Hypergeometric Functions

JIWU JANG

June 19 – 30, 2023

These are the notes I've taken for a series of lectures on hypergeometric functions, given by Brian Grove, at the 2023 Ross Mathematics Program at Otterbein College.

References

- Poonen's notes on Arithmetic Geometry
- Silverman-Tate - Rational Points on Elliptic Curves (UTM, for beginners)
- Silverman - The Arithmetic of Elliptic Curves, Advanced topics in the Arithmetic of Elliptic Curves (GTM, quite hard)

§1 Introduction

Here are some elementary expansions of commonly used functions, which would be helpful for later (as typical, we assume $x \in \mathbb{R}$):

$$\begin{aligned}
\sin(x) &= \sum_{k=0}^{\infty}(-1)^k \frac{x^{2k+1}}{(2k+1)!} \\
\cos(x) &= \sum_{k=0}^{\infty}(-1)^k \frac{x^{2k}}{(2k)!} \\
\tan^{-1}(x) &= \sum_{k=0}^{\infty}(-1)^k \frac{x^{2k+1}}{2k+1} \text{ where } x \in [-1,1] \\
-\ln(1-x) &= \sum_{k=0}^{\infty} \frac{x^{k+1}}{k+1} \\
e^x &= \sum_{k=0}^{\infty} \frac{x^k}{k!}
\end{aligned}$$

Now, our goal is to find a "master power series" of some sort.

Definition 1.1 (Pochhammer symbol)**.** Let $y \in \mathbb{Q}$ and $k \in \mathbb{N}$. Then define the *rising factorial* as

$$(y)_k := y(y+1)\dots(y+k-1)$$

where $(y)_0 := 1$. (This is also called the *Pochhammer symbol.*)

Definition 1.2. Let $a, b, c \in \mathbb{Q}$ with $c \notin \mathbb{Z}^{\leq 0}$. Define the ${}_2F_1$ hypergeometric function to be

$${}_2F_1\left[\begin{matrix} a & b \\ & c \end{matrix}; z\right] := \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(1)_k (c)_k} z^k$$

with $z \in \mathbb{C}$ with $\|z\| < 1$. (By convention, there is always an implicit $(1)_k$.)

If $1 + c > a + b$, then the ${}_2F_1$ hypergeometric function is defined when $\|z\| = 1$.

Remark. The condition $c \notin \mathbb{Z}^{\leq 0}$ is there because we don't want to divide by zero :P

Example 1.3

Let $a = b = c = 1$, then we get ${}_2F_1\left[\begin{matrix} 1 & 1 \\ & 1 \end{matrix}; z\right] = \sum_{k=0}^{\infty} z^k$, the geometric series.

Claim — $\tan^{-1}(x) = x \cdot {}_2F_1\left[\begin{matrix} 1 & \frac{1}{2} \\ & \frac{3}{2} \end{matrix}; -x^2\right]$.

Proof. Note that $\tan^{-1}(x) = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1}$ where $x \in [-1, 1]$. Moreover,

$$\begin{aligned} & x \cdot {}_2F_1\left[\begin{matrix} 1, & \frac{1}{2} \\ & \frac{3}{2} \end{matrix}; -x^2\right] \\ &= \sum_{k=0}^{\infty} \frac{(1)_k (\frac{1}{2})_k}{(1)_k (\frac{3}{2})_k} (-1)^k x^{2k+1} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{2k+1} \end{aligned}$$

hence we are done. □

Example 1.4

Let $x = 1$, then $\frac{\pi}{4} = {}_2F_1\left[\begin{matrix} 1 & \frac{1}{2} \\ & \frac{3}{2} \end{matrix}; -1\right]$.

Definition 1.5. In general, we define the generalized hypergeometric function (GHF) to be

$${}_nF_{n-1}\left[\begin{matrix} a_1 & a_2 & a_3 & \dots & a_n \\ & b_2 & b_3 & \dots & b_n \end{matrix}; z\right] := \sum_{k=0}^{\infty} \frac{(a_1)_k (a_2)_k (a_3)_k, \dots, (a_n)_k}{(1)_k (b_2)_k (b_3)_k, \dots, (b_n)_k} z^k$$

Remark. This is often called the *sum definition* of the hypergeometric function. (As you would've probably guessed, there is an integral definition as well.)

Example 1.6

Here's another example of a hypergeometric function:

$${}_3F_2\left[\begin{matrix} a_1 & a_2 & a_3 \\ & b_2 & b_3 \end{matrix}; z\right] := \sum_{k=0}^{\infty} \frac{(a_1)_k (a_2)_k (a_3)_k}{(1)_k (b_2)_k (b_3)_k} z^k$$

Remark. Application of hypergeometric functions on elliptic curves.

§2 Elliptic curves

Definition 2.1. An elliptic curve over $\mathbb{Q}$ is an equation of the form $y^2 = x^3 + ax + b$ (whose discriminant is $\Delta = -16(4a^3 + 27b^2) \neq 0$), also satisfying the following properties:

- nonsingular
- projective
- existence of a $\mathbb{Q}$-rational point

Definition 2.2. A *singularity* is either a *node* (there exists a point with an "X-like" derivative) or a *cusp* (the curve is not smooth).

Example 2.3
$y^2 = x^3 + x$ is nonsingular ($\Delta = -64 \neq 0$).

For what comes below, let $\Bbbk$ be a field.

