involve
a journal of mathematics

On supersingular elliptic curves and hypergeometric functions

Keenan Monks

mathematical sciences publishers

2012 vol. 5, no. 1

INVOLVE 5:1(2012)

On supersingular elliptic curves and hypergeometric functions

Keenan Monks

(Communicated by Ken Ono)

The Legendre family of elliptic curves has the remarkable property that both its periods and its supersingular locus have descriptions in terms of the hypergeometric function ${}_2F_1\left(\begin{smallmatrix}1/2 & 1/2\\ & 1\end{smallmatrix} \,\middle|\, z\right)$. In this work we study elliptic curves and elliptic integrals with respect to the hypergeometric functions ${}_2F_1\left(\begin{smallmatrix}1/3 & 2/3\\ & 1\end{smallmatrix} \,\middle|\, z\right)$ and ${}_2F_1\left(\begin{smallmatrix}1/2 & 5/12\\ & 1\end{smallmatrix} \,\middle|\, z\right)$, and prove that the supersingular λ-invariant locus of certain families of elliptic curves are given by these functions.

1. Introduction and statement of results

Let p be a prime and $\mathbb{F}$ a field of characteristic p. An *elliptic curve* $E/\mathbb{F}$ is a curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in \mathbb{F}$ and the points in E are elements of $\overline{\mathbb{F}} \times \overline{\mathbb{F}}$. This curve must be nonsingular in that it has no multiple roots. A point at infinity must also be included on the curve to make it projective.

There is an important invariant defined for any isomorphism class of elliptic curves (two curves are isomorphic if they have the same defining equation up to some change of coordinate system). Using the notation of an elliptic curve as before, the j-invariant $j(E)$ and discriminant $\Delta(E)$ are defined to be

$$j(E) = \frac{c_4^3}{\Delta}$$

and

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728}$$

where $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216a_3^2 - 864a_6$, $b_2 = a_1^2 + 4a_2$, and $b_4 = a_1a_3 + 2a_4$.

MSC2010: 14H52, 33C05.

Keywords: elliptic curves, hypergeometric functions.

It is well-known that the points on the curve E with coordinates in $\overline{\mathbb{F}}$ form the group $E(\mathbb{F})$ (see [Washington 2003] for an explanation of the group structure). The curve E is called *supersingular* if and only if the group $E(\mathbb{F})$ has no p-torsion. In this paper, we will determine when certain infinite families of elliptic curves are supersingular for any prime.

One well-known and widely studied family of elliptic curves is the Legendre family, which we denote by

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

for $\lambda \neq 0, 1$. We define its *supersingular locus* by

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

The locus $S_{p,\frac{1}{2}}(\lambda)$ and the periods of $E_{\frac{1}{2}}(\lambda)$ have beautiful and simple descriptions in terms of the hypergeometric function

$${}_2F_1\left(\begin{matrix} a & b \\ & c \end{matrix} \,\middle|\, z\right) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!}.$$

Here $a, b, z \in \mathbb{C}$, $c \in \mathbb{C} \setminus \mathbb{Z}^{\leq 0}$, $(x)_0 = 1$, and $(x)_n = (x)(x+1)\cdots(x+n-1)$ is the Pochhammer symbol. For any prime p, define

$${}_2F_1\left(\begin{matrix} a & b \\ & c \end{matrix} \,\middle|\, z\right)_p \equiv \sum_{n=0}^{p-1} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!} \pmod{p}.$$

It is natural to study hypergeometric functions related to elliptic integrals. An *elliptic integral of the first kind* is written as

$$K(k) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1 - k^2 \sin^2(\theta)}}.$$

From [Borwein and Borwein 1987] we have the following identities for appropriate ranges of k:

$$K(k) = \frac{\pi}{2} \, {}_2F_1\left(\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ & 1 \end{matrix} \,\middle|\, k^2\right), \tag{1-1a}$$

$$K^2(k) = \frac{\pi^2}{4} \sqrt{\frac{1 - \frac{8}{9}h^2}{1 - (kk')^2}} \left({}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \,\middle|\, h^2\right)\right)^2, \tag{1-1b}$$

$$K(k) = \frac{\pi}{2} (1 - (2kk')^2)^{-\frac{1}{4}} \, {}_2F_1\left(\begin{matrix} \frac{1}{4} & \frac{3}{4} \\ & 1 \end{matrix} \,\middle|\, \frac{(2kk')^2}{(2kk')^2 - 1}\right), \tag{1-1c}$$

$$K(k) = \frac{\pi}{2}(1-(kk')^2)^{-\frac{1}{4}}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\ \middle|\ J^{-1}\right). \tag{1-1d}$$

Here $k' = \sqrt{1-k^2}$, $J = \dfrac{(4(2kk')^{-2}-1)^3}{27(2kk')^{-2}}$ and h is the smaller of the two solutions of

$$\frac{(9-8h^2)^3}{64h^6h'^2} = J.$$

For the locus $S_{p,\frac{1}{2}}$, it is a classical result (see [Husemöller 2004] and [Silverman 1986]) that

$$S_{p,\frac{1}{2}}(\lambda) \equiv\ {}_2F_1\left(\begin{matrix}\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}\ \middle|\ \lambda\right)_p \pmod p.$$

