Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint

Frobenius distributions of elliptic curves over finite prime fields

Ernst-Ulrich Gekeler

Preprint No. 71

Saarbrücken 2002

Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Frobenius distributions of elliptic curves over finite prime fields

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
E-Mail: gekeler@math.uni-sb.de

submitted: October 14, 2002

Preprint No. 71

Saarbrücken 2002

Edited by
FR 6.1 – Mathematik
Im Stadtwald
D–66041 Saarbrücken
Germany

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

FROBENIUS DISTRIBUTIONS OF ELLIPTIC CURVES OVER FINITE PRIME FIELDS

ERNST-ULRICH GEKELER

0. Introduction.

An elliptic curve E over the finite prime field $\mathbb{F}_p$ has N rational points, where the *Frobenius trace* $t := t(E/\mathbb{F}_p) = p+1-N$ is subject to Hasse's bound

$$(0.1) \qquad |t| < 2p^{1/2}.$$

It is known that all N allowed by (0.1) actually occur, but how often? How likely is it that a random elliptic curve $E/\mathbb{F}_p$ satisfies $t(E/\mathbb{F}_p) = t_0$ with a given admissible $t_0 \in \mathbb{Z}$? According to Birch [1], small values of $|t|$ are more likely than large ones; more precisely, the distribution of the normalized quantity $\tau := \frac{t}{2p^{1/2}}$ approaches $\frac{2}{\pi}\sqrt{1-\tau^2}$ as p tends to infinity. This is in keeping with the "$\sin^2$ philosophy" of the Sato-Tate conjecture ([9]; see also [6] and [3]), but fails to give information on a finite level p.

In section 2 of the present paper, we propose a heuristic model for the behavior of

$$(0.2) \qquad H(t,p) := \begin{array}{l}\text{number of isomorphism classes of}\\ E/\mathbb{F}_p \text{ such that } t(E/\mathbb{F}_p) = t,\end{array}$$

based on ideas of Lang and Trotter [6] and the Čebotarev theorem. It turns out that, after a slight and natural correction, the expected value for $H(t,p)$ derived from the model agrees with the actual value: the corresponding result is Theorem 4.6. Among other consequences, we find that the frequency of t as a Frobenius trace for $E/\mathbb{F}_p$ is in average ($t \in \mathbb{Z}$ fixed, p variable) proportional with

$$(0.3) \qquad w(t) = \prod_{\ell \text{ prime}, \ell | t} \frac{\ell^2 - \ell}{\ell^2 - \ell - 1}.$$

The precise statement is Theorem 5.14; it also makes use of subtle estimates of David and Pappalardi [3].

The author wishes to thank Gerald Tenenbaum for valuable hints in analytic number theory given in extended email correspondence, and he is grateful to Max Gebhardt for his help with numerical calculations

and the preparation of the tables.

1. Class numbers [2] [8].

In this section, we collect a few well-known but dispersed results needed in the sequel.

Let D be a negative discriminant, i.e., $0 > D \in \mathbb{Z}$ and $D \equiv 0, 1 \pmod 4$. Write $D = f^2 D_0$, where f is maximal such that $f^2 | D$ and $D_0 = D/f^2$ is congruent to 0 or 1 (mod4). Then D_0 is the discriminant of the imaginary quadratic field $\mathbb{Q}(D_0^{1/2})$ (a so-called fundamental discriminant) and D the discriminant of the order $O(D)$ of index f in $O(D_0) =$ integers of $\mathbb{Q}(D_0^{1/2})$. An explicit expression is $O(D) = \mathbb{Z} + fO(D_0) = \mathbb{Z}[\frac{-D+D^{1/2}}{2}]$. The association $D \longmapsto O(D)$ is a bijection between negative discriminants as above and orders in imaginary quadratic fields.

We let

$$h(D) = \text{class number of } O(D) \tag{1.1}$$

(i.e., the order of the group of proper ideal classes of $O(D)$) and

$$\mathcal{H}(D) = \sum_{f'|f} h(f'^2 D_0), \tag{1.2}$$

the Gauß class number of $O(D)$. Then $\mathcal{H}(D)$ equals the number of equivalence classes (under the group $\mathrm{SL}(2, \mathbb{Z})$ that acts through substitutions) of positive definite binary quadratic forms $q(X, Y) = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}$ and discriminant $b^2 - 4ac = D$. Under that correspondence, $h(D)$ yields the number of classes of primitive such forms, i.e., those that also satisfy $(a, b, c) = 1$.

In his Disquisitiones Arithmeticae [5], Gauß found a powerful algorithm to determine $\mathcal{H}(D)$. It is suitable for large scale calculations, see e.g. [8] section 3 for details.

We will need the following result due to Deuring [4].

1.3 Theorem. *Let p be a prime and $t \in \mathbb{Z}$ satisfy $|t| < 2p^{1/2}$. The number $H(t, p)$ of (0.2) equals the Gauß class number $\mathcal{H}(t^2 - 4p)$.*

(In fact, Deuring goes much further. He determines the endomorphism rings of elliptic curves over arbitrary finite fields $\mathbb{F}_q$, which are orders either in imaginary quadratic fields or in quaternion algebras over $\mathbb{Q}$. The numerical identity of (1.3) is a mere corollary of his results.)

The class numbers $h(D_0)$ and $h(D)$ (and thus $H(t, p)$) may also be calculated through the analytic class number formula (see e.g. [12]). First,

$$h(D_0) = w(D_0)\ |D_0|^{1/2}\pi^{-1}L(1,\chi), \tag{1.4}$$

where:

$w(D_0) = 2, 3$ for $D_0 = -4, -3$, respectively, and
$w(D_0) = 1$ otherwise,

χ is the quadratic Dirichlet character (mod D_0) corresponding to $\mathbb{Q}(D_0^{1/2})$:

$$\chi(\ell) = (\frac{D_0}{\ell}) \quad \text{(quadratic symbol, } \ell > 2 \text{ prime)}, \tag{1.5}$$

$$\chi(2) = (\frac{D_0}{2})\ \begin{matrix}\text{(Kronecker}\\ \text{symbol)}\end{matrix} = \begin{cases} 1 & D_0 \equiv 1 \ (\mathrm{mod} 8) \\ 0 & D_0 \equiv 0, 4 \ (\mathrm{mod} 8) \\ -1 & D_0 \equiv 5 \ (\mathrm{mod} 8), \end{cases}$$

and

$$L(1,\chi) = \prod_{\ell \text{ prime}} (1 - \chi(\ell)\ell^{-1})^{-1} \tag{1.6}$$

is the value of its L-series of $s = 1$. Note that the product fails to converge absolutely; it must be evaluated in the given order.

