3F₂-HYPERGEOMETRIC FUNCTIONS AND SUPERSINGULAR ELLIPTIC CURVES

SARAH PITMAN

Abstract. In recent work, Monks described the supersingular locus of families of elliptic curves in terms of 2F₁-hypergeometric functions. We “lift” his work to the level of 3F₂-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

\[
hFcl_j \left( \begin{array} {cccc} \alpha_1 & \cdots & \alpha_h \\ \beta_1 & \cdots & \beta_j \end{array} | x \right) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n (\alpha_2)_n \cdots (\alpha_h)_n}{(\beta_1)_n (\beta_2)_n \cdots (\beta_j)_n} \cdot \frac{x^n}{n!}.
\]

We are interested in the hypergeometric functions

\[
2Fcl_1 \left( \begin{array} {cc} a & b \\ c \end{array} | x \right) := \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \cdot \frac{x^n}{n!}
\]

and

\[
3Fcl_2 \left( \begin{array} {ccc} a & b & d \\ c & e \end{array} | x \right) := \sum_{n=0}^{\infty} \frac{(a)_n (b)_n (d)_n}{(c)_n (e)_n} \cdot \frac{x^n}{n!},
\]

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

\[
2F1^{\text{tr}}_1 \left( \begin{array} {cc} a & b \\ c \end{array} | x \right)_p \equiv \sum_{n=0}^{p-1} \frac{(a)_n (b)_n}{(c)_n} \cdot \frac{x^n}{n!} \pmod{p}
\]

and

\[
3F2^{\text{tr}}_2 \left( \begin{array} {ccc} a & b & d \\ c & e \end{array} | x \right)_p \equiv \sum_{n=0}^{p-1} \frac{(a)_n (b)_n (d)_n}{(c)_n (e)_n} \cdot \frac{x^n}{n!} \pmod{p}.
\]
In recent work, Monk has studied elliptic curves and their relation to $2F_1^\text{tr}$-hypergeometric functions and has proved that these polynomials give the supersingular loci of certain families of elliptic curves. Here we “lift” his work from $2F_1^\text{tr}$- to $3F_2^\text{tr}$-hypergeometric functions and establish a similar result for these hypergeometric functions with additional parameters.

Remark. We note that tr denotes the truncation of a hypergeometric series after $x^{\frac{p-1}{2}}$. We note that in [4] 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 $\mathbb{F}$. In other words, there is no element of order $p$ in the group $E(\mathbb{F})$. This condition is dependent only on the $j$-invariant of $E$. There are only finitely many isomorphism classes of supersingular elliptic curves in $\mathbb{F}_p$, which Kaneko and Zagier [3] determine 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

$$E_1^4(\lambda) : y^2 = (x - 1)(x - \lambda)$$

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

$$S_{p, 4}(\lambda) := \prod_{\lambda_0 \in \mathbb{F}_p \text{ supersingular } E_1^4(\lambda_0)} (\lambda - \lambda_0).$$

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

In [2], El-Guindy and Ono studied the family of elliptic curves defined by

(1.5) $$E_3^4(\lambda) : y^2 = (x - 1)(x^2 + \lambda).$$

We also consider the following families of elliptic curves:

(1.6) $$E_3^3(\lambda) : y^2 + \lambda y x + \lambda^2 y = x^3$$

(1.7) $$E_3^{12}(\lambda) : y^2 = 4x^3 - 27\lambda x - 27\lambda.$$ 

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

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

In his paper [4], Monks studies these families with respect to hypergeometric functions, and he shows 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
   \[
   S_{p,1}(x)^2 \equiv (x + 1)^{p-1} \cdot 3F_2^{\text{tr}} \left( \begin{array}{ccc} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ 1 & 1 & x \end{array} \right)_p \pmod{p}.
   \]

