Math. Ann. (2010) 346:41–50
DOI 10.1007/s00208-009-0383-z

Mathematische Annalen

Linear growth for Châtelet surfaces

T. D. Browning

Received: 14 January 2009 / Revised: 8 May 2009 / Published online: 27 June 2009

Abstract An upper bound of the expected order of magnitude is established for the number of $\mathbb{Q}$-rational points of bounded height on Châtelet surfaces defined over $\mathbb{Q}$.

Mathematics Subject Classification (2000) 11D45 (14G05)

1 Introduction

A Châtelet surface X over $\mathbb{Q}$ is a proper smooth model of an affine surface in $\mathbb{A}^3$ of the form

$$y^2 - az^2 = f(x), \tag{1}$$

where $a \in \mathbb{Z}$ is not a square and $f \in \mathbb{Z}[x]$ is a polynomial without repeated roots and degree 3 or 4. In the birational classification of rational surfaces summarised by Iskovskikh [8], Châtelet surfaces appear as some of the simplest non-trivial surfaces. They are conic bundle surfaces of degree 4, being equipped with a dominant morphism

$$\pi : X \to \mathbb{P}^1,$$

all of whose geometric fibres are conics. If $-K_X$ denotes the anticanonical divisor, then the linear system $|-K_X|$ has no base point and gives a morphism $\psi : X \to \mathbb{P}^4$ whose image is a singular del Pezzo surface of degree 4.

Writing $H = H_4 \circ \psi$, where $H_4 : \mathbb{P}^4(\mathbb{Q}) \to \mathbb{R}_{>0}$ is the exponential height metrized by an arbitrary choice of norm, the primary goal of this paper is to study the asymptotic behaviour of

$$N(B) = \#\{x \in X(\mathbb{Q}) : H(x) \leq B\},$$

T. D. Browning (✉)
School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
e-mail: t.d.browning@bristol.ac.uk

as $B \to \infty$. We will assume that $X(\mathbb{Q}) \neq \emptyset$ for all of the Châtelet surfaces under consideration here. The problem of determining when $X(\mathbb{Q}) \neq \emptyset$ is completely handled by the work of Colliot-Thélène et al. [3,4]. Our investigation of the counting function $N(B)$ is guided by a well-known conjecture of Manin [6], which predicts the existence of a constant $c_X > 0$ such that $N(B) \sim c_X B(\log B)^{\rho_X - 1}$, as $B \to \infty$, where ρ_X is the rank of the Picard group of X. With this in mind, the following is our main result.

Theorem *Let X be a Châtelet surface defined over $\mathbb{Q}$, arising as a proper smooth model of the affine surface* (1)*. Assume that $a < 0$. Then we have*

$$N(B) = O(B(\log B)^{\rho_X - 1}),$$

where ρ_X is the rank of the Picard group of X.

Here, as throughout our work, the implied constant is allowed to depend upon the surface. Although we will not present any details, it transpires that similar, but more intricate, arguments also permit one to handle the case $a > 0$ in the theorem.

Let

$$\beta_X = \lim_{B \to \infty} \frac{\log N(B)}{\log B}$$

be the growth rate of $X(\mathbb{Q})$. As a crude corollary of our theorem it follows that $\beta_X \leq 1$ for Châtelet surfaces. The question of obtaining lower bounds has recently been addressed by Iwaniec and Munshi [9], with an analysis of the case in which f is taken to be an irreducible cubic polynomial in (1). Their lower bound is difficult to compare with our work, however, since they work with a different height function. In forthcoming work of la Bretèche, Browning and Peyre, a resolution of the Manin conjecture is achieved for a family of Châtelet surfaces that corresponds to taking $a = -1$ and f a polynomial that is totally reducible into linear factors over $\mathbb{Q}$.