Next, the class numbers for $D = f^2 D_0$ $(f > 1)$ and D_0 are related by

$$h(D) = \frac{f}{w(D_0)}\ h(D_0) \prod_{\ell \text{ prime}, \ell | f} (1 - \chi(\ell)\ell^{-1}) \tag{1.7}$$

(e.g. [2], Thm. 7.24).

In order to avoid phenomena special to the primes 2 and 3, we assume from now on that p is a prime larger than 3. Then we have for an elliptic curve E over $\mathbb{F}_p$:

$$E \text{ supersingular} \Leftrightarrow t(E/\mathbb{F}_p) = 0. \tag{1.8}$$

Combined with the preceding formulas, and going through the cases, the number of supersingular $E/\mathbb{F}_p$ is

$$H(0,p) = h, 2h, 4h, \tag{1.9}$$

if the prime $p > 3$ is congruent to (1 or 5), 7, 3 (mod8), respectively, where $h = h(D_0)$ is the class number of the field $\mathbb{Q}((-p)^{1/2})$ with fundamental discriminant $D_0 = -4p, -p, -p$.

For some reasons, it is convenient to count elliptic curves $E/\mathbb{F}_p$ according to the size of their automorphism groups $\mathrm{Aut}_{\mathbb{F}_p}(E)$ over $\mathbb{F}_p$. Under our assumption $p > 3$, $\mathrm{Aut}_{\mathbb{F}_p}(E)$ is cyclic of order $2w(E/\mathbb{F}_p)$, with

$$(1.10) \qquad w(E/\mathbb{F}_p) = \begin{cases} 3 & \text{if } p \equiv 1 \ (\mathrm{mod} 3) \text{ and } j(E) = 0 \\ 2 & \text{if } p \equiv 1 \ (\mathrm{mod} 4) \text{ and } j(E) = 1728 \\ 1 & \text{in all other cases.} \end{cases}$$

For p fixed, we have

$$(1.11) \qquad \sum_{E/\mathbb{F}_p} \frac{1}{w(E/\mathbb{F}_p)} = 2p,$$

or equivalently, the number of isomorphism classes of curves $E/\mathbb{F}_p$ is

$$\#\{E/\mathbb{F}_p\} = 2p+6, 2p+2, 2p+4, 2p \ \text{ for } p \equiv 1, 5, 7, 11 \ (\mathrm{mod} 12),$$

respectively. (There are 6 curves $E/\mathbb{F}_p$ with $j(E) = 0$ if $p \equiv 1 \ (\mathrm{mod}\, 3)$, 4 curves $E/\mathbb{F}_p$ with $j(E) = 1728$ if $p \equiv 1$ (mod4), and 2 curves $E/\mathbb{F}_p$ with a fixed j-invariant otherwise. Note that the number of "special" curves with $w \neq 1$ is universally bounded by 10 for each p, and is therefore negligible for p large.) We now slightly modify the number $H(t,p)$ of (0.2) and define

$$(1.12) \qquad H^*(t,p) := \sum_{E/\mathbb{F}_p, t(E/\mathbb{F}_p)=1} \frac{1}{w(E/\mathbb{F}_p)}.$$

Similarly, for a discriminant $D = f^2 D_0$,

$$(1.13) \qquad \begin{aligned} h^*(D) &:= h(D)/w(D) \quad \text{and} \\ \mathcal{H}^*(D) &:= \sum_{f'|f} h^*(f'^2 D_0), \end{aligned}$$

with $w(D) = \frac{1}{2}\#(\text{unit group of } O(D))$ as in (1.4). As in (1.3), we get

$$(1.14) \qquad H^*(t,p) = \mathcal{H}^*(t^2 - 4p),$$

and several formulas (e.g. (1.4), (1.7)) become smoother for the starred quantities $h^*, \mathcal{H}^*$.

2. A heuristic model.

Let $F = F(E/\mathbb{F}_p)$ be the Frobenius endomorphism of $E/\mathbb{F}_p$. It satisfies the quadratic equation

$$(1.14) \qquad F^2 - tF + p = 0,$$

where $t = t(E/\mathbb{F}_p)$. Fix $n \in \mathbb{N}$ coprime with p. Via its action on n-division points of E, F yields a conjugacy class $[F_n] \subset \mathrm{GL}(2, \mathbb{Z}/n)$.

(2.2) For fixing ideas, assume that $n < 2p^{1/2}$. There are about $2p$ curves

$E/\mathbb{F}_p$, whose Frobenius traces $t(E/\mathbb{F}_p)$ are distributed among the about $4p^{1/2}$ integers in the interval $[-2p^{1/2}, 2p^{1/2}]$. Regarding their $[F_n]$ as random and evenly distributed in $\mathrm{GL}(2, \mathbb{Z}/n)$, we expect a frequency of curves $E/\mathbb{F}_p$ with Frobenius trace in a given class $t \in \mathbb{Z}/n$ proportional to

$$\#\{A \in \mathrm{GL}(2, \mathbb{Z}/n) \mid \mathrm{tr}(A) = t, \det(A) = p\}.$$

(Here and in the sequel, we often abuse notation and write $k \in \mathbb{Z}/n$ for the class of $k \in \mathbb{Z}$.) This is a *ceteris paribus* expectation, which exploits information from n-division points only.

(2.3) Next, for coprime m and n, $[F_m]$ and $[F_n]$ should be approximately independent, at least if $m \cdot n$ is sufficiently small compared to $2p^{1/2}$.

(2.4) Let $v_\infty(t,p) = \frac{2}{\pi}\sqrt{1 - t^2/4p}$ for real t with $|t| \leq 2p^{1/2}$ and 0 otherwise. Using v_∞, we extend the crude heuristic considerations of (2.2) and (2.3) to arbitrary n with $(n,p) = 1$.

(2.5) Let us first specify the notion of probability we use. We put $\mathcal{E}_p$ for the set of isomorphism classes of elliptic curves over $\mathbb{F}_p$. By (1.11),

$$E \longmapsto \frac{1}{2p \cdot w(E/\mathbb{F}_p)}$$

yields a probability measure μ on $\mathcal{E}_p$. Writing $\mathrm{tr} : E \longmapsto t(E/\mathbb{F}_p)$ for the Frobenius trace map from $\mathcal{E}_p$ to $\mathcal{T}_p := \{t \in \mathbb{Z} \mid |t| < 2p^{1/2}\}$, we let

$$\pi^*(t,p) = (\mathrm{tr}_*(\mu))(t).$$

Then $2p\pi^*(t,p) = H^*(t,p)$, i.e., $\pi^*(?,p)$ is the probability measure on $\mathcal{T}_p$ that describes the frequency of the different Frobenius traces, the weights $w(E/\mathbb{F}_p)$ taken into account.

