PACIFIC JOURNAL OF MATHEMATICS
Vol. 112, No 2, 1984

THE NONREGULAR ANALOGUE OF TCHEBOTAREV'S THEOREM

M. FRIED

Let L/K be a Galois extension of function fields in one variable where K has exact constants $\mathbf{F}(q)$, the finite field with q elements. For l a fixed integer and $\mathfrak{C}$ a conjugacy class of $\mathfrak{G}(L/K)$, this paper counts the primes $\mathfrak{p}$ of K of degree l for which the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

equals $\mathfrak{C}$ (Theorem 1.4). The answer depends on the restriction of elements of $\mathfrak{C}$ to the algebraic closure of $\mathbf{F}(q)$ in L: a proper extension of $\mathbf{F}(q)$ in general.

For $l = 1$ [Fr; Proposition 2] followed Dirichlet's celebrated argument using the rationality of L-series. Tchebotarev's original "field crossing argument" [T] is a part of the reduction to the cyclic case ([D] and [M]) that at once removes the restriction on l and the need for L-series (other than the Riemann hypothesis for curves over finite fields). This more elementary argument also improves the error estimates and therefore such practical applications as [FrS] and explicit forms of Hilbert's irreducibility theorem [Fr; §3]. We comment briefly on the latter (§2) to facilitate its use in [Fr, 2; §4] for the explicit production of rank 12 elliptic curves over Q.

Acknowledgement. This paper is a rewrite (with improvements) of Moshe Jarden's rewrite (with improvements) of our original notes. In particular, Lemma 1.2 improves one of the original arguments.

1. The nonregular analogue. Denote by $\tilde{K}$ the algebraic closure of a field K. A field extension K/k of transcendence dimension 1 is a function field in one variable over k if k is algebraically closed in K.

Denote by $\mathbf{F}(q) = k$ the finite field of q elements. Let K be a function field of one variable over $\mathbf{F}(q)$. Choose a separating transcendence base t for K/k. Denote by $\mathcal{O}_K$ the integral closure of $k[t]$ in K. If $K' = \mathbf{F}(q^l) \cdot K$, then $\mathcal{O}_{K'} = \mathbf{F}(q^l) \cdot \mathcal{O}_{K'}$. If $\mathfrak{p}'$ is a prime ideal of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$ of degree j and $j \mid l$, then the relative residue class degree is $[\mathcal{O}_{K'}/\mathfrak{p}' : \mathcal{O}_K/\mathfrak{p}] = l/j$. Hence, if $g(\mathfrak{p})$ denotes the number of prime ideals of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$, then $g(\mathfrak{p}) = j$.

Denote by $F(q)$ the *frobenius element of* $\mathfrak{G}(\widetilde{\mathbf{F}(q)}/\mathbf{F}(q))$ (i.e., $F(q)(x) = x^q$ for each $x \in \widetilde{\mathbf{F}(q)}$). Consider a finite Galois extension L of K of degree n and a conjugacy class $\mathfrak{C}$ in $\mathfrak{G}(L/K)$ with, say, c elements. Associate to $\mathfrak{C}$ the set

$$C = \left\{\mathfrak{p} \in P'(K) \,\middle|\, \left(\frac{L/K}{\mathfrak{p}}\right) = \mathfrak{C}\right\},$$

where $P'(K)$ is the set of all prime ideals of $\mathcal{O}_K$ unramified in $\mathcal{O}_L$, and

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

is the conjugacy class associated to a *Frobenius element*

$$\left[\frac{L/K}{\mathfrak{P}}\right]$$

for $\mathfrak{P}$ a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

Use the following notation:

$$\hat{k} = \text{the algebraic closure of } k \text{ in } L;$$

$$\hat{n} = [\hat{k} : k], \quad n^0 = n/\hat{n} = [L : \hat{k} \cdot K];$$

$$P_l(K) = \{\mathfrak{p} \in P(K) \mid \deg(\mathfrak{p}) = l\};$$

$$P_l'(K) = \{\mathfrak{p} \in P(K) \mid \mathfrak{p} \text{ is unramified in } L \text{ and } \deg(\mathfrak{p}) = l\};$$

$$C_l(K) = \left\{p \in P_l'(K) \,\middle|\, \left(\frac{L/K}{\mathfrak{p}}\right) = \mathfrak{C}\right\};$$

$$R(L/K) = \{\mathfrak{p} \in P(K) \mid \mathfrak{p} \text{ is ramified in } L\};$$