According to the investigation of Iskovskikh [8, Proposition 1] a conic bundle surface $X/\mathbb{P}^1$ of degree 4 arises in two possible ways. Either the anticanonical divisor $-K_X$ is not ample, in which case X is a Châtelet surface, or else $-K_X$ is ample, in which case X is a non-singular quartic del Pezzo surface. Our proof of the theorem makes essential use of the conic bundle structure of Châtelet surfaces. It is inspired by an approach adopted by Salberger, as communicated at the conference "Higher-dimensional varieties and rational points" in Budapest in 2001, for the class of non-singular quartic del Pezzo surfaces with a conic bundle structure. For such surfaces an upper bound $O_\varepsilon(B^{1+\varepsilon})$ is achieved for the corresponding counting function by taking advantage of the morphism $\pi : X \to \mathbb{P}^1$ in order to count rational points of bounded height on the conics $\pi^{-1}(p)$, uniformly for points $p \in \mathbb{P}^1(\mathbb{Q})$ of small height. In subsequent work Leung [10] has refined this argument, replacing B^ε by $(\log B)^A$ for a certain integer $A \leq 5$. However, the value of A is often bigger than the exponent predicted by Manin. A pedestrian translation of these arguments from del Pezzo surfaces to Châtelet surfaces would lead to a similar deficiency. To overcome this, we will gain significant extra leverage by restricting the summation to only

those $p \in \mathbb{P}^1(\mathbb{Q})$ of small height that produce isotropic conics $\pi^{-1}(p)$. It seems likely that this innovation could also be put to use in the analogous situation studied by Leung [10].

2 Geometric preliminaries

Let $F(u, v) = v^4 f(\frac{u}{v})$, a binary quartic form with integer coefficients. We denote by $X_1 \subset \mathbb{P}^2 \times \mathbb{A}^1$ the hypersurface

$$y_1^2 - az_1^2 = t_1^2 F(u, 1),$$

and by $X_2 \subset \mathbb{P}^2 \times \mathbb{A}^1$ the hypersurface

$$y_2^2 - az_2^2 = t_2^2 F(1, v).$$

The Châtelet surface associated with (1) is the geometrically integral smooth projective surface obtained by patching together X_1, X_2 via the isomorphism

$$\begin{aligned} X_1 \backslash \{u = 0\} &\longrightarrow X_2 \backslash \{v = 0\}, \\ ([y_1, z_1, t_1]; u) &\longmapsto ([y_1, z_1, u^2 t_1]; u^{-1}). \end{aligned}$$

Since f has non-zero discriminant, we have a factorisation

$$F(u, v) = (\beta_1 u - \alpha_1 v)(\beta_2 u - \alpha_2 v)(\beta_3 u - \alpha_3 v)(\beta_4 u - \alpha_4 v),$$

over $\overline{\mathbb{Q}}$, with $[\alpha_1, \beta_1], \ldots, [\alpha_4, \beta_4] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ distinct. The morphisms $X_1 \to \mathbb{P}^1$ and $X_2 \to \mathbb{P}^1$ given by $([y_1, z_1, t_1]; u) \mapsto [u, 1]$ and $([y_2, z_2, t_2]; v) \mapsto [1, v]$, respectively, glue together to give a conic fibration $\pi : X \to \mathbb{P}^1$. It has four degenerate geometric fibres over the points $p_i = [\alpha_i, \beta_i] \in \mathbb{P}^1(\overline{\mathbb{Q}})$, for $1 \leq i \leq 4$. The geometric fibre above p_i is the subvariety of X defined by $u = \alpha_i$ and $y_1 \pm \sqrt{a} z_1 = 0$. This defines a union of two geometrically integral divisors that intersect transversally and are both isomorphic to $\mathbb{P}^1$ over $\overline{\mathbb{Q}}$.

Let $\mathrm{Pic}(X)$ be the Picard group of X. Then $\mathrm{Pic}(X)$ is a torsion-free $\mathbb{Z}$-module with finite rank ρ_X, say. An explicit description of ρ_X is given in the following result.

Lemma 1 *Suppose that $f = f_1 \cdots f_r$ is the factorisation into irreducibles of f over $\mathbb{Q}$. For each $1 \leq i \leq r$ let $\mathbb{Q}_{f_i} = \mathbb{Q}[x]/(f_i)$ denote the field obtained by adjoining a root of f_i to $\mathbb{Q}$. Then we have*

$$\rho_X = 2 + \#\{1 \leq i \leq r : \sqrt{a} \in \mathbb{Q}_{f_i}\}.$$

Proof There is a homomorphism $\mathrm{Pic}(X) \to \mathbb{Z}$, which to a divisor class in $\mathrm{Pic}(X)$ associates its intersection number with the fibre of the morphism $\pi : X \to \mathbb{P}^1$ above a closed point of $\mathbb{P}^1$. The image of this map has finite index in $\mathbb{Z}$. Moreover, the kernel

is generated by the "vertical" divisors, namely those which are supported in finitely many fibres of π.

