ESSENTIAL NUMBER THEORY

A Diophantine problem about Kummer surfaces

William Duke

2022

vol. 1 no. 1

msp

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.51

A Diophantine problem about Kummer surfaces

William Duke

Upper and lower bounds are given for the number of rational points of bounded height on a double cover of projective space ramified over a Kummer surface.

1. Introduction

Let $F(x) = F(x_0, \ldots, x_n)$ with $n \geq 2$ be an integral form with $\deg F \geq 2$ and set

$$N_F(T) = \#\{x \in \mathbb{Z}^{n+1} \mid F(x) = z^2 \text{ for some } z \in \mathbb{Z}, \gcd(x_0, \ldots, x_n) = 1 \text{ and } \|x\| \leq T\}, \tag{1-1}$$

where $\|x\| = \max_j(|x_j|)$. The behavior of $N_F(T)$ for large T is of basic Diophantine interest. When $\deg F$ is even, $N_F(T)$ counts rational points of bounded height on a double cover of $\mathbb{P}^n_{\mathbb{Q}}$ ramified over the hypersurface given by $F(x) = 0$.

Assume that $\deg F$ is even and that $z^2 - F(x)$ is irreducible over $\mathbb{C}$. It follows from Theorem 3 on page 178 of [Serre 1989] that for any $\epsilon > 0$

$$N_F(T) \ll T^{n+1/2+\epsilon}. \tag{1-2}$$

As discussed after Theorem 3 in [Serre 1989], it is reasonable to expect that

$$N_F(T) \ll T^{n+\epsilon}. \tag{1-3}$$

Broberg [2003] improved $\frac{5}{2}$ to $\frac{9}{4}$ in (1-2) when $n = 2$. For $n \geq 3$, various improvements and generalizations of (1-2) are given in [Munshi 2009; Heath-Brown and Pierce 2012; Bonolis 2021], assuming that $F(x) = 0$ is nonsingular. Certain nonhomogeneous F are treated in [Heath-Brown and Pierce 2012].

In this note I will consider the problem of estimating $N_F(T)$ from above *and below* when $n = 3$ for a special class of quartic F, namely those for which $F(x) = 0$ define certain Kummer surfaces. These surfaces have singularities (nodes).

For our purpose we will define a Kummer surface in terms of an integral sextic polynomial $P(t)$. For fixed $a, b, c, d, e, f, g \in \mathbb{Z}$ with $a \neq 0$ let

$$P(t) = at^6 + bt^5 + ct^4 + dt^3 + et^2 + ft + g.$$

Research supported by NSF grant DMS 1701638 and Simons Foundation Award Number 554649.
MSC2020: 11Dxx, 11E76.
Keywords: Diophantine equations, Kummer surfaces, rational points.

Suppose that the discriminant of P is not zero. Define the symmetric matrices

$$S_0 = \begin{pmatrix} a & \frac{b}{2} & 0 & 0 \\ \frac{b}{2} & c & \frac{d}{2} & 0 \\ 0 & \frac{d}{2} & e & \frac{f}{2} \\ 0 & 0 & \frac{f}{2} & g \end{pmatrix} \tag{1-4}$$

and

$$S_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}, \quad S_3 = \begin{pmatrix} 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{1-5}$$

For $x = (x_0, x_1, x_2, x_3)$ define the matrix

$$S_x = x_0 S_0 + x_1 S_1 + x_2 S_2 + x_3 S_3.$$

For a row vector v let $S(v) = vSv^t$ denote the quadratic form associated to a symmetric matrix S. It is easy to check that *for any* x we have the identity

$$x_0 P(t) = S_x(t^3, t^2, t, 1).$$

Define the associated quartic form F by

$$F(x) := 16 \det S_x. \tag{1-6}$$

Over $\mathbb{C}$ the surface given by $F(x) = 0$ is a Kummer surface, a special determinantal quartic surface that is singular with sixteen nodes, including the points $(t^3, t^2, t, 1)$ where t is a root of $P(t) = 0$. The Jacobian variety of the genus two hyperelliptic curve $y^2 = P(t)$ is a double cover of the Kummer surface ramified over these nodes. For details on the geometry of Kummer surfaces; see, e.g., [Hudson 1990; Dolgachev 2012]. Some arithmetic aspects of Kummer surfaces are considered in [Cassels and Flynn 1996]. The construction of a Kummer surface using the S_j from (1-4) and (1-5) occurs in a slightly different form in [Baker 1907, page 69]; see also [Cassels and Flynn 1996, page 42].