2. If $p \geq 5$ is prime, then
   \[
   S_{p,1}(x)^2 \equiv x^2 \cdot 3F_2^{\text{tr}} \left( \begin{array}{ccc} \frac{5}{6} & \frac{1}{2} & \frac{1}{2} \\ 1 & 1 & 0 \end{array} \right)_p \pmod{p}.
   \]

3. If $p \geq 5$ is prime, then
   \[
   S_{p,1}(x)^2 \equiv \left( c_p^{-1} \right)^2 \cdot x^2 \cdot 3F_2^{\text{tr}} \left( \begin{array}{ccc} \frac{5}{6} & \frac{1}{2} & \frac{1}{2} \\ 1 & 1 & 1 - \frac{1}{x} \end{array} \right)_p \pmod{p}.
   \]

Here $c_p = \left( \frac{p}{12} \right) + d_p$ and $d_p = 0, 2, 2, 4$ for $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively.

2. Nuts and Bolts

2.1. Statement of Clausen’s Theorem and Transformation Laws. Our main tools for establishing these congruences are a theorem of Clausen and two classical $2F_1^{\text{cl}}$ transformation laws. We make use of the a theorem of Clausen [1] which gives the following equality of hypergeometric polynomials:

\[
\tag{2.1}
3F_2^{\text{cl}} \left( \begin{array}{ccc} 2\alpha & 2\beta & \alpha + \beta \\ 2\alpha + 2\beta & \alpha + \beta + \frac{1}{2} \end{array} \right)_x = 2F_1^{\text{cl}} \left( \begin{array}{ccc} \alpha & \beta \\ \alpha + \beta + \frac{1}{2} \end{array} \right)_x^2.
\]

We also use two transformation laws in our proof so that we can apply (2.1) to the hypergeometric functions. The first is given by Bailey in [1] which states that

\[
\tag{2.2}
2F_1^{\text{cl}} \left( \begin{array}{ccc} a & b & c \\ \alpha & c - b \end{array} \right)_x = (1 - x)^{-a} \cdot 2F_1^{\text{cl}} \left( \begin{array}{ccc} a & b \\ \alpha + \frac{1}{2} \end{array} \right)_x \cdot \frac{x}{x - 1}.
\]

The second is from Vidunas given in [5]. We have that

\[
\tag{2.3}
2F_1^{\text{cl}} \left( \begin{array}{ccc} a & b \\ \alpha + \frac{1}{2} \end{array} \right)_x = 2F_1^{\text{cl}} \left( \begin{array}{ccc} a & b \\ \alpha + \frac{1}{2} \end{array} \right)_x \cdot 4x(1 - x).
\]

2.2. Elementary Reduction modulo $p$. By definition (1.4) we have that

\[
\tag{2.4}
3F_2^{\text{tr}} \left( \begin{array}{ccc} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ 1 & 1 & x^2 \end{array} \right)_p \equiv \sum_{n=0}^{p-1} \frac{\frac{1}{3}}{n} \cdot \frac{\frac{2}{3}}{n} \cdot \frac{\frac{1}{2}}{n} \frac{(108x - 2916)^n}{x^{2n}} \pmod{p}.
\]

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

\[
\tag{2.4}
3F_2^{\text{tr}} \left( \begin{array}{ccc} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ 1 & 1 & x^2 \end{array} \right)_p \equiv \sum_{n=0}^{\left\lfloor \frac{p}{3} \right\rfloor} \frac{\frac{1}{3}}{n} \cdot \frac{\frac{2}{3}}{n} \cdot \frac{\frac{1}{2}}{n} \frac{(108x - 2916)^n}{x^{2n}} \pmod{p}.
\]
Similarly by (1.4) we have that

\[ 3F_2^{tr} \left( \begin{array}{ccc} 1 & 5 & 6 \\ 1 & 1/2 & 1 \end{array} \right) \equiv \sum_{n=0}^{p-1} \frac{(1/6)_n (5/6)_n (1/2)_n}{(n!)^3} \left( 1 - \frac{1}{x} \right)^n \pmod{p}. \]

