COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 51, No. 1 2002

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Some Codes Arising from Elliptic Modular Surfaces

by

Tetsuji SHIODA

(Received April 4, 2002)

Abstract. For every $N \geq 3$, there is a linear code over $\mathbf{Z}/N\mathbf{Z}$ with some interesting properties, which arises from the Mordell-Weil lattice of the elliptic modular surface of level N. It is an $[n, k, d]$-code with the code length n equal to the number of cusps of the elliptic modular curve of level N and the rank $k = 2$ such that every code word has a constant "Bernoulli norm". The minimum distance d is equal to $n \cdot p_0/(p_0 + 1)$ if p_0 is the least prime divisor of N. Moreover it has a natural action by $SL(2, \mathbf{Z}/N\mathbf{Z})$, and a $\mathbf{Z}/N\mathbf{Z}$-valued nondegenerate bilinear pairing compatible with the action.

In particular, for a prime level $p \geq 3$, we obtain an $[n, k, d]$ constant weight code over the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ such that

$$n = \frac{p^2 - 1}{2}, \quad k = 2, \quad d = \frac{p^2 - p}{2}$$

which has an $SL(2, \mathbf{F}_p)$-action and an invariant nondegenerate pairing.

1. Introduction

The elliptic modular surface of level N is an elliptic surface obtained as a compactification of the universal family of elliptic curves with level N structure. By [8], it has N^2 sections of order dividing N while all the singular fibres are of type I_N in the sense of Kodaira [2], i.e. each singular fibre consists of N smooth rational curves forming an N-gon. Our original problem is to determine the intersection diagram of the N^2 sections and the irreducible components of all the singular fibres. The main idea is to use the height formula from the theory of Mordell-Weil lattices [9], which was not available at the time of [8]. For a torsion section, the height is of course zero, still the height formula gives a rich information about how this section intersects various singular fibres.

In trying to write down explicitly the intersection diagram of all the sections and all the singular fibres, it becomes evident that the whole situation can be best described in terms of a *linear code*, $\mathcal{C}(N)$, over the ring $\mathbf{Z}/N\mathbf{Z}$. This is the motivation for the present note.

We formulate the main results on $\mathcal{C}(N)$ first (§2), since it is of more elementary nature. We state the basic properties of this code (Theorem 1), and then we construct a concrete model of $\mathcal{C}(N)$ with explicit generators (Theorems 2 and 3). The definition of $\mathcal{C}(N)$ will

be given in §3, together with the proof of Theorem 1 except (iv). After a few examples in §4, we prove in §5 Theorem 2 and 3. Next we discuss in §6 the relation to the Bernoulli distribution ([3], [4] or [11]).

At the occasion of a colloquium talk on this subject, N. Aoki has kindly reminded us of Miranda's paper [5]. We find it is very close in motivation but it focuses more on the behaviour of a single torsion section in a more general situation. We use one of Miranda's result to determine the minimum distance of our code (§6).

2. Main results

First we introduce a norm β on the finite ring $\mathbf{Z}/N\mathbf{Z}$ defined as follows: For any $a \in \mathbf{Z}/N\mathbf{Z}$ (identified with its unique representative such that $0 \leq a < N$), we set

$$\beta(a) = \frac{a(N-a)}{N}\,. \tag{1}$$

For any $\xi = (a_v) \in (\mathbf{Z}/N\mathbf{Z})^n$, we set

$$\beta(\xi) = \sum_i \beta(a_v)\,. \tag{2}$$

We propose to call it the "Bernoulli norm" of ξ. For other terminology on codes, we follow [1] or [6].

THEOREM 1. *For every $N \geq 3$, the linear code*

$$\mathcal{C} = \mathcal{C}(N) \subset (\mathbf{Z}/N\mathbf{Z})^n \tag{3}$$

associated with the elliptic modular surface of level N has the following properties:

(i) *the code length n is equal to the number of $\Gamma(N)$-cusps*:

$$n = t(N) =: \frac{1}{2}N^2 \prod_{p|N}\left(1 - \frac{1}{p^2}\right), \tag{4}$$

(ii) *the rank $k = 2$, i.e. $\mathcal{C} \simeq (\mathbf{Z}/N\mathbf{Z})^2$,*

(iii) *the Bernoulli norm of every $\xi \in \mathcal{C}, \xi \neq 0$, is constant*:

$$\beta(\xi) = \frac{1}{6}Nt(N)\,, \tag{5}$$

(iv) *The minimum distance of the code $\mathcal{C}$ is equal to*

$$d = \frac{p_0}{p_0+1}n \tag{6}$$

where p_0 is the smallest prime divisor of N.

