Math. Proc. Camb. Phil. Soc. (1978), **84**, 219
Printed in Great Britain

Some cubic surfaces with no rational points

By ANDREW BREMNER
Emmanuel College, Cambridge

(*Received* 18 *January* 1978)

1. *Introduction.* Selmer(1) conjectured that the Hasse principle holds for all cubic surfaces of the type

$$ax^3+by^3+cz^3+dt^3=0 \quad (a,b,c,d\in\mathbf{Q}), \tag{1}$$

that is, such a surface has a rational point whenever it has points defined over every p-adic field $\mathbf{Q}_p$; and he proved this assertion in the case that $ab=cd$.

Cassels and Guy(2) disproved the general conjecture by showing that the surface

$$5x^3+12y^3+9z^3+10t^3=0 \tag{2}$$

is everywhere locally solvable but has no rational points. This example, *inter alia*, is discussed further in Manin's book(3). (2) is apparently the only known counter example to the Selmer conjecture, so we give here some further examples of surfaces of type (1) for which the Hasse principle fails to hold. In particular, we shall see that the Hasse principle fails to hold for the surface

$$x^3+4y^3+10z^3+25t^3=0. \tag{3}$$

The method of Cassels and Guy was to produce by machine computation a list of about 250 surfaces of type (1), everywhere locally solvable, but with no 'small' rational points; and then to search through the list for a suitable example on which to show the non-existence of rational points. Interestingly, (2) is the second surface on the list; the first is given by (3), and is the only surface on the list whose coefficients are divisible by just two primes.

2. *Arithmetic of the number fields.* Put $\alpha^3=2$, $\beta^3=20$; we shall work in the fields $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$, and their compositum $K=\mathbf{Q}(\alpha,\beta)$ of degree 9 over $\mathbf{Q}$. Arithmetical details such as class number, units and some prime factorizations, can be found for the cubic fields in Selmer's tables (4); so we restrict attention to K.

Denote the norm map from K to $\mathbf{Q}$ by Norm, and from K to $\mathbf{Q}(\beta)$, $\mathbf{Q}(\alpha)$ by Norm_1, Norm_2 respectively. Let $\mathfrak{O}$ be the ring of integers of K, and $\mathfrak{O}'$ the subring of $\mathfrak{O}$ generated by the 'obvious' integers, that is, all $x\in K$ with $x^3\in\mathbf{Z}$. The discriminant of $\mathfrak{O}'$ over $\mathbf{Z}$ is $2^6.3^{18}.5^6$, whence the only primes that ramify in K are 2, 3, 5. Indeed in $\mathbf{Q}(\alpha)$ we have

$$(2)=(\alpha)^3, \quad (3)=\mathfrak{p}_3^3, \quad (5)=\mathfrak{p}_5\mathfrak{p}_5', \quad \text{with} \quad \mathfrak{p}_5=(1+\alpha^2);$$

and in $\mathbf{Q}(\beta)$

$$(2)=\mathfrak{p}_2^3, \quad (3)=\mathfrak{p}_3^3, \quad (5)=\mathfrak{p}_5^3.$$

In K

$$(2)=\mathfrak{q}_2^3\mathfrak{q}_2'^3 \text{ with } \mathrm{Norm}_1\,\mathfrak{q}_2=\mathfrak{p}_2,\ \mathrm{Norm}_2\,\mathfrak{q}_2=(\alpha),$$

https://doi.org/10.1017/S0305004100055055 Published online by Cambridge University Press

$$(3) = \mathfrak{q}_3^6 \mathfrak{q}_3'^3 \text{ with Norm } \mathfrak{q}_3 = \text{Norm } \mathfrak{q}_3' = 3,$$

$$(5) = \mathfrak{q}_5^3 \mathfrak{q}_5'^3 \text{ with Norm}_1 \mathfrak{q}_5 = \mathfrak{p}_5, \text{Norm}_2 \mathfrak{q}_5 = \mathfrak{f}_5.$$

By the theorem of the different (see, for example, chapter III of Lang(5)) we have that the different of K over $\mathbf{Q}$ is divisible by at least $\mathfrak{q}_2^2\mathfrak{q}_2'^2\mathfrak{q}_3^6\mathfrak{q}_3'^3\mathfrak{q}_5^2\mathfrak{q}_5'^2$; thus the discriminant of $\mathfrak{O}$ over $\mathbf{Q}$ is divisible by at least $2^6 . 3^9 . 5^6$. However, we can write down four linearly independent integers, e.g. $\lambda = \frac{1}{3}(1+\frac{1}{2}\alpha\beta^2+\frac{1}{2}\alpha^2\beta)$, $\lambda\alpha$, $\lambda\alpha^2$ and $\mu = \frac{1}{3}(1+\alpha)^2(\frac{1}{2}\alpha^2\beta-1)$, and the subring of $\mathfrak{O}$ generated by $\{1, \frac{1}{2}\alpha\beta, \frac{1}{4}\alpha^2\beta^2, \beta, \frac{1}{2}\beta^2, \lambda, \lambda\alpha, \lambda\alpha^2, \mu\}$ has by direct calculation, discriminant $2^6 . 3^{10} . 5^6$. If the index in $\mathfrak{O}$ of this module were divisible by 3, then the discriminant would be divisible by at most 3^8, which is not the case: we deduce that this is indeed a basis for the integers of K.

