Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Congruent number problems and their variants

JAAP TOP AND NORIKO YUI

ABSTRACT. The congruent number problem asks if a natural number n can be realized as the area of a right-angled triangle with rational sides. This problem is related to the existence of rational points on some elliptic curve defined over $\mathbb{Q}$. We present a survey on this problem and several variants, with special emphasis on modularity and other arithmetic questions.

CONTENTS

1. Introduction

This survey discusses some innocent-looking longstanding unsolved problems: the *congruent number problem*, and the *perfect rational cuboid problem*,

Mathematics Subject Classification: Primary 14J27, 14J28, 14J15; Secondary 11E25, 11G05, 11G40.

Keywords: Congruent numbers, elliptic curves, rational points, rational cuboids, K3 surfaces, Kummer surfaces, elliptic modular surfaces, theta series, modular (cusp) forms.

Yui was partially supported by a Research Grant from Natural Sciences and Engineering Research Council of Canada (NSERC), and by MSRI Berkeley, CRM Barcelona, MPIM Bonn and FIM ETH Zürich.

as applications of algorithmic number theory. These problems are indeed very old; the congruent number problem dates back to the time of the Greeks; and the perfect rational cuboid problem to the time of Euler or earlier. Accordingly, there are a large number of articles attempting to solve the problems with various different approaches, most of which use elementary number theoretic methods.

We take a geometric approach to the problems, by reformulating them as arithmetic questions (e.g., the existence of rational points) on certain curves and surfaces. We first consider the classical congruent number problem and a generalization to arbitrary rational triangles (not necessarily right-angled), and in particular the $2\pi/3$-congruent number problem. The main results here were obtained by Tunnell [1983], Long [2004, §7], and S.-i. Yoshida [2001; 2002]. All these problems are recapitulated as the problem of finding rational points on elliptic curves and/or on elliptic K3 surfaces defined over $\mathbb{Q}$. Next, the "semi-perfect" rational cuboid problem will be discussed. Some results here may be found in an unpublished paper of Beukers and van Geemen [1995], in Ronald van Luijk's master's thesis [van Luijk 2000], and in Narumiya and Shiga's report [2001] on [Beukers and van Geemen 1995]. Again the problems are recapitulated as the problem of finding rational lines and points on certain K3 surfaces (e.g., Kummer surfaces of product type) defined over $\mathbb{Q}$.

The expositions of the problems discussed here involve properties of elliptic K3 surfaces, and modular forms of integral and half-integral weight for some arithmetic subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. An extensive list of literature on these topics is included. We have tried to emphasize material which is not readily available elsewhere.

2. Precursors to the congruent number problem

The problem of finding all *Pythagorean triples*, i.e., all triples of integers (a, b, c) with $c \neq 0$ and $a^2 + b^2 = c^2$, is easily seen to be equivalent to the problem of finding all pairs (r, s) of rational numbers satisfying $r^2 + s^2 = 1$. There is a well known geometric construction for all such pairs: the equation $x^2 + y^2 = 1$ defines a circle of radius 1 and center $(0, 0)$ in the (x, y)-plane. The rational points (r, s) on it arise as intersection points with a line through $(-1, 0)$ having a rational (or infinite) slope. Explicitly, the equation of such a line with slope $t \neq \infty$ is $y = t(x + 1)$ and this yields as second point of intersection

$$(r, s) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

It follows that there exist infinitely many Pythagorean triples (a, b, c), even with the additional constraint $\gcd(a, b, c) = 1$.

REMARK 2.1. In contrast, the Diophantine equation $X^n + Y^n - Z^n = 0$ of degree $n \geq 3$ has no nontrivial solutions in integers (a, b, c). Here, by a nontrivial solution we mean a triple of integers (a, b, c) with $abc \neq 0$ satisfying the equation. This is the celebrated proof of Fermat's Last Theorem [Wiles 1995; Taylor and Wiles 1995]. More generally, one considers a generalized Fermat equation $X^p + Y^q - Z^r = 0$ where p, q, r are natural numbers, and asks for solutions $(a, b, c) \in \mathbb{Z}^3$ with $abc \neq 0$, $\gcd(a, b, c) = 1$. Darmon and Granville [1995] showed that when $1/p + 1/q + 1/r < 1$, then a generalized Fermat equation has only finitely many such solutions. The interested reader is referred to [Darmon 1997] and [Kraus 1999] for a survey on generalized Fermat equations. Some quite recent developments may be found in [Beukers 1998; Bruin 1999; 2000].

The result of Darmon and Granville is based on an ingenious application of a theorem of Faltings [1983] on the set of solutions of certain Diophantine equations:

THEOREM 2.2. *Let C be a smooth, geometrically irreducible, projective curve defined over $\mathbb{Q}$ of genus at least 2. Then the set $C(\mathbb{Q})$ of rational points is finite.*

A natural question arising from this theorem is, how to *find* all rational points on a curve of genus at least 2. Recently remarkable progress has been made on this problem, using a method of Coleman [1985] and Chabauty [1941]. Chabauty's theorem asserts that if C is a smooth projective curve of genus $g \geq 2$ defined over a number field K, and if the Jacobian of C has Mordell–Weil rank $< g$ over K, then $C(K)$ is finite. Coleman [1985] gave an effective bound on the cardinality of the set $C(K)$. For instance, for $K = \mathbb{Q}$, the proof of Coleman's Corollary 4.6 readily gives the bound (compare [Joshi and Tzermias 1999]) $\#C(\mathbb{Q}) \leq \#\tilde{C}(\mathbb{F}_p) + 2g - 2$ provided that p is a rational prime $> 2g$ such that C has good reduction $\tilde{C}$ at p (and of course, the Jacobian of C should have rank $< g$). An explicit example where this is used to prove that all solutions to a certain Diophantine equation have been found, is given by Grant [1994]. Nils Bruin discusses in his thesis [1988] techniques which allow one to apply Chabauty's method in situations where the rank is not smaller than the genus.

We will now focus on congruent number problems. This is done in the sections 3, 4 and 5 below where we discuss, respectively, the congruent number problem, a generalized congruent number problem, and the $2\pi/3$-congruent number problem.

3. The classical congruent number problem

DEFINITION 3.1. A square-free natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a right-angled triangle with rational length

sides. In other words, n is a congruent number if and only if there is a right-angled triangle with rational sides $X, Y, Z \in \mathbb{Q}$ such that

$$X^2 + Y^2 = Z^2, \quad XY = 2n.$$

EXAMPLES. $n = 5$ is a congruent number as there is a rational right-angled triangle with sides $3/2, 20/3$ and $41/6$. Similarly, 41 is a congruent number as there is a rational right-angled triangle with sides $123/20, 40/3$ and $881/60$. Zagier has shown that 157 is a congruent number, since there is a rational right-angled triangle with sides

$$X = \frac{157841 \cdot 4947203 \cdot 526771095761}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441},$$

$$Y = \frac{2^2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 526771095761},$$

$$Z = \frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907 4801}{2\ 3^2\ 5\ 13\ 17\ 37\ 101\ 17401\ 46997\ 356441\ 157841\ 4947203\ 526771095761}.$$

Determining whether a given square-free natural number is congruent is the *congruent number problem*. It has not yet been solved in general. A wonderful textbook on this subject was written by Koblitz [1993].

REMARK 3.2. The congruent number problem may be formulated equivalently in terms of "squares in arithmetic progressions": a natural number n is a congruent number if and only if the equation: $\gamma^2 - \beta^2 = \beta^2 - \alpha^2 = n$ is solvable in rational numbers α, β, γ. For instance, Fibonacci found a solution for $n = 5$ ($\alpha = 31/12, \beta = 41/12$ and $\gamma = 49/12$). The transition from this problem to the congruent number problem is easy: $\alpha = (Y - X)/2$, $\beta = Z/2$, $\gamma = (Y + X)/2$.

We recall the translation of the congruent number problem into arithmetic questions concerning elliptic curves. For the necessary background on elliptic curves, the reader is referred to the text by Bjorn Poonen [2008] in this volume. Let C_n denote the curve with equation $y^2 = x^3 - n^2 x$.

PROPOSITION 3.3. *Let n be a square-free natural number. The following statements are equivalent*:

(i) *n is a congruent number*;
(ii) *the elliptic curve C_n has a rational point (x, y) with $y \neq 0$*;
(iii) *the elliptic curve C_n has infinitely many rational points*;
(iv) *the Mordell–Weil group $C_n(\mathbb{Q})$ has rank ≥ 1.*

PROOF. (i) $\Rightarrow$ (ii): Suppose that n is a congruent number. Then there is a right-angled triangle with rational sides X, Y, Z and $XY = 2n$. Put $x := (Z/2)^2$ and

$y := Z(X-Y)(X+Y)/8$. This defines a point $(x, y) \in C_n(\mathbb{Q})$ with $y \neq 0$, as is readily verified.

(ii) $\Rightarrow$ (iii): To prove this, one needs to observe that the only nontrivial torsion points (x, y) in $C_n(\mathbb{Q})$ are the ones with $y = 0$. This follows, e.g., by using that for any prime p not dividing $2n$ reduction modulo p injects the torsion subgroup of $C_n(\mathbb{Q})$ into $\tilde{C}_n(\mathbb{F}_p)$ and the latter group has order $p+1$ for all such $p \equiv 3 \bmod 4$.

(iii) $\Rightarrow$ (iv): This follows immediately from the Mordell–Weil theorem.

