Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 184

Statistics about elliptic curves over finite prime fields

Ernst-Ulrich Gekeler

Saarbrücken 2006

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 184
submitted: November 10, 2006

Statistics about elliptic curves over finite prime fields

Ernst-Ulrich Gekeler

Fachrichtung 6.1 Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany
gekeler@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

STATISTICS ABOUT ELLIPTIC CURVES OVER FINITE PRIME FIELDS

ERNST-ULRICH GEKELER

Abstract. We derive formulas for the probabilities of various properties (cyclicity, squarefreeness, generation by random points) of the point groups of randomly chosen elliptic curves over random prime fields.

MSC 2000: 11 G 20, 11 N 45
Keywords: Elliptic curves over finite fields, cyclicity, random points

1. Introduction.

Several basic algorithms in cryptography depend on calculations in the point groups $E(\mathbb{F}_p)$ of elliptic curves E over finite (notably prime) fields $\mathbb{F}_p$, see[4] or e.g. [1] and the references given therein. Analyzing these algorithms and their running times requires knowledge of the average behavior of $E(\mathbb{F}_p)$ and the likelihood of such events like: "$E(\mathbb{F}_p)$ ist cyclic" or "X generates $E(\mathbb{F}_p)$", whenever the following data are randomly chosen: a prime number p, an elliptic curve E over $\mathbb{F}_p$, a point X in $E(\mathbb{F}_p)$.

Based on earlier work [2], we provide satisfactory answers to these and related questions. We show that the probabilities $P(\mathcal{F}, A)$ of events A like the mentioned (see below for precise definitions) may be calculated as infinite products of ℓ-local contributions $P^{(\ell)}$. Here ℓ runs through the set $\mathbb{P}$ of prime numbers, and the $P^{(\ell)}$ may be deduced from the results of [2]. We find for example (see (4.3) and (5.4)):

$$P(\mathcal{F}, \text{"}E(\mathbb{F}_p) \text{ is cyclic"}) = \prod_{\ell\in\mathbb{P}}(1 - \frac{1}{(\ell^2-1)\ell(\ell-1)}) \approx 81\% \tag{1.1}$$

(which appears as Theorem 5.9 in [2]) and

$$P(\mathcal{F}, \text{"}X \text{ generates } E(\mathbb{F}_p)\text{"}) = \prod_{\ell\in\mathbb{P}}(1 - \frac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)}) \approx 44\%. \tag{1.2}$$

We first introduce some definitions and notations, where we refer to [2] (see also [3]) for discussion and explanation. The symbols p and ℓ

always denote primes, not necessarily distinct, and $\mathcal{F}$ will be the set $\{E/\mathbb{F}_p\}$, where p is any prime and $E/\mathbb{F}_p$ runs through the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$.

Recall that the group of rational points $E(\mathbb{F}_p)$ satisfies

$$||E(\mathbb{F}_p)| - (p+1)| \leq 2p^{1/2} \tag{1.3}$$

and

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m \times \mathbb{Z}/n \tag{1.4}$$

with uniquely determined $m, n \in \mathbb{N}$ and $m|n$. We put for $E/\mathbb{F}_p \in \mathcal{F}$:

$$w(E/\mathbb{F}_p) = 2|\mathrm{Aut}_{\mathbb{F}_p}(E)|^{-1} = \begin{cases} 1/3, & p \equiv 1\ (3), \quad j(E) = 0 \\ 1/2, & p \equiv 1\ (4), \quad j(E) = 12^3 \\ 1, & otherwise \end{cases} \tag{1.5}$$

(provided that $p > 3$; the precise formulas for $p = 2, 3$ are unimportant) and define the weighted cardinality of a finite subset $\mathcal{F}'$ of $\mathcal{F}$ by

$$|\mathcal{F}'|^* := \sum_{E/\mathbb{F}_p \in \mathcal{F}'} w(E/\mathbb{F}_p). \tag{1.6}$$

Summing over the $E/\mathbb{F}_p$ for a *fixed* prime p, we always have

$$|\{E/\mathbb{F}_p\}|^* = 2p. \tag{1.7}$$

For any property A of elements of $\mathcal{F}$ (or the subset characterized by A, which by abuse of notation we also label by A) and any real-valued function f on $\mathcal{F}$, the "probability" $P(\mathcal{F}, A)$ of A and the "expectation" $E(\mathcal{F}, f)$ are defined by

(1.8)

$$\begin{aligned} P(\mathcal{F}, A) &:= \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x \text{ and } E/\mathbb{F}_p \text{ has property } A\}|^*}{\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*} \\ E(\mathcal{F}, f) &:= \lim_{x\to\infty} \frac{\sum f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*} \end{aligned}$$

(summing in the numerator over $E/\mathbb{F}_p$ such that $p \leq x$), provided the limits exist. In a similar fashion, we may define other notions of probability theory, e.g. the conditional probability $P(\mathcal{F}, A|B)$ for property A under condition B. These have the obvious intuitive meaning and the usual properties, except that $P(\mathcal{F}, \cdot)$ is only finitely additive but not necessarily σ-additive (= countably additive). For example,

$$P(\mathcal{F}, \text{"}|E(\mathbb{F}_p)| = n\text{"}) = 0$$

for each $n \in \mathbb{N}$, as follows from (1.3), hence also

$$\sum_{n\in\mathbb{N}} P(\mathcal{F}, \text{“}|E(\mathbb{F}_p)| = n\text{”}) = 0$$

instead of the “correct” value $1 = P(\mathcal{F}, \mathcal{F})$.

