Summary

Let T be a homogeneous polynomial in three variables and with rational integer coëfficients. As a generalisation of Thue's equation we consider the ternary form equation $T(x, y, z) = 1$ in the integral unknowns x, y, z. We prove some general results when the degree of T is at most three and make some modest inroads into the case deg$T > 3$. Generalisations to algebraic number fields are considered at the same time.

Ternary Form Equations

F. Beukers

January 8, 2007

1.1 Introduction

Let K be an algebraic number field, which we assume embedded in $\mathbf{C}$, and let $\mathcal{O}$ be its ring of integers. Let S be a finite set of places of K, *including all infinite ones.* An element $a \in K$ is called an S-integer if $|a|_v \le 1$ for all $v \notin S$. The set of S-integers in K is denoted by $\mathcal{O}_S$. The units in $\mathcal{O}_S$ are called S-units, i.e. elements $a \in K$ such that $|a|_v = 1$ for all $v \notin S$. The set of S-units is denoted by $\mathcal{O}_S^*$. This group is known to have rank $|S| - 1$.

A diophantine equation which has been studied extensively this century is the so-called *Thue-Mahler equation*

$$F(x, y) \in \mathcal{O}_S^*$$

where $F \in \mathcal{O}_S[X, Y]$ is a binary form (=homogeneous polynomial in two variables) with non-zero discriminant. Actually, we must state the problem more accurate here. Let $\mathcal{F}$ be the fractional $\mathcal{O}_S$-ideal generated by the coefficients of F and consider the equation

$$(F(x, y)) = \mathcal{F} \cdot (x, y)^d \tag{B}$$

where $(F(x, y))$ denotes the (fractional) $\mathcal{O}_S$-ideal generated by $F(x, y)$ and d is the degree of F. We shall refer to such equations as *binary form equations.* The unknowns lie in K. Any two solutions $(x_1, y_1), (x_2, y_2)$ which are projectively equivalent as elements of $\mathbf{P}^1(K)$ are considered as equivalent. When counting solutions we count equivalence classes of solutions.

When $\deg F = 1$ there exist infinitely many solutions. When $\deg F = 2$ we have two cases. The first is when F has zeros in K and $|\mathcal{O}_S^*| < \infty$ or F has zeros quadratic over K and no place of S splits in the quadratic extension. Then there are at most finitely many solutions and examples are $xy = \pm 1$ and $x^2 + y^2 = \pm 1$ in $\mathcal{O}_S = \mathbf{Z}$. In the second, remaining, case there exist either no solutions at all or infinitely many, examples being Pell's equation for infinitely many solutions and $2x^2 - 5y^2 = \pm 1$ having no solutions in $\mathbf{Z}$. As soon as $\deg F \geq 3$ the results are less trivial. It is a well-known result of Thue-Siegel-Mahler that there are only finitely many (equivalence classes of) solutions. Among the most striking results on binary form equations are Baker's upper bound for the height of solutions [Ba, ST] and the Evertse-Bombieri-Schmidt [E1, BS] bounds for the number of solutions, which depend only on K, $\deg F$ and $|S|$.

Let us give a geometrical interpretation of binary form equations. Suppose x, y is a solution to (B). Then we have for any $v \notin S$ that $v(\mathcal{F}^{-1}F(x,y)) = (x,y)^d$, in other words, modulo every prime outside of S the projective point $(x : y)$ stays away from the points defined by $F(X,Y) = 0$. More precisely, let (F) be the zero divisor of F and extend $\mathbf{P}^1 \setminus (F)$ over $\mathrm{Spec}(\mathcal{O}_S)$ in the obvious way. Then any solution of (B) yields a section of $\mathbf{P}^1 \setminus (F) \to \mathrm{Spec}(\mathcal{O}_S)$. By abuse of language an equivalence class of solutions of (B) will be called an S-integral point on $\mathbf{P}^1 \setminus (F)$.

More generally, let C be any geometrically irreducible curve defined over K and let D be a divisor (over K) with simple points. Suppose we have a model of $C \setminus D$ over $\mathrm{Spec}(\mathcal{O}_S)$ for some S. A theorem of Siegel and Mahler [La, Chapter 8] then states that there are at most finitely many S-integral points in the following cases, $g(C) = 0$ and $|D| \geq 3$, $g(C) \geq 1$ and $|D| \geq 1$. In addition, when $g(C) \geq 2$ we know by Faltings' theorem that $C(K)$ is finite. Notice that the binary form equation is an example of the case $g(C) = 0$, and $|D| \geq 3$ corresponds to $\deg F \geq 3$.

We now turn to the subject of this paper. Let $T \in K[X,Y,Z]$ be a ternary form (=homogeneous polynomial in three variables) which may be reducible over $\mathbf{C}$, but has no multiple components. Let d be the degree of T and let $\mathcal{T}$ be the fractional $\mathcal{O}_S$-ideal generated by the coefficients of T. Consider the *ternary form equation*

$$(T(x,y,z)) = \mathcal{T} \cdot (x,y,z)^d \tag{T}$$

in the unknowns $x, y, z \in \mathcal{O}_S$. Any two solutions which are projectively equivalent as elements of $\mathbf{P}^2(K)$ are considered equivalent. Again, when counting solutions, we count equivalence classes of solutions.

Just as in the binary case we can give a geometrical interpretation. Let C be the projective curve defined by $T(X,Y,Z) = 0$. Extend $\mathbf{P}^2 \setminus C$ over $\mathrm{Spec}(\mathcal{O}_S)$ in the trivial way. Then any solution of (T) yields a section of $\mathbf{P}^2 \setminus C \to \mathrm{Spec}(\mathcal{O}_S)$. Again we call an equivalence class of solutions to (T) an S-integral point on $\mathbf{P}^2 \setminus C$.

Contrary to the binary case, literature on ternary form equations is very scant. Of the few references I could find, the most significant is from D.H.Lehmer [Le] on the equation $x^3 + y^3 + z^3 = 1$ in $x, y, z \in \mathbf{Z}$. We shall refer to his results in a few moments. A more recent paper is [Si], containing many speculations and some results on the asymptotics of numbers of integral points. Finally we mention a paper by Mordell [Mo] which has some relevance to the topic.

Let us formulate our first question. As an example, when $K = \mathbf{Q}$ and $S = \{\infty\}$, consider the equation

$$x^d + y^d + z^d = 1$$

in $x, y, z \in \mathbf{Z}$ and where d is an odd positive integer. For any such d the triples $(t, -t, 1)$ where $t \in \mathbf{Z}$ form an infinite set of inequivalent solutions. Notice however that they all lie on the projective straight line $x + y = 0$. This is an example of what we will call an *exceptional curve.* Very often we will see that (T) has infinitely many solutions but which are concentrated on a finite number of algebraic curves. A subset of $\mathbf{P}^2$ which is not contained in a finite union of algebraic curves is said to lie *Zariski dense* in $\mathbf{P}^2$.

Question 1.1.1 *When does the solution set of* (T) *lie Zariski dense in* $\mathbf{P}^2$*?*

From Lehmer [Le] it follows that the solutions to $x^3+y^3+z^3 = 1$ in $x, y, z \in \mathbf{Z}$ lie indeed Zariski dense. In fact, a computer search with the constraints $0 < |x| \leq |y| \leq |z|,\ |y| < 100,000$ yielded 78 solutions. See [GLS] for some more numerical results and some interesting problems, as well as the recent paper [HR]. Computer searches for some other cubic ternary form equations were equally rewarding in a small but continuing trickle of solutions. Compared to these, computer searches in the cases $\deg(T) \geq 4$ reveal a true desert. Discarding the (trivial) solutions on exceptional curves one usually finds a handfull of small ones (if any) and that is it. This watershed between the cases $\deg(T)$ is 3 and 4 is predicted by Vojta's Main Conjecture [V, Conjecture 3.4.3]. From this conjecture we can deduce the following conjecture.