(iv) $\Rightarrow$ (i): If the rank of $C_n(\mathbb{Q})$ is positive, then certainly a rational point (x, y) on C_n exists with $y \neq 0$. Put

$$X = \left|\frac{(x+n)(x-n)}{y}\right|, \quad Y = 2n\left|\frac{x}{y}\right|, \quad Z = \left|\frac{x^2+n^2}{y}\right|.$$

Then $X, Y, Z > 0$ and

$$X^2 + Y^2 = Z^2, \quad XY = 2n,$$

so n is a congruent number. □

REMARK 3.4. (1) There is no known algorithm guaranteed to compute the rank of $C_n(\mathbb{Q})$. Nevertheless, Nemenzo [1998] calculated all $n < 42553$ for which $C_n(\mathbb{Q})$ is infinite, hence all congruent numbers below this bound. Similarly, Elkies [1994; 2002] computed that for all natural numbers $n < 10^6$ which are $\equiv 5, 6$, or $7 \bmod 8$, the group $C_n(\mathbb{Q})$ has positive rank.

(2) The elliptic curve C_n has complex multiplication by the ring $\mathbb{Z}[\sqrt{-1}]$. This means that the endomorphism ring of C_n is isomorphic to $\mathbb{Z}[\sqrt{-1}]$. The j-invariant of C_n is $j = 12^3$ and the discriminant of C_n is $\Delta = (2n)^6$.

(3) The elliptic curve $C_n : y^2 = x^3 - n^2x$ is the quadratic twist of the elliptic curve $C_1 : y^2 = x^3 - x$ by $\sqrt{n}$. In fact, $(x, y) \mapsto (x/n, y/(n\sqrt{n}))$ yields an isomorphism over $\mathbb{Q}(\sqrt{n})$ from C_n to C_1.

(4) There are many quite old results on the rank of $C_n(\mathbb{Q})$ for special classes of integers n. For instance, Nagell [1929, pp. 16, 17] has a very short and elementary proof of the fact that this rank is zero in case $n = p$ is a prime number $\equiv 3 \bmod 8$. Hence such primes are noncongruent numbers. Nagell also points out that the same technique shows that $1, 2$ and all $n = 2q$ with q a prime $\equiv 5 \bmod 8$ are noncongruent.

(5) On the positive side, Heegner [1952] used the fact that C_1 is isogenous to $X_0(32)$ (which is also an elliptic curve) plus the theory of complex multiplication to construct a non-torsion point in $C_1(\mathbb{Q}\sqrt{-2p})$ for an arbitrary prime number $p \equiv 3 \bmod 4$. This implies that the rank of $C_{2p}(\mathbb{Q})$ is positive for such

primes, hence all $n = 2p$ with p prime $\equiv 3 \bmod 4$ are congruent. Heegner's method was later extended by P. Monsky [1984]. For example, he showed that primes $\equiv 5, 7 \bmod 8$ are congruent. Since primes $\equiv 3 \bmod 8$ are noncongruent by Nagell's result mentioned above, this only leaves the primes $\equiv 1 \bmod 8$. Here the situation is still unknown. For instance, 17 is known to be noncongruent and 41 is congruent.

To be able to say more about the rank r of the Mordell–Weil group of $C_n(\mathbb{Q})$, one invokes the conjecture of Birch and Swinnerton-Dyer. For this, one needs the L-series of $C_n/\mathbb{Q}$. Recall that n is assumed to be a square-free integer. This L-series is for $\mathrm{Re}(s) > 3/2$ defined by

$$L(C_n, s) = \prod_{p \nmid 2n} (1 - a_p p^{-s} + p^{-2s})^{-1}$$

where $a_p := p + 1 - \#\tilde{C}_n(\mathbb{F}_p)$. In fact, put

$$g(q) := \eta(q^4)^2 \eta(q^8)^2 = \sum_{n=1}^{\infty} b_n q^n,$$

with $\eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$ the Dedekind eta function. Then g is a cusp form of weight 2 for $\Gamma_0(32)$. Define

$$L(g, \chi, s) = \sum_{\substack{m=1, \\ \gcd(m,N)=1}}^{\infty} \chi(m) b_m m^{-s}$$

for $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ any primitive Dirichlet character modulo N. Then

$$L(C_n, s) = L(g, \chi_n, s),$$

in which χ_n is the nontrivial quadratic character corresponding to the extension $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$. It follows from this, that $L(C_n, s)$ extends to an analytic function on all of $\mathbb{C}$.

REMARK 3.5. The modularity theorem of Wiles [1995], Taylor and Wiles [1995], and Breuil, Conrad, Diamond and Taylor [Breuil et al. 2001] shows that analogous statements hold for an arbitrary elliptic curve $E/\mathbb{Q}$: the L-series $L(E, s)$ (defined analogously to that of C_n, see [Silverman 1986, Appendix C, § 16]) equals $L(h, s)$ for some cusp form h of weight 2 for a group $\Gamma_0(N)$. In particular, this implies that $L(E, s)$ has an analytic continuation to the entire complex plane. The conjecture of Birch and Swinnerton-Dyer for elliptic curves over $\mathbb{Q}$ (which was already formulated a long time before this analytic continuation was known to exist) predicts how $L(E, s)$ behaves near $s = 1$.

CONJECTURE [Birch and Swinnerton-Dyer 1965]. *The expansion of* $L(E,s)$ *at* $s=1$ *has the form* $L(E,s)=c(s-1)^r+$ *higher order terms, with* $c\neq 0$ *and* r *the rank of* $E(\mathbb{Q})$. *In particular,* $L(E,1)\neq 0$ *if and only if the Mordell–Weil group* $E(\mathbb{Q})$ *is finite*.

This is in fact a *weak* form of the Birch and Swinnerton-Dyer conjecture, and we will call it the BSD Conjecture. From results in [Breuil et al. 2001; Bump et al. 1990; Coates and Wiles 1977; Gross and Zagier 1986; Kan 2000; Kolyvagin 1988; Murty and Murty 1991; Taylor and Wiles 1995; Wiles 1995], the BSD Conjecture is known to be true if $L(E,s)$ vanishes to order ≤ 1 at $s=1$. However, the general case is still wide open, and this is in fact one of the seven Millennium Prize Problems announced by the Clay Mathematics Institute with \$1 million prizes. A more thorough treatment on modular forms can be found in the article of Stein [2008] in this volume. As a first application to congruent numbers, one can observe (using the sign in the functional equation which relates $L(C_n,s)$ to $L(C_n,2-s)$; see [Koblitz 1993, p. 84]) that for square-free $n>0$ the order of vanishing of $L(C_n,s)$ at $s=1$ is *odd* precisely when $n\equiv 5,6,7 \bmod 8$. Hence for these n we certainly have that $L(C_n,1)=0$, which by the BSD conjecture should imply that all such n are congruent numbers. At present, no proof of this is known, however.

Here is a characterization of congruent numbers due to Tunnell [1983], assuming the validity of the BSD conjecture. We denote by $\mathfrak{S}_k(N)$ the space of cusp forms of weight k with respect to the congruence subgroup $\Gamma_0(N)$. Moreover define

$$f(q):=\sum_{n=1}^{\infty}a_f(n)q^n=q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})\sum_{n\in\mathbb{Z}}q^{2n^2}$$

and

$$f'(q):=\sum_{n=1}^{\infty}a_{f'}(n)q^n=q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})\sum_{n\in\mathbb{Z}}q^{4n^2}.$$

These are in fact elements of $\mathfrak{S}_{3/2}(128)$ and $\mathfrak{S}_{3/2}(128,\chi_2)$, respectively (compare [Koblitz 1993, Ch. IV] for precise definitions). We owe the formulation used in (v) below to Noam Elkies.

THEOREM 3.6. *Let* n *be a square-free natural number. Assuming the validity of the BSD Conjecture for* C_n, *the following statements are equivalent*:

(i) n *is a congruent number*;
(ii) $C_n(\mathbb{Q})$ *is infinite*;
(iii) $L(C_n,1)=0$;
(iv) *For* n *odd,* $a_f(n)=0$ *and for* n *even,* $a_{f'}(n/2)=0$;

(v) *If n is odd, then there are as many integer solutions to $2x^2+y^2+8z^2=n$ with z even as there are with z odd.*

If n is even, the analogous statement holds for $x^2+y^2+8z^2=n/2$.

PROOF. (i) $\Longleftrightarrow$ (ii): This is proved in Proposition 3.3.

(ii) $\Longleftrightarrow$ (iii): This is the BSD Conjecture for C_n. As remarked earlier, the implication (ii) $\Rightarrow$ (iii) is in fact known without assuming any conjectures [Coates and Wiles 1977].

(iii) $\Longleftrightarrow$ (iv): This was proved in [Tunnell 1983], based on results by Shimura [1973] and Waldspurger [1981]. Recall that $L(C_n, s)$ equals $L(g, \chi_n, s)$ where g is a cusp form of weight 2 for $\Gamma_0(32)$. Tunnell shows that the modular forms f and f' of weight $3/2$ for $\Gamma_0(128)$ are both related under a correspondence described by Shimura to the modular form g. A formula due to Waldspurger [1981] allows him to conclude that $L(C_n, 1)$ vanishes precisely when $a_f(n)$ (resp. $a_{f'}(n/2)$) vanishes. For further details, see [Tunnell 1983] and [Koblitz 1993, IV, §4].

