PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 12, December 2011, Pages 4265–4271
S 0002-9939(2011)10854-2
Article electronically published on April 29, 2011

2-ADIC PROPERTIES OF MODULAR FUNCTIONS ASSOCIATED TO FERMAT CURVES

MATIJA KAZALICKI

(Communicated by Kathrin Bringmann)

ABSTRACT. For an odd integer N, we study the action of Atkin's $U(2)$-operator on the modular function $x(\tau)$ associated to the Fermat curve: $X^N + Y^N = 1$. The function $x(\tau)$ is modular for the Fermat group $\Phi(N)$, generically a noncongruence subgroup. If $x(\tau) = q^{-1} + \sum_{i=1}^{\infty} a(iN-1)q^{iN-1}$, we essentially prove that $\lim_{n\to 0} a(n) = 0$ in the 2-adic topology.

1. Introduction and statement of results

While the arithmetic of the 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 [14].

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 [11, 12, 13], and by A.O.L. Atkin, W.-C.L. Li, L. Long, and Z. Yang in the series of papers [5, 7, 8, 9].

For a power series $\sum_{n\geq n_0} c(n)q^n$ and prime p, Atkin's $U(p)$-operator is given by

$$\left(\sum_{n\geq n_0} c(n)q^n\right)|U(p) = \sum_{n\geq n_0} c(pn)q^n.$$

For prime p, we denote by $v_p(r)$ the p-adic valuation of a rational number r. In this paper, we study the action of $U(2)$ on the spaces of modular functions (for noncongruence subgroups) associated to Fermat curves. We prove that the Fourier coefficients $a(m)$ of these functions converge 2-adically to 0 as $v_2(m)$ goes to infinity.

Remark. D. Rohrlich [10] and T. Yang [15] have studied modular functions associated to Fermat curves.

Received by the editors April 13, 2010 and, in revised form, September 20, 2010 and October 23, 2010.

2000 *Mathematics Subject Classification.* Primary 11F03, 11F30, 11F33.

Key words and phrases. Modular forms, noncongruence subgroups, Fermat curves.

We follow the notation of [15].

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 $B := \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$. One has that $\Gamma(2) = \{\pm I\}\Delta$. Given a positive integer N, the Fermat group $\Phi(N)$ is defined to be the subgroup of Δ generated by A^N, B^N, and the commutator $[\Delta, \Delta]$. It is known that the modular curve $X(\Phi(N))$ is isomorphic to the Fermat curve $X^N + Y^N = Z^N$. The group $\Phi(N)$ is a congruence group only for $N = 1, 2, 4$ and 8 [15].

Denote by $\mathbb{H}$ the complex upper half-plane. If $\tau \in \mathbb{H}$ and $q = e^{2\pi i \tau}$, then Rohrlich [10] showed, using the theory of Dedekind η-functions, that

$$\lambda(\tau) = -\frac{1}{16} q^{-1/2} \prod_{n=1}^{\infty} \left(\frac{1 - q^{n-1/2}}{1 + q^n} \right)^8, \tag{1.1}$$

$$1 - \lambda(\tau) = \frac{1}{16} q^{-1/2} \prod_{n=1}^{\infty} \left(\frac{1 + q^{n-1/2}}{1 + q^n} \right)^8 \tag{1.2}$$

are modular functions for $\Gamma(2)$. Moreover, they are holomorphic on $\mathbb{H}$, and $\lambda(\tau) \neq 0, 1$ for all $\tau \in \mathbb{H}$. It follows that there exist holomorphic functions $\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ on $\mathbb{H}$, such that $\tilde{x}(\tau)^N = \lambda(\tau)$ and $\tilde{y}(\tau)^N = 1 - \lambda(\tau)$, so we have that

$$\tilde{x}(\tau)^N + \tilde{y}(\tau)^N = 1.$$

It turns out that both $\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ are modular functions for $\Phi(N)$. We normalize $\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ by setting

$$x(\tau) := (-1)^{\frac{1}{N}} 16^{\frac{1}{N}} \tilde{x}(\tau) \quad \text{and} \quad y(\tau) := 16^{\frac{1}{N}} \tilde{y}(\tau).$$

Now, $x(\tau)$ and $y(\tau)$ have rational Fourier coefficients, and we have that

$$x(\tau)^N - y(\tau)^N = -16. \tag{1.3}$$

Here we prove the following result for $x(\tau)$.

Theorem 1.1. *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.

