ON A QUESTION OF ZANNIER

NICHOLAS M. KATZ

1. Zannier's questions

We fix an integer $N \geq 1$ and an elliptic curve E over $\mathbb{Z}[1/6N]$, given by an equation

$$y^2 = f(x)$$

with $f(x)$ a cubic in $\mathbb{Z}[1/6N]$ whose discriminant is invertible in $\mathbb{Z}[1/6N]$. On E we have the differential of the first kind $\omega = dx/y$ and the differential of the second kind $\eta = xdx/y$. For each prime p not dividing $6N$, we look at this data mod p, and apply the Cartier operator $\mathcal{C}_p$. We get quantities $\alpha_p, \beta_p \in \mathbb{F}_p$ defined by

$$\mathcal{C}_p(\omega) = \alpha_p \omega, \quad \mathcal{C}_p(\eta) = \beta_p \omega.$$

What can one say about (α_p, β_p) as p varies? One knows that α_p is the reduction mod p of the trace of Frobenius, or equivalently that α_p is the Hasse invariant of E mod p. Is there an interpretation of β_p?

It is straightforward that one has the following "formulas" for α_p and β_p.

$$\alpha_p \equiv \text{the coef. of } x^{p-1} \text{ in } f(x)^{(p-1)/2} \mod p,$$
$$\beta_p \equiv \text{the coef. of } x^{p-2} \text{ in } f(x)^{(p-1)/2} \mod p.$$

To draw information from these formulas, we will assume our curve is given in Weierstrass form

$$y^2 = 4x^3 - g_2 x - g_3,$$

coefficients $g_2, g_3 \in \mathbb{Z}[1/6N]$ with $g_2^3 - 27g_3^2$ invertible in $\mathbb{Z}[1/6N]$.

Recall that over an $\mathbb{Z}[1/6]$-algebra R, a pair (E, ω) consisting of an elliptic curve over R together with a basis ω of $H^0(E, \Omega^1_{E/R}$ can be written uniquely as a Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3,$$

now with $g_2, g_3 \in R$ and with $g_2^3 - 27g_3^2$ invertible in R. Conversely, given $g_2, g_3 \in R$ with $g_2^3 - 27g_3^2$ invertible in R, the Weierstrass equation together with $\omega := dx/y$ is such an (E, ω). Viewed as functions of the input data (E, ω), $g_2 = g_2(E, \omega)$ is a modular form over $\mathbb{Z}[1/6]$ of weight 4, and $g_3 = g_3(E, \omega)$ is a modular form over $\mathbb{Z}[1/6]$ of weight 6.

One knows that for any $\mathbb{Z}[1/6]$-algebra R, the graded ring of modular forms over R is the ring $R[g_2, g_3][1/(g_2^3 - 27g_3^2)]$. The subring $R[g_2, g_3]$ is the graded ring of those modular forms over R whose q-expansion (value on the Tate curve with its canonical differential) is holomorphic, cf. the next section for a "baby" proof of this last fact.

If we attribute weight 2 to x, then $f(x) = 4x^3 - g_2x - g_3$ is isobaric of weight 6. Thus $f(x)^{(p-1)/2}$ is isobaric of weight $3(p-1)$. Thus α_p (respectively β_p) is an $\mathbb{F}_p$ polynomial in g_2, g_3 which is isobaric of weight $p-1$ (respectively isobaric of weight $p+1$). In other words, α_p is a mod p modular form of weight $p-1$, and β_p is a mod p modular form of weight $p+1$. There is an obvious guess, perhaps naive, as to what these forms must be, which turns out to be correct. In order to state it unambiguously, we must fix some notation, which we do in the next section.

2. Review of Eisenstein series

Over any $\mathbb{Q}$-algebra R, given an $(E, \omega) = (y^2 = 4x^3 - g_2x - g_3, dx/y)$, there is a unique formal parameter z along the zero section in terms of which $\omega = dz$. The Weierstrass $\wp$-function is the formal expansion of x in the parameter z, which we write as

$$x = \wp(E, \omega) = 1/z^2 + 2\sum_{k\geq 2} G_{2k}z^{2k-2}/(2k-2)!.$$

For each k, the coefficient G_{2k} is a modular form over $\mathbb{Q}$ of weigh $2k$, whose q-expansion is

$$G_{2k} = -b_{2k}/4k + \sum_{n\geq 1} q^n \sum_{d|n} d^{2k-1},$$

with b_{2k} the Bernoulli number. One knows (Kummer congruences) that b_{2k} is p-integral except for those p such that $p-1$ divides $2k$. If $p-1|2k$, then pb_{2k} is p-integral and is 1 mod p; in particular, $ord_p(1/b_{2k}) = 1$. One also knows that if if $p-1$ does not divide $2k$, then $b_{2k}/2k$ mod p depends only on the congruence class of $2k$ mod $p-1$.

