Conspectus materiae tomi XLII, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-04518-3 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XLII (1983)

A Goldbach theorem for polynomials of low degree over odd finite fields*

by

GOVE EFFINGER (Lewiston, Maine)

1. Introduction. Let k_q be the finite field of q elements and let M be a monic polynomial of degree r in one variable x over k_q. We call M a 3-*primes polynomial* if there exist irreducible monic polynomials P_1, P_2, and P_3 with $\deg P_1 = r$, $\deg P_2 < r$, and $\deg P_3 < r$ such that $M = P_1 + P_2 + P_3$. In this paper we shall prove the following Goldbach-type theorem for such polynomials of low degree:

THEOREM 1.1. *Let k_q be the finite field of q elements where q is odd and let M be a monic polynomial in $k_q[x]$. If the degree of M is 2, 3, 4, 5, or 6, then M is a 3-primes polynomial. Further, if $\deg M = 7$ and if $q \geqslant 207$, then again M is a 3-primes polynomial.*

This result supplements a theorem of D. R. Hayes which requires the following definition: a monic polynomial M over k_q is called *even* if $q = 2$ and M is divisible by x or $x+1$. Otherwise M is called *odd*. This theorem then is as follows (see [5] or [11]):

THEOREM (D. R. Hayes). *For every degree $r \geqslant 5$, there exists a q_r (depending on r and decreasing as r increases) such that if $q \geqslant q_r$, then every odd monic M of degree r in $k_q[x]$ is a 3-primes polynomial.*

A close analysis of the proof of the Hayes Theorem (see [5], Chapter I) reveals that $q_5 \leqslant 6{,}340{,}567$ (i.e. we are guaranteed by the theorem that if $q \geqslant 6{,}340{,}567$, then every monic 5th degree polynomial over k_q is a 3-primes polynomial), $q_6 \leqslant 5{,}297$, and $q_7 \leqslant 479$. Moreover, we observe that the Hayes Theorem says nothing at all about polynomials of degree less than 5. Theorem 1.1, therefore, supplies us with much information about the existence of 3-primes polynomials not supplied by Hayes' asymptotic result.

We will see below that the cases $r = 2$ and 3 are essentially trivial, depending only upon elementary properties of the trace function, and that the cases $r = 4$ and 5 are easy when one utilizes information about

* This paper is derived from the author's Ph.D. thesis, written under D. R. Hayes at the University of Massachusetts.

orthogonal geometries over odd finite fields. However, the cases $r = 6$ and 7 are considerably more difficult to analyze. Here an asymptotic technique, first suggested by the work of S. D. Cohen [4], is employed, resulting finally in the information that if q is odd and $\geqslant 19$ (respectively 207), then every monic 6th (respectively 7th) degree polynomial in $k_q[x]$ is a 3-primes polynomial. Finally, we will merely "check" the few remaining cases ($q = 3$ through 17) for $r = 6$ on the computer. Theorem 1.1 will then be proved.

The asymptotic technique used in what follows to analyze the cases $r = 6$ and 7 actually applies to polynomials of arbitrary degree, but here, opposite to the Hayes Theorem, the "q_r's" *increase* as r increases. Thus for polynomials of degree $\geqslant 8$, we obtain less information than the Hayes Theorem obtains; for example, the Hayes Theorem q_8 is less than or equal to 137, whereas our technique yields information only for odd fields of order approximately 2,000 or greater. This explains then why our Theorem 1.1 "stops" at $r = 7$.

The long-range goal to which the Hayes Theorem and this work contribute is the following:

THE POLYNOMIAL 3-PRIMES CONJECTURE. *Every odd monic polynomial M of degree $\geqslant 2$ over every finite field is a 3-primes polynomial, except for the case q even, $M = x^2+a$ ($a \in k_q$).*

This result is the "best possible", for it is easy to show that over k_2, the even polynomial $M = x^{2r}+x^r$ (r even but otherwise arbitrary) is not a 3-primes polynomial, and over every k_q with q even, x^2+a ($a \in k_q$) is not a 3-primes polynomial (see [5], Chapter II). The reader is referred to [5], Chapter V, for a summary of what remains at this time to be proved to obtain the above stated conjecture.

2. A general approach to low degree polynomials and the cases $r = 2$ and 3. We state here once and for all that all polynomials considered in this paper are *monic*.

Our method for solving the 3-primes problem for polynomials of low degree will be as follows: suppose M has degree r. We will seek an irreducible P_1 of degree r such that $M-P_1$ is monic of as low degree as possible. Now find P_2 (irreducible) such that $(M-P_1)-P_2$ is monic and irreducible, hence is our necessary P_3. If $r = 3$, for example, it will suffice if P_1 can be found so that $M-P_1$ is quadratic (monic) and then if P_2 is found so that $(M-P_1)-P_2$ is linear (monic), for all linear polynomials are irreducible. When $r = 5$, we would like, for example, $M-P_1$ to be cubic and then $(M-P_1)-P_2$ linear, etc.

DEFINITION 2.1. If $P = x^r+\tau x^{r-1}+\alpha x^{r-2}+\beta x^{r-3}+\ldots$, then τ will be called the *first* or *trace coefficient* of P, α will be called the *second* coefficient, etc.

It is clear from above that if we know that there exist irreducibles

of degree 2 and 3 with arbitrary first coefficient, then we can solve the 3-primes problem for quadratic and cubic polynomials. Likewise, if there exists irreducibles of degree 3 through 5 with arbitrary first *and* second coefficients, we will be able to solve the problem for the cases $r = 4$ and 5. We shall do precisely this in this and the following section.

To solve the cases $r = 2$ and 3 we need only the following:

PROPOSITION 2.2. *Let $\tau \in k_q$ and $r \geqslant 2$. Then there exists an irreducible polynomial P of degree r whose first coefficient is τ except for the case q even, $r = 2$, $\tau = 0$.*

Proof. Case 1. Let $p = \mathrm{char}(k_q)$ and suppose $p \nmid r$. Pick any t_0 primitive in the extension k_{q^r} of k_q and let $t = t_0 - \dfrac{\tau+\mathrm{trace}(t_0)}{r}$. t be also primitive in k_{q^r} and

$$\mathrm{trace}(t) = \mathrm{trace}(t_0) - \mathrm{trace}\left(\frac{\tau+\mathrm{trace}(t_0)}{r}\right) = \mathrm{trace}(t_0) - \tau - \mathrm{trace}(t_0) = -\tau.$$

Let P_t be the minimal polynomial of t over k_q, then P_t has first coefficient τ.

Case 2. Suppose $p \mid r$. Since k_{q^r}/k_q is separable, the trace function is not identically zero. Select $t_0 \in k_{q^r}$ with $\mathrm{trace}(t_0) \neq 0$, then for any $\tau \in k_q$, $t = \left(\dfrac{-\tau}{\mathrm{trace}(t_0)}\right) t_0$ has $\mathrm{trace}(t) = -\tau$, so trace: $k_{q^r} \to k_q$ is onto. But trace is also an additive homomorphism, so for every $\tau \in k_q$, $\#\{t \in k_{q^r} \mid \mathrm{trace}(t) = -\tau\} = q^r/q = q^{r-1}$. If $r > 2$ then $r-1 > r/2$, but there are at most $q^{r/2}$ non-primitive elements in k_{q^r}, so there exists a primitive t with $\mathrm{trace}(t) = -\tau$. As above P_t is our desired irreducible. Finally, however, if $r = 2$ and $q = 2^e$ ($e \geqslant 1$), then kernel(trace) $= k_q$, so there are no primitive elements t with $\mathrm{trace}(t) = 0$. This completes the proof. ∎

We observe that the technique used in Case 2 above actually applies in general, but we chose to separate off the case $p \nmid r$ because it illustrates the important idea that under this hypothesis we can obtain all trace coefficients by "translation," and hence it will suffice to study polynomials with trace coefficient = 0.

PROPOSITION 2.3 ("Translation"). *Suppose that for $a \in k_q$, there are $n_0(a)$ irreducible polynomials of degree r with trace coefficient = 0 and 2nd coefficient = a, where r and q are relatively prime. Let $\tau \in k_q$, then the number $n_\tau(a)$ of irreducible r-th degree polynomials with trace coefficient = τ and 2nd coefficient = a is exactly $n_0\left(a - \binom{r}{2}\dfrac{\tau^2}{r^2}\right)$. Hence, for any τ, the set of numbers $\{n_\tau(a) \mid a \in k_q\}$ is just a permutation of the set of numbers $\{n_0(a) \mid a \in k_q\}$.*

Proof. Suppose that $t \in k_{q^r}$ has minimal polynomial of the form $x^r+ax^{r-2}+\ldots$, then $t-\tau/r$ is also primitive in k_{q^r} and has minimal poly-

nomial

$$\left(x+\frac{\tau}{r}\right)^r+a\left(x+\frac{\tau}{r}\right)^{r-2}+\dots$$
$$=\left(x^r+\tau x^{r-1}+\binom{r}{2}\frac{\tau^2}{r^2}x^{r-2}+\dots\right)+a(x^{r-2}+\dots)+\dots$$
$$=x^r+\tau x^{r-1}+\left(\binom{r}{2}\frac{\tau^2}{r^2}+a\right)x^{r-2}+\dots$$

Since this process is clearly reversible, we obtain the stated correspondence. ■

COROLLARY 2.4. *Assume* $(q,r)=1$. *If* n *distinct values in* k_q *appear as 2nd coefficients in irreducible polynomials of degree* r *over* k_q *with trace coefficient* $=0$, *then* n *distinct values will appear for every trace coefficient.*

Proof. Obvious from Proposition 2.3. ■

We will make considerable use of these results in the sections to follow.

Proposition 2.2 allows us to solve the 3-primes problem for quadratic and cubic polynomials over odd fields. Suppose that q is odd and $M=x^2+\tau x+a$. Proposition 2.2 guarantees us that there exists an irreducible $P_1=x^2+(\tau-2)x+a'$ for some a' in k_q. Let $P_2=x+a$ and $P_3=x-a'$, then $M=P_1+P_2+P_3$ as required. Now if $M=x^3+\tau x^2+ax+b$, then there exists $P_1=x^3+(\tau-1)x^2+a'x+b'$ and $P_2=x^2+(a-a'-1)x+b''$, so that $M-P_1-P_2=x+b-b'-b''=P_3$. Hence we have:

THEOREM 2.5. *If* q *is odd, then every quadratic and cubic polynomial over* k_q *is a 3-primes polynomial.* ■

Note: A slightly closer look shows us that if q is even but $M=x^2+\tau x+a$ has $\tau\neq 0$, then M is a 3-primes polynomial, and moreover *every* cubic M over *every* finite field is a 3-primes polynomial (see [5], Theorems 2.9 and 2.10). Since we are concerned here only with odd fields, the above suffices.

3. The distribution of irreducible polynomials with respect to their first two coefficients. As observed above, we will be able to solve the 3-primes problem in the cases $r=4$ and 5 provided that arbitrary combinations of the 1st *and* 2nd coefficients of irreducibles can be found. In this section we show that for odd q this is the case. The results obtained here will also be of essential use in the case $r=6$ and 7.