Remark. We can also define k_m to be the number of 1's among the first m digits in the expansion of $\frac{1}{N}$ in the ring of 2-adic integers $\mathbb{Z}_2$. For example, if $N = 3$, then $k_m = \lfloor \frac{m}{2} \rfloor + 1$. A periodicity of the expansion implies that $k_m \approx \dfrac{l_1}{l_2} m$, where l_1 is the number of 1's in the initial period and l_2 the length of the initial period.

Example. When $N = 3$, we have that

$$x(\tau) = q^{-1} - 8/3q^2 - 4/9q^5 + 320/81q^8 + 818/243q^{11} + \ldots \text{ and}$$

$$x(\tau)|U(32) = 419737088/3^{15}q + 144174015078594388301451224172544 0/3^{62}q^4 + \ldots,$$

where $q = e^{\frac{2\pi i\tau}{6}}$. It follows that $N_4' = 11$, $k_4 = 3$, and the theorem implies that $v_2(a(32n)) \geq 9$. We can check that $v_2(a(32)) = v_2(419737088/3^{15}) = 9$, and so the inequality is sharp.

Remark. The Fourier coefficients of even index of $x(\tau)$ and $y(\tau)$ differ by the sign, so the same result holds for $y(\tau)$.

J. Lehner [6] and A.O.L. Atkin [3], using the fact that $U(p)$-operators are Hecke operators on modular functions for $\Gamma_0(p)$, 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

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

In our case, the $U(2)$-operator is not a Hecke operator. In contrast with the work of Atkin and Lehner, and similar to that of Akiyama [1], and Atkin and O'Brien [2], we express $x(\tau)|U(2^m)$ as a formal power series in $x(\tau)^{-1}$. The 2-adic properties of the coefficients of this power series are described by the following theorem. It implies Theorem 1.1.

Theorem 1.2. *Let m be a positive integer, and let $N \geq 1$ be an odd integer. We have the following equality of formal q-series:*

$$x(\tau)|U(2^m) = \sum_{i=0}^{\infty} b_m(j_m + iN)x(\tau)^{-(j_m+iN)}, \tag{1.4}$$

where $j_m = \frac{NN_m'-1}{2^m}$, and $N_m' \in \{1, 2, \ldots, 2^m - 1\}$ such that $NN_m' \equiv 1 \pmod{2^m}$. Moreover, $v_2(b_m(j_m + iN)) \geq 4i + v_2(b_m(j_m))$, and $v_2(b_m(j_m)) = 3k_m$, where k_m is the number of 1's in the binary expansion of N_m'.

Remark. It is interesting to ask whether (1.4) is an equality between the values of functions evaluated at τ. For example, if $\tau \in \mathbb{H}$ is such that $\lambda(\tau)$ is an element of some finite extension K of $\mathbb{Q}_2$ and that $v_2(16\lambda(\tau)) \leq 0$, where v_2 is the normalized valuation associated to the maximal ideal of the ring of integers of K, then the right hand side of (1.4) converges in 2-adic topology. It is natural to ask how that value is related to $x(\tau)|U(2^m)$.

2. Preliminaries for the proofs of the theorems

Throughout this section, let $N \geq 1$ be an odd integer. We express $x(\tau)^{-k}|U(2)$ as a power series in $x(\tau)^{-1}$ with rational coefficients which 2-adically converge to 0. More precisely, we prove the following theorem.

Theorem 2.1. *Let k be a positive integer. We have that*

$$x(\tau)^{-k}|U(2) = \sum_{i=0}^{\infty} c_k(j + iN)x(\tau)^{-(j+iN)},$$

where $j = k/2$ if k is even, and $\frac{k+N}{2}$ otherwise. Moreover, the coefficients $c_k(j + iN)$ are rational, $v_2(c_k(j + iN)) \geq 4(i + 1) - 1$ and $v_2(c_k(j)) = 3$ if k is odd, and $v_2(c_k(j + iN)) \geq 4i$ and $v_2(c_k(j)) = 0$ otherwise.

The following lemma is very useful for calculating the action of $U(2)$ on the powers of $x(\tau)^{-1}$.

