The Distribution of Group Structures on Elliptic Curves over Finite Prime Fields

Ernst-Ulrich Gekeler

Received: April 12, 2006

Communicated by Peter Schneider

Abstract. We determine the probability that a randomly chosen elliptic curve $E/\mathbb{F}_p$ over a randomly chosen prime field $\mathbb{F}_p$ has an ℓ-primary part $E(\mathbb{F}_p)[\ell^\infty]$ isomorphic with a fixed abelian ℓ-group $H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$.

Probabilities for "$|E(\mathbb{F}_p)|$ divisible by n", "$E(\mathbb{F}_p)$ cyclic" and expectations for the number of elements of precise order n in $E(\mathbb{F}_p)$ are derived, both for unbiased $E/\mathbb{F}_p$ and for $E/\mathbb{F}_p$ with $p \equiv 1$ (ℓ^r).

2000 Mathematics Subject Classification: 11 N 45, 11 G 20, 11 S 80
Keywords and Phrases: Elliptic curves over finite fields, group structures, counting functions

1. Introduction

Given an elliptic curve E over the finite field $\mathbb{F}_q$ with q elements, the set $E(\mathbb{F}_q)$ of rational points forms an abelian group, which satisfies

$$|E(\mathbb{F}_q) - (q+1)| \leq 2q^{1/2} \quad \text{(Hasse)} \tag{1.1}$$

and

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m \times \mathbb{Z}/n \tag{1.2}$$

with well-defined numbers m, n and $m|n$. Our aim is to study the statistics of such group structures if $E/\mathbb{F}_q$ varies through an infinite family $\mathcal{F}$. In the present article, we consider

$$\mathcal{F} = \{\mathbb{F}_p\text{-isomorphism classes of elliptic curves } E/\mathbb{F}_p \text{ over finite prime fields } \mathbb{F}_p\} \tag{1.3}$$

but note that a similar study may be performed for elliptic curves $E/\mathbb{F}_q$ over arbitrary finite fields, or for $E/\mathbb{F}_q$ where q runs through the powers of the fixed prime number p.

Given any algebraic property (A) of $E/\mathbb{F}_p$ (or any subset A of $\mathcal{F}$), we define its "probability" in $\mathcal{F}$ as

$$(1.4)\qquad P(\mathcal{F},A) := \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \le x,\ E/\mathbb{F}_p \text{ has property } A\}|}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \le x\}|},$$

provided the limit exists. Then $P(\mathcal{F},\cdot)$ is a "content" on $\mathcal{F}$, i.e., it satisfies the usual axioms of a probability measure except that the condition of σ-additivity (= countable additivity) is relaxed to finite additivity. In a similar fashion, we may define other notions of probability theory for $\mathcal{F}$, for example the conditional probability $P(\mathcal{F},A|B)$ for property A under condition B, or the expectation $E(\mathcal{F},f)$ for a function f on $\mathcal{F}$.

It is obvious from (1.1) that $P(\mathcal{F},A)=0$ for any property like

$$\text{(A)}\qquad E(\mathbb{F}_p) \cong \mathbb{Z}/m \times \mathbb{Z}/n \quad \text{with } m,n \text{ fixed };$$

i.e., such probabilities are meaningless. Instead, the typical question we will deal with is:

1.5 Question: Let a prime number ℓ and a finite abelian ℓ-group

$$H = H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$$

with $0 \le \alpha \le \beta$ be given. How likely (cf. (1.4)) is it that the ℓ-primary part $E(\mathbb{F}_p)[\ell^\infty]$ of $E(\mathbb{F}_p)$ is isomorphic with H, if $E/\mathbb{F}_p$ is randomly chosen in $\mathcal{F}$?

(Instead of fixing one prime ℓ and the finite ℓ-group H, we could fix a finite set L of primes and a finite abelian L-group H of rank less or equal to 2, and ask for the probability that the L-part of $E(\mathbb{F}_p)$ is isomorphic with H.)

In Theorem 3.15, using results of E. Howe [7], we show that the corresponding $P(\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\text{”})$ always exists, and give its value, along with an error term $O_{\ell,\alpha,\beta}(x^{-1/2})$. As prescribed by Serre's "Čebotarev theorem" ([8], Theorem 7), that probability agrees with the (non-vanishing) Haar volume $g^{(\ell)}(\alpha,\beta)$ of a certain subset $X^{(\ell)}(\alpha,\beta)$ of $\mathrm{GL}(2,\mathbb{Z}_\ell)$. The relevant Haar measures are provided by Theorem 2.3, the proof of which forms the contents of section 2.

Actually, we will see in section 4 that $P(\mathcal{F},\cdot)$ defines a probability measure (in the usual sense, that is, even σ-additive) on the discrete set of isomorphism classes of abelian groups of shape $H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$ $(0 \le \alpha \le \beta)$, and that these measures for varying primes ℓ are stochastically independent.

We use the preceding to derive (both without restrictions on p, or under congruence conditions for p) the exact values of

(a) the probability $P(\mathcal{F}, \text{“}n \mid |E(\mathbb{F}_p)|\text{”})$ that $|E(\mathbb{F}_p)|$ is divisible by the fixed natural number n (Proposition 5.1, Corollary 5.2);
(b) the expectation $E(\mathcal{F},\kappa_n)$ for the number $\kappa_n(E(\mathbb{F}_p))$ of elements of precise order n in $E(\mathbb{F}_p)$ (Proposition 5.6);
(c) the probability $P(\mathcal{F}, \text{“}E(\mathbb{F}_p) \text{ is cyclic”})$ of cyclicity of $E(\mathbb{F}_p)$ (Theorem 5.9).

Items (a) and (c) are related to results of Howe (Theorem 1.1 of [5]) and S.G. Vladut (Theorem 6.1 of [7]), the difference being that the cited authors consider elliptic curves E over one fixed finite field $\mathbb{F}_q$, while (a),(b),(c) are results averaged over all $\mathbb{F}_p$ (or all $\mathbb{F}_p$ where p lies in some arithmetic progression).

Given $E/\mathbb{F}_p$ and a prime number ℓ different from p, we let $F_\ell = F_\ell(E/\mathbb{F}_p)$ be its Frobenius element, an element of $\mathrm{GL}(2,\mathbb{Z}_\ell)$ well-defined up to conjugation ($\mathbb{Z}_\ell = \ell$-adic integers). Its characteristic polynomial $\chi_{F_\ell}(X) = X^2 - \mathrm{tr}(F_\ell)X + \det(F_\ell)$ satisfies

$$\det(F_\ell) = p,\ \mathrm{tr}(F_\ell) = p + 1 - |E(\mathbb{F}_p)|; \tag{1.6}$$

in particular, it has integral coefficients independent of ℓ. It is related with the group structure on $E(\mathbb{F}_p)$ through

$$E(\mathbb{F}_p)[\ell^\infty] \cong \mathrm{cok}(F_\ell - 1), \tag{1.7}$$

where "cok" is the cokernel of a matrix regarded as an endomorphism on $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ (see e.g. [3], appendix, Proposition 2).

In order to avoid technical problems irrelevant for our purposes, we exclude for the moment the primes $p = 2$ and 3 from our considerations, that is, $\mathcal{F} = \{E/\mathbb{F}_p \mid p \geq 5 \text{ prime}\}$. Then we define

$$w(E/\mathbb{F}_p) = 2|\mathrm{Aut}_{\mathbb{F}_p}(E/\mathbb{F}_p)|^{-1} = \begin{cases} \frac{1}{3},\ p \equiv 1\ (3),\ j(E) = 0 \\ \frac{1}{2},\ p \equiv 1\ (4),\ j(E) = 12^3 \\ 1\ ,\quad \text{otherwise.} \end{cases} \tag{1.8}$$

Thus in "most" cases, $w(E/\mathbb{F}_p) = 1$. For well-known philosophical reasons not addressed here, we will count subsets of $\mathcal{F}$ not by ordinary cardinality, but by cardinality weighted with w. That is, for a finite subset $\mathcal{F}'$ of $\mathcal{F}$, we define its weighted cardinality as

$$|\mathcal{F}'|^* = \sum_{E/\mathbb{F}_p \in \mathcal{F}'} w(E/\mathbb{F}_p). \tag{1.9}$$

Then we have for example

$$|\{E/\mathbb{F}_p\}|^* = 2p \tag{1.10}$$

for the number* of isomorphism classes of elliptic curves over a fixed prime field $\mathbb{F}_p$. Accordingly, we redefine probabilities $P(\mathcal{F}, A)$ as in (1.4), replacing ordinary "$|\ |$" by weighted cardinalities "$|\ |^*$". Of course, it doesn't matter whether or not we include the finite number of $E/\mathbb{F}_p$ with $p = 2, 3$ into $\mathcal{F}$.

With each $E/\mathbb{F}_p \in \mathcal{F}$, we associate its total Frobenius element

$$F(E/\mathbb{F}_p) = (\ldots, F_\ell(E/\mathbb{F}_p), \ldots) \in \Pi_{\ell \text{ prime}} \mathrm{GL}(2, \mathbb{Z}_\ell)$$

(well-defined up to conjugation, and neglecting for the moment the question of the p-component of F). As usual, we let

$$\hat{\mathbb{Z}} = \lim_{\substack{\longleftarrow \\ N \in \mathbb{N}}} \mathbb{Z}/N = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$$

be the profinite completion of $\mathbb{Z}$. Then $\mathrm{GL}(2, \hat{\mathbb{Z}}) = \prod \mathrm{GL}(2, \mathbb{Z}_\ell)$ is a compact group provided with a canonical projection "(mod$N$)" onto $\mathrm{GL}(2, \mathbb{Z}/N)$ for each $N \in \mathbb{N}$.

Led by the Čebotarev and other equidistribution theorems or conjectures, in particular, the "Cohen-Lenstra philosophy" [2], we make the following hypothesis:

(H) The series $(F(E/\mathbb{F}_p))_{E/\mathbb{F}_p \in \mathcal{F}}$ is equidistributed in $\mathrm{GL}(2, \hat{\mathbb{Z}})$.

In more detailed terms, this means:

(1.11) Given $N \in \mathbb{N}$ and any conjugacy class $\mathcal{C}$ in $\mathrm{GL}(2, \mathbb{Z}/N)$, the limit

$$\lim_{x \to \infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid F(E/\mathbb{F}_p)(\mathrm{mod} N) \text{ lies in } \mathcal{C} \text{ and } p \leq x\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*}$$

exists and equals $|\mathcal{C}|/|\mathrm{GL}(2, \mathbb{Z}/N)|$.