(iv) $\Longleftrightarrow$ (v): This follows by expressing f and f' in terms of theta functions (compare [Tunnell 1983]):

$$f(q) = \sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+8z^2}$$

and

$$f'(q) = \sum_{x,y,z\in\mathbb{Z}} q^{4x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} q^{4x^2+y^2+8z^2}.$$

The translation from the ternary forms used here to the criterion given in (v) is an amusing elementary exercise. □

EXAMPLE. (1) Tunnell showed that for p prime $\equiv 3 \bmod 8$, the Fourier coefficient $a_f(p)$ is $\equiv 2 \pmod 4$, hence it is nonzero. This implies, using the full force of Theorem 3.6 (no BSD conjecture is needed here) that such primes are noncongruent, providing a new proof of Nagell's half a century older result.

(2) Since it is relatively easy to calculate the number of representations of a not too large n by the ternary forms mentioned in Theorem 3.6, assuming BSD one can decide whether n is congruent at least for all $n < 10^9$.

REMARK 3.7. In general, one may find forms of weight $3/2$ such as the ones in Theorem 3.6 (iv) as follows. Starting from an arbitrary eigenform of weight 2, check whether it is in the image of the Shimura map using a criterion due to Flicker [1980]. Then finding a form of weight $3/2$ that maps to the given weight 2 form is in principle reduced to a finite amount of computation. This is because the spaces of modular (cusp) forms of fixed weight and level are finite-dimensional. (For instance, the space $\mathfrak{S}_{3/2}(128)$ has dimension 3, and testing

if an element in that space maps to the weight 2 form g of level 32 under the Shimura map or not can be done in finitely many steps.) There are algorithms available for this problem: see Basmaji's thesis [1996]. Recently, William Stein implemented Basmaji's algorithm.

4. A generalized congruent number problem

In this section, we will consider a generalized congruent number problem which asks if a natural number n can occur as the area of any rational triangle with some given angle θ. The exposition is partly based on the article by Ling Long [2004, § 7]. Classically, a triangle with rational sides and rational area is called a *Heron triangle*. Heron of Alexandria proved almost 2000 years ago that the area n of a triangle with sides a, b and c satisfy $n^2 = s(s-a)(s-b)(s-c)$, where $s = (a+b+c)/2$. Moreover, he provided the example $a = 13, b = 14, c = 15$ which shows that 84 is the area of a Heron triangle. The subject was much studied in the first half of the 17th century, with contributions by famous mathematicians such as François Viète, C.G. Bachet and Frans van Schooten, jr. Basically, they constructed examples of Heron triangles by gluing right-angled triangles along a common side. In the 19th century, many problems concerning Heron triangles were discussed in the British journal *Ladies' Diary*. Dickson [1934, pp. 191–201] mentions numerous results on Heron triangles. A natural number n occurs as the area of a Heron triangle if and only if positive rational numbers a, b, c and a real number θ with $0 < \theta < \pi$ exist such that

$$a^2 = b^2 + c^2 - 2\,b\,c\cos\theta \quad \text{and} \quad 2\,n = b\,c\sin\theta.$$

The equations imply that $(\cos\theta, \sin\theta)$ must be a rational point $\neq (\pm 1, 0)$ on the upper half of the unit circle, hence a rational number $t > 0$ exists such that

$$\sin\theta = \frac{2t}{1+t^2} \quad \text{and} \quad \cos\theta = \frac{t^2-1}{t^2+1}.$$

Now fix a rational number $t > 0$.

DEFINITION 4.1. An integer n is called t-congruent if positive rational numbers a, b, c exist such that

$$a^2 = b^2 + c^2 - 2\,b\,c\,\frac{t^2-1}{t^2+1} \quad \text{and} \quad 2\,n = b\,c\,\frac{2t}{1+t^2}.$$

The case $t = 1$ corresponds to the classical congruent number problem. The t-congruent number problem, which asks whether a given integer is t-congruent, can be reformulated as an arithmetic question of certain elliptic curves. Basically this was done using elementary methods by D. N. Lehmer [1899/1900] a century

ago. Recently Ling Long constructed a family of elliptic curves corresponding to t-congruent numbers.

PROPOSITION 4.2. *Let t be a positive rational number and $n \in \mathbb{N}$. The following statements are equivalent*:

(i) *n is a t-congruent number.*
(ii) *Either both n/t and t^2+1 are nonzero rational squares, or the elliptic curve $C_{n,t} : y^2 = x(x-n/t)(x+nt)$ has a rational point (x, y) with $y \neq 0$.*

PROOF. (i) $\Rightarrow$ (ii): Suppose that n is a t-congruent number. Then there exist positive rational numbers a, b, c satisfying the two equations given in Definition 4.1. The second of these equations can be written as $n/t = bc/(1+t^2)$. Using this, it easily follows that $(x, y) := (a^2/4, (ab^2 - ac^2)/8)$ is a point in $C_{n,t}(\mathbb{Q})$. It satisfies $y \neq 0$, unless we have $b = c$. In the latter case one verifies that $t^2 + 1 = (2b/a)^2$ and $n/t = (a/2)^2$.

(ii) $\Rightarrow$ (i): Suppose first that n/t and $t^2 + 1$ are nonzero rational squares. Then $a = 2\sqrt{n/t}$ and $b = c = \sqrt{n(t^2+1)/t}$ show that n is t-congruent. For the other case, if $P = (x, y) \in C_{n,t}(\mathbb{Q})$ with $y \neq 0$ is a rational point on $C_{n,t}$, then

$$a = \left|\frac{x^2+n^2}{y}\right|, \quad b = \left|\frac{(x+nt)(x-n/t)}{y}\right|, \quad c = n\left|\frac{x(1/t+t)}{y}\right|$$

show that n is t-congruent. □

EXAMPLE. Consider $n = 12$, $t = 4/3$. The torsion subgroup of $C_{12,4/3}(\mathbb{Q})$ is given by $C_{12,4/3}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Two generators are $(0, 0)$ and $(-6, 30)$. The latter point is not a 2-torsion point, and corresponds to a rational triangle with sides $5, 5, 6$ with area 12. Note that, contrary to the situation for classical congruent numbers, here a torsion point in $C_{n,t}(\mathbb{Q})$ leads to n being t-congruent.

Several people have given proofs of the fact that any natural number n occurs as the area of some Heron triangle. A quite elementary proof was obtained by Fine [1976], who in his paper also mentions an even simpler proof by S. and P. Chowla. Also H. Cohen showed a proof of this to Ling Long and Noriko Yui in the summer of 2000. All proofs are in the spirit of F. van Schooten's 17th century work on Heron triangles: consider two positive rational numbers r, s, both $\neq 1$. Gluing the two Pythagorian triangles with sides $(2, |r-r^{-1}|, r+r^{-1})$ and $(2, |s-s^{-1}|, s+s^{-1})$ along their common side with length 2 yields a Heron triangle with area $|r - r^{-1}| + |s - s^{-1}|$. It remains to find suitable r, s. After first multiplying n by a square (which amounts to scaling a triangle), we may assume $n > 6$. Then $r = 2n/(n-2), s = (n-2)/4$ give area $(n+2)^2/(4n)$.

Scaling the corresponding triangle by a factor $2n/(n+2)$ results in one with area n. We have proved:

THEOREM 4.3. *Any square-free natural number n can be realized as a t-congruent number for some $t \in \mathbb{Q}_{>0}$.* □

In terms of Proposition 4.2 (considering n as a variable, using r, s as above, and setting $a = 2n(r + r^{-1})/(n+2)$ and $b = 2n(s + s^{-1})/(n+2)$ and $c = 2n(r - r^{-1} + s - s^{-1})/(n+2)$), this can be interpreted as the fact that the curve $C_{n,(n-2)/4}$, given by $y^2 = x(x - 4n/(n-2))(x + n(n-2)/4)$ contains a $\mathbb{Q}(n)$-rational point (x, y) with $y \neq 0$. In fact, $((-n+2)/2, (n^2-4)/4)$ is such a point. It has infinite order in the group $C_{n,(n-2)/4}(\mathbb{Q}(n))$, as follows from the fact that it specializes for $n = 0$ to $(1, -1)$ on the curve given by $y^2 = x^3$. The latter point has infinite order, as follows from [Silverman 1986, III Prop. 2.5].

Long considered $C_{n,t} : y^2 = x(x - n/t)(x + n\,t)$ as a surface over the t-line. Note that geometrically, this defines the same surface for every nonzero n: the map $(x, y) \mapsto (x/n, y/(n\sqrt{n}))$ defines an isomorphism from $C_{n,t}$ to $C_{1,t}$. For this reason we will only consider $n = 1$. A general introduction to elliptic surfaces as considered here, may be found in [Shioda 1990].

PROPOSITION 4.4. *Let $C_{1,t} : y^2 = x(x - 1/t)(x + t)$ and let $\Phi_1 : \mathscr{E}_1 \to \mathbb{P}^1_t$ be the smooth minimal model coresponding to $C_{1,t} \to \mathbb{P}^1_t : (x, y, t) \mapsto t$.*

(a) *$\mathscr{E}_1$ is a singular elliptic K3 surface, and Φ_1 has exactly four singular fibres, which are of Kodaira type I_2, I_2, I_4^*, I_4^*, respectively.*
(b) *The Mordell–Weil group of $C_{1,t}$ over $\mathbb{C}(t)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*
(c) *In the Shioda–Inose classification of singular K3 surfaces, $\mathscr{E}_1$ corresponds to the even positive definite binary quadratic form $2x^2 + 2y^2$.*
(d) *The L-series of $\mathscr{E}_1$ is given by*

$$L(\mathscr{E}_1, s) = \zeta(s-1)^{18} L(\chi_4, s-1)^2 L(f, s)$$

where $f \in \mathfrak{S}_3(\Gamma_0(1024), (2/p))$ is the twist of $\eta(q^4)^6 = q\prod_{n=1}^{\infty}(1-q^{4n})^6$ by the quadratic character $(\frac{2}{p})$ and χ_4 is the nontrivial Dirichlet character modulo 4.