Lemma 2.2. *For a positive integer k, we have that*

$$2x(\tau)^{-k}|U(2) = x(\tau/2)^{-k} + (-1)^k y(\tau/2)^{-k}.$$

Proof. It follows from (1.1) and (1.2) that Fourier coefficients of odd index of $x(\tau)$ and $y(\tau)$ are the same, while the Fourier coefficients of even index differ by sign. Now, the lemma easily follows by induction. □

To prove Theorem 2.1, we first write $(x(\tau)^{-1} - y(\tau)^{-1})|U(2)$ and $\frac{1}{x(\tau)y(\tau)}|U(2)$ as a power series in $x(\tau)^{-1}$, and then using Lemma 2.2, we express $x(\tau)^{-k}|U(2)$ as a polynomial in $(x(\tau)^{-1} - y(\tau)^{-1})|U(2)$ and $\frac{1}{x(\tau)y(\tau)}|U(2)$. As the first step, we have the following proposition.

Proposition 2.3. *The following identities hold:*

a) $\dfrac{y(\tau)}{x(\tau)} = \displaystyle\sum_{i=0}^{\infty} \binom{1/N}{i} 16^i x(\tau)^{-iN},$

b) $\dfrac{y(2\tau)}{x^2(2\tau)} = \dfrac{1}{x(\tau)y(\tau)}.$

Hence, $\dfrac{1}{x(\tau)y(\tau)}|U(2) = \dfrac{y(\tau)}{x(\tau)^2}.$

Proof. a) It follows from $x(\tau)^N - y(\tau)^N = -16$ that $\frac{y}{x} = \sqrt[N]{1 + 16x(\tau)^{-N}}$. The Binomial Theorem now implies the claim.

b) Set $\tilde{\lambda}(\tau) := x(\tau)^N$ (i.e. $\tilde{\lambda}(\tau) = -16\lambda(\tau)$). Let $X = x(2\tau)$ and $Y = x(\tau)$. From [15], we know that $\lambda(\tau)$ has a pole only at the cusp ∞. Hence by checking that the principal part of the q-expansion vanishes, we find that the modular equation between $\tilde{\lambda}(\tau)$ and $\tilde{\lambda}(2\tau)$ can be written in the following form:

$$X^{2N} - X^N Y^N (Y^N + 16) - 16Y^N(Y^N + 16) = 0.$$

By rearranging this identity, one gets $\dfrac{y^N(2\tau)}{x^{2N}(2\tau)} = x(\tau)^{-N} y(\tau)^{-N}$, and the claim follows by taking the Nth root of both sides of the equality. □

Let $u := x(\tau)^{-1} - y(\tau)^{-1}$ and $v := \frac{1}{x(\tau)y(\tau)}$. For a positive integer k, we define polynomials $P_k(u, v) \in \mathbb{Z}[u, v]$ in the following way. Set $P_1(u, v) := u$ and $P_2(u, v) := u^2 + 2v$. For an integer $k \geq 2$, let $P_k(u, v) := P_{k-1}(u, v) \cdot u - P_{k-2}(u, v) \cdot v$. We record some properties of the polynomials $P_k(u, v)$.

Lemma 2.4. *Let k be a positive integer. Define the degree of u to be 1, and the degree of v to be 2. Then the following are true:*

a) *$P_k(u, v)$ is homogeneous of weighted degree k.*
b) *$P_k(u, v) = x(\tau)^{-k} + (-1)^k y(\tau)^{-k}$.*
c) *If k is odd, then the leading coefficient of the monomial $uv^{\frac{k-1}{2}}$ in $P_k(u, v)$ is $(-1)^{\frac{k+1}{2}}(k - 2)$.*
d) *If k is even, then the leading coefficient of the monomial $v^{\frac{k}{2}}$ in $P_k(u, v)$ is $(-1)^{\frac{k}{2}+1}2$.*

Proof. The lemma follows by induction. □

The power series that we are working with have the following property.

Definition 2.5. Let m and M be integers. We say that a power series

$$\sum_{i=0}^{\infty} e(m+iM)x^{m+iM}$$

is **special** if for every $i \geq 0$ we have that $v_2(e(m+iM)) \geq 4i + v_2(e(m))$.

Using the notion of special power series, we prove the following proposition.

Proposition 2.6. *We have that*

$$x(\tau)^{-1} - y(\tau)^{-1} = \sum_{i=0}^{\infty} b\left(\frac{N+1}{2} + iN\right) x(2\tau)^{-(\frac{N+1}{2}+iN)},$$

where $b(\frac{N+1}{2}+iN)$ *are rational numbers such that* $v_2(b(\frac{N+1}{2}+iN)) \geq 4(i+1)$ *and* $v_2(b(\frac{N+1}{2})) = 4$.