(v) *the group $SL(2, \mathbf{Z}/N\mathbf{Z})$ acts effectively on the code $\mathcal{C}$,*

(vi) *there is a nondegenerate skew pairing $\mathcal{C} \times \mathcal{C} \to \mathbf{Z}/N\mathbf{Z}$, which is compatible with action in* (v).

An explicit model of $\mathcal{C}(N)$ can be given as follows. For simplicity, we state first the case of prime level $N = p$.

THEOREM 2. *For an odd prime number p, let $r = \frac{p-1}{2}$ and let $\mathcal{C}'(p)$ be the 2-dimensional subspace of $\mathbf{F}_p^n$, $n = \frac{p^2-1}{2}$, generated by the two elements*:

$$\xi = (1^p 2^p \cdots r^p 0^r), \quad \eta = (\overline{01\cdots p-1}^{\,r}\ \overline{12\cdots r}). \tag{7}$$

Then $\mathcal{C}'(p)$ is a self-orthogonal $[n, k, d]$ code over $\mathbf{F}_p$ with

$$n = \frac{p^2-1}{2}, \quad k = 2, \quad d = \frac{p^2-p}{2}.$$

It is equivalent to the code $\mathcal{C}(N)$, for $N = p$, given in Theorem 1, *so that it has $SL(2, \mathbf{F}_p)$-action and an invariant nondegenerate pairing.*

Further it is a constant weight code. In other words, the weight enumerator of $\mathcal{C} = \mathcal{C}(p)$ (cf. [1, Ch. 3]) *is given by*

$$W_{\mathcal{C}}(x, y) = x^n + (p^2-1)x^{\frac{p-1}{2}} y^{\frac{p^2-p}{2}}, \tag{8}$$

and the symmetric weight enumerator is given by

$$swe_{\mathcal{C}}(x_0, \cdots, x_r) = x_0^n + (p^2-1)x_0^r (x_1 \cdots x_r)^p, \tag{9}$$

where the variable x_a corresponds to $\pm a \in \mathbf{F}_p$ for $a = 0, \cdots, r$.

In the first example for level $N = 3$, we obtain the code $\mathcal{C}(3)$ over $\mathbf{F}_3$ which is known as the [4, 2, 3] ternary tetra code (cf. [Ch. 3, §2.5], §4).

Next we construct an explicit model of $\mathcal{C}(N)$ for arbitrary N:

THEOREM 3. *Fix $N \geq 3$ and set $I_N = \{0, 1, 2, \cdots, N-1\}$. For each divisor d of N, let*

$$I_{N,d} = \{i \in I_N \mid \gcd(i, d) = 1\}$$

and

$$J_{N,d} = \{i \in I_N | i \leq N/2, \quad \gcd(i, N) = d\} = \{u_{d,1}, u_{d,2}, \cdots u_{d,l}\}.$$

Note that $m := |I_{N,d}| = \varphi(d)N/d$ and $l := |J_{N,d}| = \varphi(N/d)/2$ if $d < N/2$. Consider the $2 \times n$ matrix

$$M = \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} \cdots & (u_{d,1})^m & (u_{d,2})^m & \cdots & (u_{d,l})^m & \cdots \\ \cdots & I_{N,d} & I_{N,d} & \cdots & I_{N,d} & \cdots \end{pmatrix} \tag{10}$$

where d runs over divisors of N. (Here the symbol $(u)^m$ stands for u repeated m times, and $I_{N,d}$ is regarded as an ordered sequence.) Two cases need modification: (i) *In case $d = N$, $I_{N,d}$ should be replaced by $I_{N,d}/\pm$ and $l = 1, m = \varphi(N)/2$.* (ii) *In case N is even and $d = N/2$, $I_{N,d}$ should be replaced by $I_{N,d}/\pm$ and $l = 1, m = \varphi(N/2)$.*

Let $\mathcal{C}'(N)$ denote the linear code over $\mathbf{Z}/N\mathbf{Z}$ generated by the row vectors ξ and η of M. Then $\mathcal{C}'(N)$ is equivalent to the code $\mathcal{C}(N)$ of Theorem 1.