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

\[ (2.5) \quad 3F_2^{tr} \left( \begin{array}{ccc} 1 & 5 & 6 \\ 1 & 1/2 & 1 \end{array} \right) \equiv \lfloor p/6 \rfloor \sum_{n=0}^{\lfloor p/6 \rfloor} \frac{(1/6)_n (5/6)_n (1/2)_n}{(n!)^3} \left( 1 - \frac{1}{x} \right)^n \pmod{p}. \]

2.3. Work of Monks. The proof of Theorem 1.1 shall rely on recent work of El-Guindy and Ono and Monks. These are formulas given on pages 2 and 3 of [4].

**Theorem 2.1 (Monks in [4]).** The following are true:

1. If \( p \geq 5 \) is prime,

\[ S_{p, 1/4}(x) \equiv 2F_1^{tr} \left( \begin{array}{ccc} 1 & 3/4 \\ 1 & 1 \end{array} \right) \pmod{p}. \]

2. If \( p \geq 5 \) is prime,

\[ S_{p, 3/4}(x) \equiv x^{1/2} \cdot 2F_1^{tr} \left( \begin{array}{ccc} 1/3 & 2/3 \\ 1 & 1 \end{array} \right) \pmod{p}. \]

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

\[ S_{p, 1/12}(x) \equiv c_p^{-1} \cdot x^{1/12} \cdot 2F_1^{tr} \left( \begin{array}{ccc} 1/12 & 5/12 \\ 1 & 1 \end{array} \right) \pmod{p}. \]

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

\[ S_{p, 1/12}(x) \equiv c_p^{-1} \cdot x^{1/12} \cdot 2F_1^{tr} \left( \begin{array}{ccc} 7/12 & 11/12 \\ 1 & 1 \end{array} \right) \pmod{p}, \]

where \( c_p = \left( 6 \left\lfloor \frac{p}{12} \right\rfloor + d_p \right) \) 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 and is therefore not technically part of Monks’ theorem in [4].

Squaring these supersingular loci in terms of the \( 2F_1^{tr} \)-hypergeometric functions, we obtain congruent \( 3F_2^{tr} \)-hypergeometric representations in Theorem 1.1.

### 3. Proofs 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 \( 2F_1^{cl} \) transformation laws to obtain the necessary forms to use Clausen’s theorem, given in (2.1), and “lift” the \( 2F_1^{tr} \)-hypergeometric functions of Monks to equivalent \( 3F_2^{tr} \) representations. First we require the following descriptions of \( 2F_1^{tr} \)-hypergeometric functions:
Lemma 3.1. The following are true:

1. If $p \geq 5$ is an odd prime, then

\[ 2F_1^{tr}\left(\frac{1}{3}, \frac{2}{3} \mid -x\right)_p^2 \equiv (x + 1)^{\frac{p+1}{2}} \cdot 3F_2^{tr}\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \mid \frac{x}{x+1}\right)_p \quad (\text{mod } p). \]

2. If $p \geq 5$ is an odd prime, then

\[ 2F_1^{tr}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{27}{x}\right)_p^2 \equiv 3F_2^{tr}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{108x - 2916}{x^2}\right)_p \quad (\text{mod } p). \]

3. For $p \equiv 1, 5 \pmod{12}$, then

\[ 2F_1^{tr}\left(\frac{1}{12}, \frac{5}{12} \mid 1 - \frac{1}{x}\right)_p^2 \equiv 3F_2^{tr}\left(\frac{1}{6}, \frac{5}{6} \mid \frac{108x - 2916}{x^2}\right)_p \quad (\text{mod } p). \]

4. For $p \equiv 7, 11 \pmod{12}$, then

\[ 2F_1^{tr}\left(\frac{7}{12}, \frac{11}{12} \mid 1 - \frac{1}{x}\right)_p^2 \equiv x \cdot 3F_2^{tr}\left(\frac{1}{6}, \frac{5}{6} \mid \frac{108x - 2916}{x^2}\right)_p \quad (\text{mod } p). \]