$$R_l(L/K) = \{\mathfrak{p} \in R(L/K) \mid \deg(\mathfrak{p}) = l\};$$

$$G = \mathfrak{G}(L/K).$$

Our first result counts the elements of $C_1(k)$, as did [**Fr**; Proposition 2]. But here a "field crossing argument" descendent from Tchebotarev's ideas ([**T**]—a similar argument appears in [**FrHJ**] applied to a different project) replaces the rationality of the Artin L-series. Thus the proof does not mimic Dirichlet's original argument. Indeed, in almost every way it is simpler than [**Fr**; Proposition 2] and it thereby simplifies the constant in the "O" notation.

THEOREM 1.1. *If an element τ (equivalently, every element) of $\mathfrak{C}$ satisfies*

$$(1) \qquad \operatorname{res}_{\hat{k}}(\tau) = \operatorname{res}_{\hat{k}}(F(q)),$$

then

$$|C_1(K)| = (c/n^0) \cdot q + O(\sqrt{q}).$$

The "O" notation indicates a function bounded by $A \cdot \sqrt{q}$ with A a computable function of $g(K)$ (the genus of K) and $|R_1(L/K)|$. Otherwise, it does not depend on q, on K or on L.

Proof. Let $\tau \in \mathfrak{C}$, $f = \mathrm{ord}(\tau)$ and $k' = \mathbf{F}(q^f)$. From (1) $\hat{n} \mid f$. Thus $K' = k' \cdot K$ is a finite Galois extension of K and for $L' = k' \cdot L$, $[L' : K'] = [L : \hat{k} \cdot K] = n^0$. Thus, we naturally identify $\mathfrak{G}(K'/K)$ with $\mathfrak{G}(k'/k)$ and thereby $\mathfrak{G}(L'/K)$ with

$$(2) \qquad \{(\sigma_1, \sigma_2) \in \mathfrak{G}(L/K) \times \mathfrak{G}(k'/k) \mid \mathrm{res}_{\hat{k}}(\sigma_1) = \mathrm{res}_{\hat{k}}(\sigma_2)\}$$

[**L**; p. 198].

In particular, consider the extension of τ to L' through the element $\tilde{\tau} = (\tau, \mathrm{res}_{k'}(F(q)))$. Then $\tilde{\tau}$ is also of order f.

Divide the rest of the proof into parts.

Part A. *Field crossing argument.* If $L^{(\tilde{\tau})}$ is the fixed field of $\tilde{\tau}$ in L' then $L^{(\tau)} = L^{(\tilde{\tau})} \cap L$ is of index f in L. The restriction of the frobenius element to $k' \cap L^{(\tilde{\tau})}$ is the identity, so $k' \cap L^{(\tilde{\tau})} = k$, $k' \cdot L^{(\tilde{\tau})} = L'$ and $L^{(\tilde{\tau})}$ is a function field of one variable over k. Let $d = [k' : \hat{k}] = [L' : L]$.

Consider $P_1^*(L^{(\tilde{\tau})}) = \{\mathfrak{q} \in P(L^{(\tilde{\tau})}) \mid \deg(\mathfrak{q}) = 1$ and $\mathfrak{q}$ is unramified over $K\}$. Define

$$C_\tau = \left\{\mathfrak{P} \in P'(L) \mid \deg(\mathcal{O}_K \cap \mathfrak{P}) = 1 \text{ and } \left[\frac{L/K}{\mathfrak{P}}\right] = \tau\right\}.$$

Then there is a map h: $P_1^*(L^{(\tilde{\tau})}) \to C_\tau$ as follows: For an element $\mathfrak{q} \in P_1^*(L^{(\tilde{\tau})})$ there exists a unique $\mathfrak{q}' \in P(L')$ lying over $\mathfrak{q}$. Then $\mathfrak{P} = h(\mathfrak{q}) = \mathfrak{q}' \cap \mathcal{O}_L$. Since

$$\left[\frac{L'/L^{(\tilde{\tau})}}{\mathfrak{q}'}\right]$$

is the frobenius acting on k', then it must be $\tilde{\tau}$ and its restriction to L is therefore τ. From the formula

$$(3) \qquad \left[\frac{L'/K}{\mathfrak{q}'}\right] = \left(\left[\frac{L/K}{\mathfrak{q}' \cap \mathcal{O}_L}\right], \left[\frac{K'/K}{\mathfrak{q}' \cap \mathcal{O}_{K'}}\right]\right),$$

$$\left[\frac{L/K}{\mathfrak{P}}\right] = \tau.$$

Also, if $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_{L^{(\tilde{\tau})}}/\mathfrak{q} = k$. So $\mathcal{O}_K/\mathfrak{p} = k$ and $\mathcal{P} \in C_\tau$.