We now choose an irreducible fibre of the morphism $\pi : X \to \mathbb{P}^1$. Furthermore, in each reducible fibre, we choose one of the two components. Let D be the free abelian group generated by all of these divisors. It plainly follows that

$$\operatorname{rank}(D) = 1 + \#\{1 \leq i \leq r : \sqrt{a} \in \mathbb{Q}_{f_i}\},$$

since the residue field of the closed point corresponding to f_i is just $\mathbb{Q}_{f_i}$.

Finally, we note that the natural map from D to $\operatorname{Pic}(X)$ is injective and it identifies D with the kernel of $\operatorname{Pic}(X) \to \mathbb{Z}$. Therefore we have

$$\rho_X = 1 + \operatorname{rank}(D),$$

as required to complete the proof of the lemma. □

3 Proof of the theorem

In what follows it will be convenient to use the notation Z^m for the set of primitive vectors in $\mathbb{Z}^m$. The following result translates the problem to one involving a family of conics.

Lemma 2 *Suppose that the exponential height H_4 on $\mathbb{P}^4(\mathbb{Q})$ is metrized by a norm $\|\cdot\|$ on $\mathbb{R}^5$. Then we have $N(B) = \frac{1}{4}T(B)$, where*

$$T(B) = \#\left\{(y, z, t; u, v) \in Z^3 \times Z^2 : \begin{array}{l} \|(v^2t, uvt, u^2t, y, z)\| \leq B \\ y^2 - az^2 = t^2F(u, v) \end{array}\right\}.$$

Proof Suppose that $f(x) = c_0x^4 + \cdots + c_4$ in (1) for $c_i \in \mathbb{Z}$. Consider the maps $\psi_i : X_i \to \mathbb{P}^4$ given by

$$\psi_1 : ([y_1, z_1, t_1]; u) \longmapsto [t_1, ut_1, u^2t_1, y_1, z_1],$$
$$\psi_2 : ([y_2, z_2, t_2]; v) \longmapsto [v^2t_2, vt_2, t_2, y_2, z_2].$$

These induce a morphism $\psi : X \to \mathbb{P}^4$ whose image is the del Pezzo surface

$$\begin{cases} x_0x_2 = x_1^2, \\ x_3^2 - ax_4^2 = c_4x_0^2 + c_3x_0x_1 + c_2x_0x_2 + c_1x_1x_2 + c_0x_2^2, \end{cases}$$

which we denote by Y. Let us write $Q(x_0, x_1, x_2)$ for the quadratic form appearing on the right hand side of the second equation.

Let $H = H_4 \circ \psi$, where H_4 is the exponential height on $\mathbb{P}^4(\mathbb{Q})$ defined by $H_4([\mathbf{x}]) = \|\mathbf{x}\|$ if $\mathbf{x} \in Z^5$. Then we have

$$N(B) = \frac{1}{2}\#\{\mathbf{x} \in Z^5 : [\mathbf{x}] \in Y,\ \|\mathbf{x}\| \leq B\}.$$

There is a $1:2$ correspondence between integer solutions of the equation $x_0x_2 = x_1^2$ and vectors $(t, u, v) \in \mathbb{Z}^3$ such that u, v are coprime, given by $(x_0, x_1, x_2) = t(v^2, uv, u^2)$. Furthermore, the primitivity of $\mathbf{x}$ is equivalent to the vector (t, x_3, x_4) being primitive. Substituting this into the second equation, with $Q(v^2, uv, u^2) = F(u, v)$, we therefore arrive at the statement of Lemma 2. □