REMARK. We note that the number of columns of M

$$n = \sum_{d|N} m \cdot l = \sum_{d|N} \frac{1}{2}\varphi(d)\varphi\left(\frac{N}{d}\right)\frac{N}{d}$$

is equal to $t(N)$, as it should be. This can be verified directly (say, by induction on N), or by the following observation. It is easy to check that the column vectors of M gives a full set of representatives for the set

$$V = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \bmod N | a, b \in \mathbf{Z}, \gcd(a, b) = 1 \right\} \Big/ \begin{pmatrix} a \\ b \end{pmatrix} \sim - \begin{pmatrix} a \\ b \end{pmatrix} \tag{11}$$

As is wellknown, the set V is in a bijective correspondence with $\Gamma(N)$-cusps, whose number is $t(N)$ (see Shimura [7, 1.6]). Hence we have $n = t(N)$.

3. Definition of the linear code $\mathcal{C}(N)$

3.1. The height formula

First we recall the explicit height formula for the sections of an elliptic surface

$$f : S \longrightarrow C ,$$

as defined in the theory of Mordell-Weil lattices [9]. For any section $P \neq O$, we have

$$\langle P, P \rangle = 2\chi + 2(PO) - \sum_v Contr_v(P) . \tag{12}$$

Here χ is the arithmetic genus of the surface S, (PO) denotes the intersection number of the section (P) and the zero-section (O) on S, and the summation runs over $v \in C$ such that $f^{-1}(v)$ is a reducible singular fibre. The local contribution term $Contr_v(P)$ is a non-negative rational number, which is determined by the type of the singular fibres and the position of its component intersecting with the given section (P).

In particular, if P is a section of finite order and the base field has characteristic 0, then the above formula reduces to the following:

$$\sum_v Contr_v(P) = 2\chi . \tag{13}$$

3.2. Elliptic modular surface of level N

Now let us consider the case where $S = S(N)$ is the elliptic modular surface of level $N \geq 3$, where the base curve $C = X(N)$ is the elliptic modular curve of level N over the complex number field. See [8, §5] (cf. [2, §8], [7, 1.6]) for what follows.

As a Riemann surface, $X(N)$ is obtained from the quotient $\Gamma(N)\backslash\mathcal{H}$ by adjoining the cusps, where $\Gamma(N)$ is the principal congruence subgroup of level N of $\Gamma(1) = SL(2, \mathbf{Z})$ acting on the upper half plane $\mathcal{H}$ by the familiar manner: $\tau \mapsto \tau' = (a\tau + b)/(c\tau + d)$. The number of the cusps is given by $t(N)$ as defined in (4).

The elliptic surface $S(N)$ is obtained from the quotient $\Gamma(N) \cdot \mathbf{Z}^2 \backslash \mathcal{H} \times \mathbf{C}$ by adjoining the singular fibres. Here the action is defined by

$$\tilde{\gamma} = (\gamma, n, m) : (\tau, z) \mapsto (\tau', \frac{z + n\tau + m}{c\tau + d}) , \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N) . \tag{14}$$

For each cusp $v \in X(N)$, the singular fibre $f^{-1}(v)$ has Kodaira type I_N, i.e. the irreducible components are N rational curves $\Theta_{v,i} (0 \leq i \leq N-1)$ forming an N-gon; let $\Theta_{v,0}$ denote the unique component meeting the zero-section and we order $\Theta_{v,i}$ in a cyclic way. (N.B. There are two choices for the ordering. Choose either one.) The smooth part $f^{-1}(v)^{\#}$ is isomorphic to $\mathbf{G}_m \times \mathbf{Z}/N\mathbf{Z}$. If a section (P) meets the i-th component $\Theta_{v,i}$ of $f^{-1}(v)$, then we have

$$Contr_v(P) = i(N-i)/N \quad (0 \leq i \leq N-1) \tag{15}$$

(see [9]); let us write $i = i_v(P)$ in this case.