Finally, we conclude that for $\mathcal{P} \in C_\tau$, $h^{-1}(\mathcal{P})$ contains exactly d elements. Since $\mathcal{O}_L/\mathcal{P} = k'$, for $\mathfrak{q}'$ a prime of $\mathcal{O}_{L'}$ over $\mathcal{P}$, $\mathcal{O}_{L'}/\mathfrak{q}' = k'$. So there are $[L' : L] = d$ primes $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_d \in P(L')$ above $\mathcal{P}$ and

$$\left[\frac{L'/K}{\mathfrak{q}'_i}\right] = \tilde{\tau}, \qquad i = 1, \ldots, d.$$

Thus, if $\mathfrak{q}'_i \cap \mathcal{O}_{L^{(\tilde{\tau})}} = \mathfrak{q}_i$, then $\mathcal{O}_{L^{(\tilde{\tau})}}/\mathfrak{q}_i = k$ and $\mathfrak{q}_i \in h^{-1}(\mathcal{P})$ with $\mathfrak{q}'_i$ the unique element of $P(L')$ that lies over $\mathfrak{q}_i$. Clearly, therefore, $\mathfrak{q}_1, \ldots, \mathfrak{q}_d$ are the distinct elements of $h^{-1}(\mathcal{P})$.

Part B. *Counting the cardinality of* C_τ. From the Riemann hypothesis for curves

(4) $$|P_1(L^{(\tilde{\tau})})| = q + O(\sqrt{q})$$

where $O(\sqrt{q})$ is bounded by $A \cdot \sqrt{q}$ with A equal to twice the genus of $L^{(\tilde{\tau})}$. Thus A is bounded by the maximum of 1 and $([L^{(\tilde{\tau})} : k(t)] - 1) \cdot ([L^{(\tilde{\tau})} : k(t)] - 2)$, for any nonconstant $t \in L$. In particular, A is bounded by $[L : \hat{k}(t)]^2$. From (4)

(5) $$|P_1^*(L^{(\tilde{\tau})})| = q + O(\sqrt{q}),$$

but here the O notation must be adjusted to include a function of $|R_1(L/K)|$ as stipulated in the statement of the theorem. Since there are d primes of $P_1^*(L^{(\tilde{\tau})})$ for each one of C_τ,

$$|C_\tau| = (1/d) \cdot q + O(\sqrt{q}).$$

Part C. *Conclusion of the proof*. From Part B

(6) $$\left|\bigcup_{\tau \in \mathfrak{C}} C_\tau\right| = (c/d) \cdot q + O(\sqrt{q}).$$

Over every element of $C_1(K)$ there lie exactly $g = [L^{(\tau)} : K]$ elements of $\bigcup C_\tau$. If we show that $g \cdot d = n^0$, then $|C_1(K)| = (c/n^0) \cdot q + O(\sqrt{q})$ and the theorem is done. But $g = n/f$ and $d = f/[k' : \hat{k}]$ and the result follows immediately. □

The next two lemmas consider the cardinality of $C_l(K)$ for l general, but L/K is cyclic. Again, let K be a function field in one variable over $\mathbf{F}(q) = k$.

LEMMA 1.2. *Let K' be a finite extension of K and let $\mathbf{F}(q^u)$ be the algebraic closure of k in K'. For a multiple v of u let*

$$P'_{v/u}(K'/K) = \{\mathfrak{p}' \in P_{v/u}(K') \mid \deg(\mathfrak{p}' \cap \mathcal{O}_K) \neq v\}.$$

Then, for any $\varepsilon > \frac{1}{2}$, $|P'_{v/u}(K'/K)| = O(q^{\varepsilon \cdot v})$. The constant in the O notation may be chosen independent of v.