Now our assumption is that $\pi^*(t,p)$ is approximately given by

$$P^*(t,p) = c(p) \prod_{\ell \text{ prime}} v_\ell(t,p)\; v_\infty(t,p), \tag{2.6}$$

where

$$v_\ell(t,p) = \lim_{k\to\infty} \frac{\#\{A \in \mathrm{Mat}(2, \mathbb{Z}/\ell^k) \mid \mathrm{tr}(A) = t, \det(A) = p\}}{\ell^{2k-2}(\ell^2 - 1)}$$

and $c(p)$ is a normalizing constant determined such that $\sum_t P^*(t,p) = 1$. Note that:

(2.7) for $\ell \neq p$, the denominator $\ell^{2k-2}(\ell^2 - 1)$ is the average over all $t \in \mathbb{Z}/\ell^k$ of $\#\{A \in \mathrm{Mat}(2, \mathbb{Z}/\ell^k) \mid \mathrm{tr}(A) = t, \det(A) = p\}$;

(2.8) the limit $\lim_{k\to\infty}$ defining $v_\ell(t,p)$ exists and is in fact attained for all $k \geq k_0$, where k_0 depends on t, p, and ℓ; its value will be determined in the next section;

(2.9) regarding $v_\ell(t,u)$ as a continuous function on the compact group $\mathbb{Z}_\ell \times \mathbb{Z}_\ell^*$, i.e., replacing $p \neq \ell$ by an ℓ-adic variable $u \in \mathbb{Z}_\ell^*$, its average is one, due to (2.7);

(2.10) for a fixed prime p, the factors $v_\ell(t,p)$ fluctuate around 1, and the infinite product $\prod_\ell v_\ell(t,p)$ will turn out to converge (but fail to converge absolutely).

Hence the meaning of (2.6) is that $P^*(t,p)$ is built up from independent local contributions of the primes ℓ (including $\ell = p$), which reflect the frequency of matrices in $\mathrm{Mat}(2,\mathbb{Z},\ell^k)$ with the given characteristic polynomial (2.1). The factor v_∞, which of course is motivated from Birch's result and the Sato-Tate conjecture, plays a similar role for the "infinite prime" of $\mathbb{Q}$. Namely, (0.1) says that the conjugacy class of the normalized Frobenius endomorphism $p^{-1/2}F(E/\mathbb{F}_p)$ is represented by an element of the compact subgroup $\mathrm{SO}(2)$ of $\mathrm{GL}(2,\mathbb{R})$. Writing $v_\infty(t,p) = f(\tau) = \frac{2}{\pi}\sqrt{1-\tau^2}$ for $|\tau| \leq 1$ and $f(\tau) = 0$ otherwise, with $\tau = t/2p^{1/2}$, the measure $f(\tau)d\tau$ on $\mathbb{R}$ is the direct image of the normalized Haar measure on $\mathrm{SO}(2)$ under the map $A \longmapsto \mathrm{tr}(A)$ from $\mathrm{SO}(2)$ to $\mathbb{R}$.

Our model (2.6) is inspired from the considerations of [6]. We will see in section 4 that it accurately describes the actual behavior of $H^*(t,p)$, and thus yields a refinement of Birch's result.

3. The local weight factors $v_\ell(t,p)$.

Let ℓ be a fixed prime number, $k \geq 1$, and t, u arbitrary elements of $\mathbb{Z}_\ell$. As before, we also write t, u for their canonical images in $\mathbb{Z}/\ell^k$. Our aim here is to calculate the precise value of

$$(3.1) \qquad \alpha^{(k)}(t,u) := \#\{A \in \mathrm{Mat}(2,\mathbb{Z}/\ell^k) \mid \mathrm{tr}(A) = t, \det(A) = u\}.$$

(We are only interested in the case where $u =$ some prime p, which for $\ell \neq p$ is invertible in $\mathbb{Z}_\ell$, but the induction procedure as well as the case $\ell = p$ leads us naturally to consider the general case.) To simplify, we use the following notation:

$$(3.2) \qquad \begin{array}{rcl} R_k & = & \mathbb{Z}/\ell^k,\ M_k = \mathrm{Mat}(2,R_k),\ G_k = \mathrm{GL}(2,R_k), \\ I & = & I_2 \text{ the unit } 2\times 2\text{-matrix.} \end{array}$$

If A is a 2×2-matrix over the ring R, we put $T(A) = (\mathrm{tr}(A), \det(A)) \in R \times R$. The residue class of $a \in R_k$ or $\mathbb{Z}$ in $R_1 = \mathbb{F}_\ell$ (resp. of $A \in M_k$ or $\mathrm{Mat}(2,\mathbb{Z}) \in M_1$) is denoted by $\overline{a}$ (resp. $\overline{A}$). For $(t,u) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$

with discriminant $D = D(t,u) = t^2 - 4u$, we put

$$(\frac{t,u}{\ell}) = 1, 0, -1$$

if the polynomial $X^2 - \overline{t}X + \overline{u} \in \mathbb{F}_\ell[X]$ has $2, 1, 0$ different roots in $\mathbb{F}_\ell$, respectively. Its value depends only on D; we have

$$\begin{array}{rcll} (\frac{t,u}{\ell}) & = & (\frac{D}{\ell}) & \text{(quadratic symbol, if } \ell > 2) \\ (\frac{t,u}{2}) & = & (\frac{D}{2}) & \text{(Kronecker symbol, see (1.5)).} \end{array}$$

3.3 Lemma. *Put $\beta^{(k)}(t,u) = \ell^{2k} + \ell^{2k-1}, \ell^{2k} - \ell^{2k-2}, \ell^{2k} - \ell^{2k-1}$ if $(\frac{t,u}{\ell}) = 1, 0, -1$, respectively. There are precisely $\beta^{(k)}(t,u)$ matrices $A \in M_k$ such that $T(A) = (t,u) \in R_k \times R_k$ and $\overline{A}$ is non-scalar in M_1, and all these A are conjugate in M_k.*

Proof (induction on k). $k = 1$. Working over a field, all the non-scalar $A \in M_1$ with $T(A)$ fixed are conjugate, so their number is determined through the order of its centralizer $Z_1(A) \subset G_1$, which has $(\ell-1)^2$, $(\ell-1)\ell$, $\ell^2 - 1$ elements if $(\frac{t,u}{\ell}) = 1, 0, -1$. Since $\#G_1 = (\ell-1)\ell(\ell^2-1)$, we get the desired formula.

