BELYĬ UNIFORMIZATION OF ELLIPTIC CURVES

D. SINGERMAN AND R. I. SYDDALL

ABSTRACT

Belyĭ's Theorem implies that a Riemann surface X represents a curve defined over a number field if and only if it can be expressed as $\mathbf{U}/\Gamma$, where $\mathbf{U}$ is simply-connected and Γ is a subgroup of finite index in a triangle group. We consider the case when X has genus 1, and ask for which curves and number fields Γ can be chosen to be a lattice. As an application, we give examples of Galois actions on Grothendieck dessins.

Introduction

We begin by stating Belyĭ's Theorem [**2**, **8**].

A compact Riemann surface X is isomorphic to the Riemann surface of a non-singular algebraic curve defined over a number field if and only if there is a non-constant meromorphic function $\beta\colon X \to P_1(\mathbf{C})$ ramified over at most 3 points.

For short we shall call such a Riemann surface a *Belyĭ surface*. Wolfart [**12**] (or see [**8**]) gave the following alternative description of a Belyĭ surface.

X is a Belyĭ surface if and only if $X = \mathbf{U}/\Gamma$, where $\mathbf{U}$ is a simply-connected Riemann surface and Γ is a subgroup of finite index in a triangle group.

Here $\mathbf{U}$ is isomorphic to $P_1(\mathbf{C})$, the Riemann sphere, $\mathbf{C}$, the complex plane, or $\mathbf{H}$, the upper half-plane. These spaces carry a spherical, Euclidean or hyperbolic metric, respectively, and the triangle group is the orientation-preserving subgroup of the group generated by reflections in the sides of a triangle whose angles are $\pi/l, \pi/m$, π/n, where l, m, n are integers and $1/l+1/m+1/n$ is greater than, equal to, or less than 1 in the spherical, Euclidean or hyperbolic cases, respectively. We denote this triangle group by $\Delta(l, m, n)$.

The Classical Uniformization Theorem tells us that every Riemann surface is isomorphic to a Riemann surface of the form $\mathbf{U}/K$, where K is a discontinuous group acting freely on $\mathbf{U}$. We shall define a *Belyĭ uniformization* of X as a representation of X in the form $\mathbf{U}/\Gamma$, where Γ is a subgroup of a triangle group. Thus a compact Riemann surface admits a Belyĭ uniformization if and only if it is defined over a number field. Now Belyĭ's Theorem does not require Γ to act freely. However, it is an interesting problem to determine when this is the case; that is, when is a Belyĭ uniformization the same as a classical uniformization? In this note we shall solve this problem completely for elliptic curves defined over $\mathbf{Q}$, and quadratic and cubic extensions of $\mathbf{Q}$. In the final section we give an application to Grothendieck dessins.

Received 14 March 1996; revised 1 August 1996.

1991 *Mathematics Subject Classification* 30F10, 11G05.

Bull. London Math. Soc. 29 (1997) 443–451

An *elliptic curve over a field F* is a curve of genus 1 with coefficients in F, which contains at least one point with coordinates in F. In this paper all fields are subfields of the field $\mathbf{C}$ of complex numbers. Such a curve can be put in *Weierstrass normal form* $y^2 = 4x^3 - g_2 x - g_3$, where $g_2, g_3 \in F$. Furthermore, the Riemann surface X of such a curve is isomorphic to $\mathbf{C}/\Lambda$, where Λ is a *lattice*, that is, a group generated by two independent Euclidean translations $z \to z + \omega_1$ and $z \to z + \omega_2$. We let $\tau = \omega_2/\omega_1$, and order ω_1, ω_2 so that τ has positive imaginary part. Then $\tau \in \mathbf{H}$ is an invariant of the similarity class of the lattice Λ and hence of the Riemann surface X. In fact, a similar lattice, which we denote by Λ_τ, is generated by 1 and τ. A similar lattice is generated by 1 and τ' ($\tau' \in \mathbf{H}$), if and only if $\tau' = A(\tau)$, $A \in \mathrm{PSL}_2(\mathbf{Z})$, the modular group. The relationships between g_2, g_3 and the lattice Λ are well-known:

$$g_2 = 60 \sum_{\omega \in \Lambda}{}' \omega^{-4}, \quad g_3 = 140 \sum_{\omega \in \Lambda}{}' \omega^{-6},$$

where $\sum'$ denotes the sum over the non-zero lattice points of Λ.