Proof. If $\mathfrak{p}' \in P'_{v/u}(K'/K)$, then $\mathcal{O}_{K'}/\mathfrak{p}' = \mathbf{F}(q^v)$. Therefore, the residue field of $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{p}'$ is $\mathbf{F}(q^j)$, with j a proper divisor of v. So $j \leq v/2$. Over every such $\mathfrak{p}$ there lie at most $[K' : K]$ elements of $P(K')$. Thus, from the simple estimate $|P_j(K)| = O(q^j)$, conclude that

$$\begin{aligned} |P'_{v/u}(K'/K)| &\leq [K' : K] \sum_{j \leq v/2} |P_j(K)| \\ &= O\big((v/2) \cdot q^{v/2}\big) = O(q^{\varepsilon \cdot v}). \end{aligned}$$ □

Return to the notation of the proof of Theorem 1.1 where $\hat{k}$ is the algebraic closure of k in L.

LEMMA 1.3. *Assume that L/K is a cyclic extension and that the unique element τ of $\mathfrak{C}$ generates $\mathfrak{G}(L/K)$. Let v be a positive integer for which*

$$\text{(7)} \qquad \operatorname{res}_{\hat{k}}(\tau) = \operatorname{res}_{\hat{k}}(F(q^v)).$$

For any $\varepsilon > \frac{1}{2}$, $|C_v(K)| = (1/v \cdot n^0) \cdot q^v + O(q^{\varepsilon \cdot v})$ where the constant in the O notation may be chosen to be independent of v.

Proof. Let $k' = \mathbf{F}(q^v)$, $\hat{k}' = k' \cdot \hat{k}$ and $L' = k' \cdot L$. Then L' is a cyclic extension of K' and $\hat{k}'$ is the algebraic closure of k' in L'. Also, (7) implies that $\hat{k} \cap k' = k$. As in the proof of Theorem 1.1, identify $\mathfrak{G}(L'/K)$ with $\{(\sigma_1, \sigma_2) \in \mathfrak{G}(L/K) \times G(k'/k) \mid \operatorname{res}_{\hat{k}}(\sigma_1) = \operatorname{res}_{\hat{k}}(\sigma_2)\}$. Consider $\tau' = (\tau, \operatorname{res}_{k'}(F(q^v)))$. Since τ' fixes k', $\tau' \in \mathfrak{G}(L'/K')$. Define

$$C_{\tau'} = \left\{\mathfrak{p}' \in P(K') \text{ of degree 1 (over } k') \;\Big|\; \left(\frac{L'/K'}{\mathfrak{p}'}\right) = \tau'\right\}.$$

As $R_1(L'/K')$ consists of extensions of elements of $\bigcup_{j|v} R_j(L/K)$,

$$|R_1(L'/K')| \leq |R(L/K)| \cdot \max\{\deg(\mathfrak{p}) \mid \mathfrak{p} \in R(L/K)\}.$$

From Theorem 1.1 conclude

$$\text{(8)} \qquad |C_{\tau'}| = (1/n^0) \cdot q^v + O(q^{v/2}).$$

Define $C'_{\tau'} = \{\mathfrak{p}' \in C_{\tau'} \mid \deg(\mathcal{O}_K \cap \mathfrak{p}') = v\}$.

From (8) and Lemma 1.2, $|C'_{\tau'}| = (1/n_0) \cdot q^v + O(q^{\varepsilon \cdot v})$.

Compare $C_v(K)$ and $C'_{\tau'}$ by the argument of Part A of the proof of Theorem 1.1, especially expression (3): for every element $\mathfrak{p} \in C_v(K)$ there are exactly v primes $\mathfrak{p}'_1, \dots, \mathfrak{p}'_v$, of $\mathcal{O}_{K'}$ over $\mathfrak{p}$ with

$$\left(\frac{L'/K'}{\mathfrak{p}'_i}\right) = \tau'.$$

Thus $\mathfrak{p}'_i \in C'_{\tau'}$. Conversely, if $\mathfrak{p}' \in C'_{\tau'}$ then (3) shows $\mathcal{O}_K \cap \mathfrak{p}' \in C_v(K)$. The lemma follows easily. □

The proof of our main theorem reduces the computation of $|C_l(K)|$ in the general case to the case where L/K is cyclic. Among other places, **[D]** and **[M]** contain the idea for this.

THEOREM 1.4. *Let $\mathfrak{C}$ be a conjugacy class of cardinality c of $\mathfrak{G}(L/K)$ represented by an element τ. Let v be a positive integer for which*

$$\operatorname{res}_{\hat{k}}(\tau) = \operatorname{res}_{\hat{k}}(F(q^v)). \tag{9}$$

For any integer $l > 0$, $C_l(K)$ is empty if $l \not\equiv v \bmod \hat{n}$. Otherwise, if $\varepsilon > \frac{1}{2}$, then

$$|C_l(K)| = (c/l \cdot n_0) \cdot q^l + O(q^{\varepsilon \cdot l}) \tag{10}$$

where the constant in the O notation may be chosen independent of v.

