\{\bar{a} \in X : f(\bar{a}) = 0\} = \{\bar{a} \in X : g(\bar{a}) = 0\}$$

holds. Moreover, one can always choose $d \in \mathbb{N}$ such that $g \in \mathbb{Z}[x_1, \dots, x_n]$.

Proof. Obvious. □

Based on this reduction, the polynomials in equations in [3] are assumed to be integral.

Proposition 2 *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a homogeneous polynomial and let*

$$A = \{\bar{a} \in \mathbb{Z}^n \setminus \{\bar{0}\} : f(\bar{a}) = 0 \text{ \& } (a_1, \dots, a_n) = 1\}.$$

Then for every $d \in \mathbb{N}$ and every $\bar{a} \in A$, the n -tuple $d^{-1} \cdot \bar{a}$ is a nontrivial rational solution of the equation $f(\bar{x}) = 0$, and every nontrivial rational solution has this form.

Proof. Obvious. □

Here $(a_1, \dots, a_n) = 1$ means that the integers a_i are altogether coprime; if $m \in \mathbb{N}$ divides all of them, then $m = 1$. Nontrivial solutions are solutions different from $\bar{0}$.

Proposition 3 *For any nonzero polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$ with degree $d \in \mathbb{N}_0$, let*

$$g(y_1, \dots, y_{n+1}) := y_{n+1}^d \cdot f(y_1/y_{n+1}, \dots, y_n/y_{n+1}).$$

Then $g \in \mathbb{Z}[y_1, \dots, y_{n+1}]$ and is a nonzero homogeneous polynomial. As for the solution sets of the equations

$$f(\bar{x}) = 0 \text{ and } g(\bar{y}) = 0,$$

there is a bijection between the rational solutions $\bar{x}$ and the integral solutions $\bar{y}$ satisfying $y_{n+1} > 0$ \& $(y_1, \dots, y_{n+1}) = 1$.

Proof. Obvious. In fact, let $A \subset \mathbb{Q}^n$ and $B \subset \mathbb{Z}^{n+1}$ be the two solution sets. We consider a map $F: \mathbb{Q}^n \rightarrow \mathbb{Z}^{n+1}$ defined for

$$\bar{\alpha} = \left\langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \right\rangle = \left\langle \frac{a'_1}{d}, \dots, \frac{a'_n}{d} \right\rangle \in \mathbb{Q}^n,$$

where $a_i, b_i, a'_i \in \mathbb{Z}$, $(a_i, b_i) = 1$ for $i = 1, \dots, n$, and $d \in \mathbb{N}$ is the least common multiple of the denominators $b_1, \dots, b_n$, by

$$F(\bar{\alpha}) = \langle a'_1, \dots, a'_n, d \rangle.$$

Clearly, the restriction $F|_A$ is a bijection from A to B . □

Mordell has the conditions $y_{n+1} \neq 0$ and $(y_1, \dots, y_{n+1}) = 1$, and 1-1 correspondence (bijection). However, we think that with $y_{n+1} \neq 0$ one obtains 1-2 correspondence.

Proposition 4 *Let $f_i \in \mathbb{Z}[x_1, \dots, x_n]$ with $i = 1, \dots, r$ and $r \in \mathbb{N}$ be any polynomials, let $g(\bar{x}) = \sum_{i=1}^r f_i(\bar{x})^2$, and let $X \subset \mathbb{Q}^n$. Then $g(\bar{x})$ is an integral polynomial and the equality of solution sets*

$$\{\bar{a} \in X: f_1(\bar{a}) = f_2(\bar{a}) = \dots = f_r(\bar{a}) = 0\} = \{\bar{a} \in X: g(\bar{a}) = 0\}$$

holds.

Proof. Obvious. □

We summarize the necessary conditions for the solvability of Diophantine equations, given towards the end of the chapter, in one proposition.

Proposition 5 *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be any polynomial and let $X \subset \mathbb{Q}^n$. The following are necessary conditions for solvability of the equation $f(\bar{x}) = 0$ in X .*

1. *It is necessary that the equation $f(\bar{x}) = 0$ has a solution in $\mathbb{R}^n$.*
2. *Let $X \subset \mathbb{Z}^n$. It is necessary that the congruence $f(\bar{x}) \equiv 0 \pmod{p^a}$ has a solution in $\mathbb{Z}^n$ for every prime p and every $a \in \mathbb{N}$.*
3. *Let $X \subset \mathbb{Z}^n$, f be homogeneous, and let only nontrivial solutions of $f(\bar{x}) = 0$ be allowed. It is necessary that the congruence $f(\bar{x}) \equiv 0 \pmod{p^a}$ has a solution in $\mathbb{Z}^n$ with not all x_i divisible by p for every prime p and every $a \in \mathbb{N}$.*