It is then easy to see that the following expression, known as Klein's modular invariant, depends only on the similarity class of the lattice and hence only on τ:

$$j(\tau) = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2}.$$

In fact, $j(\tau_1) = j(\tau_2)$ if and only if the corresponding lattices are similar, and hence if and only if the corresponding Riemann surfaces are isomorphic. In particular, $j(A(\tau)) = j(\tau)$, for all $A \in \mathrm{PSL}_2(\mathbf{Z})$. Furthermore, if $j(\tau)$ lies in a field F, then we can find g_2, g_3 lying in F satisfying the above equation for $j(\tau)$, and thus obtain an equation for the curve. For all this, see any book on elliptic curves, for example [**10**].

Euclidean Belyĭ uniformizations of rational elliptic curves

DEFINITION. A Riemann surface X of genus 1 has a *Euclidean Belyĭ uniformization* if and only if $X = \mathbf{C}/\Lambda$, where Λ is a subgroup of a Euclidean triangle group.

Thus we are searching for those X defining rational elliptic curves which admit Euclidean Belyĭ uniformizations. All Euclidean triangle groups are conjugate to $\Delta(2,4,4)$, $\Delta(3,3,3)$ or $\Delta(2,3,6)$ in the isometry group of $\mathbf{C}$. As $\Delta(3,3,3) < \Delta(2,3,6)$, it follows that Λ is a subgroup of a Euclidean triangle group if and only if it is a subgroup of $\Delta(2,4,4)$ or $\Delta(2,3,6)$.

LEMMA 1. *$\Delta(2,4,4)$ contains a lattice similar to Λ_τ if and only if $\tau \in \mathbf{Q}(i)$; $\Delta(2,3,6)$ contains a lattice similar to Λ_τ if and only if $\tau \in \mathbf{Q}(\rho)$, where $\rho = \frac{1}{2}(-1 + \sqrt{(-3)})$.*

Proof. (Compare [**7**, §7].) We can consider $\Delta(2,4,4)$ to be the group $\langle R, S, T \mid R^2 = S^4 = T^4 = RST = 1 \rangle$, where $R: z \to -z + 1$ and $S: z \to iz$. In this representation, $\Delta(2,4,4)$ just consists of all transformations of the form $z \to az + b$, where $a = \pm 1, \pm i$ and $b \in \mathbf{Z}[i]$. Thus the Gaussian integer lattice Λ_i is the normal subgroup of index 4 consisting of the transformations with $a = 1$, and every other torsion-free subgroup is a subgroup of Λ_i. Thus every lattice that is a subgroup of $\Delta(2,4,4)$ is generated by two Gaussian integers, and hence is similar to some Λ_τ, where τ is the quotient of two Gaussian integers and hence lies in $\mathbf{Q}(i)$. Conversely, every such Λ_τ is similar to a

sublattice of Λ_i and hence lies in $\Delta(2,4,4)$. The proof for $\Delta(2,3,6)$ is similar; this group is $\langle R,S,T \mid R^2=S^3=T^6=RST=1\rangle$, with $R: z\to -z+1$ and $S: z\to \rho z-1$. In this representation, $\Delta(2,3,6)$ just consists of all transformations $z\to az+b$, where $a=\pm 1, \pm\rho, \pm\rho^2$ and $b\in \mathbf{Z}[\rho]$. Thus $\Delta(2,3,6)$ contains Λ_ρ as a subgroup of index 6, and every other torsion-free subgroup of $\Delta(2,3,6)$ lies in Λ_ρ, and the proof proceeds as before.

Let τ be a quadratic imaginary number, and suppose that τ is a root of a quadratic equation $a\tau^2+b\tau+c=0$, where a,b,c are integers, $a>0$, $(a,b,c)=1$ and $d=b^2-4ac<0$. The values of $j(\tau)$ are known as singular moduli and have been intensively studied in the theory of complex multiplication; for example, see [**3**, **4**, **5**]. In particular, it is known that $j(\tau)$ is an algebraic integer of degree $h(d)$, where $h(d)$ is the class number of primitive binary quadratic forms of discriminant d. More precisely, the minimum polynomial of $j(\tau)$ over $\mathbf{Z}$ is the equation

$$\prod (X-j(\alpha))=0, \tag{1}$$

where α runs over the quadratic imaginary numbers of discriminant d that lie in the modular region (see [**4**, p. 377]).

