COMPOSITIO MATHEMATICA

KUANG-YEN SHIH

P-division points on certain elliptic curves

Compositio Mathematica, tome 36, nº 2 (1978), p. 113-129

<http://www.numdam.org/item?id=CM_1978__36_2_113_0>

COMPOSITIO MATHEMATICA, Vol. 36, Fasc. 2, 1978, pag. 113–129
Sijthoff & Noordhoff International Publishers–Alphen aan den Rijn
Printed in the Netherlands

P-DIVISION POINTS ON CERTAIN ELLIPTIC CURVES

Kuang-yen Shih*

1. Introduction

Let p be an odd prime, $\epsilon = (-1)^{(p-1)/2}$, and $k = \mathbf{Q}(\sqrt{\epsilon p})$. Consider an elliptic curve E defined over k. Adjoin to k the x-coordinates of the points of order p on E and denote the resulting field by $F_p(E)$, or simply F_p. It is known (see [7, 6.1]) that F_p is a Galois extension of k and $\mathrm{Gal}(F_p/k)$ can be identified with a subgroup of $GL_2^*(\mathbf{Z}/p\mathbf{Z})/\{\pm 1_2\}$, where

$$GL_2^*(\mathbf{Z}/p\mathbf{Z}) = \{\alpha \in GL_2(\mathbf{Z}/p\mathbf{Z}) \,|\, \det \alpha \text{ is a square}\}.$$

Note that if $\mathrm{Gal}(F_p/k)$ is the whole $GL_2^*(\mathbf{Z}/p\mathbf{Z})/\{\pm 1_2\}$, then F_p contains a subfield F normal over the quadratic field k such that $\mathrm{Gal}(F/k)$ is isomorphic to $PSL_2(\mathbf{Z}/p\mathbf{Z})$. One purpose of this paper is to discuss some conditions on E under which $F_p(E)$ contains a subfield K normal over the rational number field $\mathbf{Q}$ so that $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to $PSL_2(\mathbf{Z}/p\mathbf{Z})$.

Denote the non-trivial automorphism of k by σ. Suppose there are a quadratic non-residue N modulo p, and an N-cyclic isogeny λ of E to its conjugate E^σ such that

(1.1) $\qquad C = \ker \lambda$ *is rational over* k, *and*

(1.2) $$\lambda(E(N)) = C^\sigma.$$

Here $E(N)$ stands for the group of N-division points on E. The existence of such λ implies that F_p is not only normal over k, but also over $\mathbf{Q}$. This will be proved in §2. We also determine the Galois group $\mathrm{Gal}(F_p/\mathbf{Q})$. We show in particular that $\mathrm{Gal}(F_p/\mathbf{Q})$ is a group extension of $PSL_2(\mathbf{Z}/p\mathbf{Z})$ if

(1.3) $$\mathrm{Gal}(F_p/k) \cong GL_2^*(\mathbf{Z}/p\mathbf{Z})/\{\pm 1_2\}.$$

Using the theory of arithmetic automorphic functions, we constructed in [5] Galois extensions over $\mathbf{Q}$ with $PSL_2(\mathbf{Z}/p\mathbf{Z})$ as Galois groups for a certain family of primes p. In §3, we show that the above result serves as a modular interpretation of this construction. We work out some numerical examples in §4.

Careful consideration of the generic case enables us to write down general equations with Galois group $PSL_2(\mathbf{Z}/p\mathbf{Z})$ for small p's. In §5, we carry this out for $p = 5$, 7, 11 and 13 in the fashion of Fricke [2].

2. The Galois group $\mathrm{Gal}(F(p^n)/\mathbf{Q})$

Let E be an elliptic curve defined over $k = \mathbf{Q}(\sqrt{\epsilon p})$ and λ an N-isogeny of E to E^σ satisfying conditions (1.1) and (1.2). We further assume that $\mathrm{Aut}(E) = \{\pm\mathrm{id.}\}$. Take a non-zero holomorphic differential ω on E rational over k. Then

$$\omega^\sigma \circ \lambda = s\omega \tag{2.1}$$

for some $s \in \mathbf{C}$. (See [8, §10] for similar discussion.) For $\tau \in \mathrm{Aut}(\mathbf{C}/k)$, $\lambda^\tau \colon E \to E^\sigma$ is an isogeny, and by (1.1), $\ker \lambda^\tau = C$. In view of the assumption $\mathrm{Aut}(E) = \{\pm\mathrm{id.}\}$, this shows $\lambda^\tau = \pm\lambda$. Hence $s^\tau = s$ or $-s$, depending on whether $\lambda^\tau = \lambda$ or $-\lambda$. It follows that λ is defined over $k(s)$, and $[k(s):k] = 1$ or 2.

Now let τ be an automorphism of $\mathbf{C}$ such that $\tau = \sigma$ on k. From (2.1) we have $\omega \circ \lambda^\tau = s^\tau \omega^\sigma$. Hence

$$\omega \circ (\lambda^\tau \circ \lambda) = s^\tau s\omega. \tag{2.2}$$

Observe that $\lambda^\tau \circ \lambda$ has $E(N) = \ker(N \cdot \mathrm{id.})$ as its kernel. In fact, by (1.2) we have

$$(\lambda^\tau \circ \lambda)(E(N)) = \lambda^\tau(C^\sigma) = \lambda(C)^\tau = 0.$$

Since the degree of $\lambda^\tau \circ \lambda$ is N^2, this proves our assertion. Therefore $\lambda^\tau \circ \lambda = \pm N \cdot \mathrm{id}$. By (2.2), we have

$$s^\tau s = \pm N. \tag{2.3}$$

From this we see that s does not belong to k, for otherwise (2.3) would imply that N is a quadratic residue modulo p. Therefore $[k(s):k] = 2$. Especially, λ is *not* defined over k.

