Journal of Number Theory **67**, 277–290 (1997)
Article No. NT972189

Some Interesting Curves of genus 2 to 7

Andrew Bremner

Department of Mathematics, Arizona State University,
Tempe, Arizona 85287-1804
E-mail: bremner@asu.edu

Communicated by Alan C. Woods

Received February 12, 1997; revised May 1, 1997

Counterexamples to the Hasse Principle are constructed for curves of genus 2 to 7. These have the property that their Jacobian splits as a product of elliptic curves, all of positive rational rank. © 1997 Academic Press

In a startling paper, Ekedahl and Serre [4] construct curves of genus g whose Jacobian is isogenous to a product of elliptic curves, for values of g in the set $\{1, 2, ..., 29, 31, 33, ..., 649, 1297\}$. These arise either as modular curves or as coverings of curves of genus 2 or 3. We present here a rather more modest range of examples concerned with the following related but more delicate arithmetic question. Construct over $\mathbf{Q}$ curves C of a given genus g such that (i) the Jacobian of C is ($\mathbf{Q}$-isogenous to) a product of elliptic cuves, (ii) each factor of the Jacobian has positive Mordell–Weil rank over $\mathbf{Q}$, (iii) the curve C possesses a point everywhere locally, that is, in $\mathbf{R}$, and in all p-adic fields $\mathbf{Q}_p$, and (iv) the curve C has no $\mathbf{Q}$-point. It is this latter condition that provides for interesting and non-trivial examples; a global rational point on C induces global points on the elliptic curves comprising the Jacobian, which will then in general all have positive rank. A curve satisfying (iii) and (iv) by definition fails the Hasse Principle and must accordingly have genus at least one. The first examples of such curves, of genus one, appear to be the curve $2y^2 = x^4 - 17$ of Reichardt [5] and $3x^3 + 4y^3 + 5z^3 = 0$ of Selmer [6]. Obviously a curve of genus one cannot simultaneously satisfy (ii) and (iv), so the examples of this paper necessarily have genus $g \geqslant 2$. As an extra restriction, it was decided to demand that the elliptic curves in the Jacobian of C be distinct, more particularly, non-isogenous, so that the positive ranks of the factors of the Jacobian arise genuinely independently. In practice, it was surprising how first attempts to construct examples often led to cases of multiple factors (cf. Ekedahl and Serre).

0022-314X/97 $25.00

Condition (i), that the Jacobian of C be isogenous to a product of elliptic curves, has its origins in the study of Abelian integrals during the 19th century. For our purposes, it may be verified for a particular curve C by exhibiting explicit rational maps from C to the appropriate number (g) of distinct elliptic curves. Standard arguments then imply that these maps induce an isogeny from the Jacobian of C to the product of the elliptic curves.

In the case of genus 3, Bremner, Lewis, and Morton [2] give the following example,

$$C\colon 3x^4+4y^4=19z^4$$

mapping to the three elliptic cuves

$$\begin{aligned} E_1&: 3X^2+4y^4=19z^4\\ E_2&: 3x^4+4Y^2=19z^4\\ E_3&: 3x^4+4y^4=19Z^2 \end{aligned}$$

with respective points of infinite order (10, 1, 2), (1, 2, 1), (5, 8, 31). They also show that C satisfies (iii) and (iv), as required.

In the case of genus 5, Bremner [1] exhibits the curve in projective 4-space

$$\begin{aligned} C\colon 4x^2-11y^2&=r^2\\ 17x^2+y^2&=s^2\\ x^2+y^2&=t^2 \end{aligned}$$

with all the properties (i)–(iv); see [1] for details.

The purpose of this paper is to provide examples for instances of other genus, and we shall restrict attention to the cases $g=2, 4, 6, 7$. We try to motivate in each instance the relevant construction, though many relatively tedious details have been suppressed. In practice, as many parameters as possible were retained until a search by specialization proved the only sensible step forward. Extensive use was made of PARI-gp, and the elliptic curve programs "mrank" of Cremona, and "Apecs" of Connell.