Note that in the form just given, the hypothesis does not require specifying the p-component of $F(E/\mathbb{F}_p)$, since for given N and $\mathcal{C}$ we may omit the finite number of terms indexed by $E/\mathbb{F}_p$ with $p|N$ without changing the limit. Note also that the number of $E/\mathbb{F}_p$ with $w(E/\mathbb{F}_p) \neq 1$ over a fixed $\mathbb{F}_p$ is uniformly bounded, and is therefore negligible for large p. That is, though (1.11) appears to be the "right" formula, the limit (provided it exists) doesn't change upon replacing weighted by unweighted cardinalities.

Now (H) may be derived from the general "Čebotarev theorem" (Theorem 7 of [8]) of Serre, applied to the moduli scheme of elliptic curves endowed with a level-N structure, and also from Theorem 3.1 of [1]. We thus regard (H) as established, although our proofs are independent of its validity.

In [6], we studied the frequency of $E/\mathbb{F}_p$ with a fixed Frobenius trace $\mathrm{tr}(E/\mathbb{F}_p) \in \mathbb{Z}$. The results (*loc. cit.*, Theorems 5.5 and 6.4) turned out to be those expected by (H) (and other known properties of $E/\mathbb{F}_p$, like the result of [2]). On the other hand, (H) in the form (1.11) applied to prime powers $N = \ell^n$ along with (1.7) predicts that for each group $H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$, the probability $P(\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\text{”})$ equals the Haar volume in $\mathrm{GL}(2, \mathbb{Z}_\ell)$ of $\{\gamma \in \mathrm{GL}(2, \mathbb{Z}_\ell) \mid \mathrm{cok}(\gamma - 1) \cong H^{(\ell)}_{\alpha,\beta}\}$. Our Theorem 3.15 states an effective version of that identity, i.e., including the error term.

Notation. Apart from standard mathematical symbols, we use the following notation.

$\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathbb{P} = \{2, 3, 5, \ldots\}$ denote the sets of natural, of non-negative integral, of prime numbers, respectively, and $|X|$ the cardinality of the set X. For $m, n \in \mathbb{N}$, "$m|n$" means "m divides n" and "$m\|n$" that m is an exact divisor of n, i.e., $m|n$ and m is coprime with n/m.

$\mathbb{Z}/n$ is the residue class group $\mathbb{Z}/n\mathbb{Z}$, and for each abelian group A and $n \in \mathbb{N}$, $A[n] = \{x \in A \mid nx = 0\}$. Further, for $\ell \in \mathbb{P}$, $A[\ell^\infty] = \bigcup_{r\in\mathbb{N}} A[\ell^r]$.

The symbols p and ℓ always stand for primes, and e.g. "$\sum_{p\leq x}\cdots$" means the sum over all primes $p \leq x$.

If f and g are functions defined on suitable subsets of $\mathbb{R}$, then

$$f \sim g :\Leftrightarrow \lim_{x\to\infty} f(x)/g(x) = 1;$$

$f = O(g) :\Leftrightarrow$ there exists a constant $C > 0$ such that $f(x) \leq Cg(x)$. We write $f = O_{\alpha,\beta}(g)$ to indicate that C might depend on the parameters $\alpha, \beta, \ldots$

2. Some Haar measures in $\mathrm{GL}(2, \mathbb{Z}_\ell)$.

In the present section, we calculate the volumes with respect to Haar measure of certain subsets of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ relevant for our purposes.

(2.1) Fix a prime number ℓ, and let

$M \;=\; \mathrm{Mat}(2, \mathbb{Z}_\ell)$ be the ring of 2×2-matrices over $\mathbb{Z}_\ell$, and

$G \;=\; \mathrm{GL}(2, \mathbb{Z}_\ell)$, with normalized Haar measures μ on M and ν on G, respectively.

For each natural number n, we put

$$M_n = \mathrm{Mat}(2, \mathbb{Z}/\ell^n) \text{ and } G_n = \mathrm{GL}(2, \mathbb{Z}/\ell^n).$$

By abuse of language, and if the context allows for no ambiguity, we often write "a" for the image of $a \in \mathbb{Z}_\ell$ (or of $a \in \mathbb{Z}/\ell^m$ with $m \geq n$) in $\mathbb{Z}/\ell^n$, etc. The reduction mapping $a \longmapsto \overline{a} : \mathbb{Z}_\ell \longrightarrow \mathbb{F}_\ell = \mathbb{Z}/\ell$ and everything derived from it will be denoted by a bar, e.g. $\gamma \longmapsto \overline{\gamma} : M \longrightarrow M_1$. Finally, v_ℓ denotes both the ℓ-adic valuation on $\mathbb{Z}_\ell$ and the truncated valuation $\mathbb{Z}/\ell^n \longrightarrow \{0, 1, \ldots, n\}$.

(2.2) The possible ℓ-torsion of an elliptic curve over a finite field is of shape

$$H = H_{\alpha,\beta} = H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta,$$

where $0 \leq \alpha \leq \beta$ are well-defined by H. (We omit some ℓ's in the notation.) For reasons explained in the introduction, we are interested in the volumes (with respect to ν) of the subsets

$$X(\alpha, \beta) = \{\gamma \in G \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}\}$$

and

$$X_r(\alpha, \beta) = \{\gamma \in G \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta},\ v_\ell(\det(\gamma) - 1) = r\}$$

of G. Here $\mathrm{cok}(\delta) = \mathbb{Z}_\ell^2/\delta(\mathbb{Z}_\ell^2)$ is the module determined by the matrix $\delta \in M$. We will show:

2.3 THEOREM.

(i) *Given* $\alpha, \beta \in \mathbb{N}_0$ *with* $\alpha \le \beta$, *we have* $\mathrm{vol}_\nu(X(\alpha,\beta)) = g(\alpha,\beta)$ *with*

$$g(\alpha,\beta) = \begin{cases} \frac{\ell^3-2\ell^2-\ell+3}{(\ell^2-1)(\ell-1)}, & 0=\alpha=\beta \\ \frac{\ell^2-\ell-1}{(\ell-1)\ell}\ell^{-\beta}, & 0=\alpha<\beta \\ \ell^{-4\alpha}, & 0<\alpha=\beta \\ \frac{\ell+1}{\ell}\ell^{-\beta-3\alpha}, & 0<\alpha<\beta\ . \end{cases}$$

(ii) *Given* $\alpha \le \beta$ *and* $r \in \mathbb{N}_0$, $X_r(\alpha,\beta)$ *is empty if* $r < \alpha$. *Otherwise,* $\mathrm{vol}_\nu(X_r(\alpha,\beta))$ *is given by the following table.*

$\mathrm{vol}_\nu(X_r(\alpha,\beta))$	$r=\alpha$	$r>\alpha$
$0=\alpha=\beta$	$(\frac{\ell-2}{\ell-1})^2$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-r}$
$0=\alpha<\beta$	$\frac{\ell-2}{\ell-1}\ell^{-\beta}$	$\frac{\ell-1}{\ell}\ell^{-\beta-r}$
$0<\alpha=\beta$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-4\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha-r}$
$0<\alpha<\beta$	$\ell^{-\beta-3\alpha}$	$\frac{\ell+1}{\ell}\ell^{-\beta-2\alpha-r}$

We need some preparations to prove the theorem. We start with three simple observations, stated without proof, where we always assume that $0 \le \alpha \le \beta$.

(2.4) For $\delta \in M$ we have the equivalence

$$\mathrm{cok}(\delta) \cong H_{\alpha,\beta} \quad \Leftrightarrow \quad \begin{array}{l} \delta \equiv 0\ (\ell^\alpha),\ \delta \not\equiv 0\ (\ell^{\alpha+1}) \text{ and} \\ v_\ell(\det\ \delta) = \alpha+\beta. \end{array}$$

(2.5) If $\delta \in M$ satisfies $\mathrm{cok}(\delta) \cong H_{\alpha,\beta}$ and $\delta \equiv \delta'(\ell^n)$ with $n > \beta$ then $\mathrm{cok}(\delta') \cong H_{\alpha,\beta}$.

As a consequence we get:

(2.6) If $n > \beta$ then

$$\mathrm{vol}_\mu\{\delta \in M \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\} = \ell^{-4n}|\{\delta \in M_n \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\}|.$$

That number is easy to determine.

2.7 PROPOSITION.

$$\mathrm{vol}_\mu\{\delta \in M \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\} = \begin{cases} (1-\ell^{-1})(1-\ell^{-2})\ell^{-4\alpha}, & 0 \le \alpha = \beta \\ (1-\ell^{-2})^2\ell^{-\beta-3\alpha}, & 0 \le \alpha < \beta. \end{cases}$$

Proof. In view of (2.4) and the bijection $\delta \longmapsto \ell^{-\alpha}\delta$ of $\{\delta \in M_n \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\}$ with $\{\epsilon \in M_{n-\alpha} \mid \mathrm{cok}(\epsilon) \cong H_{0,\beta-\alpha}\}$, valid for $n > \beta$, the proof boils down to counting of matrices ϵ in $M_{n-\alpha}$ with $\overline{\epsilon} \neq 0$ and given value of $v_\ell(\det\ \epsilon)$. We omit the details. $\square$

2.8 Remark. The volume of $\{\delta \in \mathrm{Mat}(n, \mathbb{Z}_\ell) \mid \mathrm{cok}(\delta) \cong H\}$ has been calculated by Friedman and Washington in full generality, i.e., for arbitrary n and abelian ℓ-groups H (see Proposition 3.1 of [5]). In our special case however, it is less complicated to apply the simple proof scheme given above than to extract (2.7) from the general result.

Similar to (2.6) we have

$$
\begin{array}{llcl}
 & \mathrm{vol}_\nu(X(\alpha,\beta)) & = & |G_n|^{-1}|\{\gamma \in G_n \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}\}| \\
 & \text{and} & & \\
(2.9) & \mathrm{vol}_\nu(X_r(\alpha,\beta)) & = & |G_n|^{-1}|\{\gamma \in G_n \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}, \\
 & & & \qquad v_\ell(\det(\gamma) - 1) = r\}|,
\end{array}
$$

where $n > \beta$ in the first and $n > \max(\beta, r)$ in the second case.