In our work we are only interested in an upper bound for $N(B)$. By equivalence of norms it will suffice to work with the norm $\|\mathbf{x}\| = \max_{0\leq i\leq 4} |x_i|$ on $\mathbb{R}^5$. Since a is not a square we must have $|t| \geq 1$ in each solution to be counted, whence $\max\{u^2, v^2\} \leq B$. There will be no loss of generality in fixing attention on the contribution from u, v such that $|u| \leq |v|$. Let $\mathcal{A}$ denote the set of $(u, v) \in Z^2$ for which $|u| \leq |v| \leq \sqrt{B}$ and $F(u, v) \neq 0$. Then it follows from Lemma 2 that

$$N(B) \ll \sum_{(u,v)\in\mathcal{A}} M_{u,v}(B),$$

where

$$M_{u,v}(B) = \#\left\{(y, z, t) \in Z^3 : \begin{array}{l} \max\{v^2|t|, |y|, |z|\} \leq B \\ y^2 - az^2 = t^2F(u, v) \end{array}\right\}.$$

We would now like to thin down the outer summation by restricting attention to those $(u, v) \in \mathcal{A}$ for which the conic $y^2 - az^2 = t^2F(u, v)$ has a non-trivial rational point.

For our purposes it will suffice to restrict attention to those $(u, v) \in \mathcal{A}$ for which the Legendre symbol $(\frac{a}{p})$ is distinct from -1 for each odd prime p such that $p\|F(u, v)$. Here we write $p\|n$ for $n \in \mathbb{Z}$ if $p \mid n$ but $p^2 \nmid n$. To see that this is satisfactory one merely notes that if $p\|F(u, v)$ then the equation for the conic implies that $y^2 \equiv az^2 \bmod p$ and $p \nmid \gcd(y, z)$, since $\gcd(y, z, t) = 1$ in each solution counted.

Define the arithmetic function

$$\vartheta(n) = \prod_{p\|n} 2^{-1}\left(1 + \left(\frac{a}{p}\right)\right), \tag{2}$$

where we have extended the Legendre symbol to all primes by setting $(\frac{a}{2}) = 0$. The function ϑ is multiplicative, non-negative and satisfies

$$\vartheta(p^\ell) = \begin{cases} \frac{1}{2}, & \text{if } \ell = 1 \text{ and } p \mid 2a, \\ 0, & \text{if } \ell = 1 \text{ and } (\frac{a}{p}) = -1, \\ 1, & \text{otherwise,} \end{cases}$$

for any prime power p^ℓ. We will use ϑ as a characteristic function to weed out values of $(u, v) \in \mathcal{A}$ that produce anisotropic conics. In this way we obtain

$$N(B) \ll \sum_{(u,v)\in\mathcal{A}} \vartheta(|F(u, v)|)M_{u,v}(B).$$

The task of estimating $M_{u,v}(B)$ boils down to counting rational points on a geometrically integral plane conic, with the points constrained to lie in a lop-sided region. For this we can take advantage of work of Browning and Heath-Brown [2, Corollary 2], a key feature of which being its uniformity with respect to the height of the conic. Since $a < 0$ it follows that we may replace the height restrictions on y, z, t in $M_{u,v}(B)$ by

$$y, z \ll \frac{B|F(u, v)|^{\frac{1}{2}}}{v^2}, \quad |t| \le \frac{B}{v^2},$$

as follows from the equation for the conic. Our conic is defined by a ternary quadratic form $\mathbf{x}^T\mathbf{M}\mathbf{x}$, where $\mathbf{x} = (y, z, t)$ and $\mathbf{M} = \mathrm{Diag}(1, -a, -F(u, v))$. In particular the greatest common divisor of the 2×2 minors of $\mathbf{M}$ is $O(1)$ and its determinant is $aF(u, v)$. The inequalities satisfied by y, z, t above define a box in $\mathbb{R}^3$ with volume $O(v^{-6}B^3|F(u, v)|)$. It now follows from [2, Corollary 2] that

$$M_{u,v}(B) \ll 2^{\omega(F(u,v))}\left(1 + \frac{B}{v^2}\right) \ll B\frac{2^{\omega(F(u,v))}}{v^2},$$

since $|v| \le \sqrt{B}$. Note that we have replaced the divisor function by the function $2^{\omega(\cdot)}$ in our application of this result, where $\omega(n)$ denotes the number of distinct prime divisors of n. An inspection of the proof reveals that is permissible.