(1.9) For properties A that depend only on the ℓ-part $E(\mathbb{F}_p)^{(\ell)}$ of the finite abelian group $E(\mathbb{F}_p)$ (and perhaps the ℓ-adic valuation of $p-1$), $P(\mathcal{F}, A)$ has been determined in [2]. We call such properties *(weakly) of type* ℓ; examples are “$\ell \mid |E(\mathbb{F}_p)|$” or “$E(\mathbb{F}_p)^{(\ell)} \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$” for $0 \le \alpha \le \beta$ fixed. A property A *localizes* if it is fulfilled if and only if for each $\ell \in \mathbb{P}$ some condition $A^{(\ell)}$ weakly of type ℓ is satisfied. “$E(\mathbb{F}_p)$ is cyclic” or “$|E(\mathbb{F}_p)|$ is squarefree” are localizing properties, while “$E(\mathbb{F}_p)|$ is prime” fails to localize.

The main purpose of the present paper is to show the formula

$$P(\mathcal{F}, A) = \prod_{\ell\in\mathbb{P}} P(\mathcal{F}, A^{(\ell)})$$

for localizing properties A (see Theorem 3.3), and to draw some conclusions (sections 4 and 5).

Notation.

$\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ and $\mathbb{P} = \{2, 3, 5, \ldots\}$ denote the sets of natural, non-negative integral, prime numbers, respectively. 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 is coprime with n/m. The symbol $\mathbb{Z}/n$ is brief for $\mathbb{Z}/n\mathbb{Z}$, and for a finite abelian group G, $\ell \in \mathbb{P}$, and $x \in G$, $G^{(\ell)}$ denotes the ℓ-primary part of G and $x^{(\ell)}$ the projection of x to $G^{(\ell)}$. Finally, $\mathcal{P}(S)$ is the power set (set of subsets) of the set S.

2. Local statistics: resumé of known results.

The possible candidates for $E(\mathbb{F}_p)^{(\ell)}$, where $E/\mathbb{F}_p \in \mathcal{F}$ and $\ell \in \mathbb{P}$, are of shape

$$H = H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta \quad \text{with } 0 \le \alpha \le \beta.$$

The likelihood that H occurs over a fixed $\mathbb{F}_p$ depends on congruence conditions on p. Describing the dependence requires the following definition. Given ℓ and p, put

$$r = r(p,\ell) = \max\{i \in \mathbb{N}_0 \mid p \equiv 1 \ (\mathrm{mod}\ell^i)\}, \tag{2.1}$$

that is, $\ell^r \| p-1$. Then e.g. $E(\mathbb{F}_p)^{(\ell)} \cong H^{(\ell)}_{\alpha,\beta}$ implies $r \geq \alpha$, as results from the properties of the Weil pairing on $E(\mathbb{F}_p)^{(\ell)}$ (see [5], pp. 95–99).

In what follows, we fix $\ell \in \mathbb{P}$ and let $\mathfrak{X}^{(\ell)}$ be the set of pairs $\{(H,r)\}$, where $H = H^{(\ell)}_{\alpha,\beta}$ with $0 \leq \alpha \leq \beta$ and $\alpha \leq r$. We often identify $\mathfrak{X}^{(\ell)}$ with $\{(\alpha,\beta,r) \in \mathbb{N}_0^3 \mid \alpha \leq \min(\beta,r)\}$. For such (α,β,r), define numbers $g^{(\ell)}(\alpha,\beta)$ and $g^{(\ell)}_r(\alpha,\beta)$ through the table below. Put further $g^{(\ell)}_r(\alpha,\beta) = 0$ for $r < \alpha$.

2.2 Table	$g^{(\ell)}(\alpha,\beta)$	$g^{(\ell)}_\alpha(\alpha,\beta)$	$g^{(\ell)}_r(\alpha,\beta),\ r>\alpha$
$0=\alpha=\beta$	$\frac{\ell^3-2\ell^2-\ell+3}{(\ell^2-1)(\ell-1)}$	$\frac{\ell-2}{\ell-1}$	$\frac{\ell^2-\ell-1}{\ell^2-1}$
$0=\alpha<\beta$	$\frac{\ell^2-\ell-1}{(\ell-1)\ell}\ell^{-\beta}$	$\ell^{-\beta}$	$\frac{\ell-1}{\ell}\ell^{-\beta}$
$0<\alpha=\beta$	$\ell^{-4\alpha}$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-3\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha}$
$0<\alpha<\beta$	$\frac{\ell+1}{\ell}\ell^{-\beta-3\alpha}$	$\ell^{-\beta-2\alpha}$	$\frac{\ell-1}{\ell}\ell^{-\beta-2\alpha}$

The following has been proved in [2].

