involve
a journal of mathematics

${}_3F_2$-hypergeometric functions and supersingular elliptic curves

Sarah Pitman

msp

2015 vol. 8, no. 3

INVOLVE 8:3 (2015)
dx.doi.org/10.2140/involve.2015.8.481

${}_3F_2$-hypergeometric functions and supersingular elliptic curves

Sarah Pitman

(Communicated by Ken Ono)

In recent work, Monks described the supersingular locus of families of elliptic curves in terms of ${}_2F_1$-hypergeometric functions. We lift his work to the level of ${}_3F_2$-hypergeometric functions by means of classical transformation laws and a theorem of Clausen.

1. Introduction and statement of results

Dating back to the works of Gauss, hypergeometric functions play an important role in mathematics. More recently, these complex functions and their analogs have been studied in terms of the complex periods of elliptic curves. The purpose of this paper is to further develop these sorts of connections. We begin by setting the notation and defining the hypergeometric functions which will be used throughout. If n is a nonnegative integer, we recall the Pochhammer symbol $(\gamma)_n$, defined 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 $\alpha_1, \ldots, \alpha_h, \beta_1, \ldots, \beta_j \in \mathbb{C}$ is defined by

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

We are interested in the hypergeometric functions

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} a & b \\ & c \end{matrix} \,\middle|\, x\right) := \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n} \cdot \frac{x^n}{n!} \tag{1-1}$$

and

$${}_3F_2^{\mathrm{cl}}\left(\begin{matrix} a & b & d \\ & c & e \end{matrix} \,\middle|\, x\right) := \sum_{n=0}^{\infty} \frac{(a)_n(b)_n(d)_n}{(c)_n(e)_n} \cdot \frac{x^n}{n!}, \tag{1-2}$$

MSC2010: 11G20, 33C20.
Keywords: hypergeometric functions, supersingular, elliptic curves.

and their truncations modulo primes p. For any odd prime p, we define these truncations by

$$ {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} a & b \\ & c \end{matrix}\,\middle|\, x\right)_p \equiv \sum_{n=0}^{(p-1)/2} \frac{(a)_n(b)_n}{(c)_n}\cdot\frac{x^n}{n!} \pmod p \tag{1-3} $$

and

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} a & b & d \\ & c & e \end{matrix}\,\middle|\, x\right)_p \equiv \sum_{n=0}^{(p-1)/2} \frac{(a)_n(b)_n(d)_n}{(c)_n(e)_n}\cdot\frac{x^n}{n!} \pmod p. \tag{1-4} $$

Monks [2012] studied elliptic curves and their relation to ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions and proved that these polynomials give the supersingular loci of certain families of elliptic curves. Here we lift his work from ${}_2F_1^{\mathrm{tr}}$- to ${}_3F_2^{\mathrm{tr}}$-hypergeometric functions and establish a similar result for these hypergeometric functions with additional parameters.

Remark. We note that above, tr denotes the truncation of a hypergeometric series after $x^{(p-1)/2}$, but in [Monks 2012], tr implies truncation after x^{p-1}. We will see that the relevant polynomials agree when reduced modulo p.

Let p be an odd prime and let $\mathbb{F}$ be a field of characteristic p. An elliptic curve $E/\mathbb{F}$ is said to be *supersingular* if it has no p-torsion over $\bar{\mathbb{F}}$. In other words, there is no element of order p in the group $E(\bar{\mathbb{F}})$. This condition is dependent only on the j-invariant of E. There are only finitely many isomorphism classes of supersingular elliptic curves in $\bar{\mathbb{F}}_p$, which Kaneko and Zagier [1998] determined using the theory of modular forms.

Here we consider supersingular elliptic curves in certain families. A well-known subfamily of elliptic curves is the Legendre family, which is denoted by

$$ E_{1/2}(\lambda) : y^2 = x(x-1)(x-\lambda) $$

for $\lambda \neq 0, 1$. These curves can be studied by means of the *supersingular locus*

$$ S_{p,1/2}(\lambda) := \prod_{\substack{\lambda_0\in\bar{\mathbb{F}}_p \\ \text{supersingular } E_{1/2}(\lambda_0)}} (\lambda-\lambda_0). $$

These polynomials have coefficients in $\mathbb{F}_p$.

