HASSE INVARIANTS FOR THE CLAUSEN ELLIPTIC CURVES

AHMAD EL-GUINDY AND KEN ONO

ABSTRACT. Gauss's ${}_2F_1\left(\begin{matrix}\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}\mid x\right)$ hypergeometric function gives periods of elliptic curves in Legendre normal form. Certain truncations of this hypergeometric function give the Hasse invariants for these curves. Here we study another form, which we call the *Clausen form*, and we prove that certain truncations of ${}_3F_2\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2}\\ 1 & & 1\end{matrix}\mid x\right)$ and ${}_2F_1\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ & 1\end{matrix}\mid x\right)$ in $\mathbb{F}_p[x]$ are related to the characteristic p Hasse invariants.

1. INTRODUCTION

We begin by recalling three types of hypergeometric functions which give invariants of the Legendre normal form elliptic curves

$$E_{\mathrm{L}}(\lambda): \quad y^2 = x(x-1)(x-\lambda), \qquad \lambda \in \mathbb{C}\setminus\{0,1\}. \tag{1.1}$$

If n is a nonnegative integer, then define $(\gamma)_n$ by

$$(\gamma)_n := \begin{cases} 1 & \text{if } n = 0,\\ \gamma(\gamma+1)(\gamma+2)\cdots(\gamma+n-1) & \text{if } n \geq 1. \end{cases}$$

The *classical hypergeometric function* in parameters $\alpha_1,\dots,\alpha_h,\beta_1,\dots,\beta_j \in \mathbb{C}$ is defined by

$${}_hF_j^{\mathrm{cl}}\left(\begin{matrix}\alpha_1, & \alpha_2, & \dots & \alpha_h\\ & \beta_1, & \dots & \beta_j\end{matrix}\mid x\right) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n(\alpha_2)_n(\alpha_3)_n\cdots(\alpha_h)_n}{(\beta_1)_n(\beta_2)_n\cdots(\beta_j)_n}\cdot\frac{x^n}{n!}.$$

By the theory of elliptic integrals, it is well known that Gauss's hypergeometric function ${}_2F_1^{\mathrm{cl}}(x) := {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}\mid x\right)$ gives the periods (for example, see page 184 of [7]) of the Legendre normal form elliptic curves. In particular, if we denote the real period of $E_{\mathrm{L}}(\lambda)$ by $\Omega_{\mathrm{L}}(\lambda)$, then for $0<\lambda<1$ we have

$$\Omega_{\mathrm{L}}(\lambda) = \pi\cdot\ {}_2F_1^{\mathrm{cl}}(\lambda). \tag{1.2}$$

Truncated hypergeometric functions also give invariants for these curves. Throughout let p be an odd prime. Recall that an elliptic curve in characteristic p is said to be *supersingular* if

2000 *Mathematics Subject Classification.* Primary 11G, 14H.

Key words and phrases. Hypergeometric functions, Hasse invariants.

The second author thanks the support of the NSF, the Hilldale Foundation and the Manasse family.

it has no p-torsion over $\overline{\mathbb{F}}_p$. We define the relevant *truncated hypergeometric functions* by

$$ {}_2F_1^{\mathrm{tr}}(x)_p := \sum_{n=0}^{\frac{p-1}{2}} \left(\frac{(\frac{1}{2})_n}{n!} \right)^2 x^n, \tag{1.3}$$

and we define the characteristic p Hasse invariant for the Legendre normal form elliptic curves by

$$ H_{\mathrm{L}}(x)_p := \prod_{\substack{\lambda \in \overline{\mathbb{F}}_p \\ E_{\mathrm{L}}(\lambda) \text{ supersingular}}} (x - \lambda). \tag{1.4}$$