We are interested in rational elliptic curves. These are precisely the curves with rational j-invariants. Then $j(\tau)$ is rational, and hence $h(d)=1$. By the well-known solution to the class-number one problem [**4**, **5**], the only $d<0$ for which $h(d)=1$ are $d=-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163$. By Lemma 1, τ is in $\mathbf{Q}(i)$ or $\mathbf{Q}(\rho)$. If $\tau\in\mathbf{Q}(i)$, then $\sqrt{(-d)}$ is an integer, and as $-d=4ac-b^2\equiv 0,3 \bmod 4$, we must have $d=-4m^2$; similarly, if $\tau\in\mathbf{Q}(\rho)$, then $d=-3m^2$. This gives $d=-3,-4,-12,-16,-27$. It is then easy to find the corresponding values of τ. For example, let $d=-16$; then $\tau=(-b+4i)/2a$ and $b^2-4ac=-16$. One solution is $b=0$, $a=1$, $c=4$, giving $\tau=2i$. Other solutions come from the points in the orbit of $2i$ under the modular group. But as $h(d)=1$, these are the only solutions. In other words, all quadratic forms of discriminant -16 are equivalent to x^2+4y^2. From [**5**] we can find the corresponding values of j, and we display the results in Table 1. (In general, if $h(d)=k$, we obtain k values of τ in the modular region.)

TABLE 1

d	τ	$j(\tau)$
-3	ρ	0
-4	i	1728
-12	$1+2\rho$	54000
-16	$2i$	287496
-27	$2+3\rho$	-12288000

As a consequence, we have the following result.

THEOREM 1. *There are* 5 *rational elliptic curves that admit a Euclidean Belyĭ uniformization. Their j-invariants are* 0, 1728, 54000, 287496 *and* -12288000. *Every other rational elliptic curve is* (*by Belyĭ's Theorem*) *of the form* $\mathbf{H}/\Gamma$, *where* Γ *is a subgroup of a hyperbolic triangle group.*

Note that the subgroup Γ, being a genus 1 hyperbolic group, must have torsion.

On elliptic curves defined over quadratic and cubic extensions of **Q**

Theorem 1 was obtained by finding all solutions to $h(-3m^2)=1$ or $h(-4m^2)=1$. To find elliptic curves defined over extension fields of degree k over **Q**, we need to find those d for which $h(d)=k$. In general, this is an unsolved problem, but when $d=-3m^2$ or $-4m^2$, we can find d using the following formulae, which can be obtained from the class-number formula given, for example, in [**5**, p. 148].

$$h(-3m^2)=\begin{cases}1 & m=1,\\ \dfrac{m}{3}\displaystyle\prod_{p\mid m}\left(1-\left(\frac{-3}{p}\right)\frac{1}{p}\right) & m>1,\end{cases}$$

$$h(-4m^2)=\begin{cases}1 & m=1,\\ \dfrac{m}{2}\displaystyle\prod_{p\mid m}\left(1-\left(\frac{-4}{p}\right)\frac{1}{p}\right) & m>1,\end{cases}$$

where $(\frac{-v}{p})$ $(v=3,4)$ is the Legendre symbol if p is an odd prime and the Kronecker symbol if $p=2$, so that $(\frac{-4}{2})=0$, $(\frac{-3}{2})=-1$. Observing that $3h(-3m^2)$ and $2h(-4m^2)$ are multiplicative functions, it is a simple matter, given a small positive integer k, to find all the values of m such that $h(-3m^2)=k$ or $h(-4m^2)=k$. In particular, when $k=1$ we obtain the results of Theorem 1. (For some values of k there are no solutions m; for example, when k is an odd number which is not a power of 3.) In general, this method allows us to find all the lattices Λ_τ, for $\tau\in\mathbf{Q}(i)$ or $\tau\in\mathbf{Q}(\rho)$, where $j(\tau)$ is an algebraic integer of degree k. These j-values and their associated elliptic curves cannot always be computed, but using the work of Berwick [**3**], we can find them when $k=2$ and $k=3$. When $k=2$, the only solutions of $h(-4m^2)=2$ are $m=3,4,5$, giving $d=-36,-64,-100$, and the only solutions of $h(-3m^2)=2$ are $m=4,5,7$, giving $d=-48,-75,-147$. Using [**3**], we obtain the results in Table 2.