Note that s has exactly four conjugates over $\mathbf{Q}$, namely, s, $-s$, N/s and $-N/s$. Hence $k(s)$ is normal over $\mathbf{Q}$ and $\mathrm{Gal}(k(s)/\mathbf{Q})$ is isomorphic to the Klein four-group. We use σ_1 (resp. σ_2) to denote the element of $\mathrm{Gal}(k(s)/\mathbf{Q})$ which sends s to $-s$ (resp. N/s). The restriction of σ_1 (resp. σ_2) to k is id. (resp. σ).

Let

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in k,$$

be an affine equation of E. Then the canonical function h on E is defined to be

$$h((x, y)) = (g_2g_3/\Delta) \cdot x, \quad \Delta = g_2^3 - 27g_3^2.$$

Let $E(p^n)$ be the group of p^n-division points on E. Then

$$F(p^n) = k(h(t) \mid t \in E(p^n)) \tag{2.4}$$

is a Galois extension of k. Fix $t_1, t_2 \in E(p^n)$ so that $E(p^n) = \mathbf{Z}t_1 + \mathbf{Z}t_2$. Then we can define an injective homomorphism ϕ of $\mathrm{Gal}(F(p^n)/k)$ into $GL_2(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$, as in [7, 6.1]. For $\tau \in \mathrm{Gal}(F(p^n)/k)$, $\phi(\tau)$ is represented by the integral matrix α such that

$$\begin{bmatrix} t_1^\tau \\ t_2^\tau \end{bmatrix} = \alpha \cdot \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}.$$

It is known that the field $F(p^n)$ contains the cyclotomic field $\mathbf{Q}(\zeta)$, $\zeta = \exp(2\pi i/p^n)$. If $\alpha \in M_2(\mathbf{Z})$ represents $\phi(t)$, $\tau \in \mathrm{Gal}(F(p^n)/k)$, then $\zeta^\tau = \zeta^{\det \alpha}$, see [7, prop. 6.3]. Since $\tau = \mathrm{id.}$ on $k = \mathbf{Q}(\sqrt{\epsilon p})$, we see that $\det \alpha$ is a quadratic residue modulo p^n. Therefore G, the image of ϕ, is contained in $GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$, where

$$GL_2^*(\mathbf{Z}/p^n\mathbf{Z}) = \{\alpha \in GL_2(\mathbf{Z}/p^n\mathbf{Z}) \mid \det \alpha \text{ is a square in } (\mathbf{Z}/p^n\mathbf{Z})^\times\}.$$

Let $E' = E^\sigma$, h' the canonical function on E', and

$$F'(p^n) = k(h'(t) \mid t \in E'(p^n)).$$

Obviously the composite $F(p^n)F'(p^n)$ is normal over $\mathbf{Q}$. We show that $F(p^n) = F'(p^n)$, so $F(p^n)$ is a Galois extension of $\mathbf{Q}$. Let τ be an automorphism of $\mathbf{C}$ which induces the identity map on $F(p^n)$. Then we have

$$\begin{bmatrix} t_1^\tau \\ t_2^\tau \end{bmatrix} = \pm \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}.$$

Put $t_1' = \lambda(t_1)$ and $t_2' = \lambda(t_2)$. Then $E'(p^n) = \mathbf{Z}t_1' + \mathbf{Z}t_2'$. As observed earlier, $\lambda^\tau = \lambda$ or $-\lambda$. Using this we see easily that

$$\begin{bmatrix} t_1'^\tau \\ t_2'^\tau \end{bmatrix} = \pm \begin{bmatrix} t_1' \\ t_2' \end{bmatrix}.$$

In other words, τ induces the identity map on $F'(p^n)$. So $F'(p^n)$ is a subfield of $F(p^n)$. Similarly, $F(p^n)$ is a subfield of $F'(p^n)$. Hence $F(p^n) = F'(p^n)$.

Thus $F(p^n)$ is a Galois extension of $\mathbf{Q}$. Identify $\mathrm{Gal}(F(p^n)/k)$ with the subgroup

$$A = \{\tau \in \mathrm{Gal}(F(p^n)/\mathbf{Q} \mid \tau = \text{id. on } k\}$$

of $\mathrm{Gal}(F(p^n)/\mathbf{Q})$, and denote the non-trivial coset of A by B. An element ρ of $\mathrm{Gal}(F(p^n)/\mathbf{Q})$ belongs to B if and only if $\rho = \sigma$ on k. Let $t_1, t_2 \in E(p^n)$ and $t_1', t_2' \in E'(p^n)$ be as above. Then for $\rho \in B$ we have

$$\begin{bmatrix} t_1^\rho \\ t_2^\rho \end{bmatrix} = \beta \cdot \begin{bmatrix} t_1' \\ t_2' \end{bmatrix}$$

for some $\beta \in M_2(\mathbf{Z})$.

PROPOSITION 1: *The determinant of β is a quadratic residue modulo p^n.*

PROOF: Let e (resp. e') be the Weil pairing [7, 4.3] on $E(p^n) \times E(p^n)$ (resp. $E'(p^n) \times E'(p^n)$). Then $\zeta = e(t_1, t_2)$ is a primitive p^n-th root of unity. We have

$$\begin{aligned} \zeta^\rho &= e(t_1, t_2)^\rho = e'(t_1', t_2')^{\det \beta} = e'(\lambda(t_1), \lambda(t_2))^{\det \beta} \\ &= e(t_1, t_2)^{N \cdot \det \beta} = \zeta^{N \cdot \det \beta}. \end{aligned}$$

Since $\rho = \sigma$ on k and N is a quadratic non-residue modulo p, we conclude that $\det \beta$ is a quadratic residue modulo p^n.

Let $\psi(\rho)$ be the element of $GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$ represented by β. Then ψ is a well-defined one-to-one map from B to $GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$. The image G' of ψ is a coset of G. (It can happen that $G' = G$.) Obviously we have

$$\begin{aligned} \phi(\tau\tau') &= \phi(\tau)\phi(\tau'), \\ \psi(\tau\rho) &= \phi(\tau)\psi(\rho), \\ \psi(\rho\tau) &= \psi(\rho)\phi(\tau), \end{aligned}$$

for $\tau, \tau' \in A$ and $\rho \in B$. And it is not hard to see that

$$\phi(\rho\rho') = N\psi(\rho)\psi(\rho')$$

for $\rho, \rho' \in \beta$, using the fact that $\lambda^{\delta} \circ \lambda = \pm N$, where δ is any automorphism of $\mathbf{C}$ extending ρ.