Proof. We use formula (1.3) and $P_N(u,v)v^{-N} = 16$ to calculate the $x(2\tau)^{-1}$-expansion of $u = x(\tau)^{-1} - y(\tau)^{-1}$ recursively. First note that Proposition 2.3 implies that

$$v = x(2\tau)^{-1} + \sum_{i=1}^{\infty} A(iN+1)x(2\tau)^{-(iN+1)},$$

where $v_2(A(iN+1)) \geq 4i$. Thus, we have that

$$v^{-1} = x(2\tau) + \sum_{i=1}^{\infty} B(iN-1)x(2\tau)^{-(iN-1)},$$

where $v_2(B(iN-1)) \geq 4i$. Hence v^{-1} is special.

Lemma 2.4 implies that the monomials of $P_N(u,v)v^{-N}$ are of the form $c(i)u^i v^{\frac{i+N}{2}}$, $i = 1, 3, \ldots, N$, and that $c(1)$ is odd. It follows that $v_2(b(\frac{N+1}{2})) = v_2(16) = 4$. Denote by $d(\frac{(i-1)N}{2})x(2\tau)^{-\frac{(i-1)}{2}N}$ the leading $x(2\tau)^{-1}$-term of $c(i)u^i v^{\frac{i+N}{2}}$. It is easy to see that $v_2(d(\frac{(i-1)N}{2})) \geq 4i$. Using the fact that the product of the special power series is special, an easy inductive argument (using the fact that $c(1)$ is odd) implies that u is special. Hence, the proposition follows. □

We are now ready to prove Theorem 2.1.

Proof of Theorem 2.1. By Propositions 2.3 and 2.6, we have that $u = \frac{8}{N}x(2\tau)^{-\frac{N+1}{2}} + \ldots$ and $v = x(2\tau)^{-1} + \ldots$.

First, we assume that k is even. Lemma 2.4 implies that

$$P_k(u,v) = \sum_{i=0}^{\frac{k}{2}} d_k(i)v^i u^{k-2i},$$

where $d_k(k/2) = \pm 2$, and the leading coefficients of the $x(2\tau)^{-1}$-expansions of monomials $d_k(i)v^i u^{k-2i}$ are of degree $k/2 + \frac{k-2i}{2}N$. Hence, $j = k/2$, and $c_k(j) = 1$. Propositions 2.3 and 2.6 imply that each monomial $d_k(i)v^i u^{k-2i}$ is special (with respect to the $x(2\tau)^{-1}$-expansion) and that the 2-adic valuations of the leading coefficients in their expansions are $\geq 4(k-2i)$. Since $v_2(d_k(k/2)) = 1$, it follows that $P_k(u,v)$ is special with the 2-adic valuation of the leading $x(2\tau)^{-1}$ term equal to 1. Now the claim follows from Lemma 2.2.

Next, assume that k is odd. Lemma 2.4 implies that

$$P_k(u,v) = \sum_{i=0}^{\frac{k-1}{2}} d_k(i) v^i u^{k-2i},$$

where $d_k(\frac{k-1}{2})$ is odd and the leading coefficients of $x(2\tau)^{-1}$-expansions of monomials $d_k(i)v^i u^{k-2i}$ are of degree $k/2 + \frac{k-2i}{2}N$. Hence $j = \frac{N+k}{2}$ and $v_2(c_k(j)) = 4$. Now, an argument as in the previous case completes the proof. □

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.2. Since $x(\tau) = q^{-1} + \sum_{i=1}^{\infty} a(iN-1)q^{iN-1}$, we have that $j_1 = \frac{N-1}{2}$, and $j_m = j_{m-1}/2$ if j_{m-1} is even, and $j_m = \frac{j_{m-1}+N}{2}$ otherwise. The formula for j_m now follows by induction. Note that in the first case $N'_m = N'_{m-1}$, while in the second $N'_m = N'_{m-1} + 2^{m-1}$. Hence, the number of 1's in binary expansion of N'_m counts the number of odd elements in the sequence j_i, for $i \in \{0, 1, \dots m-1\}$, where we define $j_0 = -1$.

