Can. J. Math., Vol. XXX, No. 6, 1978, pp. 1183–1205

SIMPLE FACTORS IN THE JACOBIAN OF A FERMAT CURVE

NEAL KOBLITZ AND DAVID ROHRLICH

1. Introduction. Let

$$F(N) = \{(X, Y, Z) \in P^2(\mathbf{C}) : X^N + Y^N = Z^N\}, \quad N \geqq 3,$$

denote the Nth Fermat curve. The period lattice of $F(N)$ is contained with finite index in the product of certain lattices $L_{r,s}$ (see [**6**]), and to this inclusion of lattices there corresponds an isogeny of the Jacobian of $F(N)$ onto a product of abelian varieties. The purpose of this paper is to determine when two factors in this product are isogenous over $\mathbf{C}$, and whether they are absolutely simple.

Since we shall view abelian varieties as complex tori and shall work exclusively with the lattices $L_{r,s}$, it will be convenient to say that a lattice L is simple (rather than that $\mathbf{C}^d/L$ is simple) or that L and L' are isogenous (rather than that $\mathbf{C}^d/L$ and $\mathbf{C}^d/L'$ are isogenous).

We begin by recalling the definition of the lattices $L_{r,s}$. Given a pair of integers (r, s) with $1 \leqq r, s$ and $r + s \leqq N - 1$, let M be the integer defined by

$$N/M = \text{g.c.d.}(N, r, s).$$

Let $\langle a \rangle$ denote the unique representative of a modulo N between 0 and $N - 1$, and let $H_{r,s}$ be the subset of $(\mathbf{Z}/M\mathbf{Z})^*$ of all elements h such that

$$\langle hr \rangle + \langle hs \rangle \leqq N - 1.$$

Then $H_{r,s}$ is a set of coset representatives for $\{-1, 1\}$ in $(\mathbf{Z}/M\mathbf{Z})^*$. Making the usual identification of $(\mathbf{Z}/M\mathbf{Z})^*$ with Gal $(\mathbf{Q}(e^{2i\pi/M})/\mathbf{Q})$,

$$h \mapsto \sigma_h, \quad \text{where } \sigma_h(e^{2\pi i/M}) = e^{2\pi h i/M},$$

we define $L_{r,s}$ as the lattice in $\mathbf{C}^{\varphi(M)/2}$ consisting of all vectors

$$(\cdots, \sigma_h(z), \cdots)_{h \in H_{r,s}}$$

where z runs through the integers of $\mathbf{Q}(e^{2\pi i/M})$.

Observe that

$$H_{r,s} = hH_{\langle hr \rangle, \langle hs \rangle}$$

for any h in $H_{r,s}$. Consequently, since we have not prescribed an ordering on $H_{r,s}$, we have

$$L_{r,s} = L_{\langle hr \rangle, \langle hs \rangle}.$$

Received June 28, 1977.

Now the period lattice of $F(N)$ (relative to a suitable basis for the holomorphic differentials) is contained with finite index in the product

$$\prod_{[r,s]} L_{r,s}$$

taken over equivalence classes of pairs (r, s) with $1 \leqq r, s$ and $r + s \leqq N - 1$. The equivalence relation is

$$(r, s) \approx (\langle hr \rangle, \langle hs \rangle)$$

for h in $H_{r,s}$. The observation of the preceding paragraph shows that this product over equivalence classes is well-defined. In what follows, when we consider the simplicity of $L_{r,s}$ or the existence of isogenies between $L_{r,s}$ and $L_{r',s'}$, we allow ourselves to replace (r, s) by any member of its equivalence class. In particular, if g.c.d. $(r, N) = 1$, we may assume that the pair is actually $(1, s)$.

To determine when $L_{r,s}$ is simple, we use a criterion of Shimura-Taniyama [**7**]: Let

$$W_{r,s} = \{w \in (\mathbf{Z}/M\mathbf{Z})^* : wH_{r,s} = H_{r,s}\}.$$

Then $W_{r,s}$ is a subgroup of $(\mathbf{Z}/M\mathbf{Z})^*$, and $L_{r,s}$ is simple if and only if $W_{r,s} = \{1\}$. Suppose $W_{r,s} \neq \{1\}$. Then $L_{r,s}$ is isogenous to a product of $|W_{r,s}|$ isomorphic simple factors, where $|W_{r,s}|$ is the cardinality of $W_{r,s}$. These factors have complex multiplication by an order of the fixed field of $W_{r,s}$ and CM-type equal to $H_{r,s}/W_{r,s}$ (viewed as a subset of the Galois group of the fixed field of $W_{r,s}$ over $\mathbf{Q}$).

If g.c.d. $(r, s, N) =$ g.c.d. (r', s', N) and $H_{r,s} = hH_{r',s'}$ for some h in $(\mathbf{Z}/N\mathbf{Z})^*$, then $L_{r,s}$ and $L_{r',s'}$ are identical lattices. On the other hand, suppose $L_{r,s}$ and $L_{r',s'}$ are isogenous. Then the CM-types of their simple factors must be the same up to an automorphism of the field of complex multiplication, so that $hH_{r,s} = H_{r',s'}$ for some h in $(\mathbf{Z}/N\mathbf{Z})^*$.

From now on we shall introduce a superfluous t into our notation, writing $H_{r,s,t}$ instead of $H_{r,s}$, where $r + s + t = N$. The point of this is the following: One verifies immediately that for any h in $(\mathbf{Z}/M\mathbf{Z})^*$ (where $N/M =$ g.c.d. (r, s, N)) either

$$\langle hr \rangle + \langle hs \rangle + \langle ht \rangle = N \quad \text{or} \quad \langle hr \rangle + \langle hs \rangle + \langle ht \rangle = 2N$$

and that $H_{r,s} = H_{r,s,t}$ is the set of those h for which

$$\langle hr \rangle + \langle hs \rangle + \langle ht \rangle = N.$$

Consequently, $H_{r,s,t}$ depends on $\{r, s, t\}$ only up to permutation, so that if ρ is a permutation of $\{r, s, t\}$, then

$$L_{r,s,t} = L_{\rho r, \rho s, \rho t}.$$

In addition, for any $h \in H_{r,s,t}$ we have

$$L_{r,s,t} = L_{\langle hr \rangle, \langle hs \rangle, \langle ht \rangle}.$$

Thus it is natural to define an *equivalence* $\{r, s, t\} \sim \{r', s', t'\}$ if and only if there exists $h \in (\mathbf{Z}/N\mathbf{Z})^*$ such that, up to a permutation, we have

$$\{r', s', t'\} = \{\langle hr\rangle, \langle hs\rangle, \langle ht\rangle\}.$$

Remark. This is a weaker equivalence relation than the one mentioned previously, when no permutation was allowed. Only this new equivalence will play a role from now on, in determining isogeny classes of lattices.

The equality of lattices $L_{r,s,t}$ resulting from an equivalence of triples will be called an *obvious equality*, or *obvious isogeny.*

THEOREM 1. *Suppose N is prime to 6. Then:*
(i) $H_{r,s,t} = H_{r',s',t'}$ *if and only if* $\{r, s, t\} \sim \{r', s', t'\}$.
(ii) *The only isogenies between the lattices $L_{r,s,t}$ are the obvious equalities.*

It is clear that (ii) follows from (i). Most of the rest of the paper is devoted to proving (i).

The same combinatorial result will allow us to determine when a lattice $L_{r,s,t}$ is simple. For if w is in $W_{r,s,t}$, then

$$H_{r,s,t} = wH_{r,s,t} = H_{\langle w^{-1}r\rangle,\langle w^{-1}s\rangle,\langle w^{-1}t\rangle}$$

so that

$$\{r, s, t\} = \{\langle w^{-1}r\rangle, \langle w^{-1}s\rangle, \langle w^{-1}t\rangle\}.$$

If at least one of $rM/N, sM/N, tM/N$ is prime to M (where $N/M = \text{g.c.d.}(r, s, t, N)$) then one deduces that for $w \neq 1$, either

$$1 + w + w^2 = 0 \quad \text{in } \mathbf{Z}/M\mathbf{Z}$$

or

$$w^2 = 1 \quad \text{in } \mathbf{Z}/M\mathbf{Z}.$$

It follows that after multiplying by an element of $(\mathbf{Z}/N\mathbf{Z})^*$, we have

$$\{r, s, t\} = \{N/M, \langle wN/M\rangle, \langle w^2N/M\rangle\}$$

or

$$\{r, s, t\} = \{N/M, \langle wN/M\rangle, \langle -(1 + w)N/M\rangle\}$$

respectively. On the other hand, suppose rM/N, sM/N, tM/N each have a common factor with M. Then necessarily

$$\langle w^{-1}r\rangle = r, \ \langle w^{-1}s\rangle = s, \ \langle w^{-1}t\rangle = t,$$

whence $w \equiv 1 \bmod M$. Hence $L_{r,s,t}$ is simple. To summarize:

THEOREM 2. *Suppose N is prime to 6. The only lattices $L_{r,s,t}$ which are not simple are those for which $\{r, s, t\}$ is equivalent to a triple of the form*

$$\{N/M, \langle wN/M\rangle, \langle w^2N/M\rangle\},$$

for some divisor M of N, and some $w \in \mathbf{Z}/M\mathbf{Z}$ such that $1 + w + w^2 = 0$, or to a triple of the form

$$\{N/M, \langle wN/M\rangle, \langle -(1 + w)N/M\rangle\},$$

for some divisor M of N, and some $w \in \mathbf{Z}/M\mathbf{Z}$ such that $w^2 = 1$, $w \neq \pm 1$. In particular, if N equals a prime p, then all the factors $L_{r,s,t}$ are simple if $p \equiv 2 \bmod 3$, and all but two are simple if $p \equiv 1 \bmod 3$.