Proof. Obvious. □

Chapter 2 (pp. 3–11)

Equations proved impossible by congruence considerations

We skip results in paragraph 1 which are rather trivial. From paragraph 2 on, things get more interesting. If it is not said else, the range for the unknowns x_i , $i \in \mathbb{N}$, and the parameters $a, b, c, d, e, k, p, \dots$ is $\mathbb{Z}$. We state the moduli in brackets after [3].

Proposition 6 (modulus 4) *The following holds.*

1. $x_1^2 + x_2^2 = 4x_3 + 3$ has no solutions.
2. $x_1^2 + x_2^2 = (4a + 3)x_3^2$ has only the trivial solution $x_1 = x_2 = x_3 = 0$.
3. If $a + b$ is even, $cd \equiv 1 \pmod{4}$, and k is odd, then $x_3^2 = (ax_1^2 + bx_2^2)^2 - 2k(cx_1^2 + dx_2^2)^2$ has only the trivial solution $x_1 = x_2 = x_3 = 0$,

Proof. 1. Squares modulo 4 are only $\{0, 1\}$.

2. Suppose that $x_1, x_2, x_3 \in \mathbb{N}_0$ is a nontrivial solution with $(x_1, x_2, x_3) = 1$. The case that x_3 is even is impossible because then one of x_1 and x_2 is odd and, modulo 4, the left-hand side is 1 or 2, but the right-hand side is 0. If x_3 is odd, then the right-hand side is 3 modulo 4, which is impossible by part 1. Thus, the only solution is the trivial one.

3. Suppose first that x_1 is odd and x_2 is even. We get the impossible mod 4 congruence $x_3^2 \equiv a^2 - 2c^2 \equiv -1$ or 2. Similarly, if x_1 is even and x_2 is odd. If both x_1 and x_2 are odd, we get the same impossible mod 4 congruence

$$\left(\frac{x_3}{2}\right)^2 \equiv \left(\frac{a+b}{2}\right)^2 - 2k\left(\frac{c+d}{2}\right)^2 \equiv -1 \text{ or } 2.$$

□

Proposition 7 (modulus 8) *The following holds.*

1. $x_1^2 + 2x_2^2 = 8x_3 + a$ for $a \in \{5, 7\}$ and $x_1^2 - 2x_2^2 = 8x_3 + b$ for $b \in \{3, 5\}$ have no solutions.
2. $x_1^2 + x_2^2 + x_3^2 = 4^a(8x_4 + 7)$, $a \in \mathbb{N}_0$, has no solutions.
3. We assume that $abc \neq 0$. Let a, b, c be odd and congruent mod 4, or let $a/2, b, c$ be odd and mod 8 let $b + c$ be a or 4. Then $ax_1^2 + bx_2^2 + cx_3^2 = 0$ has only the trivial solution $x_1 = x_2 = x_3 = 0$.

Proof. We only prove part 2. If $a > 0$, then all x_i are even (by modulus 4) and we can cancel factor 4. Thus we may assume that $a = 0$. However, squares modulo 8 are only $\{0, 1, 4\}$. □

Proposition 8 (modulus 16) $ax_1^4 + bx_2^4 + cx_3^4 + dx_4^4 = 0$ has only the trivial solution $x_1 = x_2 = x_3 = x_4 = 0$, if

$$\forall X \subset \{a, b, c, d\}, X \neq \emptyset: \sum_{x \in X} x \not\equiv 0 \pmod{16}.$$

Proof. Any nontrivial solution yields a solution with $(x_1, \dots, x_4) = 1$, hence with some odd x_i . However, $x^4 \equiv 1 \pmod{16}$ for odd x , and we contradict the assumption. $\square$

By the remark on [3, p. 6], the hypothesis is satisfied if, modulo 16, $\{a, b, c, d\}$ is a four-element subset of $\{1, 2, 3, 4, 5, 6\}$.