PROOF. Since most of the notions used in the statement have not been defined here, we only sketch the proof and meanwhile, explain these notions a bit more.

(a,b) The elliptic surface $C_{1,t}$ is birationally equivalent to the elliptic surface $y^2 = x(x - t)(x + t^3)$ by the birational map $(x, y) \mapsto (x/t^2, y/t^3)$. Using Tate's algorithm [Birch and Kuyk 1975], one can read off the singular fibres of Φ_1 from the latter equation. They occur at $t = \pm\sqrt{-1}, 0, \infty$ and are of type I_2, I_2, I_4^* and I_4^*, respectively. From this, one concludes that $\mathscr{E}_1$ has Euler characteristic 24 and hence is an elliptic K3 surface.

The Shioda–Tate formula (see [Shioda 1990]) asserts that the rank of the Néron–Severi group (which is by definition the group of 1-cycles modulo algebraic equivalence) of $\mathscr{E}_1$ equals $2+\sum_{v\in\Sigma}(m_v-1)+r$ where Σ is the finite set of points $v\in\mathbb{P}^1_t$ such that the fiber of Φ_1 over v is a reducible curve; m_v denotes its number of irreducible components. Moreover, r denotes the rank of the group of sections of Φ_1 (which equals the rank of $C_{1,t}(\mathbb{C}(t))$).

For an elliptic K3 surface in characteristic 0, the rank of the Néron–Severi group is at most 20. By definition, a singular K3 surface is one for which this rank is maximal. In the present case we have

$$2+\sum_{v\in\Sigma}(m_v-1)+r=2+(2-1)+(2-1)+(9-1)+(9-1)+r=20+r\le 20$$

hence $r=0$ and $\mathscr{E}_1$ is a singular K3 surface.

The torsion subgroup of $C_{1,t}(\mathbb{C}(t))$ certainly contains a group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. Moreover, the torsion subgroup injects in the torsion subgroup of any fibre of Φ_1. Since $\mathscr{E}_1$ contains a fiber of type I_4^*, whose torsion subgroup we read off from the tables in [Birch and Kuyk 1975] to be isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, we conclude that the Mordell–Weil group is isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

(c) Shioda and Inose [1977] (see also [Inose 1978] for a very explicit description) have shown that there is a one-to-one correspondence between singular K3 surfaces and $SL_2(\mathbb{Z})$-equivalence classes of positive definite even integral binary quadratic forms. Moreover, under this correspondence the discriminant of a quadratic form (by which we mean the determinant of the associated symmetric matrix) coincides up to sign with the determinant of the corresponding Néron–Severi lattice. In case $r=0$, this determinant equals the product over the singular fibres of the number of irreducible components with multiplicity one, divided by the square of the order of the torsion subgroup of the Mordell–Weil group. In our case, this yields $2\cdot2\cdot4\cdot4/16=4$. The unique equivalence class of forms with this discriminant is that of $2x^2+2y^2$.

(d) One way to interpret this assertion is that for every odd prime p, the number $\#\tilde{\mathscr{E}}_1(\mathbb{F}_p)$ of points equals $p^2+1+18p+\chi_4(p)+(\frac{2}{p})a_p$ where a_p is the coefficient of q^p in $\eta(q^4)^6$. The factor $\zeta(s-1)^{18}L(\chi_4,s-1)^2$ in the assertion refers to the fact that the Néron–Severi group has rank 20 and is generated by 18 rational 1-cycles and two conjugate ones over $\mathbb{Q}(i)$. The fact that the remaining factor (in case of a singular K3 surface) is the L-series of some modular form of weight 3 follows from a general result of Livné [1995]. Arguing as in [Stienstra and Beukers 1985] (or alternatively, as in [Livné 1987] and [Peters et al. 1992, §4]), one can verify that this modular form is as given in the proposition. □

The (unique) singular K3 surface corresponding to the form $2x^2+2y^2$ has been studied by many authors, including Vinberg [1983] and Inose [1976].

Next, we consider the family of elliptic curves

$$C_{t,(t-2)/4} : y^2 = x(x-4t/(t-2))(x+t(t-2)/4),$$

which appeared in the proof of Theorem 4.3.

PROPOSITION 4.5. *$C_{t,(t-2)/4}$ defines a (smooth, relatively minimal) elliptic surface $\Phi_2 : \mathscr{E}_2 \to \mathbb{P}^1_t$.*

(a) *$\mathscr{E}_2$ is a singular elliptic K3 surface, and Φ_2 has exactly five singular fibres, which are of Kodaira type $I_2, I_2, I_4, I_0^*, I_4^*$, respectively.*
(b) *The Mordell–Weil group of $C_{t,(t-2)/4}$ over $\mathbb{C}(t)$ is isomorphic to*

$$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

(c) *The L-series of $\mathscr{E}_2$ is given by $L(\mathscr{E}_2, s) = \zeta(s-1)^{18} L(\chi_4, s-1)^2 L(f, s)$, where $f \in \mathfrak{S}_3(\Gamma_0(20), (-5/p))$.*

PROOF. This is quite analogous to the proof of Proposition 4.4. Tate's algorithm shows that there are two I_2-fibres at the roots of $t^2-4t+20=0$, an I_4-fibre at $t=\infty$, an I_0^*-fibre at $t=0$ and an I_4^*-fibre at $t=2$. It follows that $\mathscr{E}_2$ is a K3 surface.

We already saw that $C_{t,\frac{t-2}{4}}(\mathbb{Q}(t))$ contains a point of infinite order. So the Mordell–Weil rank r is ≥ 1. The Shioda–Tate formula in this case yields

$$19+1 \leq 19+r \leq 20,$$

hence $r=1$ and the surface is a singular K3. For the torsion part of the Mordell–Weil group of $\mathscr{E}_2$, apply the same argument as in Proposition 4.4. Hence the Mordell–Weil group of $\mathscr{E}_2$ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The determinant of the Néron–Severi lattice in this case equals the product over all bad fibers of the number of components with multiplicity one, multiplied by the height of a generator of the Mordell–Weil group modulo torsion, and divided by the square of the order of the torsion subgroup of the Mordell–Weil group. This yields $16h(P)$ where h is the height and P a generator. For a given point, this height can be calculated using an algorithm of Shioda [1990, Thm. 8.6]; in the present case it yields the answer $5/4$ which both implies that the point we have is indeed a generator, and that the determinant is 20. Note that there exist precisely two inequivalent forms here: $2x^2+10y^2$ and $4x^2+4xy+6y^2$. Which of these corresponds to $\mathscr{E}_2$ can possibly be settled by determining a finite morphism to some Kummer surface.

The statement concerning the L-series can be proven analogously to the previous case. Here we find

$$f(q) = q+2q^2-4q^3-4q^4-5q^5-8q^6+4q^7-24q^8-11q^9-10q^{10}+16q^{12} \\ +8q^{14}+20q^{15}-16q^{16}-22q^{18}+20q^{20}-16q^{21}-44q^{23}+96q^{24}-100q^{25} \\ +152q^{27}-16q^{28}-22q^{29}+40q^{30}+160q^{32}-20q^{35}+O(q^{36}).$$

The form $f(q)$ cannot be written as a product of η-functions, as follows from [Dummit et al. 1985] where a complete list of weight 3 newforms that can be written in such form is given. □

5. The $2\pi/3$-congruent number problem

Fujiwara [1998] and Kan [2000] considered a variant of the congruent number problem, called the *θ-congruent number problem*. Suppose that there is a triangle with rational sides containing an angle θ. Then $\cos\theta$ is a rational number, so write $\cos\theta = s/r$ with $r, s \in \mathbb{Z}$, $|s| \le r$, $\gcd(r,s) = 1$. Note that $\sin\theta = \frac{1}{r}\sqrt{r^2-s^2}$, hence the following makes sense.

DEFINITION 5.1. Suppose θ is a real number with $0 < \theta < \pi$, such that $\cos\theta = s/r$ with $r, s \in \mathbb{Z}$, $|s| \le r$, $\gcd(r,s) = 1$. A natural number n is called *θ-congruent* if $n\sqrt{r^2-s^2}$ occurs as the area of a triangle with rational sides and an angle θ.

In terms of the cosine rule and a formula for the area of a triangle, using the same notations, n is θ-congruent precisely when positive rational numbers a, b, c exist such that $c^2 = a^2+b^2-2abs/r$ and $2nr = ab$. The θ-congruent number problem is the problem of describing all θ-congruent integers n. Our exposition is based on [Yoshida 2001; 2002; Fujiwara 1998; Kan 2000].

REMARK 5.2. The classical congruent number problem is a special case of the t-congruent number problem, obtained by taking $t = 1$. The t-congruent number problem is a special case of the θ-congruent number problem in the following sense. Write $t = k/\ell$ for integers $\ell \ge k \ge 1$ with $\gcd(k,\ell) = 1$. Take the unique real number θ such that $\cos\theta = (t^2-1)/(t^2+1)$, $0 < \theta < \pi$. Then $\cos\theta$ is written in lowest terms as $(\ell^2-k^2)/(\ell^2+k^2)$ in case one of k, ℓ is even, respectively $\big((\ell^2-k^2)/2\big) / \big((\ell^2+k^2)/2\big)$ in case both k, ℓ are odd. So it follows that an integer n is θ-congruent precisely when $k\ell n$ is t-congruent (in case both k, ℓ are odd), respectively $2k\ell n$ is θ-congruent (in case one of k, ℓ is even). In particular, the classical congruent number problem also equals the $\pi/2$-congruent number problem.