Proof. If $C_l(K)$ contains a prime $\mathfrak{p}$ and if $\mathfrak{P} \in P(L)$ lies over $\mathfrak{p}$, then

$$\operatorname{res}_{\hat{k}}\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right) = \operatorname{res}_{\hat{k}}(F(q^l)).$$

But (9) implies

$$\operatorname{res}_{\hat{k}}\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right) = \operatorname{res}_{\hat{k}}(F(q^v)).$$

Clearly, $l \equiv v \bmod \hat{n}$. Now assume that $\hat{n} \mid l - v$.

Let $d = (v, \hat{n}) = (l, \hat{n})$. Then the algebraic closure of k in the fixed field $K' = L^{(\tau)}$ of τ is $\mathbf{F}(q^d)$. Define:

$$C'_{l/d}(K') = \left\{\mathfrak{p}' \in P(K') \mid \left(\frac{L/K'}{\mathfrak{p}'}\right) = \tau, \deg(\mathfrak{p}') = l/d,\right.$$
$$\left.\mathfrak{p}' \text{ is unramified over } K \text{ and } \deg(\mathcal{O}_K \cap \mathfrak{p}') = l\right\}.$$

From Lemmas 1.2 and 1.3, with $n' = [L : \hat{k} \cdot K']$,

$$(11) \qquad |C'_{l/d}(K')| = (d/l \cdot n') \cdot (q^d)^{l/d} + O(q^{d \cdot \varepsilon \cdot (l/d)})$$
$$= (d/l \cdot n') \cdot q^l + O(q^{\varepsilon \cdot l}).$$

Consider the map h: $C'_{l/d}(K') \to C_l(K)$ by $h(\mathfrak{p}') = \mathcal{O}_K \cap \mathfrak{p}'$. Since

$$\left(\frac{L/K'}{\mathfrak{p}'}\right) = \tau$$

there exists a unique element $\mathfrak{P} \in P(L)$ over $\mathfrak{p}'$ and it satisfies

$$\left[\frac{L/K'}{\mathfrak{P}}\right] = \tau.$$

By the definition of K',

$$\tau = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Thus $\mathfrak{p} \in C_l(K)$.

Conversely, suppose $\mathfrak{p} \in C_l(K)$ and $\mathfrak{P} \in P(L)$ lies over $\mathfrak{p}$ with

$$\left[\frac{L/K}{\mathfrak{P}}\right] = \tau.$$

Then for $\mathfrak{p}' = K' \cap \mathfrak{P}$,

$$\left[\frac{L/K'}{\mathfrak{p}'}\right] = \tau.$$

So $\mathfrak{p}' \in C'_{l/d}(K')$ and $h(\mathfrak{p}') = \mathfrak{p}$.

The order of $h^{-1}(\mathfrak{p})$ is therefore the number of $\mathfrak{P} \in P(L)$ that lie over $\mathfrak{p}$ and satisfy

$$\left[\frac{L/K}{\mathfrak{P}}\right] = \tau.$$

They are conjugate among each other by the centralizer, $C_G(\tau)$, of τ. Thus,

$$|h^{-1}(\mathfrak{p})| = |C_G(\tau)|/|D(\mathfrak{P})| = |G|/|D(\mathfrak{P})| \cdot |\mathfrak{C}| = [K' : K]/c$$

where $D(\mathfrak{P}) = \mathfrak{G}(L/K')$ is the decomposition group of $\mathfrak{P}$ in G. From (11),

$$|C_l(K)| = (d \cdot c/l \cdot n' \cdot [K' : K]) \cdot q^l + O(q^{\varepsilon \cdot l})$$
$$= (c/l \cdot n^0) \cdot q^l + O(q^{\varepsilon \cdot l}). \qquad \square$$

2. Application to Hilbert's irreducibility theorem. We review quickly (so as to display the improvements) the heart of the application of Theorem 1.1. to the explicit form of Hilbert's Irreducibility Theorem of [**Fr**; §3]. For simplicity start over $\mathbf{Q}$, but the idea works as well over any number field.

Consider $f(x, y) \in \mathbf{Z}[x, y]$, an irreducible polynomial that is monic in y.