Further, by [8], the group of sections (which is naturally identified with the group $E(K)$ of the rational points of the generic fibre E over the function field $K = \mathbf{C}(X(N)))$ is a finite group isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$.

On the other hand, the genus of $X(N)$ and the arithmetic genus of $S(N)$ are given by

$$g(N) = 1 + \frac{N-6}{N} t(N), \quad \chi(N) = \frac{Nt(N)}{12}. \tag{16}$$

3.3. Definition

By (13) and (15), we have the following relation: for every $P \in E(K)$, $P \neq O$,

$$\sum_v \frac{i_v(P)(N - i_v(P))}{N} = \frac{N}{6} t(N). \tag{17}$$

Fixing an ordering of $t(N)$ cusps, we consider the map

$$s : E(K) \simeq (\mathbf{Z}/N\mathbf{Z})^2 \longrightarrow (\mathbf{Z}/N\mathbf{Z})^{t(N)} \tag{18}$$

sending P to $(i_v(P))$. The map s is a group homomorphism and it is injective by (17). Therefore we can define a linear code over $\mathbf{Z}/N\mathbf{Z}$ by letting

$$\mathcal{C}(N) := Im(s) \subset (\mathbf{Z}/N\mathbf{Z})^{t(N)}. \tag{19}$$

This is what we called the code associated with the elliptic modular surface of level N in Theorem 1.

3.4. Proof of Theorem 1 (except (iv))

By the above definition, (i) and (ii) are obvious, and (iii) is just a restatement of (17). We prove (iv) later in §6.

Next, in order to show (v), we recall first that the group $SL(2, \mathbf{Z}/N\mathbf{Z}) = \Gamma(1)/\Gamma(N)$ acts on the elliptic modular curve $X(N)$ inducing a transitive permutation group of the set of cusps. This action lifts to the elliptic modular surface $S(N)$ via $\gamma \mapsto \tilde{\gamma} = (\gamma, n, m)$ in (14) where we take $\gamma \in \Gamma(1)$ and $n = m = 0$ (cf. [8]). Its action on $E(K)$ is given by $P \mapsto P^{\gamma}$ where we define $P^{\gamma} = \tilde{\gamma}^{-1} \circ P \circ \gamma$. (The same letter γ is used here to denote the image in $\Gamma(1)/\Gamma(N)$, but it should not cause any confusion.) Then we have

$$i_v(P^{\gamma}) = \varepsilon \cdot i_{\gamma \cdot v}(P) \text{ in } \mathbf{Z}/N\mathbf{Z} \tag{20}$$

where $\varepsilon = \pm 1$ is independent of $P \in E(K)$, depending only on v and γ.

This implies that $SL(2, \mathbf{Z}/N\mathbf{Z})$ induces a group of automorphisms of the code $\mathcal{C}(N)$. Compare the proof of Theorem 2 (§5) where we examine the above situation in more detail.

Finally (vi) is just the Weil pairing on the N-torsion group (see e.g. [10, Ch. III, §8]) stated as a property of our code. q.e.d.

4. Examples

Let us work out a few examples before going further.

For a fixed N, let $n = t(N)$ as in (4). Given $\xi = (a_1, \cdots, a_n) \in (\mathbf{Z}/N\mathbf{Z})^n$, denote by $w_a = w_a(\xi)$ for $a \in \mathbf{Z}/N\mathbf{Z}$ the number of the indices ν such that $a_\nu = a$. Then ξ satisfies the condition (17) if and only if $\bar{\xi} = (w_a)$ is an integral solution of the following equations:

$$\sum_{a=1}^{N-1} \frac{a(N-a)}{N}\, w_a = \frac{1}{6}Nn\,, \quad \sum_a w_a = n, \quad w_a \geq 0\,. \tag{21}$$

We call ξ a *Bernoulli vector* (of level N) if all multiples $c\xi (\neq 0)$ satisfy the condition (17), or the equivalent condition (21).

4.1. Level $N = 3$

For $N = 3$, we have $n = 4$. By (21), ξ is a Bernoulli vector iff

$$w_1 + w_2 = 3\,, \quad w_0 = 1\,.$$

Hence ξ is equal to $(1, 1, 1, 0)$ up to permutation and changing some of 1 to $2 = -1$.