For local sovability, frequent application is made of the Weil inequality, that for a curve C of genus g, there exists a point on C over $\mathbf{Q}_p$ for all primes p satisfying $p+1>2g\sqrt{p}$, provided C is non-singular at p. For global insolvability, we provide *ad aequationem* arguments in each case. The hypothesis that each factor of the Jacobian of C has positive rank implies that the rank of Jac(C) is at least equal to g, so that Chabauty's Theorem, for instance, and its attendant methods, is inapplicable. See

Cassels and Flynn [3], Chapter 13, for a worked example of the determination of all rational points on a curve C of genus 2 where Jac(C) has rank equal to 1.

Genus 2

Despite the recent burgeoning of interest and knowledge in the area of curves of genus 2, I am not aware in the literature of an example of such a curve satisfying the properties (i)–(iv). There are several lines of attack: we choose naively to consider curves of type

$$y^2 = Ax^6 + B \tag{1}$$

mapping to the two curves of genus 1 given by

$$Y_1^2 = AX_1^3 + B, \qquad Y_2^2 = A + BX_2^3,$$

via the maps

$$(X_1, Y_1) = (x^2, y), \qquad (X_2, Y_2) = \left(\frac{1}{x^2}, \frac{y}{x^3}\right). \tag{2}$$

Searching over the parameters A, B for curves of positive rank is not difficult. But one needs some method for establishing that (1) has no **Q**-point, not obvious if it has to possess points everywhere locally. It was decided to fix $B = -29$, chosen because the class-number of $\mathbf{Q}(\sqrt{-29})$ equals 6.

THEOREM. *The curve* $C: y^2 = 5x^6 - 29$ *satisfies properties* (i)–(iv).

Proof. C maps via (2) to the elliptic curves

$$Y_1^2 = 5X_1^3 - 29 \qquad \text{and} \qquad Y_2^2 = 5 - 29X_2^3,$$

with conductors $2^4 \cdot 3^3 \cdot 5^2 \cdot 29^2$ and $2^2 \cdot 3^3 \cdot 5^2 \cdot 29^2$, and respective points of infinite order $(9/5, 2/5)$, $(-19, 446)$; so (i) and (ii) hold. The curve C is singular only at the primes 2, 3, 5, 29, so the Weil inequality mandates a p-adic point for $p \geqslant 17$ $(p \neq 29)$. To verify (iii) therefore it is only necessary to exhibit a point on C over $\mathbf{Q}_p$ for $p = \infty$, 2, 3, 5, 7, 11, 13, 29. But $(0, \sqrt{-29})$ is a point for $p = 3$, 5, 11, 13; $(\sqrt[6]{29/5}, 0)$ for $p = \infty$, 2; and $(1, \sqrt{-24})$ for $p = 7$, 29. Finally, suppose $a, b, c \in \mathbf{Z}$ satisfy

$$c^2 = 5a^6 - 29b^6, \qquad (a, b) = 1. \tag{3}$$

Clearly $a \equiv b \equiv 1 \pmod 2$, $c \equiv 0 \pmod 2$, and

$$(c + b^3\sqrt{-29})(c - b^3\sqrt{-29}) = 5a^6.$$

The two principal ideals $(c \pm b^3\sqrt{-29})$ in $\mathbf{Z}[\sqrt{-29}]$ are coprime, and it follows that there exists an ideal $\mathfrak{a}$ of $\mathbf{Z}[\sqrt{-29}]$ such that

$$(c + b^3\sqrt{-29}) = \mathfrak{p}_5\mathfrak{a}^6, \tag{4}$$

where $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ in $\mathbf{Z}[\sqrt{-29}]$; and $\mathfrak{p}_5 = (5, 1 + \sqrt{-29})$ is non-principal.