We make the assumption for the remainder of this paper that q is odd.

DEFINITION 3.1. Let t be a primitive element of k_{q^r} and let P_t be its minimal polynomial over k_q. We shall denote the 2nd coefficient of P_t by $A(t)$.

PROPOSITION 3.2.

$$A(t)=t^{1+q}+t^{1+q^2}+\dots+t^{q^{r-2}+q^{r-1}}=\sum_{\substack{0\leq i,j<r\\ i<j}}t^{q^i+q^j}.$$

Proof. Just multiply out $P_t(x)=(x-t)(x-t^q)\dots(x-t^{q^{r-1}})$. ■

Unlike the trace, $A(t)$ fails to be a linear functional of k_{q^r}. However, it does have the following nice property with respect to addition which will be important in what follows:

PROPOSITION 3.3. *Suppose* $t, s\in k_{q^r}$ *with* $\operatorname{trace}(t)=0$. *Then*

$$A(t+s)=A(t)+A(s)-\operatorname{trace}(ts).$$

Proof. Observe that since $q=p^e$, $p=\operatorname{char}(k_q)$, we have $(t+s)^{q^i}=t^{q^i}+s^{q^i}$. Now,

$$\begin{aligned}A(t+s)&=\sum_{\substack{0\leq i,j<r\\ i\neq j}}(t+s)^{q^i+q^j}\\
&=(t+s)(t+s)^q+(t+s)(t+s)^{q^2}+\dots+(t+s)^{q^{r-2}}(t+s)^{q^{r-1}}\\
&=(t+s)(t^q+s^q)+(t+s)(t^{q^2}+s^{q^2})+\dots+(t^{q^{r-2}}+s^{q^{r-2}})(t^{q^{r-1}}+s^{q^{r-1}})\\
&=(t^{1+q}+ts^q+t^qs+s^{1+q})+(t^{1+q^2}+ts^{q^2}+t^{q^2}s+s^{1+q^2})+\\
&\quad+\dots+(t^{q^{r-2}+q^{r-1}}+t^{q^{r-2}}s^{q^{r-2}}+t^{q^{r-1}}s^{q^{r-2}}+s^{q^{r-2}+q^{r-1}})\\
&=A(t)+A(s)+s(t^q+t^{q^2}+\dots+t^{q^{r-1}})+\\
&\quad+s^q(t+t^{q^2}+\dots+t^{q^{r-1}})+\dots+s^{q^{r-1}}(t+t^q+\dots+t^{q^{r-2}})\\
&=A(t)+A(s)-ts-t^qs^q-\dots-t^{q^{r-1}}s^{q^{r-1}}\qquad(\text{since trace}(t)=0)\\
&=A(t)+A(s)-\operatorname{trace}(ts).\ \blacksquare\end{aligned}$$

Note that this proposition requires that only one argument have trace $=0$. We also have

PROPOSITION 3.4. *If* $a\in k_q$, *then* $A(at)=a^2A(t)$.

Proof.

$$\begin{aligned}A(at)&=(at)^{1+q}+\dots+(at)^{q^{r-2}+q^{r-1}}\\
&=a^2t^{1+q}+\dots+a^2t^{q^{r-2}+q^{r-1}}\qquad(a=\text{all its conjugates})\\
&=a^2A(t).\ \blacksquare\end{aligned}$$

Together these give us the key result:

COROLLARY 3.5. *If* $t\in k_{q^r}$ *has* $\operatorname{trace}(t)=0$, *then*

$$A(t)=-\tfrac{1}{2}\operatorname{trace}(t^2).$$

Proof. $4A(t) = A(2t) = A(t+t) = A(t)+A(t)-\text{trace}(t^2)$, so

$$-\text{trace}(t^2) = 2A(t). \blacksquare$$

Note that the generality of Proposition 3.3 is not needed to obtain this corollary, but 3.3 will itself be used in the sequel. Also note that this result makes sense only when q is odd.

Corollary 3.5 allows us to view the 2nd coefficient of an irreducible polynomial in a way which immediately gives us considerable information about it. Let V be kernel(trace: $k_{q^r} \to k_q$), then V is an $(r-1)$-dimensional vector space over k_q. If $(q, r) = 1$, then $V \cap k_q = \{0\}$ since if $0 \neq a \in k_q$, then $\text{trace}(a) = ra \neq 0$. We define now a pairing $*$ of V into k_q given by $t * s = \text{trace}(ts)$, and one checks immediately that $*$ is in fact an inner product on V, and that V is *nonsingular* with respect to $*$ (see, e.g., [1], page 106). For if $0 \neq t \in V$ has $\text{trace}(ts) = 0$ for every $s \in V$, then $tV \subseteq V$ by definition of V, and then since $\sharp(tV) = \sharp V < \infty$, we must have $tV = V$, which implies that $1 \in V$, which it is not. Thus V is nonsingular. Hence we see that if $t \in V$ and is primitive in k_{q^r}, then the minimal polynomial P_t of t is of degree r with 1st coefficient $= 0$ and second coefficient $= A(t) = -\frac{1}{2}\text{trace}(t^2) = -\frac{1}{2}(t * t)$.

But now the theory of vector spaces over finite fields (of odd characteristic) equipped with an "orthogonal geometry", i.e., a symmetric inner product, with respect to which the vector space is nonsingular has been thoroughly studied, an excellent source being Emil Artin's *Geometric algebra* ([1]), pages 143–148. On these pages Artin gives exact formulas for the numbers of isotropic vectors (i.e., vectors of length $= 0$) and also the quadratic forms associated with the inner product. We summarize this latter information as follows:

Let V be a vector space of degree n over k_q where q is odd, and suppose V is equipped with a symmetric inner product $*$ with respect to which V is non-singular. Let g be any quadratic non-residue in k_q. Then using Artin's notation, for $n \geqslant 3$ we have 4 possible geometry types, the former two for n odd and the latter two for n even. These are:

Type	Associated quadratic form	Discriminant
I	$2x_1x_2+\ldots+2x_{n-2}x_{n-1}+x_n^2$	$(-1)^{(n-1)/2}$
II	$2x_1x_2+\ldots+2x_{n-2}x_{n-1}+gx_n^2$	$(-1)^{(n-1)/2}g$
III	$2x_1x_2+\ldots+2x_{n-1}x_n$	$(-1)^{n/2}$
IV	$2x_1x_2+\ldots+2x_{n-3}x_{n-2}+x_{n-1}^2-gx_n^2$	$(-1)^{n/2}g$

For any given value $a \in k_q$, the number of solutions of the equation quadratic form $= a$ gives the number of vectors t in V, the square of whose length is a (i.e. the number of t such that $t * t = a$).

LEMMA 3.6. *Let V be as above, $n \geqslant 3$, and $a \in k_q^*$. Then the $\sharp$ of elements t of V^* with $t * t = a$, is as follows:*

Type	$t * t = 0$	$t * t = a$, a quadratic residue	$t * t = a$, a non-quadratic residue
n odd I	$q^{n-1}-1$	$q^{n-1}+q^{(n-1)/2}$	$q^{n-1}-q^{(n-1)/2}$
n odd II		$q^{n-1}-q^{(n-1)/2}$	$q^{n-1}+q^{(n-1)/2}$
n even III	$(q^{n/2}-1)(q^{n/2-1}+1)$	$q^{n-1}-q^{n/2-1}$	
n even IV	$(q^{n/2}+1)(q^{n/2-1}-1)$	$q^{n-1}+q^{n/2-1}$	

Proof. We consider first the case where n is even, i.e. types III and IV. The case $t * t = 0$ is given directly by Artin [1], p. 146. Now since $\sharp V = q^n$ and since it is clear that the number of solutions of the type III and IV quadratic forms will be independent of the value of a (and of its quadratic character), we have

$$\sharp V = \sharp\{t \in V \mid t * t = 0\} + (q-1)\sharp\{t \in V \mid t * t = a\}.$$

Call this last number N. Hence for type III,

$$q^n = (q^{n/2}-1)(q^{n/2-1}+1)+1+(q-1)N,$$

which yields

$$\begin{aligned} N &= \frac{q^n-1}{q-1} - \frac{q^{n/2}-1}{q-1}(q^{n/2-1}+1) \\ &= (q^{n-1}+q^{n-2}+\ldots+1)-(q^{n-2}+q^{n-3}+\ldots+q^{n/2-1}+q^{n/2-1}+q^{n/2-2}+\ldots+1) \\ &= q^{n-1}-q^{n/2-1}. \end{aligned}$$

Likewise, for type IV,

$$\begin{aligned} N &= \frac{q^n-1}{q-1} - \frac{q^{n/2-1}-1}{q-1}(q^{n/2}+1) \\ &= (q^{n-1}+q^{n-2}+\ldots+1)-(q^{n-2}+\ldots+q^{n/2}+q^{n/2-2}+q^{n/2-3}+\ldots+1) \\ &= q^{n-1}+q^{n/2-1}, \end{aligned}$$

as claimed.

Now let n be odd. Again [1], p. 146, gives us q^{n-1} isotropic vectors for both types I and II. Observe now that in type I, we will get a different number of solutions depending on the quadratic nature of a. Suppose first that a is a quadratic non-residue, then regardless of the value of x_n, $2x_1x_2+\ldots+2x_{n-2}x_{n-1}$ must be non-zero. By the above argument for

type III, this can occur in $q^{n-2}-q^{(n-1)/2-1}$ ways, so the total number of solutions is

$$q(q^{n-2}-q^{(n-1)/2-1}) = q^{n-1}-q^{(n-1)/2}.$$

Now suppose a is a quadratic residue and let $N = \{t \in V \mid t*t = a\}$, then

$$q^n = q^{n-1} + \left(\frac{q-1}{2}\right)(q^{n-1}-q^{(n-1)/2}) + \left(\frac{q-1}{2}\right)N,$$

which yields

$$N = 2q^{n-1} - (q^{n-1}-q^{(n-1)/2}) = q^{n-1}+q^{(n-1)/2}.$$

Finally we observe that type II is analyzed exactly like type I, but with the role of quadratic residues and non-residues reversed. This completes the proof. ■

This lemma will now yield much information about the distribution of irreducible polynomials over k_q with respect to their first two coefficients. Using $r = 4$ and 5 as examples, we now demonstrate the kind of specific information which we can obtain.