Take $\xi = (1, 1, 1, 0)$. Suppose that η is another Bernoulli vector such that any nonzero linear combination $c\xi + d\eta$ is again a Bernoulli vector. Then it is easy to see that $\eta = (b_\nu)$ must be such that $b_4 = 0$ and $\{b_1, b_2, b_3\} = \{0, 1, 2\}$. Thus we can take $\eta = (0, 1, 2, 1)$ by changing, if necessary, η by $\pm\eta$ and adjusting the order of the first three coordinates.

In terms of the elliptic modular surface of level $N = 3$, the above can be rephrased as follows. By a suitable choice of generators $P, Q \in E(K)$ and by reordering the $n = 4$ cusps, we can normalize the code $\mathcal{C}(3)$ so that

$$s(P) = \xi = (1, 1, 1, 0)\,, \quad s(Q) = \eta = (0, 1, 2, 1)\,.$$

In other words, $\mathcal{C}(3)$ and $\mathcal{C}'(3)$ are equivalent codes over $\mathbf{F}_3$. Note that the code $\mathcal{C}'(3)$ with generators ξ, η is a self-dual $[4, 2, 3]$ code, known as the ternary tetra code (denoted $\mathcal{C}_4$ in [1, Ch. 3, §2.5]).

Now let M denote the generator matrix:

$$M = \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

The group $SL(2, \mathbf{Z})$ (and hence $SL(2, \mathbf{F}_3)$ too) has standard generators:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{22}$$

Considering the contragradient action, we have

$$
{}^tS^{-1}M = \begin{pmatrix} -\eta \\ \xi \end{pmatrix} = M \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
$$

$$
{}^tT^{-1}M = \begin{pmatrix} \xi \\ \xi + \eta \end{pmatrix} = M \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .
$$

This shows that the group $SL(2, \mathbf{F}_3)$ acts on $\mathcal{C}(3)$. According to [1, Ch. 3, §2.5], the automorphism group of this code is $2.S_4$. The above should be equivalent to the action of its subgroup $2.A_4$, which is isomorphic to $SL(2, \mathbf{F}_3)$.

4.2. Level $N = 4$

For $N = 4$, we have $n = 6$. As in the previous case, it is easy to check that every Bernoulli vector of exact order 4 corresponds to the solution of

$$w_1 + w_3 = 4\,, \quad w_0 = w_2 = 1\,.$$

Hence it is equal to

$$\xi = (1, 1, 1, 1, 2, 0)$$

up to permutation and changing some of 1 to $3 = -1$. Taking this ξ, the choice of the second vector η is subject to the condition that any linear combination $c\xi + d\eta (\neq 0)$ is again a Bernoulli vector. Again we can take

$$\eta = (0, 1, 2, 3, 1, 1)$$

by adjusting the order of $n = 6$ cusps v and by reorienting the N-gon in each singular fibre (i.e. by numbering the irreducible components $\Theta_{v,i}$ in the reverse order), if necessary.

In this way, we obtain the [6, 2, 4] linear code $\mathcal{C}'(4)$ over $\mathbf{Z}/4\mathbf{Z}$. Let us identify $\mathcal{C}(4) = \mathcal{C}'(4)$. The generator matrix of the code $\mathcal{C}(4)$ is:

$$M = \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix} .$$

Of the $4^2 = 16$ elements in $\mathcal{C}(4)$, the 12 elements of exact order 4 have the weight 5, while the 3 elements of order 2 have the weight 4. Thus the weight enumerator is given by

$$W_{\mathcal{C}}(x, y) = x^6 + 3x^2y^4 + 12xy^5\,.$$

The symmetric weight enumerator is given by

$$swe_{\mathcal{C}}(x_0, x_1, x_2) = x_0^6 + 3x_0^2x_2^4 + 12x_0x_2x_1^4\,,$$

where x_0, x_1, x_2 are the variables corresponding to $0, \pm 1, 2 \in \mathbf{Z}/4\mathbf{Z}$.

This code is "doubly" self-orthogonal, since the Euclidean norm of ξ, η are as follows:

$$\xi \cdot \xi = 8\,, \quad \xi \cdot \eta = 8\,, \quad \eta \cdot \eta = 16\,.$$

The action of $SL(2, \mathbf{Z}/4\mathbf{Z})$ on $\mathcal{C}(4)$ is given as before, and will be omitted.

