HYPERGEOMETRIC FUNCTIONS AND ELLIPTIC CURVES

JEREMY ROUSE

1. Introduction and Statement of Results

If $\lambda \in \mathbb{C} - \{0, 1\}$, then let E_λ be the elliptic curve

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

in Legendre normal form. A simple change of variables yields an equation for the curve of the form

$$y^2 = 4x^3 - g_2 x - g_3.$$

Such curves parametrized by $(\wp(z, \Lambda), \wp'(z, \Lambda))$ for $z \in \mathbb{C}$, where $\wp(z, \Lambda)$ is the Weierstrass $\wp$-function with period lattice Λ.

It is a classical problem (see [4] Ch. 6, Sec. 5-9, [7] Ch. 6, Sec. 5) to find a suitable lattice Λ given an elliptic curve. In the case when $\lambda \in \mathbb{R}$, Λ can be chosen to be of the form $\Lambda = \Omega(E_\lambda)\mathbb{Z} + \Omega'(E_\lambda)\mathbb{Z}$, where $\Omega(E_\lambda)$ is real and $\Omega'(E_\lambda)$ is strictly imaginary. Here $\Omega(E_\lambda)$ is called the "real period" of E_λ.

If $\lambda \in \mathbb{Q} - \{0, 1\}$, then $E_\lambda(\mathbb{Q})$, the group of rational points on E_λ, is finitely generated. For such λ, the Hasse-Weil L-function of E_λ is

$$L(E_\lambda, s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p(E_\lambda)p^{-s} + p^{1-2s}} \prod_{p \mid \Delta} \frac{1}{1 - a_p(E_\lambda)p^{-s}}.$$

Here Δ is the discriminant of E_λ and $a_p(E_\lambda)$ is the trace of Frobenius. The Birch and Swinnerton-Dyer conjecture predicts that $\mathrm{ord}_{s=1}(L(E_\lambda, s)) = \mathrm{rk}(E_\lambda(\mathbb{Q}))$, the rank of $E_\lambda(\mathbb{Q})$. Moreover it predicts that

$$\lim_{s \to 1} \frac{L(E_\lambda, s)}{(s-1)^{\mathrm{rk}(E_\lambda(\mathbb{Q}))}}$$

is an explicit multiple of $\Omega(E_\lambda)$ depending on the arithmetic invariants of $E_\lambda/\mathbb{Q}$. Therefore, given E_λ, computing $\Omega(E_\lambda)$ and $a_p(E_\lambda)$ is an important task. Here we give analogous formulas for $\Omega(E_\lambda)$ and $a_p(E_\lambda)$ in terms of hypergeometric functions.

If $a \in \mathbb{R}$ and n is a non-negative integer, then

$$(a)_n := \begin{cases} a(a+1)(a+2)\cdots(a+n-1) & n > 0 \\ 1 & n = 0. \end{cases}$$

This research was supported by K. Ono's NSF grant.

The ordinary hypergeometric function ${}_2F_1$ is given by

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

First we observe that $\Omega(E_\lambda)$ can be expressed in terms of ordinary hypergeometric functions. For our purposes, we slightly abuse terminology by defining $\Omega(E_\lambda)$ to be the real period of the curve $y^2 = 4x^3 - g_2 x - g_3$ which is obtained from the equation of E_λ in the usual way.

Theorem 1. *If $0 < \lambda < 1$, then the real period $\Omega(E_\lambda)$ is given by*

$$ \frac{\Omega(E_\lambda)}{\pi} = {}_2F_1\left(\begin{matrix} 1/2, & 1/2 \\ & 1 \end{matrix} ; \lambda\right). $$

If $\lambda \in \mathbb{Q}$ and p is a prime of good reduction for E_λ, then the number of points on E_λ over $\mathbb{F}_p$ (including the point at infinity) is given by

$$ |E_\lambda(\mathbb{F}_p)| = 1 + \sum_{x=0}^{p-1} (1 + \phi_p(x(x-1)(x-\lambda))) = p + 1 - a_p(E_\lambda). $$

Here ϕ_p denotes the Legendre symbol over p, and $a_p(E_\lambda)$ is the trace of Frobenius.