K contains four cubic subfields:

$$K_1 = \mathbf{Q}(\sqrt[3]{2}), \quad K_2 = \mathbf{Q}(\sqrt[3]{5}), \quad K_3 = \mathbf{Q}(\sqrt[3]{10}), \quad K_4 = \mathbf{Q}(\sqrt[3]{20})$$

with fundamental units ϵ_i and class-numbers h_i, $i = 1, 2, 3, 4$. Denote the index of $\mathfrak{O}'$ in $\mathfrak{O}$ by I, and similarly define i_j, $j = 1, 2, 3, 4$. Further, the fundamental units ϵ_j of the K_j together with -1 generate a group of finite index, say J, in the group of units of K. Then two fundamental lemmas from Cassels and Guy(2) are:

LEMMA. *The class-number H of K satisfies $HI = J \prod_{1 \leqslant j \leqslant 4} (h_j i_j)$*

LEMMA. *Let H', h_j' denote the parts of the class-numbers of K, k_j prime to 3. Then $H' = h_1' h_2' h_3' h_4'$.*

From Selmer(4) we have $h_1 = h_2 = h_3 = 1$, $h_4 = 3$; $i_1 = i_2 = i_4 = 1$, $i_3 = 3$; so H is a power of 3. Since we have shown above that $I = 3^4$, J is also a power of 3.

We claim that the following four units together with -1 give a fundamental basis for the units of K:

$$\eta_1 = -1+\alpha \quad (\eta_1 = \epsilon_1),$$

$$\eta_2 = \frac{2+\alpha^2}{\beta-2} \quad (\eta_2^3 = \epsilon_1^{-1}\epsilon_4^{-1}),$$

$$\eta_3 = \tfrac{1}{3}(\alpha+\beta-\tfrac{1}{4}\alpha^2\beta^2) \quad (\eta_3^3 = \epsilon_3),$$

$$\eta_4 = \tfrac{1}{3}(2-\tfrac{1}{2}\alpha\beta)(1-\alpha+\alpha^2) \quad (\eta_4^3 = \epsilon_1\epsilon_2).$$

Since J is a power of 3, it suffices to show that if

$$\eta_1^{a_1}\eta_2^{a_2}\eta_3^{a_3}\eta_4^{a_4} = \text{cube} \tag{4}$$

then $$a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 0 \text{ modulo } 3.$$

This is shown by recourse to congruences modulo the first-degree prime factors of 127 (the least rational prime to split into 9 first-degree factors in K). Jacobi(6) is invaluable for the numerical calculation.

The details are given in the following table; the first two columns identify the particular prime divisor $\mathfrak{P}$ of 127 in K by giving the residue classes of α and β mod $\mathfrak{P}$. The next four columns give the residue classes of $\eta_1, \eta_2, \eta_3, \eta_4$ mod $\mathfrak{P}$; and underneath, the

https://doi.org/10.1017/S0305004100055055 Published online by Cambridge University Press

indices of those columns (i.e. the power to which the primitive root 3 has to be raised to obtain the residue class), taken modulo 3.

α	β	η_1	η_2	η_3	η_4
122	105	121	110	41	45
122	59	121	74	79	42
122	90	121	97	2	102
32	105	31	116	104	80
		1	−1	−1	−1
		1	−1	1	−1
		1	1	0	0
		1	−1	1	0

Hence (4) implies that

$$\begin{aligned} a_1-a_2-a_3-a_4 &\equiv 0 \bmod 3,\\ a_1-a_2+a_3-a_4 &\equiv 0 \bmod 3,\\ a_1+a_2 \qquad\quad &\equiv 0 \bmod 3,\\ a_1-a_2+a_3 \qquad &\equiv 0 \bmod 3, \end{aligned}$$

whence $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 0 \bmod 3$, as required.

Consequently $J = 3^3$, and $H = 3$.

Denote the ideal class of $\mathfrak{q}_2$ by Γ; Γ is not the principal class, since $\mathrm{Norm}_1\, \mathfrak{q}_2 = \mathfrak{p}_2$, and $\mathfrak{p}_2$ is non-principal.