It turns out that $H_{\mathrm{L}}(x)_p$ is in $\mathbb{F}_p[x]$, and it satisfies (for example, see page 261 of [7])

$$ H_{\mathrm{L}}(x)_p \equiv {}_2F_1^{\mathrm{tr}}(x)_p \pmod{p}. \tag{1.5}$$

There is a third kind of hypergeometric function, the finite field hypergeometric function. These functions also give information about the Legendre normal form elliptic curves. We first recall their definition which is due to J. Greene [4]. If q is a prime power and A and B are two Dirichlet characters on $\mathbb{F}_q$ (extended so that $A(0) = B(0) = 0$), then let $\binom{A}{B}$ be the normalized Jacobi sum

$$ \binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}) = \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_p} A(x)\overline{B}(1-x). $$

Here $\overline{B}$ is the complex conjugate of B. If $A_0, \dots, A_n$, and $B_1, \dots, B_n$ are characters on $\mathbb{F}_q$, then the *finite field hypergeometric function* in these parameters is defined by

$$ {}_{n+1}F_n^{\mathrm{ff}} \left(\begin{matrix} A_0, & A_1, & \dots & A_n \\ & B_1, & \dots & B_n \end{matrix} \,\middle|\, x \right)_q := \frac{q}{q-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x). $$

Here $\sum_\chi$ denotes the sum over all characters χ of $\mathbb{F}_q$.

It has been observed by many authors (see [6], [4], [8], [9], [11], and [13], to name a few) that the Gaussian analog of a classical hypergeometric series with rational parameters is obtained by replacing each $\frac{1}{n}$ with a character χ_n of order n (and $\frac{a}{n}$ with χ_n^a). Let ϵ_q be the trivial character on $\mathbb{F}_q$ and let ϕ_q be the character of order 2. Then the finite field analog of ${}_2F_1^{\mathrm{cl}}(x)$ is

$$ {}_2F_1^{\mathrm{ff}}(x)_q := \left(\begin{matrix} \phi_q & \phi_q \\ & \epsilon_q \end{matrix} \,\middle|\, x \right)_q. $$

More generally, we let

$$ {}_{n+1}F_n^{\mathrm{ff}}(x)_q := {}_{n+1}F_n^{\mathrm{ff}} \left(\begin{matrix} \phi_q, & \phi_q, & \dots & \phi_q \\ & \epsilon_q, & \dots & \epsilon_q \end{matrix} \,\middle|\, x \right)_q. \tag{1.6}$$

M. Koike proved [9] that if $p \geq 5$ is a prime for which $E_{\mathrm{L}}(\lambda)$ has good reduction, and q is a power of p then

$$ {}_2F_1^{\mathrm{ff}}(\lambda)_q = -\frac{\phi_q(-1)}{q} \cdot a_{\mathrm{L}}(\lambda; q), \tag{1.7}$$

where $a_{\mathrm{L}}(\lambda; q)$ is the *trace of Frobenius* at q for $E_{\mathrm{L}}(\lambda)$.

We have now seen that the ${}_2F_1^{\mathrm{cl}}(x)$, ${}_2F_1^{\mathrm{tr}}(x)_p$ and ${}_2F_1^{\mathrm{ff}}(x)_q$ hypergeometric functions encode some of the most important invariants for the Legendre normal form elliptic curves. Loosely speaking, we have that

$$\text{“}\pi\text{”} \cdot {}_2F_1^{*}(x) \text{ “}=\text{”} \begin{cases} \text{Periods} & \text{if } * = \mathrm{cl}, \\ \text{Hasse invariants} & \text{if } * = \mathrm{tr}, \\ \text{Traces of Frobenius} & \text{if } * = \mathrm{ff}. \end{cases} \tag{1.8}$$

Motivated by (1.7), the second author identified [11, 12] a second form, the *Clausen form*, which is similarly related to finite field hypergeometric functions. These curves are given by

$$E_{\mathrm{C}}(\lambda): \quad y^2 = (x-1)(x^2+\lambda). \tag{1.9}$$

If $\lambda \notin \{0, -1\}$, then $E_{\mathrm{C}}(\lambda)$ is an elliptic curve with discriminant and j-invariant

$$\Delta(E_{\mathrm{C}}(\lambda)) = -64\lambda(\lambda+1)^2 \quad \text{and} \quad j(E_{\mathrm{C}}(\lambda)) = \frac{64(3\lambda-1)^3}{\lambda(\lambda+1)^2}.$$