TABLE 2

d	τ_1	τ_2	$j(\tau_1), j(\tau_2)$*	Field
-36	$3i$	$\dfrac{-1+3i}{2}$	$76\,771\,008\pm 44\,330\,496\sqrt{3}$	$\mathbf{Q}(\sqrt{3})$
-48	$2+4\rho$	$\dfrac{2+4\rho}{3}$	$1\,417\,905\,000\pm 818\,626\,500\sqrt{3}$	$\mathbf{Q}(\sqrt{3})$
-64	$4i$	$\dfrac{-1+2i}{2}$	$41\,113\,158\,120\pm 29\,071\,392\,966\sqrt{2}$	$\mathbf{Q}(\sqrt{2})$
-75	$\dfrac{1+5\rho}{3}$	$2+5\rho$	$-327\,201\,914\,880\pm 146\,329\,141\,248\sqrt{5}$	$\mathbf{Q}(\sqrt{5})$
-100	$5i$	$\dfrac{-1+5i}{2}$	$22\,015\,749\,613\,248\pm 9\,845\,745\,509\,376\sqrt{5}$	$\mathbf{Q}(\sqrt{5})$
-147	$\dfrac{2+7\rho}{3}$	$3+7\rho$	$-17\,424\,252\,776\,448\,000\pm 3\,802\,283\,679\,744\,000\sqrt{(21)}$	$\mathbf{Q}(\sqrt{(21)})$

*$j(\tau_1)$ with positive sign

As a consequence we have the following result.

THEOREM 2. *There are* 12 *elliptic curves defined over* $\mathbf{Q}(\sqrt{m})$ (*m a square-free integer*) *that admit a Euclidean Belyĭ uniformization. Their j-invariants are those listed in Table* 2. *Every other elliptic curve defined over a quadratic extension of* $\mathbf{Q}$ *is of the form* $\mathbf{H}/\Gamma$, *where* Γ *is a subgroup of a hyperbolic triangle group. In particular, this is the case for elliptic curves defined over* $\mathbf{Q}(\sqrt{m})$ *for* $m \neq 2, 3, 5, 21$.

Similarly, the only solutions of $h(-3m^2) = 3$ are $m = 6, 9$, giving $d = -108$, $d = -243$, while there are no solutions of $h(-4m^2) = 3$. Given the values of d, we can find the values of τ by the method given just before Table 1. From [**3**, pp. 62–63], we can find the corresponding fields and the j-values. As the j-values are rather complicated, we omit them, and set out the other results in Table 3.

TABLE 3

d	τ_1	Field	τ_2	Field	τ_3	Field
-108	$3+6\rho$	$\mathbf{Q}(2^{1/3})$	$\frac{1+3\rho}{2}$	$\mathbf{Q}(2^{1/3}\rho)$	$\frac{2+3\rho}{2}$	$\mathbf{Q}(2^{1/3}\rho^2)$
-243	$4+9\rho$	$\mathbf{Q}(3^{1/3})$	$\frac{6+9\rho}{7}$	$\mathbf{Q}(3^{1/3}\rho)$	$\frac{3+9\rho}{7}$	$\mathbf{Q}(3^{1/3}\rho^2)$

THEOREM 3. *There are* 6 *elliptic curves defined over cubic extensions* $\mathbf{Q}(\theta)$ *of* $\mathbf{Q}$ *that admit a Euclidean Belyĭ uniformization. These are defined over* $\mathbf{Q}(\theta)$, *where* $\theta^3 = 2$ *or* $\theta^3 = 3$. *Every other elliptic curve defined over a cubic extension of* $\mathbf{Q}$ *is of the form* $\mathbf{H}/\Gamma$, *where* Γ *is a subgroup of a hyperbolic triangle group.*

More generally, the total number of elliptic curves defined over extension fields of degree k over $\mathbf{Q}$ that admit a Euclidean Belyĭ uniformization is given by $kf(k)$, where $f(k)$ is the number of solutions to $h(-3m^2) = k$ or $h(-4m^2) = k$. (As previously noted, $f(k)$ may be zero.) However, when $k > 3$, we cannot easily find the j-invariants and hence the equations of the curves.