Goal: Find an explicit arithmetic progression P in $\mathbf{Z}$ for which $f(x_0, y)$ is irreducible over $\mathbf{Q}$ for $x_0 \in P$. Here is how to find P.

Let Ω_f be the splitting field of f over $\mathbf{Q}(x)$. Identify $\Omega_f/\mathbf{Q}(x))$ with a (transitive) subgroup G of S_n, $n = \deg_y(f)$. Let I be any proper subset of $\{1, 2, \ldots, n\}$ and let $S_{n,I}$ be the subgroup of S_n consisting of elements that map I into itself. Let $G_I = G \cap S_{n,I}$ and let T_I be the transitive representation of G arising from the action of G on the right cosets of G_I. Choose $\tau_I \in G$ such that $T_I(\tau_I)$ fixes no integer. Finally, choose $\mathfrak{L} = \{\tau(1), \ldots, \tau(r)\} \subseteq G$ such that $\tau_I \in \mathfrak{L}$ for each I.

Let $p(i)$ be a prime of $\mathbf{Z}$ and $a(i) \in \mathbf{Z}$, $i = 1, \ldots, r$, with the following properties. Let L_i be the reduction modulo $p(i)$ of Ω_f and use the notation of §1 to define $\widehat{\mathbf{F}(p(i))}$ as the algebraic closure of $\mathbf{F}(p(i))$ in L_i. Then the decomposition group of some prime lying over $x - a(i) \bmod (p(i))$ in L_i contains $\tau(i)$ whose restriction to $\widehat{\mathbf{F}(p(i))}$ is $F(p(i))$, and $L_i^{(\widetilde{\tau(i)})}$ (as in Part A of the proof of Theorem 1.1) has an $\mathbf{F}(p(i))$-rational point lying over $x - a(i) \bmod (p(i))$. Let $g(L)$ be the genus of L.

THEOREM 2.1. *Let $P = \{a, a + \prod_{i=1}^r p(i), a + 2 \cdot \prod_{i=1}^r p(i), \ldots\}$ with $a \equiv a(i)\,(p(i))$, $i = 1, \ldots, r$. Then $f(x_0, y)$ is irreducible for $x_0 \in P$. The distinct primes $p(i)$, $i = 1, \ldots, r$ may be chosen subject only to the conditions*

(1) *restriction of $\tau(i)$ to $\widehat{\mathbf{F}(p(i))}$ generates $\mathfrak{G}(\widehat{\mathbf{F}(p(i))}/\mathbf{F}(p(i)))$; and*

(2) $p(i) > \sqrt{2 \cdot g\left(L_i^{(\tilde{\tau}(i))}\right)}$.

Proof. The proof of [**Fr**; Theorem 3] shows that it is sufficient to choose the p's and a's so that the decomposition group of a prime of L_i over $x - a(i) \bmod (p(i))$ contains $\tau(i)$. Note that this is so according to the proof of Theorem 1.1 if $L_i^{(\tilde{\tau}(i))}$ has an $\mathbf{F}(p(i))$-rational point lying over $x - a(i) \bmod (p(i))$; it is irrelevant whether $L_i/\mathbf{F}(p(i))(x)$ is ramified over $x - a(i) \bmod (p(i))$. Condition (2), according to the Riemann hypothesis for curves, guarantees the existence of an $a(i)$ corresponding to an allowable $p(i)$. □

REFERENCES

[D] M. Deuring, *Über den Tchebotareffschen Dichtigkeitsatz*, Math. Ann., **110** (1934), 415–415.

[Fr] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory, **6** (1974), 211–231.

[FrHJ] M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, Adv. Math., **50** (3) (1983), 1–35.

[FrS] M. Fried and G. Sacerdote, *Sovling diophantine problems over all residue class fields of a number field...*, Annals of Math. **104** (1976), 203–233.

[Fr,2] M. Fried, *On constructions arising from Neron's high rank curves*, TAMS, **281** (1983), 1–17.

[L] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading 1964.

[M] C. R. MacCluer, *A reduction in the Čebotarev density theorem to the cyclic case*, Acta Arith., **15** (1968), 45–47.

[T] N. Tchebotarev, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welch zu einer gegebenen Substitutionsklasse gehoren*, Math. Ann., **95** (1926), 191–228.

Received May 20, 1982. Supported by NSF Grant MCS 80-03253.

UNIVERSITY OF CALIFORNIA
IRVINE, CA 92717