Distribution Agreement

In presenting this thesis as a partial fulfillment of the requirements for a degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter now, including display on the World Wide Web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Signature:

______________________________ April 14, 2014

Sarah Christine Pitman Date

$_3F_2$-Hypergeometric Functions and Supersingular Elliptic Curves

By

Sarah Pitman

Ken Ono

Advisor

Department of Mathematics and Computer Science

Ken Ono, Ph.D.

Advisor

Dr. José Luis Boigues

Committee Member

Dr. Vaidy Sunderam

Committee Member

2014

$_3F_2$-Hypergeometric Functions and Supersingular Elliptic Curves

By

Sarah Christine Pitman

Ken Ono, Ph.D.

Advisor

An abstract of

a thesis submitted to the Faculty of Emory College of Arts and Sciences

of Emory University in partial fulfillment

of the requirements for the degree of

Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2014

Abstract

${}_3F_2$-Hypergeometric Functions and Supersingular Elliptic Curves

By Sarah Christine Pitman

Here we explore elliptic curves, specifically supersingular elliptic curves, and their relationship to hypergeometric functions. We begin with some background on elliptic curves, supersingularity, hypergeometric functions, and then use work of El-Guindy, Ono, Kaneko, Zagier, and Monks to extend results. 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.

${}_3F_2$-Hypergeometric Functions and Supersingular Elliptic Curves

By

Sarah Christine Pitman

Ken Ono, Ph.D.
Advisor

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements for the degree of
Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2014

Acknowledgments

First, I would like to express my sincere gratitude to Ken Ono for serving as my advisor and mentor for the past four years. Second, I would like to thank the Emory Department of Mathematics and Computer Science and the NSF Emory REU grant for their generous support. I would like to thank all of the people who have inspired me and mentored me along the way: Jennifer Bryson, Michael Griffin, Marie Jameson, Robert Lemke Oliver, Larry Rolen, Robert Schneider, and Mckenzie West. Finally, I would like to express my appreciation to my thesis committee members Dr. José Luis Boigues and Dr. Vaidy Sunderam.

Contents

List of Figures

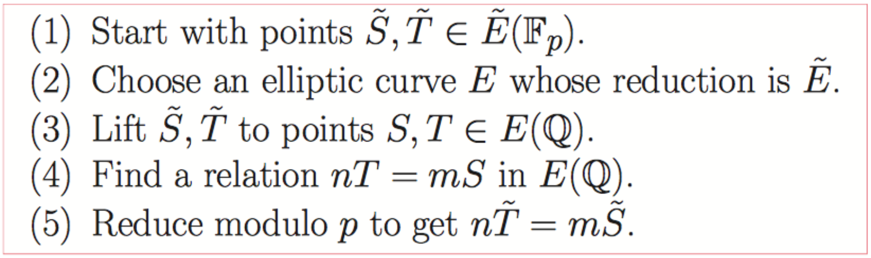
1. Background: Introduction and statement of results

1.1. **Elliptic curves.** Elliptic curves play a major role not just in theoretical mathematics and number theory, but also in a more concrete and practical application: cryptography. Typically, public key cryptographic algorithms, called RSA (named for its developers) and Diffie-Hellman, have been the methods used to protect and secure data. However in recent decades, new techniques have been developed which are not only more secure, but also more efficient. These new methods are based on the arithmetic of elliptic curves. The advanced level of security and the computational efficiency of these elliptic curve cryptosystems is almost essential in today's world with the recent advances in the Internet and technology. For security purposes, the National Security Agency has moved towards elliptic curve-based cryptography, which essentially uses elliptic curves defined over finite fields with large prime moduli. Other governments and nations throughout the world have also made this change. In the next few years, it appears as though many vendors will be upgrading their systems because of the added security and computational bandwidth advantages that these elliptic curve cryptosystems offer. For instance, the RSA cryptographic method uses a key system of size 4096 bits, while an elliptic curve key system, offering the same level of security, requires just 313 bits. In terms of efficiency, it was measured to take 3.4 minutes to generate a 512-bit RSA key, compared to only 0.597 seconds for a 163-bit ECC-DSA (Elliptic Curve Cryptography-Digital Signature Algorithm) key [**?**].

The arithmetic of elliptic curves offer ways to construct ciphers, not just for espionage, but also for telecommunication and finance purposes. This cipher construction begins with two arbitrary large primes (hundreds of digits), call them p and q. The product $N = pq$ is calculated and published. In order to encipher (encode) a message, only the value of N is needed, but to decipher (decode) a message, the specific factors p and q are needed. In simple terms, the larger the primes p and q chosen, the larger the product N, and the longer it will take for a potential enemy to factor N into p and q and break the code. Factoring a large composite number N can be tricky and take a while. It would be very inefficient to start with small integer divisors and test all of the possibilities, so techniques have been developed using algorithms in number theory to facilitate this.

One of the ways to decipher codes in cryptography, is to solve what is called the Elliptic Curve Discrete Logarithm Problem (ECDLP). One of the more efficient methods to do so is called Lenstra's Elliptic Curve Algorithm, which relies on elliptic curves. For general elliptic curves, another fast way to solve such problems is using Pollard's ρ Method, which runs through random multiples $mS + nT$ until a "collision", or solution point, is found that satisfies the conditions. The benefit of this is that it only requires a small amount of storage space and a minimum number of steps to find such a point. The difficulty in solving such a problem comes from the fact that for some elliptic curves, E, it is easy to solve for such S and T, but S and T are almost always independent, while for other elliptic curves, S and T are dependent, but are difficult to find. In Figure 1 [**?**] below, we see the basic outline of the steps for solving ECDLP with regards to an elliptic curve E.

Figure 1. Solving ECDLP [**?**]



(1) Start with points $\tilde{S}, \tilde{T} \in \tilde{E}(\mathbb{F}_p)$.
(2) Choose an elliptic curve E whose reduction is $\tilde{E}$.
(3) Lift $\tilde{S}, \tilde{T}$ to points $S, T \in E(\mathbb{Q})$.
(4) Find a relation $nT = mS$ in $E(\mathbb{Q})$.
(5) Reduce modulo p to get $n\tilde{T} = m\tilde{S}$.

Lenstra's Elliptic Curve Algorithm differs from Pollard's method in that Pollard's method only works, in a practical sense, if one of the prime divisors of N satisfies

$$p - 1 = product\,of\,small\,primes\,to\,small\,powers.$$

There are many other algorithms using elliptic curves that have been tested and found to be very useful and practical in cryptographic systems and ciphers, and much more research has been done and many advancements made. To begin to understand this theory, we begin with the definition of an elliptic curve.

