REND. SEM. MAT. UNIV. PADOVA, Vol. 116 (2006)

On the Greatest Prime Factor of Markov Pairs.

PIETRO CORVAJA (*) - UMBERTO ZANNIER (**)

1. Introduction.

Markov triples appear in several contexts of elementary Number-Theory. They are defined as the solutions (x, y, z) to the remarkable diophantine equation

$$x^2 + y^2 + z^2 = 3xyz, \qquad x, y, z \text{ positive integers.} \tag{1}$$

The coefficient 3 here is particularly relevant. In fact, by the descent procedure to be recalled below, one may show the following, on replacing 3 with a positive integer coefficient k: for $k = 1$ we reduce to $k = 3$ after observing that necessarily x, y, z must all be multiples of 3; for $k = 2$ one finds that a possible solution must have all even entries, and we reduce to $k = 4$; finally, for $k \geq 4$ there are no solutions (so in fact there are no solutions for $k = 2$ as well).

The equation on the left of (1) defines an affine surface X which admits a group Γ of automorphisms generated by the permutations on x, y, z and the involution $(x, y, z) \mapsto (x, y, 3xy - z)$. (This comes on viewing the equation as a quadratic in z; since the sum of its roots is $3xy$, if z_0 is a solution, so is also $3xy - z_0$.)

Naturally Γ acts on the set of positive integer solutions, and it may be shown (see [C] or [M]) that there is a single orbit. This follows by the descent alluded to above: one proves that, by applying the involution after suitable permutation of the coordinates, the maximum absolute value of the entries descreases until we reach the solution $(1, 1, 1)$.

It is relevant in the remarks of §4 that these transformations preserve

(*) Indirizzo dell'A.: Dip. di Matematica e Informatica, Via delle Scienze, 33100 - Udine (Italy); e-mail: corvaja@dimi.uniud.it

(**) Indirizzo dell'A.: Scuola Normale Superiore, Piazza dei Cavalieri, 7 - 56100 Pisa (Italy); e-mail: u.zannier@sns.it

the gcd of the entries, so this gcd is always 1. We also note that this orbit is Zariski-dense in X. ([1])

These triples appear in the theory of continued fractions and there are many amusing open problems among them; for instance see [W, Conj. 1.9].

The numbers which occur in some triple are called Markov numbers. It is a question on their arithmetical properties whether the greatest prime factor of a Markov number tends to infinity; in other words, *are there infinitely many Markov numbers which are S-units, for a prescribed finite set S?* We have not an answer to this; however if we look at Markov numbers in the ring of integers of number fields other than $\boldsymbol{Q}$ the answer is YES (see §4 below, over the Gaussian integers).

On the other hand we can look at *Markov pairs*, namely pairs of coordinates from some solution; and we can ask whether there are infinitely many Markov pairs of S-units. These Markov pairs correspond to the S-integral points for a certain affine surface which we shall later describe. A well-known conjecture of Vojta (see [L]), applied in our very special case, predicts now a set of solutions which is not Zariski-dense and from this one may easily recover finiteness.

The purpose of this note is to prove this statement over $\boldsymbol{Z}$. (In §4 we shall point out possible generalizations to number fields.) We formulate it in the following way:

THEOREM 1. *The greatest prime factor of xy, for (x, y, z) a solution of* (1)*, tends to infinity with* $\max(x, y, z)$.

Plainly this is equivalent to the following: *Let S be a finite set of prime numbers. Then the equation $x^2 + y^2 + z^2 = 3xyz$ has only finitely many solutions with $x, y, z \in \boldsymbol{Z}$ and x, y in the group of S-units.*

In the next section we shall operate some simple transformations of the equation and we shall relate the problems to Vojta's conjecture. Also, we shall formulate another theorem more general than Theorem 1. In §3 we shall give the proofs and in the short §4 we shall briefly point out some remarks.

([1]) In fact, observe e.g. that by composing the automorphisms $(x, y, z) \mapsto$ $\mapsto (x, y, 3xy - z)$ and $(x, y, z) \mapsto (x, 3xz - y, z)$ of Γ one gets that $(x, y, z) \mapsto$ $\mapsto (x, (9x^2 - 1)y - 3xz, 3xy - z)$ also lies in Γ; for fixed integer $x \neq 0$ this has infinite order, so if the orbit were contained in a fixed curve, the coordinate x would have only finitely many possibilities; by simmetry the same would then be true for y and z, a contradiction.