Conjecture 1.1.2 *When the curve defined by* $T(X, Y, Z) = 0$ *has normal crossings and* $\deg(T) \geq 4$*, the solution set to* (T) *is contained in a finite set of plane algebraic curves.*

It is probably possible to weaken the condition 'normal crossing', but lacking any evidence we dare not make any improved conjecture.

To get any grasp on Question 1.1.1 we must get an idea of the shape of the exceptional curves. Let us consider the curves in $\mathbf{P}^2$ which contain infinitely many solutions of (T) . Let X be such an irreducible curve. First of all we remark that, containing infinitely many K-rational points, X can be given by an equation over K. Let $\tilde{X}$ be a normalisation of X and let D be the divisor on $\tilde{X}$ cut out by the curve C. Since there are infinitely many S-integral points on $\tilde{X} \setminus D$ we conclude from the Siegel-Mahler theorem that $g(\tilde{X}) = 0$ and $|D| \leq 2$. In other words, $X \setminus X \cap C$ is the image of a morphism from $\mathbf{P}^1 \setminus \{0\}$ or $\mathbf{P}^1 \setminus \{0, \infty\}$ to $\mathbf{P}^2 \setminus C$. Forgetting for the moment that X is defined over K we adopt this property as definition

Definition 1.1.3 *Let C be an algebraic curve in $\mathbf{P}^2$ defined over $\mathbf{C}$ and possibly reducible. An exceptional curve in $\mathbf{P}^2 \setminus C$ is the image of a non-constant morphism from $\mathbf{P}^1 \setminus V$ to $\mathbf{P}^2 \setminus C$, where $V = \{0\}$ or $\{0, \infty\}$.*

Before answering Question 1.1.1 it seems appropriate to study the following geometrical question first.

Question 1.1.4 *Let C be a plane projective curve over $\mathbf{C}$ without multiple components. Does the union of all exceptional curves in $\mathbf{P}^2 \setminus C$ lie Zariski dense in $\mathbf{P}^2$?*

Notice that, when $\deg(C) \leq 3$, the answer is *yes*. If $\deg(C) \leq 2$ every straight line in $\mathbf{P}^2$ is exceptional. If $\deg(C) = 3$ and C is non-singular take the set of tangents at the points of C. If $\deg(C) = 3$ and C is singular take the pencil of straight lines passing through a singularity. Whether or not a positive answer to Question 1.1.4 implies a positive answer to Question 1.1.1 is a subtle problem. When $\deg(C) \leq 3$ we shall deal with this in section 3 and show that under very mild conditions the solutions of (T) lie Zariski dense.

In section 4 we shall say as much as we can about the cases $\deg(C) \geq 4$. The latter cases are notoriously difficult to handle. As an example consider the equation $x^5 - y^2 z^3 = 1$. Presumably this simple looking equation has only the trivial solutions with $x = 1$, but I could not prove it. As a side remark we note that a number of the form $y^2 z^3$ is a socalled *powerful* number, all of whose primes occur with exponent at least 2. So the equation $x^5 - y^2 z^3 = 1$ can be reformulated as the question for which $x \in \mathbf{Z}$ the number $x^5 - 1$ is powerful. Up to this day not a single polynomial $P \in \mathbf{Z}[X]$ with at least three distinct roots is known for which the finiteness of the set of powerful values is proved. That P requires at least three distinct roots is illustrated by $x^2 - 1 = 8y^2$ which is a Pellian equation having infinitely many solutions. Finally we remark that the finiteness of the set of powerful values of $x(x^2-1)$ implies the existence of infinitely many primes p for which $2^p \not\equiv 2 \pmod{p^2}$ (see [Ri, p 270ff]). There are other cases of ternary form equations which give rise to diophantine problem that look amusing, but seem extremely hard to crack. Consider for example

$$(x^2 + y^2 + z^2)yz \in \mathcal{O}_S^*$$

in $x, y, z \in \mathcal{O}_S^*$. This implies that $y, z \in \mathcal{O}_S^*$ and $x^2 + y^2 + z^2 \in \mathcal{O}_S^*$. Hence x^2 is the sum of three S-units. The difficult question seems to be, how often can the sum of three S-units be a square? One more example, consider

$$x^5 + y^5 - zx^2y^2 = 1 \qquad x, y, z \in \mathbf{Z}.$$

This is equivalent to the problem, find $x, y \in \mathbf{Z}$ such that both $x^5 \equiv 1(\text{mod } y^2)$ and $y^5 \equiv 1(\text{mod} x^2)$.

Finally, in section 5 we collect some results on the set of exceptional curves corresponding to a given curve C.

Remark. There are a number of topics in diophantine equations which are closely related to ternary form equations. We mention for example the work of Manin et al where they count solutions of height bounded by H of $x^3+y^3+z^3 = 1$ and similar equations. Asymptotic results of these counting procedures can be found in [MaTsch]. It might be of interest to know what the asymptotics for integral solutions of $x^3 + y^3 + z^3 = 1$ might be. There is also the remark that when studying $T(x, y, z) = 1$ we are actually looking at points on the projective surface $T(x, y, z) = w^d$ which are integral with respect to $w = 0$. When $d = 4$ and the surface is a K3-surface, there can be a Zariski-dense set of rational points on it, which conjecturally does not happen for integral points. Finally one can apply the ABC-conjecture to three term equations like $x^5 - y^2z^3 = 1$ and see what can be expected.

Acknowledgement. I would like to thank Frans Oort for goading me into a geometrical approach of the subject, which turned out to be quite illuminating.

1.2 Technical preparations

In this section we gather some results which are a basic tool in the sections that follow. The symbols K, S, $\mathcal{O}_S$, $\mathcal{O}_S^*$ have the same meaning as in the introduction. The notation (α, β, γ) stands for the fractional $\mathcal{O}_S$-ideal generated by $\alpha, \beta, \gamma \in K$. To avoid confusion with coordinates of a point in $\mathbf{P}^2$ we denote a projective point by $(\alpha : \beta : \gamma)$.

Theorem 1.2.1 *Let L be a straight line in $\mathbf{P}^2$ defined over K. Let P be a K-rational point on L. Then there exists an S-integral point on $L \setminus P$. Moreover, let $P = (p : q : r)$ and let $Q = (x_0 : y_0 : z_0)$ be an S-integral point on $L \setminus \{P\}$. Then, for any $\mu \in (x_0, y_0, z_0)(p, q, r)^{-1}$ we have that $(x_0 + \mu p : y_0 + \mu q : z_0 + \mu r)$ is S-integral on $L \setminus \{P\}$. Consequently, there exist infinitely many S-integral points on $L \setminus \{P\}$.*

Remark. This theorem does not immediately generalise to rational curves of higher degree. Consider for example the conic $x^2 - 2y(y + 5z) = 0$ and the point $P = (0 : 0 : 1)$. We take $K = \mathbf{Q}$ and $S = \{\infty\}$. Note that any rational point reduces to P modulo 5. Hence there cannot be any S-integral points on the conic minus P.