Our main result is the following.

Theorem 1. *Suppose that* $P(t) = at^6 + bt^5 + ct^4 + dt^3 + et^2 - 2t$ *with integral* a, b, c, d, e *has nonzero discriminant and* $a \neq 0$. *Let* F *be defined in* (1-6) *and* $N_F(T)$ *in* (1-1). *Then for any* $\epsilon > 0$

$$T^2 \ll N_F(T) \ll T^{3+\epsilon}, \tag{1-7}$$

where the first implied constant depends only on P *and the second depends only on* P *and* ϵ.

Our approach to these estimates relies on the special form of the Kummer surfaces we consider. In particular, for the upper bound we use that in P we assume that $g = 0$. For the lower bound we use that $g = 0$ and $f = -2$. The upper bound coincides with that given in (1-3). An example of an equation to which Theorem 1 applies, when $P(t) = t^6 - 2t$, is

$$z^2 = x_3^2(x_1^2 + 8x_0x_2) + x_3(-16x_0^3 - 2x_1x_2^2) - 4x_0x_1^3 - 8x_0^2x_1x_2 + x_2^4.$$

Numerical calculations in this case show that we seem to have $N_F(T) \gg T^{3-\epsilon}$. It would be of interest to find the correct order of magnitude of $N_F(T)$ for some P.

Remark. Most research on $N_F(T)$ in (1-1) has concentrated on giving upper bounds for $N_F(T)$ for quite general F, where $F(x) = 0$ is usually assumed to be nonsingular. The proofs often make use of intricate estimates of character and exponential sums; for example, see [Heath-Brown and Pierce 2012]. In contrast, the proof of the upper bound of (1-7) is rather straightforward. Although it is likely not sharp, the lower bound of (1-7) is probably more interesting and certainly deeper. Its proof uses a remarkable and not well-known identity of Schottky to explicitly produce solutions to $F(x) = z^2$. Along somewhat similar lines, invariant theory was recently applied to asymptotically count integer points on quadratic twists of certain elliptic curves and give a class number formula for binary quartic forms [Duke 2021]. It is reasonable to hope that some other classical identities of algebraic geometry and syzygies of invariant theory, some of which are beautifully presented in [Dolgachev 2012], could have still undiscovered applications to the problem of finding lower bounds for counting functions like $N_F(T)$.

2. Proof of the theorem

Upper bound. The mechanism behind the proof of the upper bound in (1-7) is that a quadratic Diophantine equation in two variables has "few" solutions. The argument relies on the fact that for $P(t)$ of the assumed form (so that in particular $g = 0$), the associated F has the property that it is quadratic in one of its variables. It will become clear that similar arguments can be applied to other F with this property.

For a general $P(t)$ we have the explicit formula

$$\begin{aligned}F(x) = x_0^4&(16aceg - 4acf^2 - 4ad^2g - 4b^2eg + b^2f^2)\\ &- 2x_0^3(-8acgx_1 + 2adfx_1 - 4adgx_2 - 8aegx_3 + 2af^2x_3 + 2b^2gx_1\\ &\qquad + bdfx_2 + 2bdgx_3)\\ &+ x_0^2(-4aex_1^2 + 4afx_1x_2 + 16agx_1x_3 - 4agx_2^2 - 4bex_1x_2 - 2bfx_1x_3\\ &+ 2bfx_2^2 + 4bgx_2x_3 - 4cex_2^2 - 4cfx_2x_3 - 4cgx_3^2 + d^2x_2^2)\\ &- 2x_0(2ax_1^3 + 2bx_1^2x_2 + 2cx_1x_2^2 + dx_1x_2x_3 + dx_2^3 + 2ex_2^2x_3 + 2fx_2x_3^2 + 2gx_3^3)\\ &+ (x_2^2 - x_1x_3)^2.\end{aligned}$$

For $P(t)=at^6+bt^5+ct^4+dt^3+et^2-2t$ we have that F has an expansion that is quadratic in x_3:

$$\begin{aligned}F(x)=x_3^2(x_1^2+8x_2x_0)&\\ &+x_3(-16ax_0^3+4bx_0^2x_1+8cx_0^2x_2-2dx_0x_1x_2-4ex_0x_2^2-2x_1x_2^2)\\ &+4b^2x_0^4-16acx_0^4+8adx_0^3x_1-4aex_0^2x_1^2-4ax_0x_1^3+4bdx_0^3x_2\\ &-8ax_0^2x_1x_2-4bex_0^2x_1x_2-4bx_0x_1^2x_2-4bx_0^2x_2^2+d^2x_0^2x_2^2\\ &-4cex_0^2x_2^2-4cx_0x_1x_2^2-2dx_0x_2^3+x_2^4.\end{aligned} \tag{2-1}$$