2.3 Theorem *(loc. cit. Theorem* 3.15*):*
The probability $P(\mathcal{F}$, "$E(\mathbb{F}_p)^{(\ell)} \cong H^{(\ell)}_{\alpha,\beta}$") *and the conditional probability* $P(\mathcal{F}$, "$E(\mathbb{F}_p)^{(\ell)} \cong H^{(\ell)}_{\alpha,\beta}$"$|$ "$\ell^r \| p-1$") *for the same event under the condition "*$\ell^r \| p-1$*" are given by* $g^{(\ell)}(\alpha,\beta)$ *and* $g^{(\ell)}_r(\alpha,\beta)$*, respectively.*

In both cases, the remainder terms (i.e., the differences between the limit and the right hand side of (1.8)) are of shape $O_{\ell,\alpha,\beta}(x^{-1/2})$ with constants that may be worked out as in [2] sect. 3. We will however not further care for remainder terms in the present work.

Next, for $(\alpha,\beta,r) \in \mathfrak{X}^{(\ell)}$ we define

$$A_{\alpha,\beta,r} = \{E/\mathbb{F}_p \in \mathcal{F} \mid r(p,\ell) = r,\ E(\mathbb{F}_p)^{(\ell)} \cong H^{(\ell)}_{\alpha,\beta}\} \tag{2.4}$$

and let $\mathfrak{A}^{(\ell)}$ be the σ-algebra of subsets of $\mathcal{F}$ generated by $A_{\alpha,\beta,r}$ (i.e, the smallest subset of $\mathcal{P}(\mathcal{F})$ containing $\emptyset$, $\mathcal{F}$, the $A_{\alpha,\beta,r}$, and closed under

taking complements and under countable unions). Thus elements of $\mathfrak{A}^{(\ell)}$ are of shape

$$A_{\mathfrak{Y}} = \bigcup_{(\alpha,\beta,r)} A_{\alpha,\beta,,r}$$

with subsets $\mathfrak{Y}$ of $\mathfrak{X}^{(\ell)}$, and $\mathfrak{Y} \longmapsto A_{\mathfrak{Y}}$ is a bijection of $\mathcal{P}(\mathfrak{X}^{(\ell)})$ with $\mathfrak{A}^{(\ell)}$. Furthermore, by (2.3) we have

$$g_r^{(\ell)}(\alpha,\beta) = \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p \in A_{\alpha,\beta,r} \mid p \le x\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid r(p,\ell) = r, p \le x\}|^*}.$$

2.5 Proposition. *$P(\mathcal{F},\cdot)$ is well-defined on $\mathfrak{A}^{(\ell)}$ and σ-additive, i.e., a probability measure on $\mathfrak{A}^{(\ell)}$. Its value $P(\mathcal{F}, A_{\alpha,\beta,r})$ on $A_{\alpha,\beta,r}$ is*

$$\tfrac{\ell-2}{\ell-1} g_0^{(\ell)}(\alpha,\beta), \quad r = 0$$

$$\ell^{-r} g_r^{(\ell)}(\alpha,\beta), \quad r > 0.$$

This is a restatement of Proposition 4.2, loc. cit.

A real-valued function f on $\mathcal{F}$ is *of type ℓ* if $f(E/\mathbb{F}_p)$ depends only on $E(\mathbb{F}_p)^{(\ell)}$, and is *weakly of type ℓ* if it depends only on $E(\mathbb{F}_p)^{(\ell)}$ and $r(p,\ell)$. Thus, ℓ being fixed, if f is of type ℓ (weakly of type ℓ), we may regard it as a function on pairs (α,β) with $0 \le \alpha \le \beta$ (as a function on $\mathfrak{X}^{(\ell)}$), respectively.

2.6 Proposition.

(i) *Suppose that $f : \mathcal{F} \longrightarrow \mathbb{R}$ is bounded and of type ℓ. Then the expectation $E(\mathcal{F}, f)$ is defined and satsifies*

$$E(\mathcal{F}, f) = \sum_{\alpha,\beta\in\mathbb{N}_0,\alpha\le\beta} f(\alpha,\beta) g^{(\ell)}(\alpha,\beta).$$

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

$$\sum_{\alpha,\beta\in\mathbb{N}_0,\alpha\le\min(\beta,r)} f(\alpha,\beta,r) g_r^{(\ell)}(\alpha,\beta).$$

The total expectation is

$$E(\mathcal{F}, f) = \sum_{\alpha,\beta,r\in\mathbb{N}_0,\alpha\le\min(\beta,r)} f(\alpha,\beta,r) P(\mathcal{F}, A_{\alpha,\beta,r})$$

with the value of $P(\mathcal{F}, A_{\alpha,\beta,r})$ given by (2.5).

Again, this is proved in [2], Lemma 5.4. Note that the formula for $E(\mathcal{F}, f)$ corresponds to the usual definition of expectation in probability, but is non-tautological in our case in view of the definition (1.8) of $E(\mathcal{F}, f)$. It would be interesting to know under which conditions it generalizes to unbounded functions f for which the right hand sum still converges. See also Remark 5.11.

