Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jörg JAHNEL

More cubic surfaces violating the Hasse principle

Tome 23, n° 2 (2011), p. 471-477.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_471_0>

Journal de Théorie des Nombres de Bordeaux **23** (2011), 471-477

More cubic surfaces violating the Hasse principle

par Jörg JAHNEL

Résumé. Nous généralisons la construction due à L. J. Mordell de surfaces cubiques pour lesquelles le principe de Hasse est faux.

Abstract. We generalize L. J. Mordell's construction of cubic surfaces for which the Hasse principle fails.

1. Introduction and main result

Sir Peter Swinnerton-Dyer [4] was the first to construct a cubic surface over $\mathbb{Q}$ for which the Hasse principle provably fails. Swinnerton-Dyer's construction had soon been generalized by L. J. Mordell [3] who found two series of such examples. The starting points of Mordell's construction are the cubic number fields contained in $\mathbb{Q}(\zeta_p)$ for $p = 7$ and $p = 13$, respectively.

In this note, we will show that Mordell's construction may be generalized to an arbitrary prime $p \equiv 1 \pmod 3$.

Notation. i) We denote by $K/\mathbb{Q}$ the unique cubic field extension contained in the cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.
ii) We fix the explicit generator $\theta \in K$ given by $\theta := \mathrm{tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p - 1)$. More concretely, $\theta = -n + \sum\limits_{i \in (\mathbb{F}_p^*)^3} \zeta_p^i$ for $n := \frac{p-1}{3}$.

Theorem 1.1. *Consider the cubic surface $X \subset \mathbf{P}^3_{\mathbb{Q}}$, given by*

$$T_3(a_1T_0 + d_1T_3)(a_2T_0 + d_2T_3) = \prod_{i=1}^{3} \left(T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2T_2\right).$$

Here, a_1, a_2, d_1, d_2 are integers and $\theta^{(i)}$ are the images of θ under $\mathrm{Gal}(K/\mathbb{Q})$.

i) *Then, the reduction X_p of X at p is given by*

$$T_3(a_1T_0 + d_1T_3)(a_2T_0 + d_2T_3) = T_0^3.$$

Over the algebraic closure, X_p is the union of three planes. These are given by

$$T_3/T_0 = s_1, \quad T_3/T_0 = s_2, \quad T_3/T_0 = s_3$$

for s_i the zeroes of $T(a_1 + d_1T)(a_2 + d_2T) - 1$, considered as a polynomial over $\mathbb{F}_p$.

Manuscrit reçu le 10 août 2009.

ii) *Suppose* $p \nmid d_1 d_2$ *and* $\gcd(d_1, d_2) = 1$*. Then, for every*

$$(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q})$$

the term $s := (t_3/t_0 \bmod p)$ *admits the property that*

$$\frac{a_1 + d_1 s}{s}$$

is a cube in $\mathbb{F}_p^*$*.*

In particular, if $(a_1 + d_1 s_i)/s_i \in \mathbb{F}_p^*$ *is a non-cube for every* i *such that* $s_i \in \mathbb{F}_p$ *then* $X(\mathbb{Q}) = \emptyset$*.*

iii) *Assume that* $p \nmid d_1 d_2$ *and that* $\gcd(a_1, d_1)$ *and* $\gcd(a_2, d_2)$ *contain only prime factors that completely split in* K*. Suppose further that* $T(a_1 + d_1 T)(a_2 + d_2 T) - 1 \in \mathbb{F}_p[T]$ *has at least one simple zero in* $\mathbb{F}_p$*.*

Then, $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$*.*

Remarks. i) $K/\mathbb{Q}$ is an abelian cubic field extension. It is totally ramified at p and unramified at all other primes. A prime $q \neq p$ is split in K if and only if q is a cube modulo p.

ii) We will write $\mathfrak{p}$ for the prime ideal in K lying above (p). Note that $\mathfrak{p} = (\theta)$ by virtue of our definition of θ.

iii) We have $\prod_{i=1}^{3} (T_0 + \theta^{(i)} T_1 + (\theta^{(i)})^2 T_2) = N_{K/\mathbb{Q}}(T_0 + \theta T_1 + \theta^2 T_2)$.

Remark. For $p = 7$ and 13, we recover exactly the result of L. J. Mordell. The original example of Sir Peter Swinnerton-Dyer reappears for $p = 7$, $a_1 = d_1 = a_2 = 1$, and $d_2 = 2$.