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 $x = \frac{27}{x}$, we see that

\[ 2F_1^{cl}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{27}{x}\right) = 2F_1^{cl}\left(\frac{1}{6}, \frac{1}{3} \mid \frac{108x - 2916}{x^2}\right). \]

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 $x = \frac{108x - 2916}{x^2}$ to obtain

\[ 2F_1^{cl}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{27}{x}\right)^2 = 2F_1^{cl}\left(\frac{1}{6}, \frac{1}{3} \mid \frac{108x - 2916}{x^2}\right)^2 \]

\[ = 3F_2^{cl}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{108x - 2916}{x^2}\right). \]

By definition (1.1) when we expand the infinite hypergeometric series on the left hand side of this equation, we obtain

\[ 2F_1^{cl}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{27}{x}\right)^2 = \left(\sum_{N=0}^{\infty} \frac{(\frac{1}{3})_N(\frac{2}{3})_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N\right)^2, \]

and when we expand the right hand side by definition (1.2) we get

\[ 3F_2^{cl}\left(\frac{1}{3}, \frac{2}{3} \mid \frac{108x - 2916}{x^2}\right) = \sum_{N=0}^{\infty} \frac{(\frac{1}{3})_N(\frac{2}{3})_N(\frac{1}{2})_N}{(N!)^3} \cdot \left(\frac{108x - 2916}{x^2}\right)^N. \]
By (3.1) we have that these two infinite series expansions are equal

\[(3.2) \quad \left( \sum_{n=0}^{\infty} \frac{(\frac{1}{3})_N \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{27}{x} \right)^2 = \sum_{N=0}^{\infty} \frac{(\frac{1}{3})_N \left(\frac{2}{3}\right)_n}{(n!)^3} \cdot \left( \frac{108x - 2916}{x^2} \right)^N.\]

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

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

and by the Binomial Theorem

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

We note that for \(b(N)\) only \(\lceil \frac{N}{2} \rceil \leq n \leq N\) 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

\[(3.3) \quad \sum_{N=0}^{p-1} \sum_{n=0}^{N} \frac{(\frac{1}{3})_n \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{(\frac{1}{3})_{N-n} \left(\frac{2}{3}\right)_{N-n}}{((N-n)!)^2} \cdot 27^N \cdot x^{-N}\]

\[(3.4) \quad = \sum_{N=0}^{p-1} \sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{3})_n \left(\frac{2}{3}\right)_n}{(n!)^3} \cdot \left( \frac{n}{2n-N} \right) (108)^{2n-N} (-2916)^{N-n} \cdot x^{-N}.\]

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 \(\frac{p-1}{2} < N \leq p-1\) and \(n \geq \frac{p-1}{2}\). We can write these simplified congruences as

\[(3.5) \quad \sum_{N=0}^{p-1} \sum_{n=0}^{N} \frac{(\frac{1}{3})_n \left(\frac{2}{3}\right)_n}{(n!)^2} \cdot \frac{(\frac{1}{3})_{N-n} \left(\frac{2}{3}\right)_{N-n}}{((N-n)!)^2} \cdot \left( \frac{27}{x} \right)^N \equiv \left( \sum_{N=0}^{p-1} \frac{(\frac{1}{3})_N \left(\frac{2}{3}\right)_N}{(N!)^2} \cdot \left( \frac{27}{x} \right)^N \right)^2 \quad \text{(mod } p)\]

and

\[\sum_{N=0}^{p-1} \sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{3})_n \left(\frac{2}{3}\right)_n \left(\frac{1}{3}\right)_n}{(n!)^3} \cdot \left( \frac{n}{2n-N} \right) (108)^{2n-N} (-2916)^{N-n} \cdot x^{-N}\]