COROLLARY 3.7. *Suppose that q is odd and not a power of 5. Then the number of 5th degree irreducible polynomials with trace $= 0$ and 2nd coefficient $= a$ over k_q is:*

	$a = 0$	each $a \neq 0$
$q \equiv 1$ or 4 (mod 5)	$\frac{(q^2-1)(q+1)}{5}$	$\frac{q^3-q}{5}$
$q \equiv 2$ or 3 (mod 5)	$\frac{(q^2+1)(q-1)}{5}$	$\frac{q^3+q}{5}$

Proof. Let $V = \text{kernel}(\text{trace}: k_{q^5} \to k_q)$. As discussed just after Corollary 3.5 above, since q is not a power of 5, V is a 4-dimensional vector space over k_q which is non-singular with respect to $t*s = \text{trace}(ts)$. We observe that since $V \cap k_q = 0$, every element of V^* is primitive in k_{q^5}, and each fifth degree irreducible polynomial over k_q with 1st coefficient $= 0$ corresponds to 5 (conjugate) elements of V. Now it is easy to see that if D_V and $D_{k_{q^5}}$ are the discriminants of V and k_{q^5} over k_q respectively, then $D_{k_{q^5}} = 5D_V$. Since $D_{k_{q^5}}$ is always a square in k_{q^5} (see, e.g., [3], p. 405) and lies in k_q, it must be a square in k_q also ($k_{q^5} \cap k_{q^2} = k_q$). Thus the quadratic character of D_V will match that of 5 in k_q, and by quadratic reciprocity we have then that D_V is a quadratic residue if and only if $q \equiv 1$ or 4 (mod 5). Hence we see that V is of type III if $q \equiv 1$ or 4 (mod 5), type IV otherwise.

The corollary now follows directly from Lemma 3.6 by setting $n = 4$ and using the above-mentioned 5 to 1 correspondence of elements of V^* with irreducible 5th degree polynomials with 1st coefficient $= 0$. ■

COROLLARY 3.8. *Let q be odd. Then the number of 4th degree irreducible polynomials with trace $= 0$ and 2nd coefficient $= a$ over k_q is:*

	$a = 0$	each a quadratic residue $\neq 0$	each a quadratic non-residue
$q \equiv 1$ (mod 8)	$\frac{q^2-1}{4}$	$(q^2-q)/4$	$(q^2+q-2)/4$
$q \equiv 5$ (mod 8)		$(q^2+q-2)/4$	$(q^2-q)/4$
$q \equiv 7$ (mod 8)		$(q^2-q-2)/4$	$(q^2+q)/4$
$q \equiv 3$ (mod 8)		$(q^2+q)/4$	$(q^2-q-2)/4$

Proof. Again let $V = \text{kernel}(\text{trace}: k_{q^4} \to k_q)$, so that V is 3-dimensional over k_q and non-singular with respect to *. The discriminant D_V satisfies $D_{k_{q^4}} = 4D_V$ so that the two discriminants match in their quadratic characters in k_q. If t is primitive in k_{q^4} and if $f(x)$ is its minimal polynomial, then $D_{k_{q^4}} = N(f'(t))$ where N is the norm function. One shows easily that if t has trace $= 0$ over k_{q^2}, then $N(f'(t))$ and $N(t)$ have the same quadratic character, and further that $N(t)$ is always a quadratic non-residue. Hence D_V is a quadratic non-residue in k_q.

Of the four cases of the corollary, we now go through one carefully and remark that the other three are very similar. Suppose $q \equiv 1$ (mod 8). Since

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2} \quad \text{and} \quad \left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8},$$

we see that in this case, both -1 and 2 are quadratic residues in k_q. Since D_V is a quadratic non-residue, we see that V must be of type II. Suppose $a\ (= A(t)$ for some $t \in k_{q^4}$; see Definition 3.1) is a zero non-quadratic residue, then since $A(t) = -\frac{1}{2}\text{trace}(t^2) = -\frac{1}{2}(t*t)$, we see that a and $a = t*t$ have the same quadratic character. Now by Lemma 3.6, there must be q^2-q elements t of V with $t*t = a$. Likewise if a is a quadratic non-residue, then so is a, and we get q^2+q elements t with $t*t = a$.

Now unlike the cases of 5th degree irreducibles, here it is not true that all elements of V^* are primitive in k_{q^4}. Let $0 \neq t \in k_{q^2} \cap V$, then $\text{trace}_{k_{q^2}/k_q}(t) = 0$ and so $t = -t^q$. Using this fact and Proposition 3.2, we obtain $A(t) = -2t^2$. Were $A(t)$ a non-zero quadratic residue in k_q, then so would t^2 be (we are assuming that -2 is), whence $t \in k_q$, which it is not since $t = -t^q$. Hence the equation $A(t) = -2t^2$ has no solutions if $A(t)$ is a non-zero quadratic residue, 2 solutions if it is a non-residue,

and 1 solution ($t = 0$) if $A(t) = 0$. Finally dividing by 4 (4 to 1 correspondence of primitive elements of V to trace 0 irreducibles), we obtain the desired count in this case.

The other 3 cases follow similarly. ■

We must now study the case where r is divisible by the characteristic of k_q. Here the translation technique (Proposition 2.3) does not apply and so it does not suffice to study polynomials with trace $= 0$. Thus we look at two cases: when the trace τ is nonzero, and when $\tau = 0$.

A. The case $\tau \neq 0$. Fix a value $\tau \neq 0$ in k_q and fix a $t_0 \in k_{q^r}$ such that $\operatorname{trace}(t_0) = \tau$. Let V be the orthogonal complement of $\langle t_0 \rangle$, i.e., $V = \{t \in k_{q^r} \mid \operatorname{trace}(t_0 t) = 0\}$, then V is of dimension $r-1$ over k_q. Let $W = \operatorname{kernel}(\operatorname{trace}|_V)$, i.e., $W = \{s \in V \mid \operatorname{trace}(s) = 0\}$, then W has dimension $r-2$ over k_q and W is a nonsingular orthogonal space (exactly as in the discussion following Corollary 3.5). Observe now that $W \cap k_q = \{0\}$, for if $a \in k_q^*$, then $\operatorname{trace}(at_0) = a \operatorname{trace}(t_0) = a\tau \neq 0$. Hence kernel (trace) $= W \oplus k_q$, and every element with trace $= \tau$ has unique representation $t_0 + s + \sigma$ where $s \in W$ and $\sigma \in k_q$. But by Proposition 3.3, since both s and σ have trace $= 0$, we have

$$A(t_0+s+\sigma) = A(t_0)+A(s)+A(\sigma)-\operatorname{trace}(t_0 s)-\operatorname{trace}(\sigma t_0)-\operatorname{trace}(\sigma s)$$
$$= A(t_0)+A(s)+0-0-\sigma\tau-0 = A(t_0)+A(s)-\sigma\tau.$$

Fix $s \in W$ for the moment and let σ run through k_q, so that $\sigma\tau$ also runs through k_q, and thus $A(t_0+s+\sigma)$ runs through k_q, i.e., each value appears exactly once. Hence as s runs through W, each value appears exactly q^{r-2} times.

B. The case $\tau = 0$. This situation is a bit more complicated. Let $V = \operatorname{kernel}(\operatorname{trace}: k_{q^r} \to k_q)$, then V is now a singular $(r-1)$-dimensional vector space over k_q which contains k_q itself. Let W be any complement of k_q in V. Then automatically k_q and W are orthogonal since $\operatorname{trace}(k_q V) = 0$. W is an $(r-2)$-dimensional space over k_q and is *nonsingular*, for as before if $0 \neq t \in W$ satisfies $\operatorname{trace}(tW) = 0$, then $tW = W$, so that $1 \in W$, which it is not. Now the elements of V which correspond to irreducible rth degree polynomials are exactly $S = \{\sigma + s \in k_q \oplus W \mid s \neq 0\}$. Moreover, since $A(\sigma+s) = A(\sigma)+A(s)-\operatorname{trace}(\sigma s) = A(s)$, we have $\#\{\sigma+s \in S \mid A(\sigma+s) = a\} = q\big(\#\{s \in W \mid s \neq 0 \text{ and } A(s) = a\}\big)$. We have proved:

LEMMA 3.9. *Suppose $(q, r) \neq 1$ and $r \geqslant 3$. The number of elements of k_{q^r} with* trace $= \tau$ *and A-value $= a$ is q^{r-2} if $\tau \neq 0$, and is $q\big(\#\{t \in W^* \mid A(t) = a\}\big)$ where W is any complement of k_q in $V = \operatorname{kernel}(\operatorname{trace})$ if $\tau = 0$.* ■

For an application of this result, we have:

COROLLARY 3.10. *If $q = 5^e$ for some $e \geqslant 1$, then the number of 5th degree irreducibles over k_q having trace coefficient $= \tau$ and 2nd coefficient $= a$ is $q^3/5$ if $\tau \neq 0$, $q(q^2-1)/5$ if $\tau = a = 0$, and either $q(q^2+q)/5$ or $q(q^2-q)/5$ if $\tau = 0$, $a \neq 0$, depending on the quadratic nature of a in k_q.*

Proof. This follows directly from Lemma 3.9 with $r = 5$ and Lemma 3.6 with $n = 3$. ■

In order to solve the 3-primes problem for the case $r = 4$ through 7, we will use the following corollary of the orthogonal geometric information obtained so far, together with the "Translation Lemma" (Proposition 2.3).

COROLLARY 3.11. *Let q be odd and let τ and a be arbitrary elements of k_q. Then the minimum number of irreducible polynomials of degree r with trace coefficient $= \tau$ and 2nd coefficient $= a$ is as follows:*

Degree r	Minimum # of irreducibles $x^r + \tau x^{r-1} + a x^{r-2} + \ldots >$
4	$(q^2-q-2)/4$
5	$(q^3-q^2)/5$
6	$(q^4-q^2-2q-2)/6$ *if* $p \neq 3$, $(q^4-q^3-q^2-q)/6$ *if* $p = 3$
7	$(q^5-q^3)/7$

Proof. (1) $r = 4$: Corollary 3.8 together with Proposition 2.3 ("Translation") immediately yield the result.

(2) $r = 5$: Corollary 3.7 with Proposition 2.3 and Corollary 3.10 yield the result.

(3) $r = 6$: First suppose that $p = \operatorname{char}(k_q) \neq 3$, so that Lemma 3.6 and Proposition 2.3 will apply. Setting $n = 5$ in Lemma 3.6 (recall that $\dim V = n = r-1$), we see immediately that the minimal count for elements of V with any given "length" is q^4-q^2. As with 4th degree polynomials, we must now remove non-primitive elements of V. If $t \in k_{q^2}$ with $\operatorname{trace}(t) = 0$, then using Proposition 3.2 and the fact that $t = -t^q$, we obtain $A(t) = -3t^2$ which clearly has at most two roots. If $t \in k_{q^3}$ with $\operatorname{trace}(t) = 0$, then using $t^{q^2} = -t-t^q$ and some sweat, we obtain $A(t) = -2(t^{2q}+t^{1+q}+t^2)$, which has at most $2q$ solutions for any fixed value of $A(t)$. We conclude that the number of primitive elements of V with given A-value is at least q^4-q^2-2q-2, and the result follows.

Now suppose that $p = 3$. Lemma 3.9 now applies with W having dimension 4 over k_q, so by Lemma 3.6 with $n = 4$ we obtain a minimum count of $q\big((q^2+1)(q-1)\big) = q^4-q^3+q^2-q$. Again we must eliminate non-primitive elements, and we use a rough (but sufficient for our purposes) method: we simply eliminate all q^2 elements of k_{q^2} and the at most q^2 elements of k_{q^3} with the prescribed trace value, so that our new lower bound becomes $q^4-q^3-q^2-q$. The desired result follows.