When N is not prime to 6, the situation is more complicated. To illustrate this, we shall prove:

THEOREM 3. *Suppose $N = 3^n$. Then the only isogenies apart from the obvious ones are between pairs of lattices corresponding to the triples*

$$(3^m, 3^{n-1} - 2(3^m), 2(3^{n-1}) + 3^m) \text{ and } (3^{m+1}, 3^{n-1} - 2(3^m), 2(3^{n-1}) - 3^m)$$

for $0 \leqq m \leqq n - 2$.

THEOREM 4. *Suppose $N = 2^n$. Then the only isogenies apart from the obvious ones are between pairs of lattices corresponding to the triples*

a) $(2^m, 2^{n-1} - 2^{m+1}, 2^{n-1} + 2^m)$ *and* $(2^{m+1}, 2^{n-2} - 2^m, 3(2^{n-2}) - 2^m)$

for $0 \leqq m \leqq n - 3$, or

b) $(2^m, 2^{n-1} - 2^{m+1}, 2^{n-1} + 2^m)$ *and* $(2^{m+1}, 2^{n-2} - 2^m, 3(2^{n-2}) - 2^m)$

for $0 \leqq m \leqq n - 3$, or

c) $(2^m, 2^m, 2^n - 2^{m+1})$ *and* $(2^{m+1}, 2^{n-1} - 2^m, 2^{n-1} - 2^m)$

for $0 \leqq m \leqq n - 2$, or

d) $(2^m, 3(2^m), 2^n - 2^{m+2})$ *and* $(2^{n-1} - 2^m, 2^{n-1} - 2^{m+1}, 3(2^m))$

for $0 \leqq m \leqq n - 4$, or

e) $(2^m, 2^{n-1}, 2^{n-1} - 2^m)$ *and* $(2^m, 2^m, 2^n - 2^{m+1})$

for $0 \leqq m \leqq n - 2$.

Furthermore, a lattice of type $a)_m$ is isogenous to the product of two lattices of type $e)_{m+1}$.

Finally, we note that Theorems 1 through 4 may equally well be interpreted as statements about when two Stickelberger elements are distinct. The Stickelberger elements referred to here are the elements

$$\Theta_{r,s,t} = \sum \left(\frac{\langle hr\rangle + \langle hs\rangle + \langle ht\rangle}{N} - 1\right)\sigma_{-h}^{-1}$$

of $\mathbf{Z}[\text{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q}]$, see [**2**] or [**5**]; the classical Stickelberger relations show that $\Theta_{r,s,t}$ annihilates the ideal class group of $\mathbf{Q}(\zeta)$. For distinct triples (r, s, t) and (r', s', t'), the preceding theorems give conditions under which $\Theta_{r,s,t}$ and

$\Theta_{r',s,'t'}$ are or are not essentially distinct—essentially distinct means that we do not have

$$\Theta_{r,s,t} = \sigma\Theta_{r',s',t'}$$

for some σ in Gal $(\mathbf{Q}(\zeta)/\mathbf{Q})$.

2. The relatively prime case when N is prime to six. We must show that if N is prime to 6 and $H_{r,s,t} = H_{r',s',t'}$ then $\{r, s, t\} = \{r', s', t'\}$. Without loss of generality, we may assume that g.c.d. $(N, r, s, t) = 1$, whence $M = N$. In this section we shall assume in addition that

$$(r, N) = (s, N) = (t, N) = 1 \quad \text{(``the relatively prime case'')};$$

in subsequent sections the remaining "boundary cases" will be considered.

The statement to be proved can be formulated in the group algebra $\mathbf{Q}[\text{Gal}\ (\mathbf{Q}(e^{2\pi i/N})/\mathbf{Q})]$ as follows: If

$$\sum_{h\in(\mathbf{Z}/N\mathbf{Z})^*} (\langle hr\rangle + \langle hs\rangle + \langle ht\rangle)\sigma_h = \sum_{h\in(\mathbf{Z}/N\mathbf{Z})^*} (\langle hr'\rangle + \langle hs'\rangle + \langle ht'\rangle)\sigma_h$$

then $\{r, s, t\} = \{r', s', t'\}$ up to a permutation. Equivalently, we can define, for any $r \in (\mathbf{Z}/N\mathbf{Z})^*$,

$$G(r) = \sum_{h\in(\mathbf{Z}/N\mathbf{Z})^*} B_1(hr)\sigma_h, \quad \text{where } B_1(a) = \frac{\langle a\rangle}{N} - \frac{1}{2}.$$

Then the statement becomes: If

$$(*) \qquad G(r) + G(s) + G(t) = G(r') + G(s') + G(t')$$

then $\{r, s, t\} = \{r', s', t'\}$ up to a permutation.

We shall now follow an idea of Carlitz-Olson [**1**] to prove this statement. Assuming the truth of (*), let us apply a character

$$\chi : \text{Gal}\ (\mathbf{Q}(e^{2\pi i/N})/\mathbf{Q}) \rightarrow \mathbf{C}^*$$

to both sides of the equation. We get

$$B_{1,\chi}\bar{\chi}(r) + B_{1,\chi}\bar{\chi}(s) + B_{1,\chi}\bar{\chi}(t) = B_{1,\chi}\bar{\chi}(r') + B_{1,\chi}\bar{\chi}(s') + B_{1,\chi}\bar{\chi}(t')$$

where $B_{1,\chi}$ is the generalized Bernoulli number

$$B_{1,\chi} = \sum_h B_1(h)\chi(h).$$

If $B_{1,\chi}$ does not equal 0, we get

$$\bar{\chi}(r) + \bar{\chi}(s) + \bar{\chi}(t) - \bar{\chi}(r') - \bar{\chi}(s') - \bar{\chi}(t') = 0.$$

Let us now consider exclusively *odd* characters χ, i.e. those for which $\chi(-1) = -1$. Such a character χ may be written $\chi = \chi_0\psi$, where ψ is an *even* character and χ_0 is a fixed odd character chosen once and for all. Then the above equation may be rewritten

$$\bar{\chi}_0(r)\bar{\psi}(r) + \bar{\chi}_0(s)\bar{\psi}(s) + \bar{\chi}_0(t)\bar{\psi}(t) - \bar{\chi}_0(r')\bar{\psi}(r') - \bar{\chi}_0(s')\bar{\psi}(s') - \bar{\chi}_0(t')\bar{\psi}(t') = 0$$

for any even character ψ such that $B_{1,\chi_0\psi} \neq 0$. In other words, we have a relation of linear dependence between the six row vectors v_a, $a = r, s, t, r', s', t'$, where

$$v_a = (\cdots, \bar{\psi}(a), \cdots)_{\psi \in S},$$

with S the set of even characters ψ such that $B_{1,\chi_0\psi} \neq 0$. Now if N is a prime power, then S is the set of all even characters, hence by the independence of characters we must have

$$\{r, s, t\} = \{\langle \pm r' \rangle, \langle \pm s' \rangle, \langle \pm t' \rangle\}.$$

Since $\langle r' \rangle + \langle -r' \rangle = N$, and similarly for s', t', we conclude that

$$\{r, s, t\} = \{r', s', t'\}.$$

Thus if N is a prime power, the desired statement is an immediate consequence of the linear independence of the $G(r)$ for $1 \leqq r < p^n/2$, $(r, p) = 1$. The reader interested only in this case need proceed no further. Unfortunately, for composite N the set S is smaller than the set of all even characters, so that the linear dependence of the vectors v_a does not give an immediate contradiction. However, we have the following lemma:

LEMMA. *Let G be an abelian group, S a subset of $\hat{G}$, T a subset of G. If*

$$|S| > \frac{|T| - 1}{|T|} |G|$$

then the rows of

$$(\psi(g))_{g \in T, \psi \in S}$$

are linearly independent.

Proof. Assuming the contrary, let

$$\sum_{g \in T} a_g \psi(g) = 0 \quad \text{for all } \psi \text{ in } S$$

be a nontrivial relation of linear dependence and choose g_0 such that

$$|a_{g_0}| \geqq |a_g| \quad \text{for all } g \in T.$$

Then if we multiply

$$a_{g_0}\psi(g_0) = -\sum_{\substack{g \in T \\ g \neq g_0}} a_g \psi(g)$$

by $\psi(g_0)^{-1}$ and sum over all ψ in S, we get

$$a_{g_0}|S| = -\sum_{\substack{g\in T\\ g\neq g_0}} a_g \sum_{\psi\in S} \psi(g)\psi(g_0)^{-1}$$
$$= \sum_{\substack{g\in T\\ g\neq g_0}} a_g \sum_{\psi\notin S} \psi(g)\psi(g_0)^{-1}$$

by the orthogonality relations. Hence

$$|a_{g_0}|\ |S| \leqq \sum_{\substack{g\in T\\ g\neq g_0}} |a_g|(|G| - |S|) \leqq |a_{g_0}|(|T| - 1)(|G| - |S|)$$

whence

$$|S| \leqq \frac{|T| - 1}{|T|}|G|,$$

a contradiction.

We apply the lemma by letting $G = (\mathbf{Z}/N\mathbf{Z})^*/\pm 1$, S be the set of even characters ψ such that $B_{1,\chi_0\psi} \neq 0$, and T be the set consisting of r, s, t, r', s', t', viewed as elements of $(\mathbf{Z}/N\mathbf{Z})^*/\pm 1$. But first we must know that

$$|S| > (5/6)|G|,$$

i.e. we must know that for more than five-sixths of the odd characters χ of $(\mathbf{Z}/N\mathbf{Z})^*$, $B_{1,\chi} \neq 0$. This is what we turn to now.