Note that

$$|G_n| = |G_1|\ell^{4(n-1)} = (\ell^2 - 1)(\ell - 1)\ell^{4n-3}. \tag{2.10}$$

Thus (2.3) will be established as soon as we determine the numerators in (2.9).

Let $\gamma \in G$ with residue class $\overline{\gamma} \in G_1 = \mathrm{GL}(2, \mathbb{F}_\ell)$ be given, and suppose that $\mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}$ with $0 \le \alpha \le \beta$.

2.11 Lemma. *We have*

(I) $0 = \alpha = \beta \Leftrightarrow 1$ *is not an eigenvalue of* $\overline{\gamma}$*. There are* $\ell(\ell^3 - 2\ell^2 - \ell + 3)$ *such elements* $\overline{\gamma} \in G_1$*, among which there are* $\ell(\ell^2 - \ell - 1)$ *with determinant* 1*;*

(II) $0 = \alpha < \beta \Leftrightarrow \overline{\gamma} - 1$ *has rank* 1
$\Leftrightarrow \overline{\gamma}$ *is conjugate to* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *(case* IIa*) or*
$\overline{\gamma}$ *is conjugate to* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ *with* $d \in \mathbb{F}_\ell - \{0, 1\}$ *(case* IIb*).*
There are $\ell^2 - 1$ *(case* IIa*) and* $(\ell + 1)\ell(\ell - 2)$ *(case* IIb*) such* $\overline{\gamma} \in G_1$*;*

(III) $0 < \alpha \le \beta \Leftrightarrow \overline{\gamma} = 1$.

Proof. For $\delta = \gamma - 1$ we have $\mathrm{cok}(\delta)/\ell\, \mathrm{cok}(\delta) = \mathrm{cok}(\overline{\delta})$, and thus the equivalences are obvious. Now the centralizer of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (resp. of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$) in G_1 consists of the matrices of shape $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ (resp. the diagonal matrices) in G_1, from which we find the numbers of $\overline{\gamma}$ subject to condition IIa (resp. IIb) and, finally, of $\overline{\gamma}$ subject to I. There are $\ell^3 - \ell$ elements $\overline{\gamma}$ of determinant 1, of which $\ell^2 - 1$ (resp. 1) are of type II (resp. III), thus $\ell^3 - \ell^2 - \ell$ of type I. □

Next, we need a series of lemmas that count numbers of matrices in M_n with various properties.

2.12 Lemma. (i) *The number of* $\overline{\delta} \in M_1$ *such that* $\det(\overline{\delta}) \neq 0$ *equals* $\ell(\ell^2 - 1)(\ell - 1)$*. A share of* $\ell \cdot (\ell^2 - 1)^{-1}$*, i.e., precisely* $\ell^2(\ell - 1)$ *of them, satisfy* $\mathrm{tr}(\overline{\delta}) = 0$.

(ii) *The number of* $0 \neq \overline{\delta} \in M_1$ *such that* $\det(\overline{\delta}) = 0$ *equals* $(\ell-1)(\ell+1)^2$. *A share of* $(\ell+1)^{-1}$, *i.e., precisely* $\ell^2 - 1$ *of them, satisfy* $\mathrm{tr}(\overline{\delta}) = 0$.

Proof. Omitted. □

2.13 Lemma. *Let* $n \in \mathbb{N}$ *and* $\delta_n \in M_n = \mathrm{Mat}(2, \mathbb{Z}/\ell^n)$ *be given, and suppose that*

$$\mathrm{tr}(\delta_n) + \det(\delta_n) \equiv 0 \ (\ell^n).$$

Then there are precisely ℓ^3 *elements* $\delta_{n+1} \in M_{n+1}$ *such that* $\delta_{n+1} \equiv \delta_n(\ell^n)$ *and*

$$\mathrm{tr}(\delta_{n+1}) + \det(\delta_{n+1}) \equiv 0 \ (\ell^{n+1}).$$

Proof. Writing $\delta_n = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}/\ell^n$, we have

$$(*) \qquad a + d + ad - bc = 0.$$

If $\overline{a} \neq -1$, we write the left hand side as $d(1+a) + a - bc$, choose arbitrary lifts $\tilde{a}, \tilde{b}, \tilde{c}$ of a, b, c in $\mathbb{Z}/\ell^{n+1}$ and solve for $\tilde{d}$ such that $(*)$ holds for $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$. If $\overline{a} = -1$ but $\overline{d} \neq -1$, we may exchange the parts of a and d. If both $\overline{a}$ and $\overline{d}$ equal -1 then $\overline{b}\overline{c} = -1$, we may arbitrarily choose lifts $\tilde{a}, \tilde{b}, \tilde{d}$ of a, b, d and solve for $\tilde{c}$. In any case, we get precisely ℓ^3 matrices $\delta_{n+1} = \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right) \in M_{n+1}$ as required. □

2.14 Lemma. *Let* $0 < \beta < n$ *and* $\overline{d} \in \mathbb{F}_\ell - \{0\}$ *be fixed. The number of matrices* $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_n$ *such that* $\overline{\delta} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & \overline{d} \end{smallmatrix}\right)$ *and* $v_\ell(ad - bc) = \beta$ *is* $(\ell-1)\ell^{4n-4-\beta}$.

Proof. For each of the $(\ell-1)\ell^{n-1-\beta}$ possible values of "det" in $\mathbb{Z}/\ell^n$ with $v_\ell(\det) = \beta$, the quantities b, c and d may be freely chosen subject to $\overline{b} = 0 = \overline{c}$ and $d \equiv \overline{d}(\ell)$, and then $a = d^{-1}(\det + bc)$. □

2.15 Lemma. *Let* $t, u \in \mathbb{Z}/\ell^n$ *be given with* $\overline{t} = 0 = \overline{u}$. *There are precisely* $(\ell^2-1)\ell^{2(n-1)}$ *elements* $\epsilon = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *of* M_n *such that* $\overline{\epsilon} \neq 0$, $\mathrm{tr}(\epsilon) = t$ *and* $\det(\epsilon) = u$.

Proof. Choose $a \in \mathbb{Z}/\ell^n$, which determines $d = t - a$. If $\overline{a} \neq 0$ then $\overline{d} \neq 0$, and we may freely choose $b \in (\mathbb{Z}/\ell^n)^*$ and solve for c in

$$(*) \qquad ad - u = bc.$$

If $\overline{a} = 0$ then $\overline{d} = 0$, either b or c is invertible, and we may solve for the other one in $(*)$. Counting the number of possible choices yields the stated value. □

Now we are ready for the

Proof of Theorem 2.3. At several occasions, we will use the trivial identity

$$(1) \qquad \det(1+\delta) = 1 + \mathrm{tr}(\delta) + \det(\delta)$$

for 2×2-matrices δ. Among other things, it implies (together with (2.4)) that $X_r(\alpha, \beta)$ is empty for $r < \alpha$.

Case $\boxed{\boxed{0 = \alpha = \beta}}$ From (2.9), putting $n = 1$, and (2.11), we see after a little calculation that the volumes of $X(0,0)$ and $X_0(0,0)$ are as asserted. Let $\overline{\gamma} = 1+\overline{\delta} \in G_1$ be such that $\overline{\delta}$ also belongs to G_1. By (2.11), there are precisely $\ell(\ell^2-\ell-1)$ such $\overline{\gamma}$ with determinant 1, i.e., using (1), such that $\mathrm{tr}(\overline{\delta}) + \det(\overline{\delta}) = 0$. By induction on n, using (2.13), we see that among the $\ell^{4(n-1)}$ lifts $\gamma_n = 1+\delta_n$ of $\overline{\gamma}$ to G_n, there are precisely $\ell^{3(n-1)}$ that satisfy $\det(\gamma_n) \equiv 1 \ (\ell^n)$, if $n \geq 2$. For $r \geq 1$ and $n := r+1$, (2.9) yields

$$\mathrm{vol}(X_r(0,0)) = \frac{\ell(\ell^2-\ell-1)\ell^{3(r-1)}(\ell^4-\ell^3)}{(\ell^2-1)(\ell-1)l^{4r+1}} = \frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-r}.$$

Case $\boxed{\boxed{0=\alpha<\beta}}$ According to (2.4) and (2.9), we have for $n > \beta$

$$\mathrm{vol}(X(0,\beta)) = |G_n|^{-1}|\{\gamma \in G_n \mid \overline{\gamma} \neq 1,\ v_\ell(\det(\gamma-1)) = \beta\}|.$$

Any $\gamma = 1+\delta$ as above satisfies (see (2.11)):

- $\overline{\gamma} \in G_1$ is conjugate to $\binom{1\,1}{0\,1}$, which happens ℓ^2-1 times, or
- $\overline{\gamma}$ is conjugate to $\binom{1\,0}{0\,d'}$, which happens $(\ell+1)\ell(\ell-2)$ times.

Thus we have to count the number of lifts $\gamma \in G_n$ of $\overline{\gamma}$ such that $v_\ell(\det(\gamma-1)) = \beta$, i.e., of lifts δ of $\overline{\delta}$ with $v_\ell(\det\delta) = \beta$. Clearly, that number is invariant under conjugation, so we may assume that

- $\overline{\gamma} = \binom{1\,1}{0\,1}$, i.e., $\overline{\delta} = \binom{0\,1}{0\,0}$, or
- $\overline{\gamma} = \binom{1\,0}{0\,d'}$, i.e., $\overline{\delta} = \binom{0\,0}{0\,d}$ with $d = d'-1 \in \mathbb{F}_\ell - \{0,-1\}$.