(4) $r = 7$: Here, as with $r = 5$, there is no difficulty with non-primitive elements, and the result follows directly by applying Lemma 3.6

(with $n = 6$), Proposition 2.3, and Lemma 3.9 (with $\dim W = 5$). In fact the minimum value occurs in the case $p = 7$, $\tau = 0$, $\alpha \neq 0$.

This completes the proof. ■

We conclude this section by looking at irreducible cubic polynomials as we will need information about them in the following section. First suppose that $p \neq 3$, then it suffices to use the techniques of Lemma 3.6. However, V now has dimension 2 over k_q, and by [1], p. 143, we have that $A(t)$ maps onto k_q^*, but if $q \equiv 2 \pmod 3$ then the value 0 is not taken on. Upon translation we then obtain:

LEMMA 3.12. *If $p \neq 3$ and $l \in k_q$ is given, then there exist irreducible polynomials of the form x^3+lx^2+hx+j for at least $q-1$ values of h.* ■

Suppose now that $p = 3$, then Lemma 3.9 applies with W of dimension 1. By [1], p. 143, $A(t)$ takes on exactly $(q-1)/2$ values, so if $\tau = 0$, $A(t)$ is far from onto. However, if $\tau \neq 0$, $A(t)$ is onto, in fact each value gets taken on exactly q times. Thus:

LEMMA 3.13. *If $p = 3$ and if $l \neq 0$ and h are given, then there exists an irreducible polynomial of the form x^3+lx^2+hx+j.* ■

4. A solution of the 3-primes problem for $r = 4$ and 5. We continue to assume that q is odd. The following theorem is an immediate corollary of the preceding section.

THEOREM 4.1. *Every 4th degree polynomial over every finite field of odd characteristic is a 3-primes polynomial.*

Proof. Let $M = x^4+\tau x^3+\alpha x^2+\beta x+\gamma$ be arbitrary in $k_q[x]$. By Corollary 3.11 there exists an irreducible $P_1 = x^4+\tau x^3+(\alpha-1)x^2+\beta' x+\gamma'$, so that $M-P_1 = x^2+(\beta-\beta')x+(\gamma-\gamma')$. By Proposition 2.2, there exists an irreducible $P_2 = x^2+(\beta-\beta'-1)x+\gamma''$. Let $P_3 = x+(\gamma-\gamma'-\gamma'')$, and we are done. ■

The case $r = 5$ is a bit more involved. Here it is necessary to separate off the two cases $p \neq 3$ and $p = 3$. The following will be used for the case $p \neq 3$:

LEMMA 4.2. *Let τ and α be prescribed elements of k_q where $q > 5$, then there exists $\beta \in k_q$ such that*

$$x^5+\tau x^4+\alpha x^3+\beta x^2+\gamma_1 x+\delta_1$$

and

$$x^5+\tau x^4+\alpha x^3+\beta x^2+\gamma_2 x+\delta_2$$

are both irreducible for some γ_1, γ_2, δ_1, $\delta_2 \in k_q$ and $\gamma_1 \neq \gamma_2$.

Proof. Suppose not, then each β which appears in an irreducible with first two coefficients τ and α respectively would be matched with a single γ. But then there would exist at most $q(q-1)$ such polynomials

($\delta_i \neq 0$). Corollary 3.11 guarantees us at least $q^2(q-1)/5$ such polynomials. Since $q > 5$, this is a contradiction. ■

For the case $p = 3$, we will need:

LEMMA 4.3. *Let τ and α be prescribed elements of k_q where $q > 5$, then there exist $\beta_1 \neq \beta_2$ such that $x^5+\tau x^4+\alpha x^3+\beta_1 x^2+\gamma_1 x+\delta_1$ and $x^5+\tau x^4+\alpha x^3+\beta_2 x^2+\gamma_2 x+\delta_2$ are both irreducible for some γ_1, γ_2, δ_1, $\delta_2 \in k_q$.*

Proof. If not, then a single β would appear as a third coefficient, so there would again be at most $q(q-1)$ such polynomials, again contradicting Corollary 3.11 since $q > 5$. ■

We are now in a position to solve the 3-primes problem for all 5th degree polynomials over fields of odd characteristic. Let $M = x^5+\tau x^4+\alpha x^3+\beta x^2+\gamma x+\delta$.

Case 1. Suppose $p \neq 3$, $q \neq 5$, q odd. By Lemma 4.2 there exists a β' which is matched with at least two distinct γ_1' and γ_2' in an irreducible 5th degree polynomial. By Lemma 3.12 there exists an irreducible cubic either of the form $x^3+(\beta-\beta')x^2+(\gamma-\gamma_1'-1)x+\delta_1''$ or $x^3+(\beta-\beta')x^2+(\gamma-\gamma_2'-1)x+\delta_2''$, and we assume the former. Let $P_1 = x^5+\tau x^4+(\alpha-1)x^3+\beta' x^2+\gamma_1' x+\delta'$ (for some δ'), $P_2 = x^3+(\beta-\beta')x^2+(\gamma-\gamma_1'-1)x+\delta_1''$, and $P_3 = x+(\delta-\delta'-\delta_1'')$, then $M = P_1+P_2+P_3$ as required.

Case 2. Suppose $p = 3$, $q \geqslant 9$. By Lemma 4.3 there exists a β' with $\beta-\beta' \neq 0$ so that $P_1 = x^5+\tau x^4+(\alpha-1)x^3+\beta' x^2+\gamma' x+\delta'$ is irreducible for some γ' and δ'. By Lemma 3.13 there exists an irreducible cubic of the form $P_2 = x^3+(\beta-\beta')x^2+(\gamma-\gamma'-1)x+\delta''$ for some δ''. Letting $P_3 = x+(\delta-\delta'-\delta'')$, we again have $M = P_1+P_2+P_3$.

Case 3. Suppose $q = 5$. A listing by the computer of irreducible 5th degree polynomials over k_5 shows that there exist more than $q^2(q-1)/5 = 20$ irreducibles for each pair of first two coefficients except $\tau = 0$, $\alpha = 1$ and $\tau = 0$, $\alpha = 4$, where there are exactly 20 of each. However, x^5+x^3+2x+2, x^5+x^3+3x+2, x^5+4x^3+2x+1, and x^5+4x^3+3x+1 are all irreducible, so the conclusion of Lemma 4.2 still holds, and the above proof (Case 1) still goes through.

Case 4. Suppose $q = 3$. Here we must take a slightly different task. It suffices (by translation) to study polynomials with trace $= 0$. A computer check of the 16 $(= (q^4-1)/5)$ irreducibles of this type reveals that we have all possible combinations of the first *three* coefficients except none of the form $x^5+2x^3+\alpha x+b$. Let $f(x) = x^5+2x^3+x^2+\gamma x+\delta$. For all M polynomials of degree 5 except for f, subtracting an appropriate P_1 (of degree 5) from M will result in a (monic) quadratic polynomial, and this can now be written as the sum of *two* irreducibles (by Prop. 2.2). Hence we have left to analyze $f(x)$. But $x^5+2x^3+x^2+1$, $x^5+2x^3+x^2+x+2$, and $x^5+2x^3+x^2+2x+2$ are all irreducible, so letting $P_1 = x^5+2x^3+x^2+$

$+(\gamma-2)x+\delta'$ chosen from these three, then $f-P_1 = 2x+(\delta-\delta')$, and now let $P_2 = x+(\delta-\delta')$ and $P_3 = x$.

We have finally proved:

THEOREM 4.4. *Every 5th degree polynomial over every finite field of odd characteristic is a 3-primes polynomial.* ■

5. An asymptotic result on the first $n-1$ coefficients of irreducible polynomials. The technique developed in Section 3 above will not, by itself, solve the 3-primes problem for polynomials of degree $r = 6$ or higher, simply because for such r, $r-2-2 > 1$, so we have no assurance that the $M-P_1-P_2$ is irreducible. In this section we change tactics radically and prove an asymptotic result which will then give us information about the existence of 6th and 7th degree 3-prime polynomials not provided by the Hayes Theorem (see Section 1).

We continue to assume that q is odd.

The central theorem of this section is the following:

THEOREM 5.1. *Let $f(x)$ be a polynomial of degree n in $k_q[x]$ where $(n, q) = 1$ such that $f'(x)$ has $n-1$ distinct roots all giving rise to distinct values of $f(x)$. Then for sufficiently large q, there exists an $\omega \in k_q$ such that $f(x)-\omega$ is irreducible.*

This theorem tells us quite simply that given a polynomial f whose derivative is "well-behaved", then if q is large enough (depending on the degree of f), we can make f irreducible by altering its constant term. The general procedure for using this theorem to solve the 3-primes problem (for large enough q) will be as follows:

Starting with an arbitrary rth degree polynomial M, obtain P_1 irreducible of degree r so that $(M-x)-P_1 = f(x)$ has degree $r-2$ and satisfies the hypotheses of Theorem 5.1. Then if ω is as guaranteed by the theorem, we have

$$M = P_1+\big(f(x)-\omega\big)+(x+\omega),$$

i.e., we have successfully written M as the sum of 3 irreducibles, one of degree r, one of degree $r-2$, and one linear.

Of course this technique works for arbitrary r, but it is asymptotic in q, and it turns out that only for $r = 6$ and $r = 7$ does the technique improve on the Hayes Theorem (of course, the cases $2 \leqslant r \leqslant 5$ are already solved).

The proof of Theorem 5.1 involves considerable machinery from algebraic and analytic number theory and depends centrally on the generalized Riemann Hypothesis for function fields as proved by A. Weil. We now state the theorem in a more directly provable form.

In all that follows we assume that $f(x)$ is an nth degree polynomial in $k_q[x]$ where q *is odd* and that $f(x)$ satisfies the hypotheses of Theorem 5.1, i.e., its derivative $f'(x)$ has $n-1$ distinct roots all of which give rise to distinct values of $f(x)$. We let t be an indeterminate and let E = splitting field of $f(x)-t$ over $k_q(t)$, the rational function field in t. If $\omega \in k_q$ and if $t-\omega$, which of course is a prime in $k_q[t]$, is unramified in E, then

$$\left[\frac{E/k_q(t)}{t-\omega}\right]$$

is the *Artin symbol* for $t-\omega$, i.e., is the conjugacy class of elements of $\mathrm{Gal}\big(E/k_q(t)\big)$ which are the Frobenius automorphisms of primes $\mathfrak{p}$ lying over $t-\omega$ (see, e.g., [15], p. 91).