Remark. The map

$$G : \mathbf{Z}/N\mathbf{Z} \rightarrow \mathbf{Q}[\mathrm{Gal}\ (\mathbf{Q}(\zeta)/\mathbf{Q})]$$
$$r \mapsto G(r)$$

extends uniquely to a map of vector spaces

$$G : \mathbf{Q}[\mathbf{Z}/N\mathbf{Z}] \rightarrow \mathbf{Q}[\mathrm{Gal}\ (\mathbf{Q}(\zeta)/\mathbf{Q})]$$

and it is easy to verify that G is an "odd distribution", i.e. that it satisfies the relations

1) $\displaystyle\sum_{j=0}^{M-1} G\left(r + \frac{N}{M}j\right) = G(Mr)$ and

2) $G(-r) = -G(r)$

for any r in $\mathbf{Z}/N\mathbf{Z}$ and M dividing N. Furthermore, it is a fact (see [**4**]) that *all* relations satisfied by G are a consequence of relations 1) and 2) above. In particular, to show that the relation

$$G(r) + G(s) + G(t) = G(r') + G(s') + G(t')$$

does not hold, one need only show that it does not follow from 1) and 2) above. However, we have not been able to get from this line of argument a proof which is simpler than the present one.

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

TABLE 1

All primes $\geqq 5$ dividing $p^m - 1$ for certain p and m

$m \backslash p$	5	7	11	13	17	19	23	29
1	—	—	5	—	—	—	11	7
2	—	—	5	7	—	5	11	5,7
3	31	19	5,7,19	61	307	127	7,11,79	7,13,67
4	13	5	5,61	5,7,17	5,29	5,181	5,11,53	5,7,421
5	11,71	2801	5,3221					
6	7,31	19,43	5,7,19,37					
7	19531	29,4733						
8	13,313	5,1201						
9	19,31,829	19,37,1063						

PROPOSITION. *Suppose* $2, 3 \nmid N$. *Let* $S(N)$ *be the set of odd characters of* $(\mathbf{Z}/N\mathbf{Z})^*$, *and let* $S_0(N) \subset S(N)$ *be the set of "bad" characters, i.e.,*

$$S_0(N) = \{\chi \in S(N) | B_{1,\chi} = 0\}.$$

Then $\#S_0(N) < \frac{1}{6}\#S(N)$.

Proof. For $\chi \in S(N)$ let $N_0|N$ be the conductor of χ, and let χ_0 be the character mod N_0 which induces χ. Then

$$B_{1,\chi} = B_{1,\chi_0} \prod_{p|N} (1 - \chi_0(p)).$$

Thus $\chi \in S_0(N)$ if and only if there exists $p|N/N_0$ such that $\chi_0(p) = 1$. Let

$$N = \prod_{i=1}^{m} p_i^{\alpha_i}$$

be the prime factorization. Let $N_i = N/p_i^{\alpha_i}$, and let ord_i denote the order of p_i in $(\mathbf{Z}/N_i\mathbf{Z})^*$. If $\chi \in S_0(N)$, then for some i the corresponding χ_0 must be an odd character mod N_i such that $\chi_0(p_i) = 1$. For fixed i, the number of such χ_0 is

$$\begin{cases} 0 & \text{if } p_i \text{ is a root of } -1 \text{ mod } N_i, \\ \#((\mathbf{Z}/N_i\mathbf{Z})^*/\{\pm p_i^{\,j}\}) = \dfrac{\varphi(N_i)}{2\,\text{ord}_i}, & \text{otherwise.} \end{cases}$$

Thus,

$$s(N) \underset{\text{def}}{=} \frac{\#S_0(N)}{\#S(N)} \leqq \sum_{i=1}^{m} \frac{1}{\varphi(p_i^{\alpha_i})\,\text{ord}_i}.$$

We claim that this sum is $< \frac{1}{6}$. It clearly suffices to prove this when all $\alpha_i = 1$. So suppose N is a product of m distinct primes,

$$N = \prod_{i-1}^{m} p_i, \quad 5 \leqq p_1 < p_2 < \cdots < p_m.$$

Note that $\text{ord}_i > \log_{p_i} N_i \geqq m - i$. Thus

(1) $\quad \text{ord}_i \geqq m + 1 - i.$

Also,

(2) $\quad \text{ord}_m = 1 \quad \text{only if } p_m \geqq 2 \prod_{i<m} p_i + 1.$

Case 1. $m = 2$, $s(N) = \dfrac{1}{(p_1 - 1)\,\text{ord}_1} + \dfrac{1}{(p_2 - 1)\,\text{ord}_2}$.

By Table 1, if $p_i = 5$ or 7, then $\text{ord}_i \geqq 3$ with equality only if $p_2 = 31$ or 19. If $p_1 \geqq 11$, then $(p_1 - 1)\,\text{ord}_1 \geqq 20$ by (1). Thus in either case

$$s(N) \leqq \frac{1}{(5-1)\cdot 3} + \frac{1}{p_2 - 1} \leqq \frac{1}{6} \quad \text{if } p_2 \geqq 13 \text{ (with at least one} \leqq \text{strict).}$$

For the remaining case $p_1 = 5, p_2 = 11 : s(55) = 1/4.5 + 1/10 = 3/20 < 1/6$.

Case 2. $m = 3$.

If $p_i = 5$ or 7, then for $j < 5$ Table 1 shows that $p_i^j - 1$ is not divisible by two distinct primes $\geqq 5$. Hence $\text{ord}_i \geqq 5$ and $(p_i - 1)\,\text{ord}_i \geqq 20$. If $p_i \geqq 11$, then by (1) and (2) also $(p_i - 1)\,\text{ord}_i \geqq 20$. Thus $s(N) \leqq 3/20 < 1/6$.

Case 3. $m = 4$.

If $p_i = 5$ or 7, then $\text{ord}_i \geqq 9$ by Table 1. This, together with (1) and (2), gives:

$$\frac{1}{(p_1 - 1)\,\text{ord}_1} \leqq \frac{1}{4\cdot 9}, \quad \frac{1}{(p_2 - 1)\,\text{ord}_2} \leqq \frac{1}{10.3}, \quad \frac{1}{(p_3 - 1)\,\text{ord}_3} \leqq \frac{1}{10.2},$$
$$\frac{1}{(p_4 - 1)\,\text{ord}_4} \leqq \frac{1}{12.2},$$

and so

$$\sum \frac{1}{(p_i - 1)\,\text{ord}_i} < \frac{1}{6}.$$

Case 4. $5 \leqq m \leqq 9$.

From Table 1, if $p_i = 5, 7, 11$, then $\text{ord}_i \geqq 10, 10, 6$, respectively, and if $13 \leqq p_i \leqq 29$, then $\text{ord}_i \geqq 5$. Thus,

$$\frac{1}{(p_i - 1)\,\text{ord}_i} \leqq \begin{cases} \dfrac{1}{4\cdot 10}, & p_i = 5, \\[4pt] \dfrac{1}{6\cdot 10}, & p_i = 7, \\[4pt] \dfrac{1}{10\cdot 6}, & p_i = 11, \\[4pt] \dfrac{1}{12\cdot 5}, & p_i = 13, \cdots, 29, \\[4pt] \dfrac{1}{30\cdot 2}, & p_i \geqq 31. \end{cases}$$

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

Hence,

$$s(N) \leqq \frac{1}{40} + \frac{m-1}{60} < \frac{m+1}{60} \leqq \frac{1}{6}.$$

Case 5. $m \geqq 10$.

We show that for all b_i we have $(p_i - 1)\operatorname{ord}_i > 6m$, which will imply

$$s(N) = \sum_{i=1}^{m} \frac{1}{(p_i - 1)\operatorname{ord}_i} < \frac{1}{6}.$$

(1) $p_i = 5$.

$$\operatorname{ord}_i > \log_5 n/5 \geqq \log_5 (7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41^{m-10}) > 16 + 5(m - 10)/2 > 3m/2,$$

so that $(p_i - 1)\operatorname{ord}_i > 4 \cdot 3m/2 = 6m$.

(2) $p_i = 7$.

$$\operatorname{ord}_i > \log_7(5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41^{m-10}) > 13 + 3(m - 10)/2 > m,$$

so that $(p_i - 1)\operatorname{ord}_i > 6m$.

(3) $p_i = 11$.

$$(p_i - 1)\operatorname{ord}_i \geqq 10(m - 2) > 6m \quad \text{by} \quad (1).$$

(4) $13 \leqq p_i \leqq 3m/2 + 1$.

There are clearly no more than $m/2 - 1$ primes p with $5 \leqq p \leqq 3m/2 - 1$. (This holds for $m = 10, 11, 12, 13$, and for $m + 4$ whenever it holds for m, since any sequence of 6 consecutive integers has at most 2 primes.) Since any prime $p < p_i$ must be $\leqq p_i - 2 \leqq 3m/2 - 1$, there are at least $m/2$ primes $> p_i$ among $p_1, \cdots, p_m$. Then

$$\operatorname{ord}_i > \log_{p_i} p_i^{m/2} = m/2,$$

so that $(p_i - 1)\operatorname{ord}_i > 6m$.

(5) $3m/2 + 1 < p_i \leqq 6m + 1$.

If suffices to prove that $\operatorname{ord}_i \geqq 4$. But if $\operatorname{ord}_i \leqq 3$, then $\log_{p_i} n/p_i < 3$, and so $n < p_i^4 \leqq (6m + 1)^4$. But $(6m + 1)^4$ is less than the product of the first m primes starting with 5 as soon as $m \geqq 7$.