2. The proofs

Observations 2.1. i) *For* s *any solution of* $T(a_1 + d_1 T)(a_2 + d_2 T) - 1 = 0$*, the expression* $(a_1 + d_1 s)/s$ *is well defined and non-zero.*

ii) *No* $\mathbb{Q}_p$*-valued point on* X *reduces to the triple line "*$T_0 = T_3 = 0$*".*

iii) *For every* $(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q}_p)$*, the fraction* $(a_1 t_0 + d_1 t_3)/t_3$ *is a* p*-adic unit.*

Proof. i) By assumption, we have $s \neq 0$ and $a_1 + d_1 s \neq 0$.

ii) Suppose, $(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q}_p)$ is a point reducing to the triple line. We may assume $t_0, t_1, t_2, t_3 \in \mathbb{Z}_p$ are coprime. Then $\nu_p(t_0) \geq 1$ and $\nu_p(t_3) \geq 1$ together imply that $\nu_p(t_3(a_1 t_0 + d_1 t_3)(a_2 t_0 + d_2 t_3)) \geq 3$. On the other hand,

$$\nu_p\Big(\prod_{i=1}^{3} (t_0 + \theta^{(i)} t_1 + (\theta^{(i)})^2 t_2)\Big)$$

equals 1 or 2 since t_1 or t_2 is a unit and $\nu_p(\theta^{(i)}) = \frac{1}{3}$.

iii) Again, assume $t_0, t_1, t_2, t_3 \in \mathbb{Z}_p$ to be coprime. Assertion ii) implies that t_3 is a p-adic unit. Hence, $(a_1t_0 + d_1t_3)/t_3 \in \mathbb{Z}_p$. Further,

$$\Big(\frac{a_1t_0 + d_1t_3}{t_3} \bmod p\Big) = \frac{a_1 + d_1s}{s}$$

for $s := (t_3/t_0 \bmod p)$ a solution of $T(a_1 + d_1T)(a_2 + d_2T) - 1 = 0$. $\square$

Lemma 2.1. *Let ν be any valuation of $\mathbb{Q}$ different from ν_p and w an extension of ν to K. Further, let X be as in Theorem 1.1.ii) and $(t_0 : t_1 : t_2 : t_3) \in X(\mathbb{Q}_\nu)$.*

Then, $(a_1t_0 + d_1t_3)/t_3 \in \mathbb{Q}_\nu^*$ is in the image of the norm map $N\colon K_w \to \mathbb{Q}_\nu$.

Proof. First step: Elementary cases.

If q is a prime split in K then every element of $\mathbb{Q}_q^*$ is a norm. The same applies to the infinite prime.

Second step: Preparations.

It remains to consider the case that q remains prime in K. Then, an element $x \in \mathbb{Q}_q^*$ is a norm if and only if $3|\nu(x)$ for $\nu := \nu_q$.

It might happen that θ is not a unit in K_w. However, as $K_w/\mathbb{Q}_q$ is unramified, there exists some $t \in \mathbb{Q}_q^*$ such that $\underline{\theta} := t\theta \in K_w$ is a unit. The surface $\widetilde{X}$ given by

$$T_3(a_1T_0 + d_1T_3)(a_2T_0 + d_2T_3) = \prod_{i=1}^{3} (T_0 + \underline{\theta}^{(i)}T_1 + (\underline{\theta}^{(i)})^2T_2)$$

is isomorphic to $X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_q$. Even more, the map

$$\iota\colon X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_q \to \widetilde{X}, \quad (t_0 : t_1 : t_2 : t_3) \mapsto (t_0 : \tfrac{t_1}{t} : \tfrac{t_2}{t^2} : t_3)$$

is an isomorphism that leaves the rational function $(a_1T_0 + d_1T_3)/T_3$ unchanged. Hence, we may assume without restriction that $\theta \in K_w$ is a unit.

Third step: The case that θ is a unit.