Proposition 9 (modulus 2^m) *If $a \equiv b \equiv c \equiv \pm 1 \pmod{4}$, then $ax_1^2 + bx_2^2 + cx_3^2 = 2dx_1x_2x_3$ has only the trivial solution $x_1 = x_2 = x_3 = 0$.*

Proof. Suppose that $x_i \in \mathbb{Z}$, $i = 1, 2, 3$, is a solution. We first show that all x_i are even. If one or all three are odd, we have the impossible congruence $1 \equiv 0 \pmod{2}$. If two are odd, we have the impossible congruence $1 + 1 \equiv 0 \pmod{4}$. Thus all are even, we write $x_i = 2X_i$ and $d' = 2d$, and we get for X_i (almost) the same equation

$$aX_1^2 + bX_2^2 + cX_3^2 = 2d'X_1X_2X_3.$$

It follows that $2^m \mid x_i$ for every $i = 1, 2, 3$ and every $m \in \mathbb{N}$. We conclude that the only solution is the trivial one. $\square$

Note that the polynomial $f(\bar{x})$ in the equation is nonhomogeneous, and therefore we cannot use the proof method of taking a nontrivial solution x_i with $(x_1, x_2, x_3) = 1$. The proof for the first time transforms the equation to itself. In other words, the proof is by the infinite descent.

Proposition 10 (modulus 32) *Suppose that the a_i and b_i , $i = 1, \dots, 4$, are all odd, that the a_i are all equal modulo 8, that the same holds for the b_i , and that $\sum_{i=1}^4 c_i \cdot \sum_{i=1}^4 d_i \equiv 0 \pmod{16}$. Then*

$$\sum_{i=1}^4 a_i x_i^2 \cdot \sum_{i=1}^4 b_i x_i^2 = 2k \sum_{i=1}^4 c_i x_i^2 \cdot \sum_{i=1}^4 d_i x_i^2$$

has only the trivial solution $x_1 = x_2 = x_3 = x_4 = 0$.

Proposition 11 (modulus 3) *$(3a + 1)x_1^2 + (3b + 1)x_2^2 = 3c$, $c \not\equiv 0 \pmod{3}$, has no solutions.*

Proof. Suppose that $x_i \in \mathbb{Z}$, $i = 1, 2$, is a solution. If some of the x_i is 0 modulo 3, we get that 3 divides c , which is excluded. If none of the x_i is divisible by 3, we get the impossible congruence $1 + 1 \equiv 0 \pmod{3}$. $\square$

Proposition 12 (modulus 9) *The following holds.*

1. $x_1^3 + x_2^3 + x_3^3 = 9x_4 \pm 4$ has no solutions.
2. $x_1^3 + 2x_2^3 + 4x_3^3 = 9x_4$ has only the trivial solution $x_1 = x_2 = x_3 = 0$.
3. If $a \equiv d \equiv 4 \pmod{9}$, $b \equiv 0 \pmod{3}$, and $c \equiv \pm 1 \pmod{3}$, then

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = z^3$$

has no solutions.

It follows that then $ax^3 + 3bx^2y + 3cxy^2 + dy^3 = 1$ has no rational solutions.

Proposition 13 (modulus 7)

$$(7a + 1)x_1^3 + (7b + 2)x_2^3 + (7c + 4)x_3^3 + (7d + 1)x_1x_2x_3 = 0$$

has only the trivial solution $\bar{x} = \bar{0}$.

Proposition 14 (modulus 49)

$$x_1^3 + 2x_2^3 = 7(x_3^3 + 2x_4^3)$$

has only the trivial solution $\bar{x} = \bar{0}$.

Proof. Suppose, for the contrary, that $x_i \in \mathbb{Z}$ for $i = 1, \dots, 4$ is a nontrivial solution with $(x_1, x_2, x_3, x_4) = 1$. Since cubes mod 7 are just $\{-1, 0, 1\}$, we see that 7 divides both x_1 and x_2 . We write $x_i = 7X_i$ for $i = 1, 2$ and get

$$7^2(X_1^3 + 2X_2^3) = x_3^3 + 2x_4^3.$$

So $x_i = 7X_i$ for $i = 3, 4$ and $(x_1, x_2, x_3, x_4) \geq 7$, which is a contradiction. $\square$

It follows that $x^3 + 7y^3 = 7(z^3 + 2)$ has no rational solution.

Proposition 15 (prime modulus p) *The following holds.*

1. If $p \equiv 3 \pmod{4}$ then

$$x_1^2 + x_2^2 - p(x_3^2 + x_4^2) = 0$$

has only the trivial solution $\bar{x} = \bar{0}$.

2. If $abc \not\equiv 0 \pmod{p}$, then

$$ax_1^3 + bp_2x_2^3 + cp^2x_3^3 = 0$$

has only the trivial solution $\bar{x} = \bar{0}$.