Definition 2.4. Define the *affine n-space* as $\mathbb{A}^n(\Bbbk) = \Bbbk^n$.

Remark. Technically you need more than this, but this suffices for our purposes.

Definition 2.5. Define the *projective n-space* as

$$\mathbb{P}^n(\Bbbk) = {}^{\Bbbk^{n+1} - \{\mathbf{0}\}}\!\big/\!_{\sim}$$

where $\sim$ is some equivalence relation and $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$ and $\lambda \in \Bbbk - \{\mathbf{0}\}$ is the determinant of $\sim$.

We want to make the equation for the elliptic curve to be nice, that is, to make the equation respect the projective n-space.

Remark. Goal: write a homogeneous equation for the elliptic curve.

Definition 2.6 (Homogenization)**.** We send $x \mapsto \frac{x}{z}$ and $y \mapsto \frac{y}{z}$, where $z \neq 0$. This homogenizes the equation.

Example 2.7
For $y^2 = x^3 + Ax + B$, it becomes $y^2 z = x^3 + Axz^2 + Bz^3$, so it's homogenized.

Example 2.8
Why $z \neq 0$? In projective space $\mathbb{P}^n(\Bbbk)$, we don't have $(0, 0, 0)$.

Let $z = 0$, in our previous example, then $x^3 = 0 \implies x = 0$, so we get $\mathcal{O} = (0, 1, 0)$, the point at infinity.

Definition 2.9. Let $E : y^2 = x^3 + Ax + B$. Then, define

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \text{ satisfies } E\} \cup \{\mathcal{O}\}$$

Theorem 2.10 (Bézout's theorem)
For a line L, we have that $L \cap E$ has exactly 3 intersection points (provided that we count multiple points and point at infinity).

Theorem 2.11
$E(\mathbb{Q})$ is an abelian group.

Proof. By Bézout's theorem, we call $P \star Q$ the third point on the line with P, Q.
Then, we take the second intersection point of the tangent of $P \star Q$ as $P + Q$, that is,

$$P + Q = \mathcal{O} \star (P \star Q)$$

Then, since the line-point labeling is not order-dependent, it is obviously abelian. □

Lemma 2.12
The identity of E is the point at infinity $\mathcal{O}$.

Proof. Obviously $P + \mathcal{O} = \mathcal{O} \star (P \star \mathcal{O}) = P$. □

Now, obviously we want $P + (-P) = \mathcal{O}$.

Lemma 2.13
The inverse of P, denoted as $(-P)$, is constructed as follows:
We take the tangent line from $\mathcal{O}$, whose intersection is $P \star (-P)$.

Proof. Note that we have

$$P + (-P) = \mathcal{O} \star (P \star (-P)) = \mathcal{O}$$

Thus, by construction, inverses are unique. □

> **Remark.** No one actually cares about the underlying lines once we prove that they form a group.

Definition 2.14. The Legendre form of E is the following:

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

where $\lambda \in \mathbb{Q} \setminus \{0, 1\}$.

Definition 2.15. An alternative form is to take $x \mapsto \frac{1}{\lambda}x$ and $y \mapsto \frac{1}{\lambda}y$, thus

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

Definition 2.16. Let $s \in \mathbb{C}$. Define

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$$

for $\Re(s) > 0$. An alternative definition is

$$\Gamma(s) = \lim_{k\to\infty} \frac{k^{s-1}k!}{(s)_k}$$

for $s \in \mathbb{C} \setminus \{\mathbb{Z}_{\leq 0}\}$. (Exercise: Prove that these two definitions are indeed equivalent.)

Example 2.17 (Facts about $\Gamma(s)$)

We have the following facts about $\Gamma(s)$:

- $\Gamma(1) = 1$
- $\Gamma(s+1) = s\Gamma(s)$ for $s \in \mathbb{C} \setminus \{\mathbb{Z}_{\leq 0}\}$ (functional equation)
- $\Gamma(k+1) = k!$
- $\Gamma(a+k) = (a)_k\Gamma(a)$
- ${}_2F_1\left[\begin{matrix} a & b \\ & c \end{matrix}; z\right] = \sum_{k=0}^{\infty} \frac{\Gamma(a+k)\Gamma(b+k)\Gamma(c)}{\Gamma(a)\Gamma(b)\Gamma(c+k)} \cdot \frac{2^k}{k!}$
- $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$, where $s \in \mathbb{C} \setminus \mathbb{Z}$
- $(1-z)^{-a} = \sum_{k=0}^{\infty} \frac{(a)_k}{k!}$ for $|z| < 1$
- $(a)_k = \frac{\Gamma(a+k)}{\Gamma(a)}$
- $\pi = \Gamma\left(\frac{1}{2}\right)^2 = B\left(\frac{1}{2}, \frac{1}{2}\right)$

Exercise 2.18. Prove the above facts.

Definition 2.19. Define $B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$, for $\Re(x), \Re(y) > 0$.

Exercise 2.20. Prove that $B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ for $x, y > 0$.