In [El-Guindy and Ono 2012], El-Guindy and Ono studied the family of curves defined by

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

They proved a result analogous to the classical case, namely

$$\prod_{\substack{\lambda_0\in\overline{\mathbb{F}}_p\\ \text{supersingular } E_{\frac{1}{4}}(\lambda_0)}} (\lambda-\lambda_0) \equiv\ {}_2F_1\left(\begin{matrix}\frac{1}{4} & \frac{3}{4}\\ & 1\end{matrix}\ \middle|\ -\lambda\right)_p \pmod p.$$

Here we prove two other cases of this phenomenon that cover the other hypergeometric functions related to elliptic integrals listed in (1-1). We define the following families of elliptic curves:

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

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

We note that $E_{\frac{1}{3}}(\lambda)$ is singular for $\lambda \in \{0, 27\}$, and that $E_{\frac{1}{12}}(\lambda)$ is singular for $\lambda \in \{0, 1\}$.

We also define, for each $i \in \left\{\frac{1}{3}, \frac{1}{4}, \frac{1}{12}\right\}$ and all primes $p \geq 5$,

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

Generalizing the results above, we prove the following for $E_{\frac{1}{3}}(\lambda)$ and $E_{\frac{1}{12}}(\lambda)$.

Theorem 1.1. *For any prime $p \geq 5$, we have*

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

Theorem 1.2. *For any prime $p \geq 5$, we have the following*:

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

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

(2) *if* $p \equiv 7, 11 \pmod{12}$, *then*

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

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* $p \equiv 1, 5, 7, 11 \pmod{12}$.

Remark. The j-invariant of $E_{\frac{1}{3}}(\lambda)$ is $\lambda(\lambda - 24)^3/(\lambda - 27)$ and the j-invariant of $E_{\frac{1}{12}}(\lambda)$ is $1728\lambda/(\lambda - 1)$. Notice that $E_{\frac{1}{3}}(\lambda)$ is singular when $\lambda = 0$ and $j = 0$. Also, $E_{\frac{1}{12}}(\lambda)$ is singular when its j-invariant is 0 and undefined when $j = 1728$.

In addition to the stated result, the proof of Theorem 1.2 yields some fascinating combinatorial identities as well. The following is one such identity obtained for a specific class of p modulo 12. Similar results also hold for primes in the other congruence classes, but are omitted for brevity.

Corollary 1.3. *Let* $p \geq 5$ *be a prime congruent to* 1 *modulo* 12, *and let* $m = \frac{p-1}{12}$. *Then for all* $0 \leq n \leq m$,

$$4^n \binom{3m - n}{3m - 3n} \binom{6m}{3m - n} \binom{6m}{m} \equiv 27^n \sum_{t=n}^{m} \binom{m}{t} \binom{5m}{t} \binom{6m}{3m} \pmod{p}.$$

In particular, *when* $n = m$,

$$4^m \binom{6m}{2m} \binom{6m}{m} \equiv 27^m \binom{5m}{m} \binom{6m}{3m} \pmod{p}.$$

2. Preliminaries

Throughout, let $p \geq 5$ be prime.

Definition 2.1. The *Hasse invariant* of an elliptic curve defined by $f(w, x, y) = 0$ is the coefficient of $(wxy)^{p-1}$ in $f(w, x, y)^{p-1}$. Likewise, the *Hasse invariant* of a curve defined by $y^2 = f(x)$ is the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$.

Remark. The projective completions of $E_{\frac{1}{3}}(\lambda)$ and $E_{\frac{1}{12}}(\lambda)$ are

$$wy^2 + \lambda wxy + \lambda^2 y - x^3 = 0$$

and

$$wy^2 - 4x^3 + 27\lambda w^2 x + 27\lambda w^3 = 0.$$

Here is a well-known characterization of supersingular elliptic curves.

Lemma 2.2 [Husemöller 2004, Definition 3.1 of Chapter 13]. *An elliptic curve E is supersingular if and only if its Hasse invariant is* 0.

It is well-known that two elliptic curves defined over $\overline{\mathbb{F}}_p$ are isomorphic if and only if they have the same j-invariant. Recall the following formula for the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (see [Washington 2003]). We write $p-1=12m_p+6\epsilon_p+4\delta_p$, where $\epsilon_p, \delta_p \in \{0, 1\}$.

Lemma 2.3. *Up to isomorphism, there are exactly*

$$m_p+\epsilon_p+\delta_p$$

supersingular elliptic curves in characteristic p.

Remark. It is known that $\delta_p = 1$ only when $p \equiv 2 \pmod 3$ (i.e., when 0 is a supersingular j-invariant) and $\epsilon_p = 1$ only when $p \equiv 3 \pmod 4$ (when 1728 is a supersingular j-invariant). Also, in all cases $m_p = \left\lfloor \frac{p}{12} \right\rfloor$.

3. Proof of main results

We first prove several preliminary lemmas.

