Conspectus materiae tomi XXXIII, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXXIII (1977)

Atkin-Lehner involutions and class number residuality

by

M. A. KENKU (Ibadan)

1. Introduction. Let $Y_0(N)$ denote the set of isomorphism classes of pairs $(E; F)$, where E is an elliptic curve defined over C, the field of complex numbers, and F a cyclic group of order N on E.

$Y_0(N)$ corresponds to $\Gamma_0(N)/H$, where H is the upper half plane and

$$\Gamma_0(N) = \left\{\alpha \in \mathrm{SL}(2, \mathbf{Z}) \mid \alpha \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N\right\}.$$

Denote by $X_0(N)$ the compactification of $Y_0(N)$. It is well known that $X_0(N)$ is an algebraic curve defined over Q. A non-cusp point of $X_0(N)$, rational over an algebraic number field k, corresponds to a rational class and each rational class has a member $(E; F)$, rational over k.

The genus $p_0(N)$ of $X_0(N)$ is easily computed from the Riemann–Hurwitz formula. Let μ be the index of $\Gamma_0(N)$ in $\mathrm{SL}(2, \mathbf{Z})$, μ_2 (resp. μ_3) the number of elliptic fixed points of order 2, (resp. 3) and μ_∞ the number of cusps on $X_0(N)$. Then

$$p_0(N) = 1 + \frac{\mu}{12} - \frac{\mu_2}{4} - \frac{\mu_3}{3} - \frac{\mu_\infty}{2}.$$

For each positive integer N', $N' \mid N$ and $(N/N', N') = 1$ there is an involution $W_{N'}$ of $X_0(N)$.

These Atkin–Lehner [1] involutions form a group A of order 2^r. Let U be a subgroup of A. The quotient space $X_0^u(N)$ is also an algebraic curve defined over Q. The genus $p'(N)$ of $X_0^u(N)$ can be computed using again the Riemann–Hurwitz formula by regarding $X_0(N)$ as a covering of degree 2^t over $X_0^u(N)$. $p_0(N)$ and $p_0'(N)$ are related, thus

$$2\big(p_0(N)\big) - 2 = 2^t\big(2p_0'(N) - 2\big) + \sum_{z \in B}(e_z - 1)$$

where B is the set of ramification points of the covering and e_z is the ramification degree.

Each ramification point has degree 2 and the number of ramification points can be expressed as a sum of multiples of the class-number of some complex quadratic field.

The formula we shall prove next was first proved by Newman [7] in the case where $(N, 6) = 1$. By using the moduli property of $X_0(N)$, Ogg [8] removed this restriction, although he did not state the formula in full. Apart from specific references to Ogg [8] the author would like to acknowledge his debt to Andrew Ogg from which he had learnt a lot about modular curves.

2. Atkin-Lehner involutions of $X_0(N)$. Let $N = N'N''$, where $(N', N'') = 1$, the involution $w = w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ of $X_0(N)$ factors as $w = w'w''$ $(w' = w_{N'})$.

The following theorem is proved by Ogg [8]:

THEOREM 1. *W' has no fixed points at cusps (given $N' > 1$), except for the case $N' = 4$, where the cusps $\begin{pmatrix} x \\ d \end{pmatrix}$, with $d' = (d, N') = 2$, are fixed.*

Following Ogg we determine the non-cusps points which are fixed by W'.

Let $(E; C)$ represent a point on $Y_0(N)$. If (ω_1, ω_2) is a basis of E, with ω_2/N generating C, and $\tau \in H$, then the orbit of τ under $\Gamma_0(N)$ is the point of $Y_0(N)$ represented. Suppose $C = C' + C''$ where the sum is direct, C' (resp. C'') of order N' (resp. N''). W' sends the isomorphism class of $(E; C)$ to the class of $(\bar{E}; \bar{C})$ where $\bar{E} = E/C'$ and $\bar{C} = E_{N'} + C''/C'$.

If $(E; C)$ represents a fixed point of W', then $(E; C)$ and $(\bar{E}; \bar{C})$ are isomorphic so that E admits complex multiplication by λ

$$0 \longrightarrow C' \longrightarrow E \xrightarrow{\lambda} E \longrightarrow 0$$

such that $\lambda^2 = N' \cdot \varphi$, where φ is an automorphism of E and $\lambda(C'') = C''$.

If $N' > 3$ then $\varphi = -1$ and $\lambda = \pm\sqrt{-N}$.

If $N' = 2$, $\lambda = \sqrt{-2}$ or $1+i$ and its conjugates.

If $N' = 3$, $\lambda = \sqrt{-3}$ and its conjugates.