2. Some reformulations.

Viewing (1) as a quadratic equation in z, if (x, y, z) is an integral solution, the discriminant $9x^2y^2 - 4(x^2 + y^2)$ must be a square and conversely if this is verified we may solve for z obtaining an integral solution. Therefore we are led to the equation

$$t^2 = ax^2y^2 + bx^2 + cy^2 \tag{2}$$

where a, b, c are given nonzero integers (which in the above special case are given by $a = 9$, $b = c = -4$). This equation defines an affine surface $Y \subset \boldsymbol{G}_m^2 \times \boldsymbol{A}^1$: nameley we consider the solutions (x, y, t) to (2) with $xy \neq 0$. We note that Y contains a finite number of so called *special curves* to be described below. Each of these curves may contain infinitely many integer solutions with x, y being S-units, depending on whether or not a, b, c, S satisfy certain conditions.

First of all we have twelve special curves obtained by equating to zero the sum of a pair of terms on the right side of (2); namely, they are the inverse images with respect to the xy-projection of the lines $y = \pm\sqrt{-b/a}$, $x = \pm\sqrt{-c/a}$, $\sqrt{b}x = \pm\sqrt{-c}y$. These curves may contain infinitely many integral points, provided certain obvious conditions on a, b, c are satisfied.

Eight further special curves are obtained by varying the sign for t, after setting $y = \pm 2\dfrac{\sqrt{ab}}{c}x^2$ and $x = \pm 2\dfrac{\sqrt{ac}}{b}y^2$ (after these substitutions the right-hand side becomes the square of a binomial in a single variable). Again, there may be infinitely many integral points for large enough S (actually if and only if a is a square and b or c is a square).

With this description we have the following result, which will immediately imply Theorem 1.

THEOREM 2. *Let S be a finite set of prime numbers. Then the equation* (2) *has only finitely many solutions with x, y integers in the group of S-units, outside the special curves.*

In particular, the set of integral solutions with S-units x, y is never Zariski-dense in Y. See the final remarks for the fact that there may be a Zariski-dense set of integral solutions such that either x or y is an S-unit.

We pause to establish the alluded relations with Vojta's conjectures on integral points on general algebraic varieties. On dividing by y^2 and setting

$u = ax^2$, $v = x/y$, $w = t/y$, we find the equation

$$w^2 - bv^2 - c = u$$

to be solved in S-units u, v and S-integer w. This corresponds to the search of integral points for $\boldsymbol{P}_2 \setminus D$ where the divisor D is the sum of a conic and two lines in general position; one of the lines is at infinity, the other one is $v = 0$ and the conic has equation $w^2 - bv^2 - c = 0$.

Vojta's conjecture for this affine surface predicts a set of integral points which is not Zariski-dense, working moreover with S-integer points over any number field. We are not able to prove this for general rings of S-integers; however here we may deal with the special case of the theorem, namely restricting to rational integers. In the remarks of §4 we shall point out how our arguments may be extended to cover some other situations. In the same remarks we shall also prove the observation after Theorem 2, namely that the integral points may be Zariski-dense (over suitable number fields) if we drop the restriction that v be an S-unit. This corresponds to the integral points for $\boldsymbol{P}_2 \setminus$(line + conic). The divisor to be removed has now degree 3 so we fall out of the hypotheses for Vojta's conjecture.

3. Proofs.

We shall follow a method introduced in [CZ1], which works on expanding the square root of the right side of (2) by the binomial theorem. By truncating the binomial series this provides a good approximation to t if the term ax^2y^2 is "dominant" with respect to the other two terms. This approximation produces a small linear form to which the Subspace Theorem may be applied. Here we shall have no need to repeat this argument since a relevant lemma, to be recalled below, appears in [CZ2], as well as in the booklet [Z].

If the alluded term is not dominant, either x or y must be small compared to the height of the point. But then we shall see that for a suitable prime $p \in S$ there is a dominant term in the p-adic sense; this allows another application of the lemma, for the p-adic topology.

This proof-pattern, namely using approximating forms with respect to two different places, according to the relative sizes of x, y, appears in the paper [CZ1] to deal with certain equations $f(a^m, y) = b^n$ where f is a polynomial and a, b are given integers which are not coprime.

As mentioned above, for the reader's convenience, preliminary to the

proof we repeat a lemma from [CZ2]; we denote by $H(\boldsymbol{x})$ the usual projective Weil height of the vector $\boldsymbol{x} = (x_1, \ldots, x_n)$, by $\mathcal{O}_S^*$ the group of S-units in $\boldsymbol{Q}$ and by v a fixed place in S.