El-Guindy and Ono [2013] studied the family of elliptic curves defined by

$$ E_{1/4}(\lambda) : y^2 = (x-1)(x^2+\lambda). \tag{1-5} $$

We also consider the following families of elliptic curves:

$$ E_{1/3}(\lambda) : y^2 + \lambda yx + \lambda^2 y = x^3, $$
$$ E_{1/12}(\lambda) : y^2 = 4x^3 - 27\lambda x - 27\lambda. $$

For $i \in \{\frac{1}{4}, \frac{1}{3}, \frac{1}{12}\}$ and all primes $p \geq 5$, we let

$$S_{p,i}(\lambda) := \prod_{\substack{\lambda_0 \in \overline{\mathbb{F}}_p \\ \text{supersingular } E_i(\lambda_0)}} (\lambda - \lambda_0). \tag{1-6}$$

Monks [2012] studied these families with respect to hypergeometric functions, and he showed that their supersingular loci are given by certain ${}_2F_1$-hypergeometric functions reduced modulo p. We extend these results of Monks, El-Guindy, and Ono to prove the following theorem. Assume the notation above.

Theorem 1.1. *The following are true*:

(1) *If $p \geq 5$ is prime, then*

$$S_{p,1/4}(x)^2 \equiv (x+1)^{(p-1)/2} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, \frac{x}{x+1}\right)_p \pmod{p}.$$

(2) *If $p \geq 5$ is prime, then*

$$S_{p,1/3}(x)^2 \equiv x^{2\cdot\lfloor p/3 \rfloor} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, \frac{108x - 2916}{x^2}\right)_p \pmod{p}.$$

(3) *If $p \geq 5$ is prime, then*

$$S_{p,1/12}(x)^2 \equiv (c_p^{-1})^2 \cdot x^{\lfloor p/6 \rfloor} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)_p \pmod{p}.$$

Here

$$c_p = \binom{6 \left\lfloor \frac{p}{12} \right\rfloor + d_p}{\left\lfloor \frac{p}{12} \right\rfloor}$$

and $d_p = 0, 2, 2, 4$ for $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively.

2. Nuts and bolts

Statement of Clausen's theorem and transformation laws. Our main tools for establishing these congruences are a theorem of Clausen and two classical ${}_2F_1^{\mathrm{cl}}$ transformation laws. We make use of Clausen's theorem [Bailey 1935] which gives the following equality of hypergeometric polynomials:

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

We also use two transformation laws in our proof so that we can apply (2-1) to the hypergeometric functions. The first, given in [Bailey 1935], states that

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} a & b \\ & c \end{matrix} \,\middle|\, x\right) = (1-x)^{-a} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} a & c-b \\ & c \end{matrix} \,\middle|\, \frac{x}{x-1}\right). \tag{2-2}$$

The second, from Vidūnas [2009], gives that

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} a & b \\ & \frac{a+b+1}{2} \end{matrix} \;\middle|\; x\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{a}{2} & \frac{b}{2} \\ & \frac{a+b+1}{2} \end{matrix} \;\middle|\; 4x(1-x)\right). \tag{2-3} $$

Elementary reduction modulo p. By definition (1-4), we have that

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; \frac{108x-2916}{x^2}\right)_p \equiv \sum_{n=0}^{(p-1)/2} \frac{\left(\frac{1}{3}\right)_n\left(\frac{2}{3}\right)_n\left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \frac{(108x-2916)^n}{x^{2n}} \pmod p. $$

For $n > \lfloor p/3 \rfloor$, any p will appear in the numerator of the expansion for $\left(\frac{1}{3}\right)_n$, $\left(\frac{2}{3}\right)_n$, or $\left(\frac{1}{2}\right)_n$, so all of these terms will be congruent to 0 modulo p and will vanish. Thus we can simplify to

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; \frac{108x-2916}{x^2}\right)_p \equiv \sum_{n=0}^{\lfloor p/3 \rfloor} \frac{\left(\frac{1}{3}\right)_n\left(\frac{2}{3}\right)_n\left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \frac{(108x-2916)^n}{x^{2n}} \pmod p. \tag{2-4} $$

Similarly by (1-4) we have that

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; 1-\frac{1}{x}\right)_p \equiv \sum_{n=0}^{(p-1)/2} \frac{\left(\frac{1}{6}\right)_n\left(\frac{5}{6}\right)_n\left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \left(1-\frac{1}{x}\right)^n \pmod p. $$