\[(3.6) \quad \equiv \sum_{N=0}^{p-1} \frac{(\frac{1}{3})_N \left(\frac{2}{3}\right)_N \left(\frac{1}{3}\right)_N}{(N!)^3} \cdot \left( \frac{108x - 2916}{x^2} \right)^N \quad \text{(mod } p).\]
Finally we see that the right hand sides of (3.5) and (3.6) 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:

$$2F_1^{tr}\left(\frac{1}{3}, \frac{2}{3} \left| \frac{27}{x} \right\rangle_p \right)^2 \equiv \left( \sum_{N=0}^{p-1} \frac{\left(\frac{1}{3}\right)N\left(\frac{2}{3}\right)_N}{N!^2} \cdot \left( \frac{27}{x} \right)^N \right)^2 \quad (\text{mod } p)$$

and

$$3F_2^{tr}\left(\frac{1}{3}, \frac{2}{3}, \frac{1}{2} \left| \frac{108x - 2916}{x^2} \right\rangle_p \right)^2 \equiv \left( \sum_{N=0}^{p-1} \frac{\left(\frac{1}{3}\right)N\left(\frac{2}{3}\right)N\left(\frac{1}{2}\right)_N}{N!^3} \cdot \left( \frac{108x - 2916}{x^2} \right)^N \right)^2 \quad (\text{mod } p).$$

It follows that

$$2F_1^{tr}\left(\frac{1}{3}, \frac{2}{3} \left| \frac{27}{x} \right\rangle_p \right)^2 \equiv 3F_2^{tr}\left(\frac{1}{3}, \frac{2}{3}, \frac{1}{2} \left| \frac{108x - 2916}{x^2} \right\rangle_p \right)^2 \quad (\text{mod } p),$$

which completes the proof.

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

$$(x + 1)^{p-1} \cdot 3F_2^{tr}\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \left| \frac{x}{x + 1} \right\rangle_p \right)^2 \equiv 2F_1^{tr}\left(\frac{1}{4}, \frac{3}{4} \left| -x \right\rangle_p \right)^2 \quad (\text{mod } p).$$

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, $S_{p, \frac{1}{4}}(x)^2$, for the family of elliptic curves given by $E_{\frac{1}{4}}(\lambda)$.

The remaining cases use the congruences of the supersingular locus given by Monks. The $2F_1^{tr}$-hypergeometric functions in (2.7), (2.8), and (2.9) are squared. Squaring (2.7) we obtain

$$S_{p, \frac{1}{3}}(x)^2 \equiv x^{2\left[\frac{1}{3}\right]} \cdot 2F_1^{tr}\left(\frac{1}{3}, \frac{2}{3} \left| \frac{27}{x} \right\rangle_p \right)^2 \quad (\text{mod } p).$$

Then using the congruence in (2) of Lemma 3.1, we have our result:

$$S_{p, \frac{1}{3}}(x)^2 \equiv x^{2\left[\frac{1}{3}\right]} \cdot 3F_2^{tr}\left(\frac{1}{3}, \frac{2}{3} \left| \frac{108x - 2916}{x^2} \right\rangle_p \right)^2 \quad (\text{mod } p).$$

In the third case after squaring (2.8), we obtain

$$S_{p, \frac{1}{12}}(x)^2 \equiv (c_p^{-1})^2 \cdot x^{2\left[\frac{1}{12}\right]} \cdot 2F_1^{tr}\left(\frac{1}{12}, \frac{5}{12} \left| 1 - \frac{1}{x} \right\rangle_p \right)^2 \quad (\text{mod } p).$$