LEMMA. *Let $\delta > 0$. Let Σ be a set of points $\boldsymbol{x} = (x_1, \ldots, x_n) \in (\mathcal{O}_S^*)^n$ such that:*

(i) $|x_1|_v \geq \big(\max_{j \geq 2} |x_j|_v\big) H(\boldsymbol{x})^{\delta}$.

(ii) *There exists $y = y_{\boldsymbol{x}} \in \boldsymbol{Q}$ with $x_1 + \ldots + x_n = y^2$.*

Then Σ is contained in a finite union of algebraic translates $\boldsymbol{u}H \subset \boldsymbol{G}_m^n$, $\boldsymbol{u} \in (\mathcal{O}_S^*)^n$, $H \subset \boldsymbol{G}_m^n$ an algebraic subgroup, such that, for a $P = P_{\boldsymbol{u}H} \in \in \boldsymbol{Q}[X_1^{\pm 1}, X_2, \ldots, X_n]$ and a $\gamma = \gamma_{\boldsymbol{u}H} \in \boldsymbol{Q}$, we have $X_1 + \ldots + X_n = \gamma X_1 P(X_1, \ldots, X_n)^2$, as functions in $\boldsymbol{Q}[\boldsymbol{u}H]$.

This is the case $d = 2, K = \boldsymbol{Q}$ of the Corollary at p. 78 of [CZ2]; see also [Z], Thm. IV.5 and Cor. IV.6.

PROOF OF THEOREM 2. We first enlarge S to contain all the primes dividing abc. We may assume that $0 < x \leq y$ are S-units in $\boldsymbol{Z}$ satisfying (2).

We set $\eta := (4 \# S)^{-1}$ and split the set of solutions (x, y) in two disjoint sets A_1, A_2, according respectively as $x > y^{\eta}$ or not. It will plainly be sufficient to prove the theorem separately for these two sets of solutions.

PROOF FOR THE SOLUTIONS IN A_1. We apply the Lemma, with $n = 3$, to the solutions $(x, y) \in A_1$, setting $x_1 = ax^2y^2$, $x_2 = bx^2$, $x_3 = cy^2$. Putting $\delta := \eta/4$, it is immediately checked that for all but finitely many solutions we shall have $|x_1| > \max(|x_2|, |x_3|)^{1+\delta}$; clearly it suffices to deal with these solutions. The condition (i) of the lemma is satisfied with v the archimedean place of $\boldsymbol{Q}$.

In view of (2) we conclude by the lemma that for $(x, y) \in A_1$ the set (x_1, x_2, x_3) is contained in a finite union of algebraic translates in $\boldsymbol{G}_m^3$, with the property in the statement. It will suffice to deal separately with each translate. By the lemma, on such a translate we shall have an equation

$$ax^2y^2 + bx^2 + cy^2 = \gamma x^2 y^2 Q(x, y)^2, \tag{3}$$

for a suitable rational function $Q \in \boldsymbol{Q}(X, Y)$ depending only on the translate; if there is some corresponding solution of (2) we see that γ is a square and so we may take $\gamma = 1$. Since $a + bU^2 + cV^2$ is not identically a square, the equation (3) cannot hold identically, and thus represents a curve con-

taining our S-unit points (x, y). This already proves that our integral points are not Zariski-dense in Y.

By a well-known theorem going back to Lang (see e.g. [Z], Thm. II.5 and Cor.) the Zariski closure in $\boldsymbol{G}_m^2$ of our set of S-unit points is a finite union of algebraic translates. The 0-dimensional translates give rise to finitely many points. The 1-dimensional translates containing infinitely many solutions may be parametrized by $x = au^r$, $y = \beta u^s$, with coprime integers r, s and nonzero rationals a, β. Since our solutions x, y are supposed to be integers we may assume that r, s are non-negative and not both zero.

Since each relevant translate must be contained in the curve defined by (3), we have an identity

$$a + \frac{b}{\beta^2} u^{-2s} + \frac{c}{a^2} u^{-2r} = R(u)^2$$

for a suitable rational function $R \in \boldsymbol{Q}(u)$. Taking into account all the possibilities when $rs = 0$ we easily recover eight of the twelve curves described above. If $rs \neq 0$, a first case occurs with $r = s = 1$, and we recover the remaining four of the twelve alluded curves; if $rs > 1$, it is an easy well-known matter to check that r, s are $1, 2$ in some order so that finally we find that, for some rational ξ, either $a + bT + c\xi^2 T^2$ or $a + cT + b\xi^2 T^2$ is a perfect square in $\boldsymbol{Q}(T)$ and we find the remaining four special curves.