Considering only the first condition: if $N' > 3$ there are

$$V(N') = \begin{cases} h(-N') + h(-4N') & \text{if} \quad N' \equiv 3 \,(4), \\ h(-4N') \end{cases}$$

isomorphism classes of such curves. If $N' = 2$ or 3 there are 2 such classes. To this we add the second condition that $\lambda(C'') = C''$ which is the same

as to require $\lambda - x$ for some integer x to contain in its kernel the subgroup C'' of order N''. This requirement is multiplicative in the prime divisors of N''.

If $N' > 3$ and N'' is odd, Ogg [8] has shown that there are

$$F(N') = V(N') \prod_{p \mid N''} \left(1 + \left(\frac{-4N'}{p}\right)\right)$$

distinct fixed points of W' which are non-cusps.

If $N' > 3$ and N'' is even: for $p \neq 2$ we have $\left(1 + \left(\frac{-4N'}{p}\right)\right)$ distinct cyclic groups C'' of order every power of p.

If $N' \equiv 1\,(4)$, $\sqrt{-N'} \equiv (\varrho)$ for all odd integers, where ϱ is the unique prime divisor of norm 2 in $Q(\sqrt{-N})$. $\sqrt{-N} - x$ is of odd degree if x is even so that there is only one cyclic subgroup of order 2 left invariant by $\sqrt{-N'}$.

Furthermore if $4 \mid N''$, since the degree of $\sqrt{-N} - x$ for any integer x is not divisible by 4, there is no subgroup of order a power of 2 bigger than 2 which is left invariant by $\sqrt{-N'}$. If $N' > 3$, $N' \equiv 1\,(4)$, the number of fixed points of W'

$$F(N') = \begin{cases} V(N') \prod_{p \mid N''} \left(1 - \left(\frac{4N'}{p}\right)\right) & \text{if} \quad 4 \nmid N, \\ 0 & \text{if} \quad 4 \mid N. \end{cases}$$

Suppose $N' \equiv 3\,(8)$.

For E with endomorphism ring $\boldsymbol{Z}\left[\frac{1+\sqrt{-N'}}{2}\right]$, $\sqrt{-N} + x$ is divisible by 2 for x odd, so that E_2 is contained in the kernel of $\sqrt{-N} + x$. This yields 3 subgroups of order 2.

Whereas for E with endomorphism ring $\boldsymbol{Z}[\sqrt{-N}]$, $\sqrt{-N} + x$ for x odd contains in its kernel a cyclic group of order 4, cyclic since $2 \nmid \sqrt{-N} + x$ in $\boldsymbol{Z}[\sqrt{-N}]$, it can be easily shown that there are two such cyclic subgroups of order 4 although they have a unique subgroup of order 2.

So if N'' is even, $N' \equiv 3\,(8)$ we have

$$F(N') = \begin{cases} 6h(-N') \prod_{\substack{p \mid N'' \\ p \text{ odd}}} \left(1 + \left(\frac{-N'}{p}\right)\right) & \text{if} \quad 8 \nmid N'', \\ 0 \quad \text{otherwise.} \end{cases}$$

Similarly if N'' is even and $N' \equiv 7(8)$

$$F(N') = \begin{cases} 4h(-N)\prod\limits_{\substack{p|N'' \\ p\,\mathrm{odd}}}\left(1+\left(\frac{-4N}{p}\right)\right) & \text{if} \quad 2\|N'', \\ 6h(-N')\prod\limits_{\substack{p|N'' \\ p\,\mathrm{odd}}}\left(1+\left(\frac{-4N'}{p}\right)\right) & \text{if} \quad 4|N''. \end{cases}$$

For E with endomorphism ring $\boldsymbol{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, $\sqrt{-3}$ and its associates have the same kernel C' and the automorphism group of the class represented by $(E; C)$ is of order 6. As above if N'' is odd, adding the point corresponding to E with endomorphism ring $\boldsymbol{Z}[\sqrt{-3}]$

$$v(3) = 2\prod_{p|N''}\left(1+\left(\frac{-12}{p}\right)\right).$$

f N'' is even, as in the case when $N' \equiv 3(8)$, $\sqrt{-3}$ leaves all the 3 subgroups of order 2 invariant, but these are permuted by the associates of $\sqrt{-3}$ so that all the 3-subgroups correspond to one point on $Y_0(N)$.