For any $n > \lfloor p/6 \rfloor$, $p \equiv 1, 5 \pmod 6$ will appear in the numerator of the expansion of $\left(\frac{1}{6}\right)_n\left(\frac{5}{6}\right)_n\left(\frac{1}{2}\right)_n$ causing all of these sequential terms to be congruent to 0 modulo p and vanish, which gives

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; 1-\frac{1}{x}\right)_p \equiv \sum_{n=0}^{\lfloor p/6 \rfloor} \frac{\left(\frac{1}{6}\right)_n\left(\frac{5}{6}\right)_n\left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \left(1-\frac{1}{x}\right)^n \pmod p. \tag{2-5} $$

Work of Monks. The proof of Theorem 1.1 relies on recent work of El-Guindy and Ono and Monks.

Theorem 2.1 [Monks 2012, pp. 2–3]. *The following are true*:

(1) *If $p \geq 5$ is prime*,

$$ S_{p,1/4}(x) \equiv {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix} \;\middle|\; -x\right)_p \pmod p. \tag{2-6} $$

(2) *If $p \geq 5$ is prime*,

$$ S_{p,1/3}(x) \equiv x^{\lfloor p/3 \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \;\middle|\; \frac{27}{x}\right)_p \pmod p. \tag{2-7} $$

(3) *For* $p \equiv 1, 5 \pmod{12}$ *and prime*,

$$S_{p,1/12}(x) \equiv c_p^{-1} \cdot x^{\lfloor p/12 \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \;\middle|\; 1 - \frac{1}{x} \right)_p \pmod{p}. \tag{2-8}$$

(4) *For* $p \equiv 7, 11 \pmod{12}$ *and prime*,

$$S_{p,1/12}(x) \equiv c_p^{-1} \cdot x^{\lfloor p/12 \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \;\middle|\; 1 - \frac{1}{x} \right)_p \pmod{p}, \tag{2-9}$$

where

$$c_p = \binom{6 \left\lfloor \frac{p}{12} \right\rfloor + d_p}{\left\lfloor \frac{p}{12} \right\rfloor}$$

and $d_p = 0, 2, 2, 4$ *for* $p \equiv 1, 5, 7, 11 \pmod{12}$ *respectively.*

Remark. We note that (2-6) is a direct result of El-Guindy and Ono [2013] and is therefore not technically part of Monks' theorem in [2012].

Squaring these supersingular loci in terms of the ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions, we obtain congruent ${}_3F_2^{\mathrm{tr}}$-hypergeometric representations in Theorem 1.1.

3. Proof of Theorem 1.1

To prove Theorem 1.1, we show the first part using the results of El-Guindy and Ono. Then we calculate the equivalent statements for the remaining cases. We use classical ${}_2F_1^{\mathrm{cl}}$ transformation laws to obtain the necessary forms to use Clausen's theorem, given in (2-1), and lift the ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions of Monks to equivalent ${}_3F_2^{\mathrm{tr}}$ representations. First we require the following descriptions of ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions:

Lemma 3.1. *The following are true*:

(1) *If* $p \geq 5$ *is an odd prime*, *then*

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

(2) *If* $p \geq 5$ *is an odd prime*, *then*

$${}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \;\middle|\; \frac{27}{x} \right)_p^2 \equiv {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; \frac{108x - 2916}{x^2} \right)_p \pmod{p}.$$

(3) *For* $p \equiv 1, 5 \pmod{12}$,

$${}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \;\middle|\; 1 - \frac{1}{x} \right)_p^2 \equiv {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \;\middle|\; 1 - \frac{1}{x} \right)_p \pmod{p}.$$

(4) *For* $p \equiv 7, 11 \pmod{12}$,

$$ {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{7}{12} & \frac{11}{12} \\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{x}\right)_p^2 \equiv x \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\, 1-\frac{1}{x}\right)_p \pmod{p}. $$

Proof. For brevity, we give the proof of (2). The remaining cases follow in a similar way. Applying the transformation law for ${}_2F_1$-hypergeometric functions given by (2-3) with $a = \frac{1}{3}$, $b = \frac{2}{3}$, and $x = 27/x$, we see that

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & 1\end{matrix}\,\middle|\, \frac{27}{x}\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{6} & \frac{1}{3} \\ & 1\end{matrix}\,\middle|\, \frac{108x-2916}{x^2}\right). $$