PROOF FOR THE SOLUTIONS IN A_2. Since y is an S-unit, there exists a prime power p^r dividing y exactly, with $p \in S$ and $p^r \geq y^{1/\#S} = y^{4\eta} \geq x^4$. We apply the lemma, this time with v equal to the p-adic valuation and $x_1 = bx^2$, $x_2 = cy^2$, $x_3 = ax^2y^2$. Assumption (i) is verified for large x, with $\delta = 1/5\,\#S$: in fact, $|x_1|_v \geq |bx^2|^{-1} \geq x^{-4}$, whence $\max(|x_2|_v, |x_3|_v) \leq \leq p^{-2r} \leq |x_1|_v p^{-r}$ and the result follows because of our choice for p^r.

The lemma leads to an equation entirely similar to (3), namely

$$ax^2y^2 + bx^2 + cy^2 = \gamma x^2 Q(x, y)^2. \tag{3'}$$

The same discussion of the preceding case completes now the proof of Theorem 2.

Proof of Theorem 1. We have already noted that an integer solution of (1) leads to an integer solution of (2), with the same x, y, where $a = 9$, $b = c = -4$. In view of Theorem 2 it is sufficient to observe that the special curves do not contain integral points, an easy verification which we leave to the interested reader.

4. Final remarks.

The above proof does not extend to general number fields; in fact in general one cannot guarantee *a priori* the existence of a "dominant term" among x^2y^2, x^2, y^2, no matter the choice for the absolute value. However, a dominant term must exist if there is a single archimedean place, so the same argument as above works for integer solutions over an imaginary quadratic field.

We finally note that if we only impose that x (or y) is an S-unit, there are cases in which equation (2) has a Zariski-dense set of solutions. Suppose for instance that $c = h^2$ is a square in K. Taking y to be an integer and (u, v) to be a solution of the Pell's type equation

$$u^2 - \Delta v^2 = 1, \qquad \Delta = ay^2 + b,$$

we find a solution of (2) by $t = uhy$, $x = vhy$. Producing solutions of the Pell's equation yields a Zariski-dense set of integral solutions of (2), with y an S-unit, for instance in the case $K = \boldsymbol{Q}$ and c a perfect square.

For equation (1), we have $c = -4$, so this procedure gives a Zariski-dense set of integer solutions with S-unit y, over the Gaussian integers.

This argument also shows that $\boldsymbol{P}_2 \setminus$(line + conic) has a Zariski-dense set of S-integral points for sufficiently large number field and finite set S of places.

An equation slightly more general than (2) is $t^2 = ax^2y^2 + bx^2 + cy^2 + d$; see e.g. [M, Ch. 13]. Our method does not apply to this equation for $d \neq 0$. The solutions in polynomials over a given field have been investigated in [SZ].

We remark that if we are interested in the solutions to these equations with x, y in the group of S-units, then we may forget about the squares (because of finite generation) and replace the equation with $t^2 = auv + bu + cv + d$.

Added in proofs: the Markov equation over number fields has been the object of recent investigation. See for instance the paper by J. Silverman: «The Markoff equation $X^2 + Y^2 + Z^2 = aXYZ$ over quadratic imaginary fields», *Journal of Number Theory* **35** (1990), 72-104 or the paper by A. Baragar «The Markoff-Hurwitz equation over number fields», *Roky Mountain Journal of Mathematics* **35** (2005), 695-712.

We are grateful to Prof. Silverman for informing us about these references.

REFERENCES

[CZ1] P. Corvaja - U. Zannier, *On the Diophantine Equation* $f(a^m, y) = b^n$, Acta Arith., **94** (2000), pp. 25-40.

[CZ2] P. Corvaja - U. Zannier, *S-unit points on analytic hypersurfaces*, Ann. Sci. E.N.S., **38** (2005), pp. 76-92.

[C] J.W.S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Tracts in Mathematics, **45**, 1957.

[L] S. Lang, *Number Theory III. Diophantine Geometry*, Encyclopoedia of Mathematics, Springer-Verlag, 1991.

[M] J.L. Mordell, *Diophantine Equations*, Academic Press, 1969.

[SZ] A. Schinzel - U. Zannier, *Distribution of solutions of Diophantine Equations* $f_1(x)f_2(x) = f_3(x)$, *where* f_i *are polynomials*, Rend. Sem. Mat. Univ. Padova, **92** (1994), pp. 29-46.

[W] M. Waldschmidt, *Open Diophantine Problems*, Moskow Math. Journal, **4** (2004), pp. 245-305.

[Z] U. Zannier, *Some Applications of Diophantine Approximation to Diophantine Equations*, Forum Editrice, Udine, 2003.

Manoscritto pervenuto in redazione il 6 ottobre 2005