But the class-number of $\mathbf{Q}(\sqrt{-29})$ is 6, so that $\mathfrak{a}^6$ is principal, and (4) implies $\mathfrak{p}_5$ is a principal ideal, which is a contradiction. Thus (3) has no non-trivial solution, and C satisfies condition (iv). ▌

Genus 4

There are two relatively amenable families of curves of genus 4, namely, intersections in affine 3-space of the type

$$r^2 = g(x), \qquad s^2 = h(x),$$

where g, h are cubics with no repeated root and with no common zero; and hyperelliptic curves in affine 2-space of type

$$C\colon y^2 = f(x) \tag{5}$$

with f a polynomial of degree 9 or 10 with distinct roots. We choose here to illustrate only examples of the latter type. The method is to suppose that f has no terms of odd degree in x, thereby giving two distinct maps $(X_1, Y_1) = (x^2, y)$ and $(X_2, Y_2) = (1/x^2, y/x^5)$ from C to curves Γ_1, Γ_2 of genus 2. We can ensure that the Jacobians of Γ_1 and Γ_2 are reducible by demanding that there exist linear fractional transformations mapping the equations of Γ_1, Γ_2 into equations of type

$$y^2 = \text{sextic in } x,$$

where the sextic has no terms of odd degree in x. Then each $\mathrm{Jac}(\Gamma_i)$ will be (isogenous to) the product of two elliptic curves; and $\mathrm{Jac}(C)$ the product of four elliptic curves. To add to the interest of the example, we actually make the demand that each Γ_i contain a rational point, so that C is indeed trying hard to possess a global rational point!

THEOREM. *The curve*

$$\begin{aligned} C\colon 146734y^2 = {}& (5x^2 - 586936)(5x^2 + 1320606)(29x^2 + 9537710) \\ & \times (125x^4 + 35362894x^2 + 1722469340480) \end{aligned}$$

satisfies properties (i)–(iv).

Proof. The Jacobian of C splits as the product of the two curves of genus 2,

$$\begin{aligned}\Gamma_1\colon 146734y_1^2 &= (5x_1-586936)(5x_1+1320606)(29x_1+9537710)\\ &\quad\times(125x_1^2+35362894x_1+1722469340480)\\ \Gamma_2\colon 146734y_2^2 &= (5-586936x_2)(5+1320606x_2)(29+9537710x_2)\\ &\quad\times(125+35362894x_2+1722469340480x_2^2),\end{aligned}$$

containing the respective points $(-146734, 465066721926)$ and $(1/146734, 2)$. Under the maps

$$(x_1, y_1)=\left(\frac{-146734(17X_1+2512)}{5(X_1+464)}, \quad \frac{3798044895758400\,Y_1)}{125(X_1+464)^3}\right)$$

and

$$(x_2, y_2)=\left(\frac{-X_2-1}{146734(X_2+9)}, \frac{4Y_2}{73367(X_2+9)^3}\right)$$

then Γ_1, Γ_2 transform respectively into

$$Y_1^2=2(X_1^2-43264)(X_1^2-215296)(-X_1^2+10496)$$

and

$$Y_2^2=146734(X_2^2-81)(81X_2^2-2401)(-9X_2^2+2009).$$

These in turn map to

$$\begin{aligned}E_1&\colon y_1^2=2(x_1-43264)(x_1-215296)(-x_1+10496)\\ E_2&\colon y_2^2=2(1-43264x_2)(1-215296x_2)(-1+10496x_2)\\ E_3&\colon y_3^2=146734(x_3-81)(81x_3-2401)(-9x_3+2009)\\ E_4&\colon y_4^2=146734(1-81x_4)(81-2401x_4)(-9+2009x_4)\end{aligned}$$

with respective conductors 840, 12983880, 335881521393600, 13771142377137600 and points of infinite order (256, 13762560), (1/256, 3360), (25, 2347744), (1/25, 2347744/125). C is singular at precisely $p=2$, 3, 5, 7, 13, 29, 41, 47, 223, and the Weil inequality mandates a point on C over $\mathbf{Q}_p$ for $p\geqslant 67$, $p\neq 223$. There is a point on C over $\mathbf{Q}_p$ for $x=0$ at both $p=223$, and at primes less than 67 except $p=2$, 3, 5, 13, 23, 37, 41, 43. However, $x=1$ gives a $\mathbf{Q}_p$-point for $p=3$, 5, 41, 43; $x=2$ for $p=2$, 13, 23; $x=4$ for $p=37$; and $x=343$ for $p=\infty$. So C is everywhere locally solvable. It remains to show that C has no point in $\mathbf{Q}$.