Theorem 2.21 (Differential forms of elliptic curves)

$$\int_0^1 \frac{dx}{\sqrt{x(1-x)(1-\lambda x)}} = \pi \cdot {}_2F_1\left[\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ & 1 \end{matrix}; \lambda\right] \text{ for } \lambda \in \mathbb{Q} \setminus \{0,1\}.$$

Proof. The proof is as follows:

$$\begin{aligned}
&\int_0^1 (x(1-x))^{-\frac{1}{2}}(1-\lambda x)^{-\frac{1}{2}}dx \\
&= \int_0^1 (x(1-x))^{-\frac{1}{2}} \left[\sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!}(\lambda x)^k\right] dx \\
&= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!}\lambda^k \int_0^1 x^{k-\frac{1}{2}}(1-x)^{-\frac{1}{2}}dx \\
&= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!}\lambda^k \int_0^1 x^{k+\frac{1}{2}-1}(1-x)^{\frac{1}{2}-1}dx \\
&= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!}\lambda^k B\left(k+\frac{1}{2},\frac{1}{2}\right) \\
&= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!}\frac{\Gamma\left(k+\frac{1}{2}\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma(k+1)}\lambda^k \\
&= \sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k}{k!k!}\lambda^k \Gamma\left(k+\frac{1}{2}\right)\Gamma\left(\frac{1}{2}\right) \\
&= \Gamma\left(\frac{1}{2}\right)^2 \sum_{k=0}^{\infty} \frac{\left(\frac{1}{2}\right)_k\left(\frac{1}{2}\right)_k}{k!k!}\lambda^k \\
&= \pi \cdot {}_2F_1\left[\begin{matrix}\frac{1}{2},\frac{1}{2}\\1\end{matrix};\lambda\right]
\end{aligned}$$

and we are done. □

Example 2.22

We denote ${}_2P_1\left[\begin{matrix}\frac{1}{2}\ \frac{1}{2}\\1\end{matrix};-1\right] = B(\frac{1}{2},\frac{1}{2})\cdot {}_2F_1\left[\begin{matrix}\frac{1}{2}\ \frac{1}{2}\\1\end{matrix};\lambda\right]$.

Definition 2.23. Define ${}_2F_1\left[\begin{matrix}a\ b\\c\end{matrix};z\right] := B(b,c-b)\cdot {}_2P_1\left[\begin{matrix}a\ b\\c\end{matrix};z\right]$.

Assume $c > b$, then

$$\begin{aligned}
&{}_2P_1\left[\begin{matrix}a,b\\c\end{matrix};z\right] = \frac{\Gamma(b)\Gamma(c-b)}{\Gamma(c)}\cdot {}_2F_1\left[\begin{matrix}a,b\\c\end{matrix};z\right] \\
&\implies {}_2P_1\left[\begin{matrix}a,b\\c\end{matrix};z\right] = \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-2t)^{-a}dt \text{ when } z\in\mathbb{C}\setminus[1,\infty) \\
&\implies {}_2F_1\left[\begin{matrix}a,b\\c\end{matrix};z\right] = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)}\int_0^1 t^{b-1}(1-t)^{c-b-1}(1-2t)^{-a}dt
\end{aligned}$$

Theorem 2.24 (Gauss)

If $c > b$ and $c-a-b > 0$, then

$$ {}_2F_1\left[\begin{matrix}a\ b\\c\end{matrix};1\right] = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}$$

Proof. By Abel continuity theorem, letting $z \to 1^-$,

$$\begin{aligned}
{}_2F_1\left[\begin{matrix} a, b \\ c \end{matrix}; 1\right] &= \frac{\Gamma c}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{(c-a-b)-1} \\
&= \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} B(b, c-a-b) \\
&= \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \cdot \frac{\Gamma(b)\Gamma(c-a-b)}{\Gamma(c-a)} \\
&= \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}
\end{aligned}$$

hence we are done. □

Example 2.25

Let $a = \frac{1}{2}$, $b = \frac{1}{2}$, $c = \frac{3}{2}$. Then, since $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ and $\Gamma(s+1) = s\Gamma(s)$, we have

$${}_2F_1\left[\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ \frac{3}{2} \end{matrix}; 1\right] = \Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{1}{2}\right) = \frac{\pi}{2}$$

hence $\Gamma\left(\frac{3}{2}\right) = \frac{\sqrt{\pi}}{2}$.

Theorem 2.26 (Pfaff transformation)

$${}_2F_1\left[\begin{matrix} a & b \\ c \end{matrix}; x\right] = (1-x)^{-a} {}_2F_1\left[\begin{matrix} a & c-b \\ c \end{matrix}; \frac{x}{x-1}\right].$$

Proof. We have ${}_2F_1\left[\begin{matrix} a & b \\ c \end{matrix}; x\right] = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-2t)^{-a} dt$.

Let $t \mapsto 1-s$, then

$$\begin{aligned}
{}_2F_1\left[\begin{matrix} a, b \\ c \end{matrix}; x\right] &= \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 s^{c-k-1}(1-s)^{b-1}(1-x)^{-a}(1+s(\frac{x}{1-x}))^{-a} \\
&= (1-x)^{-a} {}_2F_1\left[\begin{matrix} a, c-b \\ c \end{matrix}; \frac{x}{x-1}\right]
\end{aligned}$$

and we are done. □

Theorem 2.27 (Euler)

$${}_2F_1\left[\begin{matrix} a & b \\ c \end{matrix}; x\right] = (1-x)^{c-a-b} {}_2F_1\left[\begin{matrix} c-a & c-b \\ c \end{matrix}; x\right].$$

Theorem 2.28 (Binet's formula)

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Exercise 2.29. Prove $F_{-n} = (-1)^{n-1}F_n$. (Use Binet's formula or induction)

Remark. Hypergeometric functions are recursive by nature.