Let $\varpi(n) = 2^{\omega(n)}\vartheta(n)$, where ϑ is given by (2). Then our analysis so far has shown that

$$N(B) \ll B \sum_{(u,v)\in\mathcal{A}} \frac{\varpi(|F(u, v)|)}{v^2}. \tag{3}$$

In view of the trivial bound $\varpi(n) = O_\varepsilon(n^\varepsilon)$ for any $\varepsilon > 0$, it would be easy to conclude at this point that $N(B) = O_\varepsilon(B^{1+\varepsilon})$. To get the correct power of $\log B$ emerging we must work somewhat harder. For given $U, V \ge 1$ it will be convenient to introduce the sum

$$S(U, V) = \sum_{|u|\le U} \sum_{|v|\le V} \varpi(|F(u, v)|).$$

The estimation of $S(U, V)$ is the subject of the following result, whose proof we will defer to the next section.

Lemma 3 *Let $V \geq U \geq 1$. Then for all $\varepsilon > 0$ we have*

$$S(U, V) \ll_\varepsilon UV(\log V)^{\rho_X - 2} + V^{1+\varepsilon}.$$

We now have everything in place to complete the proof of the theorem. Returning to (3) we see that there is an overall contribution of $O(B)$ from those $(u, v) \in \mathcal{A}$ with $u = 0$. Breaking the summation of the remaining u, v into dyadic intervals we therefore find

$$\begin{aligned} N(B) &\ll B + B \sum_{\substack{i,j \in \mathbb{Z} \\ -1 \leq i < j \leq \frac{1}{2\log 2} \log B}} \sum_{2^i < |u| \leq 2^{i+1}} \sum_{2^j < |v| \leq 2^{j+1}} \frac{\varpi(|F(u, v)|)}{v^2} \\ &\ll B + B \sum_{\substack{i,j \in \mathbb{Z} \\ -1 \leq i < j \leq \frac{1}{2\log 2} \log B}} \frac{S(2^{i+1}, 2^{j+1})}{2^{2j}}. \end{aligned}$$

Here we have dropped the conditions that $F(u, v) \neq 0$ and $\gcd(u, v) = 1$, as permitted by the fact that the summand is non-negative. Applying Lemma 3 we therefore deduce that

$$N(B) \ll B + B(\log B)^{\rho_X - 2} \sum_{\substack{i,j \in \mathbb{Z} \\ -1 \leq i < j \leq \frac{1}{2\log 2} \log B}} \frac{2^i}{2^j} \ll B(\log B)^{\rho_X - 1},$$

as required to complete the proof of the theorem.

4 Proof of Lemma 3

Determining the average order of arithmetic functions as they range over the values of polynomials has a substantial pedigree in analytic number theory. For the proof of Lemma 3 we will need to analyse the average order of the arithmetic function

$$\varpi(n) = 2^{\omega(n)} \prod_{p \| n} 2^{-1} \left(1 + \left(\frac{a}{p}\right)\right),$$

as it ranges over the values of the binary quartic form F.

The key technical tool for this argument is supplied by work of la Bretèche and Browning [1]. We recall that F has non-zero discriminant and observe that ϖ is a non-negative multiplicative arithmetic function satisfying the estimates $\varpi(n) = O_\varepsilon(n^\varepsilon)$ and $\varpi(p^\ell) \leq 2$ for $n \in \mathbb{N}$ and prime powers p^ℓ. In view of the fact that $\varpi(p) = 1 + (\frac{a}{p})$, we may therefore conclude from [1, Corollary 1] that

$$S(U, V) \ll_\varepsilon UVE_f(U) + V^{1+\varepsilon},$$

for any $\varepsilon > 0$, where

$$E_f(U) = \prod_{1 \ll p \leq U} \left(1 + \frac{\rho_f(p)(\frac{a}{p})}{p}\right).$$

Here $f(x) = F(x, 1)$ is the polynomial appearing in (1) and $\rho_f(m)$ is the number of solutions to the congruence $f(x) \equiv 0 \bmod m$ in $\mathbb{Z}/m\mathbb{Z}$.