Assume that $t_0, t_1, t_2, t_3 \in \mathbb{Z}_q$ are coprime. If

$$\nu\big(t_3(a_1t_0 + d_1t_3)(a_2t_0 + d_2t_3)\big) = 0$$

then $(a_1t_0 + d_1t_3)/t_3$ is a q-adic unit, hence clearly a norm. Otherwise, we have

$$\nu\Big(\prod_{i=1}^{3}(t_0 + \theta^{(i)}t_1 + (\theta^{(i)})^2t_2)\Big) > 0\,.$$

This means that one of the factors $t_0 + \theta^{(i)}t_1 + (\theta^{(i)})^2t_2$ vanishes after reduction to the residue field $\mathbb{F}_{q^3}$. As $\theta^{(i)}$ is reduced to a generator of the extension $\mathbb{F}_{q^3}/\mathbb{F}_q$, this implies that $\nu(t_0)$, $\nu(t_1)$, $\nu(t_2) > 0$. Consequently, t_3 must be a unit.

From the equation of X, we deduce $\nu(d_1d_2) > 0$. If $\nu(d_2) > 0$ then, according to the assumption, d_1 is a unit. This shows $\nu(a_1t_0 + d_1t_3) = 0$, from which the assertion follows.

Thus, assume $\nu(d_1) > 0$. Then, d_2 is a unit and, therefore, $\nu(a_2t_0 + d_2t_3) = 0$. Further, we note that

$$3 \,|\, \nu\Big(\prod_{i=1}^{3}(t_0 + \theta^{(i)}t_1 + (\theta^{(i)})^2t_2)\Big)$$

since the product is a norm. By consequence,

$$3 \,|\, \nu\big(t_3(a_1t_0 + d_1t_3)(a_2t_0 + d_2t_3)\big).$$

Altogether, we see that $3 \,|\, \nu(a_1t_0 + d_1t_3)$ and $3 \,|\, \nu\big((a_1t_0 + d_1t_3)/t_3\big)$. The assertion follows. $\square$

Proof of Theorem 1.1.ii). According to Lemma 2.1, $(a_1t_0 + d_1t_3)/t_3 \in \mathbb{Q}^*$ is a local norm at every prime except p. Global class field theory [5, Theorem 5.1 together with 6.3] shows that it must necessarily be a norm at that prime, too.

By Observation 2.1.iii), $(a_1t_0 + d_1t_3)/t_3$ is automatically a p-adic unit. $(p) = \mathfrak{p}^3$ is a totally ramified prime. A p-adic unit u is a norm if and only if $\overline{u} := (u \bmod p)$ is a cube in $\mathbb{F}_p^*$. As $(a_1 + d_1s)/s = \big((a_1t_0 + d_1t_3)/t_3 \bmod p\big)$, this is exactly the assertion. $\square$

Proof of Theorem 1.1.iii). We have to show that $X(\mathbb{Q}_\nu) \neq \emptyset$ for every valuation of $\mathbb{Q}$. $X(\mathbb{R}) \neq \emptyset$ is obvious. For a prime number q, in order to prove $X(\mathbb{Q}_q) \neq \emptyset$, we use Hensel's lemma. It is sufficient to verify that the reduction X_q has a smooth $\mathbb{F}_q$-valued point. Thereby, we may replace X by a $\mathbb{Q}_q$-scheme $\widetilde{X}$ isomorphic to $X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_q$.

Case 1: $q = p$.

Then, the reduction X_p is the union of three planes meeting in the line given by $T_0 = T_3 = 0$. By assumption, one of the planes appears with multiplicity one and is defined over $\mathbb{F}_p$. It contains p^2 smooth points.

Case 2: $q \neq p$.

Assume without restriction that θ is a w-adic unit. There are two subcases.

a) $q \nmid d_1d_2$. It suffices to show that there is a smooth $\mathbb{F}_q$-valued point on the intersection X'_q of X_q with the hyperplane "$T_0 = 0$". This curve is given by

$$\overline{d}_1\overline{d}_2T_3^3 = \overline{\theta}^{(1)}\overline{\theta}^{(2)}\overline{\theta}^{(3)}\prod_{i=1}^{3}(T_1 + \overline{\theta}^{(i)}T_2)\,.$$

If $q \neq 3$ then this equation defines a smooth genus one curve. It has an $\mathbb{F}_q$-valued point by Hasse's bound.