Proof. 1. Suppose that $x_i \in \mathbb{Z}$ for $i = 1, \dots, 4$ is a nontrivial solution with $(x_1, x_2, x_3, x_4) = 1$. Then $x_1^2 \equiv -x_2^2 \pmod{p}$. If one of x_1 and x_2 is nonzero mod p , we deduce that -1 is a square mod p , which is excluded by the assumption on p . Thus both x_1 and x_2 are divisible by p . We deduce in a similar way that the same holds for x_3 and x_4 . We get the contradiction that $(x_1, x_2, x_3, x_4) \geq p$.

2. Suppose again that $x_i \in \mathbb{Z}$ for $i = 1, \dots, 3$ is a nontrivial solution with $(x_1, x_2, x_3) = 1$. We easily deduce that, in this order, x_1 , x_2 , and x_3 are divisible by p , which is a contradiction. $\square$

“... since Artin has stated the *Conjecture*. A homogeneous equation $f(\bar{x}) = 0$ of degree r with $n > r^2$ variables always has a non-trivial integer solution in any p -adic field, i.e. as a congruence mod p^α , for all primes p and integers $\alpha > 0$. This has been long known for $r = 2$, $n = 5$ and is proved in Chapter 7; and it has been proven recently for $r = 3$. A counterexample with $r = 4$, $n = 18$ has just been found by Terjanian [4].”

Theorem 16 ([4]) *Let*

$$f(\bar{x}) = x_1^4 + x_2^4 + x_3^4 - x_2^2x_3^2 - x_3^2x_1^2 - x_2^2x_1^2 - x_1x_2x_3(x_1 + x_2 + x_3).$$

Then

$$f(\bar{x}) + f(\bar{y}) + f(\bar{z}) - 4(f(\bar{u}) + f(\bar{v}) + f(\bar{w})) = 0$$

has only the trivial zero solution since there is no 2-adic solution.

Proof. We assume for the contrary that $\bar{x}$, $\bar{y}$, $\bar{z}$, $\bar{u}$, $\bar{v}$, and $\bar{w}$ is a nontrivial solution with

$$(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v}, \bar{w}) = 1.$$

We first show that $f(\bar{x}) \equiv 1 \pmod{4}$, unless all three numbers x_1, x_2, x_3 are even. We have three cases.

1. Let x_i for $i = 1, \dots, 3$ be odd. Modulo 4, the first six summands in $f(\bar{x})$ cancel out, and we see that $f(\bar{x}) \equiv -x_2x_3 - x_3x_1 - x_1x_2 \equiv 1$.

2. If exactly two of x_1, x_2, x_3 are odd, say x_1 and x_2 are odd, and x_3 is even, then $f(\bar{x}) \equiv \cdots \equiv 1 \pmod{4}$.
3. Similarly, if exactly one of x_1, x_2, x_3 is odd, say x_1 is odd, and x_2 and x_3 are even, then $f(\bar{x}) \equiv \cdots \equiv 1 \pmod{4}$.

Thus $f(\bar{x})$ is even only if $\bar{x}$ is even. The equation requires that all three of $\bar{x}, \bar{y}, \bar{z}$ are even; otherwise, we get a congruence that is impossible modulo 4. Thus we can write $\bar{x} = 2\bar{X}, \bar{y} = 2\bar{Y}, \bar{z} = 2\bar{Z}$ and by canceling the factor 4 we get that

$$f(\bar{u}) + f(\bar{v}) + f(\bar{w}) - 4(f(\bar{X}) + f(\bar{Y}) + f(\bar{Z})) = 0.$$

The same argument now gives that also all three of $\bar{u}, \bar{v}, \bar{w}$ are even. We have a contradiction with the assumed summary coprimality. $\square$

“By ideas completely different from those above, a non-constructive proof has been given of the

Theorem 17 ([1]) *For every natural number r , there exists a fixed set $S(r)$ of primes such that for every prime p not in $S(r)$, every homogeneous equation $f(\bar{x}) = 0$ of degree r and with $n > r^2$ variables, always has a non-trivial solution in the p -adic field.”*

Of course, “fixed” should be “finite”.

References

- [1] J. Ax and S. Kochen, Diophantine problems over local fields I, *Amer. J. Math.* **87** (1965), 605–630
- [2] L. E. Dickson, Fallacies and misconceptions in Diophantine analysis, **27** (1921), 312–319
- [3] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York 1969
- [4] G. Terjanian, Un contre-exemple à une conjecture d’Artin, *Comptes Rendus Acad. Sci. Paris* (1966), 612