The resultant of $(5x^2-586936)$ and $(5x^2+1320606)(29x^2+9537710)(125x^4+35362894x^2+1722469340480)$ is $-2^{12}\cdot 3^8\cdot 5^4\cdot 7^{16}\cdot 13^2\cdot 47^8\cdot 223^8$, and it follows that a rational point (x, y) on C must satisfy the following, for some $u_1\in\mathbf{Q}$:

$$5x^2-586936=\lambda_1 u_1^2, \qquad \lambda_1 \mid 2.3.5.7.13.47.223. \tag{6}$$

In the same way, there must exist $u_2, u_3, u_4\in\mathbf{Q}$ such that

$$5x^2+1320606=\lambda_2 u_2^2, \qquad \lambda_2 \mid 2.5.7.13.47.223 \tag{7}$$

$$29x^2+9537710=\lambda_3 u_3^2, \qquad \lambda_3 \mid 2.3.5.7.47.223 \tag{8}$$

$$125x^4+35362894x^2+1722469340480=\lambda_4 u_4^2, \qquad \lambda_4 \mid 2.3.5.7.47.223 \tag{9}$$

with

$$\lambda_1\lambda_2\lambda_3\lambda_4\equiv 146734=2.7.47.223 \bmod \mathbf{Q}^{*2}. \tag{10}$$

Local solvability of each individual equation above reduces consideration to

$$\lambda_1\in\{5,\ 2.5.7,\ 5.47.223,\ 2.5.7.47.223,\ -1,\ -2.7,\ -47.223,\ -2.7.47.223\}$$

$$\lambda_2\in\{5,\ 2.223,\ 5.7.47,\ 2.7.47.223\}$$

$$\lambda_3=2.7.47.223$$

$$\lambda_4=5$$

so that condition (10) forces $\lambda_1\lambda_2\equiv 5 \bmod \mathbf{Q}^{*2}$, whence

$$(\lambda_1, \lambda_2)=(2.5.7.47.223,\ 2.7.47.223).$$

Writing X/Z for x and U_i/Z for u_i with $(X, Z)=1$, then (6), (7) become

$$5X^2-586936Z^2=2.5.7.47.223U_1^2$$

$$5X^2+1320606Z^2=2.7.47.223U_2^2$$

whence $5\mid Z$, $5\mid U_2$, leading to $5\mid X$, contradicting $(X, Z)=1$. ∎

Remark. It proved less troublesome constructing examples without the requirement that each Γ_i possess a global point. With the extra hypothesis, the principal difficulty was to ensure local solvability at the primes dividing the content of the defining polynomial f at (5).

Genus 6

To supply curves of genus 6 with split Jacobian, we use the following idea suggested by Jaap Top. Let Γ_1 be a curve of genus 1 given by $u^2 = f_3(x)$, f_3 a polynomial of degree 3; and let Γ_2 be a curve of genus 2 given by $v^2 = f_5(x)$, f_5 a polynomial of degree 5. Provided f_3, f_5 have no common zero, then the Riemann–Hurwitz theorem implies that the genus of the curve C of intersection

$$C\colon u^2 = f_3(x), \qquad v^2 = f_5(x)$$

equals 6. Denote by Γ_3 the curve of genus 3 given by $w^2 = f_3(x)\, f_5(x)$. Then there exist maps from C to each curve Γ_i, which induce an isogeny of the Jacobian of C with $\mathrm{Jac}(\Gamma_1) \times \mathrm{Jac}(\Gamma_2) \times \mathrm{Jac}(\Gamma_3)$ (of the correct dimension, $1+2+3$). By appropriate choice of f_3, f_5, one can achieve complete splitting of $\mathrm{Jac}(\Gamma_2)$ and $\mathrm{Jac}(\Gamma_3)$, and hence of $\mathrm{Jac}(C)$. Specifically, take $f_3(x) = (x+\lambda)(x^2 - (1/\lambda^2))$, $f_5(x) = (x-\lambda)(x^4 + \mu x^2 + 1)$ so that $\Gamma_3\colon w^2 = (x^4 - (\lambda^2 + (1/\lambda^2))\, x^2 + 1)(x^4 + \mu x^2 + 1)$; then Γ_3 contains the three distinct involutions given by

$$(x, w) \mapsto (-x, w); \qquad (x, w) \mapsto \left(\frac{1}{x}, \frac{w}{x^4}\right); \qquad (x, w) \mapsto \left(\frac{1}{x}, -\frac{w}{x^4}\right)$$