(6) $p_i > 6m + 1$.

Then obviously $(p_i - 1)\operatorname{ord}_i > 6m$. This completes the proof.

Remarks. 1. When $N = 55$, $\#S(N) = \frac{1}{2}\varphi(N) = 20$, and $\#S_0(N) = 3$ (namely, $S_0(N)$ consists of: both odd characters mod 5 and the Legendre character mod 11). Thus, $s(55) = 3/20$. It is clear from the above proof that $3/20$ is the maximum for $s(N)$.

It is also clear that

$$\lim_{\substack{N \to \infty \\ 2,3 \nmid N}} s(N) = 0.$$

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

2. If N is odd and $3|N$, it can similarly be proved that there are precisely two values of N for which $s(N) \geqq 1/6 : s(21) = 1/6$, $s(39) = 1/4$. For all other values of N, it thus follows that there can be no non-obvious isogenies between $J_{r,s,t}$ and $J_{r',s',t'}$ if r, s, t, r', s', t' are *all* prime to N. However, there *are* non-obvious isogenies in the boundary cases if $3|N$.

When $N = 21$, 39, the non-obvious isogenies in the relatively prime case all turn out to occur when $J_{r,s,t}$ is isogenous to a product of elliptic curves. In each case we can take (r, s, t) to be $(1, \rho, \langle \rho^2 \rangle)$ where ρ is a cube root of 1 mod N. For $N = 21$, $J_{1,4,16}$ is isogenous to the product of 6 copies of the same elliptic curve that occurs for $N = 7$ and the triple $(1, 2, 4)$. (Recall that if N is a prime $\equiv 1 \bmod 3$, then $J_{1,\rho,\langle\rho^2\rangle}$ splits up into 3 curves of genus $(N - 1)/6$.) For $N = 39$, $J_{1,16,22}$ is isogenous to a product of 12 copies of an elliptic curve that does *not* occur as a simple factor for prime N.

It would be interesting to understand more directly why, if τ and τ' are triples all of whose components are prime to N, then J_τ and $J_{\tau'}$ can only be isogenous when they split into a product of elliptic curves.

It is unclear to us why the "relatively prime case" should be so different from the "boundary cases."

3. The boundary cases when N is prime to six. To prove Theorem 1, it remains to establish the following proposition.

PROPOSITION. *Let* $2, 3 \nmid N$, $\tau = (r, s, t)$, $\tau' = (r', s', t')$, $r + s + t = N$. *Suppose* g.c.d. $(r, s, t, r', s', t') = 1$. *Let*

$$H_\tau = \{h \in (\mathbf{Z}/N\mathbf{Z})^* | \langle hr \rangle + \langle hs \rangle + \langle ht \rangle = N\}.$$

and similarly for $H_{\tau'}$. Suppose N is not prime to $rstr's't'$. In the case that $r = r'$ for some ordering of the triples τ and τ', suppose further that N is not prime to $sts't'$. Finally, suppose $H_\tau = H_{\tau'}$.

Then τ' is a permutation of τ.

Proof. Case 1. g.c.d.$(r, s, t, N) > 1$.

Let $p|$g.c.d.(r, s, t, N), $p \geqq 5$. Let $P = 1 + (N/p)(\mathbf{Z}/b\mathbf{Z})$, $P^* = P \cap (\mathbf{Z}/N\mathbf{Z})^*$, $\nu = \#(P \backslash P^*)$. Then

$$\nu = \begin{cases} 0 & \text{if } p^2|N \\ 1 & \text{if } p^2 \nmid N. \end{cases}$$

Since $\langle ur \rangle = r$, $\langle us \rangle = s$, $\langle ut \rangle = t$ for $u \in P$, we have:

$$P^* \subset H_\tau = H_{\tau'}.$$

Thus

$$\sum_{u \in P^*} \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle = (p - \nu)N.$$

Since $\langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle = N$ or $2N$ for $u \in P\backslash P^*$, we have

$$(3)\qquad \sum_{u\in P} \langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle \leqq (p-\nu)N.$$

Let $r_0' = \langle r'\rangle_{N/p}$, $s_0' = \langle s'\rangle_{N/p}$, $t_0' = \langle t'\rangle_{N/p}$, where for any positive integer M we let $\langle\quad\rangle_M$ denote least non-negative residue mod M. For x prime to p, note that $\langle ux\rangle$ runs through $\langle x\rangle_{N/p} + iN/p$, $i = 0, 1, \cdots, p-1$, as u runs through P.

First suppose $p \nmid r', s', t'$. Then

$$\sum_{u\in P} \langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle = p(r_0' + s_0' + t_0') + 3N/p \sum_{i=0}^{p-1} i$$

$$\geqq pN/p + 3\frac{p-1}{2}N = pN + \frac{p-1}{2}N,$$

because $r_0' + s_0' + t_0' = N/p$ or $2N/p$. This contradicts (3) because $(p-1)/2 \geqq 2 > \nu$.

Now suppose, say, $p|r'$. Since g.c.d.$(r, s, t, r', s', t') = 1$, we then have $p \nmid s', t'$. Note that if τ and τ' are replaced by $u_0\tau = (\langle u_0r\rangle, \langle u_0s\rangle, \langle u_0t\rangle)$ and $u_0\tau'$, where $u_0 \in (\mathbf{Z}/N\mathbf{Z})^*$, the assumptions of the proposition remain valid, except that $\langle u_0r\rangle + \langle u_0s\rangle + \langle u_0t\rangle$ will equal $2N$ instead of N if $u_0 \notin H_\tau$. In that case (3) can be replaced by

$$(4)\qquad \sum_{u\in P} \langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle \geqq (2p-\nu)N.$$

Since $p|r'$, we have

$$\sum_{u\in P} \langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle = p(r' + s_0' + t_0') + 2N/p \sum_{i=0}^{p-1} i$$

$$= pr' + p(s_0' + t_0') + (p-1)N.$$

We claim that τ' can be modified by a suitable $u_0 \in (\mathbf{Z}/N\mathbf{Z})^*$ so that

$$(p+\nu)N < pr' + p(s_0' + t_0') + (p-1)N < (2p-\nu)N,$$

contradicting (3) and (4). Since $0 < s_0' + t_0' < 2N/p$, we would like r' to satisfy

$$(\nu+1)N/p \leqq r' \leqq N - (\nu+1)N/p.$$

It clearly suffices if $2N/5 \leqq r' \leqq 3N/5$.

Let $x =$ g.c.d.(r', N), $y = N/x$, $\beta = [\log_2 y/\sqrt{2}]$. Then $y/2\sqrt{2} < 2^\beta < y/\sqrt{2}$. Note that $\beta \geqq 1$, since $y \geqq 5$. If $2^\beta < 2y/5$, then $3 \cdot 2^{\beta-1}$ is $<3y/5$ and $>(3/2)(y/2\sqrt{2}) > 2y/5$. If $2^\beta > 3y/5$ (in which case note that $\beta \geqq 2$), then $3 \cdot 2^{\beta-2}$ is $>(3/4)\cdot(3y/5) > 2y/5$ and $<(3/4)(y/\sqrt{2}) < 3y/5$. Now let $u_1 \in (\mathbf{Z}/N\mathbf{Z})^*$ equal either 2^β, $3\cdot 2^{\beta-1}$, or $3\cdot 2^{\beta-2}$, so that $2y/5 \leqq u_1 \leqq 3y/5$.

Then if $u_0 = u_1(r'/x)^{-1} \in (\mathbf{Z}/N\mathbf{Z})^*$, we have

$$2N/5 \leqq \langle u_0 r' \rangle \leqq 3N/5,$$

as required.

Case 2. There exists a prime p dividing N, r, r' but not dividing $sts't'$; and $r \neq r'$.

We need the following simple lemma, whose proof is straightforward and will be omitted.

LEMMA. *Let* $2, 3 \nmid N$, $1 \leqq x, y < N$, $x \neq y$, $p|N$. *Then there exists* $u \in (\mathbf{Z}/N\mathbf{Z})^*$ *such that*

$$\left| \left[\frac{\langle uy \rangle}{N/p}\right] - \left[\frac{\langle ux \rangle}{N/p}\right] \right| \geqq \begin{cases} 3 & \text{if } p > 5, \\ 2 & \text{if } p = 5. \end{cases}$$

If $x = 1$, $y \neq 2$, $(N+1)/2$, *and* $5 \nmid N$, *then there exists* $u \in (\mathbf{Z}/N\mathbf{Z})^*$ *such that*

$$\left| \left[\frac{\langle uy \rangle}{N/5}\right] - \left[\frac{\langle ux \rangle}{N/5}\right] \right| \geqq 3.$$

Let P, P^x, ν, r_0', s_0', t_0' be defined as before, $r_0 = \langle r \rangle_{N/p}$, $s_0 = \langle s \rangle_{N/p}$, $t_0 = \langle t \rangle_{N/p}$. Since $H_\tau = H_{\tau'}$, for $u \in P^*$ we have

$$\langle ur \rangle + \langle us \rangle + \langle ut \rangle = \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle.$$

For $u \in P \backslash P^*$ we have

$$|\langle ur \rangle + \langle us \rangle + \langle ut \rangle - (\langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle)| \leqq N.$$

Thus

$$\nu N/p \geqq \frac{1}{p} \left| \sum_{u \in P} \langle ur \rangle + \langle us \rangle + \langle ut \rangle - \sum_{u \in P} \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle \right|$$

$$\nu N/p \geqq |r + s_0 + t_0 - r' - s_0' - t_0'| \tag{5}$$

$$\nu \geqq \left| \left[\frac{r}{N/p}\right] - \left[\frac{r'}{N/p}\right] \right| - \frac{1}{N/p} |r_0 + s_0 + t_0 - (r_0' + s_0' + t_0')|$$

$$\nu + 1 \geqq \left| \left[\frac{r}{N/p}\right] - \left[\frac{r'}{N/p}\right] \right|. \tag{6}$$

First suppose $p > 5$, or $p = 5$ and $p^2|N$ (so that $\nu = 0$). By the lemma applied with $x = r$, $y = r'$, if we multiply through by a suitable $u \in (\mathbf{Z}/N\mathbf{Z})^*$, without loss of generality we may assume that

$$\left| \left[\frac{r}{N/p}\right] - \left[\frac{r'}{N/p}\right] \right| \geqq \nu + 2,$$

which contradicts (6).