If A and B are Dirichlet characters mod p, we define the normalized Jacobi sum $\binom{A}{B}$ as

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

Throughout, we will let ϵ_p denote the trivial character mod p. Greene [2] used these binomial symbols to define *Gaussian hypergeometric functions*, as follows. If A, B, and C are Dirichlet characters mod p, then

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & C \end{matrix} ; x\right)_p := \frac{p}{p-1} \sum_{\chi} \binom{A\chi}{\chi} \binom{B\chi}{C\chi} \chi(x), $$

where the sum is taken over all Dirichlet characters mod p. These hypergeometric functions are analogues of the ordinary hypergeometric functions. They are also considered in [6] and [5]. Next we observe that the trace of Frobenius, $a_p(E_\lambda)$, can be computed in terms of Gaussian hypergeometric functions. This result is a special case of Thm 11.6 of [6] and of Thm 3.6 of [2].

Theorem 2. *If $\lambda \in \mathbb{Q} - \{0, 1\}$ and p is a prime with $\mathrm{ord}_p(\lambda(\lambda-1)) = 0$, then the trace of Frobenius on E_λ satisfies*

$$ \frac{-\phi_p(-1) a_p(E_\lambda)}{p} = {}_2F_1\left(\begin{matrix} \phi_p, & \phi_p \\ & \epsilon_p \end{matrix} ; \lambda\right)_p. $$

Notice the similarity in the two expressions

$$\frac{\Omega(E_\lambda)}{\pi} = {}_2F_1\left(\begin{matrix} 1/2, & 1/2 \\ & 1 \end{matrix}\; ; \lambda\right)$$

and

$$\frac{-\phi_p(-1)a_p(E_\lambda)}{p} = {}_2F_1\left(\begin{matrix} \phi_p, & \phi_p \\ & \epsilon_p \end{matrix}\; ; \lambda\right)_p.$$

Replacing π with $\phi_p(-1)p$, $\Omega(E_\lambda)$ with $a_p(E_\lambda)$, and 1, 1/2 with Dirichlet characters of orders 1 and 2, respectively, and swapping ordinary and Gaussian hypergeometric functions turns the expression for the real period into the expression for the trace of Frobenius, up to sign. This sign is inherent in the definition of the Gaussian hypergeometric functions. This correspondence is further clarified by the fact that π and $\phi_p(-1)p$ naturally correspond since

$$G(\phi_p) = \sqrt{\phi_p(-1)p}$$
$$\Gamma(1/2) = \sqrt{\pi},$$

where $G(\chi)$ is the classical Gauss sum of χ (see [3], Thm. 6.1, pg. 75). This suggests a striking correspondence between hypergeometric functions and Gaussian hypergeometric functions.

For further evidence of this correspondence, we will consider the special case when $\lambda = 1/2$. In this case, simpler expressions for both hypergeometric functions are known. In particular, it can be shown (see Section 2) that

$$\frac{\sqrt{2}}{2\pi} \cdot {}_2F_1\left(\begin{matrix} 1/2, & 1/2 \\ & 1 \end{matrix}\; ; \frac{1}{2}\right) = \frac{\Gamma(5/4)}{\Gamma(3/2)\Gamma(3/4)}.$$

Now, the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Since $\Gamma(n) = (n-1)!$, the right hand side could be interpreted as $\binom{1/4}{1/2}$. A similar evaluation of the relevant Gaussian hypergeometric function yields the following result.

Theorem 3. *If $\lambda = 1/2$, then*

$$\frac{\sqrt{2}}{2\pi} \cdot \Omega(E_\lambda) = \operatorname{Re}\binom{1/4}{1/2}$$

and

$$\frac{-\phi_p(-2)}{2p} \cdot a_p(E_\lambda) = \operatorname{Re}\binom{\chi_4}{\phi_p},$$

where χ_4 is a Dirichlet character of order 4.