Let G_1 be the set consisting of all $(\mu, 1)$ with $\mu \in G$ and (μ', σ) with $\mu' \in G'$. Introduce a group structure on G_1 by employing the following multiplication table:

	$(\nu, 1)$	(ν', σ)
$(\mu, 1)$	$(\mu\nu, 1)$	$(\mu\nu', \sigma)$
(μ', σ)	$(\mu'\nu, \sigma)$	$(N\mu'\nu', 1)$

$(\mu, \nu \in G; \mu', \nu' \in G')$.

The above argument shows that $\mathrm{Gal}(F(p^n)/\mathbf{Q})$ is isomorphic to G_1.

Define a homomorphism χ of G_1 to $PSL_2(\mathbf{Z}/p^n\mathbf{Z})$ by

$$\chi((\mu, 1)) = (\det \mu)^{-1/2}\mu,$$

$$\chi((\mu', \sigma)) = (\det \mu')^{-1/2}\mu'.$$

Denote by D the subgroup of $GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$ consisting of elements represented by scalar matrices. Then the kernel of χ is

$$\ker \chi = \{(\mu, 1), (\mu', \sigma) \mid \mu \in G \cap D, \mu' \in G' \cap D\}.$$

Let K be the subfield of $F(p^n)$ corresponding to $\ker \chi$. By Galois theory, K is normal over $\mathbf{Q}$ and $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to the subgroup $\chi(G_1)$ of $PSL_2(\mathbf{Z}/p^n\mathbf{Z})$.

Now assume $G = GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$. Then $G' = G$ and $\chi(G_1) = PSL_2(\mathbf{Z}/p^n\mathbf{Z})$. Hence we have

THEOREM 2: *Let notation be as above. If* $\mathrm{Gal}(F(p^n)/k)$ *is isomorphic to the full* $GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$, *then* $F(p^n)$ *contains a subfield* K *normal over* $\mathbf{Q}$ *such that* $\mathrm{Gal}(K/\mathbf{Q})$ *is isomorphic to* $PSL_2(\mathbf{Z}/p^n\mathbf{Z})$.

3. The twisted modular curve $\tilde{X}_0(N)$

Let $H = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$ be the complex upper half plane. The group

$$GL_2^+(\mathbf{R}) = \{\alpha \in GL_2(\mathbf{R}) \mid \det \alpha > 0\}.$$

acts on H by fractional linear transformations. For a natural number M, let $\mathscr{F}_M$ be the field of modular functions of level M on H whose Fourier expansions with respect to $q_M = \exp(2\pi iz/M)$ have coefficients in the cyclotomic field $\mathbf{Q}(\zeta_M)$, $\zeta_M = \exp(2\pi i/M)$. Put $\mathscr{F} = \bigcup_{M=1}^{\infty} \mathscr{F}_M$.

Let $GL_2(\mathbf{A})$ be the adelization of GL_2 and $GL_2^+(\mathbf{A})$ the subgroup of $GL_2(\mathbf{A})$ consisting of elements whose components at infinity belong to $GL_2^+(\mathbf{R})$. The group $GL_2^+(\mathbf{A})$ acts on $\mathscr{F}$ as a group of automorphisms in the way described in [7, 6.6]. The image of $f \in \mathscr{F}$ under $x \in GL_2^+(\mathbf{A})$ will be denoted by f^x.

Denote by $\mathbf{Z}_\ell$ the ring of ℓ-adic integers. Put

$$U = \prod_\ell GL_2(\mathbf{Z}_\ell) \times GL_2^+(\mathbf{R}).$$

Then U is a locally compact open subgroup of $GL_2^+(\mathbf{A})$. For a natural number M, let U_M be the subgroup of U consisting of those $\alpha = (\alpha_\ell)$ such that $\alpha_\ell \equiv 1_2(\mathrm{mod}\ M \cdot M_2(\mathbf{Z}_\ell))$ for all finite ℓ. By [7, (6.6.3)], $\mathscr{F}_M$ is the subfield of $\mathscr{F}$ fixed by $S_M = \mathbf{Q}^\times \cdot U_M$. The field $\mathscr{F}_1$ is generated over $\mathbf{Q}$ by the modular invariant j.

Let N be a positive integer. Denote by ω_N the element of $GL_2^+(\mathbf{A})$ whose component at a rational prime dividing N is $\begin{bmatrix} 0 & 1/N \\ -1 & 0 \end{bmatrix}$, and at all other places the identity matrix 1_2. Note that ω_N can be decomposed as $x \cdot \alpha$, where $x \in U$ and $\alpha = \begin{bmatrix} 0 & 1/N \\ -1 & 0 \end{bmatrix} \in GL_2^+(\mathbf{Q})$. Therefore ω_N maps $\mathscr{F}_M$ into $\mathscr{F}_{MN}$. When $(M, N) = 1$, the Fourier coefficients of $f \in \mathscr{F}_M$ and $f^{\omega_N} \in \mathscr{F}_{MN}$ are related as follows.

PROPOSITION 3: *Suppose* $(M, N) = 1$. *Let*

$$f(z) = \sum_n a_n q_M^n, \quad a_n \in \mathbf{Q}(\zeta_M),$$

be the Fourier expansion of $f \in \mathscr{F}_M$. *Then*

$$f^{\omega_N}(z) = \sum_n a_n^\sigma q_M^{nN},$$

where σ *denotes the automorphism of* $\mathbf{Q}(\zeta_M)$ *that sends* ζ_M *to* ζ_M^N.