Thus given a solution x of $z^2=F(x)$, upon completing the square we will get a solution (y,z) of

$$y^2-(x_1^2+8x_2x_0)z^2=k(x_0,x_1,x_2) \tag{2-2}$$

where

$$k(x_0,x_1,x_2)=8x_0x_2^5-64a^2x_0^5+\cdots$$

is a homogeneous integral form of degree 6 that is not identically zero, and where

$$y=(x_1^2+8x_2x_0)x_3+(8ax_0^3-2bx_0^2x_1-4cx_0^2x_2+dx_0x_1x_2+2ex_0x_2^2+x_1x_2^2). \tag{2-3}$$

The number of x_0,x_1,x_2 with $|x_0|,|x_1|,|x_2|\le T$ where either

$$k(x_0,x_1,x_2)=0 \quad \text{or} \quad x_1^2+8x_2x_0=0$$

is $\ll T^2$. For such x_0,x_1,x_2, by (2-2) and (2-3) the total number of solutions of $F(x)=z^2$ with $|x_3|\le T$ is $\ll T^3$.

For any other x_0,x_1,x_2 with $|x_0|,|x_1|,|x_2|\le T$ we can apply the well-known estimate

$$d(k)\ll k^{\epsilon}$$

for the divisor function and [Hooley 1986, Lemma 1], which follows from [Hooley 1967, Lemma 5], to conclude that the total number of solutions of $F(x)=z^2$ with $|x_1|,|x_2|,|x_3|,|x_0|\le T$ is $\ll T^{3+\epsilon}$.

Lower bound. The tool used to obtain the lower bound of (1-7) is an explicit parametrization of solutions given by an identity of Schottky. This identity has a form that is similar to many of those coming from syzygies connecting covariants and invariants of forms. However, Schottky's identity has a different origin and does not appear to come from invariant theory.

The Jacobian of S_0,S_1,S_2,S_3 as given in (1-4) and (1-5) is

$$J(x)=J_{S_0,S_1,S_2,S_3}(x)=\det\begin{pmatrix}\partial_1S_0 & \partial_2S_0 & \partial_3S_0 & \partial_4S_0\\ \partial_1S_1 & \partial_2S_1 & \partial_3S_1 & \partial_4S_1\\ \partial_1S_2 & \partial_2S_2 & \partial_3S_2 & \partial_4S_2\\ \partial_1S_3 & \partial_2S_3 & \partial_3S_3 & \partial_4S_3\end{pmatrix}=2gx_3^3x_0-2ax_3x_0^3+\cdots.$$

In case $f=-2$ and $g=0$ this is given in full by

$$\begin{aligned}J(x)=2(&-ax_3x_0^3+3ax_0^2x_1x_2-2ax_0x_1^3-bx_3x_0^2x_1+bx_0^2x_2^2+bx_0x_1^2x_2-bx_1^4\\&-cx_3x_0x_1^2+2cx_0x_1x_2^2-cx_1^3x_2-dx_3x_1^3+dx_0x_2^3+ex_3x_0x_2^2\\&-2ex_3x_1^2x_2+ex_1x_2^3-2x_3^2x_0x_2+2x_3^2x_1^2+2x_3x_1x_2^2-2x_2^4).\end{aligned}\tag{2-4}$$

The surface defined by $J(x)=0$ is a Weddle surface. A variant of the following identity connecting the Weddle and Kummer surfaces, which can be checked directly, is apparently due to Schottky [1889, page 241]. He obtained it via theta functions and used it to show that the Kummer and Weddle surfaces are birationally equivalent over $\mathbb{C}$. It is stated (in a somewhat different form) in [Baker 1907, page 152, Example 8].

Proposition 2. *For F in* (1-6) (*and in* (2-1)) *when $P(t)=at^6+bt^5+ct^4+dt^3+et^2-2t$, we have identically*

$$F(-S_3(x),-2S_2(x),2S_1(x),S_0(x))=J^2(x),\tag{2-5}$$

where $J(x)$ is given in (2-4).