From the differential equation

$$(d\wp/dz)^2 = 4\wp^3 - g_2\wp - g_3$$

for

$$\wp = 1/z^2 + 2\sum_{k\geq 2} G_{2k}z^{2k-2}/(2k-2)!,$$

one sees that G_{2k} is an isobaric $\mathbb{Q}$-polynomial in g_2 and g_3 of weight $2k$. For example, one has

$$G_4 = \frac{g_2}{20}, \ , G_6 = \frac{3g_3}{7}, \ G_8 = \frac{3g_2^2}{10}, \ G_{10} = \frac{108g_2g_3}{11},$$

$$G_{12} = \frac{756g_2^3}{65} + \frac{16200g_3^2}{91}, \ G_{14} = 1296g_2^2g_3, \ G_{16} = \frac{174636g_2^4}{85} + \frac{1166400g_2g_3^2}{17},$$

$$G_{18} = \frac{9471168g_2^3g_3}{19} + \frac{256608000g_3^3}{133}, \ G_{20} = \frac{25147584g_2^5}{25} + \frac{678844800g_2^2g_3^2}{11},$$

$$G_{22} = \frac{10671720192g_2^4g_3}{23} + \frac{103296384000g_2g_3^3}{23},$$

$$G_{24} = \frac{73581830784g_2^6}{65} + \frac{1410877440000g_2^3g_3^2}{13} + \frac{15547365504000g_3^4}{91}.$$

We will use the notation E_{2k} for the modular form

$$E_{2k} := (-4k/b_{2k})G_{2k},$$

whose q-expansion is

$$E_{2k} = 1 - (4k/b_{2k}) \sum_{n \geq 1} q^n \sum_{d|n} d^{2k-1}.$$

By the q-expansion principle, G_{2k} is a modular form over the ring $\mathbb{Z}[b_{2k}/4k]$, and E_{2k} is a modular form over the ring $\mathbb{Z}[4k/b_{2k}]$. In particular, for any prime $p \geq 5$, E_{p-1} is a modular form over $\mathbb{Z}_p$, as are both G_{p+1} (whose constant term is conguent to $-1/24 \bmod p$) and E_{p+1}.

In particular, we have

$$g_2 = E_4/12, \quad g_3 = -E_6/216, \Delta := g_2^3 - 27g_3^2 = (E_4^3 - E_6^2)/1728.$$

So over any $\mathbb{Z}[1/6]$-algebra R, the graded ring of modular forms is the polynomial ring $R[E_4, E_6][1/(E_4^3 - E_6^2)]$. To show that the subring $R[E_4, E_6]$ consists precisely of those modular forms whose q-expansion is holomorphic, it suffices to show that an isobaric element of $R[E_4, E_6]$ whose q-expansion has vanishing constant term is divisible by $E_4^3 - E_6^2$. Since both E_4 and E_6 have q-expansions with constant term 1, the constant term of the q-expansion of an element $g = \sum_{i,j} a_{i,j} E_4^i E_6^j$ is $\sum_{i,j} a_{i,j}$. If this element is isobaric of weight $w = 2k$, then $2i + 3j = k$ for each monomial which occurs. Thus j has the same parity as $k = w/2$ for each such monomial. Suppose first $k = w/2$ is even. Then j is even, and $E_4^i E_6^j$ is congruent to $E_4^{i+3j/2} = E_4^{w/4}$ modulo the ideal $(E_4^3 - E_6^2)$. Thus g is congruent to $\sum_{i,j} a_{i,j} E_4^{w/4}$ modulo this ideal. So if $\sum_{i,j} a_{i,j} = 0$, then g is divisible by $E_4^3 - E_6^2$. If $k = w/2$ is odd, then our element g is of the form $g_0 E_6$, and we apply the previous argument to g_0.

