The Ramanujan differential operator, a certain CM elliptic curve and Kummer congruences

P. Guerzhoy

Abstract

Let τ be a point in the upper half-plane such that the elliptic curve corresponding to τ can be defined over $\mathbb{Q}$, and let f be a modular form on the full modular group with rational Fourier coefficients. By applying the Ramanujan differential operator D to f, we obtain a family of modular forms $D^l f$. In this paper we study the behavior of $D^l(f)(\tau)$ modulo the powers of a prime $p > 3$. We show that for $p \equiv 1 \bmod 3$ the quantities $D^l(f)(\tau)$, suitably normalized, satisfy Kummer-type congruences, and that for $p \equiv 2 \bmod 3$ the p-adic valuations of $D^l(f)(\tau)$ grow arbitrarily large. We prove these congruences by making a connection with a certain elliptic curve whose reduction modulo p is ordinary if $p \equiv 1 \bmod 3$ and supersingular otherwise.

Introduction

The holomorphic differential operator D (see below for the precise definition), which acts on the ring of modular forms of level 1, was introduced by Ramanujan [Ram16], and has appeared since then in numerous research papers in different connections (see e.g. [BKO04] as the most recent reference). One finds in [Kat73, Appendix 1] a conceptual geometric interpretation of this operator in the framework of the action of the Gauss–Manin connection on the symmetric powers of the first de Rham cohomology of an elliptic curve over a smooth scheme. This operator also plays an important role in the p-adic theory of modular forms developed by Serre and Swinnerton-Dyer [Ser73a, Ser73b].

In this paper we consider the following question. Let f be a modular form with respect to the full modular group of even integer weight k. If we apply the differentiation D to f repeatedly, we obtain a sequence of modular forms $D^l(f)$ with $l \geqslant 0$. Assume now that f has rational Fourier coefficients. Therefore, all $D^l(f)$ may be written as isobaric polynomials in Q and R (see § 1 below for the notation). The weights of Q and R are 4 and 6 respectively, and the weight of $D^l(f)$ is $k + 2l$. Pick a point τ on the complex upper half-plane such that the corresponding elliptic curve is defined over $\mathbb{Q}$. In other words, there is a non-zero $S = S(\tau)$ such that the numbers

$$\mathcal{Q} = Q(\tau)/S^2 \quad \text{and} \quad \mathcal{R} = R(\tau)/S^3$$

are rationals. One actually can find τ on the upper half-plane and $S(\tau) \in \mathbb{C}^*$ such that these two numbers become any prescribed pair of rationals. Now ask about p-adic properties of the rational numbers

$$b_f(l) = D^l(f)(\tau)/S^{k/2+l}.$$

Fix once and for all a prime $p > 3$, and put $\mathcal{Z} = \mathbb{Z}_{(p)}$. Assume that $\mathcal{Q}, \mathcal{R} \in \mathcal{Z}$, and at least one of these numbers is not divisible by p in $\mathcal{Z}$. There exists $M \in \mathcal{Z}$ such that $b_{Mf}(n) = Mb_f(n) \in \mathcal{Z}$

for any $n \geqslant 0$. Thus we can and will assume that $b_f(n) \in \mathcal{Z}$. Numerical experiments show that the p-adic properties in question depend crucially on the residue of $p \bmod 3$. This research was undertaken to explain this phenomenon.

We need some more notation to formulate our result. Put

$$\delta(\tau) = 1728\Delta/S^6 = \mathcal{Q}^3 - \mathcal{R}^2 = S^{-6}\, 1728q \prod_{n \geqslant 1}(1 - q^n)^{24},$$

where $q = \exp(2\pi i\tau)$. Note that δ depends on τ in a complicated way, because the choice of S depends on τ. There is a certain freedom in this choice: we only assume that $\mathcal{Q}$ and $\mathcal{R}$ are rationals and one of them is a p-unit. This defines S only up to multiplication by a p-unit. On the other hand, a choice of S only exists for those τ that correspond to elliptic curves defined over the rationals.