Note the order of the parametrizing quadrics S_j. It is not obvious (to me) how to modify (2-5) so that it holds for a general $P(t)$ or even if that is possible without changing its basic form.

Proof of Theorem 1. Let $\mathcal{S}$ be the set of six points $\alpha_j\in\mathbb{P}^3_{\mathbb{C}}$ represented by $(t_j^3,t_j^2,t_j,1)$, where $P(t_j)=0$ for $j=1,\dots,6$. Recall from the discussion around (1-6) that $S_i(\alpha_j)=0$ for each i,j. In order to apply Proposition 2 to prove the lower bound of (1-7), we must first examine the map

$$\alpha\mapsto(-S_3(\alpha),-2S_2(\alpha),2S_1(\alpha),S_0(\alpha))\tag{2-6}$$

from $\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ to $\mathbb{P}^3_{\mathbb{C}}$. Let V be the space spanned by $\{S_0,S_1,S_2,S_3\}$, which is clearly four dimensional. We need to control the degree of the map (2-6). Suppose that $\beta_1,\beta_2,\beta_3\in\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ are distinct and all have the same image in $\mathbb{P}^3_{\mathbb{C}}$ under the map (2-6). Then three independent $S,S',S''\in V$ will vanish at the nine distinct points $\{\alpha_1,\dots,\alpha_6,\beta_1,\beta_2,\beta_3\}$. This is impossible by Bezout's theorem and shows that there are at most two points in $\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ with the same image in $\mathbb{P}^3_{\mathbb{C}}$ under the map (2-6).

Therefore by Proposition 2, the lower bound of (1-7) will follow from

$$\#\{x\in\mathbb{Z}^4:\gcd(x_1,x_2,x_3,x_4)=1,\ |S_j(x)|\le T,\ j=1,2,3,4\}\gg T^2.$$

This estimate is easily established since there is a ball in $\mathbb{R}^4$ centered at the origin of positive radius, all of whose points x satisfy $|S_j(x)|\le 1$ for $j=1,2,3,4$. Thus a standard lattice point count gives the result. □

References

[Baker 1907] H. F. Baker, *An introduction to the theory of multiply periodic functions*, Cambridge University Press, 1907. Zbl

[Bonolis 2021] D. Bonolis, “A polynomial sieve and sums of Deligne type”, *Int. Math. Res. Not.* **2021**:2 (2021), 1096–1137. MR Zbl

[Broberg 2003] N. Broberg, “Rational points on finite covers of $\mathbb{P}^1$ and $\mathbb{P}^2$”, *J. Number Theory* **101**:1 (2003), 195–207. MR Zbl

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996. Zbl

[Dolgachev 2012] I. V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, 2012. MR Zbl

[Duke 2021] W. Duke, “On elliptic curves and binary quartic forms”, *International Mathematics Research Notices* (2021).

[Heath-Brown and Pierce 2012] D. R. Heath-Brown and L. B. Pierce, “Counting rational points on smooth cyclic covers”, *J. Number Theory* **132**:8 (2012), 1741–1757. MR Zbl

[Hooley 1967] C. Hooley, “On binary cubic forms”, *J. Reine Angew. Math.* **226** (1967), 30–87. MR Zbl

[Hooley 1986] C. Hooley, “On binary quartic forms”, *J. Reine Angew. Math.* **366** (1986), 32–52. MR Zbl

[Hudson 1990] R. W. H. T. Hudson, *Kummer’s quartic surface*, Cambridge University Press, 1990. MR Zbl

[Munshi 2009] R. Munshi, “Density of rational points on cyclic covers of $\mathbb{P}^n$”, *J. Théor. Nombres Bordeaux* **21**:2 (2009), 335–341. MR Zbl

[Schottky 1889] F. Schottky, “Ueber die Beziehungen zwischen den sechzehn Thetafunctionen von zwei Variabeln”, *J. Reine Angew. Math.* **105** (1889), 233–249. MR Zbl

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects Math. **E15**, Vieweg & Sohn, Braunschweig, Germany, 1989. MR Zbl

Received 21 Sep 2021. Revised 9 Dec 2021.

WILLIAM DUKE:

wdduke@ucla.edu
Mathematics Department, UCLA, Los Angeles, CA, United States

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
https://msp.org/

ESSENTIAL NUMBER THEORY

2022 vol. 1 no. 1