and by computing the relevant fixed fields, we obtain three maps to elliptic curves, and a split $\mathrm{Jac}(\Gamma_3)$. It remains to split $\mathrm{Jac}(\Gamma_2)$, and to that end we demand that a Möbius transformation of type

$$(x, y) = \left(\frac{pX+q}{rX+s}, \frac{Y}{(rX+s)^3}\right)$$

transform Γ_2 into an equation of type

$$Y^2 = PX^6 + QX^4 + RX^2 + S$$

whose Jacobian is then clearly split, with maps to

$$Y_1^2 = PX_1^3 + QX_1^2 + RX_1 + S, \qquad Y_2^2 = P + QX_2 + RX_2^2 + SX_2^3.$$

All that remains is a judicious choice of parameters λ, μ so that conditions (iii), (iv) will hold. In the construction above, the curve C contains the point at infinity $x = 1/0^2$, and to avoid this, scalar multiples of f_3 and f_5 were chosen.

Theorem. *The curve*

$$C\colon r^2 = -5(x+\tfrac{9}{5})(x^2-\tfrac{25}{81})$$
$$s^2 = 19(x-\tfrac{9}{5})(x^4-\tfrac{82}{9}x^2+1)$$

satisfies conditions (i)–(iv)

Proof. The genus 1 component of Jac(C) is

$$E_1\colon r^2 = -5(x+\tfrac{9}{5})(x^2-\tfrac{25}{81}),$$

an elliptic curve of conductor 118720, rank 1, and generator $(0, \frac{5}{3})$.

The genus 2 component of Jac(C) is

$$s^2 = 19(x-\tfrac{9}{5})(x^4-\tfrac{82}{9}x^2+1). \tag{11}$$

Under the transformation

$$(x, s) = \left(\frac{7X+1}{-X+1}, \frac{16S}{45(-X+1)^3}\right),$$

(11) becomes

$$S^2 = 855(1-147X^2+3171X^4-3025X^6),$$

which in turn maps to

$$E_2\colon \sigma_2^2 = 855(1-147\tau_2+3171\tau_2^2-3025\tau_2^3)$$

and

$$E_3\colon \sigma_3^2 = 855(\tau_3^3-147\tau_3^2+3171\tau_3-3025),$$

elliptic curves of conductors 57182400, 5198400, rank 1, and points of infinite order

$$(\tau_2, \sigma_2) = (\tfrac{2429}{15125}, \tfrac{3020544}{15125}), \qquad (\tau_3, \sigma_3) = (\tfrac{882955}{6859}, \tfrac{1219458240}{130321}),$$

respectively.

The genus 3 component of Jac(C) is

$$t^2 = -95(x^2-\tfrac{81}{25})(x^2-\tfrac{25}{81})(x^2-9)(x^2-\tfrac{1}{9}).$$

First, put $X = x^2$, fixed under the involution $x \to -x$. This results in a map to

$$E_4\colon t_4^2 = -95(X_4-\tfrac{81}{25})(X_4-\tfrac{25}{81})(X_4-9)(X_4-\tfrac{1}{9}),$$

an elliptic curve of conductor 110493075, rank 2, and independent points of infinite order

$$(X_4, t_4) = (\tfrac{433}{97}, \tfrac{24812480}{254043}), \qquad (\tfrac{729}{6161}, \tfrac{72181760}{37957921}).$$

Second, put

$$u = x + \frac{1}{x}, \qquad v = t + \frac{t}{x^4},$$

giving

$$v^2 = \frac{t^2}{x^4}\left(x^4 + \frac{1}{x^4} + 2\right) = -95\left(x^2 - \frac{7186}{2025} + \frac{1}{x^2}\right)\left(x^2 - \frac{82}{9} + \frac{1}{x^2}\right)\left(x^2 + \frac{1}{x^2}\right)^2,$$

that is,

$$\left(\frac{uv}{u^2-2}\right)^2 = -95u^2\left(u^2 - \frac{11236}{2025}\right)\left(u^2 - \frac{100}{9}\right),$$