Lemma 3.1. *There are exactly $\left\lfloor \frac{p}{3} \right\rfloor$ distinct values of λ for which $E_{\frac{1}{3}}(\lambda)$ is supersingular over $\overline{\mathbb{F}}_p$.*

Proof. To calculate the degree of $S_{p,\frac{1}{3}}(\lambda)$, we must consider how many different values for λ yield a curve $E_{\frac{1}{3}}(\lambda)$ with a given supersingular j-invariant. From [Lennon 2010] we have that

$$j(E_{\frac{1}{3}}(\lambda)) = \frac{\lambda(\lambda-24)^3}{\lambda-27} \tag{3-1}$$

and that the discriminant $\Delta(E_{\frac{1}{3}}(\lambda)) = \lambda^8(\lambda-27)$. Hence there are usually four λ-invariants for a given j-invariant, but there are certain exceptions. Since the only roots of Δ in this case are 0 and 27, we know that these and 1728 are the only possible j-invariants for which there are less than four corresponding λ-invariants. However, there are four distinct values of λ for which $j(E_{\frac{1}{3}}(\lambda)) = 27$. Also, only $\lambda = 18 \pm 6\sqrt{3}$ gives a value of 1728 for j, so the correspondence is 2-to-1 in this case. As mentioned previously, the curve is singular for $\lambda = 0$, so the only value of λ that will give a j-invariant of 0 is $\lambda = 24$. The correspondence is thus one-to-one for $j = 0$.

Using the ideas of Lemma 2.3, we have that each of the m_p supersingular j-invariants is obtained from four supersingular λ-invariants, δ_p can come from at most one λ-invariant, and ϵ_p comes from two, if any, λ-invariants. Thus the total number of λ-invariants, and the degree of $S_{p,\frac{1}{3}}(\lambda)$, is

$$4m_p + \delta_p + 2\epsilon_p = 4\left\lfloor \frac{p}{12} \right\rfloor + \delta_p + 2\epsilon_p.$$

It is easily verified that this equals $\left\lfloor \frac{p}{3} \right\rfloor$ for every prime p, and so we are done. □

Lemma 3.2. *There are exactly $\left\lfloor \frac{p}{12} \right\rfloor$ distinct values of λ for which $E_{\frac{1}{12}}(\lambda)$ is supersingular over $\overline{\mathbb{F}}_p$.*

Proof. The j-invariant of $E_{\frac{1}{12}}(\lambda)$ is

$$j(E_{\frac{1}{12}}(\lambda)) = \frac{1728\lambda}{\lambda - 1}. \tag{3-2}$$

This is a one-to-one correspondence from λ-invariants to j-invariants for $j \neq 1728$. Also, the special cases $j = 0$ and $j = 1728$ do not apply here, for the curve is singular for these respective j-invariants. Thus by Lemma 2.3 there are exactly $\left\lfloor \frac{p}{12} \right\rfloor$ values of λ for which $E_{\frac{1}{12}}(\lambda)$ is supersingular. □

Proof of Theorem 1.1. The curve $E_{\frac{1}{3}}(\lambda)$ can be defined as

$$f(w, x, y) = wy^2 + \lambda wxy + \lambda^2 w^2 y - x^3 = 0.$$

To compute its Hasse invariant, we consider a general term in the expansion of $(wy^2 + \lambda wxy + \lambda^2 w^2 y - x^3)^{p-1}$. It has the form

$$(wy^2)^a (\lambda wxy)^b (\lambda^2 w^2 y)^c (-x^3)^d,$$

where $a + b + c + d = p - 1$. In order for this to be a constant multiple of a power of wxy, we must have $a = c = d$.

Thus the terms that we are concerned with are of the form

$$(wy^2)^n (\lambda^2 w^2 y)^n (-x^3)^n (\lambda wxy)^{p-3n-1} = (-\lambda)^{p-n-1} (wxy)^{p-1}.$$

For a given n, there are

$$\binom{p-1}{n}\binom{p-n-1}{n}\binom{p-2n-1}{n}$$

ways to choose which of the $f(w, x, y)$ factors we obtain each of the wy^2, $\lambda^2 w^2 y$, and $-x^3$ terms from. Summing over all possible values of n, we determine the

Hasse invariant to be

$$\begin{aligned}
&\sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \binom{p-1}{n}\binom{p-n-1}{n}\binom{p-2n-1}{n}(-\lambda)^{p-n-1} \\
&\equiv \sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \frac{(-\lambda)^{p-n-1}(p-1)(p-2)\cdots(p-n)}{n!} \\
&\qquad \cdot \frac{(p-n-1)\cdots(p-2n)}{n!} \\
&\qquad \cdot \frac{(p-2n-1)\cdots(p-3n)}{n!} \pmod{p} \\
&\equiv \sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \frac{(3n)!}{n!^3}\lambda^{p-n-1} \pmod{p}.
\end{aligned}$$

By definition, we have

$${}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p \equiv \sum_{n=0}^{p-1} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{n!^2} \frac{27^n}{x^n} \pmod{p}.$$