We then square both sides of this equation and apply Clausen's theorem in (2-1) to the right-hand expression with $\alpha = \frac{1}{6}$, $\beta = \frac{1}{3}$, and $x = (108x - 2916)/x^2$ to obtain

$$ \begin{aligned} {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & 1\end{matrix}\,\middle|\, \frac{27}{x}\right)^2 &= {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{6} & \frac{1}{3} \\ & 1\end{matrix}\,\middle|\, \frac{108x-2916}{x^2}\right)^2 \\ &= {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\, \frac{108x-2916}{x^2}\right). \end{aligned} \tag{3-1} $$

By definition (1-1), when we expand the infinite hypergeometric series on the left-hand side of this equation, we obtain

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & 1\end{matrix}\,\middle|\, \frac{27}{x}\right)^2 = \left(\sum_{N=0}^{\infty} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N\right)^2, $$

and when we expand the right hand side by definition (1-2) we get

$$ {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\, \frac{108x-2916}{x^2}\right) = \sum_{N=0}^{\infty} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N \left(\frac{1}{2}\right)_N}{(N!)^3} \cdot \left(\frac{108x-2916}{x^2}\right)^N. $$

By (3-1), we have that these two infinite series expansions are equal and

$$ \left(\sum_{N=0}^{\infty} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N\right)^2 = \sum_{N=0}^{\infty} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N \left(\frac{1}{2}\right)_N}{(N!)^3} \cdot \left(\frac{108x-2916}{x^2}\right)^N. \tag{3-2} $$

This means that in both series expansions, the coefficients for x^{-N}, given by $a(N)$ and $b(N)$ respectively, are equal. More precisely, by squaring we have

$$ a(N) = \sum_{n=0}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{\left(\frac{1}{3}\right)_{N-n} \left(\frac{2}{3}\right)_{N-n}}{((N-n)!)^2} \cdot 27^N, $$

and by the binomial theorem,

$$b(N) = \sum_{n=\lceil N/2\rceil}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n \left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \binom{n}{2n-N} (108)^{2n-N} (-2916)^{N-n}.$$

We note that for $b(N)$, only n with $\lceil N/2\rceil \le n \le N$ will actually contribute to each coefficient value. When we truncate these series in (3-2) at $N = p-1$ (i.e., truncate at x^{1-p}), all of the coefficients will still be equal. The truncation of the series can be explicitly expressed by

$$\sum_{N=0}^{p-1} \sum_{n=0}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{\left(\frac{1}{3}\right)_{N-n} \left(\frac{2}{3}\right)_{N-n}}{((N-n)!)^2} \cdot 27^N \cdot x^{-N}$$
$$= \sum_{N=0}^{p-1} \sum_{n=\lceil N/2\rceil}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n \left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \binom{n}{2n-N} (108)^{2n-N} (-2916)^{N-n} \cdot x^{-N}. \quad (3\text{-}3)$$

We observe that since N, and consequently n, will never exceed $p-1$, all of these coefficients are p-integral since p does not appear in any of the denominators. Therefore we can take both sides of (3-3) modulo p. In fact, we know that a lot of terms will vanish modulo p because p will appear as a factor in the numerators of the coefficient expansions of these series given by $a(N)$ and $b(N)$, making them congruent to 0. More specifically, this is the case for N with $(p-1)/2 < N \le p-1$ and $n \ge (p-1)/2$. We can write these simplified congruences as

$$\sum_{N=0}^{p-1} \sum_{n=0}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{\left(\frac{1}{3}\right)_{N-n} \left(\frac{2}{3}\right)_{N-n}}{((N-n)!)^2} \cdot \left(\frac{27}{x}\right)^N$$
$$\equiv \left(\sum_{N=0}^{(p-1)/2} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N \right)^2 \pmod{p} \quad (3\text{-}4)$$

and

$$\sum_{N=0}^{p-1} \sum_{n=\lceil N/2\rceil}^{N} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n \left(\frac{1}{2}\right)_n}{(n!)^3} \cdot \binom{n}{2n-N} (108)^{2n-N} (-2916)^{N-n} \cdot x^{-N}$$
$$\equiv \sum_{N=0}^{(p-1)/2} \frac{\left(\frac{1}{3}\right)_N \left(\frac{2}{3}\right)_N \left(\frac{1}{2}\right)_N}{(N!)^3} \cdot \left(\frac{108x - 2916}{x^2}\right)^N \pmod{p}. \quad (3\text{-}5)$$