Theorem 2.30 (Dilcher)

Let $a = \frac{1-n}{2}$ and $z = \sqrt{5}$. Then,

$$
\begin{aligned}
{}_2F_1\left[\begin{matrix} \frac{1-n}{2}, 1-\frac{n}{2} \\ \frac{3}{2} \end{matrix}; 5\right] &= \frac{1}{2n\sqrt{5}}\left[(1+\sqrt{5})^n - (1-\sqrt{5})^n\right] \\
\implies F_n &= \frac{n}{2^{n-1}} \cdot {}_2F_1\left[\begin{matrix} \frac{1-n}{2}, 1-\frac{n}{2} \\ \frac{3}{2} \end{matrix}; 5\right]
\end{aligned}
$$

Here are some other folklore theorems, mainly for fun:

Theorem 2.31

$$
{}_2F_1\left[\begin{matrix} a \ \ a+\frac{1}{2} \\ \frac{3}{2} \end{matrix}; z^2\right] = \frac{1}{2z(1-2a)}\left[(1+z)^{1-2a} - (1-z)^{1-2a}\right]
$$

Theorem 2.32

$$
{}_2F_1\left[\begin{matrix} a \ \ a+\frac{1}{2} \\ \frac{1}{2} \end{matrix}; z\right] = \frac{1}{2}\left[(1+\sqrt{z})^{-2a} + (1-\sqrt{z})^{-2a}\right]
$$

Exercise 2.33. For $C_n = \dfrac{1}{n+1}\dbinom{2n}{n}$, show that $C_n = {}_2F_1\left[\begin{matrix} 1-n \ \ -n \\ 2 \end{matrix}; 1\right]$.

Proof. Expand by definition, then represent the summation as

$$
\sum_{k=0}^{n} \frac{\binom{n}{k}\binom{n}{n-k-1}}{n}
$$

which is just $\frac{\binom{2n}{n}}{n+1}$ by Vandermonde's identity. □

§3 Relation with the Riemann zeta function

Definition 3.1 (Riemann, 1859)**.** Define the Riemann zeta function as

$$
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}}
$$

for $\Re(s) > 1$.

Example 3.2 (Basel problem)

For example, $\zeta(2) = \frac{\pi^2}{6}$.

Note that $\pi = {}_2F_1\left[\begin{matrix} 1 \ \frac{1}{2} \\ \frac{3}{2} \end{matrix}; -1\right]$, so

$$\zeta(2) = \frac{1}{6}\left({}_2F_1\left[\begin{matrix} 1 \ \frac{1}{2} \\ \frac{3}{2} \end{matrix}; -1\right]\right)^2$$

Definition 3.3. Let $B_0 = 1$ and $\displaystyle\sum_{k=0}^{n-1}\binom{n}{k}B_k = 0.$

$B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, ...

Exercise 3.4. Prove that $B_{2k+1} = 0$ for $k \geq 1$.

We may write $\zeta(2k) = \dfrac{(-1)^{k+1}B_{2k}(2\pi)^{2k}}{2(2k)!}$ for $k \in \mathbb{N}$.

Remark. Special ζ values $\leftrightarrow$ Bernoulli numbers $\overset{\text{Byrd}}{\leftrightarrow}$ Fibonacci numbers $\overset{\text{Dilcher}}{\leftrightarrow}$ Truncated ${}_pF_q$'s.

Theorem 3.5 (Byrd)

If $N \geq 0$, then

$$F_{2N+2} = 2\sum_{k=0}^{N} A_{2k,N}B_{2k}$$

where

$$A_{2k,N} = \sum_{n=0}^{N-k}\binom{2N+1-n}{n}\binom{2N+1-2n}{2k}\frac{1}{2N-2n-2k+2}$$

We also have $B_2 = \frac{F_4}{2} - \frac{4}{3}$ and

$$\begin{aligned} F_4 &= \frac{1}{2}{}_2F_1\left[\begin{matrix} -\frac{3}{2}, -1 \\ \frac{3}{2} \end{matrix}; 5\right] \\ \implies B_2 &= \frac{1}{4}{}_2F_1\left[\begin{matrix} -\frac{3}{2}, -1 \\ \frac{3}{2} \end{matrix}; 5\right] - \frac{4}{3} \implies \zeta(2) \\ &= \left(\frac{1}{4}{}_2F_1\left[\begin{matrix} -\frac{3}{2}, -1 \\ \frac{3}{2} \end{matrix}; 5\right] - \frac{4}{3}\right)\cdot\left({}_2F_1\left[\begin{matrix} -1, \frac{1}{2} \\ \frac{3}{2} \end{matrix}; -1\right]\right)^2 \end{aligned}$$

thus

$$\zeta(4) = \left(\frac{64}{3}{}_2F_1\left[\begin{matrix} -\frac{3}{2} \ -1 \\ \frac{3}{2} \end{matrix}; 5\right] - \frac{11392}{45}\cdot\left({}_2F_1\left[\begin{matrix} 1 \ \frac{1}{2} \\ \frac{3}{2} \end{matrix}; -1\right]\right)^4\right)$$

and by using $\zeta(s) = \zeta(1-s)$ and $\zeta(-k) = \dfrac{(-1)^{k+1}B_{k+1}}{k+1}$, we have

$$\zeta(-1) = \frac{2}{3} - \frac{1}{8}\cdot{}_2F_1\left[\begin{matrix} -\frac{3}{2}, -1 \\ \frac{3}{2} \end{matrix}; 5\right] = -\frac{1}{12}$$

$$\zeta(-3) = \frac{89}{120} - \frac{1}{8}\cdot{}_2F_1\left[\begin{matrix} -\frac{3}{2}, -1 \\ \frac{3}{2} \end{matrix}; 5\right] = \frac{1}{120}$$

Example 3.6

We have $L_p \equiv 1 \pmod{p}$ and $F_p \equiv \left(\frac{p}{s}\right) \pmod{p}$ (we can relate it to B_k, then to $\zeta(s)$ as well.). The relation chain is basically ${}_2F_1 \to F_n \to B_k \to \zeta$.