$k > 1$. Let $A \in M_k$ be such that $\overline{A}$ is non-scalar, and A_{k-1} its image in M_{k-1}, with respective centralizers $Z_k(A) \subset G_k$ and $Z_{k-1}(A) \subset G_{k-1}$. It is easy to see that $\#Z_k(A) = \ell^2 Z_{k-1}(A)$. Counting and using the induction hypothesis, we get that all such A with a fixed value of $T(A)$ are conjugate and have the right number. □

By the lemma, we are reduced to determine the number of $A \in M_k$ with $\overline{A}$ scalar, i.e., $A \equiv sI \pmod{\ell}$ with $s \in \{0, 1, \ldots, \ell - 1\}$. We first note that (3.3) gives

$$\alpha^{(1)}(t,u) = \ell^2 + (\frac{t,u}{\ell})\ell. \tag{3.4}$$

From now on, we assume that $k \geq 2$.

Let $A, A_1 \in M_k$ be such that $A = A_1 + sI$ with some $s \in R_k$. If $T(A) = (t,u)$, $T(A_1) = (t_1, u_1)$ then

$$t = 2s + t_1,\ u = s^2 + t_1 s + u_1,\ D(t,u) = D(t_1,u_1) \text{ in } R_k. \tag{3.5}$$

Conversely, if (t,u) and (t_1,u_1) satisfy the above relation with some s, then $\alpha^{(k)}(t,u) = \alpha^{(k)}(t_1,u_1)$, in view of the bijection $A_1 \longmapsto A_1 + sI$ of the relevant sets of matrices. Writing those $A \in M_k$ with $\overline{A}$ scalar in a unique fashion as $A = A_1 + sI$ with $s \in \{0, 1, \ldots, \ell - 1\} \subset R_k$ and $A_1 \in \ell M_k$, we get

$$\alpha^{(k)}(t,u) = \beta^{(k)}(t,u) + \#\{(s, A_1)\}, \tag{3.6}$$

where s and A_1 are subject to the above restrictions and

$$T(A_1) = (t_1, u_1) = (-2s + t, s^2 - ts + u).$$

Let $(t, u) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ be given. Recall that $D(t, u) = t^2 - 4u$.

3.7 Lemma.

(i) *A necessary and sufficient condition for the existence of pairs* (s, A_1) *as in* (3.6) *is:*

$l > 2$: $D(t, u) \equiv 0 \pmod{\ell^2}$. *In this case, s is determined through* $2s \equiv t \pmod{\ell}$.

$l = 2$: $t \equiv 0 \pmod{2}$ *and* $u \equiv 0 \pmod{4}$*; here* $s = 0$*; or* $t \equiv 0 \pmod{2}$ *and* $u \equiv t - 1 \pmod{4}$*; here* $s = 1$.

(ii) *Condition* (i) *for* $\ell = 2$ *may be summarized as* $D(t, u) \equiv 0$ *or* $4 \pmod{16}$.

(iii) *If condition* (i) *is fulfilled, solutions* (s, A_1) *as in* (3.6) *correspond bijectively to solutions* $B = \ell^{-1} A_1 \in M_{k-1}$ *of*

$$\mathrm{tr}(B) = \ell^{-1} t_1, \ \det(B) \equiv \ell^{-2} u_1 \pmod{\ell^{k-2}}.$$

Proof. (i) is straightforward. For (ii) we note that, although the condition depends only on $(t, u) \pmod{4}$, the relevant discrimiant $D(t, u)$ is defined $(\mathrm{mod} 16)$. Inspection of the cases now leads to the equivalent condition $D(t, u) \equiv 0, 4 \pmod{16}$. As to (iii), $B \longmapsto \ell B$ is a well-defined bijection from M_{k-1} to ℓM_k, and $\det(\ell B) = \ell^2 \det(B)$. □

3.8 Corollary. *Either the conditions of* (3.7)(i) *are fulfilled with* $s \in \{0, 1, \ldots, \ell - 1\}$ *and* (t_1, u_1) *as in* (3.6). *Then*

$$\alpha^{(k)}(t, u) = \beta^{(k)}(t, u) + \sum_{c \in \ell^{k-2} R_{k-1}} \alpha^{(k-1)}(\ell^{-1} t_1, \ell^{-2} u_1 + c).$$

Or they fail, in which case $\alpha^{(k)}(t, u) = \beta^{(k)}(t, u)$.

(3.9) Again, let $(t, u) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, and suppose moreover that $D(t, u) = t^2 - 4u \neq 0$. We put $\delta = \delta(t, u)$ for the largest integer $i \geq 0$ such that $\ell^{2i} | D$ and, in case $\ell = 2$, $D/2^{2i} \equiv 0$ or $1 \pmod{4}$. Note that δ depends only on D and remains unchanged if D is replaced by $D - 4c$, provided that $c \equiv 0 \pmod{\ell^{2\delta+2}}$. With these notations, we have:

3.10 Proposition. *Suppose that* $k \geq 2\delta + 2$. *The number* $\alpha^{(k)}(t, u)$ *of matrices* $A \in \mathrm{Mat}(2, \mathbb{Z}/\ell^k)$ *with trace t and determinant u is given by*

$$\alpha^{(k)}(t, u) = \ell^{2k} + \ell^{2k-1} + \left\{ \begin{array}{c} 0 \\ -(\ell+1)\ell^{2k-\delta-2} \\ -2\ell^{2k-\delta-1} \end{array} \right\} \quad if(\frac{D/\ell^{2\delta}}{\ell}) = \left\{ \begin{array}{c} 1 \\ 0 \\ -1 \end{array} \right\}.$$

Proof (by induction on δ). If $\delta = 0$ then $\alpha^{(k)}(t,u) = \beta^{(k)}(t,u)$, and the formula is given by (3.3). Thus let $\delta > 0$. With notations as in (3.8) and (3.6), $D(\ell^{-1}t_1, \ell^{-2}u_1) = \ell^{-2}D(t,u)$ and $\delta(\ell^{-1}t_1, \ell^{-2}u_1) = \delta(t,u) - 1 = \delta - 1$. In view of $k \geq 2\delta + 2$, $k - 2 \geq 2(\delta - 1) + 2$, and hence $\delta(\ell^{-1}t_1, \ell^{-2}u_1 + c) = \delta - 1$ for each $c \in \ell^{k-2}R_{k-1}$ as in (3.8). The induction hypothesis applies to all the $\alpha^{(k-1)}(\ell^{-1}t_1, \ell^{-2}u_1 + c)$, which are evaluated through the same value

$$\left(\frac{D(\ell^{-1}t_1, \ell^{-2}u_1 + c)/\ell^{2(\delta-1)}}{\ell}\right) = \left(\frac{D(t,u)/\ell^{2\delta}}{\ell}\right).$$

Plugging in, we get the result. □

3.11 Remarks. (i) The numbers $\alpha^{(k)}(t,u)$ for $k < 2\delta(t,u) + 2$ may be determined through analogous but more complicated considerations. Since the resulting less smooth formulas are useless for our purposes, they are omitted.