An *elliptic curve*, E, is a smooth, projective curve of genus 1 with a distinguished base point, and when defined over a field K, this point is K-rational. Therefore, we note that not every smooth projective curve of genus 1 is an elliptic curve; it must have at least one rational point.

Elliptic curves are usually expressed by their Weierstrass equations, in either a short form or a long form. The general Weierstrass equation that holds in any field is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

where $a_1, a_2, ..., a_6 \in K$. We define the *characteristic of a field* K, char(K), to be the smallest number m such that m times the identity element of K is zero. In the cases where char$(K) \neq 2, 3$, we can simplify, and after some manipulation obtain a "short" form of the Weierstrass equation. Let $A, B \in K$ with $4A^3 + 27B^2 \neq 0$. The short form of the Weierstrass equation is

$$E : y^2 = x^3 + Ax + B,$$

where the rational base point is (0, 1, 0). It is a fact that every elliptic curve over K can be defined in this way.

1.2. **Points on an elliptic curve form an Abelian group (over $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$).** Take E to be an elliptic curve over a field K defined by a given Weierstrass equation. Let P and Q be two rational points on E. Then by Bezout's theorem, the line $\overline{PQ}$ intersects E at a third rational point, R. From this, we are able to generate new rational points on E.

We can define a group operation on $E(K)$ for any elliptic curve defined over a field K given by addition of these rational points, i.e. $P + Q = R$. The identity element of this group is the point (0, 1, 0) at infinity, and the inverse of $P = (x, y, z)$ is the point $-P = (x, -y, z)$. We can see that the property of commutativity follows: $P + Q = Q + P$, and associativity will hold as well: $P + (Q + R) = (P + Q) + R$. It is also true in general that

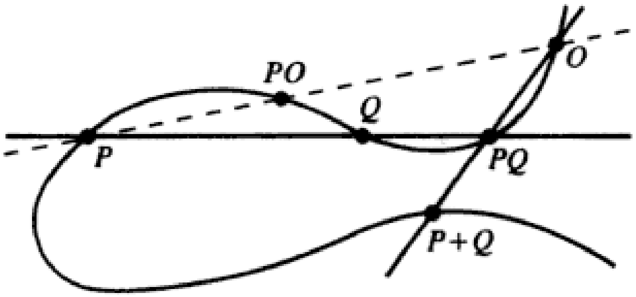
$$nP = P + \cdots + P,$$

where P is added together n times for any positive n, $0P = 0$ and $(-n)P = -nP$. Thus scalar multiplication holds in this group for any integer n.

More explicitly, let two points on E be given by $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$. Define

$$P + Q = R = (x_3, y_3, z_3).$$

Figure 2. Chord-tangent law [?]



Note that if either P or Q is the point at infinity, $(x_k, y_k, 0)$, then R is simply equal to the other point. We can therefore assume that P and Q are structurally affine, meaning that the linear combination or sum of the two is 1, i.e. $z_1 + z_2 = z_3 = 1$.

In the case $x_1 \neq x_2$, we can construct the line $\overline{PQ}$ which has slope

$$m = \frac{(y_2 - y_1)}{(x_2 - x_1)},$$

and gives the equation, $y = m(x - x_1) + y_1$. To obtain the coordinates of R, we see that the point $-R$ is on the line $\overline{PQ}$, $-R = (x_3, y_3, 1)$. We substitute this point into the equation, solve for y_3, then substitute that into the Weierstrass equation for E: $y_3^2 = x_3^3 + Ax_3 + B$ to obtain

$$0 = x_3^3 - m^2x_3^2 + \cdots .$$

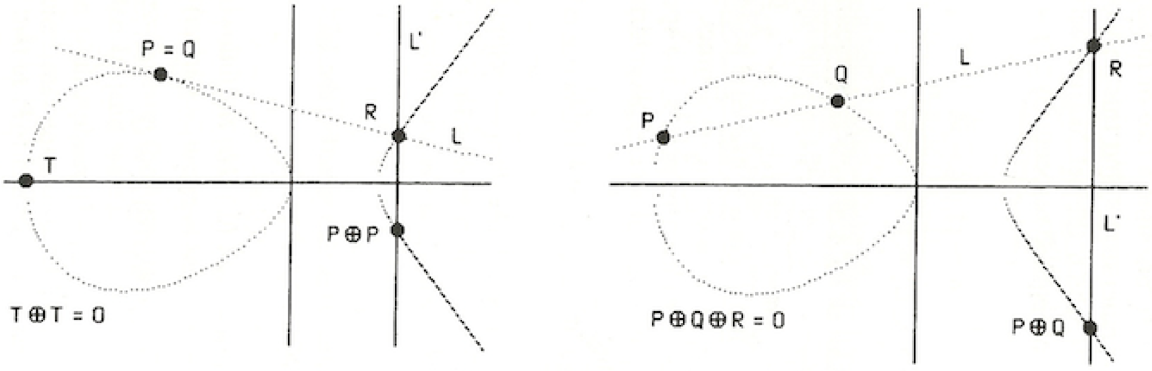
We see that x_1 and x_2 will satisfy this same cubic equation. Therefore the roots of this cubic are x_1, x_2, x_3.

In the case $x_1 = x_2$, if $y_1 \neq y_2$, then P and Q must be opposite points and $R = 0$. If $y_1 = y_2$, then $P = Q$ and $R = 2P$.

In Figure 3 [?], this group law for elliptic curves is illustrated.

Examining this group law, first we will look at the case of a finite field F_p. The group $E(F_p)$ is finite, with order $p + 1$. The following is well-known:

Figure 3. Group law [?]



Proposition 1.1. *When working over a finite field, the group of points $E(\mathbb{F}_p)$ is either a cyclic group or the product of two cyclic groups.*

Next we look at the case for the field of all real numbers, $\mathbb{R}$, i.e. $K = \mathbb{R}$. Here we have the following analogous relationship:

Proposition 1.2. *Either $E(\mathbb{R})$ is isomorphic to S^1, $E(\mathbb{R}) \cong S^1$, where S^1 denotes the circle group, or $E(\mathbb{R})$ is isomorphic to two copies of the circle group $(S^1 \times C_2)$, i.e.*

$$E(\mathbb{R}) \cong (S^1 \times C_2) \cdot (S^1 \times C_2).$$

Finally we investigate $K = \mathbb{C}$. Here, $E(\mathbb{C})$ forms a torus, and we have that

Proposition 1.3. *For all $N \geq 1$,*

$$E(\mathbb{C})_N \cong C_N \times C_N,$$

where C_N denotes a cyclic groups of order N.