Proof. Suppose L is given by $ax+by+cz = 0$, $a, b, c \in K$ and $P = (p : q : r)$. The problem comes down to finding points $X = (x : y : z)$, $x, y, z \in K$ such that $X \in L$ and

$$(qz - ry, pz - rx, py - qx) = (x, y, z)(p, q, r).$$

Since $\subset$ is trivial, it remains to show the existence of $x, y, z \in K$ such that

$$(x, y, z) \subset (qz - ry, pz - rx, py - qx)(p, q, r)^{-1} \tag{1}$$

Without loss of generality we may assume $r = 1$. We take $X = (b + \mu p : -a + \mu q : \mu)$. Then automatically $X \in L$ and (1) becomes

$$(b + \mu p, -a + \mu q, \mu) \subset (a, b, c)(p, q, 1)^{-1}.$$

Putting $J = (a, b, c)(p, q, 1)^{-1}$ this comes down to determining $\mu \in K$ such that

$$\mu, \quad b + \mu p, \quad -a + \mu q \in J.$$

To determine such μ we observe that the ideal $(p, q)(a, b, c)$ contains $cp, cq, c = -ap - bq$. Hence $c \in (p, q)J$. Choose $j_1, j_2 \in J$ such that $c = pj_1 + qj_2$. We also have $c = -ap - bq$. Subtraction of these equalities gives $p(a + j_1) + q(b + j_2) = 0$, hence $(j_1 + a)/q = (-j_2 - b)/p$. If $(j_1 + a)/q \in J$ we are done by simply taking $\mu = (j_1 + a)/q$, which yields $\mu \in J$, $-a + \mu q = j_1$, $b + \mu p = -j_2$.

If however $(j_1 + a)/q \notin J$ we adapt our choice of j_1, j_2 as follows. Let $\gamma \in J \cap \frac{q}{p} J$. Then $j_1 - \gamma$ and $j_2 + \frac{p}{q}\gamma$ are both in J and they satisfy $p(j_1 - \gamma) + q(j_2 + \frac{p}{q}\gamma) = c$. It thus remains to show that there exists $\gamma \in J \cap \frac{q}{p} J$ such that $(j_1 - \gamma + a)/q \in J$. In other words, we must show that

$$\frac{j_1 + a}{q} \in J + p^{-1}J \cap q^{-1}J. \tag{2}$$

Notice that the fractional ideal $J + p^{-1}J \cap q^{-1}J$ is the set of $\alpha \in K$ such that

$$v(\alpha) \geq \min(v(J), v(J) + \max(-v(p), -v(q)))$$

for every valuation $v \notin S$. We must show that $v((j_1 + a)/q)$ satisfies these inequalities. Suppose $v(p) \geq v(q)$. Then

$$\begin{aligned} v((j_1 + a)/q) &\geq -v(q) + \min(v(j_1), v(a)) \\ &\geq -v(q) + \min(v(J), v(J) + \min(0, v(p), v(q))) \\ &= v(J) + \min(0, -v(q), v(p) - v(q)) \\ &= v(J) + \min(0, -v(q)) \\ &= v(J) + \min(0, \max(-v(p), -v(q))) \end{aligned}$$

The last two lines follow from $v(p) \geq v(q)$. If $v(p) < v(q)$ we find, similarly,

$$v((j_1 + a)/q) = v((j_2 + b)/p) \geq v(J) + \min(0, \max(-v(p), -v(q))).$$

Hence (2) is satisfied.

To prove the infinity of the number of points notice that whenever $\mu \in (x_0, y_0, z_0)(p, q, r)^{-1}$ we have that $(x_0, y_0, z_0) \supset (x_0 + \mu p, y_0 + \mu q, z_0 + \mu r)$. This proves our theorem. □

Proposition 1.2.2 *Let $A, B, C \in \mathbf{P}^2(\bar{K})$, not all three on a straight line. Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ be the ideals generated by the coefficients of A, B, C respectively. We distinguish the following cases,*

i) *$A, B, C \in \mathbf{P}^2(K)$.*

ii) *$A \in \mathbf{P}^2(K)$, B is defined over a quadratic extension M of K and C is its conjugate. We let S' be the set of places of M above S.*

iii) *A is defined over a cubic extension N of K and B, C are its conjugates. We let S'' be the set of places of N above S.*

In each of the three cases let $\delta = (\det(A,B,C))\mathcal{A}^{-1}\mathcal{B}^{-1}\mathcal{C}^{-1}$*. Let* $U = \{x \in \mathcal{O}_S^* \mid x \equiv 1 \pmod{\delta}\}$ *and define* U'*,* U'' *similarly by replacing* $\mathcal{O}_S^*$ *with* $\mathcal{O}_{S'}^*$ *and* $\mathcal{O}_{S''}^*$ *respectively. Then we have in each of the cases the following result,*

i) To any triple $\lambda, \mu, \nu \in U$ *there exists* $T \in GL(3, \mathcal{O}_S)$ *such that* $T(A) = \lambda A,\ T(B) = \mu B,\ T(C) = \nu C$*. Here, and in the following cases,* T *acts on the projective points written columnwise.*

ii) To any pair $\lambda \in U$*,* $\mu \in U'$ *there exists* $T \in GL(3, \mathcal{O}_S)$ *such that* $T(A) = \lambda A,\ T(B) = \mu B$*.*

iii) To any $\lambda \in U''$ *there exists* $T \in GL(3, \mathcal{O}_S)$ *such that* $T(A) = \lambda A$*.*

Proof. This is quite straightforward and we sketch it only in case iii). Let $\bar{\lambda}$ and $\bar{\bar{\lambda}}$ be such that $\bar{\lambda}$ is the conjugate of λ which lies in the field generated by the coordinates of B, and similarly for $\bar{\bar{\lambda}}$. Let $\mathcal{M}$ be the matrix spanned by the coordinates of A, B, C written columnwise. Let $\mathcal{L}$ be the diagonal matrix $\mathrm{diag}(\lambda, \bar{\lambda}, \bar{\bar{\lambda}})$. We simply take

$$T = \mathcal{M}\mathcal{L}\mathcal{M}^{-1}.$$

First, T is independent of the choice of coordinates of A, B, C. Secondly, because of Galois invariance and because we took $\lambda \equiv 1 \pmod{\delta}$ the coordinates of T are in $\mathcal{O}_S$. Thirdly, $\det(T) = \lambda\bar{\lambda}\bar{\bar{\lambda}} \in \mathcal{O}_S^*$.

Theorem 1.2.3 *Let* C *be a line or an irreducible conic in* $\mathbf{P}^2$*, defined over* K*. Let* $A, B \in C$ *be distinct points. We distinguish the following cases,*

i) A, B *are defined over* K*.*

ii) A *is defined over a quadratic extension* M *of* K *and* B *is its conjugate.*

Let V *be the set of* S*-integral points on* $C \setminus \{A, B\}$*. Then* V *is finite in the following cases: case i) and* $\mathcal{O}_S^*$ *finite, case ii) and no place of* S *splits in* M*. In all other cases* V *is either empty or infinite.*

Remark. To mention a very simple case, take $K = \mathbf{Q}$, $S = \infty$ and take for C the straight line $Z = 0$. For A and B take $(0:1:0)$ and $(1:0:0)$. A point $(x:y:0)$, $x, y \in \mathbf{Z}$ can only be S-integral on $C \setminus \{A, B\}$ if $xy = \pm 1$, i.e. x and y contain no prime divisors. So the only possibilities are $(1:1:0)$ and $(1:-1:0)$. If, on the other hand, we take $S = \{\infty, p\}$ for some prime p then any point of the form $(1:\pm p^k:0)$, $k \in \mathbf{Z}$ is S-integral. So there exist infinitely many.