If $E_{\mathrm{C}}(\lambda)$ has good reduction at a prime $p \geq 5$ and if q is a power of p, then the second author proved[1] (see Theorem 5 of [11]) the following analog of (1.7):

$$q + q^2\phi_q(\lambda+1)^{-1} \cdot {}_3F_2^{\mathrm{ff}}\left(\frac{\lambda}{\lambda+1}\right)_q = a_{\mathrm{C}}(\lambda; q)^2, \tag{1.10}$$

where $a_{\mathrm{C}}(\lambda; q)$ is the trace of the Frobenius at q for $E_{\mathrm{C}}(\lambda)$. It could be computed by the formula

$$a_{\mathrm{C}}(\lambda; q) = -\sum_{b \in \mathbb{F}_q} \phi_q((b-1)(b^2+\lambda)). \tag{1.11}$$

Remark. This result implies that the ${}_3F_2^{\mathrm{ff}}\left(\frac{\lambda}{\lambda+1}\right)_q$ is essentially the square of the character sum which gives the trace of Frobenius on $E_{\mathrm{C}}(\lambda)$. Greene and R. Evans [5] have obtained a generalization of this phenomenon for further ${}_3F_2^{\mathrm{ff}}$ hypergeometric functions.

Remark. A special case of (1.10), which can be viewed as a finite field analog of the Clausen Theorem (see Theorem 2.1), was proved first by Greene and Stanton [6].

Motivated by (1.8) and (1.10), D. McCarthy studied the relationship between ${}_3F_2^{\mathrm{cl}}(x) := {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1\end{matrix} \mid x\right)$ and the $E_{\mathrm{C}}(\lambda)$, and he proved that this classical hypergeometric function gives (see Theorem 2.1 of [10]) the square of real periods of these curves. Namely, if $\lambda > 0$, then

$$\pi^2 \cdot (\lambda+1)^{-\frac{1}{2}} \cdot {}_3F_2^{\mathrm{cl}}\left(\frac{\lambda}{\lambda+1}\right) = \Omega_{\mathrm{C}}(\lambda)^2, \tag{1.12}$$

where $\Omega_{\mathrm{C}}(\lambda)$ is the real period of $E_{\mathrm{C}}(\lambda)$.

[1]This result may be interpreted in terms of local zeta functions for a certain family of $K3$ surfaces [1].

To obtain the full analogy with (1.8), we now show that the squares of Hasse invariants for the Clausen curves are given by truncated hypergeometric functions. If p is an odd prime, then define the *truncated hypergeometric function* in parameters $\alpha_1, \dots, \alpha_h, \beta_1, \dots, \beta_j \in \mathbb{C}$ by

$$ {}_hF_j^{\mathrm{tr}}\left(\begin{matrix}\alpha_1, & \alpha_2, & \dots & \alpha_h \\ & \beta_1, & \dots & \beta_j\end{matrix} \mid x\right)_p := \sum_{n=0}^{\frac{p-1}{2}} \frac{(\alpha_1)_n(\alpha_2)_n(\alpha_3)_n\cdots(\alpha_h)_n}{(\beta_1)_n(\beta_2)_n\cdots(\beta_j)_n}\cdot\frac{x^n}{n!}.$$

Following our earlier convention, we let

$$ {}_3F_2^{\mathrm{tr}}(x)_p := {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1\end{matrix} \mid x\right)_p = \sum_{n=0}^{\frac{p-1}{2}} \left(\frac{(\frac{1}{2})_n}{n!}\right)^3 x^n, \tag{1.13}$$

and we have the Hasse invariant

$$ H_{\mathrm{C}}(x)_p := \prod_{\substack{\lambda\in\overline{\mathbb{F}}_p \\ E_{\mathrm{C}}(\lambda)\ \text{supersingular}}} (x-\lambda)\,. \tag{1.14}$$