PROPOSITION 5.3. *Let $n > 0$ be an integer. The following statements are equivalent.*

(i) *n is a $2\pi/3$-congruent number*;
(ii) *the elliptic curve $C_n : y^2 = x^3 - 2nx^2 - 3n^2x = x(x+n)(x-3n)$ contains a point (x, y) with $y \neq 0$*;
(iii) *the Mordell–Weil group $C_n(\mathbb{Q})$ has rank ≥ 1.*

PROOF. (i) $\Longleftrightarrow$ (ii): Suppose that n is a $2\pi/3$-congruent number. Then there exist positive rational numbers a, b, c such that $c^2 = a^2 + b^2 + ab$ and $ab = 4n$. Substituting $b = 4n/a$ in the first equality and multiplying by a^2 yields $(ca)^2 = a^4 + 4na^2 + 16n^2$. Now put $x = (ca + a^2 + 2n)/2$ and $y = a(ca + a^2 + 2n)/2$. Then (x, y) is a rational point on C_n with $y \neq 0$.

Conversely, if (x, y) is a rational point with $y \neq 0$ on C_n, then after possibly changing the sign of y we have that

$$a = \frac{(x+n)(x-3n)}{y} = \frac{y}{x} > 0 \quad \text{and} \quad b = 4n\frac{x}{y} > 0 \quad \text{and} \quad c = \frac{x^2 + 3n^2}{|y|}$$

show that n is a $2\pi/3$-congruent number.

(ii) $\Longleftrightarrow$ (iii): Since all 2-torsion on C_n is rational, the torsion subgroup $C_n(\mathbb{Q})_{\text{tors}}$ is isomorphic to a group of the form $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2M\mathbb{Z})$ for some $M \in \{1, 2, 3, 4\}$ by a theorem of Mazur [1978]. Hence if the torsion subgroup of $C_n(\mathbb{Q})$ is unequal to the 2-torsion subgroup, then a rational torsion point of order 3 or 4 exists. The 3-division polynomial of C_n is $n^4(3(\frac{x}{n})^4 - 8(\frac{x}{n})^3 - 18(\frac{x}{n})^2 - 9)$, which is irreducible over $\mathbb{Q}$. The 4-division polynomial is $4y(x-n)(x+3n)(x^2+3n^2)(x^2-6nx-3n^2)$. All its rational zeroes correspond to points of order 2. Therefore the Mordell–Weil group $C_n(\mathbb{Q})$ has rank ≥ 1 if and only if $C_n(\mathbb{Q})$ has a rational point (x, y) with $y \neq 0$. □

Similarly, all of the $\pi/3$-congruent numbers can be characterized. The proof is left to the interested reader as an exercise.

PROPOSITION 5.4. *Let $n > 0$ be an integer. Then the following statements are equivalent.*

(i) *n is a $\pi/3$-congruent number*;
(ii) *the elliptic curve $C_{-n} : y^2 = x(x-n)(x+3n)$ has a rational point (x, y) with $y \neq 0$*;
(iii) *the Mordell–Weil group $C_{-n}(\mathbb{Q})$ has rank ≥ 1.*

REMARK 5.5. (1) The j-invariant of the elliptic curves C_n and C_{-n} is $\frac{2^4 13^3}{3^2} \notin \mathbb{Z}$. This implies that they have no complex multiplication. In this respect, these variants are different from the classical congruent number problem; compare Remark 3.4(2).

(2) The elliptic curves C_n and C_{-n} are quadratic twists of C_1.

The weak form of the conjecture of Birch and Swinnerton-Dyer for the elliptic curves C_n and C_{-n} plus modularity of C_1 allow one to obtain results analogous to the result of Tunnell [1983] for the $\pi/2$-congruent number problem. There is a modular form of weight $3/2$ on some congruence subgroup of $\mathrm{PSL}(2,\mathbb{Z})$ such that the vanishing of the n-th coefficient in its Fourier expansion gives a criterion for $2\pi/3$-congruent numbers. A prototypical result is given in the following theorem.

THEOREM 5.6. *Let n be a positive square-free integer such that $n \equiv 1, 7$ or $13 \pmod{24}$. Assume the validity of the conjecture of Birch and Swinnerton-Dyer for $C_n : y^2 = x(x+n)(x-3n)$. The following statements are equivalent.*

(i) *n is a $2\pi/3$-congruent number*;
(ii) *$C_n(\mathbb{Q})$ has infinitely many rational points*;
(iii) *$L(C_n, 1) = 0$*;
(iv) *$a_f(n) = 0$, where $a_f(n)$ is the n-th Fourier coefficient of the modular form f of weight $3/2$ for $\Gamma_0(576)$ defined by*

$$f(q) = \sum_{n=1}^{\infty} b(n)q^n = \sum_{x,y,z\in\mathbb{Z}} q^{Q_1(x,y,z)} - \sum_{x,y,z\in\mathbb{Z}} q^{Q_2(x,y,z)} - G_2,$$

where

$$Q_1(x,y,z) = x^2 + 3y^2 + 144z^2, \quad Q_2(x,y,z) = 3x^2 + 9y^2 + 16z^2$$

and

$$G_2 = \frac{1}{2}\sum_{n\in\mathbb{Z}} \chi_{-3}(n) n\, q^{n^2} + 4\sum_{n\in\mathbb{Z}} \chi_{-3}(n) n\, q^{4n^2} + 8\sum_{n\in\mathbb{Z}} \chi_{-3}(n) n\, q^{16n^2}.$$

Here χ_{-3} is the nontrivial Dirichlet character modulo 3.

PROOF. This is due to Yoshida [2002]. Note in particular that the BSD conjecture is only used in (iii) $\Rightarrow$ (ii).

Also, note that for square-free $n > 1$, the form G_2 does not contribute to $a_f(n)$. Hence, assuming BSD, the theorem claims that n is $2\pi/3$-congruent if and only if the number of representations of n by $x^2 + 3y^2 + 144z^2$ equals the number of representations by $3x^2 + 9y^2 + 16z^2$. □

Considering the sign in the functional equation for $L(C_{\pm n}, s)$, the BSD conjecture predicts the following.

PROPOSITION 5.7 [Yoshida 2001]. *Let n be a square-free natural number. Assume the BSD conjecture for C_n and C_{-n}.*

(*a*) *If $n \equiv 5, 9, 10, 15, 17, 19, 21, 22, 23 \pmod{24}$, then n is $2\pi/3$-congruent.*
(*b*) *If $-n \equiv 3, 6, 11, 17, 18, 21, 22, 23 \pmod{24}$, then n is $\pi/3$-congruent.*

As for the classical congruent number problem, so-called Heegner point constructions (compare [Kan 2000]) can be used to show that certain types of numbers are indeed $2\pi/3$-congruent (or $\pi/3$-congruent).

THEOREM 5.8. *If p be a prime such that $p \equiv -1 \pmod{24}$, then $p, 2p$ and $3p$ are $2\pi/3$-congruent and $p, 2p$ and $6p$ are $\pi/3$-congruent.*

REMARK 5.9. Some negative results may be obtained by showing directly that the rank of $C_{\pm 1}(\mathbb{Q})$ is zero for certain sets of numbers n, or alternatively, by checking that $L(C_n, 1)$ or $L(C_{-n}, 1)$ is nonzero.

(a) Let p be a prime such that $p \equiv 7, 13 \pmod{24}$. Then a direct computation in the spirit of [Silverman 1986, X, Prop. 6.2] reveals that p is not $2\pi/3$-congruent. Alternatively, the p-th Fourier coefficient $a_p(f)$ of the appropriate modular form f is given by

$$\#\{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 3y^2 + 144z^2 = p\} \\ -\#\{(x, y, z) \in \mathbb{Z}^3 \mid 3x^2 + 9y^2 + 16z^2 = p\},$$

which is congruent to $4 \pmod 8$. Hence $a_p(f) \neq 0$, and consequently p is not a $2\pi/3$-congruent number.

(b) A similar argument shows that a prime $p \equiv 5, 7, 19 \pmod{24}$ is not $\pi/3$-congruent. (See [Goto 2001; 2002; Kan 2000; Yoshida 2001; 2002] for more general n like $2p$, $3p$, $6p$ or pq, $2pq$, etc.)

6. The rational cuboid problems

DEFINITION 6.1. We say that a cuboid $\mathcal{H}$ is a *perfect* rational cuboid if the sides and the three face diagonals and the body diagonal are all integers.

The existence of a perfect rational cuboid is easily seen to be equivalent to the existence of a rational point with nonzero coordinates on the surface $\mathcal{S}_{\mathcal{H}}$ in $\mathbb{P}^6$ defined by

$$X^2 + Y^2 = P^2,\ Y^2 + Z^2 = Q^2,\ Z^2 + X^2 = R^2,\ X^2 + Y^2 + Z^2 = W^2.$$

REMARK 6.2. The problem of whether a perfect rational cuboid $\mathcal{H}$ exists was known to Euler and is still unsolved. It is shown by Korec [1984] that no perfect rational cuboid $\mathcal{H}$ exists with shortest side $\leq 10^6$. In December 2004, B. Butler improved the search up to smallest side $\leq 2.1 \cdot 10^{10}$, not finding any examples. Ronald van Luijk [van Luijk 2000] showed that the surface $\mathcal{S}_{\mathcal{H}}$ *is of general type.*

If one relaxes the rationality requirement for one of the seven coordinates, then the resulting problem of finding *semi-perfect* rational cuboids turns out to be more tractable. We will take this direction in this survey. From a geometric

point of view, this means passing from the surface $\mathcal{S}_{\mathcal{H}}$ to a quotient by some automorphism. We first formulate the problems that we will consider.

