Variations on theorems of Mertens

Nobushige Kurokawa*   Hidekazu Tanaka†

September 16, 2022

Abstract

We present variations on theorems of Mertens as special cases of Density Hypothesis. Moreover, we study a Serre's estimate concerning Lang-Weil estimate.

1 Introduction

In 1874 Mertens [M] proved the following theorems:

Theorem A(Mertens) .

$$\prod_{p\le t}\left(1-\frac{1}{p}\right)\sim e^{-\gamma}(\log t)^{-1}$$

as $t\to\infty$, where p runs over prime numbers.

Theorem B(Mertens) .

$$\prod_{p:odd\ prime}\left(1-\frac{(-1)^{\frac{p-1}{2}}}{p}\right)=\frac{4}{\pi}.$$

In this paper we present an interpretation to these theorems as special cases of the following expectation:

Density Hypothesis(DH) . *Let X be an algebraic variety over the rational number field $\mathbb{Q}$. Define the density function for $t>0$ as*

$$||X||_t=\prod_{p\le t}\frac{|X(\mathbb{F}_p)|}{p^{\dim(X)}}.$$

*Department of Mathematics, Tokyo Institute of Technology
†6-15-11-202 Otsuka, Bunkyo-ku, Tokyo

Then there would exist a positive constant $C(X)$ and an integer $r(X)$ satisfying

$$||X||_t \sim C(X)(\log r)^{r(X)}$$

as $t \to \infty$.

Theorem 0. *Theorem A and Theorem B are cases*

(1) $X = \mathbb{G}_m = \mathrm{GL}(1)$

and

(2) $X = \mathcal{C} = \{(x, y)|x^2 + y^2 = 1\}$ *(circle).*

Proof of Theorem 0. (1) Let $X = \mathbb{G}_m = \mathrm{GL}(1)$. Then we have

$$|X(\mathbb{F}_p)| = |\mathrm{GL}(1, \mathbb{F}_p)| = p - 1.$$

Thus we have

$$\begin{aligned} ||X||_t = ||\mathrm{GL}(1)||_t &= \prod_{p \le t} \frac{|\mathrm{GL}(1, \mathbb{F}_p)|}{p} \\ &= \prod_{p \le t} (1 - p^{-1}). \end{aligned}$$

(2) Let $X = \{(x, y)|x^2 + y^2 = 1\}$. Then we have

$$|X(\mathbb{F}_p)| = \begin{cases} 2 & \cdots \quad p = 2, \\ p - 1 & \cdots \quad p \equiv 1 \bmod 4, \\ p + 1 & \cdots \quad p \equiv 3 \bmod 4. \end{cases}$$

Thus we have

$$\begin{aligned} ||X||_t &= \prod_{p \le t} \frac{|X(\mathbb{F}_p)|}{p} \\ &\sim \prod_{p\text{:odd prime}} \frac{p - (-1)^{\frac{p-1}{2}}}{p} \quad (t \to \infty). \end{aligned}$$

□

Hereafter we explain many examples satisfying DH. We remark that DH is quite difficult in general. For example let X be an abelian variety (e.g. elliptic curve), then DH is the original version of BSD [BS] with $r(X) = \mathrm{rank} X(\mathbb{Q})$ and it will imply the Riemann hypothesis for the associated L-function $L(s, X)$ as indicated by [G] (at least for $\dim(X) = 1$.) We remark that the Deep Riemann Hypothesis is studied in [KK, KKK].