affording a map from C to

$$E_5\colon t_5^2 = -95X_5(X_5 - \tfrac{11236}{2025})(X_5 - \tfrac{100}{9}),$$

an elliptic curve of conductor 31569450, rank 1, and point of infinite order $(\frac{256}{25}, \frac{8512}{135})$. Third, put

$$u = x + \frac{1}{x}, \qquad v = t - \frac{t}{x^4}$$

and, as above, there is a map from C to

$$E_6\colon t_6^2 = -95(X_6 - 4)(X_6 - \tfrac{11236}{2025})(X_6 - \tfrac{100}{9}),$$

an elliptic curve of conductor 2084775, rank 2, and independent points of infinite order

$$(\tfrac{7636}{1125}, \tfrac{1906688}{50625}), \qquad (-\tfrac{60820}{171}, \tfrac{103548928}{1539}).$$

Consequently, $\mathrm{Jac}(\Gamma_3)$ is isogenous to $E_4 \times E_5 \times E_6$; and $\mathrm{Jac}(C)$ to the product of $E_1, \ldots, E_6$. Thus C satisfies (i) and (ii). By writing $x = -(X+25)/45$, the equations for C become

$$R^2 = X(X-56)(X+50) \tag{12}$$

$$S^2 = -95(X-110)(X+10)(X+40)(X+106)(X+160). \tag{13}$$

Now C is singular only at the primes 2, 3, 5, 7, 11, 19, 53, so the Weil inequality guarantees a point on C over $\mathbf{Q}_p$ for $p \geqslant 149$. Further, for $p < 149$ and $p = \infty$, there are $\mathbf{Q}_p$ points on C for either $X = 0$, 56 or -50, except in the instances $p = 2$, 5, 11, 19, 29, 37, 47, 53. When $X = 110$, there is a point over $\mathbf{Q}_5$, $\mathbf{Q}_{19}$, $\mathbf{Q}_{53}$, and when $X = -40$, a point over $\mathbf{Q}_{29}$, $\mathbf{Q}_{47}$. This leaves $p = 2$, 11, 37 with $\mathbf{Q}_p$ points provided by $X = 2$, 2, 1 respectively. Thus C satisfies (iii), and it remains to verify that C has no point over $\mathbf{Q}$. The curve (12) has rank 1 with generator $(-25, 225)$, and torsion group generated by the points of order 2. Consequently, a rational point (X, R) satisfies $X = \delta U^2/V^2$ for $\delta = \pm 1$, ± 2, ± 7, ± 14, and coprime integers U, V. Mod 5, $U \not\equiv 0$, otherwise the numerator of the right-hand side of (13) is exactly divisible by 5^5, impossible. Also $V \not\equiv 0 \bmod 5$, for otherwise the denominator of the right-hand side of (13) is exactly divisible by an odd power of 5, impossible. It now follows from (12), (13) that

$$\delta U^2 - 56 V^2 \equiv \square \bmod 5 \tag{14}$$

$$\delta U^2 + 106 V^2 \equiv 0 \bmod 5. \tag{15}$$

Adding, $2\delta U^2 \equiv \square \bmod 5$, so that $(\delta/5) = -1$, contradicting (15). Thus C satisfies (iv). ▮

Remark. The genus 1, 2, and 3 components of Jac(C) each contain a global rational point, with, respectively, r, s, t being 0.

Genus 7

The model chosen for the curve C is the following intersection of three elliptic curves:

$$E_1 : r^2 = f(x), \qquad E_2 : s^2 = g(x), \qquad E_3 : t^2 = h(x),$$

where f, g, h are rational cubics with no pairwise common zero. The Riemann–Hurwitz formula implies that the genus of C is 7. Note that there are already three obvious projections from C to the curves E_i.