However, if $n > \lfloor \frac{p}{3} \rfloor$, then p will appear in the numerator of either $\left(\frac{1}{3}\right)_n$ or $\left(\frac{2}{3}\right)_n$, making those terms congruent to 0 modulo p, so

$$\begin{aligned}
\lambda^{p-1}\,{}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p &\equiv \sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{n!^2} 27^n \lambda^{p-n-1} \pmod{p} \\
&\equiv \sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \frac{27^n \frac{1}{3}\frac{2}{3}\frac{4}{3}\frac{5}{3}\cdots\frac{3n-2}{3}\frac{3n-1}{3}}{n!^2}\lambda^{p-n-1} \pmod{p} \\
&\equiv \sum_{n=0}^{\lfloor \frac{p}{3} \rfloor} \frac{(3n)!}{n!^3}\lambda^{p-n-1} \pmod{p}.
\end{aligned}$$

Thus $\lambda^{p-1}\,{}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$ is congruent modulo p to the Hasse invariant of $E_{\frac{1}{3}}(\lambda)$. So by Lemma 2.2, λ is a root of $\lambda^{p-1}\,{}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p \equiv 0 \pmod{p}$ if and only if $E_{\frac{1}{3}}(\lambda)$ is supersingular, i.e., if and only if λ is a root of $S_{p,\frac{1}{3}}(x)$.

The least power of λ in ${}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$ is $-\lfloor \frac{p}{3} \rfloor$. Hence $\lambda^{\lfloor p/3 \rfloor}\,{}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$ has the same roots as $\lambda^{p-1}\,{}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$, with the exception of 0, which is not a λ-invariant as shown in Lemma 3.1, and thus is not a root of $S_{p,\frac{1}{3}}$.

The degree of $\lambda^{\lfloor \frac{p}{3} \rfloor} {}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$ is exactly $\lfloor \frac{p}{3} \rfloor$. Since the degree of $S_{p,\frac{1}{3}}(\lambda)$ is also $\lfloor \frac{p}{3} \rfloor$ by Lemma 3.1, it follows that $\lambda^{\lfloor \frac{p}{3} \rfloor} {}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p \equiv c \cdot S_{p,\frac{1}{3}}(\lambda) \pmod{p}$. However, c is 1 since $\lambda^{\lfloor \frac{p}{3} \rfloor} {}_2F_1\left(\begin{matrix} \frac{1}{3} & \frac{2}{3} \\ & 1 \end{matrix} \middle| \frac{27}{\lambda}\right)_p$ is monic: we are done. □

Proof of Theorem 1.2. Assume $p \equiv 1, 5 \pmod{12}$. The function

$$f(z) = {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \middle| z\right)$$

satisfies the second order differential equation

$$z(1-z)\frac{d^2 f}{dz^2} + \left(1 - \frac{3}{2}z\right)\frac{df}{dz} - \frac{5}{144}f = 0.$$

Substituting $z = 1 - \frac{1}{x}$, we see that $g(x) = {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \middle| 1 - \frac{1}{x}\right)$ satisfies

$$x^2(x-1)\frac{d^2 g}{dx^2} + x\left(\frac{3}{2}x - \frac{1}{2}\right)\frac{dg}{dx} - \frac{5}{144}g = 0.$$

Hence, $h(\lambda) = \lambda^{\frac{p-1}{4}} {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \middle| 1 - \frac{1}{\lambda}\right)$ satisfies

$$\begin{aligned}(\lambda^3 - \lambda^2)\frac{d^2 h}{d\lambda^2} &+ \left(\left(2 - \frac{p}{2}\right)\lambda^2 + \left(\frac{p}{2} - 1\right)\lambda\right)\frac{dh}{d\lambda} \\ &+ \left(\left(\frac{p^2 - 4p + 3}{16}\right)\lambda + -\frac{p^2}{16} + \frac{1}{36}\right)h = 0. \qquad (3\text{-}3)\end{aligned}$$

The function $h(\lambda)$ is a Laurent series in $\frac{1}{\lambda}$ with p-integral rational coefficients. However, its reduction modulo p yields a polynomial in λ. This polynomial must satisfy the reduction of (3-3) modulo p, so $F(\lambda) = \lambda^{\frac{p-1}{4}} {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \middle| 1 - \frac{1}{\lambda}\right)_p$ satisfies

$$(\lambda^3 - \lambda^2)\frac{d^2 F}{d\lambda^2} + (2\lambda^2 - \lambda)\frac{dF}{d\lambda} + \left(\frac{3}{16}\lambda + \frac{1}{36}\right)F \equiv 0 \pmod{p}.$$

A similar calculation shows that $F(\lambda) = \lambda^{\frac{p-3}{4}} {}_2F_1\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \middle| 1 - \frac{1}{\lambda}\right)_p$ also satisfies the same differential equation when $p \equiv 7, 11 \pmod{12}$.