The following theorem, which nicely complements (1.10) and (1.12), completes the analogies of (1.8) for the Clausen elliptic curves and gives

$$ \text{“}\pi^2\text{”}\cdot(\lambda+1)^{\text{“}-\frac{1}{2}\text{”}}\cdot {}_3F_2^*\left(\frac{\lambda}{\lambda+1}\right) \text{ “}=\text{” } \begin{cases} (\text{Periods})^2 & \text{if } *=\mathrm{cl}, \\ (\text{Hasse invariants})^2 & \text{if } *=\mathrm{tr}, \\ (\text{Traces of Frobenius})^2 & \text{if } *=\mathrm{ff}. \end{cases} \tag{1.15}$$

Theorem 1.1. *If p is an odd prime, then $H_{\mathrm{C}}(x)_p$ is in $\mathbb{F}_p[x]$, and it satisfies*

$$ \mathfrak{p}_p^2\cdot(x+1)^{\frac{p-1}{2}}\cdot {}_3F_2^{\mathrm{tr}}\left(\frac{x}{x+1}\right)_p \equiv H_{\mathrm{C}}(x)_p^2 \pmod p,$$

where $\mathfrak{p}_p$ is the reciprocal product of binomial coefficients

$$ \mathfrak{p}_p := \frac{1}{\binom{\frac{p-1}{2}}{\lfloor\frac{p-1}{4}\rfloor}\binom{\frac{p-1}{2}}{2\lfloor\frac{p-1}{4}\rfloor}}.$$

Remark. Since supersingular elliptic curves have models defined over $\mathbb{F}_{p^2}$ (for example, see p. 269 of [7] or p. 137 of [14]), it follows that the irreducible factors of ${}_3F_2^{\mathrm{tr}}(x)_p$ in $\overline{\mathbb{F}}_p[x]$ are linear or quadratic.

The proof of Theorem 1.1 shows that

$$ H_{\mathrm{C}}(x)_p \equiv \mathfrak{p}_p\cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix} \mid -x\right)_p \pmod p, \tag{1.16}$$

which in turn implies that all of the roots of this truncated hypergeometric function are in $\mathbb{F}_{p^2}$ and are simple. Furthermore, we note that McCarthy (see the proof of corollary 2.2 in [10]) also obtained the classical analog of (1.16), namely

$$ \Omega_{\mathrm{C}}(\lambda) = \pi\cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix} \mid -\lambda\right). \tag{1.17}$$

It is natural to wonder if a similar relation holds for Gaussian hypergeometric function with appropriate parameters. Indeed the following result is valid.

Proposition 1.2. *Let p be an odd prime and $\lambda \in \mathbb{Q}\setminus\{0,-1\}$ be such that $\mathrm{ord}_p(\lambda(\lambda+1)) = 0$. If q is a power of p such that $q \equiv 1 \pmod 4$ and χ_4 is a character of order 4 defined on $\mathbb{F}_q$, then we have*

$$a_{\mathrm{C}}(\lambda;q) = -q\cdot\ {}_2F_1^{\mathrm{ff}}\left(\begin{matrix}\chi_4 & \chi_4^3\\ & \epsilon_q\end{matrix}\ \middle|\ -\lambda\right)_q. \tag{1.18}$$

Proof. Following the proof of Theorem 5 in [11] we see that if we define a function $f(x)$ by

$$f(x) := \frac{q}{q-1}\sum_{\chi}\binom{\phi_q\chi^2}{\chi}\binom{\phi_q\chi}{\chi}\chi\left(\frac{x}{4}\right),$$

then for $\mathrm{ord}_p(\mu) = 0$ we have

$$f\left(\frac{4}{\mu}\right) = \frac{\phi_q(2)}{q}\sum_{x\in\mathbb{F}_p\setminus\{-\mu^2\}}\phi_q(x^3-\mu^2x^2+\mu^3(4-\mu)x-\mu^5(4-\mu)). \tag{1.19}$$