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

Now suppose $N = 5N_0$, $5 \nmid N_0$, $5|r, r'$. If there is another prime $p > 5$ with $p|N$ and $p|r$ or $p|r'$, we can use either Case 1 or Case 2 for $p > 5$ above or Case 3 below. So suppose g.c.d. $(N, r) =$ g.c.d.$(N, r') = 5$.

If $r/r' \not\equiv 2^{\pm 1} \bmod N_0$, then we use the above lemma (with N_0, r/r' in place of N, y) to find u prime to N_0 such that

$$3 \leqq \left| \left[\frac{\langle u\, r/r' \rangle_{N_0}}{N_0/5} \right] - \left[\frac{\langle u \rangle_{N_0}}{N_0/5} \right] \right| = \left| \left[\frac{\left\langle \frac{u}{r'/5}\, r \right\rangle}{N/5} \right] - \left[\frac{\left\langle \frac{u}{r'/5}\, r' \right\rangle}{N/5} \right] \right| .$$

Here $r'/5 \in (\mathbf{Z}/N\mathbf{Z})^*$. If $5|u$, replace u by $u + N_0 \in (\mathbf{Z}/N\mathbf{Z})^*$. Thus, we can find $u_0 = 5u/r'$ or $(5u + N)/r'$ prime to N, such that

$$\left| \left[\frac{\langle u_0 r \rangle}{N/5} \right] - \left[\frac{\langle u_0 r' \rangle}{N/5} \right] \right| \geqq 3,$$

which contradicts (6).

It remains to consider the case $r/r' \equiv 2^{\pm 1} \bmod N_0$, say $r \equiv 2r' \bmod N$. Multiplying through by $(r/5)^{-1} \in (\mathbf{Z}/N\mathbf{Z})^*$, we may assume $r = 5$, $r' = (N + 5)/2$. By (5) we have

$$N_0 \geqq |r + s_0 + t_0 - r' - s_0' - t_0'|$$
$$= |r_0 + s_0 + t_0 - r_0' - s_0' - t_0' - 2N_0|.$$

Thus,

$$(7) \qquad r_0 + s_0 + t_0 = 2N_0, \quad r_0' + s_0' + t_0' = N_0.$$

Say $\tau = (5, iN_0 - a, jN_0 - b)$, where $a, b > 0$, $a + b = 5$. Multiplying through by a suitable $u \in P^*$, without loss of generality we may assume $\tau = (5, N - a, N - b)$ (namely, if $iN_0 - a \equiv k \bmod 5$, let $u = \langle -i/k \rangle_5 N_0 + 1$). Since $2 \notin H_\tau = H_\tau'$, and $\langle 2r' \rangle = 5$, we must have $2\tau' = (5, N - a', N - b')$, where $a', b' > 0$, $a' + b' = 5$. Say a' is even. Then $\tau' = ((N + 5)/2, N - a'/2, (N - b')/2)$, and $r_0' + s_0' + t_0' = 2N_0$, contradicting (7).

Case 3. There exists a prime $p|N, r, p \nmid str's't'$.

Multiplying through by a suitable element of $(\mathbf{Z}/N\mathbf{Z})^*$, without loss of generality we may assume that $r =$ g.c.d.(N, r). Let P, P^*, r_0, s_0, t_0, r_0', s_0', t_0' be defined as in Cases 1 and 2. We have

$$\nu N \geqq \left| \sum_{u \in P} \langle ur \rangle + \langle us \rangle + \langle ut \rangle - \sum_{u \in P} \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle \right|$$
$$= \left| pr + \sum_{i=0}^{p-1} (s_0 + iN/p + t_0 + iN/p - r_0' - iN/p - s_0' - iN/p - t_0' - iN/p) \right|$$
$$= p \left| r + s_0 + t_0 - r_0' - s_0' - t_0' - \frac{p-1}{2} N/p \right| .$$

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

Hence

$$(8)\qquad \nu N/p \geqq \frac{p-1}{2} N/p + r_0' + s_0' + t_0' - r - s_0 - t_0$$

$$> \frac{p-1}{2} N/p + N/p - 2N/p - r,$$

$$(9)\qquad \frac{r}{N/p} > \frac{p-3}{2} - \nu.$$

Let $\alpha = N/r \geqq 5$. If $p \geqq 11$, (9) implies

$$0 < p/\alpha - p/2 + 5/2 \leqq 5/2 - 3p/10 < 0,$$

a contradiction. If $p = 7$ and $\alpha \geqq 7$. then we obtain

$$0 < p/7 - p/2 + 5/2 = 0,$$

again a contradiction.

It remains to consider the case $p = 7$, $\alpha = 5$ and the case $p = 5$. Note that when $\nu = 0$, (9) gives

$$0 < p/\alpha - p/2 + 3/2 \leqq 0$$

for all $\alpha \geqq 5$, $p \geqq 5$. So suppose $p^2 \nmid N$.

First suppose $p = 7$, $\alpha = 5$. If a prime $q > 7$ divides r, we can use Case 1, 2, or 3 with $p = q > 7$ instead of $p = 7$. If $5|r$, so that $5^2|N$, we can use Case 1, 2, or 3 with $p = 5$, $v = 0$. The only remaining case when $p = 7$, $\alpha = 5$, $7^2 \nmid N$ is when $r = 7$, i.e., $N = 35$; this case is easily checked by hand.

We now consider the case $p = 5$, $5^2 \nmid N$. If $r > 5$, there is a prime $q > 5$ dividing r and N, and we can use Case 1, 2, or 3 with $p = q > 5$. So suppose $r = 5$.

By (8),

$$N/5 \geqq 2N/5 + r_0' + s_0' + t_0' - (5 + s_0 + t_0),$$

which is only possible if $r_0' + s_0' + t_0' = N/5$, $5 + s_0 + t_0 = 2N/5$. Thus, $\tau = (5, iN/5 - a, jN/5 - b)$, where $a, b > 0$, $a + b = 5$. Multiplying through by a suitable element in P^*, without loss of generality we may assume that $\tau = (5, N - a, N - b)$.

But for this τ we know $H_\tau \subset (\mathbf{Z}/N\mathbf{Z})^*$ explicitly. Namely, if $h \in (\mathbf{Z}/N\mathbf{Z})^*$, then

$$(10)\qquad h \in H_\tau \quad \Leftrightarrow \quad \left[\frac{\langle h \rangle}{5}\right] + \left[\frac{\langle h \rangle}{a}\right] + \left[\frac{\langle h \rangle}{b}\right] \text{ is odd.}$$

In particular, whether or not $h \in H_\tau$ depends only on $[\langle h \rangle / 5ab]$ (here $5ab = 20$ or 30). By a tedious examination of possible ranges of values for r', s', t', we verified that no $\tau' \neq \tau$ has $H_{\tau'}$ given by (10). This part of the proof will be omitted in the interest of brevity.

This completes the proof of Case 3 of the proposition, and hence of Theorem 1.

4. Isogenies for N a power of 3. Theorem 3 can be restated as follows.

PROPOSITION. *Let* $N = 3^n$, $N_1 = 3^{n-1}$, $\tau = (r, s, t)$, $\tau' = (r', s', t')$, $H_\tau = H_{\tau'}$. *Suppose that* τ' *is not a permutation of* τ, *and that* g.c.d.$(r, s, t, r', s', t') = 1$. *Then for some* $u \in (\mathbf{Z}/N\mathbf{Z})^*$, $u\tau = (\langle ur\rangle, \langle us\rangle, \langle ut\rangle)$ *and* $u\tau'$ *are permutations of* $(1, N_1 - 2, 2N_1 + 1)$ *and* $(3, N_1 - 2, 2N_1 - 1)$.

Proof. Let ord m denote the highest power of 3 that divides an integer m. Without loss of generality, we may suppose ord $r \geqq$ ord $s \geqq$ ord t and ord $r' \geqq$ ord $s' \geqq$ ord t'. Note that then ord $s =$ ord t, ord $s' =$ ord t' and either ord $s = 0$ or ord $s' = 0$. We may suppose ord $s' = 0$.

The proof that $\tau = \tau'$ if $3 \nmid rst\, r's't'$ or if $r = r'$ and $3 \nmid st\, s't'$ is included in the proof of Theorem 1 in the relatively prime case (§ 2).

Case 1. ord $s > 0$.

If $3|r'$, multiply through by a suitable $u \in (\mathbf{Z}/N\mathbf{Z})^*$ so that $N_1 \leqq \langle ur'\rangle \leqq 2N_1$ (namely, let $u = (3^{-\text{ord}\, r'}\, r')^{-1}((3^{-\text{ord}\, r'}\, N - 1)/2)$). Thus, without loss of generality we may suppose

(11) $\quad N_1 \leqq r' \leqq 2N_1 \quad$ if $3|r'$.