4.3. Level $N = 5$

In this case, we have $N = 5, n = 12$. The code $\mathcal{C}(5)$ has the generator matrix:

$$M = \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

Since

$$\xi \cdot \xi = 25\,, \quad \xi \cdot \eta = 30\,, \quad \eta \cdot \eta = 65\,,$$

it is a self-orthogonal $[12, 2]$ code over $\mathbf{F}_5$. Moreover it is a constant weight $[12, 2, 10]$ code whose weight enumerator is given by

$$W_{\mathcal{C}}(x, y) = x^{12} + 24x^2y^{10}\,.$$

The symmetric weight enumerator is given by

$$swe_{\mathcal{C}}(x_0, x_1, x_2) = x_0^{12} + 24x_0^2x_1^5x_2^5\,,$$

where x_0, x_1, x_2 are the variables corresponding to $0, \pm 1, \pm 2 \in \mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$.

The action of the group $SL(2, \mathbf{F}_5)$ on the $\mathcal{C}(5)$ can be described as before (so omitted here), but it suggests that this code might be related to the geometry of icosahedron.

5. Proof of Theorems 2 and 3

It is enough to prove Theorem 3, since Theorem 2 is a special case for N prime.

Fix $N \geq 3$ and let $f : S(N) \to X(N)$ be the elliptic modular surface of level N. With the same notation as in §3.4, the group $SL(2, \mathbf{Z}/N\mathbf{Z}) = \Gamma(1)/\Gamma(N)$ acts on both $S(N)$ and $X(N)$ so that $\gamma \circ f = f \circ \tilde{\gamma}$.

The N^2 sections of f are given by $P = P_{(m_1,m_2)} : X(N) \to S(N)$, which is defined by the map $\mathcal{H} \to \mathcal{H} \times \mathbf{C}$ sending τ to $(\tau, (m_1\tau + m_2)/N)$:

$$P_{(m_1,m_2)}([\tau]) = [\tau, (m_1\tau + m_2)/N] \quad (\tau \in \mathcal{H})\,. \tag{23}$$

Here (m_1, m_2) is any pair of integers modulo N. (We denote by $[\tau]$ the image point of $\tau \in \mathcal{H}$ under the natural map $\mathcal{H} \to \mathcal{H}/\Gamma(N) \subset X(N)$, and similarly for $[\tau, z]$.)

It is immediate to check that for $\gamma \in \Gamma(1)/\Gamma(N)$, we have

$$(P_{(m_1,m_2)})^{\gamma} = P_{(m_1,m_2)\gamma}\,. \tag{24}$$

Now we examine how these sections behave at the cusps. First look at the cusp at infinity $v_\infty = [i\infty] \in X(N)$. The local parameter at v_∞ is given by $q_N = e^{2\pi i\tau/N}$. For the section $P = P_{(m_1,m_2)}$, we have

$$e^{2\pi i(m_1\tau+m_2)/N} = q_N^{m_1} \cdot e^{2\pi i m_2/N}\,. \tag{25}$$

In view of Kodaira's description of a singular fibre of type I_N ([2, §8, p. 598–]), it follows that the section P intersects the m_1-th component Θ_{m_1} of $f^{-1}(v_\infty)$, i.e.

$$i_{v_\infty}(P_{(m_1,m_2)}) = m_1 \in \mathbf{Z}/N\mathbf{Z}\,. \tag{26}$$

(More precisely, we can choose one of the two cyclic ordering of irreducible components so that the above equality holds for all (m_1, m_2) mod N.)

Next, given any cusp $v \in X(N)$, there is some $\gamma \in \Gamma(1)$ such that $v = \gamma \cdot v_\infty$. By (20) and (24), we have then

$$i_v(P_{(m_1,m_2)}) = \varepsilon i_{v_\infty}((P_{(m_1,m_2)})^\gamma) = \varepsilon i_{v_\infty}(P_{(m_1,m_2)\gamma}) \tag{27}$$

where $\varepsilon = \varepsilon_v = \pm 1$ is independent of (m_1, m_2).