Dividing the right side by $\phi_q(\mu^6) = 1$, setting $\lambda := \frac{4-\mu}{\mu}$, and applying (1.11) we get

$$f(\lambda+1) = \frac{\phi_q(2)}{q}(-a_{\mathrm{C}}(q;\lambda) - \phi_q(-2(\lambda+1)).$$

Following Greene and Evans [5], we set

$$F^*(\phi_q,\epsilon_q;x) := f(x) + \frac{\phi_q(-x)}{q}.$$

Thus

$$F^*(\phi_q,\epsilon_q;\lambda+1) = -\frac{\phi_q(2)}{q}a_{\mathrm{C}}(q;\lambda). \tag{1.20}$$

Since $\chi_4^2 = \phi_q$, we deduce (using well-known properties of Jacobi sums) from Theorem 1.2 in [5] that

$$F^*(\phi_q,\epsilon_q;x) = \phi_q(2)\chi_4(-1)\ {}_2F_1^{\mathrm{ff}}\left(\begin{matrix}\chi_4 & \chi_4^3\\ & \epsilon_q\end{matrix}\ \middle|\ x\right)_q. \tag{1.21}$$

However, for $x \neq 0, 1$, Theorem 4.4(i) of [4] gives

$${}_2F_1^{\mathrm{ff}}\left(\begin{matrix}\chi_4 & \chi_4^3\\ & \epsilon_q\end{matrix}\ \middle|\ x\right)_q = \chi_4(-1){}_2F_1^{\mathrm{ff}}\left(\begin{matrix}\chi_4 & \chi_4^3\\ & \epsilon_q\end{matrix}\ \middle|\ 1-x\right)_q, \tag{1.22}$$

and the result follows by setting $x = \lambda+1$ and noting that $\chi_4^2(-1) = \phi_q(-1) = 1$ for $q \equiv 1 \pmod 4$. □

Remark. Note that Theorem 1.5 of [5], together with (1.10) imply that

$$a_{\mathrm{C}}(\lambda;q)^2 = q^2\cdot\ {}_2F_1^{\mathrm{ff}}\left(\begin{matrix}\chi_4 & \chi_4^3\\ & \epsilon_q\end{matrix}\ \middle|\ -\lambda\right)_q^2.$$

However, it seems one must go through an argument as in the proof above in order to obtain the more precise formula (1.18) .

Remark. A formula similar to (1.18) was stated, without an explicit proof, in [9] for the family

$$E_{\mathrm{K}}(\lambda) : y^2 = x^3 + x^2 + \frac{\lambda}{4}x.$$

Note that $E_{\mathrm{K}}(\lambda)$ is the $\frac{1}{2}$-quadratic twist of $E_{\mathrm{C}}(\lambda - 1)$.

It follows that we have the following analog of (1.8) and (1.15), where the last line is valid only when an analog of "$\frac{1}{4}$" exists; i.e. when $q \equiv 1 \pmod 4$.

$$\text{(1.23)} \qquad \text{“}\pi\text{”} \cdot {}_2F_1^*\left(\begin{matrix}\text{“}\frac{1}{4}\text{”} & \text{“}\frac{3}{4}\text{”} \\ & \text{“}1\text{”}\end{matrix} \mid -\lambda\right) \text{ “}=\text{” } \begin{cases}\text{Periods} & \text{if } * = \mathrm{cl},\\ \text{Hasse invariants} & \text{if } * = \mathrm{tr},\\ \text{Traces of Frobenius} & \text{if } * = \mathrm{ff}.\end{cases}$$

Remark. It is well-known that the Gauss sum $G(\chi)$ is the finite field analog of the gamma function (see section 1.10 of [2] for instance). Since $G(\phi_q)^2 = \phi_q(-1)q$ and $\Gamma(\frac{1}{2})^2 = \pi$, we see that $\phi_q(-1)q$ is indeed the Gaussian analog of π. On the other hand, the congruence for truncated hypergeometric series is one between *polynomials*, rather than complex numbers. Hence its main content is that the zeros of the truncated hypergeometric series are the supersingular locus. The constant is merely present to make the truncated hypergeometric series monic. It can't really be given an interpretation as a truncated analog of the gamma function at the parameter $\frac{1}{2}$ since the corresponding constant in (1.8) is just "1", which simply means that the truncation in that case happens to be monic without the need for further normalization.