Notice that replacing $\sqrt{2}$ with $\phi_p(2)$, π with $\phi_p(-1)p$, χ_4 and ϕ_p (Dirichlet characters of order 4 and 2, respectively) with $1/4$ and $1/2$, and $\Omega(E_\lambda)$ with $a_p(E_\lambda)$ turns the second formula into the first, up to sign. This provides more evidence that there is a natural correspondence between ordinary hypergeometric functions and Gaussian hypergeometric functions.

2. Proofs

Proof of Theorem 1. The change of variables $(x, y) \mapsto \left(x + \frac{1+\lambda}{3}, y/2\right)$ takes the elliptic curve E_λ to

$$E : y^2 = 4x^3 - g_2x - g_3 = 4(x-a)(x-b)(x-c),$$

where $a = -\frac{\lambda+1}{3}$, $b = \frac{2\lambda-1}{3}$, and $c = \frac{2-\lambda}{3}$. Knapp ([4], Prop. 6.33) shows that the periods of the elliptic curve E may be taken to be

$$\omega_1 = \int_a^b \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}}$$
$$\omega_2 = \int_b^c \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}}.$$

Note that for $a < x < b$, $(x-a)$ is positive, while $(x-b)$ and $(x-c)$ are negative. Hence, ω_1 is the real period.

Making the substitution $\sqrt{x-a} = \sqrt{b-a} \cdot \sin\theta$ in the first integral yields the following formula:

$$\Omega(E) = 2\int_0^{\pi/2} \frac{d\theta}{\sqrt{(c-a)-(b-a)\sin^2\theta}}.$$

Now, noting that $b - a = \lambda$ and $c - a = 1$ gives

$$\Omega(E) = 2\int_0^{\pi/2} \frac{d\theta}{\sqrt{1-\lambda\sin^2\theta}}.$$

Using the binomial expansion for $\frac{1}{\sqrt{1-\lambda\sin^2\theta}}$ and integrating termwise yields

$$\Omega(E) = 2\sum_{n=0}^{\infty}\prod_{i=0}^{n-1}\left(i+\frac{1}{2}\right)\frac{\lambda^n}{n!}\int_0^{\pi/2}\sin^{2n}\theta\, d\theta.$$

Note that if n is a non-negative integer, then

$$\int_0^{\pi/2}\sin^{2n}\theta\, d\theta = \frac{2\pi}{4^{n+1}}\binom{2n}{n}.$$

Also,

$$\binom{2n}{n}\frac{1}{n!4^n} = \frac{(2n)!}{(n!)^3 4^n} = \frac{\prod_{i=0}^{n-1}\left(\frac{1}{2}+i\right)}{n!\prod_{i=0}^{n-1}(1+i)}.$$

These formulas yield that

$$\begin{aligned}\frac{\Omega(E_\lambda)}{\pi} = \frac{\Omega(E)}{\pi} &= \sum_{n=0}^{\infty} \frac{\prod_{i=0}^{n-1}\left(\frac{1}{2}+i\right)^2}{n!\prod_{i=0}^{n-1}(1+i)}\lambda^n \\ &= \sum_{n=0}^{\infty} \frac{\left(\frac{1}{2}\right)_n\left(\frac{1}{2}\right)_n}{(1)_n}\frac{\lambda^n}{n!} \\ &= {}_2F_1\left(\begin{matrix}1/2, & 1/2 \\ & 1\end{matrix}\; ; \lambda\right),\end{aligned}$$

as desired. □

Proof of Theorem 3. First we establish that

$$\Omega(E_{1/2}) = \pi\sqrt{2}\frac{\Gamma(5/4)}{\Gamma(3/2)\Gamma(3/4)}.$$

As shown in the proof of Theorem 1,

$$\Omega(E_\lambda) = 2\int_0^{\pi/2} \frac{d\theta}{\sqrt{1-\lambda\sin^2\theta}}.$$

