ILLINOIS JOURNAL OF MATHEMATICS
Volume 22, Number 1, March 1978

ON THE WEIERSTRASS POINTS OF $X_0(N)$

BY

A. P. OGG[1]

Let N be a positive integer and let $\Gamma_0(N)$ be the subgroup of the modular group $\Gamma = SL(2, \mathbf{Z})/(\pm 1)$ defined by the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with c divisible by N. It acts on the upper half-plane $\mathfrak{H}$, and we let $X_0(N)$ be the compactification of $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$ obtained by adding cusps. We give $X_0(N)$ its standard structure of an algebraic curve over $\mathbf{Q}$, let $g(N)$ denote its genus, and suppose throughout that $g(N) \geq 2$.

In his article [1], which extended previous work of Lehner and Newman [6], Atkin showed that the cusp at ∞ is a Weierstrass point on $X_0(N)$, abbreviated by $N \in W$, for various sufficiently composite values of N. Atkin concluded his paper with: "It would be of great interest to find an instance (if one exists) of $n \in W$ when n is quadratfrei. On the other hand, it has not yet been proved that $n \notin W$ for an infinity of n." In 1973, Atkin proved that $p \notin W$ for any prime p (I learned of this more recently [2], [3]), thus disposing of the second sentence just quoted, but the first still stands, so far as I know. An examination of (what I surmise to be an algebro-geometrization of) Atkin's proof led to the following generalization.

THEOREM. *Let $N = p \cdot M$ have $g(N) \geq 2$, where p is a prime, and $p \nmid M$. Let P be any $\mathbf{Q}$-rational point on $X_0(N)$ whose reduction $\tilde{P}$ modulo p is not supersingular (e.g., any rational cusp). Let c be a nongap at P, i.e., there is a function f on $X_0(N)$ with a pole of order c at P and regular elsewhere. Then*

$$c \geq 1 + g(N) - 2 \cdot g(M).$$

In particular, P is not a Weierstrass point (i.e., the gaps at P are $1, 2, \ldots, g(N)$) if $g(M) = 0$, i.e., if $M =$ 1–10, 12, 13, 16, 18, 25, and so $pM \notin W$ in those cases.

This theorem conflicts with Theorem 1 of [5], which states that $16 \cdot p \in W$.

Most of the results of this paper are discussed (without proof) in [8]. Correspondence and conversations with Atkin were very helpful.

Before giving the proof of the theorem, let us discuss briefly the modular interpretation of $X_0(N)$ and its reduction modulo primes. If l is a good prime (not dividing N), then by a theorem of Igusa, $X_0(N)$ has a good reduction

Received June 25, 1976.
[1] Partially supported by a National Science Foundation grant.

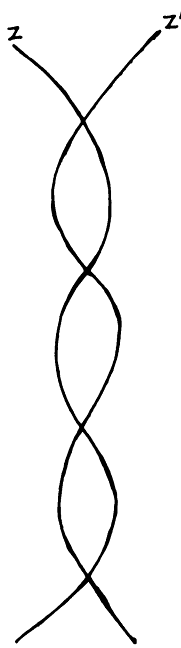
Copyright © Board of Trustees, University of Illinois

modulo l, still denoted by $X_0(N)$, over the field $\mathbf{F}_l$. In characteristic 0 or l, the points of $Y_0(N)$ parameterize the isomorphism classes of pairs (E, C), where E is an elliptic curve and C is a cyclic subgroup of order N, or if you prefer the isomorphism classes of cyclic isogenies $E \to E'$, of degree N, of elliptic curves. A point of $Y_0(N)$ is rational over a field K (of characteristic 0 or l) if and only if it is represented by a K-rational pair (E, C).

Assuming now that $N = p \cdot M$ as in the theorem, we will need the Igusa–Deligne–Rapoport determination of the reduction modulo p of $X_0(N)$. The undesingularized reduction modulo p, which is all that we need, consists of two copies Z and Z' of $X_0(M)$ in characteristic p, meeting transversally in the supersingular points:

$Z = X_0(M)$ $\qquad\qquad$ $Z' = X_0(M)$

(1)