Remark. As noted in [10] and confirmed by (1.7) and (1.18), the Gaussian analog of the real period is the *negative* of the trace of Frobenius.

Example. The set of supersingular Clausen curves for $p = 23$ is

$$\{E_{\mathrm{C}}(5), E_{\mathrm{C}}(8), E_{\mathrm{C}}(11), E_{\mathrm{C}}(14), E_{\mathrm{C}}(17)\},$$

and so it follows that

$$H_{\mathrm{C}}(x)_{23} := \prod_{\substack{\lambda \in \overline{\mathbb{F}}_{23} \\ E_{\mathrm{C}}(\lambda) \text{ supersingular}}} (x - \lambda) = (x-5)(x-8)(x-11)(x-14)(x-17).$$

One directly finds that $\mathfrak{p}_{23} = \frac{1}{5082} \equiv -1 \pmod{23}$, and we have

$$(x+1)^{11} \cdot {}_3F_2^{\mathrm{tr}}\left(\frac{x}{x+1}\right)_{23} = 1 + \frac{89}{8}x + \frac{28827}{512}x^2 + \cdots + \frac{185685617347012755}{2^{57}}x^{11}$$

$$\equiv x^{10} + 5x^9 + 19x^8 + \cdots + 9x^2 + 14x + 1 \equiv H_{\mathrm{C}}(x)_{23}^2 \pmod{23}.$$

Also,

$${}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix} \mid -x\right)_{23} = 1 - \frac{3}{16}x + \frac{105}{1024}x^2 - \frac{1155}{16384}x^3 + \frac{225225}{4194304}x^4 - \frac{2909907}{67108864}x^5$$

$$\equiv 22x^5 + 9x^4 + 8x^3 + 3x^2 + 7x + 1 \equiv -H_{\mathrm{C}}(x) \pmod{23}.$$

2. Proof of Theorem 1.1

We refer to the elliptic curves $E_{\mathrm{C}}(\lambda)$ as Clausen curves because they arise naturally in connection with an identity of Clausen relating ${}_2F_1^{\mathrm{cl}}$ and ${}_3F_2^{\mathrm{cl}}$ classical hypergeometric functions. First we recall this identity, along with other crucial observations.

2.1. **Nuts and bolts.** We begin by recalling the following identity of Clausen. Throughout this section we view the classical hypergeometric series as a formal one.

Theorem 2.1. [Clausen] *We have that*

$$ {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2}\\ 1 & 1\end{matrix} \mid x\right) = (1-x)^{-\frac{1}{2}} \cdot \ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ 1\end{matrix} \mid \frac{x}{x-1}\right)^2.$$

Proof. A theorem of Clausen (see p. 86 of [3]) implies that

$$ {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}2\alpha & 2\beta & \alpha+\beta\\ & 2\alpha+2\beta & \alpha+\beta+\frac{1}{2}\end{matrix} \mid x\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\alpha & \beta\\ & \alpha+\beta+\frac{1}{2}\end{matrix} \mid x\right)^2.$$

By the classical ${}_2F_1^{\mathrm{cl}}$ transformation (see p. 10 of [3]), we have that

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}a & b\\ & c\end{matrix} \mid x\right) = (1-x)^{-a} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}a & c-b\\ & c\end{matrix} \mid \frac{x}{x-1}\right).$$

The claim follows by letting $\alpha=\beta=\frac{1}{4}$, and by then letting $a=b=\frac{1}{4}$ and $c=1$. □

This theorem implies a mod p version for truncated hypergeometric functions.