Example 3.7 (${}_pF_q$ in the p-adics)

$${}_2F_1\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; x\right]_{p-1} = \sum_{k=0}^{p-1} \frac{(\frac{1}{2})_k(\frac{1}{2})_k}{k!k!} x^k.$$

Lemma 3.8

The multiplicative group of a field is cyclic.

Definition 3.9. Let $\varphi : G \to H$ and $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character.

Example 3.10

Let $p = 5$, that is, in $\mathbb{F}_5^\times$. Then, $\chi : \mathbb{F}_5^\times \to \mathbb{C}^\times$. $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$, $\chi(4) = \chi(2)\chi(2) = -1$.

Example 3.11

One example of a character is the trivial character $\varepsilon : \mathbb{F}_p^\times \to \mathbb{C}^\times$, where $\varepsilon \equiv 1$.

Example 3.12

The Legendre symbol ϕ is a character.

Example 3.13

$\widehat{\mathbb{F}_p^\times}$ is the group of characters on $\mathbb{F}_p^\times$.

Lemma 3.14

There are two different types of character sums:

- Fix χ. Then,

$$\sum_{q \in \mathbb{F}_p^\times} \chi(q) = \begin{cases} p-1 & \chi = \varepsilon \\ 0 & \text{otherwise} \end{cases}$$

- Fix $q \in \mathbb{F}_p^\times$. Then,

$$\sum_{\chi \in \mathbb{F}_p^\times} \chi(q) = \begin{cases} p-1 & q = e \\ 0 & \text{otherwise} \end{cases}$$

Example 3.15

For $a_1 = \frac{1}{2}$, we have $\chi = \omega^{\frac{p-1}{2}} = \phi$, which is the Legendre symbol.

Example 3.16

For $a_1 = \frac{3}{4}$, we have $\chi = \omega^{\frac{3(p-1)}{4}} = \eta$.

§4 Finite fields

Definition 4.1. Let ω be a generator of $\widehat{\mathbb{F}_p^\times}$, that is,

$$\widehat{\mathbb{F}_p^\times} = \langle \omega \rangle$$

Then, define $A := \omega^{(p-1)a}$ and $B := \omega^{(p-1)b}$.

The following are the finite field analogs of classical hypergeometric functions:

Classical	Finite fields
$a \in \mathbb{Q}$	$\chi = \omega^{(p-1)a}$
$-a$	$\overline{\chi}$
$\Gamma(a) = \int_0^\infty t^{a-1}e^{-t}dt$	$g(A) = \sum_{x \in \mathbb{F}_p^\times} A(x)\zeta_p^\times$ where $A(a) = \omega^{(p-1)a}$
$\Gamma(a)\Gamma(1-a) = \frac{\pi}{\sin(\pi a)}$	$g(A)g(\overline{A}) = A(-1)p$ if $A \neq \varepsilon$
$B(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt$	$J(A,B) = \sum_{x \in \mathbb{F}_p^\times} A(x)B(1-x)$
$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$	$J(A,B) = \frac{g(A)g(B)}{g(AB)}$ if $AB \neq \varepsilon$
x^a	$A(x)$
$a+b$	AB

Table 1: Finite field analogs of classical hypergeometric functions.

Theorem 4.2 (Beukers, Coher, Mellit, 2015)

A hypergeometric function over $\mathbb{F}_p$ looks like:

$$\begin{aligned} H_p\left[\begin{matrix} a,b \\ c \end{matrix}; \lambda\right] &:= \sum_{k=0}^{p-2} \frac{g(A\omega^k)g(B\omega^k)g(\overline{C\omega^k})}{g(\varepsilon)g(A)g(B)g(\overline{C})}\chi(\lambda) \\ &= \frac{1}{1-p}\sum_{x \in \widehat{\mathbb{F}_p^\times}} \frac{g(Ax)g(Bx)g(\overline{Cx})}{g(\varepsilon)g(A)g(B)g(\overline{C})}\chi(\lambda) \quad \text{where } x = \omega^k \\ &= \frac{1}{J(B, C\overline{B})}\sum_{x \in \mathbb{F}_p^\times} B(x)C\overline{B}(1-x)\overline{A}(1-\lambda x) \end{aligned}$$

Definition 4.3. Over $\mathbb{F}_{p^r}$, we define $\Phi(x) = \zeta_p^{\mathrm{Tr}(x)}$, where $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}$.