With $\lambda = 1/2$, multiplying the numerator and denominator by $\sqrt{2}$ and setting $\sin^2\theta = 1-\cos^2\theta$ gives

$$\Omega(E_{1/2}) = 2\sqrt{2}\int_0^{\pi/2} \frac{d\theta}{\sqrt{1+\cos^2\theta}}.$$

Making the change of variables $t = \cos\theta$ gives

$$\Omega(E_\lambda) = 2\sqrt{2}\int_0^1 \frac{dt}{\sqrt{1-t^4}}.$$

Again, making the change of variables $u = t^4$ gives

$$\Omega(E_{1/2}) = \frac{\sqrt{2}}{2}\int_0^1 u^{-3/4}(1-u)^{-1/2}\,du.$$

It is well-known that if $a, b \in \mathbb{R}$, $a, b \geq 0$, then

$$\int_0^1 t^{a-1}(1-t)^{b-1} = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

Hence,

$$\Omega(E_{1/2}) = \frac{\sqrt{2}}{2}\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)}.$$

Now, using that $\Gamma(1/2) = \sqrt{\pi}$, and $s\Gamma(s) = \Gamma(s+1)$, it is easy to see that

$$\frac{\sqrt{2}}{2}\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)} = \sqrt{2}\pi\frac{\Gamma(5/4)}{\Gamma(3/2)\Gamma(3/4)},$$

and the first result follows.

For the second result, note that making the change of variables $x_1 = 1/x$ in E_λ gives

$$\begin{aligned} y^2 &= (1/x_1)(1/x_1 - 1)(1/x_1 - \lambda) \\ y^2 &= \frac{\lambda}{x_1^4} x_1(x_1 - 1)(x_1 - 1/\lambda). \end{aligned}$$

Thus,

$$-a_p(E_{1/\lambda}) = \sum_{x \in \mathbb{F}_p} \phi_p\left(\lambda x_1(x_1 - 1)(x_1 - \lambda)\right) = -\phi_p(\lambda) a_p(E_\lambda).$$

Similarly, making the change of variables $x_1 = 1 - x$ in E_λ gives

$$\begin{aligned} y^2 &= (1 - x_1)(1 - x_1 - 1)(1 - x_1 - \lambda) \\ y^2 &= -x_1(x_1 - 1)(x_1 - (1 - \lambda)). \end{aligned}$$

Thus,

$$-a_p(E_{1-\lambda}) = \sum_{x \in \mathbb{F}_p} \phi_p\left(-x_1(x_1 - 1)(x_1 - \lambda)\right) = -\phi_p(-1) a_p(E_\lambda).$$

These two results yield that $-a_p(E_{1/2}) = -\phi_p(1/2) a_p(E_2) = -\phi_p(-1/2) a_p(E_{-1})$. Since $\phi_p(-1/2) = \phi_p(-2)$, it suffices to show that

$$-a_p(E_{-1}) = 2p \operatorname{Re} \binom{\chi_4}{\phi_p}.$$

First, suppose that $p \equiv 3 \pmod 4$. It is easy to see that in this case

$$\begin{aligned} -a_p(E_{-1}) &= \sum_{x=0}^{p-1} \phi_p(x^3 - x) = \sum_{x=0}^{p-1} \phi_p((-x)^3 - (-x)) \\ &= \sum_{x=0}^{p-1} \phi_p(-x^3 + x) = \phi_p(-1) \sum_{x=0}^{p-1} \phi_p(x^3 - x). \end{aligned}$$

Since $\phi_p(-1) = -1$, $-a_p(E_{-1}) = 0$. Now, if $p \equiv 3 \pmod 4$, then $\chi_4 = \chi^{(p-1)/4}$, for some primitive character χ. Since 4 does not divide $p-1$, we take $\chi_4 = \left(\chi^{(p-1)/2}\right)^{1/2} =$