Finally, we see that the right-hand sides of (3-4) and (3-5) are congruent modulo p to the definitions of the truncated forms of the squares of the ${}_2F_1$- and

${}_3F_2$-hypergeometric functions, respectively, given by:

$$ {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3}\\ & 1\end{matrix}\,\middle|\,\frac{27}{x}\right)_p^2 \equiv \left(\sum_{N=0}^{(p-1)/2}\frac{\left(\frac{1}{3}\right)_N\left(\frac{2}{3}\right)_N}{(N!)^2}\cdot\left(\frac{27}{x}\right)^N\right)^2 \pmod p $$

and

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2}\\ & 1 & 1\end{matrix}\,\middle|\,\frac{108x-2916}{x^2}\right)_p \equiv \sum_{N=0}^{(p-1)/2}\frac{\left(\frac{1}{3}\right)_N\left(\frac{2}{3}\right)_N\left(\frac{1}{2}\right)_N}{(N!)^3}\cdot\left(\frac{108x-2916}{x^2}\right)^N \pmod p. $$

It follows that

$$ {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3}\\ & 1\end{matrix}\,\middle|\,\frac{27}{x}\right)_p^2 \equiv {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2}\\ & 1 & 1\end{matrix}\,\middle|\,\frac{108x-2916}{x^2}\right)_p \pmod p, $$

which completes the proof. □

Proof of Theorem 1.1. For the proof of (1), we begin with Lemma 3.1(1) which gives

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

Substituting the left-hand side of the above congruence into the square of (2-6), we obtain the congruence for the square of the supersingular locus $S_{p,(1/4)}(x)^2$ for the family of elliptic curves given by $E_{1/4}(\lambda)$.

The remaining cases use the congruences of the supersingular loci given by Monks. We begin by squaring the ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions in (2-7)–(2-9). Squaring (2-7), we obtain

$$ S_{p,1/3}(x)^2 \equiv x^{2\cdot\lfloor p/3\rfloor}\cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3}\\ & 1\end{matrix}\,\middle|\,\frac{27}{x}\right)_p^2 \pmod p. $$

Then using the congruence in Lemma 3.1(2), we have

$$ S_{p,1/3}(x)^2 \equiv x^{2\cdot\lfloor p/3\rfloor}\cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2}\\ & 1 & 1\end{matrix}\,\middle|\,\frac{108x-2916}{x^2}\right)_p \pmod p, $$

completing the proof of (2).

In the third case, after squaring (2-8), we obtain

$$ S_{p,1/12}(x)^2 \equiv (c_p^{-1})^2\cdot x^{2\cdot\lfloor p/12\rfloor}\cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\,1-\frac{1}{x}\right)_p^2 \pmod p. $$

Then we use our congruence given in Lemma 3.1(3) and substitute the ${}_3F_2$-hypergeometric function to give

$$S_{p,1/12}(x)^2 \equiv (c_p^{-1})^2 \cdot x^{\lfloor p/6 \rfloor} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)_p \pmod{p}.$$

We see in (3) and (4) of Lemma 3.1, for $p \equiv 1, 5 \pmod 6$, the squared ${}_2F_1^{\mathrm{tr}}$-hypergeometric functions are congruent apart from the x in (4). We combine these cases and alter the exponent of x to satisfy both, which then gives our result.

4. Examples

Example. Here we consider $E_{1/12}(x)$ when $p = 13$. By Monks' theorem, we know that there is just one supersingular elliptic curve for $E_{1/12}(x)$. It turns out that $E_{1/12}(3)$ is that supersingular elliptic curve. To see this, we note that $E_{1/12}(3)$ over $\mathbb{F}_{13}$ has 13 points including the point at infinity. By Monks, this implies that

$$S_{13,1/12}(x) \equiv (x - 3) \equiv (x + 10) \pmod{13}.$$

We square this to obtain

$$S_{13,1/12}(x)^2 \equiv (x + 10)^2 \equiv (x^2 + 20x + 100) \equiv x^2 + 7x + 9 \pmod{13}.$$