(Cf. [4, p. 144]; a point of $X_0(M)$ is supersingular if the underlying elliptic curve is.) The points of $Y_0(p \cdot M)$ still represent cyclic isogenies of degree $p \cdot M$, of elliptic curves, which we separate into subisogenies of degree M and p. There are just as many M-isogenies in characteristic p as in characteristic 0, on an elliptic curve, but there are (in general and up to isomorphism) only two p-isogenies: the Frobenius $\phi: E \to E^{(p)}$, which is inseparable, and its transpose $\hat{\phi}: E^{(p)} \to E$ (or rather a conjugate, to have E instead of $E^{(p)}$ as domain), which is separable if E is not supersingular, i.e., if $p = \hat{\phi} \quad \phi: E \to E$ is not totally inseparable. Then Z, minus cusps, consists of points of $Y_0(M)$ together with the

Frobenius ϕ, and Z', minus cusps, consists of points of $Y_0(M)$ together with $\hat{\phi}$, and $Z \cap Z'$ consists of the supersingular points, where the p-isogeny can be thought of as either a ϕ or a $\hat{\phi}$. The cusps cause no difficulty; $X_0(M)$ has as many cusps in characteristic p as in characteristic 0, and $X_0(p \cdot M)$ has twice as many cusps as $X_0(M)$, in characteristic p or in characteristic 0.

By the specialization principle, the arithmetic genus p_a of $Z + Z'$ is the same as the genus $g(p \cdot M)$ in characteristic 0, so we get

$$\begin{aligned} 1 + g(p \cdot M) &= 1 + p_a(Z + Z') \\ &= p_a(Z) + p_a(Z') + Z \cdot Z' \\ &= 2 \cdot g(M) + Z \cdot Z'. \end{aligned}$$

Since Z meets Z' transversally, $Z \cdot Z'$ is the number $n_p(M)$ of supersingular points on $X_0(M)$ in characteristic p, so we have

$$n_p(M) = 1 + g(p \cdot M) - 2 \cdot g(M). \tag{2}$$

We can now prove the theorem. Let P be a rational point on $X_0(p \cdot M)$, whose reduction $\tilde{P}$ modulo p is not supersingular; let c be a nongap at P, and let f be a function with a pole of order c at P and no other poles. Since P is rational, we can assume that f is defined over $\mathbf{Q}$.

Let $w = w_N$ be the canonical involution on $X_0(N)$, corresponding to the transpose on isogenies, and defined in characteristic 0 by the matrix

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Since w is defined over $\mathbf{Q}$, $P' = w(P)$ is also rational, and we assume that $f(P') = 0$. On the reduced curve $Z + Z'$ modulo p, the involution w interchanges the two components Z and Z', so $\tilde{P}$ and $\tilde{P}'$ are on different components, say $\tilde{P} \in Z$ and $\tilde{P}' \in Z'$. Multiplying f by a suitable rational constant if necessary, we will have a nonconstant reduced function $\tilde{f}$ modulo p. Since we have two components, $\tilde{f}$ is really two separate functions on Z and Z', agreeing on the intersection $Z \cap Z'$. Now on Z', $\tilde{f}$ has a zero at $\tilde{P}'$ and no poles, so is identically 0, and in particular vanishes at the $n_p(M)$ supersingular points in $Z \cap Z'$. On Z, then, $\tilde{f}$ has at least $n_p(M)$ zeroes, and at most one pole of order c, so $c \geq n_p(M)$, which, by (2), is the inequality of the theorem.

Since the proof involves only the reduction modulo p of $X_0(N)$, we have the same result, assuming only that P is rational over $\mathbf{Q}_p$.

For the rest of the paper we shall take for P the cusp ∞. As mentioned earlier, Atkin showed that with certain possible exceptions (see below), if N is not square-free, then $N \in W$ (i.e., the cusp ∞ is a Weierstrass point on $X_0(N)$). We can add one case to Atkin's list, namely $2 \cdot p^2 \in W$, if p is a prime ≥ 7, since

$$f = \eta_{p^2}\eta_2^2/\eta\eta_{2p^2}^2$$

is a function on $X_0(2 \cdot p^2)$ with divisor $((p^2-1)/8)((1/2)-(\infty))$, so $c = (p^2-1)/8$ is a nongap at ∞, and it is less than $g(2 \cdot p^2)$ for $p \geq 7$. (As usual, $\eta = \Delta^{1/24}$ is Dedekind's function, and $\eta_m(\tau) = \eta(m\tau)$.) For example, for $N = 2 \cdot 7^2 = 98$, we have $c = 6$ and $g = 7$ (actually the gaps are 1–5, 7, 8), and since $g(49) = 1$, $c = 6$ is also the bound of the theorem. In view of the above, we can restate Theorem 1* of Atkin [1] as follows:

Suppose N is not square-free, $g(N) \geq 2$, and N is not of the form $p \cdot M$ with $p \nmid M$ and $g(M) = 0$. Then $N \in W$, except in case (1) below and possibly cases (2) and (3):

(1) $N = 81$.