Next, we prove by induction that $x(\tau)|U(2^m)$ is special, and the formula for $v_2(b_m(j_m))$. If $m = 1$, then $N'_1 = 1$, and Proposition 2.3 together with Proposition 2.6 implies that $x(\tau)|U(2)$ is special and that $v_2(b_1(j_1)) = 3$. Assume that $m > 1$ is such that j_{m-1} is even. Then Theorem 2.1 implies that $v_2(b_m(j_m)) = v_2(b_{m-1}(j_{m-1}))$. If j_{m-1} is odd, then both $b_{m-1}(j_{m-1})x(\tau)^{-j_{m-1}}|U(2)$ and $b_{m-1}(j_{m-1} + N)x(\tau)^{-(j_{m-1}+N)}|U(2)$ contribute the $b_m(j_m)x(\tau)^{-j_m}$ term of $x(\tau)|U(2^m)$. However, an induction hypothesis implies that $v_2(b_m(j_m)) = v_2(b_{m-1}(j_{m-1})) + 3$, since $v_2(b_{m-1}(j_{m-1} + N)) \geq 4 + b_{m-1}(j_{m-1})$. Thus, the formula follows. Using Theorem 2.1 and the induction hypothesis, an argument similar to the previous one implies that $x(\tau)|U(2^m)$ is special, and so the theorem follows. □

Proof of Theorem 1.1. The theorem follows directly from Theorem 1.2 and the definition of $U(2)$. □

Acknowledgements

The author would like to thank Ken Ono for his comments on drafts of the paper. Also, he would like to thank Tonghai Yang and Pavel Guerzhoy for helpful conversations. Finally, he would like to thank the referee for careful comments that improved the exposition of the paper.

References

[1] S. Akiyama, *On the 2^n divisibility of the Fourier coefficients of J_q functions and the Atkin conjecture for $p = 2$*, Analytic number theory and related topics (Tokyo, 1991), World Sci. Publishing, 1993, 1–15. MR1342302 (96d:11046)

[2] A. O. L. Atkin, J. N. O'Brien, *Some properties of $p(n)$ and $c(n)$ modulo powers of 13*, Trans. Amer. Math. Soc. **126** (1967), 442–459. MR0214540 (35:5390)

[3] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14–32. MR0205958 (34:5783)

[4] A. O. L. Atkin, H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. of California, Los Angeles, 1968), Amer. Math. Soc., 1971, 1–25. MR0337781 (49:2550)

[5] A. O. L. Atkin, W.-C. W. Li, L. Long, *On Atkin-Swinnerton-Dyer congruence relations. II*, Math. Ann. **340** (2008), no. 2, 335–358. MR2368983 (2009a:11102)

[6] J. Lehner, *Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$*, Amer. J. Math. **71** (1949), 136–148. MR0027801 (10:357a)
[7] W.-C. W. Li, L. Long, Z. Yang, *Modular forms for noncongruence subgroups*, Quart. J. Pure Appl. Math. **1** (2005), 205–221. MR2155139 (2006k:11077)
[8] W.-C. W. Li, L. Long, Z. Yang, *On Atkin-Swinnerton-Dyer congruence relations*, J. Number Theory **113** (2005), no. 1, 117–148. MR2141761 (2006c:11053)
[9] L. Long, *On Atkin-Swinnerton-Dyer congruence relations. III*, J. Number Theory **128** (2008), no. 8, 2413–2429. MR2394828 (2009e:11085)
[10] D. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. **39** (1977), 95–127. MR0441978 (56:367)
[11] A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences*, Invent. Math. **79** (1985), 49–77. MR774529 (86j:11045)
[12] A. J. Scholl, *Modular forms on noncongruence subgroups*, Séminaire de Théorie des Nombres, Paris 1985–86, Progr. Math., Vol. 71, Birkhäuser, Boston, MA, 1987, 199–206. MR1017913 (90k:11049)
[13] A. J. Scholl, *The l-adic representations attached to a certain noncongruence subgroup*, J. Reine Angew. Math. **392** (1988), 1–15. MR965053 (90e:11064)
[14] J. G. Thompson, *Hecke operators and noncongruence subgroups*, Group Theory, Singapore, 1987, de Gruyter, Berlin, 1989, including a letter from J.-P. Serre, 215–224. MR981844 (90a:20105)
[15] T. Yang, *Cusp form of weight* 1 *associated to Fermat curves*, Duke Math. J. **83** (1996), 141–156. MR1388846 (97e:11053)

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: kazalick@math.wisc.edu
Current address: Department of Mathematics, University of Zagreb, Bijenicka cesta 30, 10000 Zagreb, Croatia
E-mail address: mkazal@math.hr