We now state the equivalent:

THEOREM 5.2. *Let $f(x)$ be an n-th-degree polynomial in $k_q[x]$ which satisfies the hypotheses of Theorem 5.1 and let t and E be as above. Then $\mathrm{Gal}\big(E/k_q(t)\big) = S_n$ (the symmetric group) and for sufficiently large q, there exists an $\omega \in k_q$ such that $\left[\frac{E/k_q(t)}{t-\omega}\right]$ is the class of n-cycles, and $t-\omega$ is unramified in E.*

Theorem 5.2 implies Theorem 5.1. Suppose that Theorem 5.2 is true and that $\omega \in k_q$ is as guaranteed by that theorem. Let $\mathfrak{p}$ be a prime in E which lies over $t-\omega \in k_q[t]$. Since $\sigma_{\mathfrak{p}} \in \left[\frac{E/k_q(t)}{t-\omega}\right]$ is an n-cycle, the decomposition group $D_{\mathfrak{p}}$ is cyclic of order n ($t-\omega$ is unramified), but $D_{\mathfrak{p}} \simeq \mathrm{Gal}\big(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ over $(k_q[t])/t-\omega\big)$ (see, e.g., [15], p. 89; by $\mathcal{O}_{\mathfrak{p}}$ we mean the local ring of $\mathfrak{p}$-integers in E), i.e., the residual degree of $\mathfrak{p}$ over $t-\omega$ is n. But now let x_1 be a root of $f(x)-t$ in E and view x_1 as lying in the completion $E_{\mathfrak{p}}$ and $f(x)-t$ as being a polynomial over the completion $k_q(t)_{t-\omega}$. Here x_1 is integral, i.e., $x_1 \in \mathcal{O}_{\mathfrak{p}}$, and in fact $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} \simeq k_q(\bar{x}_1)$ where $\bar{x}_1$ is the image of x_1 under $\mathcal{O}_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. Since $k_q(t)/(t-\omega) \simeq k_q$, we have then that $\deg\big(k_q(\bar{x}_1)/k_q\big) = n$. But $\bar{x}_1$ is a root of $\overline{f(x)-t} = f(x)-\omega$ and is primitive in $k_q n$, so $f(x)-\omega$ must be irreducible. ■

We will prove Theorem 5.2 by producing for fixed n an asymptotic formula ($q \to \infty$) for the number N_n of unramified linear primes $t-\omega \in k_q(t)$ such that $\left[\frac{E/k_q(t)}{t-\omega}\right]$ is the class of n-cycles. This formula will be of the form

$$N_n = \frac{q+1}{n} + O\big(\sqrt{q}\big)$$

where the constant in the error term depends only on n. We should state here that we are much indebted to the work of S. D. Cohen, for in a 1970 paper [4] he proves a result (Theorem 1, p. 256) of which our Theorem 5.2 is an easy corollary. However, his proof technique does not yield the

actual error term constant easily and hence is not ideal for our purposes. Recall that our goal here is not only a proof of Theorem 5.2 but also the specific calculation of the error term. To get the desired result we use the theory of Artin non-abelian L-functions and the work of A. Weil.

We follow here the definition of the Artin L-functions as developed by Martinet in [6], pp. 1–11, but specialize the notation slightly to fit only the cases which we need.

Let ϱ be an irreducible, non-trivial complex representation of S_n and let χ be the associated character, i.e., $\forall \tau \in S_n$, $\chi(\tau) = \operatorname{trace} \varrho(\tau)$. Observe that χ is a class function on S_n since $\chi(\tau_1\tau_2) = \chi(\tau_2\tau_1)$. Let P be any finite prime in $k_q(t)$ and let $\mathfrak{p}$ be any prime over P in E, the splitting field of $f(x)-t$ over $k_q(t)$ as in the previous section. If P is unramified in E then we let $\sigma_\mathfrak{p}$ be the Frobenius automorphism, i.e., a generator of the decomposition group $D_\mathfrak{p}$. More generally, whether or not P is ramified, we may define $\sigma_\mathfrak{p} \in D_\mathfrak{p}/I_\mathfrak{p}$ where $I_\mathfrak{p}$ is the inertial group of $\mathfrak{p}$. If $\varrho\colon S_n \to \mathrm{GL}(V)$, then we define

$$V^{I_\mathfrak{p}} = \{x \in V \mid \varrho(\tau)(x) = x,\ \forall \tau \in I_\mathfrak{p}\},$$

i.e., $V^{I_\mathfrak{p}}$ is that part of V left fixed by all elements of $I_\mathfrak{p}$. Observe that on $V^{I_\mathfrak{p}}$, $\varrho(\sigma_\mathfrak{p})$ is well-defined. Moreover, if $c \in \boldsymbol{C}$, then $\det_{V^{I_\mathfrak{p}}}(1-c\varrho(\sigma_\mathfrak{p}))$ does not depend on the particular prime $\mathfrak{p}$ over P which is picked, for the conjugate transformations $\varrho(\sigma_{\mathfrak{p}_1})$ on $V^{I_{\mathfrak{p}_1}}$ and $\varrho(\sigma_{\mathfrak{p}_2})$ on $V^{I_{\mathfrak{p}_2}}$ have the same minimal polynomial and hence eigenvalues, so that $1-c\varrho(\sigma_{\mathfrak{p}_1})$ and $1-c\varrho(\sigma_{\mathfrak{p}_2})$ also have the same eigenvalues.

We are now in a position to make the

DEFINITION. The *Artin non-abelian L-function associated with* χ is

$$L(s,\chi) = \prod_{\substack{P \text{ all} \\ \text{primes in } k_q(t)}} \left(\det_{V^{I_\mathfrak{p}}}\left(1-(q^{\deg P})^{-s}\varrho(\sigma_\mathfrak{p})\right)\right)^{-1}$$

where $\mathfrak{p}$ is any prime of E lying over P and s is a complex number satisfying $\operatorname{Re}(s) > 1$.

FACT. This series is convergent for $\operatorname{Re}(s) > 1$ (see [6]). For convenience we substitute $u = q^{-s}$, so that we may write

$$L(u,\chi) = \prod_P \left(\det_{V^{I_\mathfrak{p}}}\left(1-\varrho(\sigma_\mathfrak{p})u^{\deg P}\right)\right)^{-1}.$$

The central fact that we will need in the sequel is the following.

THEOREM (Generalized Riemann Hypothesis for Function Fields — A. Weil). *$L(u,\chi)$ is a polynomial in u of degree $(2g-2)n_\varrho + \deg \mathfrak{f}\chi$ where g is the genus of the base field $k_q(t)$, n_ϱ is the degree of the non-trivial representation ϱ, and $\mathfrak{f}\chi$ is the conductor of the character χ. Moreover, all the roots of $L(u,\chi)$ have absolute value $q^{-1/2}$.*

Proof. See [18], p. 79. ∎

We observe that since the genus g of the rational function field $k_q(t)$ is 0, we obtain in our case that $L(u,\chi)$ is a polynomial of degree $= \deg \mathfrak{f}\chi - 2n_\varrho$.

DEFINITION 5.3. For P an unramified prime in $k_q(t)$, let $\chi(\sigma_P) = \chi(\sigma_\mathfrak{p}) = \operatorname{trace}(\varrho(\sigma_\mathfrak{p}))$ for any $\mathfrak{p} \mid P$, where $\sigma_\mathfrak{p}$ is a generator of $D_\mathfrak{p}$. As remarked earlier, $\chi(\sigma_P)$ is well-defined since χ is a class function. More generally, if m is a positive integer, then by $\chi(\sigma_P^m)$ we simply mean $\operatorname{trace}\varrho(\sigma_\mathfrak{p}^m)$.

DEFINITION 5.4. Let P be a ramified prime in $k_q(t)$ and let $\mathfrak{p}$ in E divide P, then we define

$$\chi(\sigma_P^m) = \frac{1}{\sharp I_\mathfrak{p}} \sum_{\substack{\tau \mapsto \sigma_\mathfrak{p}^m \\ \text{under} \\ D_\mathfrak{p} \to D_\mathfrak{p}/I_\mathfrak{p}}} \chi(\tau);$$

that is, for ramified primes we define $\chi(\sigma_P^m)$ as an average over preimages of $\sigma_\mathfrak{p}^m$.

We are now in a position to use the ultra-important theorem of Weil to obtain an upper bound for $\left|\sum_{\deg P=1} \chi(\sigma_P)\right|$ where χ is the character associated with any non-trivial irreducible representation ϱ of S_n. In order to make the connection between the above definition for ramified primes and the calculation below, we need the following:

LEMMA 5.5. *Let P be ramified. If $\chi(\sigma_P^m)$ is as in Definition 5.4, then*

$$\chi(\sigma_P^m) = \operatorname{trace}_{V^{I_\mathfrak{p}}} \varrho(\sigma_\mathfrak{p}^m) \qquad (\mathfrak{p} \mid P).$$

Proof. Let $\mathfrak{p}$ be any prime over P and let $\tau \in D_\mathfrak{p}$ be a preimage of $\sigma_\mathfrak{p}^m$ under $D_\mathfrak{p} \to D_\mathfrak{p}/I_\mathfrak{p}$. If $\iota \in I_\mathfrak{p}$ and $v \in V^{I_\mathfrak{p}}$, then

$$\varrho(\iota)\left(\varrho(\tau)(v)\right) = \varrho(\iota\tau)(v) = \varrho(\tau\iota')(v) = \varrho(\tau)\left(\varrho(\iota')(v)\right) = \varrho(\tau)(v),$$

where we have used the definition of $V^{I_\mathfrak{p}}$ and the fact that $I_\mathfrak{p}$ is normal in $D_\mathfrak{p}$. Hence $\varrho(\tau)$ restricts to a transformation of $V^{I_\mathfrak{p}}$ and induces a transformation on $V/V^{I_\mathfrak{p}}$, both of which we shall call $\varrho(\tau)$. Now

$$\begin{aligned}\chi(\sigma_P^m) &= \frac{1}{\sharp I_\mathfrak{p}} \sum_{\iota \in I_\mathfrak{p}} \chi(\tau\iota) = \frac{1}{\sharp I_\mathfrak{p}} \sum_{\iota \in I} \operatorname{trace}_V \varrho(\tau\iota) \\ &= \operatorname{trace}_{V^{I_\mathfrak{p}}}\left(\varrho(\tau)\frac{1}{\sharp I_\mathfrak{p}}\sum_\iota \varrho(\iota)\right) + \operatorname{trace}_{V/V^{I_\mathfrak{p}}}\left(\varrho(\tau)\frac{1}{\sharp I_\mathfrak{p}}\sum_\iota \varrho(\iota)\right).\end{aligned}$$

In the first term, each $\varrho(\iota)$ is the identity transformation, so $\frac{1}{\#I_\mathfrak{p}}\sum_\iota \varrho(\iota)$ is also the identity transformation. In the second term, we observe simply that if $\bar{v} \in V/V^{I_\mathfrak{p}}$ and $\iota \in I_\mathfrak{p}$, then

$$\varrho(\iota)\left(\left(\sum_\iota \varrho(\iota)\right)(\bar{v})\right) = \left(\sum_\iota \varrho(\iota)\right)(\bar{v}), \quad \text{i.e.,}$$

$$\left(\sum_\iota \varrho(\iota)\right)(\bar{v}) = \bar{0}, \quad \text{i.e.,}$$

$\sum_\iota \varrho(\iota)$ is the zero transformation on $V/V^{I_\mathfrak{p}}$.