Uniform dessins on the torus

We can associate to a subgroup M of a triangle group, a map or dessin on the Riemann surface $\mathbf{U}/M$ [**7**]. (We are dealing here only with the so-called *clean dessins*, the ones that come from triangle groups containing a period 2 [**11**, p. 5].) This is particularly simple in our case, where the subgroup is a lattice Λ in one of the Euclidean triangle groups; for example, if the triangle group is $\Delta(2, 4, 4)$, then the dessin is the image under the natural projection from $\mathbf{C}$ to $\mathbf{C}/\Lambda$ of the Gaussian integer lattice on the torus. The dessins we obtain are examples of *uniform dessins* of type $(4, 4)$, that is, each vertex has the same valency (in this case equal to 4), and each face has the same number of edges (in this case 4 as well). Similarly, lattices in $\Delta(2, 3, 6)$ give uniform dessins of type $(3, 6)$ or $(6, 3)$. By Lemma 1 we see that we can represent each uniform dessin of type $(4, 4)$ by an orbit under the modular group of a point $\tau \in \mathbf{Q}(i)$ lying in $\mathbf{H}$, and a uniform dessin of type $(6, 3)$ by an orbit of a point $\tau \in \mathbf{Q}(\rho)$. For example, the point $\tau = (a+ib)/(c+id)$ represents the lattice Λ_τ generated by $a+ib$ and $c+id$. This lattice has a fundamental parallelogram of area $\mu = |ad-bc|$,

and so gives a subgroup of index μ in $\mathbf{Z}[i]$. We also say that the *dessin has index* μ. If $\alpha = p+iq \in \mathbf{Z}[i]$, then the lattice generated by $\alpha(a+ib)$ and $\alpha(c+id)$ has index $(p^2+q^2)\mu$ in $\mathbf{Z}[i]$ and is also represented by τ. Thus τ represents a unique *minimal dessin* (corresponding to a maximal lattice) in the case where $a+ib$ and $c+id$ are coprime Gaussian integers. (We can multiply both by i, but this gives an isomorphic dessin.)

Grothendieck [**6**, **11**] observed that Belyĭ's Theorem enables us to associate a dessin with an algebraic curve defined over a number field, and hence an action of the universal Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the set of all dessins. It has been shown by Jones and Streit [**9**] that most of the combinatorial properties of the dessin, such as numbers of edges, vertices and faces, genus, vertex and face valencies, are preserved by this action. If, for example, we are considering uniform dessins of type $(4,4)$ on the torus, then the vertex and face valencies as well as the genus are already determined, while the numbers of vertices, edges and faces are determined by the index of the dessin (if μ is this index, then there are 2μ edges, μ vertices and μ faces [**7**]). So in this case the Jones–Streit Theorem tells us that if two genus 1 uniform dessins of type $(4,4)$ are in the same $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ orbit, then their indices are equal (of course, the converse of this statement is not true). The elliptic curves that we have been considering give us particularly simple examples of the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

EXAMPLE 1. Consider the two elliptic curves in Table 2 that have discriminant -100. Their j-values and hence elliptic curves are conjugate in the field $\mathbf{Q}(\sqrt{5})$. The elliptic curve with the j-value with a positive sign corresponds to the point $5i$. The corresponding maximal lattice has index 5 in $\mathbf{Z}[i]$, giving the rectangular minimal dessin of index 5 with 10 edges shown in Figure 1. The Galois action then takes this elliptic curve to the curve with the corresponding j-value with a negative sign. This value is $j((-1+5i)/2)$, and as j is injective on modular group orbits, the corresponding dessin is one of those based at $(-1+5i)/2$. In reduced form,

$$\frac{-1+5i}{2} = \frac{-3+2i}{1+i},$$

which shows that there is a unique minimal dessin of index 5 based at this point. (This is illustrated in Figure 2.) So even though there are infinitely many dessins based at $(-1+5i)/2$, the index invariant discussed above shows that it is only the dessin of Figure 2 that lies in the same Galois orbit as the dessin in Figure 1.