Although not modular forms, it will be convenient to introduce the q-series

$$G_2 = -b_2/4 + \sum_{n\geq 1} q^n \sum_{d|n} d = -1/24 + \sum_{n\geq 1} q^n \sum_{d|n} d$$

and

$$E_2 = 1 - 24 \sum_{n\geq 1} q^n \sum_{d|n} d = \text{Ramanujan's } P.$$

3. Relation of α_p and β_p to E_{p-1} and E_{p+1}

Fix a prime $p \geq 5$. Define $\alpha_p, \beta_p \in \mathbb{F}_p[g_2, g_3]$ to be

$$\alpha_p \equiv \text{the coef. of } x^{p-1} \text{ in } (4x^3 - g_2 x - g_3)^{(p-1)/2} \mod p,$$
$$\beta_p \equiv \text{the coef. of } x^{p-2} \text{ in } (4x^3 - g_2 x - g_3)^{(p-1)/2} \mod p.$$

Theorem 3.1. *For any prime $p \geq 5$, α_p is the reduction mod p of E_{p-1}, and β_p is the reduction mod p of $E_{p+1}/12$. Moreover, α_p and β_p have no common zero.*

Proof. The first assertion is a congruence due to Deligne, cf [**?**, 2.1]. One knows that α_p, the Hasse invariant in characteristic p, has q-expansion identically 1, as does the reduction mod p, for any $p \geq 5$, of E_{p-1} (because, by the Kummer congruence, $ord_p(4(p-1)/b_{p-1}) = 1$). So the first assertion results from the q-expansion principle.

For the second assertion, we argue as follows. We know that $\beta_p - E_{p+1}/12$ is a modular form over $\mathbb{F}_p$ of weight $p+1$. To show that it vanishes identically, it suffices to show that

$$\frac{(\beta_p - E_{p+1}/12)^6}{(g_2^3 - 27g_3^2)^{(p+1)/2}},$$

which is an $\mathbb{F}_p$ polynomial in $j = 1728g_2^3/(g_2^3 - 27g_3^2)$ of degree $(p+1)/2$, vanishes identically. The number of supersingular j values in the algebraic closure $\overline{\mathbb{F}_p}$ is $(p-1)/12, 1+(p-5)/12, 1+(p-7)/12, 2+(p-11)/12$ when p is respectively congruent mod 12 to $1, 5, 7, 11$. After checking low p by hand, one sees that for any $p \geq 5$, there are strictly more than $(p+1)/2$ **ordinary** (i.e., not supersingular) j-values in $\mathbb{F}_p$. So it suffices to show that β_p agrees with $E_{p+1}/12$ at every pair $(E/\mathbb{F}_p, \omega)$ with $E/\mathbb{F}_p$ ordinary. Since we already know that α_p is E_{p-1} mod p, it suffices to show that β_p/α_p agrees with the reduction mod p of $E_{p+1}/12E_{p-1}$ at every pair $(E/\mathbb{F}_p, \omega)$ with $E/\mathbb{F}_p$ ordinary.

To see this, we must recall some facts about $H^1_{DR}(E/\mathbb{F}_p)$ and the action of $Frob_p$ on it, for **any** $E/\mathbb{F}_p$, not necessarily ordinary, cf [Ka-PPMF, A1.2.3]. First, the inclusion of the complex

$$\mathcal{O}_E \to \Omega^1_{E/\mathbb{F}_p}$$

into the complex

$$I^{-1}(0) \to \Omega^1_{E/\mathbb{F}_p} \otimes I^{-2}(0)$$

induces isomorphisms

$$H^1_{DR}(E/\mathbb{F}_p) \cong \mathbb{H}^1(E, I^{-1}(0) \to \Omega^1_{E/\mathbb{F}_p} \otimes I^{-2}(0))$$

$$\cong H^0(E, \Omega^1_{E/\mathbb{F}_p} \otimes I^{-2}(0)) = \mathbb{F}_p dx/y \oplus \mathbb{F}_p x dx/y.$$

In general cf. [Ka-NCMT, 7.1.2, 7.2,7.3.6], one has a short exact sequence

$$0 \to H^1(E, \mathcal{H}^0_{DR}(E/\mathbb{F}_p)) \to H^1_{DR}(E/\mathbb{F}_p) \to H^0(E, \mathcal{H}^1_{DR}(E/\mathbb{F}_p)) \to 0.$$