It follows that $\chi(\sigma_P^m) = \operatorname{trace}_{V^{I_\mathfrak{p}}}\left(\varrho(\tau)\right) = \operatorname{trace}_{V^{I_\mathfrak{p}}}\left(\varrho(\sigma_\mathfrak{p}^m)\right)$. ■

Now we do some computing. Let $\lambda_1(P), \lambda_2(P), \ldots, \lambda_r(P)$ be the eigenvalues of $\varrho(\sigma_\mathfrak{p})$ where $r = \dim V^{I_\mathfrak{p}}(\mathfrak{p}|P)$, and note that $r = n_\varrho = \deg$ of ϱ if P is unramified. Then

$$\det_{V^{I_\mathfrak{p}}}\left(1 - u^{\deg P}\varrho(\sigma_\mathfrak{p})\right) = \prod_{i=1}^{r}\left(1 - u^{\deg P}\lambda_i(P)\right).$$

Hence,

$$\log\left(\left(\det\left(1-u^{\deg P}\varrho(\sigma_\mathfrak{p})\right)\right)^{-1}\right) = -\sum_{i=1}^{r}\log\left(1-u^{\deg P}\lambda_i(P)\right)$$

$$= \sum_{i=1}^{r}\sum_{m=1}^{\infty}\frac{u^{m\deg P}\lambda_i^m(P)}{m} \qquad \text{(by Taylor's Theorem)}$$

$$= \sum_{m=1}^{\infty}\frac{u^{m\deg P}\chi(\sigma_P^m)}{m} \qquad \text{(by Definitions 5.3 and 5.4, and Lemma 5.5).}$$

So the logarithmic derivative of $L(u,\chi)$ with respect to u is

$$\frac{L'(u,\chi)}{L(u,\chi)} = \frac{d}{du}\left(\log L(u,\chi)\right) = \frac{d}{du}\left(\sum_P \log\left(\det\left(1-u^{\deg P}\varrho(\sigma_\mathfrak{p})\right)\right)^{-1}\right)$$

$$= \sum_P \frac{d}{du}\left(\sum_{m=1}^{\infty}\frac{u^{m\deg P}\chi(\sigma_P^m)}{m}\right)$$

$$= \sum_P\sum_{m=1}^{\infty}\frac{m\deg P u^{m\deg P-1}\chi(\sigma_P^m)}{m} \qquad (\text{let } v = \deg P)$$

$$= \frac{1}{u}\sum_{v=1}^{\infty} v \sum_{\deg P = v}\sum_{m=1}^{\infty} u^{mv}\chi(\sigma_P^m) \qquad (\text{replace } mv \text{ by } d)$$

$$= \frac{1}{u}\sum_{d=1}^{\infty}\left(\sum_{mv=d} v \sum_{\deg P=v}\chi(\sigma_P^m)\right)u^d$$

$$= \sum_{d=1}^{\infty}\left(\sum_{v|d} v\pi_{d/v}(\chi)\right)u^{d-1}$$

where we define $\pi_{d/v}(\chi) = \sum_{\deg P = v}\chi(\sigma_P^{d/v})$.

On the other hand, we know by the Weil Theorem that $L(u,\chi)$ is a polynomial of degree $= \deg f\chi - 2n_\varrho$. Let $\{\theta_i\}$ be the roots of this polynomial. Then $|\theta_i| = q^{-1/2}$ and we write

$$\frac{L'(u,\chi)}{L(u,\chi)} = \sum_{i=1}^{N}\frac{1}{u-\theta_i} \qquad (\text{we have set } N = \deg f\chi - 2n_\varrho)$$

$$= -\sum_{i=1}^{N}\sum_{d=0}^{\infty}\frac{u^d}{\theta_i^{d+1}} \qquad \text{(power series expansion)}$$

$$= -\sum_{d=0}^{\infty}u^d\left(\sum_{i=1}^{N}\theta_i^{-(d+1)}\right) \qquad \text{(replace } d \text{ by } d-1 \text{ below)}$$

$$= -\sum_{d=1}^{\infty}u^{d-1}\left(\sum_{i=1}^{N}\theta_i^{-d}\right).$$

We now set these two expressions for $\frac{L'(u,\chi)}{L(u,\chi)}$ equal, obtaining

$$\sum_{d=1}^{\infty}\left(\sum_{v|d} v\pi_{d/v}(\chi)\right)u^{d-1} = -\sum_{d=1}^{\infty}\left(\sum_{i=1}^{N}\theta_i^{-d}\right)u^{d-1}.$$

Equating coefficients, we must have

$$\sum_{v|d} v\pi_{d/v}(\chi) = -\sum_{i=1}^{N}\theta_i^{-d}.$$

Finally, setting $d = 1$, we get simply

$$\sum_{\deg P=1}\chi(\sigma_P) = -\sum_{i=1}^{N}\theta_i^{-1}$$

so that

$$\left|\sum_{\deg P=1}\chi(\sigma_P)\right| \leq N\sqrt{q}\,.$$

We save this result as

THEOREM 5.6. *Let ϱ be a non-trivial irreducible representation of S_n of* $\deg n_\varrho$ *and let χ be its associated character with conductor $\mathfrak{f}\chi$. Then,*

$$\Big|\sum_{\deg P=1}\chi(\sigma_P)\Big| \leqslant (\deg \mathfrak{f}\chi - 2n_\varrho)\sqrt{q}\,.$$

This theorem will allow us to write down our desired asymptotic formula.

Let $f(x)$ satisfy the hypotheses of Theorem 5.1. Then by Lemma 3, p. 423 of [2], the Galois group of E (the splitting field of $f(x)-t$) over $k_q(t)$ is the full symmetric group S_n. This then is the first part of Theorem 5.2.

DEFINITION 5.7. Let N_n = number of unramified 1st degree primes $t-\omega$ in $k_q(t)$ such that $\left[\frac{E/k_q(t)}{t-\omega}\right]$ is the class of n-cycles.

LEMMA 5.8. *Let G be any finite group and let $\chi_1, \ldots, \chi_h$ be the characters of the irreducible complex representations of G, so that $h = \#$ of conjugacy class in G. Let $c(g) = \#$ of elements in the conjugacy class of $g \in G$ and denote $\chi_i(g^{-1})$ by $\chi_i(g)^*$. Then*

$$\sum_{i=1}^{h}\chi_i(g)^*\chi_i(g') = \begin{cases} \#G/c(g) & \text{if } g' \text{ is conjugate to } g,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. This is Proposition 7, p. 20 of [16]. ■

COROLLARY 5.9. *Let σ be an n-cycle in S_n, then*

$$\frac{1}{n}\sum_{\chi\,\text{irred}}\chi(\sigma)^*\chi(\tau) = \begin{cases} 1 & \text{if } \tau \text{ is an } n\text{-cycle},\\ 0 & \text{if } \tau \text{ is not an } n\text{-cycle}.\end{cases}$$

Proof. σ and τ are conjugate in S_n if and only if τ is also an n-cycle. Moreover, $c(\sigma) = \#$ of n-cycles $= (n-1)!$, so $\#S_n/c(\sigma) = n$. The result follows now from Lemma 5.8. ■

We use Corollary 5.9 now to get a generating formula for N_n (see Definition 5.7). Fix an n-cycle σ in S_n. Now,

$$N_n = \sum_{\substack{\deg P=1\\ P\,\text{unramified}}}\frac{1}{n}\sum_{\chi\,\text{irred}}\chi(\sigma)^*\chi(\sigma_P) \qquad \text{(by Corollary 5.9 and Definitions 5.3 and 5.7)}$$

$$= \sum_{\text{all}\,\deg P=1}\frac{1}{n}\sum_{\chi\,\text{irred}}\chi(\sigma)^*\chi(\sigma_P) - \sum_{\substack{\deg P=1\\ P\,\text{ramified}}}\frac{1}{n}\sum_{\chi\,\text{irred}}\chi(\sigma)^*\chi(\sigma_P) \qquad \text{(see Definition 5.4)}$$

$$= \frac{q+1}{n} + \frac{1}{n}\sum_{\chi\neq\chi_0}\chi(\sigma)^*\Big(\sum_{\deg P=1}\chi(\sigma_P)\Big) - \sum_{\substack{\deg P=1\\ P\,\text{ramified}}}\frac{1}{n}\sum_{\chi}\chi(\sigma)^*\chi(\sigma_P)$$

where we have split off the trivial character in the first term and used the fact that there are $q+1$ primes in $k_q(t)$ of deg $= 1$, the finite primes $\{t-a \mid a \in k_q\}$ and the (unique) infinite prime P_∞.

DEFINITION 5.10. Let

$$E_1 = \frac{1}{n}\sum_{\chi\neq\chi_0}|\chi(\sigma)|\cdot(\deg\mathfrak{f}\chi - 2n_\varrho)\sqrt{q}$$

and let

$$E_2 = \Big|\sum_{\substack{\deg P=1\\ P\,\text{ramified}}}\frac{1}{n}\sum_{\chi}\chi(\sigma)^*\chi(\sigma_P)\Big|.$$

We have established above that $N_n \geqslant (q+1)/n - E_1 - E_2$, where in writing E_1 we have used Theorem 5.6 to get an upper bound for $\big|\sum_{\deg P=1}\chi(\sigma_P)\big|$. Below, we will establish that E_1 is in fact $O(\sqrt{q})$ by establishing an upper bound for $(\deg\mathfrak{f}\chi - 2n_\varrho)$ independent of q (Proposition 5.17), provided only that $(n, q) = 1$. Moreover, it will also be shown below (Corollary 5.13) that there are at most $n-1$ finite linear ramified primes, so that there are at most n terms in the outer sum for E_2. By Definition 5.4 and Corollary 5.9,

$$\frac{1}{n}\sum_{\chi}\chi(\sigma)^*\chi(\sigma_P)$$

will equal the number of preimages of $\sigma_\mathfrak{p}$ in $D_\mathfrak{p}$ which are n-cycles, so the sum has greatest value when all preimages are n-cycles, in which case

$$\frac{1}{n}\sum\chi(\sigma)^*\chi(\sigma_P) = \frac{1}{\#I_\mathfrak{p}}\sum_{\iota\in I_\mathfrak{p}}\Big(\frac{1}{n}\sum_{\chi}\chi(\sigma)^*\chi(\tau_\iota)\Big) = 1.$$

Hence $E_2 \leqslant n$, which of course is $O(1)$. We will have shown, then, that

$$N_n = \frac{q+1}{n} + O(\sqrt{q}) + O(1),$$

so Theorem 5.2 will be established.

We wish to save

THEOREM 5.11. *Let N_n be as in Definition 5.7 and E_1 and E_2 as in Definition 5.10. Then,*

$$N_n \geqslant (q+1)/n - E_1 - E_2.$$ ■

The task before us now is (specifically) to evaluate the error terms E_1 and E_2 in order to find the minimal q (depending on n) for which N_n is positive. Both E_1 and E_2, however, depend upon the ramified primes: with E_2 this is obvious since it is a sum over ramified primes, but E_1 also depends on the ramified primes precisely because the degree of $\mathfrak{f}\chi$ is a sum of degrees of "local" conductors, and these degrees are non-zero exactly when the corresponding primes are ramified. Hence we must ask the following questions: (1) What are the ramified primes in $k_q(t)$ for the extension E, or at least, what is the sum of their degrees? (2) What are their ramification indices? And (3), using (1) and (2), what can we say about $\deg\mathfrak{f}\chi$ for an irreducible character χ? We now will answer these questions one at a time.