Theorem 4.4

We have $g(A)g(\overline{A}) = A(-1)p - (p-1)\delta(A)$, where

$$\delta(A) = \begin{cases} 1 & \text{if } A = \varepsilon \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $\Phi(x) = \zeta_p^{\times}$. Then,

$$\begin{aligned}
g(A)g(\overline{A}) &= \sum_{x \in \mathbb{F}_p^\times} A(x)\Phi(x) \cdot \sum_{y \in \mathbb{F}_p^\times} A\left(\frac{1}{y}\right)\Phi(y) \\
&= \sum_{x,\, y \in \mathbb{F}_p^\times} A\left(\frac{x}{y}\right)\Phi(x+y) \\
&= \sum_{x,\, t \in \mathbb{F}_p^\times} A(t)\ \Phi\left(x\left(1+\frac{1}{t}\right)\right) \quad \text{where } t = \frac{x}{y} \\
&= \sum_{t \in \mathbb{F}_p^\times,\, t \neq -1} A(t) \sum_{x \in \mathbb{F}_p^\times} \Phi\left(x\left(1+\frac{1}{t}\right)\right) + A(-1)\sum_{x \in \mathbb{F}_p^\times} \Phi(0) \\
&= A(-1) + A(-1)(p-1) \\
&= A(-1) \cdot p
\end{aligned}$$

since

$$\sum_{t \in \mathbb{F}_p^\times} A(t) = 0$$

$$\sum_{t \in \mathbb{F}_p^\times} A(t) = -A(-1)$$

$$\sum_{x \in \mathbb{F}_p} \Phi\left(x\left(1+\frac{1}{t}\right)\right) = 0$$

and

$$\sum_{x \in \mathbb{F}_p^\times} \Phi\left(x\left(1+\frac{1}{t}\right)\right) = -1$$

thus we are done. $\square$

To finish this section, we state a folklore theorem on hypergeometric functions over finite fields:

Theorem 4.5

$$H_p\left[\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ & 1 \end{matrix}; \lambda\right] = \frac{1}{1-p} \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \frac{g(\phi\chi)g(\phi\chi)g(\overline{\chi})}{g(\varepsilon)g(\phi)g(\phi)g(\varepsilon)} \chi(\lambda)$$

§5 Algebraic hypergeometric functions

Definition 5.1. Let $\boldsymbol{\alpha} = \{a_1, a_2, \dots, a_n\}$ and $\boldsymbol{\beta} = \{b_1, b_2, \dots, b_n\}$, where $a_1 \le a_2 \le \dots \le a_n$ and $b_1 \le b_2 \le \dots \le b_n$. We say $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ *interlace* if one of the following two cases hold:

- $a_1 < b_1 < a_2 < b_2 < \dots < a_n < b_n$
- $b_1 < a_1 < b_2 < a_2 < \dots < b_n < a_n$

Theorem 5.2 (Beukers-Heckman, 1975)
The data $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ is algebraic if and only if $\boldsymbol{\alpha}, \boldsymbol{\beta}$ interlace.

Example 5.3
$H_p\left[\begin{matrix}\frac{1}{3} & \frac{2}{3} \\ & \frac{1}{2}\end{matrix}; \lambda\right]$ is algebraic, since $\boldsymbol{\alpha} = \{\frac{1}{3}, \frac{2}{3}\}$ and $\boldsymbol{\beta} = \{1, 1\}$ interlace.

Theorem 5.4 (Multiplication formula)
Let $m \in \mathbb{N}$. Then
$$\prod_{\chi \in \widehat{\mathbb{F}_p^\times}\ \chi^m = \varepsilon} \frac{g(A\chi)}{g(\chi)} = -g(A^m)A(m^{-m})$$

Theorem 5.5 (Special case)
If $m = 2$, then $g(A)g(\phi A) = g(A)g(\phi)\overline{A}(4)$, where ϕ is the quadratic character.

Theorem 5.6

$$H_p\left[\begin{matrix}\frac{1}{4} & \frac{3}{4} \\ & \frac{1}{2}\end{matrix}; \lambda\right] = \left(\frac{1+\phi(\lambda)}{2}\right)\left[\phi(1+\sqrt{\lambda}) + \phi(1-\sqrt{\lambda})\right]$$

where $\phi(x) = x^{\frac{p-1}{2}}$ is the quadratic character, and $p \equiv 1 \pmod 4$.

Proof. Note that H_p collapses to 0 if λ is not a square mod p, due to the $\frac{1+\phi(\lambda)}{2}$ term. Otherwise, let $\lambda \neq 0$ be a quadratic residue mod p and η_4 be a character of order 4. Then, we have $\frac{1+\phi(\lambda)}{2} = 1$. Before proving the main result, we first need a lemma:

Lemma 5.7 (Double-angle formula)
$g(A)g(\phi A) = g(A^2)g(\phi)\overline{A}(4)$.