The first term is $H^1(E, \mathcal{O}^p_E)$, which is precisely the image $Frob_p(H^1_{DR}(E/\mathbb{F}_p))$, and the sequence can be rewritten, via the Cartier operator, as

$$0 \to Frob_p(H^1_{DR}(E/\mathbb{F}_p)) \to H^1_{DR}(E/\mathbb{F}_p) \stackrel{\mathcal{C}_p}{\to} H^0(E, \Omega^1_{E/\mathbb{F}_p}) \to 0.$$

In terms of the basis $(dx/y, xdx/y)$ of $H^1_{DR}(E/\mathbb{F}_p)$, and the basis dx/y of $H^0(E, \Omega^1_{E/\mathbb{F}_p})$, the map

$$\mathcal{C}_p : H^1_{DR}(E/\mathbb{F}_p) \twoheadrightarrow H^0(E, \Omega^1_{E/\mathbb{F}_p})$$

sends dx/y to $\alpha_p dx/y$ and sends xdx/y to $\beta_p dx/y$. Because this map is surjective, at least one of α_p or β_p must be nonzero, and the image $Frob_p(H^1_{DR}(E/\mathbb{F}_p))$ is the subspace $Ker(\mathcal{C}_p)$, spanned by $\beta_p dx/y - \alpha_p x dx/y$.

When $E/\mathbb{F}_p$ is ordinary, the image $Frob_p(H^1_{DR}(E/\mathbb{F}_p))$ is precisely the "unit root subspace U", spanned by

$$xdx/y - (\beta_p/\alpha_p)dx/y.$$

Its"direction", in the coordinates $(dx/y, xdx/y)$, is β_p/α_p. It is proven in [Ka-PPMF, A2.4] that this direction is the reduction mod p of the p-adic modular form of weight 2 given by $P/12$. By the Kummer congruences, P and E_{p+1}/E_{p-1} have q-expansions which are p-integral and congruent mod p. By the q-expansion principle [Ka-PPMF, 2.7.1], the reduction mod p of P is the reduction mod p of E_{p+1}/E_{p-1}, the latter viewed as a p-adic modular form. Thus the direction of the unit root subspace, β_p/α_p, is the reduction mod p of $E_{p+1}/12E_{p-1}$ at each ordinary $(E/\mathbb{F}_p, \omega)$. □

4. Experimental findings: the CM case

Suppose we start with an elliptic curve $E/\mathbb{Z}[1/6N]$ which has CM by an order $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ in a quadratic imaginary field K, given by an equation $y^2 = f(x)$ with $f(x)$ a cubic in $\mathbb{Z}[1/6N]$ whose discriminant is invertible in $\mathbb{Z}[1/6N]$. Then

$$\mathbb{H} := H^1_{DR}(E/\mathbb{Z}[1/6N])$$

is the free $\mathbb{Z}[1/6N]$ of rank 2 with basis dx/y and xdx/y. For each prime p not dividing $6N$, $\mathbb{H}/p\mathbb{H} \cong H^1_{DR}(E \otimes \mathbb{F}_p/\mathbb{F}_p)$. If we extend scalars from $\mathbb{Z}[1/6N]$ to $\mathcal{O}_K[1/6N]$, the CM is defined on $E \otimes_{\mathbb{Z}[1/6N]} \mathcal{O}_K[1/6N]$, and so acts on $\mathbb{H} \otimes_{\mathbb{Z}[1/6N]} \mathcal{O}_K[1/6N]$. An element $u \in \mathcal{O}$ maps dx/y to udx/y; as u has eigenvalues u and $\overline{u}$, the matrix of u in the basis $dx/y, xdx/y$ must be of the form

$$\begin{pmatrix} u & a \\ 0 & \overline{u} \end{pmatrix}$$

for some $a \in \mathcal{O}_K[1/6N]$.