Remark. Let $M = K(\sqrt{d})$. To get an idea of the splitting condition for elements of S we remark that there exists an infinite valuation of K which splits in M/K unless K is totally real and d is totally negative. To mention a very simple case take $K = \mathbf{Q}$, $S = \infty$ and take for C the straight line $Z = 0$. For A and B take $(\sqrt{2} : 1 : 0)$ and $(\sqrt{2} : -1 : 0)$. Any point $(x : y : 0)$ with $x, y \in \mathbf{Z}$ satisfying $x^2 - 2y^2 = 1$ can be seen to be an S-integral point on $L \setminus \{A, B\}$. So there are infinitely many of them. If, on the other hand, we take $A = (\sqrt{-1} : 1 : 0)$ and $B = (\sqrt{-1} : -1 : 0)$ any S-integral point on $L \setminus \{A, B\}$ must have the form $(x : y : 0)$ with $x, y \in \mathbf{Z}$ and $x^2 + y^2 = 1$. So there exist only finitely many.

Proof. Let us first construct an auxiliary point P. In case C is a straight line we take for P any K-rational point outside of C. In case C is a conic we take for P the point of intersection of the tangents at C through the points A and B. Note that P is K-rational in both cases. Consider the function

$$u(x) = \det(A, P, x)/\det(B, P, x))$$

on $\mathbf{P}^2$. When C is a line, $u(x)$ is a coordinate on C, when C is a conic, $u(x)$ has order 2 on C.

Suppose in case i) that $\mathcal{O}_S^*$ is infinite and in case ii) that at least one place of S splits in M. Consider the pencil of conics

$$\alpha \det(A, P, x) \det(B, P, x) + \beta \det(A, B, x)^2 = 0.$$

In particular, when C is a conic, it is a member of this pencil. We now choose units λ, μ, ν as follows. In case i) we take them to be S-units, in case ii) we take λ an S-unit, μ an S'-unit and ν its conjugate. Moreover, they should be in the subgroups U, U' as prescribed by Proposition 1.2.2. Finally we want that $\lambda^2 = \mu\nu$. Construct the projective automorphism T as in Proposition 1.2.2 so that we have

$$T(A) = \mu A, \qquad T(B) = \nu B, \qquad T(P) = \lambda P.$$

Notice that

$$\begin{aligned}
\det(A, P, Tx) &= \nu \det(A, P, x) \\
\det(B, P, Tx) &= \mu \det(A, P, x) \\
\det(A, B, Tx) &= \lambda \det(A, B, x)
\end{aligned}$$

Hence, because of $\lambda^2 = \mu\nu$, T stabilises the conics of our pencil, in particular C.

Notice that $u(Tx) = (\nu/\mu)u(x)$. Suppose that V is not empty and that $x_0 \in V$. In particular, $u(Tx_0) = (\nu/\mu)T(x_0)$. The point Tx_0 is again S-integral on $C \setminus \{A, B\}$. Because of our assumption that $\mathcal{O}_S^*$ infinite in case i) and at least one $v \in S$ splits in M in case ii), there are infinitely many choices for ν/μ and hence infinitely many S-rational points on $C \setminus \{A, B\}$.

Suppose in case i) that $\mathcal{O}_S^*$ is finite and in case ii) that no place of S splits in M. Let x be an S-integral point on $C \setminus \{A, B\}$ and put $x = \alpha A + \beta B + \gamma P$. Denote by $\mathcal{A}, \mathcal{B}, \mathcal{P}$ the ideals generated by the coefficients of A, B, P respectively. The condition that x does not reduce to A for any $v \notin S$ implies that for every $v \notin S$,

$$|\alpha\mathcal{A}|_v \le \max(|\beta\mathcal{B}|_v, |\gamma\mathcal{P}|_v).$$

Similarly

$$|\beta\mathcal{B}|_v \le \max(|\alpha\mathcal{A}|_v, |\gamma\mathcal{P}|_v).$$

When C is a straight line we have $\gamma = 0$ and $|\alpha\mathcal{A}|_v = |\beta\mathcal{B}|_v$ for every $v \notin S$. Notice also that $|u(x)|_v = |\beta/\alpha|_v$. Hence, if C is a straight line, $|u(x)|_v = |\mathcal{A}/\mathcal{B}|_v$. So in case i) $u(x), x \in V$ has only finitely many values. In case ii), we know by construction that $u(x)$ is a norm one element of M. Hence there are finitely many possibilities as well.

When C is an irreducible conic things are only slightly more involved. The conic can be described by the equation

$$\det(A, P, x)\det(B, P, x)/\det(A, B, x)^2 = \delta$$

for some fixed $\delta \in K$. Notice that for any $x \in V$ we have $\alpha\beta/\gamma^2 = \delta$. If $|\alpha\mathcal{A}|_v \ne |\beta\mathcal{B}|_v$ fpr some $v \notin S$, we have necessarily

$$|\gamma\mathcal{P}|_v \ge \max(|\beta\mathcal{B}|_v, |\alpha\mathcal{A}|_v).$$

Take squares and divide by $|\gamma\mathcal{P}|_v^2 = c_v|\beta\mathcal{B}|_v|\alpha\mathcal{A}|_v$ where $c_v = |\mathcal{P}^2/\mathcal{B}\mathcal{A}|_v|\delta|_v^{-1}$. Hence

$$c_v \ge \max(|\beta\mathcal{B}/\alpha\mathcal{A}|_v, |\alpha\mathcal{A}/\beta\mathcal{B}|_v)$$

We conclude that $|\beta/\alpha|_v$ is 1 for almost all $v \notin S$. and that it has finitely many possible values for the remaining v. Hence there are at most finitely many possibilities for α/β, hence V is finite.

Remark. We expect that a similar theorem holds for higher degree rational curves, but did not see how to prove this.

1.3 The case 'degree ≤ 3'

In this section we show that if $\deg(T) \leq 3$, equation (T) has a Zariski dense set of solutions under fairly mild conditions.

Theorem 1.3.1 *Let L be a straight line in $\mathbf{P}^2$ defined over K. Then the set of S-integral points on $\mathbf{P}^2 \setminus L$ is Zariski dense in $\mathbf{P}^2$.*

Remark. The fact that for any straight line L there exists an S-integral point on $\mathbf{P}^2 \setminus L$ is equivalent to saying that $\mathbf{P}^2 \setminus L$ is isomorphic over $\mathrm{Spec}(\mathcal{O}_S)$ to the affine plane. The infinity of the number of S-integral points on $\mathbf{P}^2 \setminus L$ is then obvious.

Proof. Choose a point $P \in L$, defined over K. Let L_P be any line through P, distinct from L modulo every prime outside of S. According to the dual version of Theorem 1.2.1 there exist infinitely many such lines. For any such line L_P there exist infinitely many S-integral points on $L_P \setminus \{P\}$. By varying L_P we find a Zariski dense set of S-integral points on $\mathbf{P}^2 \setminus L$. □

Theorem 1.3.2 *Let C be a geometrically irreducible conic defined over K. By K_v we shall denote the completion of K with respect to a valuation v.*

- *i) Suppose that $C(K_v)$ is empty for every place $v \in S$. Then there exist at most finitely many S-integral points on $\mathbf{P}^2 \setminus C$.*
- *ii) Suppose that for at least one place $v \in S$ the equation $C(K_v)$ is not empty. Then the set of S-rational points on $\mathbf{P}^2 \setminus C$ is either empty or Zariski dense in $\mathbf{P}^2$.*

Remark. Let us point out the necessity of the conditions in the case $K = \mathbf{Q}$ and $S = \{\infty\}$. The form $X^2 + Y^2 + Z^2$ does not represent zero in $\mathbf{R} = K_\infty$ and sure enough, $x^2 + y^2 + z^2 = \pm 1$ has only finitely many solutions. The form $2X^2 + 5Y^2 - 5Z^2$ does represent zero in $\mathbf{R}$ but $2x^2 + 5y^2 - 5z^2 = \pm 1$ does not have any solution, as one can see by looking modulo 5.