Considering elements with small norms, we find $\mathrm{Norm}\,(\eta_4 - 1) = -2.3^2$,

$$\mathrm{Norm}\,(2\eta_2 + 1) = 3^2.5.$$

$\mathrm{Norm}\,(\eta_4)$ and $\mathrm{Norm}\,(\eta_4 + 1)$ are prime to 3, so both $\mathfrak{q}_3, \mathfrak{q}_3'$ divide $(\eta_4 - 1)$; thus $(\eta_4 - 1) = \mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_3'$. Similarly $(2\eta_2 + 1) = \mathfrak{q}_3\,\mathfrak{q}_3'\,\mathfrak{q}_5$, and we deduce that

$$\mathfrak{q}_2' \in \Gamma^2, \quad \mathfrak{q}_5 \in \Gamma, \quad \mathfrak{q}_5' \in \Gamma^2.$$

3. *The family of surfaces.* Let $m \in \mathbf{Z}$, not divisible by 5, have the following property: m is the norm of an ideal of $\mathbf{Q}(\beta)$, but it is not the norm of any *principal* ideal of $\mathbf{Q}(\beta)$. For instance, take m to be any prime of the form $3n+2$ which has non-principal factors in $\mathbf{Q}(\beta)$. Then we claim that the Hasse principle fails to hold for the family of surfaces:

$$m(x^3 + 2y^3) = 10z^3 + 25t^3. \tag{5}$$

That (5) has a point everywhere locally, is easy. For the only primes needing special consideration are 2, 3, 5, and the primes dividing m. Suppose that any cube factor in m has been absorbed into x, y. Then if $p \mid m$, $p \neq 2, 3$, we have that 20 is a cube modulo p, and there is a p-adic solution with $x = y = 0$.

5-adically, we have a solution with $z = t = 0$.

If m is odd, there is a 2-adic solution with $y = z = 0$; if 2 exactly divides m, then a solution with $y = t = 0$; and if 4 exactly divides m, then a solution with $x = z = 0$.

It is easily seen that solubility mod 9 is sufficient for 3 adic solubility (cf. Skolem (7), p. 8); and since cubes mod 9 are 0, ± 1 the cubic form $u^3 + 2v^3$ represents $\{0, \pm 1, \pm 2, \pm 3\}$ mod 9. Thus

$$m(x^3 + 2y^3) \equiv z^3 + 2(-t)^3 \bmod 9 \text{ is always soluble.}$$

https://doi.org/10.1017/S0305004100055055 Published online by Cambridge University Press

We now show that (5) has no global point.

Denote the norm map from $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ to $\mathbf{Q}$ by norm_1, norm_2 respectively; then (5) may be written

$$5\mathfrak{m}\,\mathrm{norm}_1(x+\alpha y) = \mathrm{norm}_2(5t+\tfrac{1}{2}\beta^2 z). \tag{6}$$

Assume x, y, z, t are integers satisfying (6); without loss of generality, we can assume that x, y, z, t have no common factor. We now construct an integral ideal $\mathfrak{C}$ of K, and an ideal $\mathfrak{m}$ of $\mathbf{Q}(\beta)$ with norm m, such that

$$\begin{aligned}(x+\alpha y) &= \mathrm{Norm}_2\mathfrak{C},\\ (5t+\tfrac{1}{2}\beta^2 z) &= \mathfrak{p}_5\mathfrak{m}\,\mathrm{Norm}_1\mathfrak{C}.\end{aligned} \tag{7}$$

For write $(x+\alpha y) = n_1\gamma_1$, $(5t+\frac{1}{2}\beta^2 z) = n_2\gamma_2$, where n_1, n_2 are rational integers, and γ_1, γ_2 algebraic integers with no rational prime factor. Clearly 5 cannot divide n_1; moreover, only first degree primes in $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ can divide γ_1, γ_2 respectively. Let us deal with those primes dividing n_1. By assumption $(n_1, n_2) = 1$. Let $q \neq 2, 5$ be a prime which divides each side of equation (5), and let q divide n_1 to the rth power, m to the sth power, and $\mathrm{norm}_1(\gamma_1)$ to the tth power. $\mathfrak{q}_i = (q, \gamma_1)$, $i = 1, 2$, is a first degree prime factor of q in $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ respectively, and $\mathfrak{q}_2^{3r+s+t}$ divides γ_2. We make $\mathfrak{C}$ divisible by $\mathfrak{q}_2^r\mathfrak{Q}^t$, where $\mathfrak{Q} = (\mathfrak{q}_1, \mathfrak{q}_2)$ is a first degree prime factor of q in K, and make $\mathfrak{m}$ divisible by $\mathfrak{q}_2^s$. The remainder of the argument is in similar tedious vein, but straightforward when one remarks that for fixed x, y, z, t only one prime in $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ lying above a rational prime, can divide γ_1, γ_2 respectively.