1.3. **My work.** Elliptic curves play an important role in all areas of math. For example, the famous Fermat's Last Theorem depends on the deep (and recently proved) fact that all elliptic curves are modular. This means that the L-function for $E(\mathbb{Q})$ is the L-function of a modular form given by

$$f = \sum a(n)q^n,$$

where $q = e^{2\pi iz}$. The *L-function* for an elliptic curve is defined to be the product

$$L(E,s) = \prod_p (1 - a(p)p^{-s} + p^{1-2s})^{-1},$$

for all primes p for which

$$E : y^2 = x^3 + Ax^2 + Bx + C \not\equiv 0 \pmod p,$$

where A, B, and C are fixed, and

$$a(p) = p - \{\text{number of solutions over } F_p \text{ to } y^2 = x^3 + Ax^2 + Bx + C \pmod p\}.$$

Over F_p, there are only finitely many elliptic curves, and we choose the coefficients from 0 to $p-1$. Most of these curves have the property that $a(p) \neq 0$. It turns out that the curves for which $a(p) = 0$, up to isomorphism, are special and are called *supersingular*. Each elliptic curve, up to isomorphism, is distinguished by its j-invariant, $j(E) \in F$. If E is given by (**??**), then j is a rational function of the coefficients. When the characteristic of F is not 2 or 3, and E is given by the simpler Weierstrass equation,

$$y^2 = x^3 + Ax + B, \Delta := 4A^3 + 27B^3 \neq 0,$$

we have the expression

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^3}.$$

In this paper, we compute polynomials whose roots are the j-values of these supersingular elliptic curves, among the Legendre and Clausen families. In his paper [**?**], Monks shows that these j-values are indeed the roots of ${}_2F_1$-hypergeometric polynomials. These polynomials can then be described as analogous ${}_3F_2$-hypergeometric polynomials, which follow the transformations outlined in this paper.

1.4. **Hypergeometric functions.** 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 $\alpha_1, ..., \alpha_h, \beta_1, ..., \beta_j \in \mathbb{C}$ is defined by

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

We are interested in the hypergeometric functions

$$(1.2)\qquad {}_2F_1^{\text{cl}}\left(\begin{matrix} a & b \\ & c \end{matrix}\,\middle|\, x\right) := \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n} \cdot \frac{x^n}{n!}$$

and

$$(1.3)\qquad {}_3F_2^{\text{cl}}\left(\begin{matrix} a & b & d \\ & c & e \end{matrix}\,\middle|\, x\right) := \sum_{n=0}^{\infty} \frac{(a)_n(b)_n(d)_n}{(c)_n(e)_n} \cdot \frac{x^n}{n!},$$

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

$$(1.4)\qquad {}_2F_1^{\text{tr}}\left(\begin{matrix} a & b \\ & c \end{matrix}\,\middle|\, x\right)_p \equiv \sum_{n=0}^{\frac{p-1}{2}} \frac{(a)_n(b)_n}{(c)_n} \cdot \frac{x^n}{n!} \pmod{p}$$

and

$$(1.5)\qquad {}_3F_2^{\text{tr}}\left(\begin{matrix} a & b & d \\ & c & e \end{matrix}\,\middle|\, x\right)_p \equiv \sum_{n=0}^{\frac{p-1}{2}} \frac{(a)_n(b)_n(d)_n}{(c)_n(e)_n} \cdot \frac{x^n}{n!} \pmod{p}.$$

Monks 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 [**?**] tr implies truncation after x^{p-1}. We will see that the relevant polynomials agree when reduced modulo p.

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

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

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

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

These polynomials have coefficients in $\mathbb{F}_p$. In [**?**], El-Guindy and Ono study other families of elliptic curves. In his paper [**?**], 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 1.4. *The following are true:*

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

$$S_{p,\frac{1}{4}}(x)^2 \equiv (x+1)^{\frac{p-1}{2}} \cdot {}_3F_2^{\text{tr}} \left(\begin{array}{ccc|c} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{x}{x+1} \\ & 1 & 1 & \end{array} \right)_p \pmod{p}.$$

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

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

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

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

Here $c_p = \binom{6\lfloor \frac{p}{12} \rfloor + d_p}{\lfloor \frac{p}{12} \rfloor}$ *and* $d_p = 0, 2, 2, 4$ *for* $p \equiv 1, 5, 7, 11 \pmod{12}$ *respectively.*

The proof of Theorem **??** shall rely on recent work of El-Guindy and Ono and Monks. The following are formulas given on pages 2 and 3 of [**?**].

Theorem 1.5 (Monks in [**?**])**.** *The following are true:*

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

$$S_{p,\frac{1}{4}}(x) \equiv {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix} \,\middle|\, -x\right)_p \pmod{p}. \tag{1.6}$$

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

$$S_{p,\frac{1}{3}}(x) \equiv x^{\lfloor \frac{p}{3} \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \,\middle|\, \frac{27}{x}\right)_p \pmod{p}. \tag{1.7}$$

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

$$S_{p,\frac{1}{12}}(x) \equiv c_p^{-1} \cdot x^{\lfloor \frac{p}{12} \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)_p \pmod{p}. \tag{1.8}$$

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

$$S_{p,\frac{1}{12}}(x) \equiv c_p^{-1} \cdot x^{\lfloor \frac{p}{12} \rfloor} \cdot {}_2F_1^{\mathrm{tr}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)_p \pmod{p}, \tag{1.9}$$

where $c_p = \binom{6\lfloor \frac{p}{12} \rfloor + d_p}{\lfloor \frac{p}{12} \rfloor}$ *and* $d_p = 0, 2, 2, 4$ *for* $p \equiv 1, 5, 7, 11 \pmod{12}$ *respectively.*

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

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

2. Supersingular elliptic curves

In this section we define *supersingularity* of elliptic curves and delve deeper into the theory examining works of Kaneko, Zagier, and Monks.

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

First we recall the statement and proof for deciding whether or not a given curve over a finite field $\mathbb{F}_q$, $q = p^r$, p odd, is supersingular or not.