PROBLEM 1. Find semi-perfect rational cuboids $\mathcal{H}$ with rational face diagonals P, Q and a rational body diagonal W (dropping the integrality condition for R). In other words, find rational points with nonzero coordinates on the surface in $\mathbb{P}^5$ defined by

$$X^2 + Y^2 = P^2, \quad Y^2 + Z^2 = Q^2, \quad X^2 + Y^2 + Z^2 = W^2.$$

EXAMPLE. $(X, Y, Z, P, Q, W) = (104, 153, 672, 185, 680, 697)$ is a solution to Problem 1. In Section 7 below we show that infinitely many solutions exist.

PROBLEM 2. Find semi-perfect rational cuboids $\mathcal{H}$ with rational face diagonals P, Q, R (relaxing the integrality condition for W). In other words, find rational points with nonzero coordinates on the surface in $\mathbb{P}^5$ defined by

$$X^2 + Y^2 = P^2, \quad Y^2 + Z^2 = Q^2, \quad Z^2 + X^2 = R^2.$$

EXAMPLE. Some small solutions are $(X, Y, Z, P, Q, R) = (44, 117, 240, 125, 267, 244)$, $(231, 160, 792, 281, 808, 825)$, and $(748, 195, 6336, 773, 6339, 6380)$. We show in Section 8 below that infinitely many such solutions exist.

The "semi-perfect" rational cuboid problems have attracted considerable attention. There are many papers on the problem, such as [Colman 1988]; see the references in [van Luijk 2000].

7. The semi-perfect rational cuboid problem, I

In this section we find solutions to Problem 1 following [Narumiya and Shiga 2001; Beukers and van Geemen 1995; van Luijk 2000] and we discuss arithmetic properties (e.g., L-series, modularity) of the associated varieties.

Using affine coordinates, Problem 1 becomes:

PROBLEM 1A. Find nonzero rational numbers x, y, z, q, w satisfying

$$x^2 + y^2 = 1, \quad y^2 + z^2 = q^2, \quad 1 + z^2 = w^2. \tag{$*$}$$

The substitutions

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}, \quad z = \frac{2s}{1-s^2}, \quad w = \frac{1+s^2}{1-s^2}, \quad q = \frac{2u}{(1+t^2)(1-s^2)}$$

give a birational map over $\mathbb{Q}$ from the surface defined by $(*)$ to the surface defined by

$$u^2 = (s^2t^2 + 1)(s^2 + t^2).$$

We now apply a series of birational maps (changes of variables) over $\mathbb{Q}$ in order to bring this equation into a familiar form.

(i) The change of variables $(v_1, t_1, u_1) := (st, t, tu)$ transforms our equation into $u_1^2 = (v_1^2 + 1)(v_1^2 + t_1^4)$.

(ii) The change of variables $(v_2, t_2, u_2) := (v_1, 1/(t_1 - 1), u_1/(t_1 - 1)^2)$ transforms the resulting equation into $u_2^2 = (v_2^2 + 1)(t_2^4 v_2^2 + (t_2 + 1)^4)$.

(iii) In the new variables $(v_3, t_3, u_3) := (v_2,\ (v_2^2 + 1)t_2,\ (v_2^2 + 1)u_2)$ this becomes $u_3^2 = t_3^4 + 4t_3^3 + 6(v_3^2 + 1)t_3^2 + 4(v_3^2 + 1)^2 t_3 + (v_3 + 1)^3$.

(iv) Using $(v_4, t_4, u_4) := (v_3, t_3 + 1, u_3)$ one obtains

$$u_4^2 = t_4^4 + 6v_4^2 t_4^2 + 4v_4^2(v_4^2 - 1)t_4 + v_4^2(v_4^4 - v_4^2 + 1).$$

(v) One transforms this quartic into a cubic as explained in [Cassels 1991, p. 35]. Explicitly, with $(x_1, y_1, v_5) := (-2u_4 + 2t_4^2 + 6v_4^2, 4t_4 u_4 - 4t_4^3 - 12t_4 v_4^2, v_4)$, the equation becomes

$$y_1^2 - 8v_5^2(v_5^2 - 1)y_1 = x_1^3 - 12v_5^2 x_1^2 - 4v_5^2(v_5^4 - 10v_5^2 + 1)x_1.$$

(vi) Next, put $(x_2, y_2, v_6) := (x_1 + 4v_5^2, y_1 - 4v_5^2(v_5^2 - 1), v_5)$. This transforms the equation into $y_2^2 = x_2^3 - 4v_6^2(v_6^2 + 1)^2 x_2$.

(vii) Finally, the change of variables

$$(x_3, y_3, z_3) := \left(\frac{x_2}{2v_6\,(v_6^2 + 1)}, \frac{y_2}{v_6\,(v_6^2 + 1)}, 2v_6\right)$$

gives the equation

$$y_3^2 = z_3(z_3^2 + 4)x_3(x_3^2 - 1).$$

PROPOSITION 7.1. (a) *Take* $C_1 : w_1^2 = x(x^2 - 1)$ *and* $E_2 : w_2^2 = z(z^2 + 4)$, *and let* $\iota : ((x, w_1),\ (z, w_2)) \mapsto ((x, -w_1),\ (z, -w_2))$ *be the* $[-1]$*-map on the abelian surface* $C_1 \times E_2$ *and* ι' *the* $[-1]$*-map on* $C_1 \times C_1$. *Then the algebraic surface* S *given by* $y^2 = x(x^2 - 1)z(z^2 + 4)$ *is birational to the Kummer surface* $\mathrm{Kum}(C_1 \times E_2) = (C_1 \times E_2)/\iota$.

(b) *The elliptic curves* C_1 *and* E_2 *are* 2*-isogeneous over* $\mathbb{Q}$. *The Kummer surface* $X := (C_1 \times C_1)/\iota'$, *defined by* $\eta^2 = \xi(\xi^2 - 1)\zeta(\zeta^2 - 1)$, *is a double cover of* S.

PROOF. (a) This is clear from the definitions.

(b) The 2-isogeny $C_1 \to E_2$ and its dual isogeny $E_2 \to C$ are well known; see, e.g., [Silverman and Tate 1992, p. 79]. Explicitly, the isogeny from C_1 to E_2 is given as

$$(x, w_1) \mapsto \left(\frac{w_1^2}{x^2},\ \frac{w_1(x^2 + 1)}{x^2}\right).$$

The 2 : 1 map from $X = \mathrm{Kum}(C_1 \times C_1)$ to S is then given by

$$x = \xi, \quad z = \frac{\eta^2}{\zeta^2 \xi(\xi^2 - 1)}, \quad y = \frac{\eta(1 + \zeta^2)}{\zeta^2}. \qquad \square$$

REMARK 7.2. B. van Geemen pointed out to us that the surface S is birational to the quartic Fermat surface. Hence it corresponds in the Shioda–Inose classification to the form $8x^2 + 8y^2$. A nice summary of the arithmetic of this surface, including a description of its Néron–Severi group and its L-series, is provided in [Pinch and Swinnerton-Dyer 1991]. An explicit birational map from the quartic Fermat surface to S is given in the (hand-written, Japanese) doctoral thesis of Masumi Mizukami, written around 1980.

The above considerations show that to find solutions to Problem 1A, one may construct rational points on the Kummer surface $X = \mathrm{Kum}(C_1 \times C_1)$. To describe such points, first note that a rational point on X lifts to a pair (P, Q) of points in $C_1 \times C_1$, defined over some quadratic extension $K/\mathbb{Q}$. If σ denotes conjugation in $K/\mathbb{Q}$, then the image of (P, Q) being rational precisely means that $(\sigma(P), \sigma(Q)) = \pm(P, Q)$. Hence either P and Q are both in $C_1(\mathbb{Q})$ (which means they are points of order 2 on C_1), or they are both rational points of infinite order on a quadratic twist C_n of C_1. This discussion is summarized as follows.

THEOREM 7.3. *Suppose that n is a nonzero integer, and (a, b) and (c, d) rational points on $C_n : y^2 = x^3 - n^2 x$. Then*

$$\left(\frac{a}{n}, \frac{c}{n}, \frac{bd}{n^3}\right)$$

is a rational point on the Kummer surface $X : w^2 = x(x^2 - 1)z(z^2 - 1)$. Conversely, every non-trivial rational point on X is obtained like this. $\square$

Note that the above result links congruent numbers to semi-perfect rational cuboids: from a pair of rational right-angled triangles with area n, one can construct a semi-perfect rational cuboid. In general, the problem of describing the set of rational points on a Kummer surface $\mathrm{Kum}(E_1 \times E_2)$ of a product of two elliptic curves has been studied by Kuwata and Wang [1993].