(ii) Proposition 3.10 may be rephrased as follows. Let $T : \mathrm{Mat}(2, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ be the trace-determinant map and μ, ν the normalized Haar measures on $\mathrm{Mat}(2, \mathbb{Z}_\ell)$, $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$, respectively. Then $(T_*\mu)(x) = h(x)\nu(x)$ with the continuous function

$$h(x) = 1 + \ell^{-1} + \left\{\begin{array}{c} 0 \\ -(\ell+1)\ell^{-\delta(x)-2} \\ -2\ell^{-\delta(x)-1} \end{array}\right\} \quad \text{if} \quad \left(\frac{D(x)/\ell^{2\delta(x)}}{\ell}\right) = \left\{\begin{array}{c} 1 \\ 0 \\ -1 \end{array}\right\}$$

on $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Here δ and D are the obvious functions, where $\delta(x)$ is ascribed the value ∞ if $x = (t,u)$ with $D(x) = t^2 - 4u = 0$.

Without giving an explicit expression for h, some of its qualitative properties, including the fact that it is locally constant off the locus $D(x) = 0$, have been decribed by Lang and Trotter, [6] pp. 124–132.

The next two corollaries are immediate consequences of the preceding.

3.12 Corollary. *The weight factors $v_\ell(t,p)$ of* (2.6) *are given by*

$$v_\ell(t,p) = (1 - \ell^{-2})^{-1}(1 + \ell^{-1} + \left\{\begin{array}{c} 0 \\ -(\ell+1)\ell^{-\delta-2} \\ -2\ell^{-\delta-1} \end{array}\right\})$$

with $\delta = \delta(t,p)$ and according to the values $+1, 0, -1$ of $(\frac{(t^2-4p)/\ell^{2\delta}}{\ell})$.

3.13 Corollary. *The weight factors $v_\ell(t,p)$ depend only on $D(t,p) = t^2 - 4p$. We thus also write $v_\ell(D)$ for $v_\ell(t,p)$. Then we have $v_\ell(f^2D) = v_\ell(D)$ if $(f, \ell) = 1$.*

3.14 Corollary. *Given t and p, the infinite product*

$$v(D) = v(t,p) := \prod_{\ell \text{ prime}} v_\ell(t,p)$$

converges.

Proof. As usual, $D = t^2 - 4p = f^2 D_0$ with a fundamental discriminant D_0. For a prime ℓ not dividing f, the quantity $\delta_\ell(t,u)$ vanishes. For such ℓ,

$$v_\ell(t,p) = \frac{1}{1-\chi(\ell)\ell^{-1}}, \tag{3.15}$$

where χ is the quadratic character associated to D_0, $\chi(\ell) = (\frac{D_0}{\ell}) = (\frac{D}{\ell})$. Hence the product in question agrees up to a finite number of non-vanishing factors with the product (1.6), which converges (non-absolutely) to the value $L(1,\chi)$ of the Dirichlet L-series $L(s,\chi)$ at $s = 1$. □

4. $\pi^*(t,p) = P^*(t,p)$**.**

Again, let $D = t^2 - 4p = f^2 D_0$ with a fundamental discriminant $D_0 < 0$. Combining the formulas in section 1, we get

$$\mathcal{H}^*(D) = S(f, D_0) h^*(D_0) \tag{4.1}$$

with

$$h^*(D_0) = \pi^{-1} |D_0|^{1/2} L(1,\chi)$$

and

$$S(f, D_0) = \sum_{f'|f} f' \prod_{\substack{\ell \text{ prime} \\ \ell | f}} (1 - \chi(\ell)\ell^{-1}),$$

where χ is the Dirichlet character with $\chi(\ell) = (\frac{D_0}{\ell})$.

4.2 Lemma. *Let f and g be relatively prime. Then*

$$S(fg, D_0) = S(f, D_0) S(g, D_0).$$

Proof. Straightforward. □

We are thus reduced to calculate $S(f, D_0)$ for prime powers f.

4.3 Lemma. *Let $f = \ell^k$ with a prime ℓ. Then*

$$S(f, D_0) = 1 + (\ell - \chi(\ell))(\frac{\ell^k - 1}{\ell - 1}).$$

Proof. Both sides equal 1 for $k = 0$. If $k > 0$ then $S(f, D_0) = 1 + \sum_{1 \le i \le k} \ell^i (1 - \chi(\ell)\ell^{-1})$. Evaluating yields the result. □

4.4 Lemma. *With notations as above,*

$$\ell^k v_\ell(\ell^{2k} D_0) = v_\ell(D_0) S(\ell^k, D_0).$$

Proof. This follows from comparing (3.12) with (4.3). □

4.5 Corollary. *For $D = t^2 - 4p = f^2 D_0$ as above,*

$$\mathcal{H}^*(D) = \pi^{-1}|D|^{1/2} v(t,p)$$

with

$$v(t,p) = \prod_{\ell \text{ prime}} v_\ell(t,p)$$

as in (3.14).

Proof. Insert (4.4) into (4.1)! □

In view of $|D|^{1/2} = p^{1/2} \cdot \pi \cdot v_\infty(t,p)$, the formula

$$H^*(t,p) = \frac{p^{1/2}}{c(p)} P^*(t,p)$$

comes out. Since $\sum_t H^*(t,p) = 2p$ by (1.11) and (1.12), we find upon comparing with (2.5) the following result.

4.6 Theorem. *The* a posteriori*-probability $\pi^*(t,p)$ of* (2.5) *agrees with the probability $P^*(t,p)$ prescribed by the model* (2.6)*. The constant $c(p)$ equals $\frac{1}{2p^{1/2}}$, and thus*

$$\begin{aligned} P^*(t,p) &= \tfrac{1}{2p^{1/2}} \cdot v(t,p) \cdot v_\infty(t,p), \\ H^*(t,p) &= p^{1/2} \cdot v(t,p) \cdot v_\infty(t,p). \end{aligned}$$

4.7 Corollary. *For $p > 3$ fixed, the weights $v(t,p)$ satisfy*

$$\sum_{t \in \mathbb{Z}, |t| < 2p^{1/2}} v(t,p) v_\infty(t,p) = 2p^{1/2}.$$

5. Asymptotics of $H(t,p)$.

We now use the preceding considerations to study the average behavior of $H(t,p)$. For t fixed, let

$$H_t(x) := \sum_{3 < p \le x} H(t,p). \tag{5.1}$$

Here and in the sequel, p and ℓ always denote prime numbers, where p is assumed larger than 3.