In both cases, Lemma 2.14 (after possibly permuting the rows of $\overline{\delta}$) yields the same number $(\ell-1)\ell^{4n-4-\beta}$ of lifts of the wanted type. Therefore,

$$\begin{aligned}\mathrm{vol}(X(0,\beta)) &= |G_n|^{-1}[\ell^2-1+(\ell+1)\ell(\ell-2)](\ell-1)\ell^{4n-4-\beta} \\ &= \tfrac{\ell^2-\ell-1}{(\ell-1)\ell}\ell^{-\beta}.\end{aligned}$$

In order to find $\mathrm{vol}(X_r(0,\beta))$, we must determine the number of lifts γ as above that moreover satisfy

$$\det\gamma \equiv 1 \ (\ell^r),\ \not\equiv 1 \ (\ell^{r+1}), \text{ where } r < n, \text{ i.e., } n > \max(\beta, r).$$

Suppose $\boxed{r>0}$ and $\overline{\gamma}$ conjugate to $\binom{1\,1}{0\,1}$, without restriction, $\overline{\gamma} = \binom{1\,1}{0\,1}$, $\overline{\delta} = \binom{0\,1}{0\,0}$. The number of lifts is the number of $\delta = \binom{a\,b}{c\,d} \in M_n$ such that

(2) $a \equiv c \equiv d \equiv 0,\ b \equiv 1 \ (\ell)$
(3) $a+d+ad-bc = \mathrm{tr}(\delta)+\det(\delta) \equiv 0 \ (\ell^r),\ \not\equiv 0 \ (\ell^{r+1})$
(4) $v_\ell(\det\delta) = \beta$

hold. Now there are

- $(\ell-1)\ell^{n-\beta-1}$ choices of $\det(\delta)$ subject to (4);
- ℓ^{n-1} free choices for a and b each subject to (2);
- $(\ell-1)\ell^{n-r-1}$ choices for d compatible with (2), (3) and the choices made of $\det(\delta)$ and a,

which together determine $c = b^{-1}(ad - \det(\delta))$. Therefore, $\overline{\gamma}$ has $(\ell-1)^2\ell^{4(n-1)-r-\beta}$ lifts of the wanted type. If, on the other hand, $\overline{\gamma}$ is conjugate to $\left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$ with $d' \neq 0, 1$, then any lift γ satisfies $\det(\gamma) \not\equiv 1\ (\ell^r)$. Hence

$$\mathrm{vol}(X_r(0,\beta)) = |G_n|^{-1}(\ell^2-1)(\ell-1)^2\ell^{4(n-1)-r-\beta} = \tfrac{\ell-1}{\ell}\ell^{-\beta-r}.$$

Suppose $\boxed{r=0}$. If $\overline{\gamma}$ is unipotent, no lifts of the wanted type exist. Thus let $\overline{\gamma} = \left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$ with $d' \in \mathbb{F}_\ell - \{0,1\}$. Any lift $\gamma \in G_n$ of $\overline{\gamma}$ satisfies $\det(\gamma) \not\equiv 1\ (\ell)$, so we have for $n > \beta$

$$\mathrm{vol}(X_0(0,\beta)) = |G_n|^{-1}(\ell+1)\ell(\ell-2)(\ell-1)\ell^{4n-4-\beta} = \tfrac{\ell-2}{\ell-1}\ell^{-\beta}.$$

It remains to treat the

Case $\boxed{\boxed{0 < \alpha \leq \beta}}$. Here, for $n > \beta$,

$$\mathrm{vol}(X(\alpha,\beta)) = |G_n|^{-1}|\{\gamma \in M_n \mid \overline{\gamma} = 1,\ \mathrm{cok}(\gamma-1) \cong H_{\alpha,\beta}\}|.$$

The condition on $\gamma = 1+\delta$ is equivalent with $\overline{\delta} = 0$, $\mathrm{cok}(\delta) \cong H_{\alpha,\beta}$, i.e., with $\mathrm{cok}(\delta') \cong H_{\alpha-1,\beta-1}$ for $\delta' := \ell^{-1}\delta \in M_{n-1}$. The number of such δ' is given by (2.6) and (2.7), and yields the stated result for $\mathrm{vol}(X(\alpha,\beta))$.

Now to find $\mathrm{vol}(X_r(\alpha,\beta))$, where $r \geq \alpha$, we need to analyze the condition

(5) $\mathrm{cok}(\delta) \cong H_{\alpha,\beta}$, $\det(1+\delta) \equiv 1\ (\ell^r)$, $\not\equiv 1\ (\ell^{r+1})$ for $\delta \in M_n$ and $n > \max(\beta, r)$. Note that $\mathrm{cok}(\delta) \cong H_{\alpha,\beta}$ implies $\delta \equiv 0\ (\ell^\alpha)$, $\not\equiv 0\ (\ell^{\alpha+1})$. Thus, letting $\epsilon := \ell^{-\alpha}\delta \in M_{n-\alpha}$, (5) is equivalent with

(6) $\overline{\epsilon} \neq 0$, $v_\ell(\det\epsilon) = \beta - \alpha$, $\mathrm{tr}(\epsilon) + \ell^\alpha\det(\epsilon) \equiv 0\ (\ell^{r-\alpha})$, $\not\equiv 0\ (\ell^{r-\alpha+1})$.

Suppose $\boxed{\alpha=\beta}$. If $\boxed{r=\alpha}$ then (6) is equivalent with $\epsilon \in G_{n-\alpha}$, $\mathrm{tr}(\overline{\epsilon}) \neq 0$, and the volume of $X_\alpha(\alpha,\alpha)$ comes out by (2.9) along with (2.12), putting $n = \alpha+1$.

Each of the $\ell^2(\ell-1)$ elements $\delta = \delta_{\alpha+1} \in M_{\alpha+1}$ subject to

$$\mathrm{cok}(\delta) \cong H_{\alpha,\alpha},\ \mathrm{tr}(\delta) \equiv 0\ (\ell^{\alpha+1})$$

has precisely $\ell^{3(n-\alpha-1)}$ lifts δ_n to M_n $(n \geq \alpha+1)$ such that

$$\mathrm{tr}(\delta_n) + \det(\delta_n) \equiv 0\ (\ell^n),$$

by (2.13). Therefore, for $\boxed{r > \alpha}$,

$$\begin{aligned}|\{\delta \in M_{r+1} \mid \mathrm{cok}(\delta) \cong H_{\alpha,\alpha},\ \mathrm{tr}(\delta)+\det(\delta) \equiv 0\ (\ell^r),\ \not\equiv 0\ (\ell^{r+1})\}|\\ = \ell^2(\ell-1)\ell^{3(r-\alpha-1)}(\ell^4-\ell^3),\end{aligned}$$

which together with (2.9) yields the stated result for $\mathrm{vol}(X_r(\alpha,\alpha))$.

Suppose $\boxed{\alpha < \beta}$. By virtue of Lemma 2.15, we have for $r > \alpha$ and $n >$

$\max(\beta, r)$:

$$|\{\epsilon \in M_{n-\alpha} \mid \overline{\epsilon} \neq 0,\ v_\ell(\det \epsilon) = \beta - \alpha,\ \mathrm{tr}(\epsilon) + \ell^\alpha \det(\epsilon) \equiv 0\ (\ell^{r-\alpha}),$$
$$\not\equiv 0\ (\ell^{r-\alpha+1})\}|$$
$$= (\ell^2 - 1)\ell^{2(n-\alpha-1)} \mid \{(t,u) \in \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n \mid (t,u) \text{ subject to } (7)\}|$$

with the condition

$$(7)\ \ \overline{t} = 0 = \overline{u},\ v_\ell(u) = \beta - \alpha,\ t + \ell^\alpha u \equiv 0\ (\ell^{r-\alpha}),\ \not\equiv 0\ (\ell^{r-\alpha+1}).$$

For the number of these pairs (t,u), we find $(\ell-1)^2\ell^{2n-\beta-r-2}$, which yields $\mathrm{vol}(X_r(\alpha,\beta))$ for $r > \alpha$. Finally,

$$\mathrm{vol}(X_\alpha(\alpha,\beta)) = \mathrm{vol}(X(\alpha,\beta)) - \sum_{r>\alpha} \mathrm{vol}(X_r(\alpha,\beta)),$$

which allows to fill in the last missing entry in the statement of Theorem 2.3. □

(2.16) Put $X_r := \{\gamma \in G \mid v_\ell(\det(\gamma) - 1) = r\}$. We have the obvious formula

$$\mathrm{vol}_\nu(X_r) = \begin{cases} \frac{\ell-2}{\ell-1}, & r = 0 \\ \ell^{-r}, & r > 0. \end{cases}$$

Then we may interpret Theorem 2.3 as follows. Define for $0 \le \alpha \le \beta$, $r \ge 0$ and $(r,\ell) \neq (0,2)$:

$$(2.17)\qquad g_r(\alpha,\beta) := \frac{\mathrm{vol}_\nu(X_r(\alpha,\beta))}{\mathrm{vol}_\nu(X_r)},$$

and recall that $g(\alpha,\beta) = \mathrm{vol}_\nu(X(\alpha,\beta))$. Then

$$g(\alpha,\beta) = \text{probability of } \gamma \in G \text{ to satisfy } \mathrm{cok}(\gamma - 1) \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$$

and

$$g_r(\alpha,\beta) = \text{probability for the same event under the assumption } v_\ell(\det(\gamma)-1) = r.$$

2.18 Corollary. *The conditional probability $g_r(\alpha,\beta)$ is zero if $r < \alpha$, and otherwise is given by the table below, where the two entries marked with "$*$" are undefined for $\ell = 2$.*

$g_r(\alpha,\beta)$	$r = \alpha$	$r > \alpha$
$0 = \alpha = \beta$	$\frac{\ell-2}{\ell-1}$ $*$	$\frac{\ell^2-\ell-1}{\ell^2-1}$
$0 = \alpha < \beta$	$\ell^{-\beta}$ $*$	$\frac{\ell-1}{\ell}\ell^{-\beta}$
$0 < \alpha = \beta$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-3\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha}$
$0 < \alpha < \beta$	$\ell^{-\beta-2\alpha}$	$\frac{\ell-1}{\ell}\ell^{-\beta-2\alpha}$

That is, we have $g_r(\alpha,\beta) = \pi_r(\alpha,\beta)\ell^{-\beta-2\alpha}$ with some factor $\pi_r(\alpha,\beta) \in \{0, \frac{\ell-2}{\ell-1}, \frac{\ell^2-\ell-1}{\ell^2-1}, \frac{\ell-1}{\ell}, \frac{\ell}{\ell+1}, 1\}$. Note that

(2.19) $\pi_r(\alpha,\alpha)$ *increases* if $r = \alpha$ is replaced with $r > \alpha$. On the other hand, if α is less than β then $\pi_r(\alpha,\beta)$ *decreases* upon enlarging r from α to $r > \alpha$. In any case, $g_r(\alpha,\beta)$ is independent of r as long as $r > \alpha$.

3. Probabilities of group structures.

We first summarize some results of E. Howe from [7], which will play a crucial role.

(3.1) Define the multiplicative arithmetic functions φ and ψ through their values on prime powers ℓ^α, $\alpha \geq 1$:

$$\varphi(\ell^\alpha) = \ell^{\alpha-1}(\ell-1), \quad \psi(\ell^\alpha) = \ell^{\alpha-1}(\ell+1),$$

i.e., φ is the Euler function. Further, given a prime number $p \geq 5$ and $m, n \in \mathbb{N}$ with $m|n$, put

$$w_p(m,n) = \frac{1}{2} \sum_{E(\mathbb{F}_p)[n] \cong \mathbb{Z}/m \times \mathbb{Z}/n} w(E/\mathbb{F}_p),$$

where E runs through the $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with the property that $E(\mathbb{F}_p)[n] \cong \mathbb{Z}/m \times \mathbb{Z}/n$. Up to the factor $\frac{1}{2}$ (introduced to be in keeping with [7]), $w_p(m,n)$ is a weighted cardinality $|\ |^*$ in the sense of (1.9). Howe defines the approximation

$$\hat{w}_p(m,n) = p\frac{\psi(n/m)}{m\varphi(n)\psi(n)} \prod_{\ell | \gcd(n,p-1)/m} (1-\ell^{-1}), \tag{3.2}$$

where ℓ runs through the prime divisors of $\gcd(n,p-1)/m$, if $m|p-1$, and $\hat{w}_p(m,n) = 0$ otherwise. Note that

$$p^{-1}w_p(1,1) = p^{-1}\hat{w}_p(1,1) = 1. \tag{3.3}$$

On p. 245 of [7], he obtains the inequality

$$|w_p(m,n) - \hat{w}_p(m,n)| \leq C(m,n)p^{1/2} \tag{3.4}$$

with the constant

$$C(m,n) = (1/12 + 5/6\sqrt{2})\psi(n/m)2^{\omega(n)}$$

independent of p. Here $\omega(n) :=$ number of different prime divisors of n. Briefly,

$$w_p(m,n) = \hat{w}_p(m,n) + O_{m,n}(p^{1/2}).$$

It is obvious that the 2-variable function $p^{-1}\hat{w}_p(m,n)$ localizes, that is

$$p^{-1}\hat{w}_p(m,n) = \prod_\ell p^{-1}\hat{w}_p(\ell^{\alpha_\ell}, \ell^{\beta_\ell}) \tag{3.5}$$

if $m = \prod_\ell \ell^{\alpha_\ell}$, $n = \prod_\ell \ell^{\beta_\ell}$, $0 \leq \alpha_\ell \leq \beta_\ell$ with pairwise different prime numbers ℓ. The factors on the right hand side are simple functions of ℓ, α_ℓ, β_ℓ and

$$r(p,\ell) := r \in \mathbb{N}_0 \text{ such that } \ell^r \| p-1,$$

i.e., the dependence on p is via $r(p,\ell)$ only. We therefore define for $0 \leq \alpha \leq \beta$:

$$h_r^{(\ell)}(\alpha,\beta) := p^{-1}\hat{w}_p(\ell^\alpha, \ell^\beta), \tag{3.6}$$

where $r = r(p,\ell)$. It vanishes for $r < \alpha$; otherwise, its values are given by the following table.

3.7 Table for $h_r^{(\ell)}(\alpha,\beta)$.

	$r=\alpha$	$r>\alpha$
$0=\alpha=\beta$	1	1
$0=\alpha<\beta$	$\frac{\ell}{\ell-1}\ell^{-\beta}$	$\ell^{-\beta}$
$0<\alpha=\beta$	$\frac{\ell^2}{\ell^2-1}\ell^{-3\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha}$
$0<\alpha<\beta$	$\frac{\ell}{\ell-1}\ell^{-\beta-2\alpha}$	$\ell^{-\beta-2\alpha}$

Fix ℓ, α and β for the moment, and let

$$H=H_{\alpha,\beta}^{(\ell)}=\mathbb{Z}/\ell^\alpha\times\mathbb{Z}/\ell^\beta.$$

From the above, replacing w_p by its approximation $\hat{w}_p$, and taking (1.9) into account, we may regard

$$h_r^{(\ell)}(\alpha,\beta)\approx\frac{|\{E/\mathbb{F}_p\mid E(\mathbb{F}_p)[\ell^\beta]\cong H\}|^*}{|\{E/\mathbb{F}_p\}|^*}$$

as the probability that a randomly chosen $E/\mathbb{F}_p$ (with our *fixed* p subject to $r(p,\ell)=r$) satisfies "$E(\mathbb{F}_p)[\ell^\beta]\cong H$". The associated probability of "$E(\mathbb{F}_p)[\ell^\infty]\cong H$" is

$$(3.8)\qquad \begin{aligned} g_r^{(\ell)}(\alpha,\beta) &:= h_r^{(\ell)}(\alpha,\beta)-h_r^{(\ell)}(\alpha,\beta+1), \\ &\qquad r=0 \text{ or } r>0,\ \alpha<\beta \\ &= h_r^{(\ell)}(\alpha,\alpha)-h_r^{(\ell)}(\alpha,\alpha+1)-h_r^{(\ell)}(\alpha+1,\alpha+1), \\ &\qquad r>0,\ \alpha=\beta \end{aligned}$$

since, e.g., the event "$E(\mathbb{F}_p)[\ell^\infty]\cong\mathbb{Z}/\ell^\alpha\times\mathbb{Z}/\ell^\beta$" for $\alpha<\beta$ is equivalent with: "$E(\mathbb{F}_p)[\ell^\beta]\cong\mathbb{Z}/\ell^\alpha\times\mathbb{Z}/\ell^\beta$" but not "$E(\mathbb{F}_p)[\ell^{\beta+1}]\cong\mathbb{Z}/\ell^\alpha\times\mathbb{Z}/\ell^{\beta+1}$".

More precisely, we get from (3.4) that

$$(3.9)\qquad \frac{|\{E/\mathbb{F}_p\mid E(\mathbb{F}_p)[\ell^\infty]\cong H\}|^*}{|\{E/\mathbb{F}_p\}|^*}=g_r^{(\ell)}(\alpha,\beta)+O_{\ell,\alpha,\beta}(p^{-1/2}),$$

where the constant implied by the O-symbol depends only on ℓ,α,β (and may easily be determined). Evaluating (3.8) by means of (3.7), which requires a number of case distinctions, we find:

(3.10) The present $g_r^{(\ell)}(\alpha,\beta)$ agrees with the conditional probability (where ℓ,α,β are fixed) $g_r(\alpha,\beta)$ defined in (2.17) and described by the table in (2.18).

So far, p has been fixed. Letting p vary subject to $r(p,\ell)=r$ with some fixed r and taking (1.10) into account yields for $p\le x\in\mathbb{R}$:

$$(3.11)\qquad \begin{aligned} &|\{E/\mathbb{F}_p\in\mathcal{F}\mid p\le x,\ r(p,\ell)=r,\ E(\mathbb{F}_p)[\ell^\infty]\cong H\}|^* \\ &=2g_r^{(\ell)}(\alpha,\beta)\textstyle\sum p+O_{\ell,\alpha,\beta}(\sum p^{1/2}), \end{aligned}$$

where the sum in both cases ranges through

$$\{p\in\mathbb{P}\mid p\le x,\ r(p,\ell)=r\}=\{p\le x\mid \ell^r\|p-1\}.$$

(Strictly speaking, we had to assume that $p \geq 5$, but including $p = 2, 3$ doesn't change the asymptotic behavior. Thus we will neglect from now on the restriction of $p \geq 5$.)

We need a well-known fact from analytic number theory, an explicit reference of which is nonetheless difficult to find.

3.12 Proposition. *Let $\gamma > -1$ be a real number and a, m coprime natural numbers. Then*

$$\sum_{\substack{p \leq x \text{ prime} \\ p \equiv a \ (m)}} p^\gamma \sim \frac{1}{\varphi(m)} \frac{1}{1+\gamma} \frac{x^{1+\gamma}}{\log x} ,$$

where "$\sim$" denotes asymptotic equivalence.

Proof (sketch). Note that the assertion includes the prime number theorem ($\gamma = 0$, $m = 1$) and Dirichlet's theorem on primes in arithmetic progressions ($\gamma = 0$). The general case ($\gamma > -1$ arbitrary) results from the case $\gamma = 0$ by Abel summation (see the instructions and notation given in [9] pp. 3,4) of the series $\sum_{n \leq x} a_n b(n)$ with

$$a_n = \begin{cases} 1, & n \equiv a(m), \ n \text{ prime} \\ 0, & \text{otherwise,} \end{cases}$$

and the C^1-function b with $b(x) = x^\gamma$. □

In particular,

$$\sum_{\substack{p \leq x \\ r(p,\ell) = r}} p^{1/2} \sim \frac{2}{3}\left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right)\frac{x^{3/2}}{\log x},$$

so the expression in (3.11) becomes

$$2g_r^{(\ell)}(\alpha,\beta)\sum p + \left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right)O_{\ell,\alpha,\beta}\left(\frac{x^{3/2}}{\log x}\right).$$

Applying (3.12) also to the first sum $\sum p$ in (3.11) yields

$$\begin{aligned} &\frac{|\{E/\mathbb{F}_p \mid p \leq x, \ r(p,\ell) = r, \ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x, \ r(p,\ell) = r\}|^*} \\ &= g_r^{(\ell)}(\alpha,\beta) + O_{\ell,\alpha,\beta}(x^{-1/2}), \end{aligned} \tag{3.13}$$

where the implied constant depends only on ℓ, α, β but not on r. Apart from the condition "$r(p,\ell) = r$", this expresses $g_r^{(\ell)}(\alpha,\beta)$ as a probability in the sense of (1.4). It remains to evaluate

$$P\{\mathcal{F}, \text{"}E(\mathbb{F}_p)[\ell^\infty] \cong H\text{"}\} = \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p \mid p \leq x, \ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*}.$$

It is tempting to calculate it via the conditional probabilities $g_r^{(\ell)}(\alpha,\beta)$ simply as

$$\sum_{r \geq 0}\left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right)g_r^{(\ell)}(\alpha,\beta),$$

where $\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})} = \mathrm{vol}_\nu(X_r)$ (see (2.16)) is the probability of p to satisfy $r(p,\ell) = r$. This will turn out to be true, but requires reversing the order in which we evaluate a double limit, and needs to be justified.

We have

$$\begin{aligned} &|\{E/\mathbb{F}_p \mid p \le x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^* \\ = &\textstyle\sum_{r\ge 0}[2g_r^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)=r}} p + (\frac{1}{\varphi(\ell^{r+1})} - \frac{1}{\varphi(\ell^{r+1})})O_{\ell,\alpha,\beta}(\frac{x^{3/2}}{\log x})]. \end{aligned}$$

Now $g_r^{(\ell)}(\alpha,\beta) = 0$ if $r < \alpha$ and $g_r^{(\ell)}(\alpha,\beta) = g_{\alpha+1}^{(\ell)}(\alpha,\beta)$ for $r > \alpha$. Therefore, the above is

$$2g_\alpha^{(\ell)}(\alpha,\beta) \sum_{\substack{p\le x\\ r(p,\ell)=\alpha}} p + 2g_{\alpha+1}^{(\ell)}(\alpha,\beta) \sum_{\substack{p\le x\\ r(p,\ell)>\alpha}} p + O_{\ell,\alpha,\beta}(x^{3/2}/\log x).$$

From (3.12) and (2.17) we find that

$$\begin{aligned} 2g_\alpha^{(\ell)}(\alpha,\beta)\textstyle\sum_{\substack{p\le x\\ r(p,\ell)=\alpha}} p &\sim \mathrm{vol}_\nu(X_\alpha(\alpha,\beta))x^2/\log x, \\ 2g_{\alpha+1}^{(\ell)}(\alpha,\beta)\textstyle\sum_{\substack{p\le x\\ r(p,\ell)>\alpha}} p &\sim \tfrac{\ell}{\ell-1}\mathrm{vol}_\nu(X_{\alpha+1}(\alpha,\beta))x^2/\log x. \end{aligned}$$

Comparing with (2.3) yields in all the four cases

$$\mathrm{vol}_\nu(X_\alpha(\alpha,\beta)) + \tfrac{\ell}{\ell-1}\mathrm{vol}_\nu(X_{\alpha+1}(\alpha,\beta)) = g^{(\ell)}(\alpha,\beta).$$

Thus, dividing by $|\{E/\mathbb{F}_p \mid p \le x\}|^* = 2\sum_{p\le x} p \sim x^2/\log x$, we finally get

$$\text{(3.14)} \qquad \frac{|\{E/\mathbb{F}_p \mid p \le x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \le x\}|^*} = g^{(\ell)}(\alpha,\beta) + O_{\ell,\alpha,\beta}(x^{-\frac{1}{2}}).$$

Hence, in fact

$$P(\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H\text{”}) = g^{(\ell)}(\alpha,\beta) = \mathrm{vol}_\nu(X(\alpha,\beta)),$$

where $X(\alpha,\beta) = X^{(\ell)}(\alpha,\beta)$ is the ℓ-adic set defined in (2.2).

We may summarize our results (3.13) and (3.14) as follows.

3.15 Theorem. *Let a prime number ℓ and $0 \le \alpha \le \beta$ be given.*

- (i) *The probability $P(\mathcal{F}$, “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$”) in the sense of* (1.4) *exists and equals the value $g^{(\ell)}(\alpha,\beta)$ given in* (2.3).
- (ii) *Fix moreover a non-negative integer r. The conditional probability $P(\mathcal{F}$, “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$” | “$\ell^r \| p-1$”) for “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$” under the assumption “$\ell^r \| p-1$” exists and equals the value of $g_r^{(\ell)}(\alpha,\beta)$ given in* (2.18).

In both cases the error terms are $O_{\ell,\alpha,\beta}(x^{-1/2})$.

Note that the probabilities thus found are those predicted by the hypothesis (H) formulated in the introduction.

3.16 Example. We consider the probability that the 2-part of $E(\mathbb{F}_p)$ is isomorphic with $H = \mathbb{Z}/4 \times \mathbb{Z}/4$ under congruence conditions for p. According to (3.15), it is

$$1/3 \cdot 2^{-6} \quad \text{for } p \equiv 5\ (8)$$

and *increases* to

$$2/3 \cdot 2^{-6} \quad \text{for } p \equiv 1\ (8).$$

If we replace H by $H' = \mathbb{Z}/4 \times \mathbb{Z}/8$, the probability is

$$2^{-7} \quad \text{for } p \equiv 5\ (8)$$

and *decreases* to

$$2^{-8} \quad \text{for } p \equiv 1\ (8).$$

4. The probability spaces.

Theorem 3.15 has the drawback that it relies on the ad hoc notion (1.4) of probability and does not involve probability spaces in the ordinary sense. Here we will remedy this defect and put (3.15) in the framework of "ordinary" probability theory.

(4.1) For what follows, we fix a prime ℓ and put $\mathfrak{X}^{(\ell)}$ for the set of all pairs (H, r), where H is a group of shape $\mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$ with $0 \leq \alpha \leq \beta$ and $\alpha \leq r \in \mathbb{N}_0$. Hence elements of $\mathfrak{X}^{(\ell)}$ correspond bijectively to triples $(\alpha, \beta, r) \in \mathbb{N}_0^3$ with $\alpha \leq \min(\beta, r)$, which we often use as an identification. By (2.3), the function

$$P^{(\ell)} : (\alpha, \beta, r) \longmapsto \mathrm{vol}_\nu(X_r^{(\ell)}(\alpha, \beta))$$

turns $\mathfrak{X}^{(\ell)}$ into a discrete probability space (d.p.s.). (By a d.p.s. we understand a countable set provided with a probability measure in which each non-empty subset is measurable with positive volume.)

Given $(H_{\alpha,\beta}^{(\ell)}, r) = (\alpha, \beta, r) \in \mathfrak{X}^{(\ell)}$, we define

$$A_{\alpha,\beta,r} := \{E/\mathbb{F}_p \in \mathcal{F} \mid E(\mathbb{F}_p)[\ell^\infty] \cong H_{\alpha,\beta}^{(\ell)},\ r(p,\ell) = r\}.$$

We further let $\mathfrak{A}^{(\ell)}$ be the σ-algebra of subsets of $\mathcal{F}$ generated by all the sets $A_{\alpha,\beta,r}$. Hence the elements of $\mathfrak{A}^{(\ell)}$ are the subsets $A_{\mathfrak{Y}}$ of $\mathcal{F}$, where $\mathfrak{Y}$ is an arbitrary (finite or countably infinite) subset of $\mathfrak{X}^{(\ell)}$ and

$$A_{\mathfrak{Y}} = \bigcup_{(\alpha,\beta,r) \in \mathfrak{Y}} A_{\alpha,\beta,r} \quad \text{(disjoint union)}.$$

4.2 Proposition. *For each subset $\mathfrak{Y}$ of $\mathfrak{X}^{(\ell)}$, the limit $P(\mathcal{F}, A_{\mathfrak{Y}})$ as in* (1.4) *exists, and is given as* $\sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r})$.

Here $P(\mathcal{F}, A_{\alpha,\beta,r}) = P(\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta},\ r(p,\ell) = r\text{”}) = \mathrm{vol}_\nu(X_r^{(\ell)}(\alpha,\beta))$ *by* (3.15).

Proof. We must check the identity

$$(?) \qquad \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p\in\mathcal{F} \mid p\leq x,\ (E(\mathbb{F}_p)[\ell^\infty],\ r(p,\ell))\in\mathfrak{Y}\}|^*}{|\{E/\mathbb{F}_p\in\mathcal{F} \mid p\leq x\}|^*} = \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}),$$

which is obvious from (3.15) if $\mathfrak{Y}$ is finite. Let $f_{\mathfrak{Y}}(x)$ be the argument of the limit in the left hand side of (?). Then for each finite subset $\mathfrak{Y}_0$ of $\mathfrak{Y}$,

$$\liminf_{x\to\infty} f_{\mathfrak{Y}}(x) \geq \sum_{(\alpha,\beta,r)\in\mathfrak{Y}_0} P(\mathcal{F}, A_{\alpha,\beta,r}),$$

thus

$$\liminf_{x\to\infty} f_{\mathfrak{Y}}(x) \geq \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}).$$

If $\mathfrak{Y}^c$ denotes the complement $\mathfrak{X}^{(\ell)} - \mathfrak{Y}$ of $\mathfrak{Y}$, we have $A_{\mathfrak{Y}^c} = \mathcal{F} - A_{\mathfrak{Y}}$ and $f_{\mathfrak{Y}^c}(x) = 1 - f_{\mathfrak{Y}}(x)$. Thus reversing the parts of $\mathfrak{Y}$ and $\mathfrak{Y}^c$ yields

$$\limsup_{x\to\infty} f_{\mathfrak{Y}}(x) \leq \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}).$$

$\square$

As a consequence of (4.2), the function $P(\mathcal{F}, \cdot)$ is countably additive on $\mathfrak{A}^{(\ell)}$ and therefore a probability measure. The following is then obvious.

4.3 Corollary. *The σ-algebra $\mathfrak{A}^{(\ell)}$ provided with its probability measure $P(\mathcal{F}, \cdot)$ is canonically isomorphic with the discrete probability space $(\mathfrak{X}^{(\ell)}, P^{(\ell)})$.*

It is easy to generalize the preceding to cover the case of events that involve a finite number of primes ℓ. Thus let $L \subset \mathbb{P}$ be a finite set of primes. The cartesian product

$$\mathfrak{X}^{(L)} = \prod_{\ell\in L} \mathfrak{X}^{(\ell)}$$

provided with the product measure $P^{(L)}$ is itself a d.p.s. On the other hand, given $\mathbf{x} = (\alpha_\ell, \beta_\ell, r_\ell)_{\ell\in L} \in \mathfrak{X}^{(L)}$, we define

$$A_{\mathbf{x}} := \{E/\mathbb{F}_p \in \mathcal{F} \mid \forall \ell \in L : E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha_\ell,\beta_\ell},\ r(p,\ell) = r_\ell\}$$

and let $\mathfrak{A}^{(L)}$ be the σ-algebra in $\mathcal{F}$ generated by all the $A_{\mathbf{x}}$, $\mathbf{x} \in \mathfrak{X}^{(L)}$. Then $\mathfrak{A}^{(L)} = \{A_{\mathfrak{Y}} \mid \mathfrak{Y} \subset \mathfrak{X}^{(L)}\}$ with the obvious definition $A_{\mathfrak{Y}} := \bigcup_{\mathbf{x}\in\mathfrak{Y}} A_{\mathbf{x}}$.

4.4 Proposition.

(i) *For* $\mathbf{x} = (\alpha_\ell, \beta_\ell, r_\ell)_{\ell\in L} \in \mathfrak{X}^{(L)}$,

$$P(\mathcal{F}, A_{\mathbf{x}}) = \prod_{\ell\in L} P(\mathcal{F}, A_{\alpha_\ell,\beta_\ell,r_\ell})$$

holds.

(ii) *For each subset* $\mathfrak{Y}$ *of* $\mathfrak{X}^{(L)}$, *the limit* $P(\mathcal{F}, A_{\mathfrak{Y}})$ *exists, and is given as* $\sum_{\mathbf{x}\in\mathfrak{Y}} P(\mathcal{F}, A_{\mathbf{x}})$.

Proof. (i) is a formal consequence of (3.4), (3.5) and (3.15). We omit the details. The proof of (ii) is then identical to that of (4.2). □

As in the case of one single prime, (4.4)(ii) implies that $P(\mathcal{F}, \cdot)$ is a probability measure on $\mathcal{A}^{(L)}$. In view of (4.4)(i) we get:

4.5 Corollary. *The* σ*-algebra* $\mathfrak{A}^{(L)}$ *provided with its probability measure* $P(\mathcal{F}, \cdot)$ *is canonically isomorphic with the d.p.s.* $(\mathfrak{X}^{(L)}, P^{(L)})$. *In particular, the restrictions of* $P(\mathcal{F}, \cdot)$ *to the various* $\mathfrak{A}^{(\ell)}$ $(\ell \in L)$ *are stochastically independent on* $\mathfrak{A}^{(L)}$.

4.6 Remark. For a number of reasons, no simple generalizations of (4.4) and (4.5) to infinite subsets $L \subset \mathbb{P}$ are in sight. For example, the union $\bigcup_{L_0\in L \text{ finite}} \mathfrak{A}^{(L_0)}$ is not a σ-algebra, $\prod_{\ell\in L} \mathfrak{X}^{(\ell)}$ is uncountable, and problems on the convergence of infinite products and their commutation with limits arise. Therefore, events in $\mathcal{F}$ that involve an infinite number of primes ℓ are a priori not covered by the above, and are more difficult to study. In (5.9), we investigate a significant instance of such an event, namely the property of cyclicity of $E(\mathbb{F}_p)$.

5. Some applications.

We use the preceding results to derive probabilities/expectations associated with some elementary properties of $E/\mathbb{F}_p \in \mathcal{F}$.

We start with divisibility by a fixed $n \in \mathbb{N}$.

5.1 Proposition. *Let a prime power* ℓ^a *and* $r \in \mathbb{N}_0$ *be given.*

(i) *The probability that* ℓ^a *divides* $|E(\mathbb{F}_p)|$ *equals*

$$P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”}) = \ell^{-a}\frac{\ell^3 - \ell - \ell^{2-a}}{(\ell^2-1)(\ell-1)}.$$

(ii) *The conditional probability for the same event under the assumption* $\ell^r \| p-1$ *equals*

$$\begin{aligned} P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”} \mid \text{“}\ell^r\|p-1\text{”}) \quad &= \\ \ell^{-a}\tfrac{\ell}{\ell-1}, \qquad & r < a/2 \\ \ell^{-a}\tfrac{\ell^2+\ell-\ell^{1-(a-1)/2}}{\ell^2-1}, \qquad & r > a/2,\ a \text{ odd} \\ \ell^{-a}\tfrac{\ell^2+\ell-\ell^{1-a/2}}{\ell^2-1}, \qquad & r \geq a/2,\ a \text{ even.} \end{aligned}$$

Proof. By virtue of (4.2), $P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”})$ exists and is given by $\sum g^{(\ell)}(\alpha,\beta)$, where $0 \leq \alpha \leq \beta$ and $\alpha+\beta \geq a$. The conditional probability in (ii) is given by the same expression, but $g^{(\ell)}(\alpha,\beta)$ replaced by $g_r^{(\ell)}(\alpha,\beta)$.

The stated formulae result from a lengthy but elementary calculation using (2.3) and (2.18), which will be omitted. □

5.2 COROLLARY. *For arbitrary $n \in \mathbb{N}$ with factorization $n = \prod \ell^{a_\ell}$ into primes ℓ, $P(\mathcal{F}$, "$n \mid |E(\mathbb{F}_p)|$") is given by*

$$n^{-1} \prod_{\ell | n} \frac{\ell^3 - \ell - \ell^{2-a_\ell}}{(\ell^2-1)(\ell-1)}.$$

Note that all the probabilities figuring in (5.1) and (5.2) are slightly larger than n^{-1}, the value naively expected. The probability of "$n \mid |E(\mathbb{F}_q)|$" over a *fixed* field $\mathbb{F}_q$ (i.e., the share of those $E/\mathbb{F}_q$ with the divisibility property) has been determined by Howe in [7].

(5.3) For any function $f : \mathcal{F} \longrightarrow \mathbb{R}$, we define the expectation $E(\mathcal{F}, f)$ (provided the limit exists) as

$$E(\mathcal{F}, f) = \lim_{x \to \infty} \frac{\sum f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*},$$

where the sum in the numerator is over all objects $E/\mathbb{F}_p \in \mathcal{F}$ with $p \leq x$. Restricting the domain $\mathcal{F}$ (for example by requiring congruence conditions on p), we may also define the expectation of f on subsets $\mathcal{F}'$ of $\mathcal{F}$. Given a prime number ℓ, we call f

- OF TYPE ℓ, if $f(E/\mathbb{F}_p)$ depends only on $E(\mathbb{F}_p)[\ell^\infty]$;
- WEAKLY OF TYPE ℓ, if $f(E/\mathbb{F}_p)$ depends only on $E(\mathbb{F}_p)[\ell^\infty]$ and $r(p, \ell)$.

If these conditions hold, we regard f as a function on the set of groups of shape $H^{(\ell)}_{\alpha,\beta}$ (or on the set $\mathfrak{X}^{(\ell)}$, respectively), see (4.1). More concretely, ℓ being fixed, f is a function on pairs (α, β) with $0 \leq \alpha \leq \beta$ if it is of type ℓ, and is a function on triples (α, β, r) with $0 \leq \alpha \leq \min(\beta, r)$ if it is weakly of type ℓ.

5.4 LEMMA.

(i) *Suppose that f is bounded and of type ℓ. Then $E(\mathcal{F}, f)$ is defined and agrees with the sum*

$$\sum_{\substack{\alpha,\beta \in \mathbb{N}_0 \\ \alpha \leq \beta}} f(\alpha, \beta) g^{(\ell)}(\alpha, \beta).$$

(ii) *Suppose that f is bounded and weakly of type ℓ, and let $r \in \mathbb{N}_0$ be given. Then the expectation $E(\mathcal{F}, f$, "$\ell^r \| p-1$") of f on $\{E/\mathbb{F}_p \mid \ell^r \| p-1\}$ is defined and agrees with*

$$\sum_{\substack{\alpha,\beta \in \mathbb{N}_0 \\ \alpha \leq \min(\beta, r)}} f(\alpha, \beta, r) g^{(\ell)}_r(\alpha, \beta).$$

Proof. We restrict to showing (i); the proof of (ii) is similar. Let E be the value of the absolutely convergent sum

$$\sum_{0 \leq \alpha \leq \beta} f(\alpha, \beta) g^{(\ell)}(\alpha, \beta),$$

and let $\epsilon > 0$ be given. In view of the absolute convergence, there exists a finite subset $\mathfrak{Y} \subset \{(\alpha, \beta) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid \alpha \leq \beta\}$ such that

$$\sum_{(\alpha,\beta)\notin\mathfrak{Y}} |f(\alpha, \beta)| g^{(\ell)}(\alpha, \beta) < \frac{\epsilon}{3}.$$

Let $n = |\mathfrak{Y}|$ and let x_0 be chosen sufficiently large such that for each $(\alpha, \beta) \in \mathfrak{Y}$ and each $x \geq x_0$, we have

$$|f(\alpha, \beta)| \mid g^{(\ell)}(\alpha, \beta) - \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*}| \leq \epsilon/3n.$$

Then for $x \geq x_0$,

$$|\sum_{(\alpha,\beta)\in\mathfrak{Y}} f(\alpha, \beta) \frac{|\{E/\mathbb{F}_p \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*} - E| < 2\epsilon/3$$

holds. According to (4.2), and since $f(\alpha, \beta)$ is bounded, we find x_1 such that for $x \geq x_1$, we have

$$\sum_{(\alpha,\beta)\notin\mathfrak{Y}} |f(\alpha, \beta)| \frac{|\{E/\mathbb{F}_p \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*} < \epsilon/3.$$

Thus for $x \geq \max(x_0, x_1)$,

$$\frac{\sum_{p\leq x} f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*}$$

differs by less than ϵ from E. $\square$

We apply (5.4) to the function $\kappa_n : \mathcal{F} \longrightarrow \mathbb{R}$ defined by

(5.5) $\kappa_n(E/\mathbb{F}_p)$ = number of points of precise order n in $E(\mathbb{F}_p)$ for $n \in \mathbb{N}$.

5.6 PROPOSITION. *Let a prime power $n = \ell^a$ and a non-negative integer r be given. The expectation $E(\mathcal{F}, \kappa_n,$ "$\ell^r \| p-1$"$)$ for κ_n on $\{E/\mathbb{F}_p \mid \ell^r \| p-1\}$ exists and equals* 1 *independently of r. Thus the total expectation $E(\mathcal{F}, \kappa_n)$ exists on $\mathcal{F}$ and equals* 1.

Proof. κ_n is bounded by $n^2 = \ell^{2a}$ and of type ℓ, thus by (5.4),

$$E(\mathcal{F}, \kappa_n, \text{“}\ell^r \| p-1\text{”}) = \sum_{\substack{\alpha,\beta\in\mathbb{N}_0 \\ \alpha\leq\min(\beta,r)}} \kappa_n(\alpha, \beta) g_r^{(\ell)}(\alpha, \beta).$$

Now $\kappa_n(\alpha, \beta)$ = number of elements of precise order ℓ^a in $\mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$ is easily determined; we refrain from writing down the result. Evaluating after that the right hand side above is an elementary but - due to the numerous cases - laborious exercise in summing multiple geometric series. In each of the cases, the result turns out to 1. $\square$

5.7 COROLLARY. *For each natural number n, the expectation $E(\mathcal{F}, \kappa_n)$ exists and equals* 1.

Proof. Since only the finitely many prime divisors ℓ of n are involved and κ_n is multiplicative in n, (4.4) allows to reduce the general case to (5.6). We omit the details. $\square$

5.8 Remark. The just established results on $E(\mathcal{F},\kappa)$ are "formal facts" that can be seen by "pure thought", and avoiding the extended calculations with the values of $g_r^{(\ell)}(\alpha,\beta)$. Namely, taking into account that $\kappa_n(E/\mathbb{F}_p)$ equals the number of fixed points of Frobenius on the points of precise order n of $E(\overline{\mathbb{F}}_p)$, (5.7) is almost immediate from (H) and Burnside's lemma. I owe that hint to Bas Edixhoven [4].

We conclude with determining the asymptotic probability of the property "$E(\mathbb{F}_p)$ is a cyclic group". Since it cannot be studied entirely in the framework of the probability spaces $\mathfrak{A}^{(L)}$ or $\mathfrak{X}^{(L)}$ of section 4 with finite sets of primes, some more preparations are needed. We will finally prove the following.

5.9 Theorem. *The probability $P(\mathcal{F}$, "$E(\mathbb{F}_p)$ is cyclic") exists and is given by*

$$\prod_{\ell \ prime} \left(1 - \tfrac{1}{(\ell^2-1)\ell(\ell-1)}\right) \approx 0.81377.$$

5.10 Remark. Vladut in [10] described the share of the cyclic ones among all the $E/\mathbb{F}_q$ over the fixed finite field $\mathbb{F}_q$. It depends strongly on the prime decomposition of $q-1$. In contrast, (5.9) is an average over all primes $p = q$, which balances local fluctuations.

We first determine the probability of local cyclicity.

5.11 Lemma. *Fix a prime number ℓ and $r \geq 0$.*

(i) *The probability $P(\mathcal{F}$, "$E(\mathbb{F}_p)[L^\infty]$ is cyclic")* equals

$$\tau_\ell := 1 - \tfrac{1}{(\ell^2-1)\ell(\ell-1)}.$$

(ii) *The conditional probability under the assumption $r(p,\ell) = r$ for $E(\mathbb{F}_p)[\ell^\infty]$ to be cyclic equals 1 if $r = 0$ and*

$$\sigma_\ell := 1 - \tfrac{1}{(\ell^2-1)\ell}$$

if $r > 0$.

Proof. By (4.2), the first value is given by $\sum_{\beta\geq 0} g^{(\ell)}(\alpha,\beta)$, the second one by $\sum_{\beta\geq 0} g_r^{(\ell)}(0,\beta)$. $\square$

For any $\lambda \in \mathbb{R}$, we call $E(\mathbb{F}_p)$ λ-cyclic if its ℓ-parts are cyclic for each prime $\ell \leq \lambda$. From the lemma and (4.4) we get:

5.12 Corollary. $P(\mathcal{F}$, *"$E(\mathbb{F}_p)$ is λ-cyclic"*$) = \prod_{\ell\leq\lambda} \tau_\ell$.

Hence (5.9) is established as soon as we have ensured that the limit for $\lambda \longrightarrow \infty$ commutes with the limit underlying the definition (1.4) of $P(\mathcal{F},\cdot)$.

Since cyclicity implies λ-cyclicity, at least

$$\limsup_{x\to\infty}\frac{|\{E/\mathbb{F}_p\in\mathcal{F}\mid p\le x,\ E(\mathbb{F}_p)\text{ cyclic}\}|^*}{|\{E/\mathbb{F}_p\in\mathcal{F}\mid p\le x\}|^*}\le\prod_{\ell\text{ prime}}\tau_\ell$$

holds. Thus we must find lower estimates for the left hand side. Put for each prime p

$$c(p):=\prod_{\ell\mid p-1}\sigma_\ell. \tag{5.13}$$

Then it is an easy consequence of (3.4) and the inclusion/exclusion principle (see Theorem 6.1 of [10]) that for each $\epsilon>0$ and each fixed prime p, we have

$$|\{E/\mathbb{F}_p\mid E(\mathbb{F}_p)\text{ cyclic}\}|^*=2pc(p)+O_\epsilon(p^{1/2+\epsilon}).$$

Hence

$$|\{E/\mathbb{F}_p\in\mathcal{F}\mid p\le x,E(\mathbb{F}_p)\text{ cyclic}\}|^*=2\sum_{p\le x}pc(p)+O_\epsilon(\sum_{p\le x}p^{1/2+\epsilon}). \tag{5.14}$$

5.15 Lemma. *Suppose that the average*

$$C:=\lim_{x\to\infty}\pi(x)^{-1}\sum_{p\le x}c(p)$$

exists, where $\pi(x)\sim x/\log x$ is the prime number function. Then

$$2\sum_{p\le x}pc(p)\sim Cx^2/\log x$$

and therefore $P(\mathcal{F}$, "$E(\mathbb{F}_p)$ is cyclic"$)=C$.

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be the series defined by $a_n=c(p)$ if $n=p\in\mathbb{P}$ and $a_n=0$ otherwise, and $A(x)=\sum_{n\le x}a_n=\sum_{p\le x}c(p)$. Abel summation with $b(x)=x$ yields

$$\sum_{p\le x}pc(p)=xA(x)-\int_1^x A(s)ds\sim 1/2\ Cx^2/\log x,$$

since by assumption, $A(x)\sim Cx/\log x$ and any primitive F of $x/\log x$ satisfies $F\sim 1/2\ x^2/\log x$. The last assertion follows from (5.14) and

$$\sum_{p\le x}p^{1/2+\epsilon}\sim\frac{1}{3/2+\epsilon}x^{3/2+\epsilon}/\log x.$$

□

We are left to verifying the hypothesis of (5.15), which no longer involves elliptic curves. Put

$$\begin{aligned} c_\lambda(p) &= \textstyle\prod_{\ell\mid p-1,\ \ell\le\lambda}\sigma_\ell \\ C_\lambda(x) &= \pi(x)^{-1}\textstyle\sum_{p\le x}c_\lambda(p) \\ C(x) &= \pi(x)^{-1}\textstyle\sum_{p\le x}c(p), \end{aligned} \tag{5.16}$$

the quantity whose limit we need to find. Now, since $c_\lambda(p)$ depends only on the class of p modulo $n := \prod_{\ell \le \lambda} \ell$, Dirichlet's theorem implies that for λ fixed,

$$(5.17) \qquad \begin{aligned} C_\lambda &:= \lim_{x\to\infty} C_\lambda(x) = \text{average of } c_\lambda \text{ over } (\mathbb{Z}/n)^* \\ &= \prod_{\ell\le\lambda} (\text{average of } \tilde{\sigma}_\ell \text{ over } (\mathbb{Z}/\ell)^*) = \prod_{\ell\le\lambda} \tau_\ell. \end{aligned}$$

Here $\tilde{\sigma}_\ell(x) = \sigma_\ell$, $(\tilde{\sigma}_\ell(x) = 1)$ if $x \equiv 1$, $(x \not\equiv 1)$ modulo ℓ, respectively (see Lemma 5.11(ii)).

In view of $c(p) \le c_\lambda(p)$, we have for each λ

$$\limsup_{x\to\infty} C(x) \le C_\lambda,$$

hence

$$\limsup C(x) \le \prod_{\ell \text{ prime}} \tau_\ell.$$

5.18 Claim. We have in fact

$$C := \lim_{x\to\infty} C(x) = \prod_{\ell \text{ prime}} \tau_\ell.$$

Proof of claim. Let $\lambda_0 \in \mathbb{R}$ and $\epsilon > 0$ be given. Choose x_0 large enough such that for $x \ge x_0$

$$|C_{\lambda_0}(x) - C_{\lambda_0}| < \epsilon$$

holds. For such x and $\lambda \ge \lambda_0$, we have

$$C_\lambda(x) \ge (\prod_{\lambda_0<\ell\le\lambda} \sigma_\ell) C_{\lambda_0}(x) > (\prod_{\lambda_0<\ell\le\lambda} \sigma_\ell)(C_{\lambda_0} - \epsilon).$$

Letting $\lambda \longrightarrow \infty$, we find

$$C(x) \ge (\prod_{\ell>\lambda_0} \sigma_\ell)(C_{\lambda_0} - \epsilon)$$

for each $x \ge x_0$, and therefore

$$\liminf_{x\to\infty} C(x) \ge (\prod_{\ell>\lambda_0} \sigma_\ell) C_{\lambda_0} = \prod_{\ell\le\lambda_0} \tau_\ell \prod_{\ell>\lambda_0} \sigma_\ell.$$

Since this holds for any λ_0, and $\sigma_\ell \le \tau_\ell$ for each ℓ, we finally get

$$\liminf_{x\to\infty} C(x) \ge \prod_{\ell \text{ prime}} \tau_\ell,$$

i.e., the claim. Together with (5.15), this also concludes the proof of Theorem 5.9. $\square$

References

[1] J.D. Achter: The distribution of class groups of function fields. J. Pure and Appl. Algebra 204 (2006), 316–333.

[2] B.J. Birch: How the number of points of an elliptic curve over a fixed prime field varies. J. London Math. Soc. 43 (1968), 57–60.

[3] H. Cohen–H.W. Lenstra, Jr.: Heuristics on class groups of number fields. In: Lecture Notes in Mathematics 1068, 33–62, Springer–Verlag 1984.

[4] B. Edixhoven: personal communication.

[5] E. Friedman–L.C. Washington: On the distribution of divisor class groups of curves over a finite field. In: Théorie des Nombres/Number Theory Laval 1987 (J.-M. De Koninck–C. Levesque eds.), De Gruyter 1989.

[6] E.-U. Gekeler: Frobenius distributions of elliptic curves over finite prime fields. Int. Math. Res. Notices 37 (2003), 1999–2018.

[7] E.W. Howe: On the group orders of elliptic curves over finite fields. Comp. Math. 85 (1993), 229–247.

[8] J-P. Serre: Zeta and L functions. Arithmetical Algebraic Geometry, 82–92, Harper and Row 1965.

[9] G. Tenenbaum: Introduction à la théorie analytique et probabiliste des nombres. Soc. Math. France 1995.

[10] S.G. Vladut: Cyclicity statistics for elliptic curves over finite fields. Finite Fields Appl. 5 (1999), 13–25.

Ernst-Ulrich Gekeler
FR 6.1 Mathematik
Universität des Saarlandes
D-66041 Saarbrücken
Germany
gekeler@math.uni-sb.de