PROOF: Let

$$x_\ell = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & N \end{bmatrix} & \text{if } \ell \nmid N \text{ or } \ell = \infty, \\ & \text{if } \ell \mid N. \end{cases}$$

Then $x = (x_\ell) \in U$ and

$$\omega_N = x \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1/N \end{bmatrix}.$$

Hence it is sufficient to show

$$f^x(z) = \sum_n a_n^\sigma q_M^n. \tag{3.1}$$

For $a \in M^{-1}\mathbf{Z}^2$, $\notin \mathbf{Z}^2$, define f_a as in [7, 6.1]. Then the f_a's together with the modular invariant j generate $\mathcal{F}_M$ over $\mathbf{Q}$, see [7, prop. 6.9]. The Fourier coefficients of f_a's are known explicitly, and those of j are rational. For these generating functions, (3.1) can be verified in a straightforward way. Therefore (3.1) holds for all $f \in \mathcal{F}_M$. Q.E.D.

Now let j_M be the modular function of level M defined by $j_M(z) = j(Mz)$. The field $\mathcal{L}_M = \mathbf{Q}(j, j_M)$ is the fixed subfield of $T_M = \mathbf{Q}^x \cdot U'_M$, where

$$U'_M = \left\{ \alpha = (\alpha_\ell) \in U \mid \alpha_\ell \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} (\text{mod } M \cdot M_2(\mathbf{Z}_\ell)) \right\}.$$

If $(M, N) = 1$, then $\omega_N^{-1} T_{MN} \omega_N = T_{MN}$ and $\omega_N^2 \in T_{MN}$. Therefore, ω_N induces an involution on $\mathcal{L}_{MN}$. Actually, this is exactly the Atkin-Lehner involution w_N on $\mathcal{L}_{MN}$: $j \leftrightarrow j_N$, $j_M \leftrightarrow j_{MN}$. This follows from Proposition 3, or more directly, from the observation $\omega_N w_N^{-1} \in T_{MN}$.

PROPOSITION 4: *For every M relatively prime to N, ω_N induces the Atkin-Lehner involution w_N on $\mathbf{Q}(j, j_{MN})$.*

Now take $M = p^n$, and assume that N is a quadratic non-residue modulo p. Then ω_N induces the non-trivial automorphism σ on $k = \mathbf{Q}(\sqrt{\epsilon p})$. Let $\tilde{\mathcal{L}}_{MN}$ (resp. $\tilde{\mathcal{L}}_N$) be the subfield of $k\mathcal{L}_{MN}$ (resp. $k\mathcal{L}_N$) fixed by ω_N. Then $\mathbf{Q}$ is algebraically closed in $\tilde{\mathcal{L}}_{MN}$ and in $\tilde{\mathcal{L}}_N$.

Let $X_0(N)$ (resp. $\tilde{X}_0(N)$) be a projective non-singular curve over $\mathbf{Q}$ whose function field over $\mathbf{Q}$ is isomorphic to $\mathscr{L}_N$ (resp. $\tilde{\mathscr{L}}_N$). Then both $X_0(N)$ and $\tilde{X}_0(N)$ are models of the quotient of H by the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

Let W_N be the involution of $X_0(N)$ induced by the involution $z \leftrightarrow -1/Nz$ of H. This W_N corresponds to the involution w_N on $\mathscr{L}_N$. Now $\tilde{\mathscr{L}}_N$ is the fixed subfield of $k\tilde{\mathscr{L}}_N = k\mathscr{L}_N$ under ω_N. Therefore, by a well-known fact (see [7, Appendix 6] for example), there is a birational biregular map ψ of $\tilde{X}_0(N)$ to $X_0(N)$ over k such that $\psi^\sigma \circ \psi^{-1} = W_N$. As before σ stands for the non-trivial automorphism of k. We have the following proposition, which is just a rephrasing of [5, Lemma 9].

PROPOSITION 5: *A point x of $\tilde{X}_0(N)$ is rational over $\mathbf{Q}$ if and only if $y = \psi(x) \in \tilde{X}_0(N)$ is rational over k and $y^\sigma = W_N(y)$.*

COROLLARY. *There is no $\mathbf{Q}$-rational cusps on $\tilde{X}_0(N)$.*

PROOF: Suppose $s \in \tilde{X}_0(N)$ is a $\mathbf{Q}$-rational cusp. Then by Proposition 5, $t = \psi(s)$ is rational over k. Since all cusps of $X_0(N)$ are rational over $\mathbf{Q}(\zeta_N)$, t is rational over $\mathbf{Q}$. However, we have $t^\sigma = W_N(t)$. Therefore $W_N(t) = t$, i.e. the cusp t of $X_0(N)$ is a fixed point of W_N. But this is not the case, see for example [3, prop. 3]. Q.E.D.

Now any non-cusp k-rational point y of $X_0(N)$ is represented by a pair (E, C) consisting of an elliptic curve E defined over k and a k-rational cyclic subgroup C of E of order N. If y is so represented, then $W_N(y)$ is represented by $(E/C, E(N)/C)$. Therefore, by Prop. 5 and its Corollary, any $\mathbf{Q}$-rational point of $\tilde{X}_0(N)$ is represented by a k-rational pair such that (E^σ, C^σ) is isomorphic to $(E/C, E(N)/C)$. For such (E, C), there is an isogeny λ of E to E^σ with kernel C such that $\lambda(E(N)) = C^\sigma$. Then λ satisfies (1.1) and (1.2). In the following, we shall call a pair (E, λ) rational over k and of type (N) if E is an elliptic curve over k and λ is an isogeny of E to E^σ with properties (1.1) and (1.2). We state the above observation as the first part of the following:

THEOREM 6: *Every $\mathbf{Q}$-rational point of $\tilde{X}_0(N)$ is represented by a k-rational pair (E, λ) of type (N). Conversely, every such pair represents a $\mathbf{Q}$-rational point of $\tilde{X}_0(N)$.*

The converse part of the theorem can be proved by reversing the above argument.