If $q = 3$ then the projection $X'_q \to \mathbf{P}^1$ given by $(T_1 : T_2 : T_3) \mapsto (T_1 : T_2)$ is one-to-one on $\mathbb{F}_q$-valued points. At least one of them is smooth since $\prod_{i=1}^{3}(T + \overline{\theta}^{(i)})$ is a separable polynomial.

b) $q | d_1 d_2$. Then, $X'_q := X_q \cap$ "$T_0 = 0$" is given by

$$0 = \overline{\theta}^{(1)}\overline{\theta}^{(2)}\overline{\theta}^{(3)} \prod_{i=1}^{3}(T_1 + \overline{\theta}^{(i)} T_2)\,.$$

In particular, $x = (0 : 0 : 0 : 1) \in X_q(\mathbb{F}_q)$. We may assume that x is singular.

Then, X_q is given as $Q(T_0, T_1, T_2)T_3 + K(T_0, T_1, T_2) = 0$ for Q a quadratic form and K a cubic form. If $Q \not\equiv 0$ then there is an $\mathbb{F}_q$-rational line ℓ through x such that $Q|_\ell \neq 0$. Hence, ℓ meets X_q twice in x and once in another $\mathbb{F}_q$-valued point that is smooth.

Otherwise, $(F \bmod q)$ does not depend on T_3. I.e., the left hand side of the equation of X vanishes modulo q. This means that one of the factors must vanish. We have, say, $a_1 \equiv d_1 \equiv 0 \pmod q$. Then, by assumption, q splits completely in K. At such a prime, X'_q is the union of three lines that are defined over $\mathbb{F}_q$, different from each other, and meet in one point. There are plenty of smooth points on X'_q. These points are smooth on X_q, as well. $\square$

3. Examples

Example. For $p = 19$, a counterexample to the Hasse principle is given by

$$\begin{aligned} T_3(19T_0 + 5T_3)(19T_0 + 4T_3) &= \prod_{i=1}^{3} \left(T_0 + \theta^{(i)} T_1 + (\theta^{(i)})^2 T_2\right) \\ &= T_0^3 - 19T_0^2T_1 + 133T_0^2T_2 + 114T_0T_1^2 \\ &\quad - 1\,539\,T_0T_1T_2 + 5\,054\,T_0T_2^2 - 209T_1^3 \\ &\quad + 3\,971\,T_1^2T_2 - 23\,826\,T_1T_2^2 + 43\,681\,T_2^3\,. \end{aligned}$$

Indeed, in $\mathbb{F}_{19}$, the cubic equation $T^3 - 1 = 0$ has the three solutions 1, 7, and 11. However, in any case $(a_1 + d_1 s)/s = 5$, which is a non-cube.

Example. Put $p = 19$. Consider the cubic surface X given by

$$T_3(T_0 + T_3)(12T_0 + T_3) = \prod_{i=1}^{3} \left(T_0 + \theta^{(i)} T_1 + (\theta^{(i)})^2 T_2\right).$$

Then, $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$. X violates the Hasse principle.

Indeed, in $\mathbb{F}_{19}$, the cubic equation $T(1 + T)(12 + T) - 1 = 0$ has the three solutions 12, 15, and 17. However, in $\mathbb{F}_{19}$, $13/12 = 9$, $16/15 = 15$, and $18/17 = 10$, which are three non-cubes.

Example. For $p = 19$, consider the cubic surface X given by

$$T_3(T_0 + T_3)(2T_0 + T_3) = \prod_{i=1}^{3} (T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2 T_2)\,.$$

Then, for X, the Hasse principle fails.

Indeed, in $\mathbb{F}_{19}$, the cubic equation $T(1 + T)(2 + T) - 1 = 0$ has $T = 5$ as its only solution. The two other solutions are conjugate to each other in $\mathbb{F}_{19^2}$. However, in $\mathbb{F}_{19}$, $6/5 = 5$ is a non-cube.

Example. Put $p = 19$ and consider the cubic surface X given by

$$T_3(T_0 + T_3)(6T_0 + T_3) = \prod_{i=1}^{3} (T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2 T_2)\,.$$

There are $\mathbb{Q}$-rational points on X but weak approximation fails.

Indeed, in $\mathbb{F}_{19}$, the cubic equation $T(1+T)(6+T)-1 = 0$ has the three solutions 8, 9, and 14. However, in $\mathbb{F}_{19}$, $10/9 = 18$ is a cube while $9/8 = 13$ and $15/14 = 16$ are non-cubes. The smallest $\mathbb{Q}$-rational point on X is $(14 : 15 : 2 : (-7))$. Observe that, in fact, $T_3/T_0 = -7/14 \equiv 9 \pmod{19}$.