Using Theorem 1.1(3), we calculate

$$(c_{13}^{-1})^2 \cdot x^{\lfloor 13/6 \rfloor} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)_{13} \pmod{13},$$

which gives $(c_{13}^{-1})^2 \equiv \frac{1}{10} \pmod{13}$ and $x^{\lfloor 13/6 \rfloor} = x^2$. Substituting these values into our expression gives

$$\frac{1}{10} \cdot x^2 \cdot \left(10 + \frac{5}{x} + \frac{12}{x^2}\right) \equiv x^2 + \frac{1}{2}x + \frac{6}{5} \equiv x^2 + 7x + 9 \pmod{13}.$$

This polynomial can be factored modulo 13 as

$$x^2 + 7x + 9 \equiv (x + 10)^2 \pmod{13},$$

which is what we found after directly squaring $S_{13,1/12}(x)$.

Example. We consider $E_{1/12}(x)$ when $p = 59$. By Monks' theorem, we know that there are four supersingular elliptic curves for $E_{1/12}(x)$. Those supersingular elliptic curves are found to be $E_{1/12}(32)$, $E_{1/12}(35)$, $E_{1/12}(24)$ and $E_{1/12}(22)$. To see this, we note that $E_{1/12}(x)$ for $x = 32, 35, 24$ and 22 over $\mathbb{F}_{59}$ have 59 points

including the point at infinity. By Monks, this implies that

$$\begin{aligned} S_{59,1/12}(x) &\equiv (x-32)(x-35)(x-24)(x-22) \\ &\equiv (x+27)(x+24)(x+35)(x+37) \pmod{59}. \end{aligned}$$

After squaring this directly, we obtain

$$S_{59,1/12}(x)^2 \equiv (x+27)^2(x+24)^2(x+35)^2(x+37)^2 \pmod{59}. \tag{4-1}$$

Next using Theorem 1.1(3) we calculate

$$(c_{59}^{-1})^2 \cdot x^{\lfloor 59/6 \rfloor} \cdot {}_3F_2^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)_{59} \pmod{59}.$$

For $p = 59$, we have $(c_{59}^{-1})^2 = 15$ and $x^{\lfloor 59/6 \rfloor} = x^9$, so we obtain

$$\begin{aligned} &15 \cdot x^9 \cdot \left(\frac{4}{x} + \frac{40}{x^2} + \frac{3}{x^3} + \frac{16}{x^4} + \frac{38}{x^5} + \frac{56}{x^6} + \frac{16}{x^7} + \frac{28}{x^8} + \frac{36}{x^9}\right) \\ &\qquad \equiv x^8 + 10x^7 + 45x^6 + 4x^5 + 39x^4 + 14x^3 + 4x^2 + 7x + 9 \pmod{59}. \end{aligned}$$

This polynomial of degree 8 can be factored as

$$(x+27)^2(x+24)^2(x+35)^2(x+37)^2 \pmod{59},$$

which is congruent modulo 59 to $S_{59,1/12}(x)^2$ as given in (4-1).

References

[Bailey 1935] W. Bailey, *Generalized hypergeometric series*, Cambridge Univ. Press, 1935. Reprinted 1964, etc.

[El-Guindy and Ono 2013] A. El-Guindy and K. Ono, "Hasse invariants for the Clausen elliptic curves", *Ramanujan J.* **31**:1-2 (2013), 3–13. MR 3048650

[Kaneko and Zagier 1998] M. Kaneko and D. Zagier, "Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials", pp. 97–126 in *Computational perspectives on number theory* (Chicago, IL, 1995), edited by 99b:11064, AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998. MR 99b:11064

[Monks 2012] K. Monks, "On supersingular elliptic curves and hypergeometric functions", *Involve* **5**:1 (2012), 99–113. MR 2924318

[Vidūnas 2009] R. Vidūnas, "Algebraic transformations of Gauss hypergeometric functions", *Funkcial. Ekvac.* **52**:2 (2009), 139–180. MR 2010i:33012

Received: 2013-07-17 Revised: 2013-09-02 Accepted: 2013-09-04

spitman222@gmail.com *Emory University,*
Department of Mathematics and Computer Science,
400 Dowman Drive, Atlanta, Georgia 30322, United States

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2015 is US $140/year for the electronic version, and $190/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2015 vol. 8 no. 3

1944-4176(2015)8:3;1-4