Corollary 2.2. *If p is an odd prime, then*

$$(x+1)^{\frac{p-1}{2}} \cdot {}_3F_2^{\mathrm{tr}}\left(\frac{x}{x+1}\right)_p \equiv {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ 1\end{matrix} \mid -x\right)_p^2 \pmod p.$$

Proof. After replacing x by $\frac{x}{x+1}$ in Theorem 2.1, use the fact that

$$(x+1)^{-\frac{1}{2}} \equiv (x+1)^{\frac{p-1}{2}} \pmod{p, x^p}.$$

□

To prove Theorem 1.1, we require the following description of ${}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ 1\end{matrix} \mid -x\right)_p \pmod p$. For the remainder of the paper, for an odd prime p, set $m_p := \frac{p-1}{2}$ and $\widehat{m}_p := \lfloor \frac{m_p}{2} \rfloor$.

Lemma 2.3. *If p is an odd prime then*

$${}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ 1\end{matrix} \mid -x\right)_p \equiv \sum_{b=0}^{\widehat{m}_p} \binom{m_p}{b}\binom{m_p}{2b} x^b \pmod p.$$

Proof. It suffices to show, for $0 \le b \le m_p$, that

$$\binom{m_p}{b}\binom{m_p}{2b} \equiv (-1)^b \frac{\left(\frac{1}{4}\right)_b \left(\frac{3}{4}\right)_b}{(b!)^2} \pmod p.$$

This clearly holds when $b=0$.

The proof now follows by induction. Begin by noticing the following identities:

$$\begin{aligned}\binom{m_p}{b+1} &= \frac{m_p-b}{b+1}\cdot\binom{m_p}{b},\\ \binom{\frac{1}{4}}{b+1} &= \frac{4b+1}{4}\cdot\binom{\frac{1}{4}}{b},\\ \binom{\frac{3}{4}}{b+1} &= \frac{4b+3}{4}\cdot\binom{\frac{3}{4}}{b}.\end{aligned}$$

Using these identities, it then suffices to show that

$$\frac{(m_p-b)(m_p-2b-1)(m_p-2b)}{(b+1)(2b+2)(2b+1)} \equiv -\frac{(4b+1)(4b+3)}{16(b+1)^2} \pmod{p}.$$

This follows from the elementary congruence:

$$\begin{aligned}8(m_p-b)(m_p-(2b+1))(m_p-2b) &\equiv (2m_p-2b)(2m_p-(4b+2))(2m_p-4b)\\ &\equiv (-1-2b)(-3-4b)(-1-4b) \equiv -(4b+1)(4b+3)(2b+1) \pmod{p}.\end{aligned}$$

Finally notice that $\binom{m_p}{2b}=0$ if $b>\widehat{m}_p$. □

2.2. **Proof of Theorem 1.1.** It is well known (see Chapter V of [14]) that $E_{\mathrm{C}}(\lambda)$ is supersingular at a prime $p\geq 5$ if and only if the coefficient of $(xy)^{p-1}$ is zero modulo p in $f_\lambda(x,y)^{p-1}$, where

$$f_\lambda(x,y) := y^2-(x-1)(x^2+\lambda). \tag{2.1}$$

The following lemma gives a formula for that particular coefficient.

Lemma 2.4. *If p is an odd prime, then the coefficient of $(xy)^{p-1}$ modulo p in $f_\lambda(x,y)^{p-1}$ is*

$$(-1)^{m_p}\sum_{b=0}^{\widehat{m}_p}\binom{m_p}{b}\binom{m_p}{2b}\cdot\lambda^b.$$

Proof. Obviously, we have that

$$f_\lambda(x,y)^{p-1} = \sum_{c=0}^{p-1}\binom{p-1}{c}(-1)^c(x-1)^c(x^2+\lambda)^c y^{2(p-1-c)}.$$

Now observe that $(xy)^{p-1}$ occurs only in the middle of this sum, namely where $c=m_p$, and so it suffices to compute the coefficient of x^{p-1} in $(x-1)^{m_p}(x^2+\lambda)^{m_p}$. Now notice that

$$\begin{aligned}(x-1)^{m_p}(x^2+\lambda)^{m_p} &= \sum_{a=0}^{m_p}\binom{m_p}{a}(-1)^{m_p-a}x^a\cdot\sum_{b=0}^{m_p}\binom{m_p}{b}x^{2m_p-2b}\lambda^b\\ &= \sum_{n=0}^{3m_p}\left(\sum_{a+2m_p-2b=n}(-1)^{m_p-a}\binom{m_p}{a}\binom{m_p}{b}\lambda^b\right)x^n.\end{aligned}$$