Now, we have

$$
\begin{aligned}
H_p\left[\begin{matrix}\frac14,\frac34\\ \frac12\end{matrix};\lambda\right] &= \frac{1}{p-1}\sum_{\chi}\frac{g(\eta_4\chi)g(\overline{\eta}_4)g(\overline{\chi})g(\phi\overline{\chi})}{g(\eta_4)g(\overline{\eta}_4)g(\phi)}\chi(\lambda)\\
&= \frac{1}{p-1}\sum_{\chi}\left(\frac{g(\chi^4)}{g(\chi)}\right)\left(\frac{g(\phi)}{g(\phi\chi)}\right)\left(\frac{g(\overline{\chi}g(\phi\overline{\chi}))}{g(\phi)}\right)\chi\left(\frac{\lambda}{256}\right) && \text{iterating over } \chi\in\{\phi,\varepsilon,\eta_4,\overline{\eta}_4\}\\
&= \frac{1}{p-1}\sum_{\chi}\frac{g(\chi^4)}{g(\chi^2)g(\phi)}g(\overline{\chi})g(\phi\overline{\chi})\chi\left(\frac{\lambda}{64}\right) && \text{by the double-angle formula with } A=\chi\\
&= \frac{1}{p-1}\sum_{\chi}\frac{g(\chi^4)}{g(\chi^2)g(\phi)}g(\overline{\chi}^2)g(\phi)\chi\left(\frac{\lambda}{16}\right) && \text{by the double-angle formula with } A=\overline{\chi}\\
&= \frac{1}{p-1}\sum_{\chi}\frac{g(\chi^4)g(\overline{\chi}^2)}{g(\chi^2)}\chi\left(\frac{\lambda}{16}\right)\\
&= \frac{1}{p-1}\sum_{\chi}\frac{g(\phi\chi^2)g(\overline{\chi}^2)}{g(\phi)}\chi(\lambda) && \text{by the double-angle formula with } A=\chi^2\\
&= \frac{1}{p-1}\sum_{\chi}\sum_{a\in\mathbb{F}_p\setminus\{0,1\}}\phi\chi^2(a)\overline{\chi}^2(1-a)\chi(\lambda) && \text{write as a Jacobi sum}\\
&= \frac{1}{p-1}\sum_{a\in\mathbb{F}_p\setminus\{0,1\}}\phi(a)\sum_{\chi}\chi\left(\frac{a^2\lambda}{(1-a)^2}\right) && \text{swap the order of summation}\\
&= \phi\left((1+\sqrt{\lambda})^{-1}+(1-\sqrt{\lambda})^{-1}\right) && \text{by evaluating cases where } \frac{a^2\lambda}{(1-a)^2}=1\\
&= \phi(1+\sqrt{\lambda})+\phi(1-\sqrt{\lambda})
\end{aligned}
$$

which is what we wanted to show. □

Example 5.8 (Beukers, Coher, Mellit, Grove)

$H_p\left[\begin{matrix}\frac13\ \frac23\\ \frac12\end{matrix};\lambda\right] = N_f(\lambda)-1$, where $N_f(\lambda)$ is the number of zeros of $f(x)=x^3+3x^2-4\lambda$ over $\mathbb{F}_p$.

Example 5.9 (Grove)

$H_p\left[\begin{matrix}\frac16\ \frac56\\ \frac12\end{matrix};\lambda\right] = \phi(\frac{\lambda}{27})(N_f(\lambda)-1)$ where ϕ is the quadratic character. This is basically immediate from the previous example, since if we add $\frac12$ (which is the equivalent of sending χ to $\phi(\chi)$, since ϕ is basically "$\frac12$" in $\mathbb{F}_p^\times$) and quotient $\mathbb{Z}$, we get this HG.

Remark. We implicitly define it in / $\mathbb{Q}$, where $\boldsymbol{\alpha}=\{a_1,\dots,a_n\}$ is / $\mathbb{Q}$ if $\prod_{i=1}^n(x-e^{2\pi i a_i})\in\mathbb{Z}[x]$.

§6 Hypergeometric moments

Example 6.1

The intuition comes from $\int_0^1 \frac{dx}{\sqrt{x(1-x)(1-\lambda x)}} = \pi \cdot {}_2F_1\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; \lambda\right]$.

> **Remark.** Certain H_p values have a relation with the points continuous on cubic curves over $\mathbb{F}_p$. Goal: count $\mathbb{F}_p$ solutions on $\tilde{E}$ = mod p reduction of E, where p is a good prime (i.e., doesn't make E singular).

$$\begin{aligned}|\tilde{E}(\mathbb{F}_p) &= 1 + \sum_{x\in\mathbb{F}_p}\left(1 + \left(\frac{x(1-x)(1-\lambda x)}{p}\right)\right) \quad \text{including } \mathcal{O}\text{, i.e., point at infty} \\ &= p + 1 + \sum_{x\in\mathbb{F}_p} \phi(x(1-x)(1-\lambda x))\end{aligned}$$

Definition 6.2. Define $a_p = -\sum_{x\in\mathbb{F}_p} \phi\left(x(1-x)(1-\lambda x)\right)$.

Definition 6.3. Denote $H_p(\lambda) = H_p\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; \lambda\right]$.

Definition 6.4. Good reduction refers to the reduced variety having the same properties as the original, for example, an algebraic curve having the same genus, or a smooth variety remaining smooth.

Claim 6.5 — $a_p = H_p\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; \lambda\right]$ for primes of *good reduction.*

Proof. Let $a = b = \frac{1}{2}$ and $c = 1$, so

$$\begin{aligned}H_p\left[\begin{matrix}\frac{1}{2}, & \frac{1}{2} \\ & 1\end{matrix}; \lambda\right] &= \frac{1}{J(\phi,\phi)} \sum_{x\in\mathbb{F}_p} \phi(x(1-x)(1-\lambda x)) \\ &= -\phi(-1) \sum_{x\in\mathbb{F}_p} \phi(x(1-x)(1-\lambda x)) = -\phi(-1)a_p\end{aligned}$$

hence $a_p = H_p\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; \lambda\right]$. □

Theorem 6.6 (Hasse bound)

For all H_p, we have $|H_p(\lambda)| \le 2\sqrt{p}$, or equivalently, $\frac{H_p(\lambda)}{\sqrt{p}} \in [-2, 2]$, which is referred to as the *Hasse bound.*

What is $\mathrm{End}(E)$? (For "nice" elliptic curves, since it forms an abelian group, $\mathrm{End}(E) \cong \mathbb{Z}$.)