We now examine the equations (7). By assumption $\mathfrak{m}$ is non-principal. If $\mathfrak{m} \sim \mathfrak{p}_2$ then we have

$$\begin{aligned}(\tfrac{1}{2}\beta^2 t + \beta z) &= \mathfrak{p}_2^{-1}\mathfrak{m}\,\mathrm{Norm}_1\mathfrak{D},\\ (\alpha^2 x + 2y) &= \mathrm{Norm}_2\mathfrak{D},\end{aligned}$$

where $\mathfrak{D}(= \mathfrak{q}_2^2\mathfrak{C})$ is principal; and if $\mathfrak{m} \sim \mathfrak{p}_2^2$ then we have

$$\begin{aligned}(5t+\tfrac{1}{2}\beta^2 z) &= \mathfrak{p}_5\mathfrak{m}\,\mathrm{Norm}_1\mathfrak{D},\\ (x+\alpha y) &= \mathrm{Norm}_2\mathfrak{D},\end{aligned}$$

where $\mathfrak{D}(= \mathfrak{C})$ is principal.

In either instance, $\mathrm{Norm}_1\mathfrak{D} \equiv 0 \bmod \mathfrak{p}_5$ and since $(x+\alpha y)$ cannot be divisible in $\mathbf{Q}(\alpha)$ by the second degree prime $\mathfrak{p}_5'$, we have $\mathfrak{D} \equiv 0 \bmod \mathfrak{q}_5$.

Put $\mathfrak{D} = (D)$, with $D = f + g\beta + h\beta^2$, $f, g, h \in \mathbf{Q}(\alpha)$, $f = u + v\alpha + w\alpha^2$, $u, v, w \in \mathbf{Q}$, with u, v, w 5-adic integers. Then $D \equiv f \equiv u - 2v - w \bmod \mathfrak{q}_5$ so $u - 2v - w \equiv 0 \bmod 5$.

However, $\mathrm{Norm}_2 D = f^3 + 20g^3 + 400h^3 - 60fgh$, so $\mathrm{Norm}_2\, D \equiv f^3 \bmod 5$,

i.e. $\mathrm{Norm}_2\, D \equiv (v^2w - 2vw^2) + \alpha(2v^3 - 2v^2w + w^3) + \alpha^2(v^3 - 2vw^2 - 2w^3) \bmod 5$.

Now $\mathrm{Norm}_2(\eta_4) = \epsilon_1$, so we may assume on multiplying D by an appropriate power of $\pm\eta_4$, that in the first instance

$$\alpha^2 x + 2y = \mathrm{Norm}_2 D$$

and in the second instance $\qquad x + \alpha y = \mathrm{Norm}_2 D.$

https://doi.org/10.1017/S0305004100055055 Published online by Cambridge University Press

But then comparing coefficients of α, α^2 gives $2v^3 - 2v^2w + w^3 \equiv 0$, $v^3 - 2vw^2 - 2w^3 \equiv 0$ respectively. In either case $v \equiv w \equiv u \equiv 0 \bmod 5$; and $\mathrm{Norm}_2 D \equiv 0 \bmod 5$, so

$$x \equiv y \equiv 0 \bmod 5, \quad z \equiv t \equiv 0 \bmod 5.$$

We finally observe that $m = 4$ gives the surface (3).

I extend thanks to Professor Cassels for making available the computer output, and to Professor Swinnerton-Dyer for suggesting some amendments in the manuscript.

REFERENCES

(1) Selmer E. S. Sufficient congruence conditions for the existence of rational points on certain cubic surfaces. *Math. Scand.* **1** (1953), 113–119.
(2) Cassels, J. W. S. and Guy, M. J. T. On the Hasse principle for cubic surfaces. *Mathematika* **13** (1966) 111–120.
(3) Manin, Y. I. *Cubic forms* (North Holland).
(4) Selmer, E. S. Tables for the purely cubic field $K(\sqrt[3]{m})$, *Avh. Norske Vid. Akad. Oslo I* (1955), no. 5.
(5) Lang, S. *Algebraic number theory* (Addison Wesley).
(6) Jacobi, C. G. J. *Canon arithmeticus* (*nach Berechnungen von W. Patz neu herausgegeben von H. Brandt*) (Akademie–Verlag, 1956).
(7) Skolem, Th. Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist. *Avh. Norske Vid. Akad. Oslo I* (1955), no. 4.

https://doi.org/10.1017/S0305004100055055 Published online by Cambridge University Press