Let $P = 1 + N_1(\mathbf{Z}/3\mathbf{Z}) \subset (\mathbf{Z}/N\mathbf{Z})^*$, and let $r_0' = \langle r'\rangle_{N_1}$, $s_0' = \langle s'\rangle_{N_1}$, $t_0' = \langle t'\rangle_{N_1}$. By (3) and (4), we have

$$\sum_{u\in P} \langle ur'\rangle + \langle us'\rangle + \langle ut'\rangle \begin{cases} \leqq 3N & \text{or} \\ \geqq 6N. \end{cases}$$

But if $3 \nmid r'$, this sum equals

$$3N + 3(r_0' + s_0' + t_0') = 4N \quad \text{or} \quad 5N;$$

while if $3|r'$, the sum equals

$$2N + 3(r' + s_0' + t_0'),$$

which by (11) equals $4N$ or $5N$.

We may now suppose $3 \nmid sts't'$. Also suppose ord $r \geqq$ ord r'.

Case 2. $3|r'$ and $r \neq r'$.

Let $m = n -$ ord r', $M = 3^m$, $M_1 = 3^{m-1}$. Letting $P = 1 + M(\mathbf{Z}/3^{\text{ord}\, r'}\,\mathbf{Z})$ and proceeding as in Case 2 of § 3, we obtain (see (6))

(12) $\quad 1 \geqq |[r/M] - [r'/M]|$.

The case $N = 9$ is easily checked by hand; if $m = 1$, $n \geqq 3$, then $3|r/M$, r'/M, contradicting (12). So suppose $m \geqq 2$.

We need a simple lemma, whose proof will be omitted.

LEMMA. *Suppose* $1 \leqq x, y < M$, $x \neq y$, $3 \nmid$ g.c.d.(x, y). *Then there exists* u *prime to* 3 *such that*

$$|\langle uy\rangle_M - \langle ux\rangle_M| > M_1.$$

We apply the lemma with $x = r'/3^{\text{ord } r'}$, $y = r/3^{\text{ord } r'}$. Multiplying through by the u in the lemma, without loss of generality we may assume that $|r - r'| > N_1$. But (12) gives $|r - r'| < 3M \leqq N_1$, a contradiction.

Case 3. $3 \nmid st\, r's't'$, $3^2 | r$.

Multiplying through by $(r/3^{\text{ord } r})^{-1} \in (\mathbf{Z}/N\mathbf{Z})^*$, without loss of generality we may assume that $r = 3^{\text{ord } r}$. Letting $m = n - \text{ord } r$, $M = 3^m$, $P = 1 + M(\mathbf{Z}/3^{\text{ord } r}\mathbf{Z})$, and proceeding as in Case 3 of § 3, we obtain (see (9))

$$\frac{3^{\text{ord } r} - 3}{2} < \frac{r}{M} \leqq \frac{3^{\text{ord } r}}{3},$$

a contradiction.

Case 4. $3 \nmid str'\, s't'$, ord $r = 1$.

Multiplying through by a suitable $u \in (\mathbf{Z}/N\mathbf{Z})^*$, we may assume that $r = 3$. Suppose $\tau = (r, s, t)$ and $\tau' = (r', s', t')$ are arranged so that $s \equiv 1$ ((mod 3), $t \equiv 2 \pmod 3$, $r' \leqq s' \leqq t'$. We have $3 \nmid st\, r'\, s'\, t'$.

Note that $r' \equiv s' \equiv t' \pmod 3$. We claim $r' \equiv 1 \pmod 3$. Let $r' \equiv r_0' \pmod 3$, $r_0' = 1$ or 2. Let $P = 1 + 3(\mathbf{Z}/N_1\mathbf{Z}) \subset (\mathbf{Z}/N\mathbf{Z})^*$. Then

$$\sum_{u \in P} \langle ur \rangle + \langle us \rangle + \langle ut \rangle = \sum_{u \in P} \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle.$$

The sum on the left equals

$$3 \sum_{\substack{k \equiv 3 \bmod 9 \\ 1 \leqq k < N}} k + \sum_{\substack{3 \nmid k \\ 1 \leqq k < N}} k = 9 \sum_{\substack{k \equiv 4 \bmod 9 \\ 1 \leqq k < N}} k.$$

The sum on the right equals

$$3 \sum_{\substack{k \equiv 1 \pmod 3 \\ 1 \leqq k < N}} (k + (r_0' - 1)) = 9 \sum_{\substack{k \equiv 4 \bmod 9 \\ 1 \leqq k < N}} k + (r_0' - 1)N.$$

Hence $r_0' = 1$ as claimed.

Now first suppose that $s' < N_1$. We shall call a triple *admissible* if the sum of its components is N rather than $2N$. Then, since $r' \equiv s' \equiv t' \equiv 1 \pmod 3$, we have

$$(N_1 - 1)\tau' = (N_1 - r', N_1 - s', 4N_1 - t') \text{ is admissible,}$$

i.e., $(N_1 - r') + (N_1 - s') + (4N_1 - t') = N$. Hence $N_1 - 1 \in H_{\tau'} = H_\tau$, and

$$(N_1 - 1)\tau = (N - 3, \langle (N_1 - 1)s \rangle, \langle (N_1 - 1)t \rangle) \text{ is admissible,}$$

in other words $\langle (N_1 - 1)s \rangle + \langle (N_1 - 1)t \rangle = 3$. Since $s \equiv 1 \pmod 3$, $t \equiv 2 \pmod 3$, we have $\langle (N_1 - 1)s \rangle = 2$, $\langle (N_1 - 1)t \rangle = 1$. Hence

$$s = \langle 2/(N_1 - 1) \rangle = N_1 - 2, t = \langle 1/(N_1 - 1) \rangle = 2N_1 - 1.$$

Next suppose that τ is *not* admissible. Then $\tau = (3, \langle -2 \rangle, \langle -1 \rangle)$, and

$(N_1 + 1)\tau = (3, N_1 - 2, 2N_1 - 1)$. Thus we may again obtain $\tau = (3, N_1 - 2, 2N_1 - 1)$ after multiplying through by a suitable $u \in (\mathbf{Z}/N\mathbf{Z})^*$.

Now suppose τ is admissible, and $s' > N_1$. Then we must have $N_1 < s'$, $t' < 2N_1$, and so

$$(2N_1 - 1)(r', s', t') = (2N_1 - r', 2N_1 - s', 2N_1 - t') \text{ is admissible.}$$

Thus,

$$(2N_1 - 1)\tau = (N - 3, \langle(2N_1 - 1)s\rangle, \langle(2N_1 - 1)t\rangle) \text{ is admissible,}$$

which gives

$$s = \langle 2/(2N_1 - 1)\rangle = 2N_1 - 2, \quad t = \langle 1/(2N_1 - 1)\rangle = N_1 - 1.$$

Then $(N_1 + 1)\tau = (3, N_1 - 2, 2N_1 - 1)$.

Thus, after multiplying through by a suitable $u \in (\mathbf{Z}/N\mathbf{Z})^*$, we may assume that $\tau = (3, N_1 - 2, 2N_1 - 1)$. Let $\tau_0 = (1, N_1 - 2, 2N_1 + 1)$; then $H_{\tau_0} = H_\tau = H_{\tau'}$. But $H_{\tau_0} = H_{\tau'}$ implies that τ' is a permutation of τ_0, because all components in τ' and τ_0 are prime to 3 (see beginning of this proof).

5. Isogenies for N a power of 2. Theorem 4 can be restated as follows.

PROPOSITION. *Let $N = 2^n$, $n \geqq 4$. Let $N_1 = 2^{n-1}$, $N_2 = 2^{n-2}$, $\tau = (r, s, t)$, $\tau' = (r', s', t')$, $H_\tau = H_{\tau'}$. Suppose that τ' is not a permutation of τ, and that* g.c.d.$(r, s, t, r', s', t') = 1$. *Then for some $u \in (\mathbf{Z}/N\mathbf{Z})^*$, $u\tau$ and $u\tau'$ are permutations of one of the following pairs of triples:*

(1) $(N - 4, 1, 3)$, $(N_1 - 2, N_1 - 1, 3)$;

(2) *any* 2 *of the triples* $(N - 2, 1, 1)$, $(N_1, 1, N_1 - 1)$, $(2, N_1 - 1, N_1 - 1)$;

(3) *any* 2 *of the triples* $(N - 4, 2, 2)$, $(N_1, 2, N_1 - 2)$, $(N_1 - 2, 1, N_1 + 1)$, $(2, N_2 - 1, 3N_2 - 1)$.

Proof. Most of the proof is similar to the proof of Theorem 2, and will be omitted. However, one case is somewhat harder. When $N = 2^n$, there is no "relatively prime case" when $rst\, r'\, s'\, t'$ is prime to N (since at least one component in a triple must be even). Instead, the "relatively prime case," in which divisibility is least possible, occurs when, say, $2|r, r'$; $4 \nmid r, r'$; $2 \nmid st\, s't'$. Since it does not seem to be possible to apply the Frobenius determinant formula to this situation, our proof of the "relatively prime case" when $N = 2^n$ needs another technique, based on a probabilistic consideration.

Let (r, s, t), (r', s', t') fall in the "relatively prime case," i.e., $2|r, r'$, $4 \nmid r, r'$, $2 \nmid st\, s't'$. Multiplying through by $s^{-1} \in (\mathbf{Z}/N\mathbf{Z})^*$, we may suppose that $s = 1$.