Most of the time, $\mathrm{End}(E) \cong \mathbb{Z}$.

But sometimes, $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

Example 6.7

$y^2 = x^3 - x$, then the map $(x, y) \mapsto (-x, iy)$ gives us back the original curve.

Remark. E has complex multiplication (CM) if $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

Theorem 6.8 (Sato-Tate, 2011)

Fix E_λ that is not CM. Then, $\frac{H_p(\lambda)}{\sqrt{p}} \in [-2, 2]$ gives a semicircular distribution as $p \to \infty$.

Conjecture 6.9 (Sato-Tate for families, 2021)

Fix p. Let $\lambda \in \mathbb{F}_p \setminus \{0, 1\}$ vary in $\{E_\lambda\}$. Then, what is the distribution of $\frac{H_p(\lambda)}{\sqrt{p}} \in [-2, 2]$ as λ varies, for sufficiently large p? (Answer: semicircular.)

Take an "average" of the normalized H_p values. Let m be a fixed positive integer greater than 1. Consider the hypergeometric moment

$$\frac{1}{p} \sum_{\lambda \in \mathbb{F}_p} \left(\frac{H_p(\lambda)}{\sqrt{p}} \right)^m = \frac{1}{p^{\frac{m}{2}+1}} \sum_{\lambda \in \mathbb{F}_p} H_p(\lambda)^m$$

The expression is interesting (i.e., nontrivial) if $m > 1$, since for $m = 1$, it's basically orthogonality characters, so it sums to 0 or $p - 1$.

Theorem 6.10 (Ono-Saad-Saikia, 2021)

Let m be a fixed positive integer. Then,

$$\lim_{p \to \infty} \frac{1}{p^{\frac{m}{2}+1}} \sum_{\lambda \in \mathbb{F}_p} H_p(\lambda)^m = \begin{cases} 0 & \text{if } m \text{ is odd} \\ C(n) & \text{if } m = 2n \text{ for } n \in \mathbb{N} \end{cases}$$

where $C(n) = \frac{1}{n+1}\binom{2n}{n}$.

Proof. We have $H_p(\lambda) = -H_p(\frac{1}{\lambda})$ where $\lambda \in \mathbb{F}_p^\times$, so for $2 \nmid m$, everything cancels out nicely. $\square$

Theorem 6.11 (Grove)

Let m be a fixed positive integer. Then,

$$\lim_{p \to \infty} \frac{1}{p^{\frac{m}{2}+1}} \sum_{\lambda \in \mathbb{F}_p} H_p(\lambda^2)^m = \begin{cases} 0 & \text{if } m \text{ is odd} \\ C(n) & \text{if } m = 2n \text{ for } n \in \mathbb{N} \end{cases}$$

where $C(n) = \frac{1}{n+1}\binom{2n}{n}$.

Proof. We have $H_p(\lambda) = \phi(\lambda)H_p(1-\lambda)$ for $\lambda \in \mathbb{F}_p^\times$, so for $2 \nmid m$, everything cancels out nicely. $\square$

Theorem 6.12 (Grove)
Let m be a fixed positive integer. Then,

$$\lim_{p\to\infty} \frac{1}{p^{\frac{m}{2}+1}} \sum_{\lambda\in\mathbb{F}_p} H_p\begin{bmatrix} \frac{1}{3} & \frac{2}{3} & ; \lambda \\ & 1 & \end{bmatrix}^m = \begin{cases} 0 & \text{if } m \text{ is odd} \\ C(n) & \text{if } m = 2n \text{ for } n \in \mathbb{N} \end{cases}$$

where $C(n) = \frac{1}{n+1}\binom{2n}{n}$.

Remark. The high level intuition for this theorem comes from

$$\int_{SU(2)} (\mathrm{Tr}(X))^{2n} = C(n)$$

Theorem 6.13 (Ono-Saad-Saikia, 2021)
Let m be a fixed positive integer. Then,

$$\lim_{p\to\infty} \frac{1}{p^{m+1}} \sum_{\lambda\in\mathbb{F}_p} H_p\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & ; \lambda \\ & 1 & 1 & \end{bmatrix}^m = \begin{cases} 0 & \text{if } m \text{ is odd} \\ \sum_{i=0}^m (-1)^i \binom{m}{i} C(i) & \text{if } m \text{ is even} \end{cases}$$

Remark. Again, the high level intuition for this comes from

$$\int_{O(3)} (\mathrm{Tr}(X))^m = \sum_{i=0}^m (-1)^i \binom{m}{i} C(i)$$

§7 Finale

Finally, here is an open problem to think about:

Conjecture 7.1
Let m be a fixed positive integer. Then,

$$\lim_{p\to\infty} \frac{1}{p^{\frac{m}{2}+1}} \sum_{\lambda\in\mathbb{F}_p} H_p\begin{bmatrix} \frac{1}{6} & \frac{5}{6} & ; \lambda \\ & 1 & \end{bmatrix}^m = \begin{cases} 0 & \text{if } m \text{ is odd} \\ C(n) & \text{if } m = 2n \end{cases}$$