Now, to compute the Hasse invariant, we consider a general x^{p-1} term in the expansion of $(4x^3 - 27\lambda x - 27\lambda)^{\frac{p-1}{2}}$. This is of the form

$$(4x^3)^n(-27\lambda x)^{p-3n-1}(-27\lambda)^{2n-\frac{p-1}{2}},$$

where $\frac{p-1}{4} \leq n \leq \lfloor \frac{p}{3} \rfloor$. For a given n in this range, there are exactly

$$\binom{\frac{p-1}{2}}{n}\binom{\frac{p-1}{2}-n}{p-3n-1}$$

ways to choose which of the $4x^3-27\lambda x-27\lambda$ factors the $4x^3$ terms and $-27\lambda x$ terms came from. Summing over all n yields the Hasse invariant to be

$$\sum_{n=\frac{p-1}{4}}^{\lfloor \frac{p}{3} \rfloor} 4^n(-27\lambda)^{\frac{p-1}{2}-n}\binom{\frac{p-1}{2}}{n}\binom{\frac{p-1}{2}-n}{p-3n-1},$$

into which we can substitute $n=\frac{p-1}{2}-k$, and using the fact that $4^{\frac{p-1}{2}} \equiv 1 \pmod p$, we obtain

$$\sum_{k=\frac{p-1}{2}-\lfloor \frac{p}{3} \rfloor}^{\frac{p-1}{4}} \left(-\frac{27}{4}\lambda\right)^k \binom{\frac{p-1}{2}}{k}\binom{k}{3k-\frac{p-1}{2}}.$$

We show the Hasse invariant satisfies the differential equation by showing that for any t, the λ^t term in the resulting expansion is congruent to 0 mod p. Let

$$c(k)=\left(-\frac{27}{4}\lambda\right)^k \binom{\frac{p-1}{2}}{k}\binom{k}{3k-\frac{p-1}{2}}.$$

Then the λ^t term has coefficient

$$\frac{d^2}{dt^2}c(t-1)-\frac{d^2}{dt^2}c(t)+2\frac{d}{dt}c(t-1)-\frac{d}{dt}c(t)+\frac{3}{16}c(t-1)+\frac{1}{36}c(t),$$

which we expand to obtain

$$\left(-\frac{27}{4}\right)^t \binom{\frac{p-1}{2}}{t}\binom{t}{3t-\frac{p-1}{2}}\left(-t(t-1)-t+\frac{1}{36}\right) \\ +\left(-\frac{27}{4}\right)^{t-1} \binom{\frac{p-1}{2}}{t-1}\binom{t-1}{3t-3-\frac{p-1}{2}}\left((t-1)(t-2)+2(t-1)+\frac{3}{16}\right).$$

This is congruent to 0 modulo p if and only if

$$\binom{\frac{p-1}{2}}{t}\binom{t}{3t-\frac{p-1}{2}}\left(\frac{27}{4}t^2-\frac{3}{16}\right)+\binom{\frac{p-1}{2}}{t-1}\binom{t-1}{3t-3-\frac{p-1}{2}}\left(t^2-t+\frac{3}{16}\right)$$

is also congruent to 0. We now expand the first binomials to obtain

$$\frac{1}{t!}\left(\frac{p-1}{2}\right)\cdots\left(\frac{p-1}{2}-t+1\right)\binom{t}{3t-\frac{p-1}{2}}\left(\frac{27}{4}t^2-\frac{3}{16}\right)$$
$$+\frac{1}{(t-1!)}\left(\frac{p-1}{2}\right)\cdots\left(\frac{p-1}{2}-t+2\right)\binom{t-1}{3t-3-\frac{p-1}{2}}\left(t^2-t+\frac{3}{16}\right),$$

which is congruent to 0 modulo p if and only if

$$\frac{\frac{1}{2}-t}{t}\binom{t}{3t-\frac{p-1}{2}}\left(\frac{27}{4}t^2-\frac{3}{16}\right)+\binom{t-1}{3t-3-\frac{p-1}{2}}\left(t^2-t+\frac{3}{16}\right)\equiv 0 \pmod{p}$$

as well. Using a similar cancellation method on the remaining binomials shows that it is sufficient to prove

$$\left(\frac{1}{2}-t\right)\left(\frac{p-1}{2}-2t+2\right)\left(\frac{p-1}{2}-2t+1\right)\left(\frac{27}{4}t^2-\frac{3}{16}\right)$$
$$+\left(3t-\frac{p-1}{2}\right)\left(3t-\frac{p-1}{2}-1\right)\left(3t-\frac{p-1}{2}-2\right)\left(t^2-t+\frac{3}{16}\right)\equiv 0 \pmod{p},$$

which is easily verified.

Thus the Hasse invariant satisfies the same second order differential equation as both $\lambda^{\frac{p-1}{4}}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$ and $\lambda^{\frac{p-3}{4}}\ {}_2F_1\left(\begin{matrix}\frac{7}{12} & \frac{11}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$. For $p>5$, notice that both the Hasse invariant and the truncated hypergeometric functions have no term with a degree less than 2. For each case, this implies that the truncated polynomials are congruent modulo p to the Hasse invariant up to multiplication by a constant. For the case $p=5$, it is easy to compute that $\lambda\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_5=\lambda$, and the Hasse invariant is 4λ, so this property still holds.