As usual we write $f(x) \sim g(x)$ (asymptotic equivalence) if the two functions $f(x)$ and $g(x)$ satisfy $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, and $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. Here f and g are real-valued and defined on sufficiently large real or natural numbers. We assume f and g such that all the integrals below exist. If f is defined on a subset of $\mathbb{N}$, $\int_c^x f(s)ds$

has to be interpreted as $\sum_{c\leq s\leq x} f(s)$, etc.

We want to describe $H_t(x)$ up to asymptotic equivalence. The properties of "$\sim$" we need are the following:

(5.2) Let $g(x)$ be such that $\int_c^x g(s)ds$ tends to ∞ for $x \longrightarrow \infty$, and suppose that $f(x) = o(g(x))$. Then

$$\int_c^x f(s)ds = o(\int_c^x g(s)ds)$$

as functions in x;

(5.3) if $f(x) \sim g(x)$, where $g(x)$ is as in (5.2), then

$$\int_c^x f(s)ds \sim \int_c^x g(s)ds;$$

(5.4) let $\alpha > -1$ and $F(x)$ be a primitive for $\frac{x^\alpha}{\log x}$. Then $F(x) \sim \frac{1}{1+\alpha}\frac{x^{1+\alpha}}{\log x}$.

Here (5.2) results from the obvious estimate, and (5.3), (5.4) are immediate consequences. We further recall the principle of Abel summation (see e.g. [10] pp. 3/4):

(5.5) Let $(a_n)_{n\in\mathbb{N}}$ be a series, $A(x) = \sum_{n\leq x} a_n$, and b a C^1-function on $[1, x]$. Then

$$\sum_{1\leq n\leq x} a_n b(n) = A(x)b(x) - \int_1^x A(s)b'(s)ds.$$

5.6 Lemma. *We use notation as in* (3.2). *Thus let ℓ be a prime number, $k \geq 1$, and t an element of $R_k = \mathbb{Z}/\ell^k$. The number of elements A of $G_k = \mathrm{GL}(2, R_k)$ with $\mathrm{tr}(A) = t$ is*

$$\begin{array}{ll} (\ell^2-\ell)\ell^{3k-2}, & \textit{if } t \textit{ is divisible by } \ell, \\ (\ell^2-\ell-1)\ell^{3k-2}, & \textit{if } t \textit{ is invertible in } R_k. \end{array}$$

Proof (see [6] pp. 34–36). Let $G_k(t)$ be the set of matrices in G_k with trace t. If $t \equiv t'$ (modℓ) then $A \longmapsto A + \begin{pmatrix} t'-t, & 0 \\ 0, & 0 \end{pmatrix}$ is a bijection from $G_k(t)$ to $G_k(t')$. Similarly, for $u \in R_k^*$, $A \longmapsto uA$ is bijective from $G_k(t)$ to $G_k(ut)$. It thus suffices to determine the numbers of elements of $G_1(0)$ and $G_1(1)$, which by elementary calculations are $\ell^3 - \ell^2$ and $\ell^3 - \ell^2 - \ell$, respectively. □

We fix a prime ℓ and keep the above notation. The number $\#G_k(t)$

averaged over all $t \in R_k$ is $\#(G_k)/\ell^k = \ell^{3k-3}(\ell^2-1)(\ell-1)$. We therefore put

$$u_\ell(t) := \frac{\#G_k(t)}{\#G_k/\ell^k} = \begin{cases} \frac{\ell^3-\ell^2}{(\ell^2-1)(\ell-1)} & \text{if } t \equiv 0 \ (\mathrm{mod} \ell) \\ \frac{\ell^3-\ell^2-\ell}{(\ell^2-1)(\ell-1)} & \text{if } t \not\equiv 0 \ (\mathrm{mod} \ell). \end{cases} \tag{5.7}$$

It is independent of k, and by the very definitions of $u_\ell(t)$, $v_\ell(t,u)$, we have

$$u_\ell(t) = \int_{\mathbb{Z}_\ell^*} v_\ell(t,u)du, \tag{5.8}$$

the average of the weight function $v_\ell(t,*)$. Here "du" is the normalized Haar measure on $\mathbb{Z}_\ell^*$. This means that the probability of a randomly chosen matrix $A \in \mathrm{GL}(2,\mathbb{Z}_\ell)$ to have a trace divisible by ℓ is slightly larger than ℓ^{-1}.

5.9 Proposition. *Let $\pi(x)$ denote the prime number function, $\pi(x) = \#\{p \text{ prime} \mid p \leq x\}$. Then*

$$\lim_{x\to\infty} \pi(x)^{-1} \sum_{p\leq x} v_\ell(t,p) = u_\ell(t).$$

Proof. First note that for any function f on $R_k^* = (\mathbb{Z}/\ell^k)^*$, extended by zero to R_k, the limit

$$\lim_{x\to\infty} \pi(x)^{-1} \sum_{p\leq x} f(p)$$

exists and equals the average

$$(\ell-1)^{-1}\ell^{1-k} \sum_{0\leq i<p^k} f(i),$$

by Dirichlet's theorem. Thus let $v_\ell^{(k)}(t,u)$ be the k-th step approximation of $v_\ell(t,u)$, that is,

$$v_\ell^{(k)}(t,u_0) = \mathrm{vol}_k^{-1} \int_{u\equiv u_0 \ (\bmod \ell^k)} v_\ell(t,u)du,$$

where $\mathrm{vol}_k = \mathrm{vol}\{u \in \mathbb{Z}_\ell^* \mid u \equiv u_0 \ (\mathrm{mod}\ell^k)\} = (\ell-1)^{-1}\ell^{1-k}$. By the above, we have

$$\lim_{x\to\infty} \pi(x)^{-1} \sum_{p\leq x} v_\ell^{(k)}(t,p) = u_\ell(t) \tag{$*$}$$

independently of k. Now as we see from (3.12), $|v_\ell(t,u) - v_\ell^{(k)}(t,u)|$ is bounded by a constant C which depends only on ℓ, and vanishes if $t^2 \not\equiv 4u \ (\mathrm{mod}\ell^k)$. Hence both the lim sup and the lim inf for $x \to \infty$ of $\pi^{-1}(x)\sum_{p\leq x} v_\ell(t,p)$ differ less than $\mathrm{vol}_k \cdot C$ in absolute value from

($*$). Since vol_k tends to zero, the result follows. □

Thus we have

$$\sum_{p\leq x} v_\ell(t,p) \sim u_\ell(t)\pi(x) \sim u_\ell(t)\frac{x}{\log x}. \tag{5.10}$$

It is crucial to know whether a similar property for

$$u(t) := \prod_{\ell \text{ prime}} u_\ell(t) \tag{5.11}$$

holds, i.e., do we have

$$\lim_{x\to\infty} \pi(x)^{-1} \sum_{p\leq x} v(t,p) = u(t) \ ? \tag{5.12?}$$

Equivalently, does the infinite product (5.11) commute with the averaging in (5.9)? This is a deep arithmetical question, which will be answered to the affirmative in what follows.