For E with endomorphism ring $\boldsymbol{Z}[\sqrt{-3}]$, there is only $\sqrt{-3}$ and it behaves like $\sqrt{-N'}$ for other values of N', $N' \equiv 3(8)$

$$F(3) = \begin{cases} 2\prod\limits_{\substack{p|N'' \\ p\,\mathrm{odd}}}\left(1+\left(\frac{-12}{p}\right)\right) & \text{if} \quad 8\nmid N', \\ 0 \quad \text{otherwise}. \end{cases}$$

$v(2)$ can be treated similarly. We have $(E; C)$, E with endomorphism ring $\boldsymbol{Z}[-\sqrt{2}]$ and the automorphism group of order 2, and $(E; C)$, E with endomorphism $\boldsymbol{Z}[i]$ so that the automorphism group of the class represented by $(E; C)$ is of order 4.

$$F(2) = \prod_{p|N''}\left(1+\left(\frac{-8}{p}\right)\right) + \prod_{p|N''}\left(1+\left(\frac{-4}{p}\right)\right).$$

THEOREM 2. *Let $F(N')$ be number fixed points of W'. Then if $N' > 3$, N'' odd*

$$F(N') = v(N')\prod_{p|N''}\left(1+\left(\frac{-4N'}{p}\right)\right).$$

For $N \equiv 1(4)$, N'' even

$$F(N') = h(-4N')\begin{cases} \prod\limits_{\substack{p|N'' \\ p\,\mathrm{odd}}}\left(1+\left(\frac{-4N'}{p}\right)\right) & \text{if} \quad 4\nmid N, \\ 0 & \text{if} \quad 4|N. \end{cases}$$

For $N' \equiv 3(8)$, N'' even

$$F(N') = 6h(-N')\begin{cases} \prod\limits_{p|N''}\left(1+\left(\frac{-4N'}{p}\right)\right) & \text{if} \quad 8\nmid N'', \\ 0 \quad \text{otherwise}. \end{cases}$$

If $N' \equiv 7(8)$, N'' even

$$F(N') = h(-N')\begin{cases} 4\prod\limits_{p|N''}\left(1+\left(\frac{-4N'}{p}\right)\right) & \text{if} \quad 2\|N'', \\ 6\prod\limits_{p|N''}\left(1+\left(\frac{-4N'}{p}\right)\right) & \text{if} \quad 4|N'', \ p \text{ odd}; \end{cases}$$

$$F(3) = \begin{cases} 2\prod\limits_{\substack{p|N'' \\ p\,\mathrm{odd}}}\left(1+\left(\frac{-12}{p}\right)\right) & \text{if} \quad 8\nmid N', \\ 0 \quad \text{otherwise}; \end{cases}$$

$$F(2) = \prod_{p|N''}\left(1+\left(\frac{-8}{p}\right)\right) + \prod_{p|N''}\left(1+\left(\frac{-4}{p}\right)\right).$$

Furthermore for a fixed N, no point of $Y_0(N)$ is a fixed point of W' for two distinct N's.

Proof. The first part follows from the preceeding and the latter half follows from the fact that each order of a complex quadratic field is involved at most once, so that the isomorphism class of any elliptic curve is involved with only one value of λ.

COROLLARY. *The ramification points of the covering $X_0(N) \to X_0^U(N)$ are all of degree 2 and they are all at non-cusp points of $X_0(N)$ except where $w' \in U$ for $N' = 4$ where cusps with $d' = 2$ are fixed.*

3. Class numbers and congruences modulo powers of 2. In this section we deduce the congruences satisfied by the class-number of some complex quadratic fields modulo power of 2.

To do this we consider the algebraic curves $X_0(N)$, and $X_0^A(N)$, where A is the group generated by all the involutions of Atkin–Lehner

type on $X_0(N)$. Let $p_0(N)$ (resp. $p_0'(N)$) be the genus of $X_0(N)$ (resp. $X_0^A(N)$). As stated earlier,

$$2p_0(N)-2 = 2^t\big(2p_0'(N)-2\big)+\sum_{z\in B}(e_z-1)$$

where t = the number of distinct primes dividing N, B the ramification points of the covering $X_0(N)\to X_0^A(N)$ and e_z the ramification degree. We apply this to the case $4\nmid N$ so that B is obtained as in Theorem 2.

$e_z = 2$ for all $z\in B$ so that

$$2\big(p_0(N)-1\big) = 2^{t+1}\big(p_0'(N)-1\big)+\operatorname{card} B.$$

Dividing through by 2^{t+1}

$$\frac{\operatorname{card} B}{2^{t+1}} + p_0'(N)-1 = \frac{p_0(N)-1}{2^t}.$$

Using the fact that $p_0'(N)$ is an integer, we deduce congruences satisfied by the class number $h(-4N)$ for various N.