Remark. The 'royal road' to proving the above theorem would be to remark that the condition on the places in S guarantees the existence of an infinite projective automorphism group of $\mathbf{P}^2$ over $\mathrm{Spec}(\mathcal{O}_S)$ which stabilises the conic $T(x, y, z) = 0$. Images of our solution under the group elements yield a Zariski dense set of solutions. However, the proof we present below uses a shortcut, thus avoiding a discussion of non-ramifying primes from S in the quaternion algebra associated to T.

Proof. Part i). Let C be given by the equation $T(x, y, z) = 0$. For any place v the function

$$|T(x, y, z)|_v / \max(|x|_v, |y|_v, |z|_v)^2$$

is continuous on $\mathbf{P}^2(K_v)$ with the v-adic topology. Since $\mathbf{P}^2(K_v)$ is compact, our function has a minimum which we denote by m_v. By assumption, we have $m_v > 0$ for any $v \in S$. Let now $(x : y : z)$ be a solution of our ternary form equation (T). For any $v \notin S$ we have

$$|T(x, y, z)|_v = T_v \max(|x|_v, |y|_v, |z|_v)^2$$

where T_v is the v-adic valuation of the coefficient ideal of T. Note that $T_v = 1$ with finitely many exceptions for v. When $v \in S$ we have

$$|T(x, y, z)|_v \geq m_v \max(|x|_v, |y|_v, |z|_v)^2.$$

Take the product over all valuations,

$$1 = \prod_v |T(x, y, z)|_v \geq \left(\prod_{v \notin S} T_v\right) \left(\prod_{v \in S} m_v\right) H(x, y, z)^2$$

where $H(x, y, z)$ is the height of the point $(x : y : z)$. We conclude from the inequality that $H(x, y, z)$ is bounded, hence the number of solutions to (T) is finite.

Part ii) Denote the given S-integral point in $\mathbf{P}^2 \setminus C$ by Q. Let P_v be the v-adic point on C. For any v-adic neighbourhood U of P_v there exist infinitely many lines through Q, defined over K and which intersect C in U in a point whose coordinates are in a quadratic field. Let L be such a line. It intersects C in two points, P, R say, whose coordinates are defined over a quadratic extension M of K and such that P and R are conjugates. By construction the place v splits in M. Hence, by Theorem 1.2.3, there exist infinitely many S-integral points on $L \setminus \{P, R\}$. Since we have infinitely many choices for L we have proved our theorem. □

The following theorem gives a positive answer to Question 6.10 asked by J.Silverman in [Si] in 1984.

Theorem 1.3.3 *Suppose C is a geometrically irreducible plane cubic curve. Suppose C has at least one K-rational flex F. Suppose that the tangent at C through F is not a component of C modulo any prime outside of S. Then the set of S-integral points on $\mathbf{P}^2 \setminus C$ is Zariski dense in $\mathbf{P}^2$.*

Remark. Interesting cases for which the above theorem holds are the equations $x^3+y^3+z^3=1$ and $x^3+y^3-xyz=1$. The proof given below is a very disguised generalisation of an idea of D.H.Lehmer for the case $x^3+y^3+z^3=1$ (see [Le]).

Remark. From examples it seems that the cardinality of $C(K)$ has little or no influence on the number of solutions. The curve given by $2x^3+5y^3+7z^3=0$ contains infinitely many rational points, but the equation $2x^3+5y^3+7z^3=\pm 1$ has no solutions in $\mathbf{Z}$, as can be seen by consideration modulo 7. A similar example is given by the curve $2x^3+7y^3+7z^3=0$ which even has the rational flex $(0:1:-1)$.

Proof. Let C be given by the equation $T(x,y,z)=0$. Let L be the tangent at C through F. Let M be a straight line through F, distinct from L modulo every $v\notin S$. Let $L(x,y,z), M(x,y,z)$ be linear forms corresponding to L and M. Let R be an S-integral point on $L\setminus F$ and let $a=T(R)/M(R)^3$. Then the line L intersects the cubic $T-aM^3=0$ in the points F (triple) and R. Hence L is a component of the cubic curve, i.e. $T-aM^3=L\cdot Q$ for some quadratic form Q. Notice that the conic $Q=0$ intersects C in only two points, namely the points of intersection of C and M distinct from F. Let $\mathcal{L},\mathcal{M},\mathcal{T}$ be the ideals generated by the coefficients of L, M and T respectively. The point R is S-integral on $\mathbf{P}^2\setminus M$, hence $(M(R))=\mathcal{M}\mathcal{R}$ where $\mathcal{R}$ is the ideal generated by the coordinates of R. So we obtain, $a\in\mathcal{T}\mathcal{M}^{-3}$. Suppose there is a prime $v\notin S$ such that $|(a)\mathcal{T}^{-1}\mathcal{M}^3|_v<1$. Then we have modulo v that $T\equiv L\cdot Q$, contradicting our assumption that L is not a component of C modulo v. So we conclude that $(a)=\mathcal{T}\mathcal{M}^{-3}$. After replacing of $a^{-1}T$ by T we may as well assume that $a=1$ and $\mathcal{T}=\mathcal{M}^3$. Furthermore one checks that $\mathcal{Q}$, the ideal generated by the coefficients of Q satisfies

$$\mathcal{Q}\subset\mathcal{L}^{-1}\mathcal{T}=\mathcal{M}^3\mathcal{L}^{-1}.$$

Consider the line M_λ given by $M+\lambda L=0$, where $\lambda\in(3)^{-1}\mathcal{M}\mathcal{L}^{-1}$. Then

$$T-(M+\lambda L)^3=L\cdot Q_\lambda$$

where

$$Q_\lambda=Q-3\lambda M^2-3\lambda^2 ML-\lambda^3 L^2.$$

Let P be an S-integral point on $L\setminus F$. We want $Q_\lambda=0$ to pass through P. Hence we must choose $\lambda=Q(P)/3M(P)^2$. Since P is S-integral on

$\mathbf{P}^2 \setminus M$ we have that $(M(P)) = \mathcal{M}\mathcal{P}$, where $\mathcal{P}$ is the ideal generated by the coordinates of P. Hence we can check that

$$\lambda \in (3)^{-1}\mathcal{Q}\mathcal{M}^{-2} \subset (3)^{-1}\mathcal{M}\mathcal{L}^{-1}.$$

The conic $Q_\lambda = 0$ intersects $T = 0$ in only two points, say A_λ, B_λ. We want to show that P is distinct from A_λ, B_λ modulo any $v \notin S$. If $|(\lambda)\mathcal{M}^{-1}\mathcal{L}|_v \leq 1$ this is clear, the line M_λ is distinct from L modulo v and P stays away from F, the intersection of L and M_λ. When $v|3$ and $|(\lambda)\mathcal{M}^{-1}\mathcal{L}|_v > 1$ we note that the conic Q_λ reduces to L^2 and the points A_λ, B_λ to F. Hence P, being S-integral on $L \setminus F$, is again distinct from A_λ, B_λ.