Therefore, we know that the two truncated hypergeometric functions have the same roots modulo p as the Hasse invariant, so by Lemma 2.2, λ is a root of the hypergeometric functions if and only if $E_{\frac{1}{12}}(\lambda)$ is supersingular. Notice that $\lambda^{\lfloor\frac{p}{12}\rfloor}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$ and $\lambda^{\lfloor\frac{p}{12}\rfloor}\ {}_2F_1\left(\begin{matrix}\frac{7}{12} & \frac{11}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$ have the same roots as $\lambda^{\frac{p-1}{4}}$ multiplied by the respective truncated functions with the exception of 0, which is as desired since $E_{\frac{1}{12}}(0)$ is singular. Also, when $p\equiv 1,5 \pmod{12}$ the degree of $\lambda^{\lfloor\frac{p}{12}\rfloor}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$ is $\lfloor\frac{p}{12}\rfloor$, so by Lemma 3.2, there exists a constant c_p such that

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

Similarly for primes $p \equiv 7, 11 \pmod{12}$,

$$S_{p,\frac{1}{12}} \equiv {c_p}^{-1} \lambda^{\lfloor \frac{p}{12} \rfloor} {}_2F_1\left(\begin{matrix} \frac{7}{12} & \frac{11}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{\lambda}\right)_p \pmod{p}.$$

Finally, we explicitly compute the constant c_p. Notice that $S_{p,\frac{1}{12}}$ is monic, so c_p is the coefficient of the leading term in $\lambda^{\lfloor \frac{p}{12} \rfloor} {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{\lambda}\right)_p$, the same as the constant term in ${}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{\lambda}\right)_p$. For $n > \lfloor \frac{p}{12} \rfloor$, one of $\left(\frac{1}{12}\right)_n$ or $\left(\frac{5}{12}\right)_n$ will be congruent to 0 modulo p. Hence, the constant term of

$${}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{\lambda}\right)_p = \sum_{n=0}^{\lfloor \frac{p}{12} \rfloor} \frac{\left(\frac{1}{12}\right)_n \left(\frac{5}{12}\right)_n}{n!^2} \left(1 - \frac{1}{\lambda}\right)^n$$

is

$$\sum_{n=0}^{\lfloor \frac{p}{12} \rfloor} \frac{\left(\frac{1}{12}\right)_n \left(\frac{5}{12}\right)_n}{n!^2}.$$

For $p \equiv 1 \pmod{12}$, we have

$$\frac{\left(\frac{1}{12}\right)_n}{n!} \equiv (-1)^n \frac{\frac{p-1}{12} \frac{p-13}{12} \cdots \left(\frac{p-1}{12} - n + 1\right)}{n!} \pmod{p} \equiv (-1)^n \binom{\frac{p-1}{12}}{n} \pmod{p}.$$

Also, $\frac{\left(\frac{5}{12}\right)_n}{n!} \equiv (-1)^n \binom{\frac{5p-5}{12}}{n} \pmod{p}$. Therefore,

$$c_p = \sum_{n=0}^{\lfloor \frac{p}{12} \rfloor} \frac{\left(\frac{1}{12}\right)_n \left(\frac{5}{12}\right)_n}{n!^2} \equiv \binom{6 \lfloor \frac{p}{12} \rfloor}{\lfloor \frac{p}{12} \rfloor} \pmod{p}.$$

For $p \equiv 5 \pmod{12}$,

$$c_p = \sum_{n=0}^{\lfloor \frac{p}{12} \rfloor} \frac{\left(\frac{1}{12}\right)_n \left(\frac{5}{12}\right)_n}{n!^2} \equiv \binom{6 \lfloor \frac{p}{12} \rfloor + 2}{\lfloor \frac{p}{12} \rfloor} \pmod{p}.$$

A similar method can be used to compute $c_p \equiv \binom{6 \lfloor \frac{p}{12} \rfloor + 2}{\lfloor \frac{p}{12} \rfloor} \pmod{p}$ when $p \equiv 7 \pmod{12}$ and $\binom{6 \lfloor \frac{p}{12} \rfloor + 4}{\lfloor \frac{p}{12} \rfloor}$ when $p \equiv 11 \pmod{12}$, which completes the proof. □

Proof of Corollary 1.3. Recall from the proof of Theorem 1.2 that since the Hasse invariant of $E_{\frac{1}{12}}(\lambda)$ and the polynomial $\lambda^{\frac{p-1}{4}} {}_2F_1\left(\begin{matrix} \frac{1}{12} & \frac{5}{12} \\ & 1 \end{matrix} \,\middle|\, 1 - \frac{1}{\lambda}\right)_p$ both satisfied the same second order differential equation, they are congruent up to multiplication by a constant, which we will denote b_p. The same argument and notation apply to $\lambda^{\frac{p-3}{4}}\ {}_2F_1\left(\begin{matrix}\frac{7}{12} & \frac{11}{12} \\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p$ when $p \equiv 7, 11 \mod 12$).