One easily checks that the coefficient when $n = p-1$ is

$$(-1)^{m_p} \sum_{b=0}^{m_p} \binom{m_p}{b}\binom{m_p}{2b}\lambda^b.$$

To complete the proof, notice that $\binom{p-1}{m_p} \equiv (-1)^{m_p} \pmod p$, and that $\binom{m_p}{2b} = 0$ whenever $b > \widehat{m}_p$. □

Proof of Theorem 1.1. By Corollary 2.2 and Lemma 2.3, we have that

$$(x+1)^{\frac{p-1}{2}} \cdot {}_3F_2^{\mathrm{tr}}\left(\frac{x}{x+1}\right)_p \equiv {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix} \mid -x\right)_p^2 \equiv \left(\sum_{b=0}^{\widehat{m}_p}\binom{m_p}{b}\binom{m_p}{2b}x^b\right)^2 \pmod p.$$

To complete the proof, it suffices to show that

$$0 \not\equiv H_{\mathrm{C}}(x)_p \equiv \frac{1}{\binom{m_p}{\widehat{m}_p}\binom{m_p}{2\widehat{m}_p}} \cdot \left(\sum_{b=0}^{\widehat{m}_p}\binom{m_p}{b}\binom{m_p}{2b}x^b \pmod p\right).$$

By Lemma 2.4 and the preceding discussion, both polynomials have the same roots over $\overline{\mathbb{F}}_p$, and so they agree up to a multiplicative constant. Since both polynomials are monic by construction, they must be equal in $\mathbb{F}_p[x]$. □

Remark. It follows from the proof above that $H_C(x)$ has degree $\widehat{m}_p$.

Acknowledgements

The authors thank Marie Jameson for pointing out typographical errors in an earlier version of this paper. They are also grateful to the referee for helpful suggestions.

References

[1] S. Ahlgren, K. Ono, and D. Penniston, *Zeta functions of an infinite family of K3 surfaces*, Amer. J. Math. **124** (2002), pages 353-368.
[2] G. E. Andrews, R. Askey, R. Roy, *Special Functions* ,Cambridge Univ. Press, Cambridge, 1998.
[3] W. Bailey, *Generalized hypergeometric series*, Cambridge Univ. Press, Cambridge, 1935.
[4] J. Greene, *Hypergeometric series over finite fields*, Trans. Amer. Math. Soc. **301** (1987), pages 77-101.
[5] J. Greene and R. Evans, *Clausen's theorem and hypergeometric functions over finite fields*, Finite Fields Appl. **15** (2009), pages 97-109.
[6] J. Greene and D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, J. Number Theory **23** (1986), 136-148.
[7] D. Husemöller, *Elliptic Curves*, Springer Verlag, Graduate Texts in Mathematics, 111 (2004)
[8] M. Ishibashi, H. Sato and K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math.,**48** (1994), no. 2, pages 307-321.
[9] M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. **25** (1995), pages 43-52.
[10] D. McCarthy, ${}_3F_2$ *hypergeometric series and periods of elliptic curves*, Int. J. of Number Th., **6** (2010), no. 3, pages 461-470.
[11] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), pages 1205-1223.

[12] K. Ono, *Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-Series*, Amer. Math. Soc., (2004).
[13] J. Rouse, *Hypergeometric functions and elliptic curves*, Ramanujan J., **12** (2006), no. 2, pages 197-205.
[14] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

Department of Mathematics, Faculty of Science, Cairo University, Giza, Egypt 12613

Department of Mathematics, University of Wisconsin-Madison, Madison, Wisconsin 53703
E-mail address: a.elguindy@gmail.com, ono@math.wisc.edu