PROPOSITION 5.12. *Let $f(x) \in k_q[x]$ have degree n and let x_1 be a root of $f(x)-t$ in E (the splitting field). Then,*

$$N_{k_q(x_1,t)/k_q(t)}\big(f'(x_1)\big)$$

is a polynomial in $k_q[t]$ of degree at most $n-1$.

Proof. Let v_∞ be the valuation on $k_q(t)$ with respect to the ∞-prime, so that $v_\infty\big(g(t)\big) = -\deg g$ if $g \in k_q[t]$. Let $x_1, \ldots, x_n$ be the roots of $f(x)-t$ in E and for each i, let v_{∞_i} be the extension of v_∞ to $k_q(x_i, t)$ such that $v_{\infty_i}(x_i) = -1$ (i.e., if $h(x_i)$ is a polynomial over k_q in x_i, then $v_{\infty_i}\big(h(x_i)\big) = -\deg h$). Then $v_{\infty_i}(t) = v_{\infty_i}\big(f(x_i)\big) = -n$, so each v_{∞_i} has ramification index n over v_∞. Now,

$$\begin{aligned}\deg\big(N\big(f'(x_1)\big)\big) &= -v_\infty\big(N\big(f'(x_1)\big)\big) = -\frac{1}{n}\,v_{\infty_1}\big(N\big(f'(x_1)\big)\big)\\ &= -\frac{1}{n}\,v_{\infty_1}\Big(\prod_{i=1}^{n} f'(x_i)\Big)\\ &= -\frac{1}{n}\sum_{i=1}^{N} v_{\infty_i}\big(f'(x_i)\big) = -v_{\infty_1}\big(f'(x_1)\big)\\ &= \deg f'(x_1) \leqslant n-1. \ \blacksquare\end{aligned}$$

COROLLARY 5.13. *The sum of the degrees of the finite primes of $k_q(t)$ which ramify in E (the splitting field of $f(x)-t$, $\deg f = n$) is at most $n-1$.*

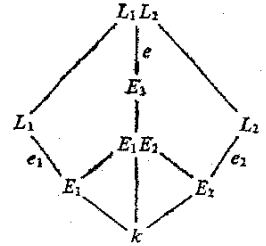
Proof. First suppose that P is a prime which does not ramify in $k_q(x_1, t)$ where x_1 is a root of $f(x)-t$ in E, then P will not ramify in $k_q(x_i, t)$ for any x_i a root by Galois action in E. Letting $\mathfrak{p}$ be any prime over P in any $k_q(x_i, t)$, then the extension of complete local fields $k_q(x_i, t)_\mathfrak{p}$ over $k_q(t)_P$ is unramified, so by Proposition 8, p. 49 in [12], P must remain unramified in E.

Hence P ramifies in E if and only if it ramifies in $k_q(x_1, t)$, which will be true if and only if $D_{k_q(x_1,t)/k_q(t)}$ is divisible by P. But since the ideal generated by $f'(x_1)$ is contained in the different d of $k_q(x_1, t)$ over $k_q(t)$ (see, for example, [15], pp. 95–96), we have $D \mid N\big(f'(x_1)\big)$. Hence P divides D implies P divides $N\big(f'(x_1)\big)$, but by Proposition 5.12, $N\big(f'(x_1)\big)$ has degree at most $n-1$. ■

We now turn to the second question concerning ramified primes, i.e., what are their ramification indices? We first prove a result which tells how under appropriate conditions we can obtain the ramification index of a prime in a composite extension given its ramification indices in some subextensions. The appropriate condition will only be that the ramification be "tame".

PROPOSITION 5.14 (The Least Common Multiple Lemma). *Let k be a field complete with respect to a valuation with residue class field of characteristic p. Let L_1 and L_2 be finite extensions of k with ramification indices e_1 and e_2 respectively over k, where $p \nmid e_1e_2$. Then the ramification index e of L_1L_2 over k is exactly $\langle e_1, e_2\rangle$.*

Proof. Let E_1 and E_2 respectively be the maximal unramified extensions of k in L_1 and L_2 and let E_3 be the maximal unramified extension of k in L_1L_2, so that in particular $E_3 \supseteq E_1E_2$ (see, for example, [12], pp. 49–54). The extensions L_1/E_1, L_2/E_2, and L_1L_2/E_3 are all totally and tamely ramified.



Let π be a uniformizer in k and let x_1 and x_2 be uniformizers in L_1 and L_2 respectively, so that $L_1 = E_1(x_1)$ and $L_2 = E_2(x_2)$, and $x_1^{e_1} = u_1\pi$ and $x_2^{e_2} = u_2\pi$, where u_1 and u_2 are units in the valuation rings of E_1 and E_2 respectively. Write $ae_1 + be_2 = d$, where $d = \text{g.c.d.}\,(e_1, e_2)$. Define $Y = x_1^b x_2^a$, so that $Y \in L_1L_2$. We claim that Y generates L_1L_2 over E_3 and that $Y^{\langle e_1,e_2\rangle} = u'\pi$ (for u' some unit in E_3), which will prove the result.

First the latter claim. We have

$$\begin{aligned}Y^{\langle e_1,e_2\rangle} &= x_1^{b\langle e_1,e_2\rangle}x_2^{a\langle e_1,e_2\rangle} = x_1^{e_1(be_2/d)}x_2^{e_2(ae_1/d)}\\ &= (u_1\pi)^{be_2/d}(u_2\pi)^{ae_1/d} = u'\pi^{(be_2+ae_1)/d} = u'\pi\end{aligned}$$

as required. Now for the former claim, it suffices to show that $x_2 \in E_3(Y)$, for then by symmetry $L_1L_2 = E_1E_2(x_1, x_2) \subseteq E_3(Y)$. Let $\omega = Y^{\langle e_1, e_2\rangle/e_2}/x_2$, then we have

$$\omega^d = Y^{e_1}x_2^{-d} = x_1^{be_1}x_2^{ae_1-d} = x_1^{be_1}x_2^{-be_2} = (u_1u_2^{-1})^b \in E_1E_2 \subseteq E_3.$$

Hence $\omega \in L_1L_2$ and $\omega^d \in E_3$. If $v_{L_1L_2}$ is the extension of the valuation v_{E_3} of E_3, then we have

$$dv_{L_1L_2}(\omega) = v_{L_1L_2}(\omega^d) = ev_{E_3}\big((u_1u_2^{-1})^b\big) = 0,$$

so ω is a unit in L_1L_2. We claim finally that in fact $\omega \in E_3$, which will give $x_2 = \omega Y^{\langle e_1, e_2\rangle/e_2} \in E_3(Y)$ as required. The extension $E_3(\omega)$ ramifies over E_3 if and only if $f'(\omega)$ is a non-unit where $f(x) = x^d - a_0$ ($a_0 \in E_3$). But $v_{E_3(\omega)}\big(f'(\omega)\big) = v_{E_3(\omega)}(d\omega^{d-1}) = v(d) + (d-1)v(\omega) = 0$ since $p \nmid d$. Hence $E_3(\omega)$ is an unramified extension of E_3 (and hence of k) in L_1L_2, so $E_3(\omega) \subseteq E_3$, i.e., $\omega \in E_3$. This completes the proof. ∎

We may now compute the ramification indices of all ramified primes of $k_q(t)$.

PROPOSITION 5.15. *Let $f(x)$ satisfy the hypotheses of Theorem* 5.1. *Then the ramification index of every finite ramified prime of $k_q(t)$ in E is* 2, *and if $p \nmid n$ (the degree of f), then the ramification index of the ∞-prime is n.*

Proof. As observed in the proof of Proposition 5.12, the ramification index of the ∞-prime in each $k_q(x_1, t)$ is n, so if $p \nmid n$, then by the L.C.M. Lemma (Proposition 5.14), its ramification index in E must be n.

Now let P be a finite prime of $k_q(t)$, i.e., an irreducible polynomial in t. Then P will, by Hensel's lemma, ramify in $k_q(x_1, t)$ (where x_1 is a root of $f(x)-t$ in E) only if when we factor $f(x)-t$ over the completion $k_q(t)_P$ and then reduce to the residue class field $k_q[t]/P \simeq k_{q^r}$ (where $\deg P = r$), $\overline{f(x)-t}$ has a multiple root (see, for example, [3], p. 271, Theorem 3, and p. 275). But by assumption $f'(x) = \big(\overline{f(x)-t}\big)'$ has distinct roots, so if $\overline{f(x)-t}$ has multiple roots, then their multiplicity can be at most 2. Thus if P ramifies in $k_q(x_1, t)$, its ramification index cannot exceed 2.

We finish the argument by merely pointing out that since q is odd, $p \nmid 2$, and so Proposition 5.14 applies again to give us the result. ∎

Finally, we must develop a way of computing $\deg \mathfrak{f}\chi$ where $\mathfrak{f}\chi$ is the conductor of the character χ. This, however, is given to us directly by Serre in his *Local fields* [17]. His terminology is as follows: G is the galois group of E/K where E and K are complete local fields (so G corresponds to the decomposition group $D_\mathfrak{p}$ in the "global" situation), and G_0 is the inertial group. The decomposition groups $G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots$ as defined in Section 1 of Chapter 4 in our case satisfy $G_1 = G_2 = \dots = 1$ by Proposition 5.14 as long as we assume $p \nmid n$ (see Corollaries 1 and 3, p. 67). In fact, also, we know that if P is a finite ramified prime, then $\#G_0 = 2$,

and if P is infinite, then $\#G_0 = n$. Now the degree of the local conductor, $f(\chi, P)$ is given on p. 100 in Corollary 1, specifically $f(\chi, P) = \sum_{i=0}^{\infty} \frac{\#G_i}{\#G_0} \times \times \big(\chi(1) - \chi(G_i)\big)$ which simplifies in our case to $f(\chi, P) = \chi(1) - \chi(G_0)$ where $\chi(1)$ is just the degree n_ϱ of the representation ϱ associated with χ and $\chi(G_0)$ is defined on p. 100 as

$$\chi(G_0) = \frac{1}{\#G_0} \sum_{s \in G_0} \chi(s).$$

We observe then that if P is unramified, $G_0 = 1$ and so $f(\chi, P) = 0$, i.e., only ramified primes contribute to the degree of the conductor. For future use we make the

DEFINITION 5.16. If χ is an irreducible character of S_n associated with ϱ and if P is a prime of $k_q(t)$, then define

$$m_\varrho(P) = \frac{1}{\#G_0} \sum_{s \in G_0} \chi(s)$$

where G_0 is the inertial group of a prime $\mathfrak{p}$ in E over P.

Now, the global conductor of χ is defined simply as

$$\mathfrak{f}\chi = \prod_{\text{all } P} P^{f(\chi, P)} \quad ([17], \text{ p. } 104),$$

and so

$$\deg \mathfrak{f}\chi = \sum_{\text{all ramified } P} f(\chi, P)(\deg P).$$

Hence we arrive at

PROPOSITION 5.17. *Let χ be the character associated with the irreducible representation ϱ of $S_n = \mathrm{Gal}\big(E/k_q(t)\big)$ where $(n, q) = 1$. Then*

$$\deg \mathfrak{f}\chi = \sum_{\substack{\text{all ramified} \\ P \text{ in } k_q(t)}} \big(n_\varrho - m_\varrho(P)\big)(\deg P)$$

where n_ϱ is the degree of the representation ϱ and m_ϱ is defined in 5.16.