There are some limitations of this method. If N is divisible by t distinct primes one can get a congruence to 2^{t+1} at most. For some N especially $N\equiv 3(4)$, the congruence can be only proved to a lower power of 2.

THEOREM 3. *Let p, q be distinct $p\equiv q\equiv 1(4)$. We have*

(i) $h(-8pq)\equiv 4h(-4p)+4h(-4q)+3h(-8p)+3h(-8q)+h(-4pq)(16)$ *if* $p\equiv q\equiv 1(16)$ *and* $(p/q)=1$;

(ii) $h(-8pq)\equiv h(-4pq)(16)$ *if* $p\equiv q\equiv 1(16)$ *and* $(p/q)=-1$;

(iii) $h(-8pq)\equiv 8+4h(-4p)+4h(-4q)+3h(-8q)+3h(-8p)+h(-4pq)(16)$ *if* $p\not\equiv q(16)$, $p\equiv 1(8)$ *and* $(p/q)=1$;

(iv) $h(-8pq)\equiv 8+h(-4pq)(16)$ *if* $p\equiv q(16)$, $p\equiv 1(8)$ *and* $(p/q)=-1$;

(v) $h(-8pq)\equiv 4+3h(-4pq)+6h(-8q)(16)$ *if* $p+q\equiv 6(16)$, $q\equiv 1(8)$ *and* $(p/q)=-1$;

(vi) $h(-8pq)\equiv 4+6h(-4p)+2h(-4q)+3h(-4pq)+6h(-8q)(16)$ *if* $(p/q)=1$, $p+q\equiv 6(16)$ *and* $q\equiv 1(8)$;

(vii) $h(-8pq)\equiv 12+h(-4pq)+6h(-8q)(16)$ *if* $p\equiv 5(8)$, $q\equiv 1(8)$, $p+q\not\equiv 6(16)$, $(p/q)=-1$;

(viii) $h(-8pq)\equiv 12+6h(-4p)+2h(-4q)+3h(-4pq)+6h(-8q)(16)$ *if* $(p/q)=1$, $p\equiv 5(8)$, $q\equiv 1(8)$ *and* $p+q\not\equiv 6(16)$;

(ix) $h(-8pq)\equiv 4+6h(-4p)+6h(-4q)+h(-4pq)(16)$ *if* $p\equiv q(16)$, $p\equiv 5(8)$ *and* $(p/q)=1$;

(x) $h(-8pq)\equiv 4+h(-4pq)+6h(-8p)+6h(-8q)(16)$ *if* $p\equiv q(16)$, $p\equiv 5(8)$ *and* $(p/q)=-1$;

(xi) $h(-8pq)\equiv 12+6h(-4p)+6h(-4q)+h(-4pq)(16)$ *if* $p\equiv q(16)$, $p\equiv 5(8)$ *and* $(p/q)=1$;

(xii) $h(-8pq)\equiv 12+h(-4pq)+6h(-8p)+6h(-8q)(16)$ *if* $p\not\equiv q(16)$, $p\not\equiv 5(8)$ *and* $(p/q)=-1$.

Proof.

$$p_0(N) = 1+\frac{3(p+1)(q+1)}{12}-\frac{\mu_2}{4}-\frac{\mu_3}{3}-\frac{\mu_\infty}{2} \quad \text{if} \quad N=2pq.$$

For $p\equiv q\equiv 1(4)$,

$$\mu_2 = 4, \quad \mu_3 = 0 \quad \text{and} \quad \mu_\infty = 8.$$

So

$$p_0(N) = 1+\frac{(p+1)(q+1)}{4}-4-1,$$

$$\frac{p_0(N)-1}{8} = \frac{(p+1)(q+1)-20}{32}.$$

If $p\equiv q(16)$, $p\equiv 1(8)$

$$\frac{p_0(N)-1}{8} \in \frac{1}{2}+\mathbf{Z}.$$

If $p\not\equiv q(16)$, $p\equiv 1(8)$

$$\frac{p_0(N)-1}{8} \in \mathbf{Z}.$$

Suppose $p\equiv q\equiv 1(8)$. Using the formula of Theorem 2

$$\operatorname{card} B = h(-8pq)+8+4h(-4p)+4h(-4q)+h(-8p)+h(-4pq)+h(-8q) \quad \text{if} \quad (p/q)=1,$$

$$\operatorname{card} B = 8+h(-4pq)+h(-8pq) \quad \text{if} \quad (p/q)=-1.$$

This gives (i)–(iv) in Theorem 3 when combined with the above value of $\big(p_0(N)-1\big)/8$.