Theorem 1 (GL(n))**.**

$$C(\mathrm{GL}(n)) = e^{-\gamma} \prod_{k=2}^{n} \zeta(k)^{-1}.$$
$$r(\mathrm{GL}(n)) = -1.$$

Theorem 2 (SL(n))**.**

$$C(\mathrm{SL}(n)) = \prod_{k=2}^{n} \zeta(k)^{-1}.$$
$$r(\mathrm{SL}(n)) = 0.$$

Theorem 3 (Sp(n))**.**

$$C(\mathrm{Sp}(n)) = \prod_{k=1}^{n} \zeta(2k)^{-1}.$$
$$r(\mathrm{Sp}(n)) = 0.$$

Theorem 4 ($\mathbb{A}^n$)**.**

$$C(\mathbb{A}^n) = 1.$$
$$r(\mathbb{A}^n) = 0.$$

Theorem 5 ($\mathbb{P}^n$)**.**

$$C(\mathbb{P}^n) = e^{\gamma} \zeta(n+1)^{-1}.$$
$$r(\mathbb{P}^n) = 1.$$

Theorem 6 ($\mathrm{Gr}(n,m) : n > m > 1$)**.**

$$C(\mathrm{Gr}(n,m)) = e^{\gamma} \frac{\prod_{k=2}^{m} \zeta(k)}{\prod_{k=n-m+1}^{n} \zeta(k)}.$$
$$r(\mathrm{Gr}(n,m)) = 1.$$

For a monic polynomial $f(x) \in \mathbb{Z}[x]$ we define

$$||f||_t = \prod_{p \le t} \frac{f(p)}{p^{\deg(f)}}$$

and study the property

$$||f||_t \sim C(f)(\log t)^{r(f)}$$

as $t \to \infty$. Then Theorems 1-6 are essentially reduced to the case of the cyclotomic polynomial Φ_n.

Theorem 7.

$$C(\Phi_n) = e^{-\gamma\mu(n)} \prod_{\substack{d|n \\ d>1}} \zeta(d)^{-\mu(\frac{n}{d})}.$$

$$\gamma(\Phi_n) = -\mu(n).$$

Now we recall a Serre's estimate [S] concerning Lang-Weil estimate [LW].

Theorem C(Serre) . *Let X be an algebraic variety over the rational number field $\mathbb{Q}$. Then we have*

$$\left| |X(\mathbb{F}_p)| - p^{\dim(X)} \right| \leq Bp^{\dim(X)-\frac{1}{2}},$$

where B is a constant independent of p.

We notice that $\left| |X(\mathbb{F}_p)| - p^{\dim(X)} \right| \leq Bp^{\dim(X)-\frac{1}{2}}$ can be written as

$$\left| \frac{|X(\mathbb{F}_p)|}{p^{\dim(X)}} - 1 \right| \leq \frac{B}{\sqrt{p}}.$$

Let $A(p)$ be a numerical sequence satisfying

$$\lim_{p\to\infty} \frac{A(p)}{p^d} = 1$$

with $d \in \mathbb{Z}_{\geq 0}$. Then we define

$$b(p) = \sqrt{p}\left(\frac{A(p)}{p^d} - 1\right),$$

that is,

$$\frac{A(p)}{p^d} = 1 + \frac{b(p)}{\sqrt{p}}.$$

We notice that by Theorem C $b(p)$ is finite ($|b(p)| \leq B$) if $b(p) = b_X(p)$ with $A(p) = |X(\mathbb{F}_p)|$.

Theorem 8 ($\mathbb{P}^n$)**.** *Let $X = \mathbb{P}^n$. Then*

$$b_X(p) = \frac{1}{\sqrt{p}} \frac{1 - p^{-n}}{1 - p^{-1}} (> 0).$$

Theorem 9 ($\mathbb{A}^n$)**.** *Let* $X = \mathbb{A}^n$. *Then*

$$b_X(p) = 0.$$

Theorem 10 (GL(1))**.** *Let* $X = \mathrm{GL}(1)$. *Then*

$$b_X(p) = -\frac{1}{\sqrt{p}}(< 0)$$

Theorem 11 (GL(2))**.** *Let* $X = \mathrm{GL}(2)$. *Then*

$$b_X(p) = -\frac{1}{\sqrt{p}} - \frac{1}{p\sqrt{p}} + \frac{1}{p^2\sqrt{p}}(< 0)$$

Theorem 12 (SL(2))**.** *Let* $X = \mathrm{SL}(2)$. *Then*

$$b_X(p) = -\frac{1}{p\sqrt{p}}(< 0)$$

The following theorem gives an example where $b(p)$ is not necessarily finite.

Theorem 13. *Let* $A(p) = p^d + p^{d-\frac{1}{3}}$. *Then* $b(p)$ *is not finite.*

Finally, we calculate $b_X(p)$ for elliptic curve X over $\mathbb{Q}$ with $A(p) = |X(\mathbb{F}_p)|$.

Theorem 14. *For sufficiently large* p *(*p *is "good") we have*

$$-2 < b_X(p) < 3.$$

2 Proof of Main results

Proof of Theorem 1. Using

$$|\mathrm{GL}(1, \mathbb{F}_p)| = p - 1$$

and Theorem A, we have

$$\begin{aligned} ||\mathrm{GL}(1)||_t &= \prod_{p \le t} \frac{|\mathrm{GL}(1, \mathbb{F}_p)|}{p} \\ &= \prod_{p \le t} \{(1 - p^{-1})\} \\ &\sim e^{-\gamma} \cdot (\log t)^{-1} \quad (t \to \infty). \end{aligned}$$

Let $n \geq 2$. Using

$$|\mathrm{GL}(n, \mathbb{F}_p)| = p^{n^2}(1-p^{-1})(1-p^{-2})\cdots(1-p^{-n})$$

and Theorem A, we have

$$\begin{aligned}
||\mathrm{GL}(n)||_t &= \prod_{p\leq t} \frac{|\mathrm{GL}(n,\mathbb{F}_p)|}{p^{n^2}} \\
&= \prod_{p\leq t}\{(1-p^{-1})(1-p^{-2})\cdots(1-p^{-n})\} \\
&= \prod_{p\leq t}(1-p^{-1}) \prod_{p\leq t}\{(1-p^{-2})\cdots(1-p^{-n})\} \\
&\sim e^{-\gamma} \prod_{k=2}^{n} \zeta(k)^{-1} \cdot (\log t)^{-1} \quad (t \to \infty).
\end{aligned}$$

□

Proof of Theorem 2. Using

$$\begin{aligned}
|\mathrm{SL}(n, \mathbb{F}_p)| &= \frac{|\mathrm{GL}(n,\mathbb{F}_p)|}{p-1} \\
&= \frac{p^{n^2}(1-p^{-1})(1-p^{-2})\cdots(1-p^{-n})}{p-1} \\
&= p^{n^2-1}(1-p^{-2})\cdots(1-p^{-n}),
\end{aligned}$$

we have

$$\begin{aligned}
||\mathrm{SL}(n)||_t &= \prod_{p\leq t} \frac{|\mathrm{SL}(n,\mathbb{F}_p)|}{p^{n^2-1}} \\
&= \prod_{p\leq t}\{(1-p^{-2})\cdots(1-p^{-n})\} \\
&\sim \prod_{k=2}^{n} \zeta(k)^{-1} \quad (t \to \infty).
\end{aligned}$$

□

Proof of Theorem 3. Using

$$|\mathrm{Sp}(n, \mathbb{F}_p)| = p^{n(2n+1)}(1-p^{-2})(1-p^{-4})\cdots(1-p^{-2n}),$$

we have

$$\begin{aligned}||\mathrm{Sp}(n)||_t &= \prod_{p\le t} \frac{|\mathrm{Sp}(n,\mathbb{F}_p)|}{p^{n(2n+1)}} \\ &= \prod_{p\le t}\{(1-p^{-2})(1-p^{-4})\cdots(1-p^{-2n})\} \\ &\sim \prod_{k=1}^{n} \zeta(2k)^{-1} \quad (t\to\infty).\end{aligned}$$

□

Proof of Theorem 4. Using

$$\mathbb{A}^n(\mathbb{F}_p) = (\mathbb{F}_p)^n,$$

we have

$$\begin{aligned}||\mathbb{A}^n||_t &= \prod_{p\le t} \frac{|\mathbb{A}^n(\mathbb{F}_p)|}{p^n} \\ &= 1 \\ &\sim 1 \quad (t\to\infty).\end{aligned}$$

□

Proof of Theorem 5. Using

$$|\mathbb{P}^n(\mathbb{F}_p)| = 1+p+\cdots+p^n = \frac{p^{n+1}-1}{p-1}$$

and Theorem A, we have

$$\begin{aligned}||\mathbb{P}^n||_t &= \prod_{p\le t} \frac{|\mathbb{P}^n(\mathbb{F}_p)|}{p^n} \\ &= \prod_{p\le t} \frac{1-p^{-(n+1)}}{1-p^{-1}} \\ &\sim \frac{e^\gamma}{\zeta(n+1)}\cdot \log t \quad (t\to\infty).\end{aligned}$$

□

Proof of Theorem 6. Using

$$|\mathrm{Gr}(n,m)(\mathbb{F}_p)| = \frac{(p^n-1)\cdots(p^{n-m+1}-1)}{(p^m-1)\cdots(p-1)}$$

and Theorem A, we have

$$\begin{aligned}
||\mathrm{Gr}(n,m)||_t &= \prod_{p\le t}\frac{|\mathrm{Gr}(n,m)(\mathbb{F}_p)|}{p^{m(n-m)}}\\
&= \prod_{p\le t}\frac{(1-p^{-(n-m+1)})\cdots(1-p^{-n})}{(1-p^{-1})\cdots(1-p^{-m})}\\
&\sim e^{\gamma}\frac{\zeta(2)\cdots\zeta(m)}{\zeta(n-m+1)\cdots\zeta(n)}\cdot\log t \quad (t\to\infty).
\end{aligned}$$

□

Proof of Theorem 7. Using

$$\Phi_n(t) = \prod_{d|n}(t^d-1)^{\mu(\frac{n}{d})}$$

and Theorem A, we have

$$\begin{aligned}
||\Phi_n||_t &= \prod_{p\le t}\frac{\Phi_n(p)}{p^{\deg(\Phi_n)}}\\
&= \prod_{p\le t}\frac{\prod_{d|n}(p^d-1)^{\mu(\frac{n}{d})}}{p^{\varphi(n)}}\\
&= \prod_{p\le t}\frac{\prod_{d|n}(p^d-1)^{\mu(\frac{n}{d})}}{p^{\sum_{d|n}\mu(\frac{n}{d})d}}\\
&= \prod_{p\le t}\prod_{d|n}(1-p^{-d})^{\mu(\frac{n}{d})}\\
&= \prod_{p\le t}(1-p^{-1})^{\mu(n)}\prod_{\substack{d|n\\ d>1}}(1-p^{-d})^{\mu(\frac{n}{d})}\\
&\sim (e^{-\gamma}(\log t)^{-1})^{\mu(n)}\prod_{\substack{d|n\\ d>1}}\zeta(d)^{-\mu(\frac{n}{d})} \quad (t\to\infty)\\
&= e^{-\gamma\mu(n)}\prod_{\substack{d|n\\ d>1}}\zeta(d)^{-\mu(\frac{n}{d})}\cdot(\log t)^{-\mu(n)}.
\end{aligned}$$

□

Proof of Theorem 8. Since

$$|X(\mathbb{F}_p)| = p^n + p^{n-1} + \cdots + 1,$$

we have

$$\begin{aligned}\frac{|X(\mathbb{F}_p)|}{p^n} &= 1 + \frac{1}{p} + \cdots + \frac{1}{p^n}\\ &= 1 + \frac{b_X(p)}{\sqrt{p}}.\end{aligned}$$

Thus we have

$$\begin{aligned}b_X(p) &= \sqrt{p}(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n})\\ &= \frac{1}{\sqrt{p}}(1 + \frac{1}{p} + \cdots + \frac{1}{p^{n-1}})\\ &= \frac{1}{\sqrt{p}}\frac{1-p^{-n}}{1-p^{-1}}.\end{aligned}$$

□

Proof of Theorem 9. Since

$$|X(\mathbb{F}_p)| = p^n,$$

we have

$$\begin{aligned}b_X(p) &= \sqrt{p}(\frac{|X(\mathbb{F}_p)|}{p^n} - 1)\\ &= 0.\end{aligned}$$

□

Proof of Theorem 10. Since

$$|X(\mathbb{F}_p)| = p - 1,$$

we have

$$\begin{aligned}\frac{|X(\mathbb{F}_p)|}{p} &= \frac{p-1}{p}\\ &= 1 - \frac{1}{p}\\ &= 1 + \frac{b_X(p)}{\sqrt{p}}.\end{aligned}$$

Thus we have

$$b_X(p) = -\frac{1}{\sqrt{p}}.$$

□

Proof of Theorem 11. Since

$$|X(\mathbb{F}_p)| = p^4(1-p^{-1})(1-p^{-2}),$$

we have

$$\begin{aligned}\frac{|X(\mathbb{F}_p)|}{p^4} &= (1-p^{-1})(1-p^{-2}) \\ &= 1 - p^{-1} - p^{-2} + p^{-3} \\ &= 1 + \frac{b_X(p)}{\sqrt{p}}.\end{aligned}$$

Thus we have

$$b_X(p) = -\frac{1}{\sqrt{p}} - \frac{1}{p\sqrt{p}} + \frac{1}{p^2\sqrt{p}}.$$

□

Proof of Theorem 12. Since

$$|X(\mathbb{F}_p)| = p^3(1-p^{-2}),$$

we have

$$\begin{aligned}\frac{|X(\mathbb{F}_p)|}{p^3} &= 1 - p^{-2} \\ &= 1 + \frac{b_X(p)}{\sqrt{p}}.\end{aligned}$$

Thus we have

$$b_X(p) = -\frac{1}{p\sqrt{p}}.$$

□

Proof of Theorem 13. Since

$$\begin{aligned}b(p) &= \sqrt{p}(\frac{A(p)}{p^d} - 1) \\ &= \sqrt{p}(\frac{p^d + p^{d-\frac{1}{3}}}{p^d} - 1) \\ &= p^{\frac{1}{6}},\end{aligned}$$

we have

$$\lim_{p\to\infty} b(p) = \infty.$$

□

Proof of Theorem 14. For

$$A(p) = |X(\mathbb{F}_p)| = p + 1 - a(p)$$

using Hasse's theorem on elliptic curves we can write

$$a(p) = 2\sqrt{p}\cos(\theta(p))$$

with $\theta(p) \in [0, \pi]$. So we obtain

$$\begin{aligned} b_X(p) &= \sqrt{p}(\frac{A(p)}{p} - 1) \\ &= \frac{1}{\sqrt{p}} - 2\cos(\theta(p)). \end{aligned}$$

Since $-2 \leq 2\cos(\theta(p)) \leq 2$, we have

$$\begin{aligned} b_X(p) &\leq \frac{1}{\sqrt{2}} + 2 < 3, \\ b_X(p) &> -2\cos(\theta(p)) \geq -2. \end{aligned}$$

□

References

[BS] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves II*, J. Reine Angew. Math. **218** (1965), 79-108.

[G] D. Goldfeld, *Sur les produits partiels eulériens attachés aux courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), 471-474.

[KK] S. Koyama and N. Kurokawa, *Chebyshev's Bias for Ramanujan's tau-function via the Deep Riemann Hypothesis*, *Proc. Japan Acad. Ser. A.*, **98** (2022), 35–39.

[KKK] I. Kaneko, S. Koyama and N. Kurokawa, *Towards the Deep Riemann Hypothesis for GL_n*, preprint (2022).

[LW] S. Lang and A. Weil, *Numbers of points of varieties in finite fields*, American J. of Math. **76** (1954), 819-827.

[M] F. Mertens, *Ueber einige asymptotische Gesetze der Zahlentheorie*, J. Reine Angew. Math. **77** (1874), 289-338.

[S] J.-P. Serre, *Lectures on* $N_X(p)$, 1st ed., Research Notes in Mathematics, vol. 11, CRC press, Boca Raton, (2011).