Let x be a $\mathbf{Q}$-rational point of $\tilde{X}_0(N)$ represented by (E, λ). Construct the algebraic number field $F(p^N)$ from E as in §2. Choose a point $z_0 \in H$ which is projected to x. Consider the Galois extension $\mathcal{F}_M\mathcal{L}_N$ $(M = p^n)$ of $k\mathcal{L}_N$. Under the specialization $f \mapsto f(z_0)$, $\mathcal{F}_M\mathcal{L}_N$ (resp. $\mathcal{L}_N$) is specialized to $F(p^n)$ (resp. k). Hence $\mathcal{F}_M\mathcal{L}_N/k\mathcal{L}_N$ is specialized to $F(p^n)/k$. Now

$$\text{Gal}(\mathcal{F}_M\mathcal{L}_N/k\mathcal{L}_N) \cong GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}. \tag{3.2}$$

Hence in view of Hilbert's irreducibility theorem, we have the following:

THEOREM 7: *Suppose $\tilde{X}_0(N)$ is a rational curve. Then there are infinitely many k-rational pairs (E, λ) of type (N) satisfying the condition* $\text{Gal}(F(p^n)/k) \cong GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$. *Here k denotes the quadratic field* $\mathbf{Q}(\sqrt{\epsilon p})$.

The situation under which $\tilde{X}_0(N)$ is a rational curve was given as table (4.4) in [5]. Especially, we know that $\tilde{X}_0(N)$ is rational when $N = 2, 3$ or 7. Combining this with Theorems 2 and 7, we obtained the main result of [5]: *If p is an odd prime such that* 2, 3, *or* 7 *is a quadratic non-residue modulo p, then $PSL_2(\mathbf{Z}/p^n\mathbf{Z})$, $n \geq 1$, can be realized as the Galois group of some Galois extension over* $\mathbf{Q}$. In the following section, we give some examples of pairs (E, λ) that generate such extensions.

REMARK 1. The Galois group $\text{Gal}(\mathcal{F}_M\mathcal{L}_N/\tilde{\mathcal{L}}_N)$ is isomorphic to G_1 of §2 with $G = GL_2^*(\mathbf{Z}/p^n\mathbf{Z})/\{\pm 1_2\}$. This can be justified as follows. Firstly, the subgroup $\text{Gal}(\mathcal{F}_M\mathcal{L}_N/k\mathcal{L}_N)$ is isomorphic to G, see (3.2). Secondly, the restriction δ of ω_N to $\mathcal{F}_M\mathcal{L}_N$ is in the center of $\text{Gal}(\mathcal{F}_M\mathcal{L}_N/\tilde{\mathcal{L}}_N)$. And thirdly, $\delta^2 = N \cdot 1_2$ under the identification (3.2). The extension $\mathcal{F}_M\mathcal{L}_N/\tilde{\mathcal{L}}_N$ is specialized to an extension of the form $F(p^n)/\mathbf{Q}$ when the functions in $\mathcal{F}_M\mathcal{L}_N$ are evaluated at a rational point of $\tilde{X}_0(N)$.

REMARK 2: We discuss briefly the case where the genus of $X_0(N)$ is 1. Under this condition, it is known [2] that $\mathcal{L}_N$ is generated over $\mathbf{Q}$ by two functions σ and τ with defining equation $\sigma^2 = f(\tau)$, where $f(x) \in \mathbf{Q}[x]$ is of degree 4. Furthermore, w_N fixes τ and changes the sign of σ. Therefore the twist $\tilde{\mathcal{L}}_N$ of $\mathcal{L}_N$ over $k = \mathbf{Q}(\sqrt{\epsilon p})$ is generated over $\mathbf{Q}$ by $x = \tau$ and $y = (\epsilon p)^{-1/2}\sigma$, with the defining equation $\epsilon p y^2 = f(x)$. So $\tilde{X}_0(N)$ is exactly the twisted curve of Birch investigated in [1]. As in [1], we see from the zeta-function of $\tilde{X}_0(N)$ that the Birch and Swinnerton-Dyer conjecture predicts that there are infinitely many rational points on $\tilde{X}_0(N)$ if $p \equiv 1 \pmod 4$. In other words, there should be infinitely many k-rational pairs (E, λ) of type (N) in view of Theorem 6. It would be interesting to know whether such pairs actually exist, and if exist, whether any of them satisfies (1.3).

4. Numerical examples

For each N such that $X_0(N)$ is a rational curve, $\mathcal{L}_N$ is generated by a *Hauptmodul* τ_N such that its image under w_N is c_N/τ_N for some rational integer c_N. Put

$$s = 2^{-1}(\tau_N + c_N/\tau_N) \quad \text{and} \quad t = (2\sqrt{\epsilon p})^{-1}(\tau_N - c_N/\tau_N).$$

Then $\tilde{\mathcal{L}}_N = \mathbf{Q}(s, t)$ and $s^2 - \epsilon p t^2 = c_N$. It follows that $\tilde{\mathcal{L}}_N$ is pure transcendental over $\mathbf{Q}$ if and only if c_N is the norm of some element from k. This gives another proof of [5, Prop. 11].

Suppose $\tilde{\mathcal{L}}_N$ is pure transcendental over $\mathbf{Q}$, and let $a, b \in \mathbf{Q}$ be such that $a^2 - \epsilon p b^2 = c_N$. Then

$$x_N = \sqrt{\epsilon p}(\tau_N + a - \sqrt{\epsilon p}b)/(\tau_N - a + \sqrt{\epsilon p}b) \tag{4.1}$$

generates $\tilde{\mathcal{L}}_N$ over $\mathbf{Q}$. Express $j \in \mathcal{L}_N = \mathbf{Q}(\tau_N)$ in terms of τ_N. Solving τ_N in terms of x_N from (4.1), we see that every rational value of x_N gives rise to a value of j in $k = \mathbf{Q}(\sqrt{\epsilon p})$. Let E be an elliptic curve defined over k with this value as its j-invariant. Then there is an isogeny λ such that (E, λ) is of type (N). Conversely, all pairs of type (N) are obtained this way. For a given (E, λ), we can check whether (1.3) is satisfied using the method of [4] and [6]. The following examples are obtained by this procedure.