Suppose $p\equiv 5(8)$, $q\equiv 1(8)$.

$$\operatorname{card} B = 4h(-4pq)+2h(-8q)+h(-8pq) \quad \text{if} \quad (p/q)=-1,$$

$$\operatorname{card} B = 4+2h(-4p)+2h(-4q)+h(-4pq)+h(-8pq)+2h(-8p) \quad \text{if} \quad (p/q)=1.$$

On the other hand

$$\frac{p_0(N)-1}{8} \in \frac{1}{2}+\mathbf{Z}, \quad \text{if} \quad \begin{matrix} p \equiv 5(16),\ q \equiv 1(16) \text{ or} \\ p \equiv 13(16),\ q \equiv 9(16). \end{matrix}$$

These give (v)–(viii) of the theorem.

Suppose $p \equiv q \equiv 5(8)$. If $(p/q) = 1$

$$\operatorname{card} B = 4+2h(-4p)+2h(-4q)+h(-4pq)+h(-8pq).$$

If $(p/q) = -1$

$$\operatorname{card} B = 4+h(-pq)+2h(-8p)+2h(-8q)+h(-8q)+h(-8pq).$$

$$\frac{p_0-1}{8} \in \frac{1}{2}+\mathbf{Z} \quad \text{if} \quad p \equiv q(16),$$

$$\frac{p_0-1}{8} \in \mathbf{Z} \quad \text{if} \quad p \not\equiv q(16).$$

This gives (ix)–(xii) of the theorem.

THEOREM 4. *For p, q distinct primes $p \equiv q \equiv 3(4)$. We have the following:*

(i) *For $p \equiv q \equiv 3(8)$*

$$h(-8pq) \equiv 12+4h(-q)+3h(-4pq)+6h(-8p)(16) \quad \text{if} \quad (p/q) = 1;$$

(ii) *For $p \equiv q \equiv 7(8)$*

$$h(-8pq) \equiv 8+h(-q)+3h(-4pq)+6h(-8q)(16) \quad \text{if} \quad (p/q) = 1;$$

(iii) *For $p \equiv 3(8)$, $q \equiv 7(8)$*

$$h(-8pq) \equiv 8+8h(-q)+3h(-4pq)(16) \quad \text{if} \quad (p/q) = 1$$
$$\equiv 8+12h(-p)+3h(-4pq)+6h(-8p)(16) \quad \text{if} \quad (p/q) = -1.$$

Proof. As in Theorem 3

$$p_0(N) = 1+\frac{(p+1)(q+1)}{4}-4$$

and we have that

$$\frac{p_0(N)-1}{8} \in \begin{cases} \mathbf{Z} & \text{if} \quad p \equiv q \equiv 3(8), \\ \frac{1}{2}+\mathbf{Z} & \text{otherwise.} \end{cases}$$

$\operatorname{card} B$ are also evaluated as in the previous theorem.

In Theorems 3 and 4 one can get the exact residue class of $h(-8pq)$ mod16 by using the results of Hasse [5], Barrucand and Cohn [2] and Brown [3] or proving them by the method of this paper.

The case of $N = pqr$, where p, q, r are primes all congruent to 1 mod 4, can be similarly treated.

Theorem 2 is of some interest by itself. One other possible application of it is that one can show that there are only finitely many involutory Weil elliptic curves as defined recently by Mazur an Swinnerton-Dyer [6]. The proof enables one to actually determine them all. For instance it is easy to show that Table 1 of [6] contains all those with prime power conductor.

In this case, it is easy to show that they have a lot of rational points so that the Mordell–Weil group of each of them is infinite. With some luck it might be possible to show that the rank is exactly one as one would expect from the results of [6]. We hope to treat this in a subsequent paper.

References

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. 185 (1970), pp. 134–160.

[2] P. Barrucand and H. Cohn, *Note on primes of type x^2-32y^2, class-number and residuality*, J. Reine Angew. Math. 237 (1969), pp. 67–70.

[3] E. Brown, *Classnumbers of complex quadratic fields*, Journal of Number Theory 6 (1974), pp. 185–191.

[4] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$*, ibid. 1 (1969), pp. 231–234.

[5] — *Über die Teilbarkeit durch 2^3 der Klassentahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, Mathematische Nachriten 46 (1970), pp. 61–70.

[6] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Inventiones Math. 25 (1974), pp. 1–61.

[7] M. Newman, *Conjugacy, Genus and class numbers*, Math. Ann. 196 (1972), pp. 198–217.

[8] A. Ogg, *Hyperelliptic modular curves* (to appear).

Received on 29. 11. 1974
and in revised form on 19. 1. 1976 (643)