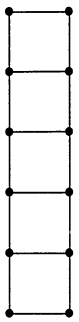

Fig. 1

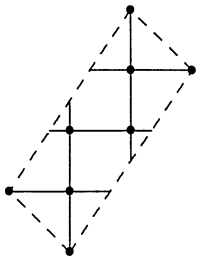

Fig. 2

A Galois orbit, $d = -100$

Similarly to the case $\mathbf{Z}[i]$, we find that the point $\tau = (a+b\rho)/(c+d\rho)$ represents a maximal lattice generated by $a+b\rho$ and $c+d\rho$ if they are coprime in $\mathbf{Z}[\rho]$, giving a minimal dessin of index $\mu = |ad-bc|$.

EXAMPLE 2. Consider the 3 elliptic curves in Table 3 that have discriminant -243. The maximal lattice corresponding to τ_1 has index 9 in $\mathbf{Z}[\rho]$, giving the minimal dessin with 27 edges illustrated in Figure 3. The Galois orbit of τ_1 consists of the points τ_1, τ_2, τ_3. Now 7 is not a prime in $\mathbf{Z}[\rho]$, as $7 = (2+3\rho)(-1-3\rho)$, so in reduced form we find that $\tau_2 = (-3)/(1+3\rho)$ and $\tau_3 = (-3)/(2+3\rho)$, which (as expected by the Jones–Streit Theorem) also give minimal dessins of index 9. The 3 minimal dessins of index 9 corresponding to τ_1, τ_2, τ_3 that are illustrated in Figures 3, 4, 5, respectively, form a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ orbit.

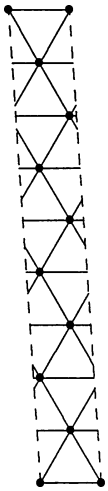

Fig. 3

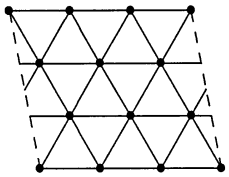

Fig. 4

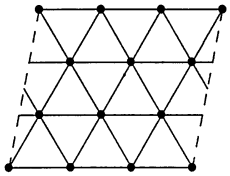

Fig. 5

A Galois orbit, $d = -243$

These examples can be generalized as follows. Let E_τ denote the elliptic curve with modulus τ. If $\tau \in \mathbf{Q}(i)$, we can write $\tau = (a+bi)/(c+di)$, where $a+bi$ and $c+di$ are coprime Gaussian integers. On E_τ we can construct, as above, the minimal dessin M_τ of type $(4,4)$ of index $\mu = |ad-bc|$. Now τ satisfies the quadratic equation

$$(c^2+d^2)\,x^2 - 2(ac+bd)\,x + (a^2+b^2) = 0, \tag{2}$$

and as $a+ib$ and $c+id$ are coprime Gaussian integers, it can be shown that the coefficients of (2) are coprime rational integers. A direct calculation now gives the discriminant of τ to be $-4(ad-bc)^2 = -4\mu^2$. Every other uniform dessin lying on E_τ will have an index strictly greater than μ. Similarly, it can be proved that every $\tau \in \mathbf{Q}(\rho)$ corresponds to a unique minimal uniform dessin M_τ with associated index μ, where τ has discriminant $-3\mu^2$.

We now fix a discriminant $d = -4\mu^2$. Let $\tau_1, \ldots, \tau_s$ be the $s = h(d)$ quadratic imaginary numbers lying in the modular region and having discriminant d (we note that $\tau_k \in \mathbf{Q}(i)$ for $1 \leqslant k \leqslant s$). The j-values $j(\tau_1), \ldots, j(\tau_s)$, being the roots of the irreducible polynomial (1), form an orbit under $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, and hence so do the

elliptic curves $E_{\tau_1}, \dots, E_{\tau_s}$. The elliptic curve $E_{\tau_k} (1 \leqslant k \leqslant s)$ carries the unique minimal dessin M_{τ_k} of index μ as defined above, with every other uniform dessin on E_{τ_k} having an index strictly greater than μ. The index of these dessins is invariant under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ (by the result of Jones and Streit mentioned above), and hence the minimal dessins $M_{\tau_1}, \dots, M_{\tau_s}$ form an orbit under $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Conversely, if M_τ and $M_{\tau'}$ $(\tau, \tau' \in \mathbf{Q}(i))$ are in the same Galois orbit, then they have the same index and hence the same discriminant. Thus we have proved the following.