1° $p = 5$, $N = 2$. Denote the fundamental unit $(1 + \sqrt{5})/2$ of $\mathbf{Q}(\sqrt{5})$ by u. Let

$$E\colon y^2 = 4x^3 - 3\sqrt{5}u^3x - u^2.$$

The discriminant of E is $\Delta = 3^3u^{14}$ and the j-invariant is

$$j_E = 2^6 3^3 5\sqrt{5}/u^5.$$

By [2, page 394], $j \in \mathcal{L}_2 = \mathbf{Q}(\tau_2)$ has the expression

$$j = j(\tau_2) = 2^6(\tau_2 + 4)^3/\tau_2^2.$$

Hence $j_E = j(\tau_2)$ with $\tau_2 = (3+\sqrt{5})/(3-\sqrt{5})$. This value of τ_2 corresponds to $x_2 = 3$. Therefore, there is an isogeny λ of E to E^σ such that (E, λ) is of type (2).

We show that the Galois group $G = \mathrm{Gal}(F(5)/\mathbf{Q}(\sqrt{5}))$ is the full $GL_2^*(\mathbf{Z}/5\mathbf{Z})/\{\pm 1_2\}$. Reduce E modulo the prime ideal $\mathfrak{l} = (6-\sqrt{5})$ of norm $n = 31$. Let A be the number of rational points on the reduced curve E modulo $\mathfrak{l}$ and $t = 1 + n - A$. Then we have $A = 34$, $t = -2$ and $t^2 - 4n = 5 \cdot (-24)$. In view of [6, Lemma 1], the order of G is divisible by 5. By [4, prop. 15], G either contains $PSL_2(\mathbf{Z}/5\mathbf{Z})$ or is contained in a Borel subgroup. The second possibility can be ruled out by looking at the curve E reduced modulo $\mathfrak{l} = (4+\sqrt{5})$. The norm of $\mathfrak{l}$ is $n = 11$, the number of rational points on the reduced curve is $A = 16$. Hence $t = 1 + n - A = -4$ and $t^2 - 4n = -28$. Since -28 is a quadratic non-residue modulo 5, G is not contained in a Borel subgroup. So G must contain $PSL_2(\mathbf{Z}/5\mathbf{Z})$. On the other hand F(5) contains $\mathbf{Q}(\zeta_5)$. Hence the image of G under the determinant map is the full subgroup of quadratic residues. This shows $G = GL_2^*(\mathbf{Z}/5\mathbf{Z})/\{\pm 1_2\}$.

2° $p = 5$, $N = 3$. Consider the curve

$$E\colon y^2 = 4x^3 - 3(5 - 4\sqrt{5})x - 7(3 - 2\sqrt{5})$$

defined over $\mathbf{Q}(\sqrt{5})$ with discriminant $-2^4 3^3 (1+\sqrt{5})^2$. The j-invariant of E is

$$j_E = -2^2 3^3 (5 - 4\sqrt{5})^3/(1+\sqrt{5})^2,$$

which can be written as

$$j_E = 3^3(\tau_3 + 1)(\tau_3 + 9)^3/\tau_3^3, \quad \tau_3 = (x_3 + \sqrt{5})/(x_3 - \sqrt{5}), \quad x_3 = 1.$$

Hence by [2, page 395], there is an isogeny λ of E to E^σ such that (E, λ) is of type (3).

The Galois group $G = \mathrm{Gal}(F(5)/\mathbf{Q}(\sqrt{5}))$ in this case is a Borel subgroup. In fact, we have

$$j_E = (\tau_5^2 + 10\tau_5 + 5)^3/\tau_5, \quad \tau_5 = -(2u-1)^3/u,$$

u being the fundamental unit of $\mathbf{Q}(\sqrt{5})$. Hence, in view of [2, page 399], E has a $\mathbf{Q}(\sqrt{5})$-rational subgroup of order 5. This shows G is contained in a Borel subgroup B. We see that G is actually equal to B using the following table. (Notation: $\mathfrak{l}$ = a prime ideal of $\mathbf{Q}(\sqrt{5})$, n = norm of $\mathfrak{l}$, A = number of rational points on E reduced mod $\mathfrak{l}$, and $t = 1 + n - A$.)

$\mathfrak{l}$	n	A	t	$t^2 - 4n$
$(4+\sqrt{5})$	11	12	0	-44
$(1-2\sqrt{5})$	19	24	-4	-60

Let $K/\mathbf{Q}$ be the subextension of $F(5)/\mathbf{Q}$ considered at the end of §1. Then $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to the subgroup

$$\left\{\begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \in SL_2(\mathbf{Z}/5\mathbf{Z})\right\}/\{\pm 1_2\}$$

of $PSL_2(\mathbf{Z}/5\mathbf{Z})$.

3°. $p = 7$, $N = 3$. Take $x_3 = 2$, $\tau_3 = (x_3 + \sqrt{-7})/(x_3 - \sqrt{-7})$ and put

$$\begin{aligned} j &= 3^3(\tau_3 + 1)(\tau_3 + 9)^3/\tau_3^3 \\ &= 2^8 3^3 (5 - 2\sqrt{-7})^3/11(2 + \sqrt{-7})^2. \end{aligned}$$

An elliptic curve over $\mathbf{Q}(\sqrt{-7})$ with this j-invariant is

$$E : y^2 = 4x^3 - 2^2 3(5 - 2\sqrt{-7})x - 2^2(15 - 14\sqrt{-7}).$$

The discriminant of E is $2^4 3^3 11(2 + \sqrt{-7})^2$. From the way we construct E we see that there is an isogeny λ such that (E, λ) is of type (3). We can show that $\mathrm{Gal}(F(7)/\mathbf{Q}(\sqrt{-7})) = GL_2^*(\mathbf{Z}/7\mathbf{Z})/\{\pm 1_2\}$ using the following data and reasoning as in example 1°.