Let c be any integer such that

$$c \equiv \begin{cases} 0 & \text{if } p \equiv 2 \mod 3, \\ \frac{1}{2}(p-1)(-1)^{(p-1)/3}\delta(\tau)^{(p-1)/6} & \text{if } p \equiv 1 \mod 3. \end{cases} \pmod{p} \tag{1}$$

THEOREM 1. *Let f be a modular form of even integral weight on the full modular group $SL_2(\mathbb{Z})$ with rational Fourier coefficients.*

For any integers $n \geqslant r > 0$ the following congruence holds:

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}c^{r-j}b_f(n + j(p-1)) \equiv 0 \mod p^r.$$

Note that if $p \equiv 2 \bmod 3$ or if $\delta(\tau)$ is divisible by p one can take $c = 0$, and the congruences degenerate to

$$b_f(n + r(p-1)) \equiv 0 \mod p^r \quad \text{as soon as } n \geqslant r > 0.$$

Otherwise the situation is quite different. For example, put $r = 1$ in Theorem 1 and obtain modulo p periodicity for the numbers $b_f(l)$:

$$b_f(n + p - 1) \equiv cb_f(n) \mod p \quad \text{for} \quad n \geqslant 1$$

with a certain p-unit c. This is an interesting phenomenon to observe in numerical experiments.

The proof of Theorem 1 splits into several parts. First, we apply the differential operator D to the modular form Q repeatedly, and construct a generating function X (see (4) below) out of the modular forms $D^l(Q)$. We calculate this function explicitly in terms of the Weierstraß $\wp$-function in Theorem 2. The generating function depends on two variables: in terms of the $\wp$-function these are a lattice and a point in the complex plane modulo the lattice. An amusing separation of variables phenomenon takes place at this moment: all the lattices that may appear for different finite values of τ correspond to the same elliptic curve over $\mathbb{C}$, namely, to the one whose j-invariant is zero.

The consideration of the degenerate case $\tau = i\infty$ yields Proposition 2, which allows us to reduce the proof of Theorem 1 for an arbitrary modular form f to the special case $f = Q$.

An application of the addition formula for the Weierstraß $\wp$-function allows us to consider X as a function on the formal group associated to the elliptic curve (9); moreover, the normalized invariant differentiation on this formal group coincides with the differentiation d/dt. This is proved in Proposition 3 and the remarks following it.

The Kummer-type congruences claimed in Theorem 1 follow in this situation from the works of Carlitz [Car41, Car49] and Snyder [Sny93, Sny85]; we formulate the exact statement that we need as Proposition 4.

We conclude the proof of Theorem 1 with the calculation of $c \bmod p$ as in (1). This quantity evidently governs the congruences, and is governed by the $\bmod\, p$ reduction of the elliptic curve (9).

In particular, the cases when c is divisible and not divisible by p correspond to the cases when the Hasse invariant of (9) is 0 and 1 respectively. Although this is a short calculation, it uses the beautiful connection between the formal group of an elliptic curve and its L-series, found by Honda, the Atkin and Swinnerton-Dyer conjecture which was proved on the basis of this connection, and an elegant elementary method of computation of the Hasse invariant invented by Manin [Man61].

In the last section of this paper we make a few remarks concerning the connection between our results and the congruence properties of Bernoulli–Hurwitz numbers.

1. Calculation of a generating function for the differential operator

For the particular Eisenstein series of low weights we use the classical notation of Ramanujan:

$$P = 1 - 24 \sum_{n \geqslant 1} \sigma_1(n) q^n,$$

$$Q = 1 + 240 \sum_{n \geqslant 1} \sigma_3(n) q^n,$$

$$R = 1 - 504 \sum_{n \geqslant 1} \sigma_5(n) q^n.$$

The holomorphic function P is not actually an Eisenstein series, and not even a modular form.

The differential operator

$$\frac{1}{2\pi i} \frac{d}{d\tau} = q \frac{d}{dq}$$

does not preserve modularity, but its corrected version

$$D = -6q \frac{d}{dq} + \frac{k}{2} P \tag{2}$$

does. Its action on Q and R is given by

$$D(Q) = 2R, \quad D(R) = 3Q^2. \tag{3}$$

We remark that our definition of D differs from the usual one [Lan76, ch. X] by the factor of -6.

Consider the generating function

$$X = X(t, \tau) = \sum_{n \geqslant 0} \frac{D^n(Q)(\tau)}{S^{n+2}} \frac{t^n}{n!} \in \mathbb{Z}[\mathcal{Q}, \mathcal{R}][[t]]. \tag{4}$$

We are going to calculate this function.