Proposition 2.1. *Let E be the elliptic curve over $\mathbb{F}_q$ defined by the equation $y^2 = f(x)$, ($f \in \mathbb{F}_q[x]$ of degree 3), and a_p the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$. Then $|E(\mathbb{F}_q)| \equiv 1 - N_{\mathbb{F}_q/\mathbb{F}_p} a_p \pmod{p}$.*

Corollary 2.2. *E is supersingular if and only if $a_p = 0$.*

Proof. The number of solutions for $x \in \mathbb{F}_q$ where $y^2 = f(x)$ is $1 + f(x)^{(q-1)/2}$. When we also include the point at infinity, we find that

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + f(x)^{\frac{q-1}{2}})$$

in $\mathbb{F}_q$. We know that the sum over $x \in \mathbb{F}_q$ of x^t is -1 for $t = q - 1$ and is 0 for all other t in $0 \leq t \leq 3(q-1)/2$, we have

$$|E(\mathbb{F}_q)| = 1 - a_q$$

in $\mathbb{F}_q$, where a_q represents the coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$ (note. a_q will belong to both $\mathbb{F}_p$ and $\mathbb{F}_q$). From the expansion of $f(x)^{\frac{q-1}{2}}$, we have

$$f(x)^{\frac{q-1}{2}} = f(x)^{\frac{p-1}{2}(1+p+\cdots+p^{r-1})} = f(x)^{\frac{p-1}{2}} f^{(p)}(x^p)^{\frac{p-1}{2}} \cdots f^{(p^{r-1})}(x^{p^{r-1}})^{\frac{p-1}{2}},$$

where $f^{(p^t)}$ is precisely the polynomial that is obtained from f after raising all of its coefficients to the power p^t. We now can see that $a_q = a_p^{(1+p+\cdots+p^{r-1})} = N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)$, which proves the proposition. For the corollary, we note that if $a_p = 0$, then $|E(\mathbb{F}_{q^n})| \equiv 1 \equiv 0 \pmod{p}$ for all n, meaning E has no p-torsion over $\overline{\mathbb{F}}_p$. If $a_p \neq 0$, then $|E(\mathbb{F}_{q^n})| \equiv 1 - (N_{\mathbb{F}_q/\mathbb{F}_p} a_p)^n$ will be divisible by p for any n that is divisible by $|N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)|$ modulo p, and thus $E(\overline{\mathbb{F}}_p)$ does contain p-torsion. □

2.2. **Supersingular locus over $\mathbb{F}_p$.** In their paper [?], Kaneko and Zagier look at E_k, the normalized Eisenstein series of weight k, specifically in the case where $k = p-1$ for a prime $p \geq 5$. They describe the modular forms E_k of weight $k = p-1$ corresponding to the polynomial in j, multiplied by $j^\delta (j-1728)^\epsilon$, and show that these reduce modulo p to the supersingular polynomial. Part of Theorem 1 in [?] states that:

Theorem 2.3. *For $k = p-1$, where $p \geq 5$ is prime and f represents any of the modular forms (in our case E_k), then the coefficients of the associated polynomial $\tilde{f}$ are p-integral and*

$$ss_p(j) \equiv \pm j^\delta (j-1728)^\epsilon \tilde{f}(j) \pmod{p}.$$

The explicit proof of this theorem is outlined in their paper, and after basic substitution we describe our specific case as

$$ss_p(j) \equiv \pm j^\delta (j-1728)^\epsilon \tilde{E}_{p-1}(j) \pmod{p}.$$

2.3. **Work of Monks.** Here we consider supersingular elliptic curves in certain families. We recall the Legendre Family of elliptic curves is the Legendre Family, denoted by

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

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

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

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

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

$$E_{\frac{1}{4}}(\lambda) : y^2 = (x-1)(x^2+\lambda). \tag{2.1}$$

We also consider the following families of elliptic curves:

$$E_{\frac{1}{3}}(\lambda) : y^2 + \lambda yx + \lambda^2 y = x^3 \tag{2.2}$$

$$E_{\frac{1}{12}}(\lambda) : y^2 = 4x^3 - 27\lambda x - 27\lambda. \tag{2.3}$$

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

$$S_{p,i}(\lambda) := \prod_{\substack{\lambda_0 \in \overline{\mathbb{F}}_p \\ \text{supersingular } E_i(\lambda_0)}} (\lambda - \lambda_0). \tag{2.4}$$

For ease of reference, we again give the formulas on pages 2 and 3 of [?].

Theorem 2.4 (Monks in [?])**.** *The following are true:*

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

$$S_{p,\frac{1}{4}}(x) \equiv {}_2F_1^{\text{tr}} \left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix} \;\middle|\; -x \right)_p \pmod{p}. \tag{2.5}$$

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

$$S_{p,\frac{1}{3}}(x) \equiv x^{\lfloor \frac{p}{3} \rfloor} \cdot {}_2F_1^{\text{tr}} \left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \;\middle|\; \frac{27}{x} \right)_p \pmod{p}. \tag{2.6}$$

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

$$S_{p,\frac{1}{12}}(x) \equiv c_p^{-1} \cdot x^{\lfloor \frac{p}{12} \rfloor} \cdot {}_2F_1^{\mathrm{tr}} \left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \middle| \, 1 - \frac{1}{x} \right)_p \pmod{p}. \tag{2.7}$$

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

$$S_{p,\frac{1}{12}}(x) \equiv c_p^{-1} \cdot x^{\lfloor \frac{p}{12} \rfloor} \cdot {}_2F_1^{\mathrm{tr}} \left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \middle| \, 1 - \frac{1}{x} \right)_p \pmod{p}, \tag{2.8}$$

where $c_p = \binom{6\,\lfloor \frac{p}{12} \rfloor + d_p}{\lfloor \frac{p}{12} \rfloor}$ and $d_p = 0, 2, 2, 4$ for $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively.

By 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 **??**.

3. Outline of proof of Theorem and tools

Now we recall our main theorem:

Theorem 3.1. *The following are true:*

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

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

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

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

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

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

Here $c_p = \binom{6\,\lfloor \frac{p}{12} \rfloor + d_p}{\lfloor \frac{p}{12} \rfloor}$ and $d_p = 0, 2, 2, 4$ for $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively.