If $t = N_1 + 1$, then $\tau = (N_1 - 2, 1, N_1 + 1)$, $H_\tau = \{\text{odd } j | 0 < j < N_2 \text{ or } N_1 < j < 3N_2\}$. Then for all $u \in (\mathbf{Z}/N\mathbf{Z})^*$ we have:

$$\langle u\rangle \in H_{\tau'} \quad \Leftrightarrow \quad \langle u + N_1\rangle \in H_{\tau'}.$$

Since $\langle(u + N_1)r'\rangle = \langle ur'\rangle$, $\langle(u + N_1)s'\rangle = \langle us' + N_1\rangle$, $\langle(u + N_1)t'\rangle =$

$\langle ut' + N_1 \rangle$, this means that exactly one of $\langle us' \rangle$, $\langle ut' \rangle$ is $< N_1$. Then for all $u < N_1$: $\langle u(t'/s' + N_1) \rangle < N_1$. By Sublemma 1 below, $t' = \langle -s' \rangle$ or $\langle N_1 + s' \rangle$. But $t' \not\equiv \langle -s' \rangle$. Hence $\tau' = s'(N_1 - 2, 1, N_1 + 1)$. Then s' preserves H_τ, and it is easy to see that then $s' = 1$ or $N_2 - 1$. If $s' = 1$, we have $\tau' = \tau$; if $s' = N_2 - 1$, we have a pair in list (3) of the proposition.

Next, if $t = 1 = s$, then $H_\tau = \{\text{odd } j < N_1\}$, and a similar application of Sublemma 1 gives a pair in list (2) of the proposition. Sublemma 1 can also be used to rule out the cases s' or $t' = 1$ or $N_1 + 1$; t, s' or $t' = N - 1$ or $N_1 - 1$ or reduce them to a pair in list (2) or (3) of the proposition.

Thus, we may assume that $s = 1$, t, s', $t' \not\equiv \pm 1 \bmod N_1$. In addition, at least one of the t, s', t' may be assumed $\not\equiv \pm 3^{\pm 1} \bmod N_1$, since otherwise we could find two with the same sign in the exponent, divide τ and τ' by one of these two, and reduce to a case already considered when one of s, t, s', t' is 1 and one is 1 or $N_1 \pm 1$.

Now we apply the Probabilistic Lemma. (We suppose $n \geqq 9$, i.e., $N \geqq 512$. The "relatively prime case" of Theorem 3 was verified by computer for $N = 16$, 32, 64, 128, 256.) Let y_1, y_2, y_3 be $\langle -t \rangle$, s', t', where y_1 is chosen $\not\equiv \pm 3^{\pm 1} \bmod N_1$. Let $u \in S_{y_i} \cap S_{y_j}$. Let k be the index in $\{1, 2, 3\}$ not equal to i or j.

First consider the case $y_k = s'$ or t'. Then $\langle us \rangle = u < N_1$, $\langle ut \rangle < N_1$, so that $u \in H_\tau$, $u + N_1 \notin H_\tau$. At least one of $\langle us' \rangle$, $\langle ut' \rangle$ is $> N_1$. If both are, then $u \notin H_{\tau'}$, a contradiction. If one is $> N_1$ and one is $< N_1$, then

$$\begin{aligned}\langle (u + N_1)r' \rangle &+ \langle (u + N_1)s' \rangle + \langle (u + N_1)t' \rangle \\ &= \langle ur' \rangle + \langle us' \rangle \pm N_1 + \langle ut' \rangle \mp N_1 = \langle ur' \rangle + \langle us' \rangle + \langle ut' \rangle,\end{aligned}$$

so that either both u, $u + N_1 \in H_{\tau'}$ or both u, $u + N_1 \notin H_{\tau'}$, also a contradiction.

Now consider the case $y_k = \langle -t \rangle$ and $u \notin S_{y_k}$, i.e., $\langle ut \rangle > N_1$. Since $\langle us' \rangle$, $\langle ut' \rangle > N_1$, we have $u \notin H_{\tau'}$, $u + N_1 \notin H_{\tau'}$. But since $\langle us \rangle = u < N_1$ and $\langle ut \rangle > N_1$, we must have either u, $u + N_1 \in H_\tau$ or u, $u + N_1 \notin H_\tau$, a contradiction. This proves the proposition assuming the Probabilistic Lemma.

Probabilistic Lemma. *Let* $N = 2^n$, $N_1 = 2^{n-1}$, $N_2 = 2^{n-2}$, $n \geqq 9$, $S = \{1, 3, 5, \cdots, N_1 - 1\}$. *Let* $\langle \quad \rangle$ *denote least positive residue* mod N. *For* $y \in (\mathbf{Z}/N\mathbf{Z})^*$, *let* $S_y = \{s \in S | \langle sy \rangle > N_1\}$. *Suppose* $y_1, y_2, y_3 \in (\mathbf{Z}/N\mathbf{Z})^*$, $y_1, y_2, y_3 \not\equiv \pm 1 \pmod{N_1}$, $y_1 \not\equiv \pm 3^{\pm 1} \pmod{N_1}$. *Then for some* $i \neq j$, $S_{yi} \cap S_{yj}$ *is not empty.*

Proof. We shall need some simple sublemmas.

Sublemma 1. *Let* $yS = \{\langle ys \rangle | s \in S\}$. *If* $yS = S$, *then* $y \equiv 1$ *or* $N_1 - 1 \pmod{N}$.

Sublemma 2. $\displaystyle\sum_{\substack{0<j<2M,\\ j \text{ odd}}} \frac{1}{j} < \log \frac{2M+1}{\sqrt{M}}$.

Sublemma 3. *Let* $a_1 \geqq a_2 \geqq \cdots \geqq a_r \geqq 0$, $b_1 \geqq b_2 \geqq \cdots \geqq b_r \geqq 0$. *For* *any permutation* σ *of* $\{1, 2, \cdots, r\}$ *define* $A_\sigma = \sum a_i b_{\sigma(i)}$. *Then* $A_\sigma \leqq A_1 = \sum a_i b_i$.

SUBLEMMA 4. *For* M *odd, let*

$$s_M(x) = \frac{4}{\pi} \sum_{\substack{j>M,\\ j \text{ odd}}} \frac{\sin 2\pi jx}{j}.$$

Then

$$|s_M(x)| \leqq \frac{1}{\pi(M+1)d(x, \frac{1}{4}\mathbf{Z})}, \quad \textit{where } d(x, \tfrac{1}{4}\mathbf{Z}) = \min_{l \in \mathbf{Z}} \{|x - l/4|\}.$$

The proofs of the first three sublemmas are very simple, and will be omitted. To prove the fourth, we write

$$\begin{aligned}
\sin 4\pi x\, s_M(x) &= \frac{4}{\pi} \sum_{\text{odd } j \geqq M+2} \frac{\sin 4\pi x \sin 2\pi jx}{j} \\
&= \frac{4}{\pi} \sum_{\text{odd } j \geqq M+2} \frac{\cos 2\pi(j-2)x - \cos 2\pi(j+2)x}{2j} \\
&= \frac{2}{\pi} \Bigg(\frac{\cos 2\pi Mx}{M+2} + \frac{\cos 2\pi(M+2)x}{M+4} \\
&\qquad + \sum_{\text{odd } j \geqq M+4} \cos 2\pi jx \left(\frac{1}{j+2} - \frac{1}{j-2} \right) \Bigg).
\end{aligned}$$

Since

$$\begin{aligned}
\sum_{\text{odd } j \geqq M+4} \left(\frac{1}{j-2} - \frac{1}{j+2} \right) &= 4 \sum_{\text{odd } j \geqq M+4} \frac{1}{j^2 - 2} < 4 \sum_{\text{even } j \geqq M+3} \frac{1}{j^2} \\
&= \sum_{j \geqq (M+3)/2} \frac{1}{j^2} < \frac{2}{M+1},
\end{aligned}$$

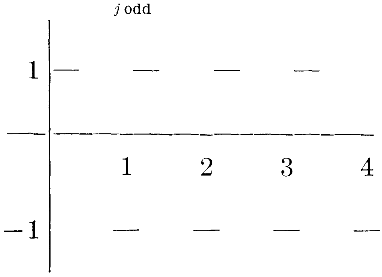
and since $|\sin 4\pi x| \geqq 8d(x, \frac{1}{4}\mathbf{Z})$, we have

$$|s_M(x)| \leqq \frac{2}{\pi \cdot 8d(x, \frac{1}{4}\mathbf{Z})} \left(\frac{2}{M+2} + \frac{2}{M+1} \right) < \frac{1}{\pi(M+1)d(x, \frac{1}{4}\mathbf{Z})}.$$

This concludes the proof of Sublemma 4.

Proceeding to the proof of the Probabilistic Lemma, we define

$$f(x) = \frac{4}{\pi} \sum_{\substack{j>0,\\ j \text{ odd}}} \frac{\sin 2\pi jx}{j} = \frac{4}{2\pi i} \sum_{j \text{ odd}} \frac{e^{2\pi ijx}}{j}.$$



For $y \in (\mathbf{Z}/N\mathbf{Z})^*$, let

$$A_y = \frac{2}{N} \sum_{\substack{0<j<N \\ j \text{ odd}}} f\left(\frac{j}{N}\right) f\left(\frac{jy}{N}\right) = \frac{4}{N} \sum_{\substack{0<j<N_1, \\ j \text{ odd}}} f\left(\frac{jy}{N}\right).$$

Clearly, $A_y = A_{y^{-1}}$, $A_y = -A_{-y} = -A_{y+N_1}$. Moreover,

$$\# S_y = \sum_{\substack{0<j<N_1 \\ j \text{ odd}}} \left(1 - f\left(\frac{jy}{N}\right)\right)/2 = \frac{N_2}{2}(1 - A_y),$$

and the lemma follows if we show that $N_2 < (N_2/2)(3 - A_{y_1} - A_{y_2} - A_{y_3})$. We shall show that $|A_{y_1}| + |A_{y_2}| + |A_{y_3}| < 1$.