To split the Jacobian of C, we shall demand that the curves of genus 2

$$\Gamma_1 : \tau^2 = f(x)\, g(x), \qquad \Gamma_2 : \sigma^2 = f(x)\, h(x)$$

both have split Jacobian. To achieve the former, take $f(x)$, $g(x)$ in the form

$$f(x) = (x + \alpha)(x^2 + \beta x + \delta), \qquad g(x) = (\alpha x + 1)(\delta x^2 + \beta x + 1)$$

so that Γ_1 is invariant under the involutions $x \to (1/x)$, $y \to (y/x^3)$ and $x \to (1/x)$, $y \to (-y/x^3)$, and consequently has split Jacobian. To split the Jacobian of Γ_2, we choose $h(x) = x(x^2 + \delta x + \varepsilon)$ and use the criterion of Cassels and Flynn [3], Chapter 14, to make linearly dependent over $\mathbf{Q}$ the quadratics $x(x+\alpha)$, $x^2+\beta x+\gamma$, $x^2+\delta x+\varepsilon$. Care has to be taken to ensure that the resuling factors of the Jacobian are defined over $\mathbf{Q}$, but the details are relatively technical, and are suppressed. As before, it is now necessary to make an appropriate choice of parameter.

THEOREM. *The Curve*

$$C\colon r^2=(x+2)(x^2+14x-3) \tag{16}$$

$$s^2=(2x+1)(-3x^2+14x+1) \tag{17}$$

$$t^2=x(4x^2+36x-7) \tag{18}$$

satisfies conditions (i)–(iv).

Proof. The curve $E_1\colon r^2=(x+2)(x^2+14x-3)$ has conductor 312, rank 1, and generator (1, 6).

The curve $E_2\colon s^2=(2x+1)(-3x^2+14x+1)$ has conductor 624, rank 1, and generator (0, 1).

The curve $E_3\colon t^2=x(4x^2+36x-7)$ has conductor 4928, rank 1, and generator $(\frac{1}{4}, \frac{3}{4})$.

The curve $\Gamma_1\colon \tau^2=(x+2)(2x+1)(x^2+14x-3)(-3x^2+14x+1)$ maps to the curve

$$E_4\colon w_4^2=(u_4+2)(-6u_4^3-71u_4^2+284u_4+1060)$$

under

$$(u_4, w_4)=\left(x+\frac{1}{x}, \frac{\tau(x+1)}{x^2}\right)$$

and maps to the curve

$$E_5\colon w_5^2=(u_5-2)(-6u_5^3-71u_5^2+284u_5+1060)$$

under

$$(u_5, w_5)=\left(x+\frac{1}{x}, \frac{\tau(x-1)}{x^2}\right).$$

E_4 has conductor 4056, rank 1, and generator (2/7, 2496/49).

E_5 has conductor 8112, rank 1, and generator (98/31, 33696/961).

On the curve $\Gamma_2\colon \sigma^2=x(x+2)(x^2+14x-3)(4x^2+36x-7)$ put $x=(2X+1)/2(X-1)$, $\sigma=3Y/4(X-1)^3$ to give

$$Y^2=3(4X^2-1)(11X^2-8)(16X^2-13),$$

which in turn maps to

$$E_6\colon y^2 = 3(4x-1)(11x-8)(16x-13),$$

of conductor 18480, rank 1, and generator (107/176, 189/44); and to

$$E_7\colon y^2 = 3(4-x)(11-8x)(16-13x)$$

of conductor 2730, rank 1, and generator (31/13, 315/13).

We now have Jac(C) is isogenous to the product of E_1, ..., E_7. For local solutions, $x=0$ gives a point on C over $\mathbf{Q}_p$ provided $(-6/p)=+1$; $x=1$, provided $(33/p)=+1$; and $x=1/4$, provided $(46/p)=+1$. The curve C is singular at precisely $p=2$, 3, 5, 7, 11, 13, 7229, so by the Weil inequality, it is only necessary to consider primes $p\leqslant 199$, together with $p=7229$. The following table provides the x-coordinate for points in $\mathbf{Q}_p$ for the remaining primes.

p	x	p	x
2	1	89	-1
13	8/5	113	3
19	-3	137	-1
23	2	7229	0
43	17	∞	1
47	-5		
71	5		

To show that C has no global rational point, argue as follows. From the known generator $(\frac{1}{4}, \frac{3}{4})$ of (18), it follows that

$$x \equiv 1,\ -7 \bmod \mathbf{Q}^{*2}.$$

(Alternatively, one can write $x=\delta u^2/w^2$, $u, w\in\mathbf{Z}$, $(u, w)=1$, δ squarefree, so that from (18),

$$4\delta u^4 + 36u^2w^2 - \frac{7}{\delta}w^4 = \square.$$

Then necessarily $\delta \mid 7$, and simple congruence arguments imply $\delta=1$, -7 only.)