Assume that $p \equiv 1 \mod 12$, and define $m = \lfloor \frac{p}{12} \rfloor$. Also, define $n = 3m-k$. We computed the Hasse invariant of $E_{\frac{1}{12}}(\lambda)$ to be

$$\sum_{k=2m}^{3m}\left(\frac{-27}{4}\lambda\right)^k\binom{6m}{k}\binom{k}{3m-6m}=\sum_{n=0}^{m}\left(\frac{-27\lambda}{4}\right)^{3m-n}\binom{6m}{3m-n}\binom{3m-n}{3m-3n}.$$

By definition,

$$\lambda^{\frac{p-1}{4}}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12} \\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p \equiv \lambda^{\frac{p-1}{4}}\sum_{k=0}^{m}\frac{\left(\frac{1}{12}\right)_k\left(\frac{5}{12}\right)_k}{k!^2}\left(1-\frac{1}{\lambda}\right)^k \pmod{p}.$$

As before,

$$\frac{\left(\frac{1}{12}\right)_k\left(\frac{5}{12}\right)_k}{k!^2}\equiv\binom{m}{k}\binom{5m}{k} \pmod{p}.$$

We expand each of the $\left(1-\frac{1}{\lambda}\right)^k$ terms and rearrange to obtain

$$\begin{aligned}\lambda^{\frac{p-1}{4}}\ {}_2F_1\left(\begin{matrix}\frac{1}{12} & \frac{5}{12} \\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_p &\equiv \sum_{k=2m}^{3m}(-\lambda)^k\sum_{t=3m-k}^{m}\binom{m}{t}\binom{5m}{t}\binom{t}{3m-k} \pmod{p}\\ &\equiv \sum_{n=0}^{m}(-\lambda)^{3m-n}\sum_{t=n}^{m}\binom{m}{t}\binom{5m}{t}\binom{t}{n} \pmod{p}.\end{aligned}$$

Since this polynomial is congruent to the Hasse invariant via multiplication by b_p, we have, for all $0 \le n \le m$,

$$\left(\frac{27}{4}\right)^{3m-n}\binom{3m-n}{3m-3n}\binom{6m}{3m-n}\equiv b_p\sum_{t=n}^{m}\binom{m}{t}\binom{5m}{t}\binom{t}{n} \pmod{p}.$$

When $n=0$, this becomes

$$\left(\frac{27}{4}\right)^{3m}\binom{6m}{3m}\equiv b_p\sum_{t=0}^{m}\binom{m}{t}\binom{5m}{t}\equiv b_p\binom{6m}{m} \pmod{p}$$

and thus

$$b_p \equiv \frac{\binom{6m}{3m}\left(\frac{27}{4}\right)^{3m}}{\binom{6m}{m}} \pmod{p}.$$

Substituting this back into our identity, we have that for all $0 \le n \le m$,

$$\left(\frac{4}{27}\right)^n \binom{3m-n}{3m-3n}\binom{6m}{3m-n}\binom{6m}{m} \equiv \binom{6m}{3m}\sum_{t=n}^{m}\binom{m}{t}\binom{5m}{t}\binom{t}{n} \pmod p.$$

In the case $n = m$, we obtain the simpler identity

$$\left(\frac{27}{4}\right)^{3m}\binom{5m}{m}\binom{6m}{3m} \equiv \binom{6m}{2m}\binom{6m}{m} \pmod p. \qquad \square$$

4. Examples

In this section we provide two examples to illustrate our main theorems.

Example of Theorem 1.1. Consider $p = 19$. The supersingular j-invariants mod 19 are known to be 18 (corresponding to 1728) and 7. From formula (3-1) we find that the values of λ where $j \equiv 18 \pmod{19}$ are $-1 \pm i\sqrt{6}$ only. The values of λ for which $j \equiv 7 \pmod{19}$ are $-6 \pm 3\sqrt{2}$ and $4 \pm 11\sqrt{13}$. Thus

$$\begin{aligned} S_{19,\frac{1}{3}}(\lambda) &= (\lambda-(-1+i\sqrt{6}))(\lambda-(-1-i\sqrt{6}))(\lambda-(-6+3\sqrt{2})) \\ &\qquad (\lambda-(-6-3\sqrt{2}))(\lambda-(4+11\sqrt{13}))(\lambda-(4-11\sqrt{13})) \\ &\equiv \lambda^6+6\lambda^5+14\lambda^4+8\lambda^3+13\lambda^2+5\lambda+12 \pmod{19} \\ &\equiv (\lambda^2+2\lambda+7)(\lambda^2+11\lambda+1)(\lambda^2+12\lambda+18) \pmod{19}. \end{aligned}$$

The Hasse invariant is the coefficient of $(wxy)^{18}$ in the expansion of

$$(wy^2+\lambda wxy+\lambda^2w^2y-x^3)^{18}.$$

This is

$$H(\lambda) \equiv \lambda^{18}+6\lambda^{17}+14\lambda^{16}+8\lambda^{15}+13\lambda^{14}+5\lambda^{13}+12\lambda^{12} \equiv \lambda^{12}\, S_{19,\frac{1}{3}}(\lambda) \pmod{19}.$$