Take standard generators of $E(K)$: $P = P_{(1,0)}$ and $Q = P_{(0,1)}$. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then (26) and (27) show that, for the cusp $v = \gamma \cdot v_\infty = [a/c]$, we have

$$\begin{pmatrix} i_v(P) \\ i_v(Q) \end{pmatrix} = \pm \begin{pmatrix} a \\ c \end{pmatrix} . \tag{28}$$

Thus if we let $\xi = s(P)$, $\eta = s(Q)$, then $\{\xi, \eta\}$ are generators of the code $\mathcal{C}(N)$, and if we fix an ordering of cusps $\Omega = \{v_\infty, \cdots, v, \cdots\}$, then we have

$$M = \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} 1 & \cdots & \pm a & \cdots \\ 0 & \cdots & \pm c & \cdots \end{pmatrix} . \tag{29}$$

In particular, each cusp $v = [a/c]$ is completely recovered from the corresponding column vector of M. Comparing this situation with the observation in the Remark at the end of §2, we see that the set V defined by (11) is equal, up to order, to the column vectors (mod N) of the matrix M, which proves Theorem 3.

6. Bernoulli distribution

6.1. Bernoulli polynomial

For a systematic study of the condition (5) (equivallently (17) or (21)), it will be useful to introduce the second Bernoulli polynomial

$$B(x) = B_2(x) = x^2 - x + \frac{1}{6} . \tag{30}$$

First note the obvious properties:

$$B(1 - x) = B(x) \tag{31}$$

$$-\frac{1}{12} = B\left(\frac{1}{2}\right) \leq B(x) \leq B(0) = B(1) = \frac{1}{6} \quad (0 \leq x \leq 1) . \tag{32}$$

More important property is the following *distribution relation*: for any positive integer N, we have

$$B(x) = N \sum_{a=0}^{N-1} B\left(\frac{x + a}{N}\right) . \tag{33}$$

For the proof, see [4, Ch. 2, §2]. In particular, by setting $x = 0$, we have

$$N \sum_{a=1}^{N-1} B\left(\frac{a}{N}\right) + (N - 1)\, B(0) = 0 . \tag{34}$$

It follows from (31) that, if $N = 2r + 1$ is odd, the above is rewritten as

$$N \sum_{a=1}^{r} B\left(\frac{a}{N}\right) + r\ B(0) = 0 \quad \left(r = \frac{N-1}{2}\right). \tag{35}$$

For example, we have for small N

$$2B\left(\frac{1}{2}\right) + B(0) = 0\,, \quad 3B\left(\frac{1}{3}\right) + B(0) = 0\,, \quad 4B\left(\frac{1}{4}\right) + 2B\left(\frac{1}{2}\right) + \frac{3}{2}B(0) = 0\,.$$

In the following, we limit $B(x)$ to the interval $0 \le x \le 1$ and regard it as a periodic function of x modulo integers.

6.2. Back to our question

LEMMA 4. *With the notation of Theorem1, $\xi = (a_\nu) \in (\mathbf{Z}/N\mathbf{Z})^n$ satisfies the equation* (5) (*equivallently* (17) *or* (21)) *if and only if*

$$\sum_{\nu=1}^{n} B\left(\frac{a_\nu}{N}\right) = 0\,. \tag{36}$$

Proof. It is enough to observe the identity:

$$N\ B\left(\frac{a}{N}\right) = N\left\{\left(\frac{a}{N}\right)^2 - \frac{a}{N} + \frac{1}{6}\right\} = -\frac{a(N-a)}{N} + \frac{N}{6} \tag{37}$$

for any a with $0 \le a < N$. q.e.d.

LEMMA 5. *Assume $N = p$, an odd prime. Then $\xi = (1^p 2^p \cdots r^p 0^r)$ given by* (7) *is a Bernoulli vector.*

Proof. By (35), we have

$$p \sum_{a=1}^{r} B\left(\frac{a}{p}\right) + r\ B(0) = 0 \quad \left(r = \frac{p-1}{2}\right) \tag{38}$$

which shows in view of Lemma 4 that ξ satisfies (5) and (21). Moreover any nonzero multiple $c\xi$ is equal to ξ up to ordering and changing the sign of coordinates (mod p). Hence $c\xi$ also satisfies (5) and (21), i.e.

$$p \sum_{a=1}^{r} B(\frac{ca}{p}) + r\ B(0) = 0\,, \quad \forall c \not\equiv 0 \ (\mathrm{mod}\ p)\,. \tag{39}$$

This proves the assertion. q.e.d.