Lemma 4.1. *Suppose the discriminant of the order $\mathcal{O}$ is invertible in $\mathbb{Z}[1/6N]$. Then there exists a $\mathbb{Z}[1/6N]$-basis of $\mathbb{H}$ of the form $dx/y, xdx/y - Adx/y$, $A \in \mathbb{Z}[1/6N]$, which diagonalizes the action of $\mathcal{O}$. In other words, we have a $\mathbb{Z}[1/6N]$-splitting $\mathbb{H} = \mathbb{H}^{1,0} \oplus \mathbb{H}^{0,1}$ which over $\mathcal{O}_K[1/N]$ diagonalizes the CM, and in which $\mathbb{H}^{1,0}$ is the $\mathbb{Z}[1/6N]$-span of dx/y.*

Proof. Take a $\mathbb{Z}$-basis $1, u$ of $\mathcal{O}$. It suffices to find an $A \in \mathbb{Z}[1/6N]$ such that the basis $dx/y, xdx/y + Adx/y$ of $\mathbb{H}$ diagonalizes the action of u on $\mathbb{H} \otimes_{\mathbb{Z}[1/6N]} \mathcal{O}_K[1/6N]$. This amounts to the requirement that

$$[u]^\star(xdx/y - Adx/y) = \overline{u}(xdx/y - Adx/y),$$

i.e., that

$$\overline{u}xdx/y + adx/y - Audx/y = \overline{u}(xdx/y - Adx/y),$$

i.e., that

$$a - Au = -A\overline{u}.$$

Thus we get

$$A = \frac{a}{u - \overline{u}}.$$

The denominator $u - \overline{u}$ is purely imaginary. Its norm down to $\mathbb{Q}$ is the discriminant of $\mathcal{O}$, which is invertible in $\mathbb{Z}[1/6N]$. Hence $u - \overline{u}$ is invertible in $\mathcal{O}_K[1/6N]$. Thus A lies in $\mathcal{O}_K[1/6N]$. To show that A lies in $\mathbb{Z}[1/6N]$, it suffices to show that the quantity a is itself purely imaginary. For this, we argue as follows.

The matrix of $\overline{u}$ is

$$\begin{pmatrix} \overline{u} & \overline{a} \\ 0 & u \end{pmatrix}.$$

The matrix of $u+\overline{u}$ is then

$$\begin{pmatrix} u+\overline{u} & a+\overline{a} \\ 0 & u+\overline{u} \end{pmatrix}.$$

But $u+\overline{u}$ lies in $\mathbb{Z}$, say $u+\overline{u}=n$, and n acts on $\mathbb{H}$ by multiplication by n. Therefore $a+\overline{a}=0$, i.e., a is purely imaginary. □

For our CM curve $E/\mathbb{Z}[1/6N]$, if we take a good prime p which is ordinary for E, the unit root subspace in $H^1_{DR}(E\otimes\mathbb{F}_p/\mathbb{F}_p)\cong\mathbb{H}/p\mathbb{H}$ is the reduction mod p of $\mathbb{H}^{0,1}$. In other words, for each good ordinary prime, we have $\beta_p/\alpha_p\equiv A \mod p$.

We did computer experiments with convenient $\mathbb{Z}[1/6N]$-forms of elliptic curves over $\mathbb{Q}$ with each of the thirteen CM j-values in $\mathbb{Q}$, chosen using the table in Silverman's book [Si-ATEC, Appendix A&3]. Experimentally, the quantity A turned out to lie in $\mathbb{Z}$ in each case. Here is the data, giving the discriminant of $\mathcal{O}_K$, the conductor of the order $\mathcal{O}$, the equation we used, and the A we found empirically (by computing β_p/α_p for a few thousand ordinary p). [Of course that $A=0$ for $y^2=x^3-1$ and for $y^2=x^3-x$ is obvious.]

Discrim. D	Cond. f	Equation	A
-3	1	$y^2=x^3-1$	0
-3	2	$y^2=x^3-15x+22$	1
-3	3	$y^2=x^3-30x+63+1/4$	2
-4	1	$y^2=x^3-x$	0
-4	2	$y^2=x^3-11x+14$	1
-7	1	$y^2=x^3-(3/4)x^2-2x-1$	0
-7	2	$y^2=x^3-595x+5586$	9
-8	1	$y^2=x^3+4x^2+2x$	-1
-11	1	$y^2=x^3-x^2-7x+10+1/4$	1
-19	1	$y^2=x^3-38x+90+1/4$	2
-43	1	$y^2=x^3-860x+9707+1/4$	12
-67	1	$y^2=x^3-7370x+243528+1/4$	38
-163	1	$y^2=x^3-2174420x+1234136692+1/4$	724

Each of these curves has good reduction over $\mathbb{Z}[1/2D]$, so the hypotheses of Lemma 4.1 are satisfied.