In the case $x\equiv 1$, then $x=u^2/w^2$, $u, w\in\mathbf{Z}$, $(u, w)=1$, and, say

$$(u^2+2w^2)(u^4+14u^2w^2-3w^4)=R^2 \tag{19}$$

$$(2u^2+w^2)(-3u^4+14u^2w^2+w^4)=S^2 \tag{20}$$

$$4u^4+36u^2w^2-7w^4=T^2. \tag{21}$$

Hence, from (19), (20)

$$\begin{aligned} u^2+2w^2 &= a^2 & &\text{or} & u^2+2w^2 &= 3a^2 \\ u^4+14u^2w^2-3w^4 &= b^2 & & & u^4+14u^2w^2-3w^4 &= 3b^2 \end{aligned} \qquad (22, 22')$$

and

$$\begin{aligned} 2u^2+w^2 &= c^2 & &\text{or} & 2u^2+w^2 &= 3c^2 \\ -3u^4+14u^2w^2+w^4 &= d^2 & & & -3u^4+14u^2w^2+w^4 &= 3d^2. \end{aligned} \qquad (23, 23')$$

Now the pairs of Eqs. (22, 23), (22, 23′), (22′, 23) lead easily to $u \equiv w \equiv 0$ mod 3, impossible; so necessarily only (22′, 23′) can pertain. Then $u^2 = -a^2+2c^2$, $w^2 = 2a^2-c^2$, from which $ac \not\equiv 0$ mod 3. From (21),

$$-96a^4+192a^2c^2-63c^4=T^2,$$

giving $T \equiv 0$ (mod 3), $3a^2(a^2+c^2) \equiv 0$ mod 9, impossible.

In the case $x \equiv -7$ mod $\mathbf{Q}^{*2}$, then $x=-7u^2/w^2$, $u, w \in \mathbf{Z}$, $(u, w)=1$, and, say

$$(-7u^2+2w^2)(49u^4-98u^2w^2-3w^4)=R^2 \qquad (24)$$

$$(-14u^2+w^2)(-147u^4-98u^2w^2+w^4)=S^2 \qquad (25)$$

$$-28u^4+36u^2w^2+w^4=T^2. \qquad (26)$$

Now $7 \mid w$ from (26) gives $7 \mid u$, so $7 \nmid w$; from (24), (25) it follows that

$$-7u^2+2w^2=\lambda a^2, \qquad -14u^2+w^2=\mu c^2$$

with $\lambda, \mu = \pm 1, \pm 3$. If $3 \mid \lambda\mu$, then immediately $u \equiv w \equiv 0$ mod 3, impossible. Further, $(\lambda/7)=+1=(\mu/7)$, so $\lambda, \mu = 1$. But then

$$3w^2=2a^2-c^2,$$

forcing $a \equiv c \equiv 0$ mod 3, implying $w \equiv 0$ mod 3 and then $u \equiv 0$ mod 3, a contradiction. Consequently, the curve C satisfies criterion (iv).

Remark. C has the additional property that the three covering curves of genus 4, given by the intersections of (16), (17); (16), (18); and (17), (18) each possess a global rational point ($x=1$, $\frac{1}{4}$, 0, respectively).

REFERENCES

1. A. Bremner, Some special curves of genus 5, *Acta Arith.* **79** (1997), 41–51.
2. A. Bremner, D. J. Lewis, and P. Morton, Some varieties with points only in a field extension, *Arch. Math.* **43** (1984), 344–350.
3. J. W. S. Cassels and V. Flynn, "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2," London Math. Soc. Lecture Notes, Vol. 230, Cambridge Univ. Press, Cambridge, 1996.
4. T. Ekedahl and J.-P. Serre, Exemples de courbes algébriques à jacobienne complètement décomposable, *C.R. Acad. Sci. Paris Sér. I Math.* **317** (1993), 509–513.
5. H. Reichardt, Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen, *J. Reine Angew. Math.* **184** (1942), 12–18.
6. E. S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951), 203–362.