Then we use our congruence given in (3) of Lemma 3.1 and substitute the $3F_2$-hypergeometric function to give

$$S_{p, \frac{1}{12}}(x)^2 \equiv (c_p^{-1})^2 \cdot x^{\left[\frac{5}{6}\right]} \cdot 3F_2^{tr}\left(\frac{1}{6}, \frac{5}{6} \left| 1 - \frac{1}{x} \right\rangle_p \right)^2 \quad (\text{mod } p).$$
We see in (3) and (4) of Lemma 3.1 for \( p \equiv 1, 5 \pmod{6} \), the squared \( {}_{2}F_{1}\)-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 \( E_{\frac{1}{13}}(x) \) when \( p = 13 \). By Monks’ theorem, we know that there is just one supersingular elliptic curve for \( E_{\frac{1}{13}}(x) \). It turns out that \( E_{\frac{1}{13}}(3) \) is that supersingular elliptic curve. To see this we note that \( E_{\frac{1}{13}}(3) \) over \( \mathbb{F}_{13} \) has 13 points including the point at infinity. By Monks, this implies that

\[
S_{13, \frac{1}{13}}(x) \equiv (x - 3) \equiv (x + 10) \pmod{13}.
\]

We square this to obtain

\[
S_{13, \frac{1}{13}}(x)^2 \equiv (x + 10)^2 \equiv (x^2 + 20x + 100) \equiv x^2 + 7x + 9 \pmod{13}.
\]

Using Theorem 1.1 we calculate

\[
(c_{13}^{-1})^2 \cdot x^{\frac{13}{12}} \cdot {}_{3}F_{2}^{1r} \left( \begin{array}{c} \frac{5}{6} \\
1 \\
1 \\
\frac{1}{x}
\end{array} \left| 1 - \frac{1}{x} \right. \right)_{13} \pmod{13}
\]

which gives \((c_{13}^{-1})^2 \equiv \frac{1}{10} \pmod{13}\) and \(x^{\frac{13}{12}} = x^2\). 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 \( S_{13, \frac{1}{13}}(x) \).

Example. We consider \( E_{\frac{1}{17}}(x) \) when \( p = 59 \). By Monks’ theorem, we know that there are four supersingular elliptic curves for \( E_{\frac{1}{17}}(x) \). Those supersingular elliptic curves are found to be \( E_{\frac{1}{17}}(32) \), \( E_{\frac{1}{17}}(35) \), \( E_{\frac{1}{17}}(24) \) and \( E_{\frac{1}{17}}(22) \). To see this we note that \( E_{\frac{1}{17}}(x) \) for \( x = 32, 35, 24 \) and 22 over \( \mathbb{F}_{59} \) have 59 points including the point at infinity. By Monks, this implies that

\[
S_{59, \frac{1}{17}}(x) \equiv (x - 32)(x - 35)(x - 24)(x - 22)
\]

\[
\equiv (x + 27)(x + 24)(x + 35)(x + 37) \pmod{59}.
\]

After squaring this directly, we obtain

\[
S_{59, \frac{1}{17}}(x)^2 \equiv (x + 27)^2(x + 24)^2(x + 35)^2(x + 37)^2 \pmod{59}.
\]

Next using Theorem 1.1 (3) we calculate

\[
(c_{59}^{-1})^2 \cdot x^{\frac{59}{12}} \cdot {}_{3}F_{2}^{1r} \left( \begin{array}{c} \frac{5}{6} \\
1 \\
1 \\
\frac{1}{x}
\end{array} \left| 1 - \frac{1}{x} \right. \right)_{59} \pmod{59}.
\]
For $p = 59$, we have $(c_{59}^{-1})^2 = 15$ and $x^{\frac{59}{11}} = x^9$, so we obtain

$$15 \cdot x^9 \cdot \left( \frac{4}{x} + \frac{40}{x^2} + \frac{3}{x^3} + \frac{16}{x^4} + \frac{38}{x^5} + \frac{56}{x^6} + \frac{16}{x^7} + \frac{28}{x^8} + \frac{36}{x^9} \right)$$

$$\equiv x^8 + 10x^7 + 45x^6 + 4x^5 + 39x^4 + 14x^3 + 4x^2 + 7x + 9 \pmod{59}.$$ 

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 $S_{59, \frac{1}{11}}(x)^2$ as given in (4.1).

References


245 Williams Road, Bryn Mawr, PA 19010

E-mail address: spitman222@gmail.com