Denote by $\wp(z, L)$ the Weierstraß $\wp$-function. Consider the lattice in the complex plane generated by 1 and $\rho = e^{\pi i/3} = (1 + \sqrt{-3})/2$. For any complex number $\alpha \neq 0$ consider the lattice $L = \alpha^{-1} \langle \rho, 1 \rangle$. The difference

$$\wp'(z, L)^2 - 4\wp(z, L)^3 = -g_3(L) \tag{5}$$

does not depend on z. It is known that

$$g_3(\langle \rho, 1 \rangle) = 140 \sum_{(m,n) \neq (0,0)} \frac{1}{(m + n\rho)^6} = \frac{1}{27} \left(\frac{\Gamma(1/3)^2}{\Gamma(2/3)} \right)^6,$$

but we do not need this precise value; we will use only the fact that $g_3(\langle \rho, 1 \rangle) \neq 0$. For any τ in the complex upper half-plane choose α such that

$$g_3(L) = \alpha^{-6} g_3(\langle \rho, 1 \rangle) = 4\delta(\tau)$$

585

and find a complex number $a = a(\tau)$ that satisfies

$$\begin{cases} \wp(a, L) = \mathcal{Q}(\tau), \\ \wp'(a, L) = 2\mathcal{R}(\tau). \end{cases} \tag{6}$$

THEOREM 2. *The following holds:*

$$X = \wp(a + t, L).$$

To prove this theorem we need the following lemma, which describes an abstract situation, and has nothing to do with modular forms. Let $\mathcal{Z}$ be a ring of characteristic zero, and assume that 2 and 3 are invertible in this ring. Any differential operator $\mathcal{D}$, which acts on the ring of polynomials in two variables $\mathcal{Z}[\mathcal{Q}, \mathcal{R}]$, is defined by its action on the generators $\mathcal{Q}$ and $\mathcal{R}$:

$$\mathcal{D} = A \frac{\partial}{\partial \mathcal{Q}} + B \frac{\partial}{\partial \mathcal{R}} \quad \text{with} \quad A, B \in \mathcal{Z}[\mathcal{Q}, \mathcal{R}].$$

Consider the generating function

$$X = \sum_{n \geqslant 0} \mathcal{D}^n(\mathcal{Q}) \frac{t^n}{n!} \in \mathcal{Z}[\mathcal{Q}, \mathcal{R}][[t]] \tag{7}$$

(we assume that $\mathcal{D}^0(\mathcal{Q}) = \mathcal{Q}$).

LEMMA 1. *Assume that $\mathcal{D}^2(\mathcal{Q}) = \lambda \mathcal{Q}^2$ with $\lambda \in \mathcal{Z}$. Then*

$$\ddot{X} = \lambda X^2,$$

where a dot denotes the differentiation with respect to t.

Proof. We have

$$\dot{X} = \sum_{n \geqslant 0} \mathcal{D}^{n+1}(\mathcal{Q}) \frac{t^n}{n!}$$

and

$$\ddot{X} = \sum_{n \geqslant 0} \mathcal{D}^{n+2}(\mathcal{Q}) \frac{t^n}{n!} = \lambda \sum_{n \geqslant 0} \mathcal{D}^n(\mathcal{Q}^2) \frac{t^n}{n!}.$$

Using induction on m and Leibnitz's rule one shows that

$$\mathcal{D}^m(\mathcal{Q}^2) = \sum_{n=0}^{m} \binom{m}{n} \mathcal{D}^n(\mathcal{Q}) \mathcal{D}^{m-n}(\mathcal{Q}).$$

Thus we have

$$\ddot{X} = \lambda \sum_{m \geqslant 0} \frac{t^m}{m!} \sum_{n=0}^{m} \binom{m}{n} \mathcal{D}^n(\mathcal{Q}) \mathcal{D}^{m-n}(\mathcal{Q}).$$

Since also

$$X^2 = \left(\sum_{n \geqslant 0} \mathcal{D}^n(\mathcal{Q}) \frac{t^n}{n!} \right)^2 = \sum_{m \geqslant 0} t^m \sum_{n=0}^{m} \frac{1}{n!} \mathcal{D}^n(\mathcal{Q}) \frac{1}{(m-n)!} \mathcal{D}^{m-n}(\mathcal{Q}),$$

the lemma is proved. $\square$

Multiply the differential equation in Lemma 1 by $\dot{X}$ and integrate it once.

COROLLARY 1. *Under the assumptions of Lemma 1 the generating function X satisfies the differential equation*

$$\dot{X}^2 = \tfrac{2}{3} \lambda X^3 + C. \tag{8}$$

with $C = (\mathcal{D}(\mathcal{Q}))^2 - \tfrac{2}{3} \lambda \mathcal{Q}^3$.

From now on we specialize to the ring of modular forms; thus Q and R become functions on the upper half-plane, and D becomes the differential operator (2). Fix the point τ, choose S and consider the differential operator $\mathcal{D} = S^{-1}D$ acting on $\mathcal{Z}[\mathcal{Q}, \mathcal{R}]$. It follows from (3) that

$$\mathcal{D}(\mathcal{Q}) = 2\mathcal{R}, \quad \mathcal{D}(\mathcal{R}) = 3\mathcal{Q}^2.$$

Both operators D and $\mathcal{D}$ satisfy the condition of Lemma 1 with $\lambda = 6$. Take $\mathcal{Z} = \mathbb{Z}_{(p)}$; thus the former operator acts on the ring $\mathcal{Z}[Q, R]$ of modular forms with rational p-integer Fourier coefficients, while the latter acts on the ring $\mathcal{Z}[\mathcal{Q}, \mathcal{R}]$ of modular forms with p-integer values at τ. The equation of the elliptic curve, defined by (8), is

$$y^2 = x^3 - \delta(\tau) \tag{9}$$

with

$$x = X \quad \text{and} \quad y = \dot{X}/2. \tag{10}$$

Proof of Theorem 2. The generating function X defined by (4) satisfies the differential equation (8), and coincides with (7). Since the Weierstraß $\wp$-function, considered as a function on the complex variable z, satisfies the differential equation (5) and the initial conditions (6), the result follows from the uniqueness of the solution. □

2. The degenerate case

Consider the constant terms of the q-expansions of the modular forms $D^n(Q)$. To do so pick $\tau = i\infty$, and solve Equation (8) with $C = 4\delta(i\infty) = 0$. Choose $S = 1$, which is suitable for this τ. The initial conditions (6) then become $X(0) = Q(i\infty) = 1$ and $\dot{X}(0) = 2R(i\infty) = 2$.

PROPOSITION 1. *As $\tau \in i\infty$, the generating function is given by*

$$X(t, i\infty) = \frac{1}{(t-1)^2}.$$

In particular, $D^n(Q)(i\infty) = D^n(\mathcal{Q})(i\infty) = (n+1)!$.

Note that the quantities $D^n(Q)(i\infty) = D^n(\mathcal{Q})(i\infty)$ clearly never vanish.

The following proposition is a standard consequence of the fact that $D^n(Q)(i\infty) \neq 0$ together with the fact that $D(\Delta) = 0$.

PROPOSITION 2. *Any modular form f with rational Fourier coefficients can be written as a finite rational linear combination*

$$f = \beta_0 D^l(Q) + \beta_1 \Delta D^{l-6}(Q) + \beta_2 \Delta^2 D^{l-12}(Q) + \cdots.$$

For a modular form f of even integer weight k with rational Fourier coefficients, consider the generating function

$$X_f = X_f(t, \tau) = \sum_{n \geqslant 0} \frac{D^n(f)}{S^{k/2+n}} \frac{t^n}{n!} \in \mathbb{Z}[\mathcal{Q}, \mathcal{R}][[t]].$$

Thus for the function X previously introduced (4) we have $X = X_Q$. Proposition 2 now implies that X_f is equal to a finite rational linear combination of the derivatives of X with respect to t:

$$X_f = \beta_0 X^{(l)} + \beta_1 \Delta X^{(l-6)} + \beta_2 \Delta^2 X^{(l-12)} + \cdots. \tag{11}$$

The first claim of Theorem 1 follows from this. Moreover, (11) implies that it is sufficient to prove Theorem 1 for $X_f = X$.

P. GUERZHOY

3. The generating function X as a function on a formal group

Theorem 2 asserts that X is a function on the elliptic curve (9), and we will now consider it as a function on the corresponding formal group, that is a formal power series in the group parameter. Let $E(V, W)$ be the formal group of the elliptic curve (9), and let $z = -x/y$ be the parameter at the origin. We refer to [Sil86, ch. IV] for the definitions and construction.

PROPOSITION 3. *Assume that* $\wp(a, L), \wp'(a, L) \in \mathcal{Z}$. *Then there exists a power series* $\varphi(z) \in \mathcal{Z}[[z]]$ *such that*
$$X = \wp(a, L) + z\varphi(z).$$
In other words, X is a function on the group.

Proof. Since we do not consider here any lattice other than L, we omit it from the notation and simply write $\wp(t) = x$ and $\wp'(t) = 2y$ for $\wp(t, L)$ and $\wp'(t, L)$. Tate's construction [Sil86, ch. IV, § 1] implies that $\wp'(t) = -1/(Uz^3)$, where U is a unit in $\mathcal{Z}[[z]]$. Thus $\wp(t) = -z\wp'(t)/2 = 1/(2Uz^2)$. Substitute $u = a$ and $v = t$ into the addition formula for the Weierstraß $\wp$-function
$$\wp(u + v) = \wp(u) + \frac{1}{2}\frac{\partial}{\partial u}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)$$
and take into the account that $\wp''(t) = 6\wp(t)^2$ to obtain
$$\wp(a + t) = \wp(a) + z^2 U\frac{6\wp(a)^2}{1 + \wp(a)z^2 U} - 2\wp'(a)zU\frac{\wp'(a)z^3 U + 1}{(1 + \wp(a)z^3 U)^2}.$$
Proposition 3 follows from this formula. $\qquad\square$

Since the normalized invariant differential on the formal group $E(V, W)$ is given by [Sil86, ch. IV]
$$\omega = \frac{dV}{E_W(V, 0)} = \frac{dx}{2y},$$
we can write the normalized invariant differentiation using (10) as
$$\mathcal{D} = E_W(V, 0)\frac{d}{dV} = 2y\frac{d}{dx} = \frac{d}{dt}. \tag{12}$$

4. Kummer congruences for functions on formal groups

Let $F = F(V, W)$ be a formal group defined over the ring $\mathcal{Z}$. We refer to [Hon68, Haz78] for basic definitions. We denote by
$$\lambda(T) = \sum_{n \geqslant 1}\frac{e(n)}{n}T^n$$
the logarithmic series for F, and by
$$\varepsilon(t) = \sum_{n \geqslant 1}\frac{a(n)}{n!}t^n$$
the exponential series with $\lambda(\varepsilon(t)) = t$. The normalized invariant differentiation after the substitution $T = \varepsilon(t)$ is given by
$$\mathcal{D} = \frac{1}{\lambda'(T)}\frac{d}{dT} = F_W(T, 0)\frac{d}{dT} = \frac{d}{dt}. \tag{13}$$

We pick any power series $\varphi \in \mathcal{Z}[[T]]$. This is a function on the formal group F. Note that the differential operator $\mathcal{D}$ acts on this function. For non-negative integers l define the numbers
$$B_\varphi(l) = \mathcal{D}^l(\varphi)(0).$$

588

Note that in the case when $F = E$, where E is the formal group of the elliptic curve (9), the invariant differentiation (13) becomes (12): both are just d/dt. Thus we have

$$B_X(l) = b_Q(l)$$

for $l \geqslant 0$. These numbers satisfy congruences. The following precise statement essentially comes from the works of Carlitz [Car41, Car49] and, in the context of formal groups, from the works of Snyder [Sny93, Sny85].

PROPOSITION 4. *Pick $c \equiv e(p) \bmod p$. For any function f and any integers $n \geqslant r > 0$ the following congruences hold:*

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}c^{r-j}b_f(n + j(p-1)) \equiv 0 \mod p^r.$$

5. Calculation of $e(p)$ modulo p

It follows from the Atkin and Swinnerton-Dyer conjecture, proved by Cartier [Car71] (see [Haz78, ch. 33] for the full and correct proof), that for the formal group of any elliptic curve E defined over $\mathbb{Q}$,

$$e(p) \equiv a_p \mod p,$$

where a_p is the pth coefficient of the Hasse–Weil L-function of E. That is

$$a_p = 1 + p - \#E(\mathbb{F}_p).$$

It follows from a classical argument (see [Man61] or [Sil86, ch. V, proof of Theorem 4.1]) that, for an elliptic curve with an equation $y^2 = \phi(x)$, this quantity is congruent modulo p to the coefficient of x^{p-1} in the polynomial $\phi(x)^{(p-1)/2}$. For the formal group of the elliptic curve (9), it follows that $e(p) \equiv c \bmod p$, where c is given by (1), and this concludes the proof of Theorem 1.