We are now ready to apply Theorem 1.2.3 and prove our theorem. All we have to do is point out that there exist infinitely many λ such that either A_λ, B_λ are K-rational in the case $|\mathcal{O}_S^*| = \infty$ or that A_λ, B_λ are conjugate points defined over a quadratic extension of K in which at least one place of S splits.

Let us make our choice of P more explicit. Let P_0 be an S-integral point on $L \setminus F$. Then any point of the form $P = P_0 + tF$ with $t \in \mathcal{P}_0\mathcal{F}^{-1}$ is S-integral on $L \setminus F$. Our choice for λ now becomes

$$\lambda = Q(P_0 + tF)/3M(P_0)^2, \qquad t \in \mathcal{P}_0\mathcal{F}^{-1}$$

hence λ is a quadratic polynomial in t. Furthermore, for any λ the discriminant (up to a square in K) of the quadratic field over which A_λ, B_λ are defined is given by a cubic polynomial $D(\lambda)$ with leading coefficient $Q(F)$. The zeros of D correspond precisely to the lines M_λ for which A_λ and B_λ coincide. That is, the 2-torsion points when C is smooth and the double point (twice) plus one extra point when C has a double point and finally, D has a triple zero corresponding to the cusp when C has such a cusp. Now let $\delta(t) = D(Q(P_0 + tF)/3M(P_0)^2)$. Notice that $\delta(t)$ is a polynomial of degree 6 whose leading coefficient, up to squares in K^*, is 3.

Suppose that $3^{-1}\delta(t)$ is the square of a polynomial in $K[t]$. Then A_λ, B_λ are defined over $K(\sqrt{3})$. One easily checks that either $\sqrt{3} \in K$ and hence $|\mathcal{O}_S^*| = \infty$, or there is an infinite place which splits in $K(\sqrt{3})/K$. Since this holds for any t our theorem is proved in this case.

Now suppose that $\delta(t)$ has at least one zero of odd multiplicity. Then there exist infinitely many $t_0 \in \mathcal{P}_0\mathcal{F}^{-1}$ such that $\delta(t_0)$ is not a square in K. If at least one infinite place of K is complex, we are done. So suppose that all infinite places of K are real. Let v be such a place. By choosing t_0 sufficiently large v-adically, we can see to it that $\delta(t_0)$ is positive, hence v

splits in $K(\sqrt{\delta(t_0)})/K$. Since there are infinitely many such possiblities for t_0 we are done. $\square$

Remark. The main idea in the above proof is the construction of exceptional conics in $\mathbf{P}^2 \setminus C$ where C is the cubic given by $T = 0$. As remarked before, there exist also infinitely many exceptional lines in $\mathbf{P}^2 \setminus C$. However, I did not see how to use them in proving Zariski denseness of the solution set of (T).

The only cases we have not dealt with yet are when C is reducible. However, using the techniques from the previous section this is quite straightforward and we give only brief proofs, if any.

Theorem 1.3.4 *Suppose C consists of two straight lines L_1, L_2 which are either defined over K or are conjugate lines over a quadratic extension M of K. Let P be the point of intersection of L_1 and L_2. Let V be the set of S-integral points on $\mathbf{P}^2 \setminus C$.*

Suppose that $\mathcal{O}_S^*$ is finite when the L_i are defined over K and suppose no place of S splits in M/K when the L_i are not defined over K. Then V is contained in a finite number of straight lines passing through P.

In all other cases V is either empty or Zariski dense in $\mathbf{P}^2$.

Theorem 1.3.5 *Suppose C consists of three distinct straight lines L_1, L_2, L_3. Let V be the set of S-integral points on $\mathbf{P}^2 \setminus C$.*

i) If the L_i pass through one point P, then V is contained in a finite set of straight lines through P.

Now suppose that the L_i do not pass through one point. Let $A = L_1 \cap L_3$, $B = L_2 \cap L_3$.

ii) Suppose either all L_i defined over K or L_1, L_2 conjugates over a quadratic extension of K and L_3 defined over K. If $\mathcal{O}_S^*$ is finite, the set V is contained in a finite set of conics which pass through A and B, tangent to L_1, L_2.

iii) Suppose L_1 is defined over a cubic field and L_2, L_3 are its conjugates, or suppose that L_1, L_2 are conjugates over a quadratic extension M of K in which at least one place of S splits and $\mathcal{O}_S^*$ infinite, or suppose that the L_i are defined over K and $\mathcal{O}_S^*$ infinite. Then V is either empty or Zariski dense in $\mathbf{P}^2$.

Proof. Part i) follows simply from the fact that there are at most finitely many S-integral points on a $\mathbf{P}^1$ minus three points.

Let $P = L_1 \cap L_2$. To prove part ii) we consider the function

$$v(x) = \frac{\det(A,P,x)\det(B,P,x)}{\det(A,B,x)^2}.$$

Since any $x \in V$ is S-integral on the lines L_i we have that $(v(x)) = \mathcal{P}^2/\mathcal{AB}$ for any $x \in V$. Furthermore, $v(x) \in K$. So, if $\mathcal{O}_S^*$ is finite, there are at most finitely many possibilities for $v(x)$ and V is contained in a finite set of conics from the pencil $\det(A,P,x)\det(B,P,x) = \alpha\det(A,B,x)^2$.

To prove part iii) we construct automorphisms T as in Proposition 1.2.2. In this case one easily verifies that the set of triples λ, μ, ν that can be chosen lies Zariski dense in $\mathbf{P}^2$. Hence, if $x_0 \in V$, its transforms constitute a Zariski dense set. □

Theorem 1.3.6 *Suppose C consists of a straight line L and an irreducible conic Q, both defined over K. Let V be the set of S-integral points on $\mathbf{P}^2 \backslash C$.*

- *i) If $\mathcal{O}_S^*$ is finite, V is contained in a finite number of conics from the pencil spanned by Q and $2L$.*

- *ii) Suppose that $\mathcal{O}_S^*$ is infinite and L intersects Q in (one or two) points rational over K. Then V is either empty or Zariski dense in $\mathbf{P}^2$.*

- *iii) Suppose that $\mathcal{O}_S^*$ is infinite and L intersects Q in two conjugate points over a quadratic extension M of K. If there exists $P \in V$ such that the tangents through P at Q are defined over K, the set V is Zariski dense in $\mathbf{P}^2$.*

Proof. Consider the function $u(x) = Q(x)/L(x)^2$. For any $x \in V$ we have $(Q(x)/L(x)^2) = \mathcal{Q}\mathcal{L}^{-2}$. Hence, if $\mathcal{O}_S^*$ is finite, $u(x),\ x \in V$ has only finitely many values. This proves part i).

To prove part ii) assume that V is not empty and $P \in V$. Let A, B be the points of intersection of Q and L. Assume that they are distinct. As a consequence of Theorem 1.2.3 the line L_{AP} through A and P contains infinitely many points of V because L_{AP} never reduces to a component of Q or L. Let R be such a point and consider the line L_{BR} through B and R. On L_{BR} we have again infinitely many points of V. The freedom of choice of R gives us the Zariski denseness of V. Now assume that L is tangent to

Q with point of tangency A. Let Q' be the conic from the pencil spanned by Q and $2L$ which passes through P. Then there exist infinitely many points on $Q' \cap V$. For each such point R we consider the line through A and R, which again contains infinitely many points of V.