3.1. **Statement of Clausen's Theorem and Transformation Laws.** Our main tools for establishing these congruences are a theorem of Clausen and two classical ${}_2F_1$ transformation laws. We make use of the a theorem of Clausen [**?**] which gives the following equality of hypergeometric polynomials:

$$(3.1)\qquad {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}2\alpha & 2\beta & \alpha+\beta \\ & 2\alpha+2\beta & \alpha+\beta+\frac{1}{2}\end{matrix}\,\middle|\, x\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\alpha & \beta \\ & \alpha+\beta+\frac{1}{2}\end{matrix}\,\middle|\, x\right)^2.$$

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

$$(3.2)\qquad {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}a & b \\ & c\end{matrix}\,\middle|\, x\right) = (1-x)^{-a}\cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}a & c-b \\ & c\end{matrix}\,\middle|\, \frac{x}{x-1}\right).$$

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

$$(3.3)\qquad {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}a & b \\ & \frac{a+b+1}{2}\end{matrix}\,\middle|\, x\right) = {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{a}{2} & \frac{b}{2} \\ & \frac{a+b+1}{2}\end{matrix}\,\middle|\, 4x(1-x)\right).$$

3.2. **Elementary Reduction modulo** p**.** Here we briefly outline the reduction modulo p that we will use, showing how it works in the proof of the second case of Theorem **??**. By definition (**??**) we have that

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

For $n > \lfloor\frac{p}{3}\rfloor$, 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

$$(3.4)\quad {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\, \frac{108x-2916}{x^2}\right)_p \equiv \sum_{n=0}^{\lfloor\frac{p}{3}\rfloor} \frac{(\frac{1}{3})_n(\frac{2}{3})_n(\frac{1}{2})_n}{(n!)^3}\cdot\frac{(108x-2916)^n}{x^{2n}} \pmod{p}.$$

Similarly by (**??**) we have that

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

For any $n > \lfloor\frac{p}{6}\rfloor$, $p \equiv 1, 5 \pmod 6$ 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

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1\end{matrix}\;\middle|\; 1-\frac{1}{x}\right)_p \equiv \sum_{n=0}^{\lfloor\frac{p}{6}\rfloor} \frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3}\cdot\left(1-\frac{1}{x}\right)^n \pmod{p}. \tag{3.5} $$

4. Proof of Theorem ??

To prove Theorem **??**, we show the first part using the results of El-Guindy and Ono in [**?**]. 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 (**??**), 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 4.1. *The following are true:*

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

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

(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 $p \equiv 1, 5 \pmod{12}$, then*

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

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

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

Proof. For the proof of (1), we observe that

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix}\,\middle|\, -x\right) $$

is not of the form

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

Therefore we must apply a transformation law for ${}_2F_1$-hypergeometric functions in order to use Clausen's theorem. Classically, we have the transformation of Bailey [**?**]

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

We use this to alter

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix}\,\middle|\, -x\right), $$

so that we can then apply Clausen's Theorem and obtain a ${}_3F_2$-hypergeometric series. We let $a = \frac{1}{4}$, $b = \frac{1}{4}$, $c = 1$, and $\dfrac{x}{x-1} = -x$, and obtain

$$ (x+1)^{-\frac{1}{4}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{4} & \frac{1}{4} \\ & 1 \end{matrix}\,\middle|\, \frac{x}{x+1}\right). $$

We have transformed

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix}\,\middle|\, -x\right) $$

into

$$ (x+1)^{-\frac{1}{4}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{4} & \frac{1}{4} \\ & 1 \end{matrix}\,\middle|\, \frac{x}{x+1}\right). $$

This hypergeometric function is now of the correct form to apply Clausen's Theorem, so we let $\alpha = \frac{1}{4}$, $\beta = \frac{1}{4}$, $\alpha + \beta + \frac{1}{2} = 1$, and $x = \dfrac{x}{x+1}$. Therefore we have

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{1}{4} \\ & 1\end{matrix}\,\middle|\,\frac{x}{x+1}\right)^2 = {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\,\frac{x}{x+1}\right). $$

Our transformation is used as follows:

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix}\,\middle|\,-x\right) = (x+1)^{-\frac{1}{4}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{1}{4} \\ & 1\end{matrix}\,\middle|\,\frac{x}{x+1}\right). $$

We square both sides to obtain

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix}\,\middle|\,-x\right)^2 = (x+1)^{-\frac{1}{2}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{1}{4} \\ & 1\end{matrix}\,\middle|\,\frac{x}{x+1}\right)^2, $$

and after substitution we have

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix}\,\middle|\,-x\right)^2 = (x+1)^{-\frac{1}{2}} \cdot {}_3F_2^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1\end{matrix}\,\middle|\,\frac{x}{x+1}\right), \tag{4.1} $$

which is what we want. By definition (**??**) when we expand the infinite hypergeometric series on the left hand side of this equation, we obtain

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & 1\end{matrix}\,\middle|\,-x\right)^2 = \left(\sum_{N=0}^{\infty} \frac{(\frac{1}{4})_N(\frac{3}{4})_N}{(N!)^2} \cdot (-x)^N\right)^2, $$

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

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

By (**??**) we have that these two infinite series expansions are equal, so

$$ \left(\sum_{N=0}^{\infty} \frac{(\frac{1}{4})_N(\frac{3}{4})_N}{(N!)^2} \cdot (-x)^N\right)^2 = \sum_{N=0}^{\infty} \frac{(\frac{1}{2})_N(\frac{1}{2})_N(\frac{1}{2})_N}{(N!)^3} \cdot \left(\frac{x}{x+1}\right)^N. \tag{4.2} $$

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

$$a(N) = \sum_{n=0}^{N} \frac{(\frac{1}{4})_n(\frac{3}{4})_n}{(n!)^2} \cdot \frac{(\frac{1}{4})_{N-n}(\frac{3}{4})_{N-n}}{((N-n)!)^2},$$

and by the Binomial Theorem

$$b(N) = \sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{2})_n(\frac{1}{2})_n(\frac{1}{2})_n}{(n!)^3} \cdot (-1)^{N-n}.$$

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 (**??**) 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

$$\sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{1}{4})_n(\frac{3}{4})_n}{(n!)^2} \cdot \frac{(\frac{1}{4})_{N-n}(\frac{3}{4})_{N-n}}{((N-n)!)^2} \cdot x^N \\ = \sum_{N=0}^{p-1}\sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{2})_n(\frac{1}{2})_n(\frac{1}{2})_n}{(n!)^3} \cdot (-1)^{N-n} \cdot x^N. \tag{4.3}$$