A_3 is easily computed directly:

$$A_3 = \frac{4}{N}\left(\frac{N}{4} - 2\left(\#\text{ of odd } j \text{ such that } \frac{N}{6} < j < \frac{N}{3}\right)\right)$$
$$= 1 - \frac{8}{N}\begin{cases} \dfrac{N+2}{6} - \dfrac{N/2-2}{6} & \text{if } n \text{ is even;} \\ \dfrac{N-2}{6} - \dfrac{N/2+2}{6} & \text{if } n \text{ is odd,} \end{cases}$$
$$= \frac{1}{3} - (-1)^n \frac{16}{3N}.$$

Thus, $|A_y| \leqq 1/3 + 16/3N$ if $y \equiv \pm 3^{\pm 1} \pmod{N_1}$.

We now prove: If $y \not\equiv \pm 1, \pm 3^{\pm 1} \pmod{N_1}$ and $n \geqq 9$, then $|A_y| < 1/3 - 32/3N$. This will give us the required $|A_{y_1}| + |A_{y_2}| + |A_{y_3}| < 1/3 - 32/3N + 2(1/3 + 16/3N) = 1$.

First suppose $\langle \pm y^{\pm 1}\rangle$ or $\langle N_1 \pm y^{\pm 1}\rangle$ is $< N_2/2$ for some choice of signs; say $0 < y < N_2/2$. For $k = 0, 1, \cdots, (y-1)/2 - 1$, clearly

$$\left| \sum_{\substack{kN/y<j<(k+1)N/y \\ j \text{ odd}}} f\left(\frac{jy}{N}\right) \right| \leqq 1,$$

while

$$\left| \sum_{\substack{(y-1)N/2y<j<N_1 \\ j \text{ odd}}} f\left(\frac{jy}{N}\right) \right| \leqq \frac{N_1 - \dfrac{y-1}{2y}N + 1}{2} = \frac{N}{4y} + \frac{1}{2}.$$

Thus,

$$|A_y| \leqq \frac{4}{N}\left(\frac{y-1}{2} + \frac{N}{4y} + \frac{1}{2}\right) = \frac{2y}{N} + \frac{1}{y}$$
$$\leqq \max\left(\frac{10}{N} + \frac{1}{5}, \frac{1}{4} + \frac{2}{N_2}\right) \quad \text{for } 5 \leqq y < \frac{N_2}{2}$$
$$= \frac{1}{4} + \frac{8}{N} \quad \text{for } n \geqq 6$$
$$< \frac{1}{3} - \frac{32}{3N} \quad \text{for } n \geqq 8.$$

https://doi.org/10.4153/CJM-1978-099-6 Published online by Cambridge University Press

Now suppose $\langle \pm y^{\pm 1}\rangle > N_2/2$ and $\langle N_1 \pm y^{\pm 1}\rangle > N_2/2$ for all choices of signs. For M odd, let

$$S_M(x) = \frac{4}{\pi}\sum_{\substack{0<j\leqq M,\\ j\text{ odd}}} \frac{\sin 2\pi jx}{j}, \quad s_M(x) = f(x) - S_M(x).$$

Applying Sublemma 4 with $M = N - 1$, $x = k/N$, we obtain

$$|s_{N-1}(k/N)| \leqq \frac{1}{\pi d(k, N_2\mathbf{Z})}, \quad \text{where } d(k, N_2\mathbf{Z}) = \min_{l\in\mathbf{Z}} \{|k - N_2 l|\}.$$

Then

$$|A_y| \leqq \frac{2}{N}\left|\sum_{\substack{0<j<N\\ j\text{ odd}}} S_{N-1}\left(\frac{j}{N}\right) S_{N-1}\left(\frac{jy}{N}\right)\right| + \frac{4}{N}\sum_{\substack{0<j<N,\\ j\text{ odd}}} \left|s_{N-1}\left(\frac{j}{N}\right)\right|$$
$$+ \frac{2}{N}\sum_{\substack{0<j<N,\\ j\text{ odd}}} \left|s_{N-1}\left(\frac{j}{N}\right)\right| \left|s_{N-1}\left(\frac{jy}{N}\right)\right|.$$

The second sum is bounded by

$$\frac{1}{\pi}\sum_{\substack{0<j<N\\ j\text{ odd}}} 1/d(j, N_2\mathbf{Z}) = \frac{8}{\pi}\sum_{\substack{0<j<N_2/2\\ j\text{ odd}}} \frac{1}{j} < \frac{8}{\pi}\log\frac{N_2+2}{\sqrt{N_2}}$$

by Sublemma 2. The third sum is bounded by

$$\frac{1}{\pi^2}\sum_{\substack{0<j<N\\ j\text{ odd}}} \frac{1}{d(j, N_2\mathbf{Z})d(jy, N_2\mathbf{Z})} \leqq \frac{8}{\pi^2}\sum_{\substack{0<j<N_2/2\\ j\text{ odd}}} 1/j^2$$

by Sublemma 3. We rewrite the first sum as

$$-\frac{4}{\pi^2}\sum_{\substack{-N<r,s<N\\ r,s\text{ odd}}}\ \sum_{\substack{0<j<N\\ j\text{ odd}}} \frac{1}{rs} e^{2\pi ij(r+ys)/N}$$
$$= -\frac{4}{\pi^2}\frac{N}{2}\sum_{\substack{-N<r,s<N,\, r,s\text{ odd}\\ r+ys\equiv 0 (\mathrm{mod}\ N_1)}} \frac{1}{rs}(-1)^{(r+ys)/N_1}$$
$$= -\frac{4N}{\pi^2}\sum_{\substack{0<s<N,\, s\text{ odd}\\ -N<r<N,\, r\equiv -ys (\mathrm{mod}\ N_1)}} \frac{1}{rs}(-1)^{(r+ys)/N_1}$$
$$= -\frac{4N}{\pi}\sum_{\substack{0<s<N\\ s\text{ odd}}} \frac{1}{s}\left(\frac{1}{\langle -ys\rangle} - \frac{1}{\langle ys\rangle} - \frac{1}{\langle N_1 - ys\rangle} + \frac{1}{\langle N_1 + ys\rangle}\right).$$

Thus,

$$|\text{first sum}| \leqq \frac{4N}{\pi^2}\sum_{\substack{0<s<N_2\\ s\text{ odd}}} g(s)g(-ys),$$
$$\text{where } g(s) = \left|\frac{1}{\langle s\rangle} - \frac{1}{\langle -s\rangle} - \frac{1}{\langle N_1 + s\rangle} + \frac{1}{\langle N_1 - s\rangle}\right|.$$

Clearly,

(1) $g(1) \geqq g(3) \geqq \cdots \geqq g(N_2 - 1)$;

(2) $\{g(-ys)\}_{\substack{0<s<N_2 \\ s \text{ odd}}}$ is a permutation of $\{g(s)\}_{\substack{0<s<N_2 \\ s \text{ odd}}}$;

(3) $g(s) < 1/s$ for $s < N_2/2$;

(4) $g(s) < 2/N_2$ for $s > N_2/2$.

Hence by Lemma 3

$$|\text{first sum}| \leqq \frac{4N}{\pi^2}\left(g(1)g(-y) + g(-1/y)g(1) + \sum_{\substack{3\leqq s<N_2 \\ s \text{ odd}}} g(s)^2\right)$$

$$< \frac{4N}{\pi^2}\left(\frac{2}{N_2} + \frac{2}{N_2} + \sum_{\substack{3\leqq s<N_2/2 \\ s \text{ odd}}} \frac{1}{s^2} + \frac{N_2}{4}\left(\frac{2}{N_2}\right)^2\right)$$

$$< \frac{4N}{\pi^2}\left(\frac{20}{N} + \frac{\pi^2}{8} - 1\right).$$

Putting the three estimates together now gives:

$$|A_y| < \frac{160}{\pi^2 N} + \frac{8}{\pi^2}\left(\frac{\pi^2}{8} - 1\right) + \frac{32}{\pi N}\log\frac{N_2 + 2}{\sqrt{N_2}} + \frac{2}{N}$$

$$< 0.28 \quad \text{if } N \geqq 512.$$

Thus,

$$|A_y| < 1/3 - 32/3N \quad \text{if } N \geqq 512.$$

This completes the proof of the Probabilistic Lemma.

References

1. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. *6* (1955), 265–269.
2. K. Iwasawa, *Lectures on p-adic L-functions*, Annals of Math. Studies *74*, Princeton, 1972.
3. M. Kac, *Statistical independence in probability, analysis, and number theory* (John Wiley and Sons, New York, 1959).
4. D. Kubert and S. Lang, *Distributions on toroidal groups*, Math. Zeit. *148* (1976), 33–51.
5. S. Lang, *Cyclotomic fields* (Springer-Verlag, New York, 1978).
6. D. Rohrlich, *Periods of the Fermat curve*, Appendix to B. Gross, *On the periods of abelian integrals and a formula of Chowla and Selberg*, Inventiones Math. *45* (1978), 193–211.
7. G. Shimura and Y. Taniyama, *Complex multiplication of abelian verieties and its applications to number theory*, Math. Soc. Japan, Tokyo, 1961.

Harvard University,
Cambridge, Massachusetts