In addition,

$${}_2F_1\left(\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & 1\end{matrix}\,\middle|\,\frac{27}{\lambda}\right)_{19} \equiv 1+\frac{6}{\lambda}+\frac{14}{\lambda^2}+\frac{8}{\lambda^3}+\frac{13}{\lambda^4}+\frac{5}{\lambda^5}+\frac{12}{\lambda^6} \equiv \frac{1}{\lambda^6}S_{19,\frac{1}{3}}(\lambda) \pmod{19}.$$

Example of Theorem 1.2. Consider $p = 59$, which is 11 modulo 12. The supersingular j-invariants mod 59 are known to be 0, 17 (corresponding to 1728), 48, 47, 28, and 15. From formula (3-2), we find the λ-invariants corresponding to 48, 47, 28, and 15 are 32, 35, 24, and 22, respectively. We do not include the cases $j = 0$ or $j = 1728$ since in these cases $E_{\frac{1}{12}}(\lambda)$ is singular. Thus

$$\begin{aligned} S_{59,\frac{1}{12}}(\lambda) &= (\lambda+27)(\lambda+24)(\lambda+35)(\lambda+37) \\ &\equiv \lambda^4+5\lambda^3+10\lambda^2+11\lambda+3 \pmod{59}. \end{aligned}$$

The Hasse invariant is the coefficient of x^{58} in $(4x^3-27\lambda x-27\lambda)^{29}$. This is

$$H(\lambda)\equiv 2\lambda^{14}+10\lambda^{13}+20\lambda^{12}+22\lambda^{11}+6\lambda^{10}\equiv 2\lambda^{10}S_{59,\frac{1}{12}}(\lambda) \pmod{59}.$$

In addition,

$${}_2F_1\left(\begin{matrix}\frac{7}{12} & \frac{11}{12}\\ & 1\end{matrix}\,\middle|\, 1-\frac{1}{\lambda}\right)_{59}\equiv 2+\frac{10}{\lambda}+\frac{20}{\lambda^2}+\frac{22}{\lambda^3}+\frac{6}{\lambda^4}\equiv\frac{2}{\lambda^4}S_{59,\frac{1}{12}}(\lambda) \pmod{59} \pmod{59}.$$

Also, $c_{59}\equiv\binom{28}{4}\equiv 2 \pmod{59}$.

5. Conclusion

We have described the supersingular loci of two infinite families of elliptic curves in terms of truncated hypergeometric functions. For the family $E_{\frac{1}{3}}(\lambda)$, the supersingular locus was a power of λ times the ${}_2F_1\left(\begin{matrix}\frac{1}{3} & \frac{2}{3}\\ & 1\end{matrix}\,\middle|\,\frac{27}{\lambda}\right)_p$ function. We found a similar result for the family $E_{\frac{1}{12}}(\lambda)$. This gives a very simple method for determining exactly which values of λ yield supersingular curves for these infinite families. Over any given field $\mathbb{F}_p$, these λ-invariants are simply the roots of these hypergeometric functions truncated modulo p.

Our results also yield interesting insights into combinatorics. We have the very nice identity given in Corollary 1.3, and analogous results can be obtained by similar methods. For example, assume that p is any prime that is congruent to 1 modulo 12 and that $12m+1=p$. If one could prove that the constant b_p from the proof of Corollary 1.3 is congruent to 1 modulo p for all such p, then the following identity is implied from Corollary 1.3:

$$\binom{6m}{3m}\equiv\left(\frac{27}{4}\right)^m\binom{2m}{m} \pmod{p}.$$

The truth of this statement has been verified for all m up to 10000. This is a fascinating identity regarding the "central" binomial coefficients modulo p, and it illustrates the types of insights one can gain into combinatorics through the study of elliptic curves and hypergeometric functions.

It is our hope that these results will be used to further understand the deep connections between elliptic curves and hypergeometric functions.

References

[Borwein and Borwein 1987] J. M. Borwein and P. B. Borwein, *Pi and the AGM: a study in analytic number theory and computational complexity*, Wiley, New York, 1987. MR 89a:11134 Zbl 0611.10001

[El-Guindy and Ono 2012] A. El-Guindy and K. Ono, "Hasse invariants for the Clausen elliptic curves", preprint, 2012, available at http://www.mathcs.emory.edu/~ono/publications-cv/pdfs/129.pdf. To appear in *Ramanujan J.*

[Husemöller 2004] D. Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics **111**, Springer, New York, 2004. MR 2005a:11078 Zbl 1040.11043

[Lennon 2010] C. Lennon, "A trace formula for certain Hecke operators and Gaussian hypergeometric functions", preprint, 2010. arXiv 1003.1157

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Washington 2003] L. C. Washington, *Elliptic curves: number theory and cryptography*, Chapman & Hall/CRC, Boca Raton, FL, 2003. MR 2004e:11061 Zbl 1034.11037

Received: 2011-09-12 Accepted: 2011-09-14

monks@college.harvard.edu *Harvard University, 2013 Harvard Yard Mail Center, Cambridge 02138, United States*

involve

msp.berkeley.edu/involve

See inside back cover or http://msp.berkeley.edu/involve for submission instructions.

The subscription price for 2012 is US $105/year for the electronic version, and $145/year (+$35 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 Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, 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

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2012 vol. 5 no. 1