THEOREM 4. *Let $M_\tau, M_{\tau'}$ $(\tau, \tau' \in \mathbf{Q}(i))$ be two minimal dessins as defined above. Then $M_\tau, M_{\tau'}$ are in the same orbit under* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *if and only if τ and τ' have the same discriminant.*

Similarly, by considering discriminants of the form $-3\mu^2$, one obtains a corresponding theorem about the orbits of minimal dessins of type $(6, 3)$ under $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

It can be seen that the dessins in Figures 4 and 5 are mirror images of each other, and the dessin in Figure 3 is symmetric under reflection in the imaginary axis, which passes through the bottom left-hand vertex and the mid-point of the top edge of the parallelogram. This is a general phenomenon; the discriminant of $a\tau^2 + b\tau + c$ is left unchanged by passing from b to $-b$, and then $\tau = (-b + \sqrt{d})/2a$ is transformed to $-\bar{\tau}$. If $h(d)$ is odd, then there must be some dessins that are fixed by this transformation. The corresponding τ must lie on the boundary of the modular region or on the imaginary axis. The corresponding elliptic curve must be real [**1**]. In fact, for all discriminants d we must obtain some points in every $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ orbit that lie on the boundary of the modular figure corresponding to some real elliptic curve. These points are associated to the *principal forms of discriminant d* [**5**, p. 34] which give equations as follows: if $d < 0$ is divisible by 4, we consider the equation $\tau^2 - d/4 = 0$, and if $d \equiv 1 \bmod 4$, we consider the equation $\tau^2 + \tau + (1-d)/4 = 0$. The solutions to these equations give values of τ in the modular region, the solutions to the former equation lying on the imaginary axis, and of the latter equation lying on the line $x = -\frac{1}{2}$. Thus for $h(d)$ even there must be at least two such values, as illustrated in Table 2.

We thank Professor J. Wolfart, Dr G. A. Jones and Dr M. Streit for their helpful advice.

References

1. N. ALLING, *Real elliptic curves* (North-Holland, Amsterdam, 1981).
2. G. V. BELYĬ, 'On Galois extensions of a maximal cyclotomic field', *Izv. Akad. Nauk SSSR* 43 (1979) 269–276 (Russian); *Math. USSR Izv.* 14 (1980) 247–256 (English translation).
3. W. E. H. BERWICK, 'Modular invariants expressible in terms of quadratic and cubic irrationalities', *Proc. London Math. Soc.* 28 (1927) 53–69.
4. H. COHEN, *A course in computational algebraic number theory* (Springer, New York, 1995).
5. D. A. COX, *Primes of the form $x^2 + ny^2$* (John Wiley, New York, 1989).
6. A. GROTHENDIECK, 'Esquisse d'un programme', Preprint, Montpellier, 1984.
7. G. A. JONES and D. SINGERMAN, 'Theory of maps on orientable surfaces', *Proc. London Math. Soc.* (3) 37 (1978) 273–307.
8. G. A. JONES and D. SINGERMAN, 'Belyĭ functions, hypermaps and Galois groups', *Bull. London Math. Soc.* 28 (1996) 561–590.
9. G. A. JONES and M. STREIT, 'Galois groups, monodromy groups and Grothendieck dessins', Preprint, Southampton, 1994.
10. A. W. KNAPP, *Elliptic curves* (Princeton University Press, 1992).

11. L. SCHNEPS (ed.), *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser. 200 (Cambridge University Press, 1994).
12. J. WOLFART, 'Mirror-invariant triangulations of Riemann surfaces, triangle groups and Grothendieck dessins: variations on a thema of Belyĭ', Preprint, Frankfurt, 1992.

Department of Mathematics
University of Southampton
Southampton SO17 1BJ