For each of these thirteen curves, we also looked what happened at supersingular primes p. At such a prime, we have $\alpha_p=0$. We looked at the variation with supersingular p of β_p/p, viewed as an element of $\mathbb{R}/\mathbb{Z}$.

Empirically, it seemed in each case that the sequence $\{\beta_p/p\}_{\text{supersingular } p}$ was equidistibuted in $\mathbb{R}/\mathbb{Z}$ for Haar measure of total mass one.

5. Experimental findings: the ordinary case

We took some non-CM curves over $\mathbb{Q}$, and looked at the distribution, as p varies over good primes of ordinary reduction, at the two sequences in $\mathbb{R}/\mathbb{Z}$ given by $\{\beta_p/p\}_{\text{ordinary } p}$ and $\{(\beta_p/\alpha_p)/p\}_{\text{ordinary } p}$. Empirically, it seemed that both of these sequences were equidistributed in $\mathbb{R}/\mathbb{Z}$ for Haar measure of total mass one. [The sequence $\{\alpha_p/p\}_{\text{ordinary } p}$ tends to 0 in $\mathbb{R}/\mathbb{Z}$ by the Weil bound, so is"not interesting" from this point of view.]

We also looked at an equicharacteristic version of this question, again empirically. We fixed a large prime p, and for each $\lambda \in \mathbb{F}_p \setminus \{0,1\}$ computed $\alpha_p = \alpha_p(\lambda)$ and $\beta_p = \beta_p(\lambda)$ for each of the curves $y^2 = x(x-1)(x-\lambda)$. It seemed that both the collections $\{\beta_p(\lambda)/p\}_{\text{ordinary } \lambda}$ and $\{(\beta_p(\lambda)/\alpha_p(\lambda))/p\}_{\text{ordinary } \lambda}$ were approximately equidistibuted in $\mathbb{R}/\mathbb{Z}$ for Haar measure of total mass one.

6. How we computed α_p and β_p

We take a prime $p \geq 5$, and a cubic polynomial $f(x) \in \mathbb{F}_p[x]$ with nonzero discriminant. Recall that α_p is the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$, and β_p, the coefficient of x^{p-2} in $f(x)^{(p-1)/2}$, is also the coefficient of x^{p-1} in $xf(x)^{(p-1)/2}$ The polynomial $f(x)^{(p-1)/2}$ has degree $3(p-1)/2 < 2p-3$. Therefore x^{p-1} is the only term x^n with $n \equiv 0 \mod p-1$ which can occur in either $f(x)^{(p-1)/2}$ or in $xf(x)^{(p-1)/2}$. For any polynomial $g(x) = \sum_i a_i x^i \in \mathbb{F}_p[x]$, the sum $\sum_{t \in \mathbb{F}_p} g(t)$ is $-\sum_{d \geq 1} a_{d(p-1)}$. We apply this to the polynomials $f(x)^{(p-1)/2}$ and $xf(x)^{(p-1)/2}$.

$$\alpha_p = -\sum_{t \in \mathbb{F}_p} f(t)^{(p-1)/2}, \quad \beta_p = -\sum_{t \in \mathbb{F}_p} tf(t)^{(p-1)/2}.$$

For χ_2 the quadratic character of $\mathbb{F}_p^\times$, extended to all of $\mathbb{F}_p$ by decreeing $\chi_2(0) = 0$, we have $\chi_2(f(t)) \equiv f(t)^{(p-1)/2} \mod p$. So we have

$$\alpha_p = -\sum_{t \in \mathbb{F}_p} \chi_2(f(t)), \quad \beta_p = -\sum_{t \in \mathbb{F}_p} t\chi_2(f(t)).$$

It was these formulas we used for computing in Mathematica.

References

[Ka-NCMT] Katz, N., Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin. Inst. Hautes tudes Sci. Publ. Math. No. 39 (1970), 175232.

[Ka-PPMF] Katz, N., p-adic properties of modular schemes and modular forms. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 69190. Lecture Notes in Mathematics, Vol. 350, Springer, Berlin, 1973.

[Si-ATEC] Silverman, J., Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu