Advanced Studies in Pure Mathematics 49, 2007
Probability and Number Theory — Kanazawa 2005
pp. 455–478

The probability of two $\mathbb{F}_q$-polynomials to be coprime

Hiroshi Sugita[†] **and Satoshi Takanobu**[‡]

Abstract.

By means of the adelic compactification $\widehat{R}$ of the polynomial ring $R := \mathbb{F}_q[x]$, q being a prime, we give a probabilistic proof to a density theorem:

$$\frac{\#\{(m,n) \in \{0,1,\ldots,N-1\}^2\,;\, \varphi_m \text{ and } \varphi_n \text{ are coprime}\}}{N^2} \to \frac{q-1}{q},$$

as $N \to \infty$, for a suitable enumeration $\{\varphi_n\}_{n=0}^{\infty}$ of R. Then establishing a maximal ergodic inequality for the family of shifts $\{\widehat{R} \ni f \mapsto f+\varphi_n \in \widehat{R}\}_{n=0}^{\infty}$, we prove a strong law of large numbers as an extension of the density theorem.

§1. Introduction

Dirichlet [2] discovered a density theorem that asserts the probability of two integers to be coprime be $6/\pi^2$, that is,

(1)
$$\lim_{N\to\infty} \frac{\#\{(m,n) \in \mathbb{N}^2\,;\, 1 \le m,n \le N,\ \gcd(m,n)=1\}}{N^2} = \zeta(2)^{-1} = \frac{6}{\pi^2}.$$

The notion of density is something like a probability, but it is not exactly a probability. In order to give a rigorous probabilistic interpretation to this theorem, Kubota-Sugita [5] gave an adelic version of (1), that is, the probability of two adelic integers to be coprime is precisely $6/\pi^2$,

Received February 17, 2006.
Revised March 20, 2006.

2000 *Mathematics Subject Classification.* Primary 60B10; Secondary 60B15, 60F15.

[†] Partially supported by Grant-in-Aid for scientific research 16654021, MEXT of Japanese government.

[‡] Partially supported by Grant-in-Aid for scientific research 15340053, MEXT of Japanese government.

and they derived (1) from the adelic version. Soon after that, Sugita-Takanobu [11] established a strong law of large numbers (S.L.L.N. for short) in Kubota-Sugita [5]'s setting, and furthermore, discovered a new limit theorem which corresponds to the central limit theorem in usual cases.

In this paper, we discuss an analogy of these works for the polynomial ring $\mathbb{F}_q[x] =: R$, q being a prime, using again the adelic compactification $\widehat{R}$ of R. As a result, an S.L.L.N. holds in this case, too.

However, the proofs here are not a complete analogue of the previous ones. Indeed, in many points R and $\widehat{R}$ resemble $\mathbb{Z}$ and its adelic compactification $\widehat{\mathbb{Z}}$ respectively, but in some points they are quite different. For example, $\mathbb{Z}$ has a natural linear order, while R does not, so that we need to define an appropriate enumeration $R = \{\varphi_n\}_{n=0}^{\infty}$. And the family of shifts $\{x \mapsto x+n\}_{n=0}^{\infty}$ in $\widehat{\mathbb{Z}}$ forms a semigroup with respect to the addition of the parameter n, while the family of shifts $\{f \mapsto f+\varphi_n\}_{n=0}^{\infty}$ in $\widehat{R}$ does not, i.e., in general, $\varphi_m+\varphi_n \neq \varphi_{m+n}$. In particular, the latter is a strong obstacle in proving an S.L.L.N. (Theorem 2 below), which is finally overcome by adopting a modification of Stroock [10, § 5.3]'s method due to Miki [8].

§2. Summary of theorems

We here present three theorems as well as definitions and a lemma to state them. The proof of the theorems will be given in the following sections.

Definition 1. Let q be a prime, $\mathbb{F}_q := \mathbb{Z}/q\mathbb{Z} \cong \{0,1,\dots,q-1\}$ be the finite field consisting of q elements, and R be the ring of all $\mathbb{F}_q$-polynomials, i.e., $R := \mathbb{F}_q[x]$. We enumerate R as follows:

$$\varphi_n(x) := \sum_{i=1}^{\infty} b_i^{(q)}(n) x^{i-1}, \quad n = 0,1,2,\dots,$$

where $b_i^{(q)}(n) \in \{0,1,\dots,q-1\}$ denotes the i-th digit of n in its q-adic expansion, namely

$$n = \sum_{i=1}^{\infty} b_i^{(q)}(n) q^{i-1}, \quad n \in \mathbb{N} \cup \{0\}.$$

Both of infinite sums above are actually finite sums for each n.

The following density theorem is an analogue of (1).

Theorem 1. *The probability of two elements in R to be coprime is $(q-1)/q$. More precisely*[1]*,*

$$(2)\quad \lim_{N\to\infty} \frac{\#\{(m,n)\in\{0,1,\dots,N-1\}^2\,;\,\gcd(\varphi_m,\varphi_n)=1\}}{N^2} = \frac{q-1}{q}.$$

More generally, for any $f,g\in R$, we have

$$(3)\quad \lim_{N\to\infty} \frac{\#\{(m,n)\in\{0,1,\dots,N-1\}^2\,;\,\gcd(f+\varphi_m,g+\varphi_n)=1\}}{N^2} = \frac{q-1}{q}.$$

The limit $(q-1)/q$ appearing in Theorem 1 is equal to $\zeta_R(2)^{-1}$, where

$$\zeta_R(s) := \left(1-\frac{1}{q^{s-1}}\right)^{-1}$$

is the zeta function associated with R. See § 4 below.

Let us introduce the adelic compactification $\widehat{R}$ of R. We say $p\in R$ is *irreducible*, if it is not a constant (or, an element of $\mathbb{F}_q$) and if p cannot be divided by any $f\in R$ with $0<\deg f<\deg p$. Let $\mathcal{P}$ denote the set of all *monic* irreducible polynomials.

Definition 2. For each $p\in\mathcal{P}$, we define a metric d_p on R by

$$d_p(f,g) = \inf\{\,q^{-n\deg p}\,;\,p^n|(f-g)\,\},\quad f,g\in R.$$

Let R_p denote the completion of R by the metric d_p. It is a compact ring and has a unique Borel probability measure λ_p which is invariant under the shifts $\{R_p\ni f\mapsto f+g\}_{g\in R_p}$ (Haar probability measure).

Now we define

$$\widehat{R} := \prod_{p\in\mathcal{P}} R_p,\quad \lambda := \prod_{p\in\mathcal{P}}\lambda_p.$$

The arithmetic operation '+' and '×' being defined coordinate-wise, $\widehat{R}$ becomes a compact ring under the product topology. And λ becomes the unique Haar probability measure on $\widehat{R}$.

[1]The function '$\gcd(f,g)$' is assumed to return the greatest common divisor of f and g that is *monic*. In particular, if there is no common divisor other than constants (or, elements of $\mathbb{F}_q$), we have $\gcd(f,g)=1$ and say 'f and g are coprime'. When $f=g=0$, any monic polynomial is their common divisor, so we do not define $\gcd(0,0)$.

$\widehat{R}$ is metrizable with the following metric[2]:

$$d((f_1,f_2,\ldots),(g_1,g_2,\ldots)) := \sum_{i=1}^{\infty} 2^{-i} d_{p_i}(f_i,g_i), \qquad f=(f_1,f_2,\ldots),\ g=(g_1,g_2,\ldots)\in\widehat{R}.$$

Lemma 1. *The diagonal set* $D := \{\,(f,f,\ldots)\in\widehat{R}\,;\ f\in R\,\}$ *is dense in* $\widehat{R}$.

Proof. According to the Chinese remainder theorem, for any $k,m\in\mathbb{N}$ and any $f_1,\ldots,f_k\in R$, there exists $f\in R$ such that $f=f_i \bmod p_i^m$, $i=1,\ldots,k$. This implies that D is dense in $R\times R\times\cdots$ with respect to the metric d. □

Identifying R with D, we can regard R as a dense subring of $\widehat{R}$ by Lemma 1. Since R is countable, we have $\lambda(R)=0$.

Now we can mention an S.L.L.N.

Theorem 2. *For each* $F\in L^1(\widehat{R}^l,\lambda^l)$,

$$\lim_{N\to\infty}\frac{1}{N^l}\sum_{n_1,\ldots,n_l=0}^{N-1}F(f_1+\varphi_{n_1},\ldots,f_l+\varphi_{n_l}) = \int_{\widehat{R}^l}F(\hat{f}_1,\ldots,\hat{f}_l)\lambda^l(d\hat{f}_1\cdots d\hat{f}_l),\quad \lambda^l\text{-}a.e.(f_1,\ldots,f_l).$$

As a special case of Theorem 2, we have an S.L.L.N.-version of Theorem 1.

Definition 3. For $f,g\in\widehat{R}$, we define

$$\rho_p(f) := \begin{cases} 1 & (f\in p\widehat{R}),\\ 0 & (f\notin p\widehat{R}),\end{cases}$$

$$X(f,g) := \prod_{p\in\mathcal{P}}(1-\rho_p(f)\rho_p(g)).$$

Note that for $f,g\in R$, $X(f,g)=1$ if and only if $\gcd(f,g)=1$.

Theorem 3.

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}X(f+\varphi_m,g+\varphi_n)=\frac{q-1}{q},\quad \lambda^2\text{-}a.e.(f,g).$$

[2] We enumerate $\mathcal{P}=\{p_i\}_{i=1}^{\infty}$ in the order given by Definition 1.

§3. $\widehat{R}$ — Preliminaries

3.1. Basic properties

Although all lemmas in this subsection can be proved essentially in the same way as in the case of $\widehat{\mathbb{Z}}$, we give them proofs to make this paper self-contained.

Lemma 2. *Let $p, p' \in \mathcal{P}$, $p \neq p'$, and $k \in \mathbb{N}$.*
(i) *$p^k R_p$ is a closed and open ball.*
(ii) *$p^k R_{p'} = R_{p'}$.*

Proof. (i) That

$$\begin{aligned} p^k R_p &= \{f \in R_p\,;\, d_p(f,0) \leq q^{-k \deg p}\} \\ &= \{f \in R_p\,;\, d_p(f,0) < q^{-(k-1)\deg p}\} \end{aligned}$$

shows $p^k R_p$ is closed and open.
(ii) Since $p^k R_{p'} \subset R_{p'}$ is clear, we show the converse inclusion. To this end, it is sufficient to show the existence of $g \in R_{p'}$ for which $p^k g = 1$. For each $m \in \mathbb{N}$, there exists $g_m \in R$ such that $p^k g_m \equiv 1 \bmod (p')^m$, i.e., $d_{p'}(p^k g_m, 1) \leq q^{-m \deg p'}$. Then for $n > m$, we have $p^k(g_n - g_m) \equiv 0 \bmod (p')^m$, and hence

$$d_{p'}(p^k g_n, p^k g_m) \,=\, d_{p'}(g_n, g_m) \leq q^{-m \deg p'}.$$

This implies $\{g_m\}_{m=1}^{\infty}$ is a Cauchy sequence in $R_{p'}$. Then its limit $g \in R_{p'}$ satisfies

$$d_{p'}(p^k g, 1) \,=\, \lim_{m\to\infty} d_{p'}(p^k g_m, 1) \,=\, 0,$$

in other words, $p^k g = 1$. □

Lemma 3. *Let $f \in R$ and $\deg f \geq 1$.*
(i) *For*[3] $-\infty \leq \deg g \leq \deg f - 1$, *the set $(f\widehat{R} + g)$ is closed and open.*
(ii) $\widehat{R} = \cup_{g \in R;\, -\infty \leq \deg g \leq \deg f - 1} (f\widehat{R} + g)$, *which is a disjoint union.*

Proof. (i) We may assume f to be monic. Let $f = \prod_{p \in \mathcal{P}} p^{\alpha_p(f)}$ be the prime factor decomposition, where $\alpha_p(f) = 0$ holds except for finite number of $p \in \mathcal{P}$. By Lemma 2,

$$f\widehat{R} \,=\, \prod_{p \in \mathcal{P}} fR_p \,=\, \prod_{p \in \mathcal{P}} p^{\alpha_p(f)} R_p, \tag{4}$$

[3] $\deg 0 := -\infty$.

where each $p^{\alpha_p(f)}R_p$ is closed and open, and hence $f\widehat{R}$ is closed and open, too. Since the shift $\widehat{R} \ni f \mapsto (f+g) \in \widehat{R}$ is a homeomorphism, $(f\widehat{R}+g)$ is closed and open, too.

(ii) Since R is dense in $\widehat{R}$ and $h \mapsto fh+g$ is a continuous and closed mapping, we have $\overline{fR+g} = f\widehat{R}+g$. On the other hand, since $R = \bigcup_{g\in R;\,-\infty\le\deg g\le\deg f-1}(fR+g)$, we see

$$\widehat{R} = \bigcup_{\substack{g\in R;\\ -\infty\le\deg g\le\deg f-1}} (f\widehat{R}+g).$$

Let us next show that the above union is disjoint. Let g, g' be distinct polynomials both of which are of lower degree than f. By (i), $A := (f\widehat{R}+g)\cap(f\widehat{R}+g')$ is an open set. If $A \neq \emptyset$, then $R\cap A \neq \emptyset$, because R is dense in $\widehat{R}$. But then, for $l \in R\cap A$, we see that

$$d_p(l-g,0) \le p^{-\alpha_p(f)}, \quad d_p(l-g',0) \le p^{-\alpha_p(f)}, \quad p \in \mathcal{P},$$

which means that for any $p \in \mathcal{P}$, $p^{\alpha_p(f)}|(g-g')$. Thus we see $f|(g-g')$, which is impossible. Consequently, we must have $A = \emptyset$. □

Lemma 4. *For $f \in R\setminus\{0\}$ and $A \in \mathcal{B}(\widehat{R})$, we have $fA \in \mathcal{B}(\widehat{R})$ and that*

$$\lambda(fA) = q^{-\deg f}\lambda(A). \tag{5}$$

Proof. Since $\widehat{R}$ is a complete separable metric space and the multiplication $\widehat{R} \ni g \mapsto fg \in \widehat{R}$ is injective and Borel measurable, it holds that $fA \in \mathcal{B}(\widehat{R})$ (cf. [9, Chapter I Theorem 3.9]). Next, let ν be a Borel probability measure on $\widehat{R}$ defined by

$$\nu(A) = \frac{\lambda(fA)}{\lambda(f\widehat{R})}, \quad A \in \mathcal{B}(\widehat{R}).$$

Then ν is clearly shift invariant, and hence $\nu = \lambda$ by the uniqueness of the Haar measure. Thus we see $\lambda(fA) = \lambda(f\widehat{R})\lambda(A)$. Lemma 3 and the shift invariance of λ imply

$$1 = \lambda(\widehat{R}) = \sum_{\substack{g\in R;\\ -\infty\le\deg g\le\deg f-1}} \lambda(f\widehat{R}+g) = q^{\deg f}\lambda(f\widehat{R}),$$

from which (5) immediately follows. □

3.2. Zeta function associated with R

Let us define the zeta function associated with R:

$$\zeta_R(s) := \sum_{f\in R\,:\,\text{monic}} \frac{1}{N(f)^s}, \quad \operatorname{Re} s > 1, \tag{6}$$

where

$$N(f) := \text{the number of residue classes } R/fR = q^{\deg f}. \tag{7}$$

Since the polynomial ring R is a unique factorization domain, and

$$N(fg) = N(f)N(g),$$

we have an Euler product representation of ζ_R:

$$\zeta_R(s) = \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{N(p)^s}\right)^{-1} = \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{q^{s\deg p}}\right)^{-1}. \tag{8}$$

Surprisingly, the following extremely simple formula holds:

$$\zeta_R(s) = \left(1 - \frac{1}{q^{s-1}}\right)^{-1}. \tag{9}$$

Let us show (9). Let $g(m) := \sum_{d|m} \mu(\frac{m}{d})q^d$, where μ is the Möbius function. Then the Möbius inversion formula implies

$$q^n = \sum_{d|n} g(d), \quad n \in \mathbb{N}.$$

We must also recall that (See [7, 3.25. Theorem])

$$\#\{p \in \mathcal{P}; \deg p = m\} = \frac{1}{m} g(m).$$

Now noting that $\log(1-t)^{-1} = \sum_{n=1}^{\infty} \frac{t^n}{n}$ $(|t| < 1)$,

$$\begin{aligned}
\log \zeta_R(s) &= \sum_{p\in\mathcal{P}} \log\left(1 - \frac{1}{q^{s\deg p}}\right)^{-1} = \sum_{p\in\mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{n} \frac{1}{q^{ns\deg p}} \\
&= \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{n} \frac{1}{q^{smn}} \#\{p \in \mathcal{P}; \deg p = m\} = \sum_{m,n=1}^{\infty} \frac{1}{mn} \frac{1}{q^{smn}} g(m) \\
&= \sum_{l=1}^{\infty} \frac{1}{l} \frac{1}{q^{sl}} \sum_{m|l} g(m) = \sum_{l=1}^{\infty} \frac{1}{l} \left(\frac{1}{q^{s-1}}\right)^l
\end{aligned}$$

$$= \log \left(1 - \frac{1}{q^{s-1}}\right)^{-1}.$$

Thus we have (9).

Theorem 3 follows from the next lemma and Theorem 2.

Lemma 5.
$$\int_{\widehat{R}^2} X(f,g)\lambda^2(dfdg) \;=\; \frac{q-1}{q}.$$

Proof.

$$\begin{aligned}\int_{\widehat{R}^2} X(f,g)\lambda^2(dfdg) &= \prod_{p\in\mathcal{P}} \int_{\widehat{R}^2} (1-\rho_p(f)\rho_p(g))\lambda^2(dfdg) \\ &= \prod_{p\in\mathcal{P}} \left(1 - \int_{\widehat{R}} \rho_p(f)\lambda(df) \int_{\widehat{R}} \rho_p(g)\lambda(dg)\right) \\ &= \prod_{p\in\mathcal{P}} \left(1 - q^{-\deg p} q^{-\deg p}\right) \\ &= \prod_{p\in\mathcal{P}} \left(1 - q^{-2\deg p}\right).\end{aligned}$$

On the other hand, plugging $s = 2$ into (8) and (9), we see that

$$\prod_{p\in\mathcal{P}} \left(1 - q^{-2\deg p}\right)^{-1} \;=\; \zeta_R(2) \;=\; \left(1 - \frac{1}{q}\right)^{-1},$$

and hence

$$\int_{\widehat{R}^2} X(f,g)\lambda^2(dfdg) = \frac{1}{\zeta_R(2)} \;=\; \frac{q-1}{q}. \qquad \square$$

3.3. Uniform distributivity of $\{\varphi_n\}_{n=0}^{\infty}$ in $\widehat{R}$

We begin with a characterization of continuous functions on $\widehat{R}$.

Definition 4. Let $f \in \widehat{R}$ and $h \in R \setminus \{0\}$. When $\deg h \ge 1$, by Lemma 3(ii), there exists a unique $g \in R$ such that $-\infty \le \deg g \le \deg h - 1$ and $f - g \in h\widehat{R}$. This g is denoted by $f \bmod h$. When $\deg h = 0$, i.e., h is non-zero constant, we always set $f \bmod h := 0$.

Definition 5. A function $F : \widehat{R} \to \mathbb{R}$ is said to be *periodic*, if there exists $h \in R$, $\deg h \ge 1$, such that

(10)
$$F(f) \;=\; F(f \bmod h) \;=\; \sum_{\substack{g\in R;\\ -\infty\le\deg g\le\deg h-1}} F(g)\mathbf{1}_{h\widehat{R}+g}(f), \quad f \in \widehat{R}.$$

And $F : \widehat{R} \to \mathbb{R}$ is said to be *almost periodic*, if there exists a sequence $\{F_m\}_{m=1}^{\infty}$ of periodic functions that converges to F uniformly .

Lemma 6. *A function $F : \widehat{R} \to \mathbb{R}$ is continuous, if and only if it is almost periodic.*

Proof. Lemma 3 implies that periodic functions on $\widehat{R}$ are continuous, and hence their uniformly convergent limits, that is, almost periodic functions are continuous.

Conversely, let F be a continuous function on $\widehat{R}$. Since $\widehat{R}$ is compact, F is uniformly continuous, in particular, for any $\varepsilon > 0$, there is $\delta > 0$ such that for any $h \in R$, $d(0, h) < \delta$, and any $f \in \widehat{R}$, it holds that $|F(f) - F(f + h)| < \varepsilon$. Now fix such an $h \in R$, and define a periodic function F' by

$$F'(f) := F(f \bmod h), \quad f \in \widehat{R}.$$

Then we have $|F(f) - F'(f)| < \varepsilon$, $f \in \widehat{R}$. Thus F is almost periodic. □

We next introduce the following lemma, which shows an important property of our enumeration $\{\varphi_n\}_{n=0}^{\infty}$.

Lemma 7. *Let $m \in \mathbb{N}$ and let $h \in R$ be a monic polynomial of degree m. Then, for any $j \in \mathbb{N}$, $\{\varphi_n \bmod h\,;\, (j-1)q^m \le n < jq^m\}$ forms a complete residue system modulo h. Namely,*

$$\begin{aligned}\{\varphi_n \bmod h\,;\, (j-1)q^m \le n < jq^m\} &= \{g \in R\,;\, -\infty \le \deg g < m\}\\ &= \{\varphi_n\,;\, 0 \le n < q^m\}.\end{aligned}$$

Proof. This lemma is due to Hodges [4, p.71]. Since the enumeration $\{\varphi_n\}_{n=0}^{\infty}$ is systematic, we can present a shorter proof here. Let $j \in \mathbb{N}$ and let $(j-1)q^m \le n < jq^m$. According to the definition of $\{\varphi_n\}_{n=0}^{\infty}$, since

$$n = (n - (j-1)q^m) + (j-1)q^m, \quad 0 \le n - (j-1)q^m < q^m,$$

we have

$$\varphi_n = \varphi_{n-(j-1)q^m} + \varphi_{j-1}\varphi_{q^m},$$

where

$$\deg \varphi_{n-(j-1)q^m} < m, \quad \deg \varphi_{j-1}\varphi_{q^m} \begin{cases} \ge m & (j > 1), \\ = -\infty & (j = 1). \end{cases}$$

Noting that $r := \varphi_{j-1}\varphi_{q^m} \bmod h$ is of degree $< m$, we see that

$$\{\varphi_n \bmod h\,;\, (j-1)q^m \le n < jq^m\}$$

$$\begin{aligned}
&= \{(\varphi_{n-(j-1)q^m} + \varphi_{j-1}\varphi_{q^m}) \bmod h\,;\,(j-1)q^m \le n < jq^m\} \\
&= \{(\varphi_n + r) \bmod h\,;\, 0 \le n < q^m\} \\
&= \{\varphi_n\,;\, 0 \le n < q^m\}. \qquad \square
\end{aligned}$$

Since $\widehat{R}$ is compact and includes R densely, each continuous function $F : \widehat{R} \to \mathbb{R}$ is determined by its values on R. In particular, the integral of F is determined by the sequence $\{F(\varphi_n)\}_{n=0}^{\infty}$. The following lemma indicates this fact explicitly.

Lemma 8. *The sequence $\{\varphi_n\}_{n=0}^{\infty}$ is uniformly distributed in $\widehat{R}$, that is, for any continuous function $F : \widehat{R} \to \mathbb{R}$, it holds that*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} F(\varphi_n) = \int_{\widehat{R}} F(\hat{f})\lambda(d\hat{f}). \tag{11}$$

Proof.

<u>1°</u> Let F be a periodic function, that is, let us assume $F(f) = F(f \bmod h)$, $f \in \widehat{R}$, for some nonconstant monic $h \in R$. Then putting $m := \deg h$ and $j_0 := \left\lfloor \frac{N}{q^m} \right\rfloor$, Lemma 7 implies that

$$\begin{aligned}
&\frac{1}{N}\sum_{n=0}^{N-1} F(\varphi_n) \\
&\quad = \frac{1}{N}\sum_{n=j_0q^m}^{N-1} F(\varphi_n \bmod h) + \frac{1}{N}\sum_{j=1}^{j_0}\sum_{n=(j-1)q^m}^{jq^m-1} F(\varphi_n \bmod h) \\
&\quad = \frac{1}{N}\sum_{n=j_0q^m}^{N-1} F(\varphi_n \bmod h) + \frac{j_0}{N}\sum_{-\infty\le\deg g<m} F(g).
\end{aligned}$$

Letting $\{t\}$ denote the fractional part of $t > 0$,

$$\begin{aligned}
&\left|\frac{1}{N}\sum_{n=0}^{N-1} F(\varphi_n) - \frac{1}{q^m}\sum_{-\infty\le\deg g<m} F(g)\right| \\
&\quad = \left|\frac{1}{N}\sum_{n=j_0q^m}^{N-1} F(\varphi_n \bmod h) + \frac{1}{N}\left(\frac{N}{q^m} - \left\{\frac{N}{q^m}\right\}\right)\sum_{-\infty\le\deg g<m} F(g)\right. \\
&\qquad \left. - \frac{1}{q^m}\sum_{-\infty\le\deg g<m} F(g)\right|
\end{aligned}$$

$$\leq \frac{1}{N}\left\{q^m \max_{-\infty\leq \deg g<m}|F(g)| + \Bigl|\sum_{-\infty\leq\deg g<m} F(g)\Bigr|\right\}$$
$$\to 0 \quad \text{as } N\to\infty.$$

Thus (11) holds for periodic functions.

<u>2°</u> Let $F:\widehat{R}\to\mathbb{R}$ be a continuous function. By Lemma 6, for any $\varepsilon>0$, there is a periodic function F_ε such that $\|F-F_\varepsilon\|_\infty<\varepsilon$. By 1°,

$$\begin{aligned}
&\left|\frac{1}{N}\sum_{n=0}^{N-1}F(\varphi_n)-\int_{\widehat{R}}F(f)\lambda(df)\right|\\
&\quad=\left|\frac{1}{N}\sum_{n=0}^{N-1}(F(\varphi_n)-F_\varepsilon(\varphi_n))+\frac{1}{N}\sum_{n=0}^{N-1}F_\varepsilon(\varphi_n)-\int_{\widehat{R}}F_\varepsilon(f)\lambda(df)\right.\\
&\qquad\left.+\int_{\widehat{R}}(F_\varepsilon(f)-F(f))\lambda(df)\right|\\
&\quad\leq 2\varepsilon+\left|\frac{1}{N}\sum_{n=0}^{N-1}F_\varepsilon(f_n)-\int_{\widehat{R}}F_\varepsilon(f)\lambda(df)\right|\\
&\quad\to 0\quad(\text{first } N\to\infty, \text{ secondly } \varepsilon\to 0).
\end{aligned}$$

Thus (11) holds for continuous functions. □

The following corollary follows from Lemma 8 and [9, Chapter III Lemma 1.1].

Corollary 1. For any continuous function $F:\widehat{R}^2\to\mathbb{R}$, we have

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}F(\varphi_m,\varphi_n)\;=\;\int_{\widehat{R}^2}F(f,g)\lambda^2(df\,dg).$$

The assertion of Corollary 1 is referred to as *the weak convergence of the sequence of probability measures*[4] $\{\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}\}_{N=1}^{\infty}$ *to* λ^2. It is well-known that the weak convergence is equivalent to the following condition (cf. [10, § 3.1]): *For any closed set $K\subset\widehat{R}^2$, it holds that*

$$\limsup_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}(K)\;\leq\;\lambda^2(K). \tag{12}$$

[4] $\delta_{(\varphi_m,\varphi_n)}$ denotes the δ-measure at $(\varphi_m,\varphi_n)\in\widehat{R}^2$.

§4. Proof of density theorem

Although Theorem 1 could be proved in an elementary way, we here prove it in the light of probability theory by means of the adelic formulation. This section is an analogue of Kubota-Sugita [5, § 6].

If the function $X(f,g)$ were continuous on $\widehat{R}^2$, Corollary 1 would imply Theorem 1. However it is not continuous. Indeed,

$$B := X^{-1}(\{1\}) = \bigcap_{p\in\mathcal{P}} (\widehat{R}^2 \setminus (p\widehat{R})^2) \subset \widehat{R}^2$$

is surely a closed set, but we can show $B = \partial B$, which means that in any neighborhood of any point of B, there exists a point for which $X = 0$. Thus X is not continuous. That $B = \partial B$ is shown in the following way: Take any $(f,g) \in B$ and any $\varepsilon > 0$. Then choose $l, m \in \mathbb{N}$ so large that $d\left(0, \prod_{i=1}^{l} p_i^m\right) < \varepsilon$. Now find $h_1, h_2 \in R$ such that

$$\begin{cases} f \bmod p_{l+1} + h_1 \prod_{i=1}^{l} p_i^m \equiv 0 \pmod{p_{l+1}}, \\ g \bmod p_{l+1} + h_2 \prod_{i=1}^{l} p_i^m \equiv 0 \pmod{p_{l+1}}. \end{cases}$$

In fact, since $\prod_{i=1}^{l} p_i^m$ and p_{l+1} are coprime, there exists $k \in R$ such that $k\prod_{i=1}^{l} p_i^m \equiv 1 \pmod{p_{l+1}}$, so that $h_1 = k(p_{l+1} - f \bmod p_{l+1})$ and $h_2 = k(p_{l+1} - g \bmod p_{l+1})$ are required ones. Then it is easily seen that $d(f, f + h_1\prod_{i=1}^{l} p_i^m) < \varepsilon$, $d(g, g + h_2\prod_{i=1}^{l} p_i^m) < \varepsilon$, and that $(f + h_1\prod_{i=1}^{l} p_i^m, g + h_2\prod_{i=1}^{l} p_i^m) \notin B$. Thus $B \subset \partial B$.

Let us begin to prove (2) in Theorem 1. For each monic polynomial $h \in R$, we set

$$hB := \{(hf, hg) \in \widehat{R}^2 \,;\, (f,g) \in B\}.$$

Since $hB \cap R^2 = \{(f,g) \in R^2 \,; \gcd(f,g) = h\}$, it is easy to see that

(13)
$$\sum_{h\in R\,:\,\text{monic}} \delta_{(\varphi_m,\varphi_n)}(hB) = \begin{cases} 1, & (m,n) \in \{0,1,2,\ldots\}^2 \setminus \{(0,0)\}, \\ 0, & (m,n) = (0,0). \end{cases}$$

According to Lemma 5, $\lambda^2(B) = \int_{\widehat{R}^2} X(f,g)\lambda^2(dfdg) = (q-1)/q$. Hence by Lemma 4,

$$\lambda^2(hB) = \frac{1}{q^{2\deg h}} \cdot \frac{q-1}{q}.$$

Since hB is a closed set, (12) implies

$$\text{(14)}\qquad \frac{1}{q^{2\deg h}}\cdot\frac{q-1}{q} \;=\; \lambda^2(hB) \;\geq\; \limsup_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}(hB).$$

Note that by (6), (7) and (9) with $s=2$, we have

$$\text{(15)}\qquad \sum_{h\in R\,:\,\text{monic}}\frac{1}{q^{2\deg h}} \;=\; \frac{q}{q-1}.$$

Also, since, for $\nu\geq 0$ and $\varphi\in R$

$$-\infty \underset{(<)}{\leq} \deg\varphi\leq\nu \iff \varphi\in\big\{\varphi_m\,;\,0\underset{(<)}{\leq} m\leq q^{\nu+1}-1\big\},$$

we see that for $N\in\mathbb{N}\cap[2,\infty)$, taking $\nu\in\mathbb{N}\cup\{0\}$ so that $q^\nu\leq N-1<q^{\nu+1}$,

$$\begin{aligned}
\frac{1}{N^2}\sum_{m,n=1}^{N-1}\delta_{(\varphi_m,\varphi_n)}(hB) &\leq \frac{1}{N^2}\sum_{m,n=1}^{N-1}\delta_{(\varphi_m,\varphi_n)}(h\widehat{R}^2)\\
&\leq \frac{1}{(q^\nu+1)^2}\sum_{m,n=1}^{q^{\nu+1}-1}\delta_{(\varphi_m,\varphi_n)}(hR\times hR)\\
&= \left(\frac{1}{q^\nu+1}\sum_{m=1}^{q^{\nu+1}-1}\delta_{\varphi_m}(hR)\right)^2\\
&= \left(\frac{\#\{1\leq m\leq q^{\nu+1}-1\,;\,h\mid\varphi_m\}}{q^\nu+1}\right)^2\\
&= \left(\frac{\#\{\varphi\in R\,;\,-\infty<\deg\varphi\leq\nu,\ h\mid\varphi\}}{q^\nu+1}\right)^2\\
&= \left(\frac{\#\{k\in R\setminus\{0\}\,;\,\deg(hk)\leq\nu\}}{q^\nu+1}\right)^2\\
&= \left(\frac{\#\{k\in R\,;\,-\infty<\deg k\leq\nu-\deg h\}}{q^\nu+1}\right)^2\\
&= \begin{cases}\left(\dfrac{q^{\nu-\deg h+1}-1}{q^\nu+1}\right)^2, & \nu\geq\deg h,\\ 0, & \nu<\deg h\end{cases}
\end{aligned}$$

$$\leq \frac{q^2}{q^{2\deg h}}.$$

Here the last expression is summable in $h \in R$, monic. Then it follows from (15), (14) and the Lebesgue-Fatou theorem that

$$\begin{aligned}(16)\qquad 1-\frac{q-1}{q} &= \sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}} \frac{q-1}{q}\cdot\frac{1}{q^{2\deg h}} \\ &\geq \sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}} \limsup_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}(hB) \\ &\geq \sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}} \limsup_{N\to\infty}\frac{1}{N^2}\sum_{m,n=1}^{N-1}\delta_{(\varphi_m,\varphi_n)}(hB) \\ &\geq \limsup_{N\to\infty}\sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}} \frac{1}{N^2}\sum_{m,n=1}^{N-1}\delta_{(\varphi_m,\varphi_n)}(hB) \\ &= \limsup_{N\to\infty}\frac{1}{N^2}\sum_{m,n=1}^{N-1}\sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}}\delta_{(\varphi_m,\varphi_n)}(hB).\end{aligned}$$

Subtracting each side of (16) from 1 and noting (13), we have

$$\begin{aligned}(17)\qquad \frac{q-1}{q} &\leq \liminf_{N\to\infty}\left(1-\frac{1}{N^2}\sum_{m,n=1}^{N-1}\sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}}\delta_{(\varphi_m,\varphi_n)}(hB)\right) \\ &= \liminf_{N\to\infty}\left(\frac{1}{N^2}\sum_{m,n=1}^{N-1}\left(1-\sum_{h\in R\,;\,\deg h\geq 1,\,\mathrm{monic}}\delta_{(\varphi_m,\varphi_n)}(hB)\right)\right. \\ &\qquad\qquad \left.+\frac{1}{N^2}\sum_{\substack{0\leq m,n\leq N-1;\\ m=0 \text{ or } n=0}} 1\right) \\ &= \liminf_{N\to\infty}\left(\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}(B)\right. \\ &\qquad\qquad \left.+\frac{1}{N^2}\sum_{\substack{0\leq m,n\leq N-1;\\ m=0 \text{ or } n=0}}\Big(1-\delta_{(\varphi_m,\varphi_n)}(B)\Big)\right) \\ &= \liminf_{N\to\infty}\frac{1}{N^2}\sum_{m,n=0}^{N-1}\delta_{(\varphi_m,\varphi_n)}(B).\end{aligned}$$

Finally, (14) with $h(x) \equiv 1$ and (17) imply that

$$\lim_{N\to\infty} \frac{1}{N^2} \sum_{m,n=0}^{N-1} \delta_{(\varphi_m,\varphi_n)}(B) \;=\; \frac{q-1}{q},$$

which is equivalent to (2).

Next, let us prove (3) in Theorem 1. Take arbitrary $f, g \in R$ with $\deg f \vee \deg g \geq 0$, and set $\varphi'_m := f + \varphi_m$ and $\varphi''_n := g + \varphi_n$. Then it is easy to see that the sequence of probability measures $\{\frac{1}{N^2}\sum_{m,n=0}^{N-1} \delta_{(\varphi'_m,\varphi''_n)}\}_N$ weakly converges to λ^2. Furthermore, we have

$$\sum_{h\in R\,:\,\mathrm{monic}} \delta_{(\varphi'_m,\varphi''_n)}(hB) \;=\; \begin{cases} 1, & (\varphi'_m,\varphi''_n) \neq (0,0), \\ 0, & (\varphi'_m,\varphi''_n) = (0,0). \end{cases} \tag{18}$$

By these facts, we can deduce that

$$\lim_{N\to\infty} \frac{1}{N^2} \sum_{m,n=0}^{N-1} \delta_{(\varphi'_m,\varphi''_n)}(B) \;=\; \frac{q-1}{q}, \tag{19}$$

similarly as the case where $(f, g) = (0, 0)$.

Remark 1. If $f, g \in \widehat{R}$ fail to belong to R, (19) may not be true. The following is one of such examples: Let $\tau : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a bijective mapping. For each $N \in \mathbb{N}$, we consider a system of equations

$$\begin{aligned} (f + \varphi_m) \bmod p_{\tau(m,n)} &= 0, \\ (g + \varphi_n) \bmod p_{\tau(m,n)} &= 0, \end{aligned} \qquad m, n \;=\; 1, 2, \ldots, N,$$

with unknown variable $(f, g) \in \widehat{R}^2$. By the Chinese remainder theorem, the solution (f, g), say $(f_N, g_N) \in R^2$, exists. Since $\widehat{R}^2$ is compact, $\{(f_N, g_N)\}_{N=1}^{\infty}$ has a limit point, say $(f_\infty, g_\infty) \in \widehat{R}^2$. Then since for each $p \in \mathcal{P}$, $p\widehat{R}$ is a closed ball, it holds that

$$\begin{aligned} (f_\infty + \varphi_m) \bmod p_{\tau(m,n)} &= 0, \\ (g_\infty + \varphi_n) \bmod p_{\tau(m,n)} &= 0, \end{aligned} \qquad m, n \in \mathbb{N}.$$

Clearly, we have $X(f_\infty + \varphi_m, g_\infty + \varphi_n) \;=\; 0,\; m, n \in \mathbb{N}$, and hence

$$\lim_{N\to\infty} \frac{1}{N^2} \sum_{m,n=0}^{N-1} \delta_{(f_\infty+\varphi_m,\, g_\infty+\varphi_n)}(B) \;=\; 0.$$

§5. Proof of strong law of large numbers

5.1. Maximal ergodic inequality

Basically, we adopt the method used in Stroock [10, § 5.3]. We begin with the definition of classical maximal function.

Definition 6. For $f \in L^1(\mathbb{R}^l \to \mathbb{R})$, we define Hardy-Littlewood's maximal function Mf by

$$Mf(x) := \sup_{Q \ni x} \frac{1}{|Q|} \int_Q |f(y)| dy, \quad x \in \mathbb{R}^l,$$

where the sup is taken for all cubes Q of the form

$$Q = \prod_{j=1}^{l} [a_j, a_j + r), \quad a = (a_1, \ldots, a_l) \in \mathbb{R}^l,\ r > 0$$

such that $Q \ni x$, and

$$|Q| := \text{the Lebesgue measure of } Q.$$

Lemma 9 (The Hardy-Littlewood inequality)**.** ([10, § 5.3]) *For any* $0 < \alpha < \infty$*, it holds that*

$$\left|\left\{x \in \mathbb{R}^l; Mf(x) \geq \alpha\right\}\right| \leq \frac{12^l}{\alpha} \int_{\mathbb{R}^l} |f(y)| dy.$$

Definition 7. For each $m, n = 0, 1, 2, \ldots$, there exists a unique $k \in \mathbb{N} \cup \{0\}$ such that $\varphi_m(x) + \varphi_n(x) = \varphi_k(x)$. This k will be denoted by $m \cdot n$, that is,

$$m \cdot n := \sum_{i=1}^{\infty} \left(\left(d_i^{(q)}(m) + d_i^{(q)}(n) \right) \bmod q \right) q^{i-1}.$$

As is easily seen, $m \cdot n \neq m + n$ in general. Therefore the method used in Stroock [10, § 5.3] does not work to derive the maximal ergodic inequality. In this paper, we adopt a modification of Stroock's method due to Miki [8].

Lemma 10. ([8]) *Let* $m, n, l = 0, 1, 2, \ldots$.
(i) $m \cdot 0 = m$, $m \cdot n = n \cdot m$, $(l \cdot m) \cdot n = l \cdot (m \cdot n)$.
(ii) *The mapping* $\mathbb{N} \cup \{0\} \ni k \mapsto m \cdot k \in \mathbb{N} \cup \{0\}$ *is bijective.*
(iii) $(m \vee n) - (q-1)(m \wedge n) \leq m \cdot n \leq m + n$.

Proof. (i) and (ii) are obvious. We here check (iii). Since, for $a, b \in \{0, 1, \ldots, q-1\}$

$$(a+b) \bmod q = \begin{cases} a+b, & \text{if } \ a+b < q, \\ a+b-q, & \text{if } \ a+b \geq q, \end{cases}$$

it follows that

$$\begin{aligned} &(a+b) \bmod q \leq a+b, \\ &(a+b) \bmod q + (q-1)a = \begin{cases} a+b+(q-1)a \\ \quad = b+qa, \ \text{if } a+b<q, \\ a+b-q+(q-1)a \\ \quad = b+q(a-1), \ \text{if } a+b \geq q > b \end{cases} \\ &\qquad\qquad\qquad\qquad\qquad \geq b. \end{aligned}$$

Hence, for $0 \leq m \leq n$

$$\begin{aligned} m \cdot n &= \sum_{i=1}^{\infty} \left(\left(d_i^{(q)}(m) + d_i^{(q)}(n) \right) \bmod q \right) q^{i-1} \\ &\begin{cases} \leq \displaystyle\sum_{i=1}^{\infty} \left(d_i^{(q)}(m) + d_i^{(q)}(n) \right) q^{i-1} = m+n, \\ \geq \displaystyle\sum_{i=1}^{\infty} \left(d_i^{(q)}(n) - (q-1) d_i^{(q)}(m) \right) q^{i-1} = n-(q-1)m. \end{cases} \end{aligned}$$

□

Lemma 11. *For any square array $\{a_{k_1,k_2}\}_{k_1,k_2 \in \{0,1,2,\ldots\}} \subset [0,\infty)$ with $\sum_{k_1,k_2=0}^{\infty} a_{k_1,k_2} < \infty$, the following inequality holds: For any $\alpha > 0$,*

$$\begin{aligned} &\#\left\{ (k_1,k_2) \in \{0,1,2,\ldots\}^2 \, ; \, \sup_{n \geq 1} \left(\frac{1}{qn} \right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1 \cdot j_1, k_2 \cdot j_2} \geq \alpha \right\} \\ &\quad \leq \frac{12^2}{\alpha} \sum_{k_1,k_2=0}^{\infty} a_{k_1,k_2}. \end{aligned}$$

Proof. Put

$$f(x) := \sum_{k_1,k_2=0}^{\infty} a_{k_1,k_2} \mathbf{1}_{C(k_1,k_2)}(x), \quad x \in \mathbb{R}^2,$$

where

$$C(k_1,k_2) := [k_1, k_1+1) \times [k_2, k_2+1).$$

Then clearly we have

$$\int_{\mathbb{R}^2} f(x)dx \;=\; \sum_{k_1,k_2=0}^{\infty} a_{k_1,k_2} < \infty, \tag{20}$$

and maximal function Mf becomes

$$\begin{aligned} Mf(x) &= \sup_{Q\ni x} \frac{1}{|Q|}\int_Q f(y)dy \\ &= \sup_{Q\ni x} \frac{1}{|Q|} \sum_{l_1,l_2\geq 0} a_{l_1,l_2}\big|C(l_1,l_2)\cap Q\big|. \end{aligned} \tag{21}$$

Now suppose that $x \in C(k_1,k_2)$ $(k_1,k_2 \in \{0,1,2,\ldots\})$, $n \in \mathbb{N}$, and $0 \leq j_1, j_2 \leq n-1$. If we take $Q = [k_1-(q-1)n, k_1+n)\times[k_2-(q-1)n, k_2+n)$, then $Q \ni x$ and

$$Q \supset C(k_1\cdot j_1, k_2\cdot j_2) \tag{22}$$

holds. Because Lemma 10(iii) implies

$$\begin{aligned} k_1\cdot j_1 &\geq k_1-(q-1)n, \\ k_2\cdot j_2 &\geq k_2-(q-1)n \end{aligned}$$

and

$$\begin{aligned} k_1\cdot j_1 \leq k_1+j_1 \;\leq\; k_1+n-1, \\ k_2\cdot j_2 \leq k_2+j_2 \;\leq\; k_2+n-1, \end{aligned}$$

we see

$$\begin{aligned} [k_1\cdot j_1, k_1\cdot j_1+1) \subset [k_1-(q-1)n, k_1+n), \\ [k_2\cdot j_2, k_2\cdot j_2+1) \subset [k_2-(q-1)n, k_2+n), \end{aligned}$$

and hence (22) holds.

If we take this Q for (21), we have for $x \in C(k_1,k_2)$, $n \in \mathbb{N}$ that

$$\begin{aligned} Mf(x) &\geq \frac{1}{|Q|}\sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2}\big|C(k_1\cdot j_1, k_2\cdot j_2)\cap Q\big| \\ &= \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2}. \end{aligned}$$

Taking sup in n,

$$Mf(x) \geq \sum_{k_1,k_2=0}^{\infty} \left(\sup_{n\in\mathbb{N}} \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2} \right) \mathbf{1}_{C(k_1,k_2)}(x).$$

Then for $0 < \alpha < \infty$,

$$\begin{aligned}
&\left\{ x \in [0,\infty)^2; Mf(x) \geq \alpha \right\} \\
&\supset \Bigg\{ x \in [0,\infty)^2; \\
&\qquad \sum_{k_1,k_2=0}^{\infty} \left(\sup_{n\in\mathbb{N}} \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2} \right) \mathbf{1}_{C(k_1,k_2)}(x) \geq \alpha \Bigg\} \\
&= \bigcup_{\substack{k_1,k_2\geq 0; \\ \sup_{n\in\mathbb{N}} \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2} \geq \alpha}} C(k_1,k_2).
\end{aligned}$$

Therefore Lemma 9 and (20) imply

$$\begin{aligned}
&\frac{12^2}{\alpha} \sum_{k_1,k_2=0}^{\infty} a_{k_1,k_2} \\
&= \frac{12^2}{\alpha} \int_{\mathbb{R}^2} f(x)dx \\
&\geq \left| \left\{ x \in \mathbb{R}^2; Mf(x) \geq \alpha \right\} \right| \\
&\geq \left| \left\{ x \in [0,\infty)^2; Mf(x) \geq \alpha \right\} \right| \\
&\geq \sum_{k_1,k_2=0}^{\infty} \mathbf{1}_{\sup_{n\in\mathbb{N}} \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2} \geq \alpha} \\
&= \# \left\{ (k_1,k_2) \in \{0,1,2,\ldots\}^2 ; \sup_{n\in\mathbb{N}} \left(\frac{1}{qn}\right)^2 \sum_{j_1,j_2=0}^{n-1} a_{k_1\cdot j_1,k_2\cdot j_2} \geq \alpha \right\}. \square
\end{aligned}$$

Lemma 12 (Maximal ergodic inequality)**.** *Let $F : \widehat{R}^2 \to [0,\infty)$ be a Borel measurable function such that*

$$\mathbb{E}^{\lambda^2}[F] := \int_{\mathbb{R}^2} F(f,g)\lambda^2(dfdg) < \infty.$$

Then for any $0<\alpha<\infty$, it holds that

$$\lambda^2\left(\sup_{N\geq 1}\frac{1}{N^2}\sum_{j_1,j_2=0}^{N-1}F(f+\varphi_{j_1},g+\varphi_{j_2})\geq q^2\alpha\right)\ \leq\ \frac{24^2}{\alpha}\mathbb{E}^{\lambda^2}[F].$$

Proof. Fix $M\in\mathbb{N}$ and $(f,g)\in\widehat{R}^2$. For each $k_1,k_2\in\{0,1,2,\ldots\}$, we define

$$a_{k_1,k_2}(f,g)\ :=\ \begin{cases} F(f+\varphi_{k_1},g+\varphi_{k_2}), & \text{if}\ \ 0\leq k_1,k_2\leq 2M-1,\\ 0, & \text{otherwise.}\end{cases}$$

Then Lemma 11 implies that

$$\begin{aligned}&\#\left\{k_1,k_2\geq 0\,;\,\sup_{N\geq 1}\left(\frac{1}{qN}\right)^2\sum_{j_1,j_2=0}^{N-1}a_{k_1\cdot j_1,k_2\cdot j_2}(f,g)\geq\alpha\right\}\\ &\quad\leq\frac{12^2}{\alpha}\sum_{k_1,k_2=0}^{\infty}a_{k_1,k_2}(f,g)\\ &\quad=\frac{12^2}{\alpha}\sum_{0\leq k_1,k_2\leq 2M-1}F(f+\varphi_{k_1},g+\varphi_{k_2}),\quad 0<\alpha<\infty.\end{aligned}$$

Noting that

$$\begin{aligned}&0\leq k_1,k_2\leq M,\quad 0\leq j_1,j_2<N,\quad 1\leq N\leq M\\ &\quad\Rightarrow\ 0\leq k_1\cdot j_1\leq k_1+j_1\leq M+N-1\leq 2M-1,\\ &\qquad\ \ 0\leq k_2\cdot j_2\leq k_2+j_2\leq M+N-1\leq 2M-1\\ &\quad\Rightarrow\ a_{k_1\cdot j_1,k_2\cdot j_2}(f,g)=F\big(f+\varphi_{k_1\cdot j_1},g+\varphi_{k_2\cdot j_2}\big)\\ &\qquad\qquad\qquad\qquad\quad=F\big(f+\varphi_{k_1}+\varphi_{j_1},g+\varphi_{k_2}+\varphi_{j_2}\big),\end{aligned}$$

we have

$$\begin{aligned}&\#\Bigg\{(k_1,k_2)\in\{0,1,2,\ldots,M\}^2\,;\\ &\qquad\max_{1\leq N\leq M}\left(\frac{1}{qN}\right)^2\sum_{j_1,j_2=0}^{N-1}F\big(f+\varphi_{k_1}+\varphi_{j_1},g+\varphi_{k_2}+\varphi_{j_2}\big)\geq\alpha\Bigg\}\\ &\quad\leq\frac{12^2}{\alpha}\sum_{k_1,k_2=0}^{2M-1}F(f+\varphi_{k_1},g+\varphi_{k_2}),\quad 0<\alpha<\infty.\end{aligned}$$

Therefore taking the expectation $\mathbb{E}^{\lambda^2}$ of both sides,

$$\sum_{k_1,k_2=0}^{M} \lambda^2\left(\max_{1\le N\le M}\left(\frac{1}{qN}\right)^2 \sum_{j_1,j_2=0}^{N-1} F\big(f+\varphi_{k_1}+\varphi_{j_1}, g+\varphi_{k_2}+\varphi_{j_2}\big) \ge \alpha\right)$$
$$\le \frac{12^2}{\alpha}\sum_{k_1,k_2=0}^{2M-1} \mathbb{E}^{\lambda^2}\Big[F(f+\varphi_{k_1}, g+\varphi_{k_2})\Big], \quad 0<\alpha<\infty.$$

Since λ^2 is shift-invariant, the above inequality reduces to

$$\lambda^2\left(\max_{1\le N\le M}\left(\frac{1}{qN}\right)^2 \sum_{j_1,j_2=0}^{N-1} F\big(f+\varphi_{j_1}, g+\varphi_{j_2}\big) \ge \alpha\right)$$
$$\le \frac{12^2}{\alpha}\left(\frac{2M}{M+1}\right)^2 \mathbb{E}^{\lambda^2}[F], \quad 0<\alpha<\infty.$$

Finally, letting $M\to\infty$, the assertion of the lemma follows. □

5.2. Proof of Theorem 2

For simplicity, we here prove Theorem 2 for $l=2$ only. The same method works for general l, too. Namely, what we prove is as follows:

For any $F\in L^1(\widehat{R}^2,\lambda^2)$,

$$\frac{1}{N^2}\sum_{m,n=0}^{N-1} F(f+\varphi_m, g+\varphi_n) \;\to\; \mathbb{E}^{\lambda^2}[F] \quad \lambda^2\text{-}a.e.(f,g). \tag{23}$$

Proof. Take sequence of continuous functions $\{F_k\}_{k=1}^{\infty}$ so that

$$\|F_k - F\|_{L^1} \;\le\; \frac{1}{k^2}, \quad k\in\mathbb{N}. \tag{24}$$

By Corollary 1, it holds for each $k\in\mathbb{N}$ that

$$\frac{1}{N^2}\sum_{m,n=0}^{N-1} F_k(f+\varphi_m, g+\varphi_n) \;\to\; \mathbb{E}^{\lambda^2}[F_k] \quad \text{as } N\to\infty,\ (f,g)\in\widehat{R}^2. \tag{25}$$

By Lemma 12, it holds for $0<\alpha<\infty$ that

$$\lambda^2\left(\sup_{N\ge 1}\frac{1}{N^2}\sum_{j_1,j_2=0}^{N-1}\big|F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - F(f+\varphi_{j_1}, g+\varphi_{j_2})\big| \ge q^2\alpha\right)$$
$$\le \frac{24^2}{\alpha}\mathbb{E}^{\lambda^2}\big[|F_k - F|\big]$$

$$\leq \frac{24^2}{\alpha} \cdot \frac{1}{k^2}.$$

From this, it follows that

$$\sum_{k=1}^{\infty} \lambda^2 \Bigg((f,g) \in \widehat{R}^2 ;\ \sup_{N\geq 1} \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} \big| F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - F(f+\varphi_{j_1}, g+\varphi_{j_2}) \big| \geq \frac{q^2}{\sqrt{k}} \Bigg) \leq \sum_{k=1}^{\infty} 24^2 \sqrt{k} \frac{1}{k^2} < \infty,$$

which means that

$$\lim_{k\to\infty} \sup_{N\geq 1} \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} \big| F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - F(f+\varphi_{j_1}, g+\varphi_{j_2}) \big| = 0, \quad \text{a.s.}$$

Consequently, by (24) and (25), we see that

$$(26)\quad \left| \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} F(f+\varphi_{j_1}, g+\varphi_{j_2}) - \mathbb{E}^{\lambda^2}[F] \right|$$
$$= \Bigg| \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} \Big(F(f+\varphi_{j_1}, g+\varphi_{j_2}) - F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) \Big) + \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - \mathbb{E}^{\lambda^2}\big[F_k\big] + \mathbb{E}^{\lambda^2}\big[F_k\big] - \mathbb{E}^{\lambda^2}\big[F\big] \Bigg|$$
$$\leq \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} \Big| F(f+\varphi_{j_1}, g+\varphi_{j_2}) - F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) \Big| + \left| \frac{1}{N^2} \sum_{j_1,j_2=0}^{N-1} F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - \mathbb{E}^{\lambda^2}\big[F_k\big] \right| + \mathbb{E}^{\lambda^2}\Big[\big| F_k - F \big| \Big]$$
$$\leq \sup_{M\geq 1} \frac{1}{M^2} \sum_{j_1,j_2=0}^{M-1} \Big| F(f+\varphi_{j_1}, g+\varphi_{j_2}) - F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) \Big|$$

$$
\begin{aligned}
&+\left|\frac{1}{N^2}\sum_{j_1,j_2=0}^{N-1} F_k(f+\varphi_{j_1}, g+\varphi_{j_2}) - \mathbb{E}^{\lambda^2}[F_k]\right| \\
&+\frac{1}{k^2} \\
&\to 0 \quad \text{a.s.} \quad (\text{first } N\to\infty, \text{ secondly } k\to\infty). \qquad \square
\end{aligned}
$$

Remark 2. If $F \in L^p(\widehat{R}^2, \lambda^2)$ for some $1 \le p < \infty$, the convergence in (23) is in fact an L^p-convergence. Indeed, for any $\varepsilon > 0$, there exists a bounded measurable function $F_\varepsilon : \widehat{R}^2 \to \mathbb{R}$ such that

$$\|F - F_\varepsilon\|_{L^p} < \varepsilon.$$

A similar estimate as (26) can be done in L^p-norm in the following way:

$$
\begin{aligned}
&\left\|\frac{1}{N^2}\sum_{m,n=0}^{N-1} F(f+\varphi_m, g+\varphi_n) - \mathbb{E}^{\lambda^2}[F]\right\|_{L^p} \\
&\le \frac{1}{N^2}\sum_{m,n=0}^{N-1} ||F(f+\varphi_m, g+\varphi_n) - F_\varepsilon(f+\varphi_m, g+\varphi_n)||_{L^p} \\
&\quad + \left\|\frac{1}{N^2}\sum_{m,n=0}^{N-1} F_\varepsilon(f+\varphi_m, g+\varphi_n) - \mathbb{E}^{\lambda^2}[F_\varepsilon]\right\|_{L^p} + ||F_\varepsilon - F||_{L^p} \\
&< \left\|\frac{1}{N^2}\sum_{m,n=0}^{N-1} F_\varepsilon(f+\varphi_m, g+\varphi_n) - \mathbb{E}^{\lambda^2}[F_\varepsilon]\right\|_{L^p} + 2\varepsilon \\
&\to 0 \quad (\text{first } N\to\infty, \text{ secondly } \varepsilon \to 0).
\end{aligned}
$$

References

[1] P. Billingsley, Convergence of probability measures, John Willey & Sons, 1968.

[2] G. L. Dirichlet, Über die Bestimmung der mittleren Werthe in der Zahlentheorie, Abhandlungen Königlich Preuss. Akad. Wiss., 1849, pp. 69–83; G. Lejeune Dirichlet's Werke. II, Chelsea, 1969, pp. 49–66.

[3] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 5-th ed., Oxford Univ. Press, 1979.

[4] J. H. Hodges, Uniform distribution of sequences in GF$[q,x]$, Acta Arith., **12** (1966), 55–75.

[5] H. Kubota and H. Sugita, Probabilistic proof of limit theorems in number theory by means of adeles, Kyushu J. Math., **56** (2002), 391–404.

[6] L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Interscience, 1974.

[7] R. Lidl and H. Niederreiter, Finite fields, with a foreword by P.M. Cohn. Second ed., Encyclopedia of Mathematics and its Applications, **20**, Cambridge Univ. Press, Cambridge, 1997.

[8] H. Miki, An extension of ergodic theorem and its applications to number theory. (Japanese), Master thesis, Department of Mathematics, Graduate School of Science, Osaka Univ., 2006.

[9] K. R. Parthasarathy, Probability measures on metric spaces, Academic Press, New York, London, 1967.

[10] D. W. Stroock, Probability theory, an analytic view, revised ed., Cambridge Univ. Press, Cambridge, 1994.

[11] H. Sugita and S. Takanobu, The probability of two integers to be co-prime, revisited — on the behavior of CLT-scaling limit, Osaka J. Math., **40** (2003), 945–976.

Hiroshi Sugita
Department of Mathematics
Graduate School of Science
Osaka University
Machikaneyama-cho 1-1
Toyonaka, Osaka 560-0043
Japan
E-mail address: sugita@math.sci.osaka-u.ac.jp

Satoshi Takanobu
Division of Mathematical and Physical Sciences
Graduate School of Natural Science and Technology
Kanazawa University
Kakuma-machi
Kanazawa, Ishikawa 920-1192
Japan
E-mail address: takanob@kenroku.kanazawa-u.ac.jp