5.13 Proposition. *Let $t \in \mathbb{Z}$, and consider the summatory functions $F(x) = \sum_{p\leq x} f(p)$ of the following functions f defined on primes $p > 3$ and extended by zero to $\mathbb{N}$:*

(i) *$v(t,p)$;*
(ii) *$p^\alpha v(t,p)$ for some fixed real number $\alpha > -1$;*
(iii) *$\frac{2}{\pi}p^{-1/2}v(t,p)$;* (iiia) *$H^*(t,p)/p$;* (iiib) *$H(t,p)/p$;*
(iv) *$\frac{2}{\pi}p^{1/2}v(t,p)$;* (iva) *$H^*(t,p)$;* (ivb) *$H(t,p)$.*

Then the following are equivalent:

(i) *$F(x) \sim u(t)\frac{x}{\log x}$ in case* (i)*, (i.e.,* (5.12) *is true);*
(ii) *$F(x) \sim \frac{u(t)}{1+\alpha}\frac{x^{1+\alpha}}{\log x}$ in case* (ii) *for one (thus each) real number $\alpha > -1$;*
(iii) *$F(x) \sim \frac{4}{\pi}u(t)\frac{x^{1/2}}{\log x}$ in one (thus all) of the cases* (iii), (iiia), (iiib)*;*
(iv) *$F(x) \sim \frac{4}{3\pi}u(t)\frac{x^{3/2}}{\log x}$ in one (thus all) of the cases* (iv), (iva), (ivb).

Proof. The difference of $H^*(t,p)$ and $H(t,p)$ is universally bounded by (1.11) and (1.12). Since, on the other hand, $H(t,p)$ grows sufficiently fast (if we write as usual $t^2 - 4p = D = f^2D_0$ with a fundamental discriminant D_0, $H(t,p) \sim H^*(t,p) = H^*(D) \geq fH^*(D_0)$ by (4.1)–(4.3), and $H^*(D_0) \sim H(D_0) = h(D_0)$ grows faster than $|D_0|^{1/2-\epsilon}$ for each $\epsilon > 0$; see [11]), the equivalence of (iiia) and (iiib) follows from (5.3). The equivalence of (iii) and (iiia) also follows from (5.3) and the formula (4.6), since $v_\infty(t,p) = \frac{2}{\pi}\sqrt{1-t^2/4p} \sim \frac{2}{\pi}$. Similarly, we get the asymptotic equivalence of the summatory functions in group (iv). It therefore suffices to prove the equivalence of (i) and (ii). Let α, β be real numbers such that $\alpha, \alpha+\beta > -1$. We will show that

$$\sum_{p\leq x} p^{\alpha} v(t,p) \sim \frac{u(t)}{1+\alpha}\,\frac{x^{1+\alpha}}{\log x}$$

implies the same formula for α replaced by $\alpha+\beta$. Define the series $(a_n)_{n\in\mathbb{N}}$ through

$$a_n := p^{\alpha} v(t,p),\ n = p > 3 \text{ prime}$$

and $a_n = 0$ otherwise, and the C^1-function $b(x) := x^{\beta}$.
Now (5.5) combined with (5.3) yields

$$\sum_{p\leq x} p^{\alpha+\beta} v(t,p) \sim \frac{u(t)}{1+\alpha}\,\frac{x^{1+\alpha+\beta}}{\log x} - \frac{u(t)\beta}{1+\alpha} F(x)$$

with a primitive $F(x)$ of $\frac{x^{\alpha+\beta}}{\log x}$. Thus, using (5.4),

$$\begin{aligned}\textstyle\sum_{p\leq x} p^{\alpha+\beta} v(t,p) &\sim \tfrac{u(t)}{1+\alpha}\left[\tfrac{x^{1+\alpha+\beta}}{\log x} - \tfrac{\beta}{1+\alpha+\beta}\,\tfrac{x^{1+\alpha+\beta}}{\log x}\right]\\ &= \tfrac{u(t)}{1+\alpha+\beta}\,\tfrac{x^{1+\alpha+\beta}}{\log x}\end{aligned}$$

as desired. □

Now the asymptotic behavior discussed in the proposition has been verified in case (iiia) (i.e., for the summatory function of $H^*(t,p)/p$) by David-Pappalardi: see equation (32) of [3]. Strictly speaking, the proof is given in their paper for odd t only, but as the authors write (*loc. cit.* p. 169), the proof is similar when t is even, and can be obtained from the case of odd t by obvious modifications. We can therefore draw the following conclusion.

5.14 Theorem. *Let t be an integer.*

(i) $H_t(x) \sim \frac{4}{3\pi} u(t) \frac{x^{3/2}}{\log x}$

(ii) *Put* $C := \frac{4}{3\pi} u(1) = \frac{4}{3\pi} \prod_{\ell} \frac{\ell^3-\ell^2-\ell}{(\ell^2-1)(\ell-1)} = 0,261070408\ldots$ *and* $w(t) := \prod_{\ell\mid t} \frac{\ell^2-\ell}{\ell^2-\ell-1}$ *(recall ℓ is always prime!). Then*

$$H_t(x) \sim w(t)\cdot C \cdot \frac{x^{3/2}}{\log x}.$$

(iii) *In the case $t = 0$ we get*

$$H_0(x) \sim \frac{2}{9}\pi \frac{x^{3/2}}{\log x}.$$

Proof. (i) is immediate from (5.13) and David-Pappalardi's result. (ii) follows from (i) by rearranging the factors in $u(t)$, which is allowed in view of the absolute convergence of the products defining $u(t)$ and $w(t)$. For $t = 0$, the constant in front of $\frac{x^{3/2}}{\log x}$ is $\frac{4}{3\pi}\prod_\ell(\frac{\ell^2}{\ell^2-1}) = \frac{4}{3\pi}\zeta(2) = \frac{2}{9}\pi$. □