6.3. Miranda's result

Now we consider the converse. Suppose $\zeta \in (\mathbf{Z}/p\mathbf{Z})^{n'}$ is a Bernoulli vector, where n' is arbitrary. Up to ordering and changing the sign of coordinates, we can assume $\zeta = (\cdots, a^{w_a}, \cdots, 0^{w_0})$. Here a runs over a fixed set of representatives, say A, of $(\mathbf{Z}/p\mathbf{Z})^\times$ modulo $a \to -a$. (In the above, $\{1, 2, \cdots, r\}$ is chosen as A, but other choice is also useful.)

Then $\{w_a\}$ satisfies a system of linear equations

$$\sum_{a\in A} w_a B(\frac{ca}{p}) + w_0\ B(0) = 0\,, \quad \forall c \not\equiv 0 \pmod{p}\,, \tag{40}$$

and this is the necessary and sufficient condition for a Bernoulli vector for $N = p$.

Observe that (39) gives a solution for this system. The following result, due to Miranda [5], asserts that it is essentially the unique solution.

LEMMA 6. *Fix p and A. If $\{w_a\}$ satisfies* (40), *then*

$$w_a = kp \quad (\forall a \in A)\,, \quad w_0 = k\frac{p-1}{2} \tag{41}$$

for some integer k and n' is equal to kn where $n = t(p) = (p^2-1)/2$.

Proof. It suffices to show that the square matrix $(B(ca/p)|c, a \in A)$ of degree $|A| = (p-1)/2$ has nonzero determinant. For the proof of this fact, see [5, Prop. 6.1] and references given there. It is based on non-vanishing of $B_{2,\chi}$, the generalized Bernoulli number, for nontrivial even Dirichlet characters $\chi \bmod p$. (Equivalently, on non-vanishing of the special value $L(-1, \chi)$ of Dirichlet L-series for the same χ.) q.e.d.

6.4. Proof of Theorem 1 (iv): Minimum distance of $\mathcal{C}(N)$

Fix N, and take a nonzero element $\zeta = (a_\nu) \in \mathcal{C}(N)$. Let d be its exact order, which is a divisor of N. If d is not a prime, say $d = d'p$ with d', $p > 1$, the element $\zeta' = d'\zeta = (d'a_\nu)$ has order p and the weight of ζ' is not greater than that of ζ: $wt(\zeta') \le wt(\zeta)$. Hence to determine the minimum distance of $\mathcal{C}(N)$, it is enough to consider the case where d is a prime divisor of N.

So suppose ζ has prime order p. Since it is a Bernoulli vector (Th. 1(iii)), we can apply Lemma 6 to see that the number of nonzero (resp. zero) coordinates a_ν is equal to $kp|A|$ (resp. $k(p-1)/2$). Hence the ratio of these two numbers is $p : 1$, and so we have

$$wt(\zeta) = \frac{p}{p+1}n \quad (n = t(N))\,. \tag{42}$$

The minimum distance of the code $\mathcal{C}(N)$ is given by the smallest among the above values for all prime divisors p of N. This proves Theorem 1 (iv). q.e.d.

References

[1] J. Conway and N. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag, 2nd ed. (1993).

[2] K. Kodaira, On compact analytic surfaces II-III, Ann. of Math. **77** (1963), 563–626; **78** (1963), 1–40; Collected Works, III, 1269–1372, Iwanami and Princeton Univ. Press (1975).

[3] D. S. Kubert and S. Lang, Modular Units, Springer-Verlag (1981).

[4] S. Lang, Cyclotomic Fields, GTM, Springer-Verlag (1978).

[5] R. Miranda, Component numbers for torsion sections of semistable elliptic surfaces, Contemporary Math., **164** (1994), 293–311.

[6] E. Rains and N. Sloane, Self-dual codes, in: Handbook of Coding Theory

[7] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton Univ. Press (1971).

[8] T. Shioda, On elliptic modular surfaces, J. Math. Soc. Japan, **24** (1972), 20–59.

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

[10] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag (1986).
[11] L. Washington, Introduction to Cyclotomic Fields, GTM, Springer-Verlag (1982).

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 171–8501 Japan