Remark. From each of the examples given, by adding multiples of p to the coefficients a_1, d_1, a_2, and d_2, a family of surfaces arises, which are of similar nature.

Remark (Lattice basis reduction)**.** The norm form in the $p = 19$ examples produces coefficients that are rather large. An equivalent form with smaller coefficients may be obtained using lattice basis reduction. In its simplest form, this means the following.

For the rank 2 lattice in $\mathbb{R}^3$, generated by $v_1 := (\theta^{(1)}, \theta^{(2)}, \theta^{(3)})$ and $v_2 := \big((\theta^{(1)})^2, (\theta^{(2)})^2, (\theta^{(3)})^2\big)$, in fact $\{v_1, v_2+7v_1\}$ is a reduced basis. Therefore, the substitution $T_1' := T_1 - 7T_2$ simplifies the norm form. We find

$$\begin{aligned}\prod_{i=1}^{3}(T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2 T_2) = T_0^3 &- 19T_0^2T_1' + 114T_0T_1'^2 + 57T_0T_1'T_2 \\ &- 133T_0T_2^2 - 209T_1'^3 - 418T_1'^2T_2 \\ &+ 1045T_1'T_2^2 - 209T_2^3\,.\end{aligned}$$

Remark (Brauer-Manin obstruction)**.** It was observed by Yu. I. Manin [2] that a class $\alpha \in \mathrm{Br}(X)$ in the Grothendieck-Brauer group may be responsible for the failure of the Hasse principle or of weak approximation. In fact, all the examples given above may be explained more conceptually in this way.

In short, this may be seen is as follows. We consider the rational function $f \in \mathbb{Q}(X)$ given by $(a_1T_0+d_1T_3)/T_3$. The principal divisor $\mathrm{div}(f)$ is the norm of a divisor $E \in \mathrm{Div}(X_K)$. Indeed, it is the sum over the three conjugate lines given by $a_1T_0 + d_1T_3 = T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2T_2 = 0$ minus the sum of the three conjugate lines given by $T_3 = T_0 + \theta^{(i)}T_1 + (\theta^{(i)})^2T_2 = 0$.

By Manin's formula [2, Proposition 31.3], such a principal divisor induces a class in $H^1(\mathrm{Gal}(K/\mathbb{Q}), \mathrm{Pic}(X_K)) \subseteq H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(X_{\overline{\mathbb{Q}}}))$. Furthermore, for cubic surfaces, the Hochschild-Serre spectral sequence shows that the latter Galois cohomology group is isomorphic to $\mathrm{Br}(X)/\,\mathrm{Br}(\mathbb{Q})$.

Hence, associated to f, we have a Brauer class $\alpha \in \mathrm{Br}(X)$, which is unique up to addition of some element from $\mathrm{Br}(\mathbb{Q})$. To evaluate $\alpha \in \mathrm{Br}(X)$ at an adelic point $x \in X(\mathbb{A}_\mathbb{Q})$ essentially means to evaluate f and to apply the norm-residue-homomorphisms $\mathbb{Q}_\nu^*/NK_w^* \to \mathbb{Q}/\mathbb{Z}$ [2, 45.2]. This is exactly what we did in the proof of Theorem 1.1.ii).

More details on this approach are given in the author's Habilitation thesis [1, Sec. III.5].

References

[1] J. Jahnel, *Brauer groups, Tamagawa measures, and rational points on algebraic varieties.* Habilitation thesis, Göttingen, 2008.

[2] Yu. I. Manin, *Cubic forms, algebra, geometry, arithmetic.* North-Holland Publishing Co. and American Elsevier Publishing Co., Amsterdam-London and New York, 1974.

[3] L. J. Mordell, *On the conjecture for the rational points on a cubic surface.* J. London Math. Soc. **40** (1965), 149–158.

[4] Sir Peter Swinnerton-Dyer, *Two special cubic surfaces.* Mathematika **9** (1962), 54–56.

[5] J. Tate, *Global class field theory.* In: Algebraic number theory, Edited by J. W. S. Cassels and A. Fröhlich, Academic Press and Thompson Book Co., London and Washington, 1967.

Jörg Jahnel
FB6 Mathematik
Walter-Flex-Str. 3
D-57068 Siegen, Germany
E-mail: jahnel@mathematik.uni-siegen.de
URL: http://www.uni-math.gwdg.de/jahnel