(2) $N = p^2q$, where p, q are distinct odd primes, not both congruent to 1 modulo 12.

(3) $N = p^2qr$, where p, q, r are distinct primes, and neither $x^2+1 \equiv 0$ nor $x^2 - x + 1 \equiv 0$ are solvable modulo pqr.

The first square-free N not covered by the theorem is $N = 3 \cdot 5 \cdot 7 = 105$. We have $g(105) = 13$ and $g(15) = g(21) = 1$, so the theorem only gives that a nongap is ≥ 12, while a computer calculation of W. Parry shows that $105 \notin W$. The first case for (2) above is $N = 3 \cdot 7^2 = 147$, where $g = 11$, and the theorem shows only that a nongap is ≥ 10. Actually the gaps are 1–10, 17, by another computation of Parry, so $147 \in W$.

Finally, the bound of the theorem can be sharpened in some cases. Suppose for example that $N = p \cdot q$, where p, q are distinct primes, with (say) $0 < g(q) \leq g(p)$. Suppose that $n_p(q) = 1 + g(pq) - 2 \cdot g(q)$, the bound of the theorem, is a nongap at ∞. By the proof of the theorem, we have a linear equivalence $n_p(q)(\infty) \sim \mathfrak{A}$ on $X_0(q)$ in characteristic p, where $\mathfrak{A}$ is the sum of the $n_p(q)$ supersingular points. The canonical involution $w = w_q$ fixes the set of supersingular points and hence fixes $\mathfrak{A}$, and interchanges the cusps 0 and ∞. Hence $n_p(q)((0) - (\infty)) \sim 0$. But the divisor class of $(0) - (\infty)$ has order equal to the numerator of $(q-1)/12$ (cf. [7]) so we get:

Proposition. *If $n_p(q)$, the least possible value, is a nongap at ∞ on $X_0(p \cdot q)$, then $n_p(q)$ is divisible by the numerator of $(q-1)/12$.*

Example. Let $N = 11 \cdot p$, where $p \geq 17$. Then $g(N) = p$, and $n_p(11) = p - 1$ is the least possible nongap at ∞, and a gap if $p \not\equiv 1 \pmod 5$. Also, p is a gap, since if $f(\tau)$ is the cusp form of weight 2 for $\Gamma_0(11)$, then the old-form $f(p\tau)$ for $\Gamma_0(N)$ has a zero of order p at ∞. Thus $11 \cdot p \notin W$ if $p \not\equiv 1 \pmod 5$.

References

1. A. O. L. Atkin, *Weierstrass points at cusps of* $\Gamma_0(n)$, Ann. of Math., vol. 85 (1967), pp. 42–45.
2. ———, Letter to A. Ogg (dated 9 Sept., 1974, received 17 April, 1975).
3. ———, *Modular forms of weight one, and supersingular equations*, U.S.–Japan seminar on modular functions, Ann Arbor, June 1975.

4. P. DELIGNE AND M. RAPOPORT, *Les schémas de modules de courbes elliptiques*, Springer Lecture Notes, no. 349, 1973, pp. 143–316.
5. H. LARCHER, *Weierstrass points at the cusps of* $\Gamma_0(16 \cdot p)$, *and hyperellipticity of* $\Gamma_0(n)$, Canad. J. Math., vol. 23 (1971), pp. 960–968.
6. J. LEHNER AND M. NEWMAN, *Weierstrass points of* $\Gamma_0(n)$, Ann. of Math., vol. 79 (1964), pp. 360–368.
7. A. OGG, "*Rational points on certain elliptic modular curves*" in *Analytic number theory*, Proc. Symposia Pure Math., no. 24, American Mathematical Society, Providence, 1973, pp. 221–231.
8. ———, *On the reduction modulo p of* $X_0(p \cdot M)$, U.S.–Japan seminar on modular functions, Ann Arbor, June 1975.

UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA