ABSTRACTS OF PAPERS

MATIJA KAZALICKI

1. Introduction

My research interests are in number theory. In particular, I am interested in modular forms and related functions. Modular forms have fundamental roles in many branches of mathematics and number theory, they are central to the proof of Fermat's last theorem, and the Langlands program, have arithmetic applications and geometric interpretations, are related to L-functions and elliptic curves, the Birch and Swinnerton-Dyer conjecture, and yield applications in string theory, combinatorics, cryptography and mathematical physics. A usual way to define modular form is as a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying a growth condition, as well as a certain symmetry under the action of $\Gamma := SL_2(\mathbb{Z})$ or some other subgroup. That is, $f(\frac{a\tau+b}{c\tau+d}) = (c\tau + d)^k f(\tau)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. A modular form $f(\tau)$ has a *Fourier expansion* $f(\tau) = \sum_{n=0}^{\infty} a_f(n)q^n$, where $q = e^{2\pi i\tau}$. Fourier coefficients a_n, often have an important arithmetic, geometric or combinatorial interpretation.

2. My work

2.1. **Linear relations between Fourier coefficients.** As mentioned in introduction, modular forms for $\mathrm{SL}_2(\mathbb{Z})$ have a Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_f(n)q^n$. It is natural to ask whether there are universal linear relations between the initial coefficients of all modular forms of weight k, i.e. one wants to describe a structure of

$$L_{k,N} := \{(c_0, \dots, c_{N+d(k)} \in \mathbb{C}^{d(k)+N+1}) : \sum_{\nu=0}^{N+d(k)} c_\nu a_f(\nu) = 0, \text{ for every } f \in \mathscr{M}_k\}. \tag{1}$$

Here $d(k)$ is a dimension of the space $\mathscr{M}_k$ of modular forms of weight k. This question was answered by Choie, Kohnen and Ono [9].

In the light of the well known analogy between number fields and function fields, it is natural to ask whether similar result should hold for Drinfeld modular forms.

Define $\sigma(k) \in \{0, q-1, 2(q-1), \dots, q(q-1)\}$ by the relation $k \equiv \sigma(k) (\mathrm{mod}\, q^2-1)$. Denote my $\mathscr{M}_k^l$ the space of Drinfeld modular forms of weight k and type l. For each $G \in \mathscr{M}_{q^2-1}N^0$, define numbers $b(k, N, G; \nu)$ by

$$\frac{Gg^q h}{E^{(\sigma(k))}\Delta^{N+d(k)}} = \sum_{\nu=0}^{N+d(k)} b(k, N, G; \nu)t^{-\nu(q-1)+1} + \sum_{\nu=1}^{\infty} c(k, N, G; \nu)t^{\nu(q-1)+1}. \tag{2}$$

Here g, h, $E^{(k)}$, and Δ are certain Drinfeld modular forms, and the function t is a Drinfeld modular form analogue of function $q = e^{2\pi i\tau}$. Generalizing the work of Choie, Kohnen and Ono [9], we have the following description of the $L_{k,N}$.

Theorem 1 (K. [17]). *The map $\phi_{k,N} : \mathscr{M}^0_{(q^2-1)N} \to L_{k,N}$ defined by*

$$\phi_{k,N}(G(z)) = (b(k, N, G; \nu) : \nu = 0, 1, \dots, d(k) + N)$$

defines a linear isomorphism between $\mathscr{M}^0_{(q^2-1)N}$ and $L_{k,N}$.

2.2. **Zeros of certain Drinfeld modular functions.** "Monstrous moonshine" is one of the most interesting results connecting modular forms and Lie algebras. Ultimately proved by Borcherds [7] in 1992, monstrous moonshine relates the Fourier coefficients of the modular $j(\tau)$ invariant to dimensions of irreducible representations of the Monster group.

Related to this, we consider the sequence of modular functions $j_m(z)$ defined by

$$j_1(z) := j(z) - 744 \qquad \text{and} \qquad j_m(z) := j_1(z)|T_0(m),$$

where $T_0(m)$ is normalized mth weight zero Hecke operator. Also, we define integer coefficients polynomials $P_n(x)$ satisfying $P_n(j(z)) = j_m(z)$.

These functions satisfy the beautiful identity

$$j(\tau) - j(z) = p^{-1} \exp\left(- \sum_{n=1}^{\infty} j_n(z) \cdot \frac{p^n}{n} \right),$$

which is equivalent to the famous denominator formula for the Monster Lie algebra

$$j(\tau) - j(z) = p^{-1} \prod_{m>0 \text{ and } n \in \mathbb{Z}} (1 - p^m q^n)^{c(mn)}.$$

Here $q = e^{2\pi i z}$, $p = e^{2\pi i \tau}$, and the exponents $c(n)$ are defined as the coefficients of $j_1(z) = \sum_{n=-1}^{\infty} c(n) q^n$.

K. Ono has conjectured that all the polynomials $P_m(x)$ are irreducible, and recently P. Guerzhoy proved a partial result toward this conjecture by presenting infinite families of these polynomials which are provably irreducible [13]. In addition, it is known that the zeros of each $j_m(z)$ in the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ are located on the unit circle $|z| = 1$ [1].

It is natural to ask does the similar result hold for Drinfeld modular functions. We establish the following theorem [18].

Theorem 2 (K. [18]). *The roots of the polynomials $P_m(x)$ have absolute value q^q. The zeros of $j_m(z)$ in the fundamental domain $\mathscr{F} = \{z \in \Omega : |z| = \inf\{|z - a| : a \in A\} \geq 1\}$ are on the unit circle $|z| = 1$. If q is odd, they are transcendental over K.*

2.3. **The class numbers of quadratic imaginary fields.** Let d be prime or the product of two primes, $K = \mathbb{Q}(\sqrt{-d})$ an imaginary quadratic field, and $Cl(\mathbb{Q}(\sqrt{-d}))$ its ideal class group. These groups are subject of many interesting theorems and conjectures, like for example, the Gauss class number problem and the Cohen-Lenstra heuristics.

Starting with Gauss, who developed genus theory, many people have investigated the structure of the 2-Sylow subgroup of $Cl(\mathbb{Q}(\sqrt{-d}))$. In the case when $d = p$ is prime, Cohn and Barrucand [5] in 1961 discovered the beautiful fact that the class number $h(-p) := h(\mathbb{Q}(\sqrt{-p}))$ is divisible by 8 if and only if $p = x^2 + 32y^2$, where x and y are integers. In the early 1980s [45], Williams showed that if $\epsilon = T + U\sqrt{p}$ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$, then

$$h(-p) \equiv T + (p-1) \pmod{16},$$

where $8|h(-p)$.

If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are primes above 2 and 3 in $\mathbb{Q}(\sqrt{d})$ (we assume that 2 and 3 split), we denote by $G_{m,n}$ the ray class group of $\mathbb{Q}(\sqrt{d})$ of modulus $\mathfrak{m} = \mathfrak{p}_1^m \mathfrak{p}_2^n$, where $m, n > C_d$, for some explicit constant C_d. Denote by $r_k(\mathbb{Q}(\sqrt{d}))$ the k-rank of any such $G_{m,n}$. The following theorem and the other similar "reflection" results are proved in [19].

Theorem 3 (K.[19]). *Suppose that $p \equiv 1 \pmod{16}$ is prime. Then we have*

$$\begin{aligned} 4||h(-p) &\iff r_4(\mathbb{Q}(\sqrt{p})) = 1 \\ 8||h(-p) &\iff r_4(\mathbb{Q}(\sqrt{p})) = 2 \text{ and } r_8(\mathbb{Q}(\sqrt{p})) = 1 \\ 16|h(-p) &\iff r_8(\mathbb{Q}(\sqrt{p})) = 2. \end{aligned}$$

As a consequence of these theorems, we recover Williams' s result and prove the following generalization.

Theorem 4 (K.[19]). *If p and q are primes for which $p, q \equiv 5 \pmod 8$, then we have*

$$16|h(-pq) \iff \begin{cases} T \equiv 9 \pmod{16} & \text{if } \left(\frac{p}{q}\right) = 1 \text{ and } \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = -1, \\ T \equiv 4 \pmod 8 & \text{if } \left(\frac{p}{q}\right) = -1, \end{cases}$$

where $\epsilon = T + U\sqrt{pq}$ is a fundamental unit of $\mathbb{Q}(\sqrt{pq})$. When $Norm(\epsilon) = -1$, we choose the fundamental unit such that $T \equiv 1 \pmod 4$.

2.4. **The central values of L-functions.** The central values of L-functions are of great importance in number theory since they encode deep relationship between invariants of the corresponding algebraic object. For example, for the Dedekind zeta function, the class number formula relates the class number and the regulator of an algebraic number field. For the L-function associated to the elliptic curve E, the Birch and Swinnerton-Dyer conjecture predicts the rank of Mordell-Weil group, and relates various invariants of E including the order of the Tate-Shafarevich group, the regulator, and the product of Tamagawa numbers.

We consider the L-functions associated to Ramanujan's Delta-function,

$$\Delta(z) = \sum_{n=0}^{\infty} \tau(n) z^n := q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

the unique weight 12 normalized cusp form for the full modular group. Also, denote by $\sigma_k(n) = \sum_{d|n} d^k$ the sum of kth powers of divisors of n. Ramanujan observed that modulo the powers of certain small primes, there are congruences relating $\tau(n)$ and $\sigma_k(n)$. For example, for the powers of two the following congruences are due to Kolberg[24]:

$$\begin{array}{llll} \tau(n) \equiv \sigma_{11}(n) & (\text{mod } 2^{11}) & \text{if } n \equiv 1 & (\text{mod } 8) \\ \tau(n) \equiv 1217\sigma_{11}(n) & (\text{mod } 2^{13}) & \text{if } n \equiv 3 & (\text{mod } 8) \\ \tau(n) \equiv 1537\sigma_{11}(n) & (\text{mod } 2^{12}) & \text{if } n \equiv 5 & (\text{mod } 8) \\ \tau(n) \equiv 705\sigma_{11}(n) & (\text{mod } 2^{14}) & \text{if } n \equiv 7 & (\text{mod } 8). \end{array}$$

By the work of Eichler, Shimura, Deligne and Serre, for every prime l there is a 2-dimensional l-adic Galois representation $\rho_l : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_l)$ with the property that $Tr(\rho(\text{Frob}_p)) = \tau(p)$ for every prime $p \neq l$ ($\text{Frob}_p \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is a Frobenius element for the prime p). Swinnerton-Dyer [41] showed that the image of these representations is "small" for primes $l = 2, 3, 5, 7$ and 691. Moreover, he showed that Kolberg's congruences determine the structure of ρ_2. More precisely, up to conjugation by an element of $GL_2(\mathbb{Q}_2)$, the image of ρ_2 consists of matrices of the form

$$\sigma = \begin{pmatrix} 1 + 2^7 A & 2^4 B \\ 2^5 C & 1 + 2D \end{pmatrix},$$

where $A, B, C, D \in \mathbb{Z}_2$. Since the representation ρ_2 is reducible modulo 2^5, inspired by the Bloch-Kato conjecture, one expects to find some congruences modulo the powers of two between the algebraic part of the central value of the L-function associated to the Delta function and its quadratic twists, and a value of the corresponding Dirichlet L-function.

For a positive fundamental discriminant d, we denote by Δ_d the twist of $\Delta(z)$ by the quadratic character $\left(\frac{d}{\cdot}\right)$. Square roots of the algebraic parts $\sqrt{L^{alg}(\Delta_d, 6)}$ will be defined later in this section. We prove the following theorem.

Theorem 5 (K. [19]). *If d is a positive fundamental discriminant, then the following are true:*

$$\begin{array}{llll} \sqrt{L^{alg}(\Delta_d, 6)} \equiv 49 \cdot 4L_2(11, \chi_d) & (\text{mod } 2^9) & \text{for } d \equiv 1 & (\text{mod } 16) \\ \sqrt{L^{alg}(\Delta_d, 6)} \equiv 71 \cdot 4L_2(11, \chi_d) & (\text{mod } 2^9) & \text{for } d \equiv 5 & (\text{mod } 16) \\ \sqrt{L^{alg}(\Delta_d, 6)} \equiv 369 \cdot 4L_2(11, \chi_d) & (\text{mod } 2^9) & \text{for } d \equiv 9 & (\text{mod } 16) \\ \sqrt{L^{alg}(\Delta_d, 6)} \equiv 7 \cdot 4L_2(11, \chi_d) & (\text{mod } 2^9) & \text{for } d \equiv 13 & (\text{mod } 16) \\ \sqrt{L^{alg}(\Delta_d, 6)} \equiv d \cdot 12L_3(15, \chi_d) & (\text{mod } 3^4) & \text{for all } d. & \end{array}$$

The question of how congruences modulo a power of a prime between the coefficients of Hecke eigenforms give rise to congruences between the algebraic parts of the critical values of the associated L-functions was initially studied by Mazur [32], [33]. Using modular symbols to study algebraic parts of L-values, Vatsal [43] proved a general result for congruences between Eisenstein series and cuspidal newforms of weight 2. Vatsal remarks that his result could be generalized to higher weights k, but only if $p > k$. Here, we consider small primes $p \in \{2, 3\}$.

Another approach to these questions, introduced by Maeda in [30], is to use Kohnen-Waldspurger theorem to translate congruences between L-values to congruences between half-integral weight modular forms that correspond to integral weight modular forms via Shimura Correspondence. More precisely, one can show ([34], p.154) that the Kohnen newform in $S^{\text{new}}_{6+\frac{1}{2}}(\Gamma_0(4))$ associated to $\Delta(z)$ is

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n = \frac{E_4(4z)\Theta(\theta_0(z))}{2} - \frac{\Theta(E_4(4z))\theta_0(z)}{16}, \tag{3}$$

where for integer k, $E_{2k}(z)$ is the normalized Eisenstein series of weight 2k on $\mathrm{SL}_2(\mathbb{Z})$, and Θ is Ramanujan's Theta-operator defined by

$$\Theta\left(\sum_{n=0}^{\infty} a(n)q^n\right) = \sum_{n=0}^{\infty} na(n)q^n.$$

Now the Waldspurger-Kohnen theorem for positive fundamental discriminants d implies that

$$L(\Delta_d, 6) = \frac{\langle \Delta, \Delta \rangle \pi^6}{120 d^{\frac{11}{2}} \langle g, g \rangle} \cdot b(d)^2$$

($\langle \cdot, \cdot \rangle$ is the standard Petersson inner product). We define the algebraic part of $L(\Delta_d, 6)$ to be $L^{alg}(\Delta_d, 6) := b(d)^2$, and we define the square root of the algebraic part to be $\sqrt{L^{alg}(\Delta_d, 6)} := b(d)$. Koblitz [22] showed that the Shimura lifting on cusp forms, as modified by Kohnen, extends to Eisenstein series. The $6 + \frac{1}{2}$ weight modular form that corresponds to $E_{12}(z)$ is the Cohen-Eisenstein series $H_{6+\frac{1}{2}}(z) \in M_{6+\frac{1}{2}}(\Gamma_0(4))$. In general, for $r \geq 1$ we have Cohen-Eisenstein series of weight $r + \frac{1}{2}$ [10]

$$H_{r+\frac{1}{2}}(z) = \sum_{N \geq 0} H(r, N)q^N \in M_{r+\frac{1}{2}}(\Gamma_0(4)),$$

where $H(r, N)$ is a certain explicit arithmetic function. For example, if $D = (-1)^r N$ is a discriminant of a quadratic field, then $H(r, N) = L(1 - r, \chi_D)$.

Koblitz proved that the congruence $\Delta(z) \equiv E_{12}(z) \pmod{691}$ descends to the congruence $g(z) \equiv -252H_{6+\frac{1}{2}}(z) \pmod{691}$, and Guerzhoy and Datskovsky [11] generalized this to other weights. We have an analogous theorem for moduli which are powers of 2. The difference is that we prove congruences modulo a theta series of weight $\frac{1}{2}$. More precisely we write

$$f(z) \equiv' g(z) \pmod{N} \iff f(z) - g(z) \equiv h(z) \pmod{N},$$

for some p-adic modular form $h(z)$, whose non-zero coefficients are supported on squares.

For a modular form $f(z) = \sum a(n)q^n$, we denote by $f(z)^+ = \sum_{n \equiv 1 \pmod 8} a(n)q^n$ and $f(z)^- = \sum_{n \equiv 5 \pmod 8} a(n)q^n$ modular forms obtained by "twisting".

Theorem 6 (K.[19]). *With $g(z)$ as in 3, we have*

$$g(z)^+ \equiv' 49 \cdot 4H_{6+\frac{1}{2}}(z)^+ \pmod{2^9}$$
$$g(z)^- \equiv' 39 \cdot 4H_{6+\frac{1}{2}}(z)^- \pmod{2^9}$$

When we compare $H_{6+\frac{1}{2}}(z)$ and $\theta_0(z)^3$ modulo powers of two and three, we get the following corollary.

Corollary 7 (K.[19]). *If d is a positive fundamental discriminant, then the following are true.*

a) If $d \equiv 1 \pmod 8$, *then we have* $2^5 | \sqrt{L^{alg}(\Delta_d, 6)} + 12h(-d)$.
b) If $d \equiv 1 \pmod 8$, *then we have* $3^3 | \sqrt{L^{alg}(\Delta_d, 6)} - 120d \cdot H(-3d)$.
Here, $H(-N)$ *denotes the Hurwitz class number.*

Kohnen first proved results similar to part b) in [23], and he used it together with the result of Davenport and Heilbronn on the 3-part of the class group to obtain nonvanishing of a positive proportion of central L-values $L(\Delta_d, 6)$.

2.5. **Modular forms associated to Fermat curves.** While the arithmetic of Fourier coefficient of modular forms for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ has been one of the central topics in number theory, little is known for modular forms on noncongruence subgroups. One of the reasons for this is that the Hecke operators, which are the main tool for studying coefficients in the classical situation, are not useful in studying modular forms for noncongruence subgroups [42].

Atkin and Swinnerton-Dyer [4] pioneered the research in this area by making a remarkable observation on the congruence properties of Fourier coefficients of certain cusp forms for noncongruence subgroups. These congruences have been further studied by A.J. Scholl in [37, 38, 39], and by A.O.L. Atkin, W.-C. L. Li, L. Long, and Z. Yang in the series of papers [3, 27, 28, 29].

We found another arithmetic phenomena that holds for some modular functions for noncongruence subgroups.

Given a positive integer N, the Fermat group $\Phi(N)$ is the subgroup of $\Gamma(2)$ with the property that the modular curve $X(\Phi(N))$ is isomorphic to the Fermat curve F_N given by the equation $X^N + Y^N = Z^N$. The group $\Phi(N)$ is a congruence group only for $N = 1, 2, 4$ and 8 [36]. For every such $\Phi(N)$, we can associated modular functions $x(\tau)$ and $y(\tau)$ with rational Fourier coefficients, such that

$$x(\tau)^N - y(\tau)^N = -16.$$

These functions have been studied by D. Rohrlich [36] and T. Yang [46].
As a result of combinatorial manipulation, we proved the following theorem in [20].

Theorem 8 (K.[20]). *Let* $N \geq 1$ *be an odd integer, and let*

$$x(\tau) = q^{-1} + \sum_{i=1}^{\infty} a(iN-1) q^{iN-1},$$

where $q = e^{\frac{2\pi i \tau}{2N}}$. *We define* $N'_m \in \{1, 2, \ldots, 2^m - 1\}$ *such that* $NN'_m \equiv 1 \pmod{2^m}$. *For positive integers* m *and* n, *we have that*

$$v_2(a(n2^m)) \geq 3k_m,$$

where k_m *is the number of* 1*'s in the binary expansion of* N'_m.

J. Lehner [26] and A. O. L. Atkin [2], using the theory of Hecke operators, obtained similar results for the coefficients of the modular j-invariant. More precisely, if $j(\tau) = q^{-1} + \sum_{k=0}^{\infty} c(k) q^k$, and if m and n are positive integers, they proved that

$$v_p(c(np^m)) \geq \begin{cases} m+1 & \text{if } p = 5 \\ m & \text{if } p = 7 \\ m & \text{if } p = 11. \end{cases}$$

Surprisingly, we have a Hecke type of phenomena in the absence of Hecke operators.

2.6. **Congruent numbers and congruences between half-integral weight modular forms, preprint.** A positive integer d is called a congruent if it is the area of a right triangle with rational side lengths. The congruent number problem asks for the classification of positive integers which are congruent. It is well

known that d is congruent if and only if the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a positive rank over $\mathbb{Q}$. Tunnell constructed weight $3/2$ Hecke eigenform

$$f(\tau) = \eta(8z)\eta(16z)\theta_0(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\frac{3}{2}}(\Gamma_0(128)),$$

whose image under Shimura correspondence $g(z)$ has property that $L(E_1, s) = L(g, s)$. Using Waldspurger's result (note that the curves E_d are quadratic twist of E_1), he proved that if d is a positive, odd and square-free integer, then

$$L(E_d, 1) = a(d)^2 \frac{\Omega}{4\sqrt{d}},$$

where $\Omega := \int_1^\infty \frac{dx}{\sqrt{x^3-x}}$. We define the square root of the algebraic part of $L(E_d, 1)$ to be $\sqrt{L^{alg}(E_d, 1)} := a(d)$.

If we assume Birch and Swinnerton-Dyer (BSD) conjecture, we have that d is a congruent number if and only if $a(d) \neq 0$. On the other hand, known results on BSD conjecture imply unconditionally that if $a(d) \neq 0$, then d is a noncongruent number.

Starting with Gauss, who developed genus theory, many people studied the structure of 2-Sylow subgroup of the class group of the imaginary quadratic fields. For a prime p, denote by $h(-p)$ the class number of quadratic imaginary field $\mathbb{Q}(\sqrt{-p})$. Cohn and Barrucand discovered that $8|h(-p)$ if and only if $p = x^2+32y^2$, for some integers x and y. Williams showed that if $\epsilon = T + U\sqrt{p}$ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ then $h(-p) \equiv T + p - 1 \pmod{16}$, where $8|h(-p)$. It is not known are there infinitely many primes p for which $16|h(-p)$.

In the light of the well known analogy between the class group and Tate-Shafarevich group of the elliptic curve, one can ask the similar questions about $Ш(E_p)$, the Tate-Shafarevich group of the elliptic curve E_p. Bruin and Hemenway [8] proved, under the assumption that the primes p for which $E_p(\mathbb{Q})$ has rank 2 have asymptotic density 0 in the set of primes, that at least one of the following is true.

a) There are infinitely many primes p such that $\mathbb{Z}/8\mathbb{Z} \hookrightarrow Ш(E_p)$.
b) There are infinitely many primes p such that $16|h(-p)$.

We prove the "L-function" analog of this result.

Theorem 9 (K. [16]). *If d is a positive square free integer, then*

$$3H(-4d) \equiv \sqrt{L^{alg}(E_d, 1)} + 8b(d) \pmod{16},$$

where $b(d)$ is dth Fourier coefficient of the certain Eisenstein series (see Proposition 3.1. ??), and $H(-4d)$ is the Hurwitz class number. In particular, if p is a prime, then

$$3h(-4p) \equiv \begin{cases} \sqrt{L^{alg}(E_p, 1)} \pmod{16} & \text{if } p \equiv 1 \pmod{16}, \\ \sqrt{L^{alg}(E_p, 1)} + 8 \pmod{16} & \text{if } p \equiv 9 \pmod{16} \end{cases}$$

Remark 1. *The author* [19] *proved a similar congruence relation between $h(-4p)$ and algebraic part of the central value of L-function associated to Ramanujan Δ-function and its quadratic twists.*

Assuming the full BSD conjecture Tunell showed that $\#Ш(E_p) = \frac{1}{4}a(p)^2$, hence we have the following corollary.

Corollary 10 (K. [16]). *Let p be a prime. If we assume the full BSD conjecture for the curve E_p, then the following are true:*

a) *If $p \equiv 1 \pmod{16}$ then*

$$16|h(-4p) \iff (\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent.}$$

b) *If $p \equiv 9 \pmod{16}$, then*

$$8||h(-4p) \iff (\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent.}$$

Chebotarev's density theorem implies that the set S of primes $p \equiv 9 \pmod{16}$ with property that $8|h(-4p)$ has a positive density in the set of primes. For $p \in S$, the sign of functional equation of $L(E_p, s)$ is 1, hence BSD conjecture implies that the rank of E_p is even. If we assume that the set of primes p for which E_p has rank at least 2 have density 0 in the set of primes, we conclude that there are infinitely many primes $p \in S$ for which p is noncongruent. Corollary 10 b) now implies that for $p \in S$ either $16|h(-4p)$ or $(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p)$.

The following theorem relates the structure of $Ш(E_p)$ to the arithmetic of real quadratic field $\mathbb{Q}(\sqrt{p})$.

Theorem 11 (K. [16]). *Let $p \equiv 1 \pmod 8$ be a prime. If we assume the full BSD conjecture for the curve E_p, then we have*

$$(\mathbb{Z}/8\mathbb{Z})^2 \hookrightarrow Ш(E_p) \text{ or } p \text{ is congruent} \iff 16|R_2,$$

where $R_2 := \log_2(\epsilon)$ is 2-adic regulator and ϵ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$.

2.7. **Modular forms, de Rham cohomology and congruences (joint with A.J. Scholl), in preparation.** In [4], Atkin and Swinnerton-Dyer described a remarkable family of congruences they had discovered, involving the Fourier coefficients of modular forms on noncongruence subgroups. Their data suggested (see [27] for a precise conjecture) that the spaces of cusp forms of weight k for noncongurence subgroup, for all but finitely many primes p, should posses a p-adic Hecke eigenbasis in the sense that Fourier coefficients $a(n)$ of each basis element satisfy

$$a(pn) - A_p a(n) + \chi(p) p^{k-1} a(n/p) \equiv 0 \pmod{p^{(k-1)(1+\mathrm{ord}_p(n))}},$$

where A_p is an algebraic integer and χ is a Dirichlet character (they depend on basis element, but not on n). This congruence relation is reminiscent of the relation between Fourier coefficients of Hecke eigenforms for congruence subgroups (which is surprising since there is no usefull Hecke theory for modular forms on noncongruence subgroups).

In this paper [21] we show that congruences like those discovered by Atkin and Swinnerton-Dyer hold for weakly holomorphic modular forms (that is, modular forms which are permitted to have poles at cusps). Unlike the case of Atkin–Swinnerton-Dyer's original congruences for cusp forms, these congruences are nontrivial even for congruence subgroups. The simplest case is the weakly modular form of level 1 and weight 12

$$\begin{aligned} E_4(z)^6/\Delta(z) - 1464 E_4(z)^3 &= q^{-1} + \sum_{n=1}^{\infty} a(n) q^n \\ &= q^{-1} - 142236q + 51123200q^2 + 39826861650q^3 + \cdots \end{aligned}$$

For every prime $p \geq 11$ and integer n with $p^s|n$, its coefficients satisfy the congruence

$$a(np) - \tau(p) a(n) + p^{11} a(n/p) \equiv 0 \pmod{p^{11s}}.$$

where $\tau(n)$ is Ramanujan's function.

As a further example, for odd integer $N > 1$, we consider a space of weight 3 cuspforms on a certain genus 0 quotient of Fermat curve $X^N + Y^N = Z^N$ (we denote by $\Phi_0(N)$ the corresponding noncongruence modular group). We prove that these cusp forms are "CM forms" in the sense that the Galois representation associated to them is a Grossencharacter of a cyclotomic field $\mathbb{Q}(\zeta_N)$. Also, we show that when $N = 5$, for primes $p \equiv 2, 3 \pmod 5$ (non-ordinary primes), the space of cuspforms does not admit a p-adic basis consisting of forms satisfying Atkin and Swinnerton-Dyer congruence relation. This gives a counterexample to the conjecture of Atkin and Swinnerton-Dyer as stated in [27] (there is another counterexample in weight 2 found by J. Kibelbeck).

To "repair" the problem, for odd N, we construct certain weakly holomorphic modular forms and prove ASD like congruences between them and certain holomorphic modular forms that form a basis for the space of cuspforms. As for illustration, consider the following (weakly holomorphic) modular forms of weight 3 for

noncongurence subgroup $\Phi_0(3)$

$$f_1(\tau) = \eta(\tau/2)^{\frac{4}{3}}\eta(\tau)^{-2}\eta(2\tau)^{\frac{20}{3}}$$
$$= \sum c_1(n)q^{\frac{n}{2}} = q^{\frac{1}{2}} - \frac{4}{3}q^{\frac{2}{2}} + \frac{8}{9}q^{\frac{3}{2}} - \frac{176}{81}q^{\frac{4}{2}} + \cdots \in S_3(\Phi_0(3)),$$

$$f_2(\tau) = \eta(\tau/2)^{\frac{20}{3}}\eta(\tau)^{-10}\eta(2\tau)^{\frac{28}{3}}$$
$$= \sum c_2(n)q^{\frac{n}{2}} = q^{\frac{1}{2}} - \frac{20}{3}q^{\frac{2}{2}} + \frac{200}{9}q^{\frac{3}{2}} - \frac{4720}{81}q^{\frac{4}{2}} + \cdots \in S_3^{weak}(\Phi_0(3)).$$

We prove that for a prime $p \equiv 2 \bmod 3$, there exist $\alpha_p, \beta_p \in \mathbb{Z}_p$ such that if $p^s|n$ then

$$c_1(pn) \equiv \alpha_p c_2(n) \bmod p^{2(s+1)},$$

$$c_2(pn) \equiv \beta_p c_1(n) \bmod p^{2(s+1)}.$$

Moreover $\alpha_p\beta_p = p^2$, and $\mathrm{ord}_p(\alpha_p) = 2$.

2.8. **Modular forms, hypergeometric functions and congruences, submitted.** Consider the family of elliptic curves given by the Legendre equation

$$y^2 = x(x-1)(x-t), \quad t \in \mathbb{C},$$

whose period integrals

$$\Omega_1(t) = \int_t^1 \frac{dx}{\sqrt{x(x-1)(x-t)}}, \quad \Omega_2(t) = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-t)}},$$

are solutions of the differential equation of Picard-Fuch type

$$t(t-1)\Omega''(t) + (2t-1)\Omega'(t) + \frac{1}{4}\Omega(t) = 0.$$

One finds that $\Omega_2(t) = \pi\, {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, t\right)$, where

$${}_2F_1\left(a, b; c, t\right) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} t^n$$

is the Gauss hypergeometric function. This further gives identity

$$\theta(\tau) = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, 16l(\tau)\right) = \sum_{n=0}^{\infty} \binom{2n}{n}^2 l(\tau)^n. \tag{4}$$

Throughout, $\tau \in \mathbb{H}$, $q = e^{\pi i \tau}$, $\theta(\tau) = \left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^2$ is the classical weight 1 theta series, and $l(\tau) = q - 8q^2 + 44q^3 - 192q^4 + \cdots$ is the normalized elliptic modular lambda function (hauptmoduln for $\Gamma(2)$). For more details see [25].

In this paper, we identify certain (weakly holomorphic) modular forms

$$f(\tau) = P(l(\tau))\theta^k(\tau)\frac{dl(\tau)}{d\tau},$$

for some $P(t) \in \mathbb{Z}[t]$, and $k \in \mathbb{F}$, whose Fourier coefficients are easily understood in terms of elementary arithmetic (e.g. a spliting behavior of primes in the quadratic extensions). Using identity (4), we exploit the

relation (via formal group theory) between the coefficients of the power series $P(t){}_2F_1\left(\frac{1}{2},\frac{1}{2};1,16t\right)^k$, and Fourier coefficients of $f(\tau)$ to prove some elementary congruences for the numbers

$$A_k(n)=\sum_{\substack{i_1,i_2\dots i_k\geq 0\\ i_1+i_2+\cdots i_k=n}}\binom{2i_1}{i_1}^2\binom{2i_2}{i_2}^2\cdots\binom{2i_k}{i_k}^2,\quad \text{for } k,n\in\mathbb{F}.$$

Beukers and Stienstra [40] invented this approach to study congruence properties of Apery numbers

$$B(n)=\sum_{k=0}^{\infty}\binom{n+k}{k}\binom{n}{k}^2.$$

Using the formal Brauer group of some elliptic K3-surface, they proved that for all primes p, and $m,r\in\mathbb{F}$ with m odd

$$B\left(\frac{mp^r-1}{2}\right)-a(p)B\left(\frac{mp^{r-1}-1}{2}\right)+(-1)^{\frac{p-1}{2}}p^2B\left(\frac{mp^{r-2}-1}{2}\right)\equiv 0\pmod{p^r},$$

where $\eta^6(4\tau)=\sum_{n=1}^{\infty}a(n)q^{2n}$.

Many authors have subsequently studied arithmetic properties of $B(n)'s$ and discovered similar three term congruence relations for other Apery like numbers. For related work see [6, 14, 35, 44, 47].

In contrast to these result, the novelity of this paper is that we use families of modular forms, as well as the weakly holomorphic modular form to extract information about congruence properties of numbers $A_k(n)$. In particular, even though Foureier coefficients of weakly holomorphic modular forms do not satisfy three term relation satisfied by coefficients of Hecke eigenforms, they sometimes satisfy three term congruence relation of Atkin and Swinnerton-Dyer type (see [21]), which then give rise to the three term congruence relations satisfied by corresponding Apery like numbers.

Let Δ be the free subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by the matrices $A=\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ and $B=\left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$. Note that $\Gamma(2)=\{\pm I\}\Delta$, and that $\Gamma_1(4)=\left(\begin{smallmatrix}1/2&0\\0&1\end{smallmatrix}\right)\Delta\left(\begin{smallmatrix}1/2&0\\0&1\end{smallmatrix}\right)^{-1}$. Divisors of $\theta(\tau)$, $l(\tau)$, and $1-16l(\tau)$ are suported at cusps. For an integer k, we denote by $M_k(\Delta)$ and $S_k(\Delta)$ the spaces of modular forms and cusp forms of weight k for group Δ.

First we identify some (weakly holomorphic) modular forms for Δ that have "simple" Fourier coefficients.

Theorem 12.
For $n\in\mathbb{F}$, let

$$h_n(\tau)=\theta(\tau)^{6n+1}(1-16l(\tau))^{\lfloor\frac{n+1}{2}\rfloor}l(\tau)^{2n}=\sum_{m=1}^{\infty}a_n(m)q^m.$$

Then $h_n(\tau)\in S_{6n+1}(\Delta)$, and for a prime $p\equiv(-1)^{n+1}\pmod 4$, we have that $a_n(p)=0$.

Theorem 13.

a) *The modular form*

$$f_1(\tau)=l(\tau)(1-16l(\tau))\theta(\tau)^5=\sum_{n=1}^{\infty}b_1(n)q^n\in M_5(\Delta)$$

is the cusp form with complex multiplication by $\mathbb{Q}(i)$. In particular, for a prime $p>2$ we have

$$b_1(p)=\begin{cases}2x^4-12x^2y^2+2y^4 & \text{if } p\equiv 1\pmod 4,\ \text{and } p=x^2+y^2,\\ 0 & \text{if } p\equiv 3\pmod 4.\end{cases}$$

b) *For an integer $n>2$, the Fourier coefficients $c_1(n)$ of the weakly holomorphic modular form $g_1(\tau)=l(\tau)^2(1-16l(\tau))^2\theta(\tau)^5=\sum_{n=2}^{\infty}c_1(n)q^n$ satisfy the following congruence relation*

$$b_1(n)\equiv 108c_1(n)\pmod{n^3}.$$

c) *For integer $n > 1$, let*

$$f_n(\tau) = \theta(\tau)^{6n-6}(1-16l(\tau))^{\lfloor \frac{n-1}{2} \rfloor} l(\tau)^{2n-2} f_1(\tau) = \sum_{m=1}^{\infty} b_n(m) q^m.$$

Then for a prime $p \equiv (-1)^n \pmod 4$, we have that $b_n(p) = 0$.

Corollary 14. *Let $p > 3$ be a prime, and $r \in \mathbb{F}$. If $p \equiv 1 \pmod 4$, let x and y be integers such that $p = x^2 + y^2$. Denote by $D_3(n) = A_3(n-1) - 16A_3(n-2)$. Then the following congruences hold*

$$A_3(mp^r - 1) - b_1(p)A_3(mp^{r-1} - 1) + \left(\frac{-1}{p}\right) p^4 A_3(mp^{r-2} - 1) \equiv 0 \pmod{p^r}, \tag{5}$$

$$D_3(mp^r - 1) - b_1(p)D_3(mp^{r-1} - 1) + \left(\frac{-1}{p}\right) p^4 D_3(mp^{r-2} - 1) \equiv 0 \pmod{p^{r - \frac{\left(\frac{-1}{p}\right)+1}{2}}}. \tag{6}$$

In particular, we have

$$A_3(p-1) \equiv \begin{cases} 16x^4 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 0 \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{7}$$

$$D_3(p-1) \equiv \begin{cases} \frac{4}{27}x^4 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 0 \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{8}$$

For integers $n \geq 1$ and $m \geq 0$, define the sequences $B_n(m)$ and $C_n(m)$ by the following identities

$$(1-16t)^{\lfloor \frac{n-1}{2} \rfloor} t^{2n-1} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, 16t\right)^{6n-1} = \sum_{m=0}^{\infty} B_n(m) t^m,$$

$$(1-16t)^{\lfloor \frac{n-1}{2} \rfloor} t^{2n-2} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, 16t\right)^{6n-3} = \sum_{m=0}^{\infty} C_n(m) t^m.$$

Corollary 15. *For $n \in \mathbb{F}$ and a prime $p > 2$, we have that $B_n(p-1) \equiv 0 \pmod p$, if $p \equiv (-1)^{n+1} \pmod 4$. Moreover, $C_n(p-1) \equiv 0 \pmod p$ if $p \equiv (-1)^n \pmod 4$.*

Example 1. *Let $p > 2$ be a prime. Consider the coefficients of ${}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, 16t\right)^2$. The corresponding modular form*

$$l(\tau)(1-16l(\tau)){}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1, 16l(\tau)\right)^4 = \sum_{k=1}^{\infty} (-1)^k \left(\sigma_3(k/2) - \sigma_3(k)\right) q^k$$

is an Eisenstein series whose p^{th} Fourier coefficient is $\equiv 1 \bmod p$ (if k is odd, we define $\sigma_3(k/2)$ to be 0). Hence Lemma ?? implies

$$\sum_{k=0}^{p-1} \binom{2k}{k}^2 \binom{2(p-1-k)}{p-1-k}^2 \equiv 1 \pmod p,$$

or equivalently $\binom{p-1}{\frac{p-1}{2}}^4 \equiv 1 \pmod p$.

2.9. **Modular parametrizations of certain elliptic curves (joint with Y.Sakai, K. Tasaka), submitted.** In this paper, we study some general properties of modular parametrizations, and as a consequences we explain and generalize the results of Kaneko and Sakai from [15].

Kaneko and Sakai (inspired by the paper of Guerzhoy [12]) observed that certain elliptic curves whose associated newforms (by the modularity theorem) are given by the eta-quotients from the list of Martin and Ono [31] can be characterized by a particular differential equation involving holomorphic modular forms.

To give an example of this phenomena, let $f_{20}(\tau)=\eta(\tau)^4\eta(5\tau)^4$ be a unique newform of weight 2 on $\Gamma_0(20)$, where $\eta(\tau)$ is the Dedekind eta function $\eta(\tau)=q^{1/24}\prod_{n>0}(1-q^n)$, $q=e^{2\pi i\tau}$, and put $\Delta_{5,4}(\tau)=f_{20}(\tau/2)^2$. Then an Eisenstein series $Q_5(\tau)$ on $M_4(\Gamma_0(5))$ associated either to cusp $i\infty$ or to cusp 0 is a solution of the following differential equation

$$\partial_{5,4}(Q_5)^2=Q_5^3-\frac{89}{13}Q_5^2\Delta_{5,4}-\frac{3500}{169}Q_5\Delta_{5,4}^2-\frac{125000}{2197}\Delta_{5,4}^3, \tag{9}$$

where $\partial_{5,4}(Q_5(\tau))=\frac{1}{2\pi i}Q_5(\tau)'-\frac{1}{2\pi i}Q_5(\tau)\Delta_{5,4}(\tau)'/\Delta_{5,4}(\tau)$ is a Ramanujan-Serre differential operator. Throughout the paper, we use symbol $'$ to denote $\frac{d}{d\tau}$. This differential equation defines a parametrization of an elliptic curve $E: y^2=x^3-\frac{89}{13}x^2-\frac{3500}{169}x-\frac{125000}{2197}$ by modular functions

$$x=\frac{Q_5(\tau)}{\Delta_{5,4}(\tau)},\quad y=\frac{\partial_{5,4}(Q_5)(\tau)}{\Delta_{5,4}(\tau)^{3/2}},$$

and $f_{20}(\tau)$ is the newform associated to E. One finds that $\Delta_{5,4}(\tau)\in S_4(\Gamma_0(5))$, so curiously the modular forms $\Delta_{5,4}, Q_5$ and $\partial(Q_5)$ appearing in this parametrization are modular for $\Gamma_0(5)$, although the conductor of E is 20.

Using the Eichler-Shimura theory, we generalize (9) to the arbitrary elliptic curve E of conductor $4N$, $E: y^2=x^3+ax^2+bx+c$, where $a,b,c\in\mathbb{Q}$, which admits a modular parametrization $\Phi: X\to E$ satisfying

$$\Phi^*\left(\frac{dx}{2y}\right)=\pi i f_{4N}(\tau/2)d\tau.$$

Here X is the modular curve $\mathbb{H}/\left(\begin{smallmatrix}\frac12&0\\0&1\end{smallmatrix}\right)^{-1}\Gamma_0(4N)\left(\begin{smallmatrix}\frac12&0\\0&1\end{smallmatrix}\right)$, and $f_{4N}(\tau)\in S_2(\Gamma_0(4N))$ is a newform with rational Fourier coefficients associated to E. It follows from the modularity theorem that in any $\mathbb{Q}$-isomorphism class of elliptic curves there is an elliptic curve E admitting such parametrization (note that for $u\in\mathbb{Q}^\times$ the change of variables $x=u^2X$ and $y=u^3Y$ implies $\frac{dX}{Y}=u\frac{dx}{y}$).

To such Φ we associate a solution $Q(\tau)=x(\Phi(\tau))f_{4N}(\tau/2)^2$ of a differential equation

$$\partial_{N,4}(Q)^2=Q^3+aQ^2\Delta_{N,4}+bQ\Delta_{N,4}^2+c\Delta_{N,4}^3, \tag{10}$$

where $\Delta_{N,4}(\tau)=f_{4N}(\tau/2)^2$, and $\partial_{N,4}(Q(\tau))=\frac{1}{2\pi i}Q(\tau)'-\frac{1}{2\pi i}Q(\tau)\Delta_{N,4}(\tau)'/\Delta_{N,4}(\tau)$.

We show that $f_{4N}(\tau/2)^2$ is modular for $\Gamma_0(N)$. In general the solution $Q(\tau)$ will not be holomorphic and will be modular only for $\left(\begin{smallmatrix}\frac12&0\\0&1\end{smallmatrix}\right)^{-1}\Gamma_0(4N)\left(\begin{smallmatrix}\frac12&0\\0&1\end{smallmatrix}\right)$, but if the preimage of the point at infinity of E under Φ is contained in cusps of X and is invariant under the action of $\left(\begin{smallmatrix}1&0\\N&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ (acting on X by Möbius transformations), $Q(\tau)$ will be both holomorphic and modular for $\Gamma_0(N)$. Moreover, we show that there are only finitely many (up to isomorphism) elliptic curves E admitting Φ with these two properties.

We also obtain similar results generalizing the other examples from [15] that correspond to the elliptic curves over $\mathbb{Q}$ with j-invariant 0 and 1728 (see the next section).

Throughout the paper, let N be a positive integer and $k\in\{4,6,8,12\}$. Let $E_k/\mathbb{Q}$ be an elliptic curve given by the short Weierstrass equation $y^2=f_k(x)$, where

$$\begin{aligned}f_4(x)&=x^3+a_2x^2+a_4x+a_6,\\ f_6(x)&=x^3+b_6,\\ f_8(x)&=x^3+c_4x,\\ f_{12}(x)&=x^3+d_6,\end{aligned}$$

and $a_2, a_4, a_6, b_6, c_4, d_6 \in \mathbb{Q}$. Moreover, we assume $j(E_4) \neq 0, 1728$.
Let

$$f_{N,k}(\tau) \in S_2\left(\Gamma_0\left(\frac{k^2}{4}N\right)\right)$$

be a newform with rational Fourier coefficients, and let $\Gamma_k := \left(\begin{smallmatrix}\frac{2}{k} & 0\\ 0 & 1\end{smallmatrix}\right)^{-1}\Gamma_0(\frac{k^2}{4}N)\left(\begin{smallmatrix}\frac{2}{k} & 0\\ 0 & 1\end{smallmatrix}\right)$. Define

$$\Delta_{N,k}(\tau) := f_{N,k}(2\tau/k)^{k/2} \in S_k(\Gamma_k).$$

For $f(\tau) \in M_4^{\mathrm{mer}}(\Gamma_k)$, we define the (Ramanujan-Serre) differential operator by

$$\partial_{N,k}(f(\tau)) = \frac{k}{8\pi i}f'(\tau) - \frac{1}{2\pi i}f(\tau)\frac{\Delta'_{N,k}(\tau)}{\Delta_{N,k}(\tau)} \in M_6^{\mathrm{mer}}(\Gamma_k).$$

Finally, assume that there is a meromorphic modular form $Q_k(\tau) \in M_4^{\mathrm{mer}}(\Gamma_k)$, such that the corresponding differential equation holds

$$\begin{array}{rcl}\partial_{N,4}(Q_4(\tau))^2 &=& Q_4(\tau)^3 + a_2Q_4(\tau)^2\Delta_{N,4}(\tau) + a_4Q_4(\tau)\Delta_{N,4}(\tau)^2 + a_6\Delta_{N,4}(\tau)^3\\ \partial_{N,6}(Q_6(\tau))^2 &=& Q_6(\tau)^3 + b_6\Delta_{N,6}(\tau)^2\\ \partial_{N,8}(Q_8(\tau))^2 &=& Q_8(\tau)^3 + c_4Q_8(\tau)\Delta_{N,8}(\tau)\\ \partial_{N,12}(Q_{12}(\tau))^2 &=& Q_{12}(\tau)^3 + d_6\Delta_{N,12}(\tau).\end{array} \tag{11}$$

Each of these four identities defines a modular parametrization $\Psi_k : X_k \to E_k$

$$\Psi_k(\tau) = \left(\frac{Q_k(\tau)}{\Delta_{N,k}(\tau)^{4/k}}, \frac{\partial_{N,k}(Q_k)(\tau)}{\Delta_{N,k}(\tau)^{6/k}}\right),$$

where X_k is the compactified modular curve $\mathbb{H}/\Gamma_k$.

Proposition 1. *Let $\frac{dx}{2y}$ be the Néron differential on E_k. Then*

$$\Psi_k^*\left(\frac{dx}{2y}\right) = \frac{4\pi i}{k}f_{N,k}(2\tau/k)d\tau. \tag{12}$$

In particular, the conductor of E_k is $\frac{k^2}{4}N$ and $f_{N,k}(\tau)$ is the cusp form associated to E_k by the modularity theorem.

Remark 2. *Note that when $k = 6, 8$ or 12, $f_{N,k}(\tau)$ is a modular form with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ respectively.*

Conversely, given a modular parametrization $\Phi_k : X_k \to E_k$ satisfying (12), we construct a differential equation (11) and its solution $Q_k(\tau)$ as follows.

Let x and y be functions on E_k satisfying Weierstrass equation $y^2 = f_k(x)$. Functions $x(\tau) := x \circ \Phi_k(\tau)$ and $y(\tau) := y \circ \Phi_k(\tau)$ satisfy $y(\tau)^2 = f_k(x(\tau))$. Moreover (12) implies that

$$\left(\frac{k}{8\pi i}x'(\tau)\right)^2 = f_{N,k}(2\tau/k)^2y(\tau)^2 = \Delta_{N,k}(\tau)^{4/k}f_k(x(\tau)). \tag{13}$$

Define $Q_k(\tau) := x(\tau)\Delta_{N,k}(\tau)^{4/k}$.

Proposition 2. *The following formula holds*

$$\partial_{N,k}(Q_k(\tau))^2 = \Delta_{N,k}(\tau)^{12/k}f_k(x(\tau)).$$

In particular, $Q_k(\tau)$ is a solution of (11).

Now we investigate conditions under which $Q_k(\tau)$ is holomorphic. The following lemma easily follows from the formula above.

Lemma 1. *Assume that $\tau_0 \in X_k$ is a pole of $x(\tau)$. Then*

$$ord_{\tau_0}(Q_k(\tau)) = \begin{cases} 0, & \text{if } \tau_0 \text{ is a cusp,} \\ -2, & \text{if } \tau_0 \in \mathbb{H}. \end{cases}$$

As a consequence, we have the following characterization of the holomorphicity of $Q_k(\tau)$ in terms of modular parametrization Φ_k. Denote by $\mathcal{C}$ the set of cusps of X_k, and by $\mathcal{O}$ the point at infinity of E_k.

Proposition 3. *We have that $Q_k(\tau)$ is holomorphic if and only if $\Phi_k^{-1}(\mathcal{O}) \subset \mathcal{C}$.*

We show that the degree of Φ_k (as a function of the conductor) grows faster than the total ramification index at cusps hence the following theorem holds.

Theorem 16. *There are finitely many elliptic curves $E/\mathbb{Q}$ (up to a $\mathbb{Q}$-isomorphism) that admit a modular parametrization $\Phi : X_k \to E$ with the property that $\Phi^{-1}(\mathcal{O}) \subset \mathcal{C}$.*

In particular, there are finitely many elliptic curves E_k (up to a $\mathbb{Q}$-isomorphism) for which $Q_k(\tau)$ (which satisfy equation (11)) is holomorphic.

Define $A = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. It is easy to see that Γ_k is generated by $\Gamma_0(N)$ and A and T , hence $Q_k(\tau)$ is modular for $\Gamma_0(N)$ if and only if it is invariant under the action of slash operators $|A$ and $|T$. The following theorem describes the modularity in terms of parametrization Φ_k.

Theorem 17. *If $\Phi_k^{-1}(\mathcal{O})$ is invariant under A and T, then $Q_k(\tau)$ is modular for $\Gamma_0(N)$.*

References

[1] T. Asai, M. Kaneko, and H. Ninomiya, *Zeros of certain modular functions and an application*, Comment. Math. Univ. St. Paul., 46 (1997), pp. 93–101.

[2] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J., 8 (1967), pp. 14–32.

[3] A. O. L. Atkin, W.-C. W. Li, and L. Long, *On Atkin and Swinnerton-Dyer congruence relations. II*, Math. Ann., 340 (2008), pp. 335–358.

[4] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, in Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1971, pp. 1–25.

[5] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math., 238 (1969), pp. 67–70.

[6] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory, 25 (1987), pp. 201–210.

[7] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras*, Invent. Math., 109 (1992), pp. 405–444.

[8] N. Bruin and H. B., *On congruent primes and class numbers of imaginary quadratic fields*, arXiv:1110.5959 (2011).

[9] Y. Choie, W. Kohnen, and K. Ono, *Linear relations between modular form coefficients and non-ordinary primes*, Bull. London Math. Soc., 37 (2005), pp. 335–341.

[10] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann., 217 (1975), pp. 271–285.

[11] B. Datskovsky and P. Guerzhoy, *On Ramanujan congruences for modular forms of integral and half-integral weights*, Proc. Amer. Math. Soc., 124 (1996), pp. 2283–2291.

[12] P. Guerzhoy, *The Ramanujan differential operator, a certain CM elliptic curve and Kummer congruences*, Compos. Math., 141 (2005), pp. 583–590.

[13] ———, *Irreducibility of some Faber polynomials*, Ramanujan J., 16 (2008), pp. 53–57.

[14] F. Jarvis and H. A. Verrill, *Supercongruences for the Catalan-Larcombe-French numbers*, Ramanujan J., 22 (2010), pp. 171–186.

[15] M. Kaneko and Y. Sakai, *The ramanujan-serre differential operators and certain elliptic curves*, preprint.

[16] M. Kazalicki, *Congruent numbers and congruences between half-integral weight modular forms*, preprint.

[17] ———, *Linear relations for coefficients of Drinfeld modular forms*, Int. J. Number Theory, 4 (2008), pp. 171–176.

[18] ———, *Zeros of certain Drinfeld modular functions*, J. Number Theory, 128 (2008), pp. 1662–1669.

[19] ———, *2-adic and 3-adic part of class numbers and properties of central values of l-functions*, Acta Arith., 147 (2011), pp. 51–72.

[20] ———, *2-adic properties of modular functions associated to fermat curves*, Proceedings of AMS, (2011), pp. 4265–4271.

[21] M. Kazalicki and A. J. Scholl, *Modular forms, de rham cohomology and congruences*, in preparation.

[22] N. Koblitz, *p-adic congruences and modular forms of half integer weight*, Math. Ann., 274 (1986), pp. 199–220.

[23] W. Kohnen, *Modular forms of half-integral weight on $\Gamma_0(4)$*, Math. Ann., 248 (1980), pp. 249–266.

[24] O. Kolberg, *Congruences for Ramanujan's function $\tau(n)$*, Arbok Univ. Bergen Mat.-Natur. Ser., 1962 (1962), p. 8.
[25] M. Kontsevich and D. Zagier, *Periods*, in Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 771–808.
[26] J. Lehner, *Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$*, Amer. J. Math., 71 (1949), pp. 136–148.
[27] W.-C. W. Li, L. Long, and Z. Yang, *Modular forms for noncongruence subgroups*, Q. J. Pure Appl. Math., 1 (2005), pp. 205–221.
[28] ———, *On Atkin-Swinnerton-Dyer congruence relations*, J. Number Theory, 113 (2005), pp. 117–148.
[29] L. Long, *On Atkin and Swinnerton-Dyer congruence relations. III*, J. Number Theory, 128 (2008), pp. 2413–2429.
[30] Y. Maeda, *A congruence between modular forms of half-integral weight*, Hokkaido Math. J., 12 (1983), pp. 64–73.
[31] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc., 125 (1997), pp. 3169–3176.
[32] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., (1977), pp. 33–186 (1978).
[33] ———, *On the arithmetic of special values of L functions*, Invent. Math., 55 (1979), pp. 207–240.
[34] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, vol. 102 of CBMS Regional Conference Series in Mathematics, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.
[35] R. Osburn and B. Sahu, *Congruences via modular forms*, Proc. Amer. Math. Soc., 139 (2011), pp. 2375–2381.
[36] D. E. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math., 39 (1977), pp. 95–127.
[37] A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences*, Invent. Math., 79 (1985), pp. 49–77.
[38] ———, *Modular forms on noncongruence subgroups*, in Séminaire de Théorie des Nombres, Paris 1985–86, vol. 71 of Progr. Math., Birkhäuser Boston, Boston, MA, 1987, pp. 199–206.
[39] ———, *The l-adic representations attached to a certain noncongruence subgroup*, J. Reine Angew. Math., 392 (1988), pp. 1–15.
[40] J. Stienstra and F. Beukers, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, Math. Ann., 271 (1985), pp. 269–304.
[41] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, in Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.
[42] J. G. Thompson, *Hecke operators and noncongruence subgroups*, in Group theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 215–224. Including a letter from J.-P. Serre.
[43] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J., 98 (1999), pp. 397–419.
[44] H. A. Verrill, *Congruences related to modular forms*, Int. J. Number Theory, 6 (2010), pp. 1367–1390.
[45] K. S. Williams, *On the class number of $\mathbf{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime*, Acta Arith., 39 (1981), pp. 381–398.
[46] T. Yang, *Cusp forms of weight 1 associated to Fermat curves*, Duke Math. J., 83 (1996), pp. 141–156.
[47] D. Zagier, *Integral solutions of Apéry-like recurrence equations*, in Groups and symmetries, vol. 47 of CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, 2009, pp. 349–366.