$\mathfrak{l}$	n	A	t	$t^2 - 4n$
$(4+\sqrt{-7})$	23	18	6	-56
$(6-\sqrt{-7})$	43	34	10	-72

4°. $p = 19$, $N = 2$. Let

$$E : y^2 = 4x^3 - 2 \cdot 3 \cdot (5 - 2\sqrt{-19})x - 2^2(7 - 6\sqrt{-19}).$$

Then

$$\Delta = 2^3 3^3 5 \cdot 17(3+2\sqrt{-19})$$

and

$$j_E = 2^6 3^3(5-2\sqrt{-19})^3/5 \cdot 17(3+2\sqrt{-19})$$
$$= 2^6(\tau_2+4)^3/\tau_2^2$$

with $\tau_2 = (x_2+2\sqrt{-19})/(x_2-2\sqrt{-19})$, $x_2 = 3$. Therefore there is an isogeny λ such that (E, λ) is of type (2). We have the following table:

$\mathfrak{l}$	n	A	t	t^2-4n
$((5+\sqrt{-19})/2)$	11	16	-4	-28
$(2+\sqrt{-19})$	23	30	-6	-56

Since -56 is a quadratic residue modulo 19, -28 a quadratic non-residue, and $(-4)^2/11 \equiv -2 \pmod{19}$, we see that (1.3) holds in view of [4, prop. 19].

5° $p = 29$, $N = 2$. Let $u = (5+\sqrt{29})/2$ be the fundamental unit of $\mathbf{Q}(\sqrt{29})$. Consider

$$E: y^2 = 4x^3 + 3ux + (4u+3)u^2.$$

Then $\Delta = -3^3 5u^6(u-1)$, and $j_E = 2^6 3^3/5u^3(u-1)$, which can be written as

$$j_E = 2^6(\tau_2+4)^3/\tau_2^2, \quad \tau_2 = (x_2+\sqrt{29})/(x_2-\sqrt{29}), \quad x_2 = 3.$$

Hence there is an isogeny λ of E to E^σ such that (E, λ) is of type (2). We have the following table:

$\mathfrak{l}$	n	A	t	t^2-4n
$((1+\sqrt{29})/2)$	7	10	-2	-24
$((9+\sqrt{29})/2)$	13	12	2	-48

By [4, prop. 19], we see that $\mathrm{Gal}(F(29)/\mathbf{Q}(\sqrt{29})) \cong GL_2^*(\mathbf{Z}/29\mathbf{Z})/\{\pm 1_2\}$.

5. Equations of degree 6, 8, 12 and 14

Let $M = p^n$ and N a quadratic non-residue modulo p. Then the Galois group of the Galois closure of $\tilde{\mathscr{L}}_{MN}$ over $\tilde{\mathscr{L}}_N$ is isomorphic to $PSL_2(\mathbf{Z}/p^n\mathbf{Z})$. We are interested in the equation of the extension $\tilde{\mathscr{L}}_{MN}/\tilde{\mathscr{L}}_N$ when $\tilde{\mathscr{L}}_N$ is pure transcendental over $\mathbf{Q}$. We consider the following cases in this section: $(M, N) = (5, 2)$, $(7, 3)$, $(11, 2)$ and $(13, 2)$.

1° $(M, N) = (5, 2)$. Let τ_2 (resp. τ_5, τ) be the Hauptmodul for $\Gamma_0(2)$ (resp. $\Gamma_0(5)$, $\Gamma_0(10)$). We have the following identities from [2, p. 407–408]:

$$\tau_2 = (2\tau + 5)/\tau(\tau + 2)^5, \tag{5.1}$$
$$\tau_5 = \tau(2\tau + 5)^2/(\tau + 2).$$

From the same source, we know that w_2 permutes τ_2 with $1/\tau_2$ and τ_5 with $\tau^2(2\tau + 5)/(\tau + 2)^2$. It follows that

$$\tau^{w_2} = -(2\tau + 5)/(\tau + 2).$$

Therefore both

$$s = \tau + \tau^{w_2} + 4 = (\tau^2 + 4\tau + 3)/(\tau + 2)$$

and

$$t = \sqrt{5}(\tau - \tau^{w_2}) = \sqrt{5}(\tau^2 + 4\tau + 5)/(\tau + 2)$$

are invariant under ω_2, hence belong to $\tilde{\mathscr{L}}_{10}$. Actually, $\tilde{\mathscr{L}}_{10} = \mathbf{Q}(s, t)$. We have $5s^2 - t^2 = -20$. Hence $\tilde{\mathscr{L}}_{10} = \mathbf{Q}(y)$ with

$$y = (t - 5)/(s - 1) = \sqrt{5}(2\tau + 5 - \sqrt{5})/(2\tau + 3 + \sqrt{5}). \tag{5.2}$$

Put

$$x = -(\tau_2 + 1)/50\sqrt{5}(\tau_2 - 1). \tag{5.3}$$

Then $\tilde{\mathscr{L}}_2 = \mathbf{Q}(x)$.

To find an equation for the extension $\mathbf{Q}(y)/\mathbf{Q}(x)$, solve τ in terms of y from (5.2):

$$\tau = -((3 + \sqrt{5})y + (5 - 5\sqrt{5}))/2(y - 5) \tag{5.4}$$

Substituting (5.4) in (5.1) and then (5.1) in (5.3), we obtain

$$(y^3+3\cdot 5y^2-5^2y+5^2)(y^3-5y^2+5^2y-5^2)x=(y-1)^2(y^2-2y+5).$$

This is an equation in y over $\mathbf{Q}(x)$ with $PSL_2(\mathbf{Z}/5\mathbf{Z})$ as Galois group.

2° $(M, N)=(7,3)$. Let

$$\tau=\eta^2(3z)\eta^2(7z)/\eta^2(z)\eta^2(21z),$$

where η is the Dedekind function. Then $\mathbf{Q}(\tau)$ is the subfield of $\mathscr{L}_{21}$ fixed by w_{21}. We have $\tau^{w_3}=1/\tau$. Therefore

$$y=(\tau-1)/\sqrt{-7}(\tau+1)$$

is fixed by ω_3, and hence belongs to $\tilde{\mathscr{L}}_{21}$. The field $\mathbf{Q}(y)$ has index 2 in $\tilde{\mathscr{L}}_{21}$.

Let τ_3 be the Hauptmodul for $\Gamma_0(3)$. Put

$$x=(\tau_3-1)/\sqrt{-7}(\tau_3+1).$$

Then $\tilde{\mathscr{L}}_3=\mathbf{Q}(x)$ and $\tilde{\mathscr{L}}_{21}=\mathbf{Q}(x,y)$.