To prove part iii) let L_P be a tangent of Q through P. Theorem 1.2.3 shows that $V \cap L_P$ is infinite. Let R be such an S-integral point and let L_R be the tangent of Q through R, distinct from L_P. Then L_R is again defined over K. Again we find that $V \cap L_R$ is infinite. The freedom of choice of R gives us the Zariski denseness of V. □

Remark. As an application of part iii) of the previous theorem we note that

$$(x^2 + y^2 - z^2)z = \pm 3^k \qquad \gcd(x, y, z) = 1, \quad k \in \mathbf{Z}_{\geq 0}$$

has a Zariski dense set of solutions. We are in the case $K = \mathbf{Q}$ and $S = \{\infty, 3\}$ and we can take $P = (1 : 1 : 1)$.

1.4 The case 'degree at least 4'

The only general case about which we can make a positive statement is when T contains at least four distinct irreducible factors. The following theorem is precisely Corollary 2.4.3 in Vojta's book [V].

Theorem 1.4.1 (Vojta) *Suppose T has at least four distinct irreducible factors over $\bar{K}$. Then the set of solutions to* (T) *is contained in a finite union of plane algebraic curves.*

Proof. Denote the four factors by T_1, T_2, T_3, T_4 Without loss of generality we may assume that these factors have coefficients in K. Let us also increase S in such a way that $\mathcal{O}_S$ has class number 1. Without loss of generality we may then assume that the coefficients of each polynomial are integral and generate $\mathcal{O}_S$. Equation (T) can be rewritten as

$$T(x, y, z) \in \mathcal{O}_S^*, \qquad x, y, z \in \mathcal{O}_S$$

and this implies,

$$T_i(x, y, z) \in \mathcal{O}_S^* \qquad i = 1, 2, 3, 4, \qquad x, y, z \in \mathcal{O}_S \tag{3}$$

There exists a polynomial $P \in K[X_1, X_2, X_3, X_4]$, irreducible over $\mathbf{C}$ such that $P(T_1, T_2, T_3, T_4)$, considered as polynomial in X, Y, Z, is identically zero. We can assume that there is no subsum $P = Q + R$, where the coefficients of Q and R have disjoint support, such that $Q(T_1, T_2, T_3, T_4) \equiv R(T_1, T_2, T_3, T_4) \equiv 0$. Extend S in such a way that all coefficients of P are S-units.

Let
$$P = \sum p_{i_1 i_2 i_3 i_4} X_1^{i_1} X_2^{i_2} X_3^{i_3} X_4^{i_4}.$$
We define the weight of a term in P as $\sum_j i_j \text{deg} T_j$. As a consequence of our subsum condition we have that all terms of P have the same weight. Consider the S-unit equation

$$\sum p_{i_1 i_2 i_3 i_4} U_{i_1 i_2 i_3 i_4} = 0 \tag{4}$$

in the S-units $U_{i_1 i_2 i_3 i_4}$. Because all terms of P have the same weight, each equivalence class of solutions of (3) gives rise to an equivalence class of solutions of (4) by putting

$$U_{i_1 i_2 i_3 i_4} = T_1(x, y, z)^{i_1} \cdots T_4(x, y, z)^{i_4}.$$

Conversely, given a solution $U_{i_1 i_2 i_3 i_4}$ we like to know which x, y, z correspond to it in this way. It is well-known from results of Evertse and Van der Poorten-Schlickewei [E2] that the solution set of (4) consists of a finite set (of equivalence classes) and a possibly infinite set for which certain subsums in (4) vanish. Each vanishing subsum in (4) defines a projective curve in the x, y, z-plane. So, the infinite part of the solutions of (4) gives rise to a finite union of curves in $\mathbf{P}^2$ on which (x, y, z) can lie. We now show that the finitely many remaining solutions do the same. Let I, I' be two 4-tuples of indices such that $p_I, p_{I'}$ are not zero. A solution $\{U_I\}_I$ of (4) gives rise to an equation

$$U_I T_1^{i'_1}(x, y, z) \cdots T_4^{i'_4}(x, y, z) = U_{I'} T_1^{i_1}(x, y, z) \cdots T_4^{i_4}(x, y, z)$$

in x, y, z. Again this defines a nontrivial projective curve in $\mathbf{P}^2$ on which (x, y, z) can lie. Since there are only finitely many such curves to be considered our proof is now concluded. □

1.5 Exceptional curves

In this section we turn to the problem of the construction of exceptional curves in $\mathbf{P}^2 \setminus C$. This turns out to be a hard geometrical problem and we can only give some straightforward results. Let us forget all arithmetic questions for the moment and take $K = \mathbf{C}$. The set of exceptional curves in $\mathbf{P}^2 \setminus C$ will be called the *exceptional set* of C.

The only examples we have found of algebraic curves C of degree at least 4 having an infinite exceptional set, arise as follows. Let $\alpha C_1 + \beta C_2$ be a pencil of rational curves such that each element sits in the exceptional set of any other element of the pencil. Take for C a union of components of elements of this pencil. Examples of such pencils are

$$\alpha X^p Y^q + \beta Z^{p+q} = 0 \qquad \alpha(YZ^{p-1} + X^p) + \beta Z^p = 0.$$

We also like to define *very exceptional curves.* They are images of non-constant morphisms of $\mathbf{C}$ into $\mathbf{P}^2 \setminus C$. Similarly we can speak of the *very exceptional set* of a curve C. For reducible curves we can describe the very exceptional set.

Theorem 1.5.1 *Let C be a plane algebraic curve without multiple components. Suppose C consists of two components given by the projective equations $F(x, y, z) = 0$ and $G(x, y, z) = 0$ of degree f and g respectively. Let $m = f/(f, g)$ and $n = g/(f, g)$. Then the generic element of the pencil $\alpha F^n + \beta G^m = 0$ is irreducible. If the very exceptional set of C is infinite, every element in the pencil $\alpha F^n + \beta G^m = 0$ is an exceptional curve or a union of them (when the element is reducible).*

Proof. The existence of a very exceptional curve E implies the existence of three polynomials $x, y, z \in \mathbf{C}[t]$ such that $F(x(t), y(t), z(t))G(x(t), y(t), z(t))$ equals 1. Hence both F an G evaluated at this triple of polynomials are constants and E is a component of $\alpha F^n + \beta G^m = 0$ for suitable α, β. Because of our choice of m and n the generic element of the pencil is irreducible. The infinite cardinality of the exceptional set implies via Bertini's theorem that the generic element of the pencil is a rational curve. Since any element of the pencil intersects any other element in at most one point, our theorem is proved. □

For non-rational irreducible curves of degree at least 4 we expect that the (very) exceptional set is finite. A very preliminary result in this direction might be the following theorem.

Theorem 1.5.2 *Let C be an irreducible curve of genus at least 2. Then the curves in the very exceptional set of C intersect C in at most finitely many points.*

Proof. Suppose that the very exceptional curve given by $F(X,Y,Z)=0$ intersects C in a smooth point P. Let Q be another smooth point of intersection with a very exceptional curve $G=0$, say. Let d_C, d_F, d_G be the degrees of the curves involved. Notice that the function F^{d_G}/G^{d_F} is a rational function on C with divisor $d_C d_G d_F(P-Q)$. Let $\tilde{C}$ be a normalisation of C. Then P,Q and the function F^{d_G}/G^{d_F} lift to $\tilde{C}$. Let $\psi:\tilde{C}\to Jac(\tilde{C})$ be the embedding of $\tilde{C}$ into its Jacobian via the map $x\in\tilde{C}\mapsto x-P$. Then Q is mapped to $Q-P$ and we have that $d_C d_F d_G(Q-P)\sim 0$. By a theorem of Raynaud [Ra] there exist only finitely many torsion points of $Jac(\tilde{C})$ on the embedded curve $\tilde{C}$. Hence there are finitely many possibilities for Q. □

For the next theorem we require a modified version of a result proved independently by Voloch [Vol] and Brownawell-Masser [BM].