Suppose that $f = f_1 \cdots f_r$ is the factorisation into irreducibles of f over $\mathbb{Q}$, with $\sum_{i=1}^{r} \deg f_i \in \{3, 4\}$. Then we have

$$E_f(U) \ll E_{f_1}(U) \cdots E_{f_r}(U).$$

Our attention now shifts to estimating $E_f(U)$ for any $U \geq 2$ and any irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d with non-zero discriminant. We will show that

$$E_f(U) \ll \begin{cases} 1, & \text{if } \sqrt{a} \notin \mathbb{Q}_f, \\ \log U, & \text{if } \sqrt{a} \in \mathbb{Q}_f, \end{cases} \tag{4}$$

where $\mathbb{Q}_f = \mathbb{Q}[x]/(f)$ denotes the field obtained by adjoining a root of f to $\mathbb{Q}$. In view of Lemma 1 this will suffice for the statement of Lemma 3.

In order to understand the asymptotic behaviour of $E_f(U)$ we must investigate the analytic properties of the L-function

$$H(s) = \prod_{p} \left(1 + \frac{\rho_f(p)(\frac{a}{p})}{p^s}\right), \quad (\Re(s) > 1).$$

We will do so by relating $H(s)$ to a certain Hecke L-function and analysing it in the neighbourhood of $s = 1$. The necessary facts are classical and can be found in the work of Heilbronn [7] and Neukirch [12, Chap. VII].

Let $K = \mathbb{Q}_f$ and and let d_K denote its discriminant. We write $\mathfrak{a} = (2ad_K)$ for the ideal generated by $2ad_K$ in $\mathfrak{o}_K$. Furthermore, let $N(\mathfrak{n}) = |\mathfrak{o}_K/\mathfrak{n}|$ denote the norm of any ideal $\mathfrak{n}$ in $\mathfrak{o}_K$. For a prime ideal $\mathfrak{p}$ in $\mathfrak{o}_K$ which is coprime to $\mathfrak{a}$ we define

$$\chi(\mathfrak{p}) = \left(\frac{a}{N(\mathfrak{p})}\right) = \left(\frac{a}{p}\right)^{\ell},$$

if $N(\mathfrak{p}) = p^{\ell}$, where $(\frac{a}{p})$ is the ordinary Legendre symbol. One extends χ to all fractional ideals coprime to $\mathfrak{a}$ by multiplicativity. Then χ is a group homomorphism from the ray class group $J^{\mathfrak{a}}/P^{\mathfrak{a}}$ to $\{\pm 1\}$. Here $J^{\mathfrak{a}}$ is the group of ideals coprime to $\mathfrak{a}$ and $P^{\mathfrak{a}}$ is the subgroup of fractional principal ideals (α) for which $\alpha \equiv 1 \bmod \mathfrak{a}$ and $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \to \mathbb{R}$. Thus χ is a generalised Dirichlet character modulo $\mathfrak{a}$. A principal character modulo $\mathfrak{a}$ is any character χ_0 such that $\chi_0(\mathfrak{n}) = 1$ for all $\mathfrak{n} \in J^{\mathfrak{a}}$. Finally, we extend χ to all integral ideals by setting $\chi(\mathfrak{n}) = 0$ if $\mathfrak{n}$ has a factor in common with $\mathfrak{a}$.

The Hecke L-function associated to the number field K and the quadratic character χ is defined to be

$$L_K(s,\chi)=\sum_{\mathfrak{n}}\frac{\chi(\mathfrak{n})}{N(\mathfrak{n})^s}=\sum_{n=1}^{\infty}\frac{b(n)}{n^s},\quad(\Re(s)>1),$$

where the first sum is over integral ideals and $b(n)=\sum_{N(\mathfrak{n})=n}\chi(\mathfrak{n})$. For a rational prime p one notes that

$$b(p)=\sum_{N(\mathfrak{p})=p}\chi(\mathfrak{p})=\left(\frac{a}{p}\right)\#\{\mathfrak{p}:N(\mathfrak{p})=p\}.$$

Now for $p\nmid d_K$ there is a well-known principle due to Dedekind [5, p. 212] which ensures that $\rho_f(p)=\#\{\mathfrak{p}:N(\mathfrak{p})=p\}$. A modern account of this fact can be found in the work of Narkiewicz [11, §4.3]. Employing a standard calculation based on partial summation and the prime ideal theorem, we therefore conclude that

$$E_f(U)\ll\exp\left(\sum_{N(\mathfrak{p})\leq U}\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})}\right)\ll\begin{cases}1, & \text{if } \chi\neq\chi_0,\\ \log U, & \text{if } \chi=\chi_0.\end{cases}$$

In order to complete the proof of (4) it therefore remains to show that χ is principal if and only if $\sqrt{a}\in K$. For any finite extension N/M of number fields, let $P(N/M)$ denote the set of all unramified prime ideals of M which admit in N a prime divisor of residue class degree 1 over M.