As a consequence of Howe's work [3], the preceding results generalize to cover events that involve finitely many primes instead of a single ℓ only. Viz, let $L \subset \mathbb{P}$ be a finite set of primes, put

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

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

$$A_{\mathbf{x}} := \bigcap_{\ell \in L} A_{\alpha_\ell, \beta_\ell, r_\ell}.$$

Further, let $\mathfrak{A}^{(L)}$ be the σ-algebra generated by $\mathfrak{A}^{(\ell)}$, $\ell \in L$. Then $\mathfrak{Y} \longmapsto A_{\mathfrak{Y}} := \bigcup_{\mathbf{x} \in \mathfrak{Y}} A_{\mathbf{x}}$ yields a bijection of $\mathcal{P}(\mathfrak{X}^{(L)})$ with $\mathfrak{A}^{(L)}$, and as a synopsis of 4.4, 4.5, 5.4 and 5.7 of [2], the following holds.

2.7 Proposition.

(i) *$P(\mathcal{F}, \cdot)$ is well-defined and σ-additive on $\mathfrak{A}^{(L)}$, i.e., a probability measure. Its value on $A_{\mathbf{x}}$ as above is*

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

In particular, the restrictions of $P(\mathcal{F}, \cdot)$ to the various $\mathfrak{A}^{(\ell)}$ ($\ell \in L$) are stochastically independent.

(ii) *Let for each $\ell \in L$ a bounded function $f^{(\ell)} : \mathcal{F} \longrightarrow \mathbb{R}$ weakly of type ℓ be given, and put $f = \prod_{\ell \in L} f^{(\ell)}$. Then $E(\mathcal{F}, f)$ is defined and equals $\prod_{\ell \in L} E(\mathcal{F}, f^{(\ell)})$.*

3. Global statistics.

Let L be any (finite or infinite) subset of $\mathbb{P}$, and let for each $\ell \in L$ an element $A^{(\ell)}$ of $\mathfrak{A}^{(\ell)}$ be given. Then $A := \bigcap_{\ell \in L} A^{(\ell)}$ localizes, and as a consequence of (2.5) and (2.7),

$$P(\mathcal{F}, A) = \prod_{\ell \in L} P(\mathcal{F}, A^{(\ell)}), \tag{3.1}$$

provided that L is finite. More generally, if for each $\ell \in L$, a function $f^{(\ell)}$ on $\mathcal{F}$ weakly of type ℓ and with values in the real unit interval $[0,1]$ is given, then the expectation for $f := \prod_{\ell\in L} f^{(\ell)}$ is defined and given by

$$E(\mathcal{F}, f) = \prod_{\ell\in L} E(\mathcal{F}, f^{(\ell)}), \tag{3.2}$$

if again L is assumed to be finite. (Note that the series of partial products of the right hand side always converges, perhaps to 0. An infinite product is always understood as the limit of the partial products.) The validity of (3.1) and (3.2) for *infinite* L requires interchanging two limit processes, and is asserted by

3.3 Theorem. *Formula* (3.2) *is valid for arbitrary sets L of primes, in particular, for $L = \mathbb{P}$.*

Note that (3.1) is implied by (3.2), by applying (3.2) to characteristic functions $\chi_{A^{(\ell)}}$ of $A^{(\ell)}$.

Proof. Without restriction, we may assume that $L = \mathbb{P}$. For each function $f : \mathcal{F} \longrightarrow \mathbb{R}$, we let

$$\varphi_f(x) := \frac{\sum_{E/\mathbb{F}_p\in\mathcal{F}, p\le x} f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \le x\}|^*}$$

be the function whose limit for $x \longrightarrow \infty$ yields $E(\mathcal{F}, f)$. Note that $f \longmapsto \varphi_f$ commutes with absolutely convergent sums. Let now $f = \prod_{\ell\in\mathbb{P}} f^{(\ell)}$ be given, and put for $\lambda \in \mathbb{R}$:

$$g_\lambda := \prod_{\ell\le\lambda} f^{(\ell)},\ h_\lambda := g_{\lambda-1} - g_\lambda.$$

Then $g_0 = 1$, $g_\infty := \lim_{\lambda\to\infty} g_\lambda = f$, and

$$1 = f + \sum_{\ell\in\mathbb{P}} h_\ell \tag{1}$$

(convergent sum with non-negative terms). Formula (3.2) is valid for each of the finite products g_λ and also for

$$h_\ell = (1 - f^{(\ell)}) \prod_{\ell'<\ell} f^{(\ell')}. \tag{2}$$

Therefore

$$\lim_{x\to\infty} \varphi_{g_\lambda}(x) = E(\mathcal{F}, g_\lambda) = \prod_{\ell\le\lambda} E(\mathcal{F}, f^{(\ell)}).$$

Since this holds for each λ and $f \leq g_\lambda$, thus $\varphi_f \leq \varphi_{g_\lambda}$, we get

$$\limsup_{x\to\infty} \varphi_f(x) \leq \prod_{\ell\in\mathbb{P}} E(\mathcal{F}, f^{(\ell)}) =: E. \tag{3}$$