$\sqrt{\phi_p}$. Thus,

$$\begin{aligned}
2\,\mathrm{Re}\left(J(\chi_4,\phi_p)\right) &= 2\,\mathrm{Re}\left(\sum_{x=1}^{p-1}\sqrt{\phi_p(x)}\phi_p(1-x)\right)\\
&= 2\,\mathrm{Re}\left(\sum_{\phi_p(x)=1}\phi_p(1-x)+i\sum_{\phi_p(x)=-1}\phi_p(1-x)\right)\\
&= 2\sum_{\phi_p(x)=1}\phi_p(1-x)=\sum_{x=1}^{p-1}\phi_p(1-x^2)\\
&= -\sum_{x=1}^{p-1}\phi_p(x^2-1)=\phi_p(-1)-\sum_{x=0}^{p-1}\phi_p(x^2-1)
\end{aligned}$$

It is easy to see that the number of solutions to $x^2-y^2=1$ is given by

$$\sum_{x=0}^{p-1}\left(1+\phi_p(x^2-1)\right).$$

It is also easy to see that the number of solutions is $p-1$. This gives

$$\sum_{x=0}^{p-1}\phi_p(x^2-1)=-1,$$

so

$$2\,\mathrm{Re}\left(J(\chi_4,\phi_p)\right)=\phi_p(-1)-\sum_{x=0}^{p-1}\phi_p(x^2-1)=-1-(-1)=0.$$

Thus, $0=2\,\mathrm{Re}\left(J(\chi_4,\phi_p)\right)=2p\,\mathrm{Re}\binom{\chi_4}{\phi_p}$, so the result holds when $p\equiv 3 \pmod 4$.

Now, suppose $p\equiv 1 \pmod 4$. From [3], pg. 306-307, the number of points on E_{-1} mod p is one more than the number of points on $u^2=v^4+4$. The number of points on this latter curve (counting the point at infinity) is

$$1+\left(p-1+\overline{\chi_4(-4)}J(\phi_p,\chi_4)+\chi_4(-4)\overline{J(\phi_p,\chi_4)}\right).$$

Since $J(\phi_p,\chi_4)=J(\chi_4,\phi_p)$, the number of points on E_{-1} is

$$p+1+2\,\mathrm{Re}\left(\overline{\chi_4(-4)}J(\chi_4,\phi_p)\right).$$

Note that

$$\chi_4(-4)=\chi_4(-1)\left(\chi_4(2)\right)^2=\chi_4(-1)\phi_p(2).$$

Recall that $\chi_4=\chi^{\frac{p-1}{4}}$, where χ is a Dirichlet character of order $p-1$. Let g be a primitive root modulo p such that $\chi(g)=e^{2\pi i/(p-1)}$. Then, $g^{\frac{p-1}{2}}=-1$ so $\chi(g^{\frac{p-1}{2}})=$

$\chi(-1) = -1$. Thus,

$$\chi_4(-1) = (\chi(-1))^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}.$$

If $p \equiv 1 \pmod 8$ then $\chi_4(-1) = 1$ and $\phi_p(2) = 1$. If $p \equiv 5 \pmod 8$ then $\chi_4(-1) = -1$ and $\phi_p(2) = -1$. Thus, the number of points on E_{-1} mod p is

$$p + 1 + 2\,\mathrm{Re}\,(J(\chi_4, \phi_p)) = p + 1 - a_p(E_{-1}),$$

and hence $-a_p(E_{-1}) = 2\,\mathrm{Re}\,(J(\chi_4, \phi_p))$, as desired. □

References

[1] G. E. Andrews, R. Askey, and R. Roy. *Special functions*, volume 71 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1999.

[2] J. Greene. Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.*, 301(1):77–101, 1987.

[3] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[4] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[5] K. Ono. Values of Gaussian hypergeometric series. *Trans. Amer. Math. Soc.*, 350(3):1205–1223, 1998.

[6] K. Ono. *Arithmetic of the Coefficients of Modular Forms and q-series*. CBMS Monographs. American Mathematical Society, in press.

[7] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

Department of Mathematics, University of Wisconsin, Madison, WI 53706

E-mail address: rouse@math.wisc.edu