6. Remarks about the connection with Bernoulli–Hurwitz numbers

The Bernoulli–Hurwitz numbers $BH(n + 2)$ are defined as the (properly normalized) values of Eisenstein series at a CM-point, and, consequently, as the Laurent expansion coefficients of the Weierstraß $\wp$-function:

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geqslant 2}\frac{BH(n + 2)}{n + 2}\frac{z^n}{n!}.$$

Hurwitz [Hur99] considered these numbers (for the Weierstraß $\wp$-function associated with the lemniscatic curve $y^2 = 4x^3 - 4x$) as being analogues for the Gaussian field of the Bernoulli numbers for the rational field $\mathbb{Q}$. (Note that one obtains Bernoulli numbers when one considers the degenerate elliptic curve at infinity, and the constant terms of Eisenstein series as their values at infinity.) In particular, Hurwitz observed congruences for the Bernoulli–Hurwitz numbers similar to the Kummer congruences for Bernoulli numbers and to the congruences in Theorem 1. Generalizations of and different approaches to such congruences have been considered since the time of Hurwitz by many authors (see, for example, [Lic80, Kat81, Kat77]).

In the case under consideration in this paper, we consider, according to Theorem 2, the Taylor expansion of the Weierstraß $\wp$-function associated with the elliptic curve (9) at a point different from the origin. This situation is easier, because we do not need to modify the function in order to kill the pole at the origin, but the result is weaker: Theorem 1 in the ordinary ($c \neq 0$) case is essentially equivalent to the existence of a $\mathbb{Z}_p$-measure with prescribed moments [Sny93], and no restriction to a $\mathbb{Z}_p^*$-measure makes sense. On the other hand, this paper provides a more general outcome: we consider bad, supersingular and ordinary primes simultaneously, and are able to prove a result for an arbitrary modular form.

589

It is amusing to remark that as Hurwitz considers the lemniscatic curve, which is attached to the point $\tau = i$, our consideration of the Ramanujan differential operator led us to the elliptic curve attached to the point $\tau = \rho = \exp(\pi i/3)$, and these two, i and ρ, are the only elliptic points in the fundamental domain for $SL_2(\mathbb{Z})$.

ACKNOWLEDGEMENT

REFERENCES

BKO04   J. H. Bruinier, W. Kohnen and K. Ono, *The arithmetic of values of modular functions and the divisors of modular forms*, Compositio Math. **140** (2004), 552–566.

Car41   L. Carlitz, *The coefficients of the reciprocal of a series*, Duke Math. J. **8** (1941), 689–700.

Car49   L. Carlitz, *Congruences for the coefficients of the Jacobi elliptic functions*, Duke Math. J. **16** (1949), 297–302.

Car71   P. Cartier, *Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques*, in *Actes du Congrès International des Mathématiciens*, Nice, 1970, tome 2 (Gauthier-Villars, Paris, 1971), 291–299.

Haz78   M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78 (Academic Press, New York, 1978).

Hon68   T. Honda, *Formal groups and zeta-functions*, Osaka J. Math. **5** (1968), 199–213.

Hur99   A. Hurwitz, *Über die Entwicklungscoefficienten der lemniscatischen Funktionen*, Math. Ann. **51** (1899), 196–226.

Kat73   N. M. Katz, *p-adic properties of modular schemes and modular forms*, in *Modular functions of one variable, III (Proc. Int. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 350 (Springer, Berlin, 1973), 69–190.

Kat77   N. M. Katz, *Formal groups and p-adic interpolation*, Astérisque **41−42** (1977), 55–65.

Kat81   N. M. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 667–678.

Lan76   S. Lang, *Introduction to modular forms*, Grundlehren Math. Wiss., vol. 222 (Springer, Berlin, 1976).

Lic80   S. Lichtenbaum, *On p-adic L-functions associated to elliptic curves*, Invent. Math. **56** (1980), 19–55.

Man61   Ju. I. Manin, *The Hasse–Witt matrix of an algebraic curve* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), 153–172; English translation in AMS Transl. **45** (1965), 245–264.

Ram16   S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Phil. Soc. **22** (1916), 159–184; *Collected papers*, reprint (Chelsea, New York, 1962), 136–162.

Ser73a   J.-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), exp. no. 416, Lecture Notes in Mathematics, vol. 317 (Springer, Berlin, 1973), 319–338.

Ser73b   J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, in *Modular Functions of One Variable, III (Proc. Int. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 350 (Springer, Berlin, 1973), 191–268.

Sil86   J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106 (Springer, New York, 1986).

Sny85   C. Snyder, *Kummer congruences in formal groups and algebraic groups of dimension one*, Rocky Mountain J. Math. **15** (1985), 1–11.

Sny93   C. Snyder, *p-adic interpolation of the coefficients of Hurwitz series attached to height one formal groups*, Rocky Mountain J. Math. **23** (1993), 339–351.

P. Guerzhoy   pasha@math.temple.edu

Department of Mathematics, Temple University, 1805 N. Broad Street, Philadelphia, PA 19122, USA