The Kummer surface X of $C_1 \times C_1$ has been studied extensively, e.g., in [Keum and Kondō 2001; Shioda and Inose 1977; Vinberg 1983; Ahlgren et al. 2002]. Here are some of its properties:

THEOREM 7.4. *Let X be the Kummer surface given by $w^2 = x(x^2-1)z(z^2-1)$.*

(a) *X is a singular $K3$ surface. Its Néron–Severi lattice has discriminant -16.*
(b) *X corresponds in the Shioda–Inose classification to the positive definite even binary quadratic form $4x^2 + 4y^2$.*

(c) *The L-series of X is*

$$L(X,s) = \zeta(s-1)^{19} L(\chi_4, s-1) L(f,s),$$

with

$$f(q) = \eta(q^4)^6 \in \mathfrak{S}_3(\Gamma_0(8), (2/\cdot)).$$

8. The semi-perfect rational cuboid problem, II

We now consider Problem 2 of finding nonzero integers satisfying

$$X^2 + Y^2 = P^2, \quad Y^2 + Z^2 = Q^2, \quad Z^2 + X^2 = R^2.$$

Euler recorded in 1772 the following parametric solution to this system:

$$\begin{aligned}
X &= 8\lambda(\lambda^2-1)(\lambda^2+1),\\
Y &= (\lambda^2-1)(\lambda^2-4\lambda+1)(\lambda^2+4\lambda+1),\\
Z &= 2\lambda(\lambda^2-3)(3\lambda^2-1),\\
P &= (\lambda^2-1)(\lambda^4+18\lambda+1),\\
Q &= (\lambda^2+1)^6,\\
R &= 2\lambda(5\lambda^4-6\lambda^2+5).,
\end{aligned}$$

The system of equations defines a surface $\mathcal{W} \subset \mathbb{P}^5$. Bremner [1988] has shown that $\mathcal{W}$ is birational to the quartic surface given by

$$(X^2-Y^2)(Z^2-R^2) = 2YZ(X^2-R^2).$$

He has produced pencils of elliptic curves on this quartic surface, and some rational curves on such pencils yield new parametric solutions over $\mathbb{Q}$ of degree 8 (different from that of Euler's) to Problem 2. A somewhat similar approach to that of Bremner was taken by Narumiya and Shiga [2001]. We briefly sketch their approach. Using affine coordinates, the surface is given by

$$x^2 + y^2 = 1, \quad y^2 + z^2 = q^2, \quad z^2 + x^2 = r^2.$$

Put $t = y/(x+1)$, so that

$$x = \frac{1-t^2}{1+t^2} \quad \text{and} \quad y = \frac{2t}{1+t^2}.$$

Next, change coordinates to $(t, x_0, x_2, x_3) := (t, z(1+t^2), q(1+t^2), r(1+t^2))$. The surface is now given by

$$x_0^2 + 4t^2 = x_2^2, \quad x_0^2 + (1-t^2)^2 = x_3^2.$$

We will denote this surface, regarded as a family of curves over the t-line, by $\mathcal{R}_t$.

LEMMA 8.1. *The family $E_t/\mathbb{Q}$ defined by $y^2 = x(x+4t^2)(x+(1-t^2)^2)$ is birational over $\mathbb{Q}$ to $\mathcal{R}_t$.*

PROOF. Put $M = 4t^2$ and $N = (1-t^2)^2$. Then the map $\mathcal{R}_t \to E_t$ is given by $(x_0, x_2, x_3) \mapsto (x, y)$ with

$$x = MN(x_3 - x_2)/\{(M-N)x_0 + Nx_2 - Mx_3\},$$
$$y = MN(N-M)/\{(M-N)x_0 + Nx_2 - Mx_3\}.$$

The inverse map $E_t \to \mathcal{R}_t$ is given by

$$x_0 = \{y^2 - M(x+N)^2\}/\,(2(x+N)y)\,,$$
$$x_2 = \{y^2 + M(x+N)^2\}/\,(2(x+N)y)\,,$$
$$x_3 = \{y^2 + N(x+M)^2\}/\,(2(x+M)y)\,.$$

The maps are clearly defined over $\mathbb{Q}$. □

Using a similar analysis as given in Section 7, Narumiya and Shiga [2001] showed that over $\mathbb{Q}(\sqrt{2})$, the surface E_t is birational to the Kummer surface associated with a product of two isogenous elliptic curves with CM by $\mathbb{Z}[\sqrt{-2}]$. An explicit rational curve in E_t is then used to show the following.

PROPOSITION 8.2 [Narumiya and Shiga 2001]. *One parametric solution to Problem* 2 *is given by*

$$X = -2(\lambda^2-4\lambda+5)^2(\lambda^2-5\lambda+5)(\lambda^2-5),$$
$$Y = -4\lambda(\lambda-2)(2\lambda-5)(\lambda^2-4\lambda+5)(\lambda^2-5\lambda+5),$$
$$Z = \lambda(\lambda-1)(\lambda-2)(\lambda-3)(\lambda-5)(2\lambda-5)(3\lambda-5),$$
$$P = -2(\lambda^2-4\lambda+5)(\lambda^2-5\lambda+5)(\lambda^4-4\lambda^3+8\lambda^2-20\lambda+25),$$
$$Q = \lambda(\lambda-2)(2\lambda-5)(-5\lambda^4+48\lambda^3-166\lambda^2+240\lambda-125),$$
$$R = 2\lambda^8-26\lambda^7+14\lambda^6-446\lambda^5+1066\lambda^4-2230\lambda^3+3525\lambda^2-3250\lambda+1250.$$

We remark that Narumiya and Shiga's method implies that E_t defines a singular K3 surface and has Mordell–Weil rank 2. One section of infinite order is given by $x = 4t^2$ (defined over $\mathbb{Q}(\sqrt{2})$). This is found using that E_t is a double cover of the rational elliptic surface defined by $y^2 = x(x+4s)(x+(1-s)^2)$. Using the table in [Oguiso and Shioda 1991], the Mordell–Weil group of the latter surface is seen to be isomorphic to $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$, with a generator modulo torsion of height $1/4$. It is then easily verified using [Shioda 1990] that $x = 4s$ defines such a generator. A second point on E_t is found by using the complex multiplication acting on the associated Kummer surface.

Acknowledgments

This text is based on a talk by Yui at the Clay Mathematics Institute Introductory Workshop (August 14–23, 2000) of the MSRI program on algorithmic number theory. Sincere thanks go to CMI for its generous support, and to MSRI for the hospitality. Parts of the article were written at CRM Barcelona, at Max-Planck-Institut für Mathematik Bonn, and at FIM ETH Zürich, during visiting professorships of the second author from January to March, April to May, and June 2001, respectively. She is especially indebted to H. Shiga, N. Narumiya, S.-i. Yoshida, and Ling Long for providing her with their respective papers (see bibliography), Ling Long also checked many calculations and suggested improvements. William Stein carried out calculations on some of the modular forms involved. Several mathematicians have given suggestions, and some have read earlier versions of this paper pointing out some inaccuracies and improvements. These include Joe Buhler, Imin Chen, Henri Cohen, Chuck Doran, Noam Elkies, Bert van Geemen, Yasuhiro Goto, Fernando Gouvêa, Ian Kiming, Kenichiro Kimura, Shigeyuki Kondo, Jyoti Sengupta, Jean-Pierre Serre, Peter Stevenhagen and Don Zagier. Last but not least, we thank Masanobu Kaneko and Takeshi Goto for reading the galley proof and pointing out typos and drawing attention to [Goto 2001; 2002].

References

[Ahlgren et al. 2002] S. Ahlgren, K. Ono, and D. Penniston, "Zeta functions of an infinite family of $K3$ surfaces", *Amer. J. Math.* **124**:2 (2002), 353–368.

[Basmaji 1996] J. Basmaji, *Ein Algorithmus zur Berechnung von Hecke-Operatoren und Anwendungen auf modulare Kurven*, Thesis, GHS-Essen (now Univ. Duisburg-Essen), 1996.

[Beukers 1998] F. Beukers, "The Diophantine equation $Ax^p + By^q = Cz^r$", *Duke Math. J.* **91**:1 (1998), 61–88.

[Beukers and van Geemen 1995] F. Beukers and B. van Geemen, "Rational cuboids", preprint, Universiteit Utrecht, 1995.

[Birch and Kuyk 1975] B. Birch and W. Kuyk (editors), *Modular functions of one variable, IV*, Lecture notes in mathematics **476**, Springer, Berlin, 1975.

[Birch and Swinnerton-Dyer 1965] B. J. Birch and H. P. F. Swinnerton-Dyer, "Notes on elliptic curves. II", *J. Reine Angew. Math.* **218** (1965), 79–108.

[Bremner 1988] A. Bremner, "The rational cuboid and a quartic surface", *Rocky Mountain J. Math.* **18**:1 (1988), 105–121.

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over **Q**: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939.

[Bruin 1999] N. Bruin, "The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$", *Compositio Math.* **118**:3 (1999), 305–321.

[Bruin 2000] N. Bruin, "On powers as sums of two cubes", pp. 169–184 in *Algorithmic number theory* (Leiden, 2000), Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.

[Buhler 2006] J. Buhler, "L-series in algorithmic number theory", in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2006.

[Bump et al. 1990] D. Bump, S. Friedberg, and J. Hoffstein, "Nonvanishing theorems for L-functions of modular forms and their derivatives", *Invent. Math.* **102**:3 (1990), 543–618.

[Cassels 1991] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, Cambridge, 1991.

[Chabauty 1941] C. Chabauty, "Sur les points rationnels des courbes algébriques de genre supérieur à l'unité", *C. R. Acad. Sci. Paris* **212** (1941), 882–885.

[Coates and Wiles 1977] J. Coates and A. Wiles, "On the conjecture of Birch and Swinnerton-Dyer", *Invent. Math.* **39**:3 (1977), 223–251.