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 (**??**) 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

$$\sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{1}{4})_n(\frac{3}{4})_n}{(n!)^2} \cdot \frac{(\frac{1}{4})_{N-n}(\frac{3}{4})_{N-n}}{((N-n)!)^2} \equiv \left(\sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{4})_N(\frac{3}{4})_N}{(N!)^2} \right)^2 \pmod{p} \tag{4.4}$$

and

$$\sum_{N=0}^{p-1}\sum_{n=\lceil \frac{N}{2}\rceil}^{N}\frac{(\frac{1}{2})_n(\frac{1}{2})_n(\frac{1}{2})_n}{(n!)^3}\cdot(-1)^{N-n}$$

$$\equiv\sum_{N=0}^{\frac{p-1}{2}}\frac{(\frac{1}{2})_N(\frac{1}{2})_N(\frac{1}{2})_N}{(N!)^3}\cdot(-1)^N \pmod{p}. \tag{4.5}$$

Finally we see that the right hand sides of (**??**) and (**??**) 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:

$${}_2F_1^{\text{tr}}\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ & 1\end{matrix}\;\middle|\; -x\right)_p^2 \equiv \left(\sum_{N=0}^{\frac{p-1}{2}}\frac{(\frac{1}{4})_N(\frac{3}{4})_N}{(N!)^2}\cdot(x)^N\right)^2 \pmod{p}$$

and

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

It follows that

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

which completes the proof.

For the proof of (2), we apply the transformation law for ${}_2F_1$-hypergeometric functions given by (**??**) where $a=\frac{1}{3}$, $b=\frac{2}{3}$, and $x=\dfrac{27}{x}$, and see that

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

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

$$\text{(4.6)}\qquad {}_2F_1^{\text{cl}}\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix}\,\middle|\, \frac{27}{x}\right)^2 = {}_2F_1^{\text{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{1}{3} \\ & 1 \end{matrix}\,\middle|\, \frac{108x - 2916}{x^2}\right)^2$$

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

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

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

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

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

By (**??**) we have that these two infinite series expansions are equal

$$\text{(4.7)}\qquad \left(\sum_{N=0}^{\infty} \frac{(\frac{1}{3})_N(\frac{2}{3})_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N\right)^2 = \sum_{N=0}^{\infty} \frac{(\frac{1}{3})_N(\frac{2}{3})_N(\frac{1}{2})_N}{(N!)^3} \cdot \left(\frac{108x - 2916}{x^2}\right)^N.$$

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

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

and by the Binomial Theorem

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

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 (**??**) 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

$$\sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{1}{3})_n(\frac{2}{3})_n}{(n!)^2} \cdot \frac{(\frac{1}{3})_{N-n}(\frac{2}{3})_{N-n}}{((N-n)!)^2} \cdot 27^N \cdot x^{-N}$$

$$= \sum_{N=0}^{p-1} \sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{3})_n(\frac{2}{3})_n(\frac{1}{2})_n}{(n!)^3} \cdot \binom{n}{2n-N}(108)^{2n-N}(-2916)^{N-n} \cdot x^{-N}. \tag{4.8}$$

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 (**??**) 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

$$\sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{1}{3})_n(\frac{2}{3})_n}{(n!)^2} \cdot \frac{(\frac{1}{3})_{N-n}(\frac{2}{3})_{N-n}}{((N-n)!)^2} \cdot \left(\frac{27}{x}\right)^N \equiv \left(\sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{3})_N(\frac{2}{3})_N}{(N!)^2} \cdot \left(\frac{27}{x}\right)^N\right)^2 \pmod p \tag{4.9}$$

and

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

$$\equiv \sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{3})_N(\frac{2}{3})_N(\frac{1}{2})_N}{(N!)^3} \cdot \left(\frac{108x-2916}{x^2}\right)^N \pmod p. \tag{4.10}$$

Finally we see that the right hand sides of (**??**) and (**??**) 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:

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

and

$$ {}_3F_2^{\mathrm{tr}}\left(\begin{array}{ccc|c} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} & \dfrac{108x-2916}{x^2} \\ & 1 & 1 & \end{array}\right)_p \equiv \sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{3})_N(\frac{2}{3})_N(\frac{1}{2})_N}{(N!)^3}\cdot\left(\frac{108x-2916}{x^2}\right)^N \quad (\text{mod } p). $$

It follows that

$$ {}_2F_1^{\mathrm{tr}}\left(\begin{array}{cc|c} \frac{1}{3} & \frac{2}{3} & \dfrac{27}{x} \\ & 1 & \end{array}\right)_p^2 \equiv {}_3F_2^{\mathrm{tr}}\left(\begin{array}{ccc|c} \frac{1}{3} & \frac{2}{3} & \frac{1}{2} & \dfrac{108x-2916}{x^2} \\ & 1 & 1 & \end{array}\right)_p \quad (\text{mod } p), $$

which completes the proof.

For the proof of (3), we observe that

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{array}{cc|c} \frac{1}{12} & \frac{5}{12} & 1-\dfrac{1}{x} \\ & 1 & \end{array}\right) $$

is of the form

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{array}{cc|c} \alpha & \beta & x \\ & \alpha+\beta+\frac{1}{2} & \end{array}\right). $$

We apply Clausen's Theorem directly, and we let $\alpha = \frac{1}{12}$, $\beta = \frac{5}{12}$, $\alpha+\beta+\frac{1}{2} = 1$, and $x = 1-\frac{1}{x}$. Therefore we have

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{array}{cc|c} \frac{1}{12} & \frac{5}{12} & 1-\dfrac{1}{x} \\ & 1 & \end{array}\right)^2 = {}_3F_2^{\mathrm{cl}}\left(\begin{array}{ccc|c} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} & 1-\dfrac{1}{x} \\ & 1 & 1 & \end{array}\right). \tag{4.11} $$

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

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{array}{cc|c} \frac{1}{12} & \frac{5}{12} & 1-\dfrac{1}{x} \\ & 1 & \end{array}\right)^2 = \left(\sum_{N=0}^{\infty} \frac{(\frac{1}{12})_N(\frac{5}{12})_N}{(N!)^2}\cdot\left(1-\frac{1}{x}\right)^N\right)^2, $$

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

$$ {}_3F_2^{\mathrm{cl}}\left(\begin{array}{ccc|c} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} & 1-\dfrac{1}{x} \\ & 1 & 1 & \end{array}\right) = \sum_{N=0}^{\infty} \frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3}\cdot\left(1-\frac{1}{x}\right)^N. $$