Suppose first that $\sqrt{a}\in K$ and write $J=\mathbb{Q}(\sqrt{a})$. Then we have a tower of separable extensions $\mathbb{Q}\subseteq J\subseteq K$. If χ is not principal then there is a prime ideal $\mathfrak{p}$ above a rational prime $p\nmid 2ad_K$ with odd residue class degree, such that $(\frac{a}{p})=-1$. In particular p is inert in J, with residue class degree 2. But then the transitivity of norms implies that the residue class degree of $\mathfrak{p}$ is even, which is a contradiction.

We now argue in the reverse direction, taking for our hypothesis the assumption that χ is principal. This is equivalent to $\chi(\mathfrak{p})=1$ for all prime ideals $\mathfrak{p}$ coprime to $\mathfrak{a}$. Any unramified rational prime p factorises as $(p)=\mathfrak{p}_1\ldots\mathfrak{p}_r$ with distinct primes $\mathfrak{p}_i$ such that $N(\mathfrak{p}_i)=p^{\ell_i}$ and $\sum_{i=1}^r\ell_i=[K:\mathbb{Q}]$. It follows that $(\frac{a}{p})=1$ for any prime $p\nmid 2ad_K$ such that $(p)\in P(K/\mathbb{Q})$. But then any such p splits completely in $J=\mathbb{Q}(\sqrt{a})$ since $(\frac{a}{p})=1$, whence $(p)\in P(J/\mathbb{Q})$. We have therefore shown that $P(K/\mathbb{Q})$ is contained in $P(J/\mathbb{Q})$, up to finitely many exceptional elements. It now follows from Bauer's theorem [12, §VII.13] that $J\subseteq K$, so that $\sqrt{a}\in K$.

Acknowledgments This article addresses a question that was posed by J.-L. Colliot-Thélène at the meeting "Rational points on curves and higher-dimensional varieties" in Warwick in June 2008. It is a pleasure to thank R. de la Bretèche, A. Gorodnik and O. Wittenberg for a number of useful comments, in addition to the anonymous referee for his careful reading of the manuscript. While working on this paper the author was supported by EPSRC grant number EP/E053262/1.

References

1. de la Bretèche, R., Browning, T.D.: Sums of arithmetic functions over values of binary forms. Acta Arith. **125**, 291–304 (2007)
2. Browning, T.D., Heath-Brown, D.R.: Counting rational points on hypersurfaces. J. Reine Angew. Math. **584**, 83–115 (2005)
3. Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, P.: Intersections of two quadrics and Châtelet surfaces. I. J Reine Angew. Math. **373**, 37–107 (1987)
4. Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, P.: Intersections of two quadrics and Châtelet surfaces. II. J Reine Angew. Math. **374**, 72–168 (1987)
5. Dedekind, R.: Gesammelte Mathematische Werke, Band, vol. 1. Braunschweig, Friedr. Vieweg & Sohn (1930)
6. Franke, J., Manin, Y.I., Tschinkel, Y.: Rational points of bounded height on Fano varieties. Invent. Math. **95**, 421–435 (1989)
7. Heilbronn, H.: Zeta-functions and L-functions. Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pp. 204–230. Academic Press, London (1967)
8. Iskovskikh, V.A.: Minimal models of rational surfaces over arbitrary fields. Math. USSR Izv. **14**, 17–39 (1980)
9. Iwaniec, H., Munshi, R.: Cubic polynomials and quadratic forms. Proc. Lond. Math. Soc. (2009, to appear)
10. Leung, F.-S.: Manin's conjecture on a non-singular quartic del Pezzo surface. D.Phil thesis, Oxford (2008)
11. Narkiewicz, W.: Elementary and analytic theory of algebraic numbers, 3rd edn. Springer Monographs in Math., Springer, Heidelberg (2004)
12. Neukirch, J.: Algebraic number theory. Grund. Math. Wissenschaften, vol. 322. Springer, Heidelberg (1999)