Solve τ in terms of y and τ_3 in terms of x. Then an equation for $\mathbf{Q}(x,y)/\mathbf{Q}(x)$ can be obtained from the modular equation connecting τ and τ_3. To obtain such a modular equation, we follow Fricke's method.

Note that $\tau_3^{w_{21}}=\tau^6/\tau_3$. Therefore the function $\tau(\tau_3+\tau^6/\tau_3)$ is invariant under w_{21}, hence belongs to $Q(\tau)$. Counting poles and zeros, we find the function is a polynomial of degree 8 in τ. The comparison of the Fourier coefficients gives us

$$\begin{aligned}3^3\tau(\tau_3+\tau^6/\tau_3)=\tau^8-14\tau^7+49\tau^6+14\tau^5-154\tau^4\\+14\tau^3+49\tau^2-14\tau+1.\end{aligned}$$

3° $(M, N)=(11,2)$. Let

$$\tau=\eta^2(z)\eta^2(11z)/2\eta^2(2z)\eta^2(22z).$$

Then τ generates the subfield of $\mathscr{L}_{22}$ fixed by w_{11}, and $\tau^{w_2}=1/\tau$. As before, we find $\tilde{\mathscr{L}}_2=\mathbf{Q}(x)$ and $\tilde{\mathscr{L}}_{22}=\mathbf{Q}(x,y)$, where

$$x=(\tau_2-1)/\sqrt{-11}(\tau_2+1),\quad y=(\tau-1)/\sqrt{-11}(\tau+1).$$

The equation for $\mathbf{Q}(x, y)/\mathbf{Q}(x)$ can be obtained from the modular equation

$$\tau_2/\tau + \tau^{11}/\tau_2 = \tau^{10} + 22\tau^9 + 194\tau^8 + 880\tau^7 + 2197\tau^6 + 3014\tau^5 + 2197\tau^4 + 880\tau^3 + 194\tau^2 + 22\tau + 1.$$

4° $(M,N) = (13, 2)$. This case is similar to case 2°. The subfield of $\mathscr{L}_{26}$ fixed by w_{26} is generated by

$$\tau = \eta^2(2z)\eta^2(13z)/\eta^2(z)\eta^2(26z)$$

We have $\tau^{w_2} = 1/\tau$. Proceeding as before, we find $\tilde{\mathscr{L}}_2 = \mathbf{Q}(x)$, and $\tilde{\mathscr{L}}_{26} = \mathbf{Q}(x, y)$, where

$$x = (\tau_2 - 1)/\sqrt{13}(\tau_2 + 1), \quad y = (\tau - 1)/\sqrt{13}(\tau + 1).$$

The modular equation relating τ_2 and τ is

$$\begin{aligned} 2^6\tau(\tau_2 + \tau^{12}/\tau_2) = \tau^{14} &- 26\tau^{13} + 273\tau^{12} - 1508\tau^{11} + 4888\tau^{10} \\ &- 10244\tau^9 + 15574\tau^8 - 18044\tau^7 \\ &+ 15574\tau^6 - 10244\tau^5 + 4888\tau^4 \\ &- 1508\tau^3 + 273\tau^2 - 26\tau + 1. \end{aligned}$$

Solving τ_2 in terms of x and τ in terms of y, and substituting the results in the above modular equation, we obtain an equation of degree 14 in y over $\mathbf{Q}(x)$ which admits $PSL_2(\mathbf{Z}/13\mathbf{Z})$ as Galois group.

REMARK 1: Our method depends on the fact that, for each of the above (M, N), $X_0(MN)$ modulo a certain Atkin-Lehner involution is a rational curve. In view of Ogg's result [3], the above 4 examples exhaust all interesting cases that can be so treated.

REMARK 2: The modular equation in 2° is equivalent to

$$3^3(\tau_3/\tau^3 + \tau^3/\tau_3) = T^4 - 14T^3 + 45T^2 + 66T - 250, \quad T = \tau + 1/\tau.$$

Note that T is the Hauptmodul for the group generated by $\Gamma_0(21)$, w_3 and w_7. Similarly, the modular equations in 3° and 4° are equivalent to respectively

$$\tau^6/\tau_2 + \tau_2/\tau^6 = T^5 + 22T^4 + 189T^3 + 792T^2 + 1620T + 1298,$$
$$T = \tau + 1/\tau,$$

and

$$2^6(\tau_2/\tau^6 + \tau^6/\tau_2) = T^7 - 26T^6 + 266T^5 - 1352T^4 + 3537T^3 - 4446T^2 + 2268T - 520,$$

$$T = \tau + 1/\tau.$$

Acknowledgment

I would like to thank Professor Atkin for showing me the equations that appear in 3°, 4° and Remark 2.

REFERENCES

[1] B. J. BIRCH: Diophantine analysis and modular functions. Proc. Conf. Algebraic Geometry (Bombay, 1968) 35–42.
[2] R. FRICKE: *Lehrbuch der Algebra III.* Braunschweig 1928.
[3] A. P. OGG: Hyperelliptic modular curves. *Bull. Math. Soc. France, 102* (1974) 449–462.
[4] J.-P. SERRE: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Math., 15* (1972) 259–331.
[5] K.-y SHIH: On the construction of Galois extensions of function fields and number fields. *Math. Ann., 207* (1974) 99–120.
[6] G. SHIMURA: A reciprocity law in non-solvable extensions. *J. Reine Angew. Math., 221* (1966) 209–220.
[7] G. SHIMURA: Introduction to the arithmetic theory of automorphic functions. *Publ. Math. Soc. Japan, No. 11,* Iwanami Shoten and Princeton University Press, 1971.
[8] G. SHIMURA: Class fields over real quadratic fields and Hecke operators. *Ann. of Math., 95* (1972) 130–190.

(Oblatum 18-X-1976)

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48104

Department of Mathematics
University of Maryland
College Park, Maryland 20742

*Partially supported by NSF grant MPS 75-07948.