By (**??**) we have that these two infinite series expansions are equal, so

$$\left(\sum_{N=0}^{\infty}\frac{(\frac{1}{12})_N(\frac{5}{12})_N}{(N!)^2}\cdot\left(1-\frac{1}{x}\right)^N\right)^2=\sum_{N=0}^{\infty}\frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3}\cdot\left(1-\frac{1}{x}\right)^N. \tag{4.12}$$

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

$$a(N)=\sum_{n=0}^{N}\frac{(\frac{1}{12})_n(\frac{5}{12})_n}{(n!)^2}\cdot\frac{(\frac{1}{12})_{N-n}(\frac{5}{12})_{N-n}}{((N-n)!)^2}\cdot\binom{N}{n}\cdot(-1)^{N-n},$$

and by the Binomial Theorem

$$b(N)=\sum_{n=0}^{N}\frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3}\cdot\binom{N}{n}\cdot(-1)^{N-n}.$$

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 (**??**) 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

$$\begin{aligned}&\sum_{N=0}^{p-1}\sum_{n=0}^{N}\frac{(\frac{1}{12})_n(\frac{5}{12})_n}{(n!)^2}\cdot\frac{(\frac{1}{12})_{N-n}(\frac{5}{12})_{N-n}}{((N-n)!)^2}\cdot\binom{N}{n}\cdot(-1)^{N-n}\cdot x^N\\ &\qquad=\sum_{N=0}^{p-1}\sum_{n=\lceil\frac{N}{2}\rceil}^{N}\frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3}\cdot(-1)^{N-n}\cdot\binom{N}{n}\cdot(-1)^{N-n}\cdot x^N.\end{aligned} \tag{4.13}$$

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 (**??**) 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

$$\sum_{N=0}^{p-1}\sum_{n=0}^{N}\frac{(\frac{1}{12})_n(\frac{5}{12})_n}{(n!)^2}\cdot\frac{(\frac{1}{12})_{N-n}(\frac{5}{12})_{N-n}}{((N-n)!)^2}\equiv\left(\sum_{N=0}^{\frac{p-1}{2}}\frac{(\frac{1}{12})_N(\frac{5}{12})_N}{(N!)^2}\right)^2\pmod p \tag{4.14}$$

and

$$\sum_{N=0}^{p-1}\sum_{n=\lceil\frac{N}{2}\rceil}^{N}\frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3}\cdot\binom{N}{n}\cdot(-1)^{N-n}$$

$$\equiv\sum_{N=0}^{\frac{p-1}{2}}\frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3}\cdot\binom{N}{n}\cdot(-1)^N \pmod{p}. \tag{4.15}$$

Finally we see that the right hand sides of (**??**) and (**??**) 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:

$${}_2F_1^{\mathrm{tr}}\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{x}\right)_p^2 \equiv \left(\sum_{N=0}^{\frac{p-1}{2}}\frac{(\frac{1}{12})_N(\frac{5}{12})_N}{(N!)^2}\cdot(x)^N\right)^2 \pmod{p}$$

and

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

It follows that

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

which completes the proof.

Finally in the proof of (4), we note that

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix}\frac{7}{12} & \frac{11}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{x}\right)$$

is not of the form

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

Therefore we must apply a transformation law for ${}_2F_1$-hypergeometric functions. We use [**??**] so that we can apply Clausen's Theorem to obtain a ${}_3F_2$-hypergeometric series. We now let $a = \frac{7}{12}$, $b = \frac{11}{12}$, $c = 1$, and $x = 1 - \frac{1}{x}$, and obtain

$$\left(\frac{1}{x}\right)^{-\frac{7}{12}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{1}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right),$$

which is equivalent to

$$\left(\frac{1}{x}\right)^{-\frac{7}{12}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{7}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right).$$

We apply the same transformation again with $a = \frac{1}{12}$, $b = \frac{7}{12}$, $c = 1$, and $x = 1 - \frac{1}{x}$, and obtain

$$(x)^{-\frac{1}{12}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right).$$

Putting this together, we have transformed

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)$$

into

$$\left(\frac{1}{x}\right)^{-\frac{7}{12}} \cdot (x)^{-\frac{1}{12}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right).$$

This is now of the correct form to apply Clausen's Theorem, so we let $\alpha = \frac{1}{12}$, $\beta = \frac{5}{12}$, $\alpha + \beta + \frac{1}{2} = 1$, and $x = 1 - \frac{1}{x}$. Therefore we have

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)^2 = {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right).$$

Our transformation is used as follows:

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right) = \left(\frac{1}{x}\right)^{-\frac{7}{12}} \cdot (x)^{-\frac{1}{12}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right).$$

We square both sides to obtain

$${}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)^2 = \left(\frac{1}{x}\right)^{-\frac{14}{12}} \cdot (x)^{-\frac{1}{6}} \cdot {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{x}\right)^2,$$

and after substitution we have

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)^2 = \left(\frac{1}{x}\right)^{-\frac{7}{6}} \cdot (x)^{-\frac{1}{6}} \cdot {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right), $$

which simplifies to

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)^2 = x \cdot {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right), \tag{4.16} $$

which is what we want.

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

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)^2 = \left(\sum_{N=0}^{\infty} \frac{(\frac{7}{12})_N(\frac{11}{12})_N}{(N!)^2} \cdot \left(1-\frac{1}{x}\right)^N\right)^2, \tag{4.17} $$

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

$$ {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right) = \sum_{N=0}^{\infty} \frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3} \cdot x \cdot \left(1-\frac{1}{x}\right)^N. $$

By (**??**) we have that these two infinite series expansions are equal, so

$$ \left(\sum_{N=0}^{\infty} \frac{(\frac{7}{12})_N(\frac{11}{12})_N}{(N!)^2} \cdot \left(1-\frac{1}{x}\right)^N\right)^2 = \sum_{N=0}^{\infty} \frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3} \cdot x \cdot \left(1-\frac{1}{x}\right)^N. $$

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

$$ a(N) = \sum_{n=0}^{N} \frac{(\frac{7}{12})_n(\frac{11}{12})_n}{(n!)^2} \cdot \frac{(\frac{7}{12})_{N-n}(\frac{11}{12})_{N-n}}{((N-n)!)^2} \cdot \binom{N}{n} \cdot (-1)^{N-n}, $$

and by the Binomial Theorem

$$ b(N) = \sum_{n=0}^{N} \frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3} \cdot \binom{N}{n} \cdot (-1)^{N-n}. $$