Theorem 1.5.3 *Let $P_1,\dots,P_n(t)$ be polynomials in $\mathbf{C}[t]$ such that*

$$P_1(t)+\cdots+P_n(t)=0,\qquad \gcd(P_1,\dots,P_n)=1.$$

Let S be the set of distinct zeros of $P_1\cdots P_n$, where we count ∞ as belonging to S as soon as $\deg P_i\neq\deg P_j$ for some i,j. Suppose that there exists no proper subset I of $\{1,\dots,n\}$ such that $\sum_{i\in I}P_i(t)=0$. Then,

$$\max_i(\deg P_i)\leq\frac{1}{2}n(n-1)\max(0,|S|-2).$$

Theorem 1.5.4 *Let $d\in\mathbf{N}$ and let I be a finite set of triples $\vec{i}=(i_1,i_2,i_3)\in\mathbf{Z}^3_{\geq 0}$ with $i_1+i_2+i_3=d$. Let*

$$T(X,Y,Z)=\sum_{\vec{i}\in I}a_{\vec{i}}X^{i_1}Y^{i_2}Z^{i_3},\qquad a_{\vec{i}}\in\overline{K}.$$

Suppose that the elements of I do not all lie on the same straight line and suppose that $(d/3,d/3,d/3)$ lies in the convex hull of I. If $d>(3/2)|I|(|I|-1)$ then there are only finitely many exceptional curves in $\mathbf{P}^2\setminus\{T=0\}$.

Proof. We must solve

$$T(x,y,z)=t^m$$

in $x,y,z\in\mathbf{C}[t]$ and $m\in\mathbf{Z}_{\geq 0}$. Without loss of generality we can assume that $(x,y,z)=1$. Suppose we have such a solution. Let n be the maximum of the degrees of x,y,z. Let S be the set of distinct zeros of $txyz$ plus the point at ∞. Let $\vec{e}_0=(e_1(0),e_2(0),e_3(0))$ be the numbers of factors t occurring in

x, y, z respectively. Let $\vec{e}_\infty = (n - \deg(x), n - \deg(y), n - \deg(z))$, i.e. the 'orders of zero at ∞'. For any $\vec{v} = (v_1, v_2, v_3)$ we define $|\vec{v}| = v_1 + v_2 + v_3$.

In principle $S = \{\text{zeros of } xyz\} \cup \{0, \infty\}$ consists of $3n + 2$ elements. However, if one of the polynomials x, y, z has a degree lower than n or vanishes at 0, this will reduce the size of S. More precisely, $|S| \leq 3n + 2 - |\vec{e}_0| - |\vec{e}_\infty|$. We now apply the above theorem to

$$\sum_{\vec{i} \in I} a_{\vec{i}} x^{i_1} y^{i_2} z^{i_3} - t^m = 0.$$

Suppose there is a vanishing subsum. This implies that

$$\sum_{\vec{i} \in J} a_{\vec{i}} x^{i_1} y^{i_2} z^{i_3} = 0$$

for some subset $J \subset I$. Since there are finitely many subsums we obtain at most finitely many exceptional curves in this way. So let us now assume that there are no vanishing subsums. We obtain

$$dn \leq \gamma(3n - |\vec{e}_0| - |\vec{e}_\infty|) + \min_{\vec{i} \in I}(\vec{i} \cdot \vec{e}_0) + \min_{\vec{i} \in I}(\vec{i} \cdot \vec{e}_\infty)$$

where $\gamma = |I|(|I| - 1)/2$ and $(\vec{v} \cdot \vec{w})$ denotes the ordinary inner product. Now choose $\vec{i}, \vec{j}, \vec{k} \in I$ such that $(d, d, d)/3 = a\vec{i} + b\vec{j} + c\vec{k}$ for some $a, b, c \geq 0, a + b + c = 1$. Notice

$$\begin{aligned}
\min_{\vec{i} \in I}(\vec{i} \cdot \vec{e}_0) &= (a + b + c) \min_{\vec{i} \in I}(\vec{i} \cdot \vec{e}_0) \\
&= \leq a(\vec{i} \cdot \vec{e}_0) + b(\vec{j} \cdot \vec{e}_0) + c(\vec{k} \cdot \vec{e}_0) \\
&= ((1, 1, 1) \cdot \vec{e}_0)d/3 = |\vec{e}_0|d/3
\end{aligned}$$

Hence

$$dn \leq \gamma(3n - |\vec{e}_0| - |\vec{e}_\infty|) + (|\vec{e}_0| + |\vec{e}_\infty|)d/3$$

and

$$(d/3 - \gamma)(3n - |\vec{e}_0| - |\vec{e}_\infty|) \leq 0.$$

Notice that we have always $3n \geq |\vec{e}_0| + |\vec{e}_\infty|$ and equality arises if x, y, z are monomials in t. The latter would imply that the points of I lie on a straight line, which is excluded by our assumptions. Hence $3n - |\vec{e}_0| - |\vec{e}_\infty| \geq 1$ and we obtain

$$d/3 - \gamma \leq 0.$$

Hence $d \leq 3\gamma$, which is again excluded by our assumptions. □

1.6 References

[Ba]–A.Baker, *Transcendental Number Theory*, Cambridge Univ. Press, 1979.

[BS]–E.Bombieri, W.M.Schmidt, On Thue's equation, Inv.Math. 88(1987), 69-82, correction in Inv.Math. 97(1989), 445.

[BM]–W.D.Brownawell, D.W.Masser, Vanishing sums in function fields, Math.Proc. Cambridge Phil.Soc. 100(1986), 427-434.

[E1]–J.H.Evertse, On equations in S-units and the Thue-Mahler equation, Inv.Math. 75(1984), 561-584.

[E2]–J.H.Evertse, On sums of S-units and linear recurrences, Compositio Math. 53(1984), 225-244.

[GLS]–V.L.Gardiner, R.B.Lazarus, P.R.Stein, Solutions of the diophantine equation $x^3 + y^3 = z^3 - d$, Math. Comp. 18(1964), 408-413.

[HLR]–D.R.Heath-Brown, W.M.Lioen, H.J.J. te Riele, Math.Comp 61(1993), 235-244.

[La]–S.Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983.

[Le]–D.H.Lehmer, On the diophantine equation $x^3 + y^3 + z^3 = 1$, J.London Math.Soc. 31(1956), 275-280.

[MaTsch]–Yu.I.Manin, Yu.Tschinkel, Points of bounded height on del Pezzo surfaces, Compositio Math. 85(1993), 315-332.

[Mo]–L.J.Mordell, The congruence $ax^3 + by^3 + c \equiv 0 (\text{mod } xy)$, and integer solutions to cubic equations in three variables, Acta Math. 88(1952), 77-83.

[Ra]–M.Raynaud, Courbes sur une variété abélienne et points de torsion, Inv.Math. 71(1983), 207-233.

[Ri]–P.Ribenboim, *The book of prime number records*, Springer, 1989.

[Si]–J.Silverman, Integral points on curves and surfaces, *Number Theory*, Ulm 1987, (H.P.Schlickewei, E.Wirsing, eds.) 202-241, Lecture Notes in Math. 1380, Springer 1989.

[ST]–T.N.Shorey, R.Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge 1986.

[V]–P.Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. 1239, Springer 1987.

[Vol]–J.F.Voloch, Diagonal equations over function fields, Bol.Soc.Bras. 16(1985), 29-39.