On the other hand (all the lim inf, lim sup are for $x \to \infty$, ℓ and ℓ' run through $\mathbb{P}$):

$$\begin{aligned}
\liminf \varphi_f(x) &= \liminf(\varphi_{1-\sum h_\ell}(x)) \\
&= \liminf(1 - \textstyle\sum \varphi_{h_\ell}(x)) \\
&= 1 - \limsup \textstyle\sum \varphi_{h_\ell}(x) \\
&\geq 1 - \textstyle\sum_\ell \limsup \varphi_{h_\ell}(x) \\
&= 1 - \textstyle\sum_\ell (1 - E(\mathcal{F}, f^{(\ell)})) \prod_{\ell'<\ell} E(\mathcal{F}, f^{(\ell')}) \\
&= 1 - (1 - E)) \\
&= E,
\end{aligned}$$

thus $\lim \varphi_f(x) = E$ as stated. □

4. Applications.

Let be given: a natural number $n = \prod_{\ell\in\mathbb{P}} \ell^{a_\ell}$, a finite subset L of $\mathbb{P}$, and for each $\ell \in L$ a finite abelian ℓ-group $H^{(\ell)}_{\alpha_\ell,\beta_\ell}$. We consider one of the following properties A of $E/\mathbb{F}_p \in \mathcal{F}$:

(4.1)

(i) $|E(\mathbb{F}_p)|$ is squarefree;
(ii) $E(\mathbb{F}_q)$ is elementary (i.e., its annihilator is squarefree);
(iii) $E(\mathbb{F}_p)$ is cyclic;
(iv) $n \mid |E(\mathbb{F}_p)|$;
(v) $n \parallel |E(\mathbb{F}_p)|$;
(vi) the L-part of $E(\mathbb{F}_p)$ is isomorphic with $\prod_{\ell\in L} H^{(\ell)}_{\alpha_\ell,\beta_\ell}$.

All these properties localize; thus by (3.3), in order to determine $P(\mathcal{F}, A)$, it suffices to calculate the corresponding local probabilities $P(\mathcal{F}, A^{(\ell)})$. For cases (i) to (vi), the local properties are equivalent with $E(\mathbb{F}_p)^{(\ell)}$ being isomorphic with $H^{(\ell)}_{\alpha,\beta}$, where

(i) $(\alpha, \beta) = (0, 0)$ or $(0, 1)$;
(ii) $(\alpha, \beta) = (0, 0), (0, 1)$ or $(1, 1)$;

(iii) $(\alpha, \beta) = (0, \beta)$, $\beta \in \mathbb{N}_0$;
(iv) (α, β) such that $\alpha + \beta \geq a_\ell$;
(v) (α, β) such that $\alpha + \beta = a_\ell$ if $a_\ell > 0$, arbitrary if $a_\ell = 0$;
(vi) $(\alpha, \beta) = (\alpha_\ell, \beta_\ell)$ if $\ell \in L$, arbitrary if $\ell \notin L$.

In the next proposition, we give the $P(\mathcal{F}, A^{(\ell)})$ in the listed cases; they may be derived by elementary but tedious calculations from the table (2.2).

4.2 Proposition. *The local probabilites $P(\mathcal{F}, A^{(\ell)})$ in the six cases of* (4.1) *are*

(i) $1 - \frac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)}$;
(ii) $1 - \frac{\ell^5-2\ell^3+\ell-1}{\ell^4(\ell^2-1)(\ell-1)}$;
(iii) $1 - \frac{1}{(\ell^2-1)\ell(\ell-1)}$;
(iv) $\ell^{-a_\ell}\frac{\ell^3-\ell-\ell^{2-a_\ell}}{(\ell^2-1)(\ell-1)}$;
(v) $\ell^{-a_\ell} - \frac{\ell^{-2a_\ell}}{\ell-1}$;
(vi) $g^{(\ell)}(\alpha_\ell, \beta_\ell)$ *as in* (2.2),

where (iv), (v), (vi) *are valid for $a_\ell > 0$, $a_\ell > 0$, $\ell \in L$, respectively, and must be replaced by* 1 *if $a_\ell = 0$, $a_\ell = 0$, $\ell \notin L$.*

Thus e.g.,

(4.3)

(i) $P(\mathcal{F}, \text{“}|E(\mathbb{F}_p)| \text{ is squarefree”}) = \prod_{\ell\in\mathbb{P}}(1 - \frac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)})$
$= 0.44014736\ldots =: S$
(ii) $P(\mathcal{F}, \text{“}E(\mathbb{F}_p) \text{ is elementary”}) = \prod_{\ell\in\mathbb{P}}(\cdots) = 0.49557478\ldots$
(iii) $P(\mathcal{F}, \text{“}E(\mathbb{F}_p) \text{ is cyclic”}) = \prod_{\ell\in\mathbb{P}}(\cdots) = 0.81375190\ldots =: C.$

The preceding are unbiased probabilities, which apply if no information about p is assumed. Restricting our attention to those $E/\mathbb{F}_p \in \mathcal{F}$ subject to $r(p, \ell) = r_\ell$, where a finite subset $L \subset \mathbb{P}$ and $r_\ell \in \mathbb{N}_0$ for all $\ell \in L$ are given, we might similarly derive the corresponding conditional probabilities $P(\mathcal{F}, A \mid \text{“}r(p, \ell) = r_\ell\ \forall \ell \in L\text{”})$. We restrict to presenting the result for the particularly important case of cyclicity.

4.4 Proposition. *Let $\ell \in \mathbb{P}$ be given. Then*

$$P(\mathcal{F}, \text{“}E(\mathbb{F}_p)^{(\ell)} \text{ is cyclic”} \mid \text{“}r(p, \ell) = r\text{”}) = \begin{cases} 1, & r = 0 \\ 1 - \frac{1}{(\ell^2-1)\ell}, & r > 0. \end{cases}$$

The proof is obvious, since the quantity$P(\mathcal{F},\cdots)$ equals $\sum_{\beta\geq 0} g_r^{(\ell)}(0,\beta)$.

4.5 Example. Let $L=\{3,5\}$ and p such that $r(p,\ell)\geq 1$ for $\ell\in L$, i.e., $p\equiv 1\ (\mathrm{mod}15)$. Then

$$\begin{aligned} P(\mathcal{F},\text{“}E(\mathbb{F}_p) \text{ is cyclic”} \mid \text{“}p\equiv 1\ (\mathrm{mod}15)\text{”}) &= \tfrac{46}{47}\cdot\tfrac{476}{479}\cdot C \\ &= 0.79145\cdots \end{aligned}$$

with the constant C of (4.3)(iii). On the other hand, if we require $r(p,\ell)=0$ for $\ell\in L$, i.e., $p\equiv 2,8,14\ (\mathrm{mod}15)$, we get

$$\begin{aligned} P(\mathcal{F},\text{“}E(\mathbb{F}_p) \text{ is cyclic”} \mid \text{“}p\equiv 2,8,14\ (\mathrm{mod}15)\text{”}) &= \tfrac{48}{47}\cdot\tfrac{480}{479}\cdot C \\ &= 0.83280\cdots \end{aligned}$$

5. Cyclic subgroups of $E(\mathbb{F}_p)$.

Choose $p\in\mathbb{P}$, $E/\mathbb{F}_p$ and $X\in E(\mathbb{F}_p)$ randomly. There are two plausible (and a priori different) definitions for the “probability” of the event “X generates $E(\mathbb{F}_p)$” (briefly: “$\langle X\rangle = E(\mathbb{F}_p)$”), namely

(5.1)
$$\lim_{x\to\infty}\frac{|\{(E/\mathbb{F}_p,X)|E/\mathbb{F}_p\in\mathcal{F},X\in E(\mathbb{F}_p)s.t.\langle X\rangle=E(\mathbb{F}_p),p\leq x\}|^*}{|\{(E/\mathbb{F}_p,X)|E/\mathbb{F}_p\in\mathcal{F},X\in E(\mathbb{F}_p),p\leq x\}|^*} =: \lim_{x\to\infty}\frac{\mathrm{num}(x)}{\mathrm{den}(x)}$$

and

(5.2) $$E(\mathcal{F},f),$$

where the cardinalities in (5.1) are weighted with $w(E/\mathbb{F}_p)$ as in (1.5), and the function $f:\ \mathcal{F}\longrightarrow[0,1]$ is defined through

$$f(E/\mathbb{F}_p)=\frac{|\{X\in E(\mathbb{F}_p)\mid\langle X\rangle=E(\mathbb{F}_p)\}|}{|E(\mathbb{F}_p)|}.$$

5.3 Theorem. The two quantities in (5.1) and (5.2) are well-defined and agree.

We label the common value by $P(\mathcal{F},\text{“}\langle X\rangle=E(\mathbb{F}_p)\text{”})$. Since f is the

product $\prod_{\ell\in\mathbb{P}} f^{(\ell)}$ of functions $f^{(\ell)}: \mathcal{F} \longrightarrow [0,1]$ of type ℓ,

$$f^{(\ell)}(E/\mathbb{F}_p) = \frac{|\{X \in E(\mathbb{F}_p)^{(\ell)} \mid \langle X\rangle = E(\mathbb{F}_p)^{(\ell)}\}|}{|E(\mathbb{F}_p)^{(\ell)}|},$$

the value $P(\mathcal{F}, \text{“}\langle X\rangle = E(\mathbb{F}_p)\text{”})$ is subject to (3.3). Now $E(\mathcal{F}, f^{(\ell)})$ is easily calculated:

$$\begin{aligned} E(\mathcal{F}, f^{(\ell)}) &= g^{(\ell)}(0,0) + \textstyle\sum_{\beta>0} g^{(\ell)}(0,\beta)(1-\ell^{-1}) \\ &= 1 - \tfrac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)}, \end{aligned}$$

which results from (2.6), $|\{X \in \mathbb{Z}/\ell^\beta \mid \langle X\rangle = \mathbb{Z}/\ell^\beta\}| = (\ell-1)\ell^{\beta-1}$, and evaluation of the series. We thus find (modulo (5.3)):

5.4 Corollary. $P(\mathcal{F}, \text{“}\langle X\rangle = E(\mathbb{F}_p)\text{”}) = \prod_{\ell\in\mathbb{P}}(1 - \frac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)})$.

Note that this agrees with $S = P(\mathcal{F}, \text{“}|E(\mathbb{F}_q)| \text{ is squarefree”})$ (see (4.3)(i)).

Proof of Theorem 5.3. The existence of $E := E(\mathcal{F}, f)$ follows from (3.3). It is the limit for $x \to \infty$ of

$$\varphi_f(x) = \frac{\sum f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{\sum w(E/\mathbb{F}_p)},$$

where both sums are extended over the $E/\mathbb{F}_p \in \mathcal{F}$ with $p \le x$. We write it as

$$\varphi_f(x) = \frac{\sum a_n}{\sum b_n},$$

where $n \in \mathbb{N}$, $n \le x$, $a_n = b_n = 0$ if n fails to be prime, and a_n, b_n are the respective contributions of $E/\mathbb{F}_p$ if $n = p \in \mathbb{P}$. According to (1.7), $b_n = 2p$ for $n = p$ and, moreover,

$$b_p(p+1) = \sum_{E/\mathbb{F}_p} |E(\mathbb{F}_p)|^*,$$

since $\{E/\mathbb{F}_p\}$ splits into pairs whose numbers of rational points add up to $2(p+1)$. From (5.6),

$$\sum_{n\le x} b_n \sim \frac{x^2}{\log x},$$

where $g(x) \sim h(x)$ denotes asymptotic equivalence $\lim_{x\to\infty} g(x)/h(x) = 1$. Again from (5.6),

$$\sum_{n\le x} b_n(n+1) \sim \sum b_n \cdot n \sim \frac{2}{3}\frac{x^3}{\log x}$$

and accordingly,

$$\sum_{n\le x} a_n \sim E\cdot\frac{x^2}{\log x}$$

and

$$\sum a_n(n+1) \sim \frac{2}{3}E\frac{x^3}{\log x}.$$

On the other hand, as results from the definition of $f(E/\mathbb{F}_p)$ and the Hasse estimate (1.3),

$$f(E/\mathbb{F}_p)(p+1) = |\{\text{generators of the group } E(\mathbb{F}_p)\}| + O(p^{1/2}),$$

hence

$$\begin{aligned}\textstyle\sum_{n\le x} a_n(n+1) &= \mathrm{num}(x) + (\textstyle\sum_{n\le x} b_n)\cdot O(x^{1/2})\\ &\sim \mathrm{num}(x)\end{aligned}$$

with the numerator $\mathrm{num}(x)$ in (5.1). Together

$$\begin{aligned}E(\mathcal{F},f) &= \lim_{x\to\infty}(\textstyle\sum_{n\le x} a_n/\sum_{n\le x} b_n)\\ &= \lim(\textstyle\sum a_n(n+1)/\sum b_n(n+1))\\ &= \lim(\mathrm{num}(x)/\mathrm{den}(x)) \quad \text{as in (5.1).}\end{aligned}$$

□

Similar reasoning shows:
(5.5)

$$E(\mathcal{F}, f^{(\ell)}) =$$

$$\lim_{x\to\infty}\frac{|\{(E/\mathbb{F}_p, X)\mid E/\mathbb{F}_p\in\mathcal{F}, X\in E(\mathbb{F}_p) s.t. \langle X^{(\ell)}\rangle = E(\mathbb{F}_p)^{(\ell)}, p\le x\}|^*}{|\{(E/\mathbb{F}_p, X)\mid E/\mathbb{F}_p\in\mathcal{F}, X\in E(\mathbb{F}_p), p\le x\}|^*}$$

In the proof, we used the following well-known fact, which may be derived from the prime number theorem by Abel summation. (For some hints, see [6] p. 3/4 and [2] 3.12.)

5.6 Proposition. *For each real number $\gamma > -1$, the asymptotic equivalence*

$$\sum_{p\in\mathbb{P}, p\le x} p^\gamma \sim \frac{1}{1+\gamma}\frac{x^{1+\gamma}}{\log x}$$

holds.

The preceding may be generalized to cover the question:

"Given $n \in \mathbb{N}$, how likely is it that a randomly chosen point $E/\mathbb{F}_p \in \mathcal{F}$ generates a subgroup $\langle X \rangle$ of index n?"

Defining

$$f_n(E/\mathbb{F}_p) = \frac{|\{X \in E(\mathbb{F}_p) \mid [E(\mathbb{F}_p) : \langle X \rangle] = n\}|}{|E(\mathbb{F}_p)|}$$

(i.e., $f_1 =$ the former f) and replacing the condition "$\langle X \rangle = E(\mathbb{F}_p)$" by "$\langle X \rangle$ has index n in $E(\mathbb{F}_p)$" at appropriate places, Theorem 5.3 along with (analogues of) its consequences (5.4) and (5.5) as well as the respective proofs remain valid for f_n.

Hence we may define $P(\mathcal{F}, "[E(\mathbb{F}_p) : \langle X \rangle] = n")$, which has an asymptotic interpretation like (5.1) and an interpretation as $E(\mathcal{F}, f_n)$ like (5.2). If, as usual, $n = \prod_{\ell \in \mathbb{P}} \ell^{a_\ell}$, f_n is an infinite product $\prod_\ell f_n^{(\ell)}$ with

$$f_n^{(\ell)}(E/\mathbb{F}_p) = \frac{|\{X \in E(\mathbb{F}_p)^{(\ell)} \mid [E(\mathbb{F}_p)^{(\ell)} : \langle X \rangle] = \ell^{a_\ell}\}|}{|E(\mathbb{F}_p)^{(\ell)}|}.$$

In order to find the value of

$$P(\mathcal{F}, "[E(\mathbb{F}_p) : \langle X \rangle] = n") = E(\mathcal{F}, f_n) = \prod_\ell E(\mathcal{F}, f_n^{(\ell)}),$$

we must determine the factors $E(\mathcal{F}, f_n^{(\ell)})$.

5.7 Proposition.

$$E(\mathcal{F}, f_n^{(\ell)}) = \begin{cases} 1 - \frac{\ell^3-\ell-1}{(\ell^2-1)\ell^2(\ell-1)}, & \text{if } a_\ell = 0 \\ \nu_n^{(\ell)} := \frac{1}{\ell-1}(\ell^{1-2a} - (\ell^2+\ell+1)\ell^{-2-3a}), & \text{if } a = a_\ell > 0. \end{cases}$$

We omit the proof, which is a straightforward but tiring calculation based on (2.6). Of course, the result for $a_\ell = 0$ is already in (5.4).

Together we find:

5.8 Proposition.

$$P(\mathcal{F}, "[E(\mathbb{F}_p) : \langle X \rangle] = n") = \prod_{\ell \in \mathbb{P},\, \ell \nmid n} \left(1 - \frac{\ell^3 - \ell - 1}{(\ell^2-1)\ell^2(\ell-1)}\right) \prod_{\ell \mid n} \nu_n^{(\ell)}.$$

Thus we have $P(\mathcal{F}, "[E(\mathbb{F}_p) : \langle X \rangle] = n") = \gamma_n \cdot S$ with the constant $S = 0.44017736\ldots$ of (4.3)(i) and rational numbers γ_n, the first few of which are given in

5.9 Table.

n	γ_n	approximate value
1	1	1
2	$\frac{27}{56}$	0.482143
3	$\frac{544}{3267}$	0.166514
4	$\frac{75}{448}$	0.167411
5	$\frac{14256}{285125}$	0.049999

5.10 Remark. Instead of the index $[E(\mathbb{F}_p) : \langle X\rangle]$ one might consider the order $|\langle X\rangle|$ of a random point $X \in E(\mathbb{F}_p)$ and ask for its statistical behavior. But it is easily seen that the probability for $|\langle X\rangle| = n$ equals 0 for each fixed n, and is thus uninteresting. On the other hand, the probability for $|\langle X^{(\ell)}\rangle| = \ell^a$ for a fixed prime power ℓ^a is positive and may be worked out following the above line of arguments.

5.11 Remark. We may formally calculate the "expectation"

$$\sum_{a\geq 0} \ell^a P(\mathcal{F}, \text{“}[E(\mathbb{F}_p)^{(\ell)} : \langle X^{(\ell)}\rangle] = \ell^a\text{”})$$

for the ℓ-part of the index $[E(\mathbb{F}_p) : \langle X\rangle]$. Its value comes out as $(1-\ell^{-1})^{-1}$. However, it is unclear whether that value is effective, i.e., has an asymptotic interpretation like (5.2). As the function $[E(\mathbb{F}_p)^{(\ell)} : \langle X^{(\ell)}\rangle]$ on triples $(p, E/\mathbb{F}_p, X \in E(\mathbb{F}_p))$ is unbounded, the reasoning in the proof of Proposition 2.6 (see [2]) is not applicable. Proving the effectiveness requires a neat estimation of remainder terms in our limit expressions, a question we largely by-passed in the present work.

References

[1] F. Blake, G. Seroussi, N.P. Smart (eds.): Advances in Elliptic Curve Cryptography. LMS Lecture Note Series **317**, Cambridge 2005.

[2] E.-U. Gekeler: The Distribution of Group Structures on Elliptic Curves over Finite Prime Fields. Doc. Math. **11** (2006), 119–142.

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

[4] H.W. Lenstra Jr.: Factoring integers with elliptic curves. Ann. Math. **126** (1987), 649–673.

[5] J. H. Silverman: The Arithmetic of Elliptic Curves. GTM **106**, Springer–Verlag 1986.

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

Ernst-Ulrich Gekeler
Fachrichtung 6.1 Mathematik
Universität des Saarlandes
Postfach 15 11 50
D-66041 Saarbrücken, Germany
gekeler@math.uni-sb.de