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 (**??**) 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

$$\begin{aligned}
&\sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{7}{12})_n(\frac{11}{12})_n}{(n!)^2} \cdot \frac{(\frac{7}{12})_{N-n}(\frac{11}{12})_{N-n}}{((N-n)!)^2} \cdot \binom{N}{n} \cdot (-1)^{N-n} \cdot x^N \\
&\qquad = \sum_{N=0}^{p-1}\sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3} \cdot (-1)^{N-n} \cdot \cdot \binom{N}{n} \cdot (-1)^{N-n} \cdot x^N. \qquad (4.18)
\end{aligned}$$

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 (**??**) 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

$$(4.19) \qquad \sum_{N=0}^{p-1}\sum_{n=0}^{N} \frac{(\frac{7}{12})_n(\frac{11}{12})_n}{(n!)^2} \cdot \frac{(\frac{7}{12})_{N-n}(\frac{11}{12})_{N-n}}{((N-n)!)^2} \equiv \left(\sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{7}{12})_N(\frac{11}{12})_N}{(N!)^2} \right)^2 \pmod{p}$$

and

$$\begin{aligned}
&\sum_{N=0}^{p-1}\sum_{n=\lceil \frac{N}{2} \rceil}^{N} \frac{(\frac{1}{6})_n(\frac{5}{6})_n(\frac{1}{2})_n}{(n!)^3} \cdot \binom{N}{n} \cdot (-1)^{N-n} \\
&\qquad \equiv \sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3} \cdot \binom{N}{n} (-1)^N \pmod{p}. \qquad (4.20)
\end{aligned}$$

Finally we see that the right hand sides of (**??**) and (**??**) 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:

$${}_2F_1^{\mathrm{tr}}\left(\begin{array}{cc|c} \frac{7}{12} & \frac{11}{12} & 1 - \dfrac{1}{x} \\ & 1 & \end{array} \right)_p^2 \equiv \left(\sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{7}{12})_N(\frac{11}{12})_N}{(N!)^2} \cdot (x)^N \right)^2 \pmod{p}$$

and

$$ {}_3F_2^{\text{tr}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)_p \equiv \sum_{N=0}^{\frac{p-1}{2}} \frac{(\frac{1}{6})_N(\frac{5}{6})_N(\frac{1}{2})_N}{(N!)^3} \cdot \left(1-\frac{1}{x}\right)^N \pmod{p}. $$

It follows that

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

which completes the proof. □

4.1. **Proof of Theorem ??.** Now we are ready to prove the main theorem.

For the proof of (1), we begin with Lemma **??** (1) which gives

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

Substituting the left hand side of the above congruence into the square of (**??**), 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 $E_{\frac{1}{4}}(\lambda)$.

For the proof of (2), we begin with Lemma **??** (2) which gives

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

Substituting the left hand side of the above congruence into the square of (**??**), we obtain the congruence for the square of the supersingular locus, $S_{p,\frac{1}{3}}(x)^2$, for the family of elliptic curves given by $E_{\frac{1}{3}}(\lambda)$.

The remaining cases use the congruences of the supersingular locus given by Monks. The ${}_2F_1^{\text{tr}}$-hypergeometric functions in (**??**), (**??**), and (**??**) are squared. Squaring (**??**) we obtain

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

After substitution, we have

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

which is an analog of Theorem 2.1 in [**?**]. We note that neither side of this equation is a polynomial, so in order to obtain the congruence to the square of the supersingular locus, we must multiply the truncated forms of these hypergeometric functions by $x^{2\lfloor \frac{p}{3} \rfloor}$. Then using the congruence in (2) of Lemma **??**, we have our result:

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

The third hypergeometric function given by

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right) $$

gives the analog of Theorem 2.1 in [**?**],

$$ {}_2F_1^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right)^2 = {}_3F_2^{\mathrm{cl}}\left(\begin{matrix} \frac{1}{6} & \frac{5}{6} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \,\middle|\, 1-\frac{1}{x}\right), $$

In the third case after squaring (**??**), we obtain

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

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

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

We see in (3) and (4) of Lemma **??** 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 results.

5. Examples

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

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

We square this to obtain

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

Using Theorem **??** we calculate

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

which gives $(c_{13}^{-1})^2 \equiv \frac{1}{10} \pmod{13}$ and $x^{\lfloor \frac{13}{6} \rfloor} = x^2$. 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 $S_{13,\frac{1}{12}}(x)$.

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

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

After squaring this directly, we obtain

$$S_{59,\frac{1}{12}}(x)^2 \equiv (x+27)^2(x+24)^2(x+35)^2(x+37)^2 \pmod{59}. \tag{5.1}$$

Next using Theorem **??** (3) we calculate

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

For $p = 59$, we have $(c_{59}^{-1})^2 = 15$ and $x^{\lfloor \frac{59}{6} \rfloor} = x^9$, 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 $S_{59,\frac{1}{12}}(x)^2$ as given in (**??**).

References

[1] W. Bailey, *Generalized hypergeometric series*, Cambridge Univ. Press, Cambridge, 1998.

[2] A. El-Guindy and K. Ono, *Hasse invariants for the Clausen elliptic curves*, Ramanujan Journal. **31** (2013), 3-13.

[3] D. Husemöller, *Elliptic Curves*, Springer-Verlag New York, Inc., New York, NY, 2004.

[4] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Proc. of the Conference on Computational Aspects of Number Theory. AMS/IP Studies in Advanced Math. **7**, International Press, Cambridge (1997), 97-126.

[5] K. Monks, *On supersingular elliptic curves and hypergeometric functions*, Involve. **Vol. 5 No. 1** (2012), 99-113.

[6] J. H. Silverman, *An Introduction of the Theory of Elliptic Curves*, Summer school on Computational Number Theory and Applications to Cryptography, University of Wyoming, 2006.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Science+Business Media, LLC, New York, NY, 2009.

[8] J. H. Silverman, *Rational Points on Elliptic Curves*, Springer Science+Business Media, Inc., New York, NY, 1992.

[9] National Security Agency, *The Case for Elliptic Curve Cryptography*, National Security Agency, NSA.gov, 2009.

[10] R. Vidunas, *Algebraic transformations of Gauss hypergeometric functions*, Funkcialaj Ekvacioj. **52** (2009), 139-180.

[11] L. C. Washington, *Elliptic Curves: number theory and cryptography*, Taylor & Francis Group, LLC, Boca Raton, FL, 2008.

245 Williams Road, Bryn Mawr, PA 19010

E-mail address: spitman222@gmail.com