[Coleman 1985] R. F. Coleman, "Effective Chabauty", *Duke Math. J.* **52**:3 (1985), 765–770.

[Colman 1988] W. J. A. Colman, "On certain semiperfect cuboids", *Fibonacci Quart.* **26**:1 (1988), 54–57.

[Darmon 1997] H. Darmon, "Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation", *C. R. Math. Rep. Acad. Sci. Canada* **19**:1 (1997), 3–14.

[Darmon and Granville 1995] H. Darmon and A. Granville, "On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$", *Bull. London Math. Soc.* **27**:6 (1995), 513–543.

[Dickson 1934] L. E. Dickson, *History of the theory of numbers*, vol. II, G. E. Stechert, New York, 1934.

[Dummit et al. 1985] D. Dummit, H. Kisilevsky, and J. McKay, "Multiplicative products of η-functions", pp. 89–98 in *Finite groups—coming of age* (Montreal, 1982), edited by J. McKay, Contemp. Math. **45**, Amer. Math. Soc., Providence, RI, 1985.

[Elkies 1994] N. D. Elkies, "Heegner point computations", pp. 122–133 in *Algorithmic number theory (ANTS-I)* (Ithaca, NY, 1994), edited by L. Adleman and M.-D. Huang, Lecture Notes in Comput. Sci. **877**, Springer, Berlin, 1994.

[Elkies 2002] N. D. Elkies, "Curves $Dy^2 = x^3 - x$ of odd analytic rank", pp. 244–251 in *Algorithmic number theory (ANTS-V)* (Sydney, 2002), edited by C. Fieker and D. R. Kohel, Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002.

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366.

[Fine 1976] N. J. Fine, "On rational triangles", *Amer. Math. Monthly* **83**:7 (1976), 517–521.

[Flicker 1980] Y. Z. Flicker, "Automorphic forms on covering groups of GL(2)", *Invent. Math.* **57**:2 (1980), 119–182.

[Fujiwara 1998] M. Fujiwara, "θ-congruent numbers", pp. 235–241 in *Number theory* (Eger, 1996), edited by K. Győry et al., de Gruyter, Berlin, 1998.

[Goto 2001] T. Goto, "Calculation of Selmer groups of elliptic curves with rational 2-torsions and θ-congruent number problem", *Comment. Math. Univ. St. Paul.* **50**:2 (2001), 147–172.

[Goto 2002] T. Goto, *A study on the Selmer groups of the elliptic curves with a rational 2-torsion*, doctoral thesis, Kyushu Univ., 2002. See http://www.ma.noda.tus.ac.jp/u/tg/files/thesis.pdf.

[Grant 1994] D. Grant, "A curve for which Coleman's effective Chabauty bound is sharp", *Proc. Amer. Math. Soc.* **122**:1 (1994), 317–319.

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320.

[Heegner 1952] K. Heegner, "Diophantische Analysis und Modulfunktionen", *Math. Z.* **56** (1952), 227–253.

[Inose 1976] H. Inose, "On certain Kummer surfaces which can be realized as non-singular quartic surfaces in P^3", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **23**:3 (1976), 545–560.

[Inose 1978] H. Inose, "Defining equations of singular $K3$ surfaces and a notion of isogeny", pp. 495–502 in *Proceedings of the International Symposium on Algebraic Geometry* (Kyoto, 1977), edited by M. Nagata, Kinokuniya, Tokyo, 1978.

[Joshi and Tzermias 1999] K. Joshi and P. Tzermias, "On the Coleman–Chabauty bound", *C. R. Acad. Sci. Paris Sér. I Math.* **329**:6 (1999), 459–463.

[Kan 2000] M. Kan, "θ-congruent numbers and elliptic curves", *Acta Arith.* **94**:2 (2000), 153–160.

[Keum and Kondō 2001] J. Keum and S. Kondō, "The automorphism groups of Kummer surfaces associated with the product of two elliptic curves", *Trans. Amer. Math. Soc.* **353**:4 (2001), 1469–1487.

[Koblitz 1993] N. Koblitz, *Introduction to elliptic curves and modular forms*, vol. 97, 2nd ed., Graduate Texts in Mathematics, Springer, New York, 1993.

[Kolyvagin 1988] V. A. Kolyvagin, "Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **52**:3 (1988), 522–540. In Russian; translated in *Math. USSR. Izv.* **32** (1989), 523–542.

[Korec 1984] I. Korec, "Nonexistence of a small perfect rational cuboid, II", *Acta Math. Univ. Comenian.* **44/45** (1984), 39–48.

[Kraus 1999] A. Kraus, "On the equation $x^p + y^q = z^r$: a survey", *Ramanujan J.* **3**:3 (1999), 315–333.

[Kuwata and Wang 1993] M. Kuwata and L. Wang, "Topology of rational points on isotrivial elliptic surfaces", *Internat. Math. Res. Notices* **1993**:4 (1993), 113–123.

[Lehmer 1899/1900] D. N. Lehmer, "Rational triangles", *Ann. of Math.* (2) **1**:1-4 (1899/1900), 97–102.

[Livné 1987] R. Livné, "Cubic exponential sums and Galois representations", pp. 247–261 in *Current trends in arithmetical algebraic geometry* (Arcata, CA, 1985), edited by K. Ribet, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, 1987.

[Livné 1995] R. Livné, "Motivic orthogonal two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$", *Israel J. Math.* **92**:1-3 (1995), 149–156.

[Long 2004] L. Long, "On Shioda-Inose structures of one-parameter families of K3 surfaces", *J. Number Theory* **109**:2 (2004), 299–318.

[van Luijk 2000] R. van Luijk, *On perfect cuboids*, Doctoraalscriptie, Universiteit Utrecht, 2000. See http://www.math.leidenuniv.nl/reports/2001-12.shtml.

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162.

[Morrison 1984] D. R. Morrison, "On $K3$ surfaces with large Picard number", *Invent. Math.* **75**:1 (1984), 105–121.

[Murty and Murty 1991] M. R. Murty and V. K. Murty, "Mean values of derivatives of modular L-series", *Ann. of Math.* (2) **133**:3 (1991), 447–475.

[Nagell 1929] T. Nagell, *L' Analyse indéterminée de degré supérieur*, vol. 39, Gauthier-Villars, Paris, 1929.

[Narumiya and Shiga 2001] N. Narumiya and H. Shiga, "On certain rational cuboid problems", *Nihonkai Math. J.* **12**:1 (2001), 75–88.

[Nemenzo 1998] F. R. Nemenzo, "All congruent numbers less than 40000", *Proc. Japan Acad. Ser. A Math. Sci.* **74**:1 (1998), 29–31.

[Oguiso and Shioda 1991] K. Oguiso and T. Shioda, "The Mordell-Weil lattice of a rational elliptic surface", *Comment. Math. Univ. St. Paul.* **40**:1 (1991), 83–99.

[Peters et al. 1992] C. Peters, J. Top, , and M. van der Vlugt, "The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes", *J. Reine Angew. Math.* **432** (1992), 151–176.

[Pinch and Swinnerton-Dyer 1991] R. G. E. Pinch and H. P. F. Swinnerton-Dyer, "Arithmetic of diagonal quartic surfaces, I", pp. 317–338 in *L-functions and arithmetic* (Durham, 1989), London Math. Soc. Lecture Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991.

[Poonen 2008] B. Poonen, "Elliptic curves", pp. 183–207 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Shimura 1973] G. Shimura, "On modular forms of half integral weight", *Ann. of Math.* (2) **97** (1973), 440–481.

[Shioda 1990] T. Shioda, "On the Mordell-Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240.

[Shioda and Inose 1977] T. Shioda and H. Inose, "On singular $K3$ surfaces", pp. 119–136 in *Complex analysis and algebraic geometry*, edited by W. Baily and T. Shioda, Iwanami Shoten, Tokyo, and Cambridge University Press, New York, 1977.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer, New York, 1992.

[Stein 2008] W. Stein, "An introduction to computing modular forms using modular symbols", pp. 641–652 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Stienstra and Beukers 1985] J. Stienstra and F. Beukers, "On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces", *Math. Ann.* **271**:2 (1985), 269–304.

[Taylor and Wiles 1995] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* (2) **141**:3 (1995), 553–572.

[Tunnell 1983] J. B. Tunnell, "A classical Diophantine problem and modular forms of weight $3/2$", *Invent. Math.* **72**:2 (1983), 323–334.

[Vinberg 1983] È. B. Vinberg, "The two most algebraic $K3$ surfaces", *Math. Ann.* **265**:1 (1983), 1–21.

[Waldspurger 1981] J.-L. Waldspurger, "Sur les coefficients de Fourier des formes modulaires de poids demi-entier", *J. Math. Pures Appl.* (9) **60**:4 (1981), 375–484.

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551.

[Yoshida 2001] S.-i. Yoshida, "Some variants of the congruent number problem, I", *Kyushu J. Math.* **55**:2 (2001), 387–404.

[Yoshida 2002] S.-i. Yoshida, "Some variants of the congruent number problem, II", *Kyushu J. Math.* **56**:1 (2002), 147–165.

JAAP TOP
INSTITUUT VOOR WISKUNDE EN INFORMATICA
P.O.BOX 800
9700 AV GRONINGEN
THE NETHERLANDS
top@math.rug.nl

NORIKO YUI
DEPARTMENT OF MATHEMATICS AND STATISTICS
QUEEN'S UNIVERSITY
KINGSTON, ONTARIO
CANADA K7L 3N6
yui@mast.queensu.ca