6. Remarks and comments.

(6.1) Part (ii) of Theorem 5.14 may be interpreted as follows: Let $t \in \mathbb{Z}$ be fixed, and let E be a randomly chosen elliptic curve over the prime field $\mathbb{F}_p$, where p is random and large compared to t. Then the probability that E has Frobenius trace $t(E/\mathbb{F}_p)$ equal to t is proportional with $w(t)$. This should be compared with H.W. Lenstra's result [7] Proposition 1.14 about the probability that $N(E/\mathbb{F}_p) = 1 + p - t(E/\mathbb{F}_p)$ is divisible by a prime $\ell \ll p$. Note that $w(t)$ depends only on the prime factors (without multiplicity) of t, and is maximal for $t = 0$, $w(0) = \prod_\ell(\frac{\ell^2-\ell}{\ell^2-\ell-1}) = 2,67411272\ldots$ Some numerical values of $H_t(x)$ are given in Table 6.5 below.

(6.2) The average number (in the sense of [10] p. 37) of supersingular elliptic curves E over $\mathbb{F}_p$ is $\frac{\pi}{3}p^{1/2}$. This follows from (1.9), (5.14)(iii) and the formula $\sum_{p\leq x} p^{1/2} \sim \frac{2}{3}\frac{x^{3/2}}{\log x}$, which in turn is an easy consequence of the prime number theorem and Abel summation (5.5). We conclude that the number of $\mathbb{F}_p$-rational supersingular j-invariants is $\frac{\pi}{6}p^{1/2}$ in average, compared to the number $\frac{p}{12}+O(1)$ of all supersingular invariants in characteristic p. These latter lie at worst in the quadratic extension $\mathbb{F}_{p^2}$ of p. The expected number of elements of a k-subset of $\mathbb{F}_{p^2}$ which lie in $\mathbb{F}_p$ is k/p; hence there is a strong bias of supersingular invariants to actually lie in the prime field $\mathbb{F}_p$.

(6.3) We didn't try to get estimates for the remainder term in $H_t(x) \sim$ const.$\frac{x^{3/2}}{\log x}$, which looks like a delicate problem of analytic number theory. If one is interested in an asymptotic formula as accurate as possible, it is advisable to use a better approximation of $\pi(x)$ than $\frac{x}{\log x}$, e.g., $li(x) = \int_2^x \frac{ds}{\log s}$. As the tables show, the formula (5.14) systematically under-estimates $H_t(x)$, which comes from the well-known under-estimation of $\pi(x)$ through $\frac{x}{\log x}$. However, the tabulated ratios $H_{t'}(x)/H_t(x)$ for small t, t' and $x = 10^6$, say, are very close to their predicted values $w(t')/w(t)$. See Table 6.5!

(6.4) It is conceiveable that the equidistribution philosophy underlying the present paper may be applied to more general situations, e.g. to curves of fixed genus over $\mathbb{F}_p$, or to abelian varieties of fixed dimension.

By lack of substitutes for (1.3) and (1.7) (at least), such generalizations seem to be inaccessible at present. However, using the well-known analogy between elliptic curves and Drinfeld modules (see e.g. the articles in [13]), similar probabilistic explanations may be given for the distribution of Frobenius elements of Drinfeld modules over finite fields. That circle of ideas will be treated in the forthcoming Saarbrücken thesis of Max Gebhardt.

Note that $H_t(x)$ as well as $H(t,p)$ is unchanged under $t \longmapsto -t$, which allows us to restrict to non-negative t in the following table. It contains, for $x = 10^i$ with $3 \leq i \leq 6$ and $0 \leq t \leq 10$, the values of $H_t(x)$ and of $H_t(x)/[H_1(x) \cdot w(t)]$, the latter rounded to 4 decimals.

6.5 Table. $H_t(x)$ and $H_t(x)/[H_1(x) \cdot w(t)]$

	$x = 10^3$		10^4		10^5		10^6	
$t = 0$	3.392	0,9949	81.380	0,9942	2.034.220	0,9965	53.157.932	0,9993
1	1.275	1,0000	30.609	1,0000	763.399	1,0000	19.892.381	1,0000
2	2.572	1,0086	60.836	0,9938	1.524.648	0,9986	39.731.198	0,9986
3	1.593	1,0412	36.532	0,9946	916.368	1,0003	23.855.268	0,9993
4	2.600	1,0196	61.441	1,0036	1.529.175	1,0016	39.765.119	0,9995
5	1.329	0,9902	32.241	1,0007	802.832	0,9991	20.929.738	0,9995
6	3.073	1,0042	73.454	0,9999	1.829.288	0,9984	47.714.735	0,9994
7	1.322	1,0122	31.315	0,9987	781.736	0,9996	20.371.883	0,9997
8	2.569	1,0074	61.209	0,9999	1.523.362	0,9977	39.770.028	0,9996
9	1.489	0,9732	36.566	0,9955	914.450	0,9982	23.865.230	0,9998
10	2.501	0,9317	64.188	0,9961	1.605.267	0,9988	41.853.998	0,9994

References

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

[2] D.A. Cox: Primes of the form $x^2 + ny^2$. John Wiley & Sons 1989.

[3] Ch. David and F. Pappalardi: Average Frobenius distributions of elliptic curves. Int. Math. Res. Notices 1999, No. **4**, 165–183.

[4] M. Deuring: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg **14**, 197–272 (1941).

[5] C.-F. Gauß: Disquisitiones Arithmeticae. Braunschweig 1801 (= Werke Band **1**, Göttingen 1870).

[6] S. Lang and H. Trotter: Frobenius distributions in GL_2-extensions. Lect. Notes Math. **504**, Springer-Verlag 1976.

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

[8] J. Oesterlé: Le problème de Gauss sur le nombre de classes. Ens. Math. **34**, 43–67 (1988).

[9] J. Tate: Algebraic cycles and poles of zeta functions. Arithmetical Algebraic Geometry, O.F.G. Schilling (ed.), 93–110, Harper & Row 1965.

[10] G. Tenenbaum: Introduction à la théorie analytique et probabiliste des nombres. Société Mathématique de France 1995.

[11] C.L. Siegel: Über die Classenzahl quadratischer Zahlkörper. Acta Arith. **1**, 83–86 (1935).

[12] D.B. Zagier: Zetafunktionen und quadratische Zahlkörper. Springer-Verlag 1981.

[13] Drinfeld Modules, Modular Schemes, and Applications. E.-U. Gekeler et al. (eds.), World Scientific 1997.

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