We now have all the information we need to evaluate the error terms E_1 and E_2 given in Definition 5.10 for any given n. In the next section we do precisely this for the cases $n = 4$ and 5.

6. A partial solution to the 3-primes problem for the cases $r = 6$ and 7. In this section we gather the fruits of our labor for the cases $n = 4$ and 5 and in so doing obtain a partial solution to the 3-primes problem for polynomials of degree 6 and 7.

We start with the following odd sounding lemma:

LEMMA 6.1. *Let* $f(x)=x^4+bx^3+cx^2+dx+e \in k_q[x]$ *and let* $\gamma \in k_{q^j}$ *for some* $j \geq 1$. *Suppose that* $d \neq (b/2)(c-b^2/4)$.

(1) *Then* $f(x)-\gamma$ *cannot have 2 roots each of multiplicity 2.*

(2) *Suppose* $p \neq 3$. *Let* β_1 *and* β_2 *be the roots of* $f''(x)=12x^2+6bx+2c$, *and suppose that* $d \neq -(4\beta_1^3+3b\beta_1^2+2c\beta_1)$ *and* $d \neq -(4\beta_2^3+3b\beta_2^2+2c\beta_2)$, *then* $f(x)$ *satisfies the hypotheses of Theorem* 5.1.

(3) *Suppose* $p=3$. *If* $c \neq 0$, *then* $f(x)$ *satisfies the hypotheses of Theorem* 5.1.

Proof. (1) Just suppose that $f(x)-\gamma$ did have 2 roots each of multiplicity 2, then

$$f(x)-\gamma = (x-a_1)^2(x-a_2)^2$$
$$= x^4-2(a_1+a_2)x^3+(a_1^2+a_2^2+4a_1a_2)x^2-2a_1a_2(a_1+a_2)x+a_1^2a_2^2.$$

Hence, $b=-2(a_1+a_2)$, $c=a_1^2+a_2^2+4a_1a_2=(a_1+a_2)^2+2a_1a_2$, and $d=-2a_1a_2(a_1+a_2)$. But then,

$$c=(-b/2)^2+2a_1a_2 \Rightarrow 2a_1a_2=c-b^2/4,$$

so

$$d=-\left(c-\frac{b^2}{4}\right)\left(-\frac{b}{2}\right)=\frac{b}{2}\left(c-\frac{b^2}{4}\right).$$

This contradiction proves statement (1) of the lemma.

(2) We assume $p \neq 3$, so $f''(x)$ is a quadratic polynomial with roots β_1 and β_2. $f'(x)$ can have a multiple root only if it shares a root with $f''(x)$, but if β_1 (say) is also a root of $f'(x)$, then we have $4\beta_1^3+3b\beta_1^2+2c\beta_1+d=0$ which contradicts our assumption. Similarly for β_2, so we conclude that $f'(x)$ must have distinct roots a_1, a_2, and a_3. Finally we must check that $f(a_1)$, $f(a_2)$, and $f(a_3)$ are distinct values. Suppose, for example that $f(a_1)=f(a_2)$, then a_1 and a_2 are both roots of $f(x)-f(a_1)$, and since $(f(x)-f(a_1))'=f'(x)$, both must be multiple roots. But this contradicts part (1) of the lemma. Hence $f(x)$ satisfies the hypotheses of Theorem 5.1.

(3) Assume $p=3$, now $f''(x)=2c \neq 0$ by assumption, so $f'(x)$ must have distinct roots since its derivative has no roots at all. The rest of the argument is as in part (2). ∎

COROLLARY 6.2. *Let* $f(x)$ *be as in Lemma* 6.1 *and satisfy all hypotheses there. Let* P *be a finite prime of* $k_q(t)$ *which ramifies in* E *and let* $\mathfrak{p}$ *be any prime of* E *over* P. *Then the inertial group* $I_\mathfrak{p}$ *is generated by a single transposition.*

Proof. This is a refining of Proposition 5.15, wherein it was shown that $\#I_\mathfrak{p}=2$. Lemma 6.1 (1) shows that $\overline{f(x)-t}=f(x)-\gamma$ can have only one multiple root, which says that the inertial group will consist

of one transposition. For if $I_\mathfrak{p}=\langle(ab)(cd)\rangle$, say, then under the canonical homomorphism

$$D_\mathfrak{p}/I_\mathfrak{p} \to \mathrm{Gal}(\mathcal{O}_\mathfrak{p}/\mathfrak{p} \text{ over } \mathcal{O}_P/P),$$

the permutation $(ab)(cd)$ of roots of $f(x)-t$ becomes the identity, which says that the roots of $\overline{f(x)-t}=f(x)-\gamma$ are identified in pairs, i.e., that $f(x)-\gamma$ has two multiple roots. ∎

We are now in a position to calculate the error terms E_1 and E_2 for the case $n=4$ (see Definition 5.10). At this point we know that the sum of the degrees of the finite ramified primes is at most 3 and each has ramification index 2, in fact satisfies $I_\mathfrak{p}=\langle(ab)\rangle$, and we know that the ∞-prime has ramification index $=4$. Hence in the expression for $\deg \mathfrak{f}\chi$ (Proposition 5.17), we may put all the finite ramified primes together and write

$$\deg \mathfrak{f}\chi \leq \big(n_\varrho - m_\varrho(\text{finite})\big)3+\big(n_\varrho-m_\varrho(P_\infty)\big)1$$

since the degree of the ∞-prime is 1 (since $\mathcal{O}_{P_\infty}/P_\infty \simeq k_q$), and where $m_\varrho(\text{finite})=\frac{1}{2}\big(\chi(\text{transposition})+\chi(1)\big)$ (see Definition 5.16) and $m_\varrho(P_\infty)=\frac{1}{4}\big(2\chi(4\text{-cycles})+\chi(\text{two transpositions})+\chi(1)\big)$. We compute then, using the character table for S_4 (see, e.g., [13], p. 265),

$$E_1=\frac{1}{n}\left(\sum_{\chi\neq\chi_0}|\chi(\sigma)|\left(\left(\sum_{P \text{ ramified}}\big(n_\varrho-m_\varrho(P)\big)\deg P\right)-2n_\varrho\right)\right)\sqrt{q}$$
$$=\tfrac{1}{4}\big[\big((3-2)3+(3-0)1-2(3)\big)+\big((3-1)3+(3-1)1-2(3)\big)+$$
$$+\big((1-0)3+(1-0)1-2(1)\big)\big]\sqrt{q}$$
$$=\tfrac{1}{4}\big((3+3-6)+(6+2-6)+(3+1-2)\big)\sqrt{q}=\tfrac{4}{4}\sqrt{q}=\sqrt{q}.$$

We turn now to the computation of E_2. As discussed following Definition 5.10, a given ramified prime contributes to E_2 only if 1 or more preimages of a generator of $D_\mathfrak{p}/I_\mathfrak{p}$ is a 4-cycle. But if P is a finite ramified prime, then we know that $I_\mathfrak{p}=\langle(ab)\rangle$ and $I_\mathfrak{p}$ must be normal in $D_\mathfrak{p}$. One checks that it is impossible for a subgroup of S_4 containing a 4-cycle to contain a normal transposition, and hence no finite ramified prime can contribute to E_2. The ∞-prime, on the other hand, satisfies $I_\mathfrak{p}=\langle(1234)\rangle$ (say), and one checks easily that $|D_\mathfrak{p}|=4$ or 8 and in any case at most 2 preimages of a generator of $D_\mathfrak{p}/I_\mathfrak{p}$ can be 4-cycles. Thus

$$E_2=\tfrac{1}{4}\sum_\chi \chi(\sigma)^*\chi(\sigma_\mathfrak{p})=\tfrac{1}{4}\sum_{\substack{\tau\in D_\mathfrak{p}\\ \tau\to\text{generator of } D_\mathfrak{p}/I_\mathfrak{p}}}\left(\tfrac{1}{4}\sum_\chi \chi(\sigma)^*\chi(\tau)\right)=\tfrac{1}{2}.$$

Hence we have shown that in this case, by Theorem 5.11,

$$N_4 \geq (q+1)/4-\sqrt{q}-1/2,$$

and the right-hand side is strictly positive provided

$$q+1-2>4\sqrt{q} \Leftrightarrow (q-1)>4\sqrt{q} \Leftrightarrow q^2-2q+1>16q$$
$$\Leftrightarrow q^2-18q+1>0 \Leftrightarrow q>(18+\sqrt{18^2-4})/2 = 17.94.$$

We have proved

THEOREM 6.3. *Let $f(x)$ satisfy all the hypotheses of Lemma 6.1. Then there exists an $\omega \in k_q$ such that $f(x)-\omega$ is irreducible provided $q \geqslant 19$ and is odd.* ■

We now solve the 3-primes problem for 6th degree polynomials provided that $q \geqslant 19$ and odd. Let M be an arbitrary 6th degree polynomial in $k_q[x]$. As outlined just following Theorem 5.1, we wish now to produce a 6th degree irreducible P_1 such that $M-x-P_1 = f(x)$ satisfies the hypotheses of Lemma 6.1. Then by Theorem 6.3 we are guaranteed of an $\omega \in k_q$ such that $f(x)-\omega$ is irreducible, and we will have $M = P_1 + (f(x)-\omega)+(x+\omega)$, i.e., we will have written M as the sum of 3 irreducibles. To find our appropriate P_1, it is unfortunately necessary to look at two cases: when $p \neq 3$ and $p = 3$.

Case 1. $p \neq 3$. We need the following:

LEMMA 6.4A. *Let τ and α be fixed. If $q \geqslant 19$ and $p \neq 2$ or 3, then there exist coefficients β, γ, and ε such that there are at least 4 distinct irreducibles of the form*

$$x^6+\tau x^5+\alpha x^4+\beta x^3+\gamma x^2+\delta_i x+\varepsilon.$$

Proof. Suppose not, then for every triple $(\beta, \gamma, \varepsilon)$ ($\varepsilon \neq 0$ since these polynomials are irreducible), there are at most 3 irreducibles with that triple as coefficients and with first two coefficients τ and α. Hence the total number of irreducibles starting with τ and α cannot exceed $q\cdot q\cdot(q-1)\cdot 3 = 3q^3-3q^2$. But on the other hand, there are at least $(q^4-q^2-2q-2)/6$ such polynomials by Corollary 3.11. Hence

$$3q^3-3q^2 \geqslant \frac{q^4-q^2-2q-2}{6} \Leftrightarrow 18q^3-18q^2 \geqslant q^4-q^2-2q-2$$
$$\Leftrightarrow q^4-18q^3+17q^2-2q-2 \leqslant 0 \Rightarrow q \leqslant 17.$$

This contradicts our assumption that $q \geqslant 19$. ■

Suppose now that $q \geqslant 19$ and let M be an arbitrary 6th degree polynomial. Suppose in fact that

$$M-x = x^6+\tau x^5+(\alpha+1)x^4+\beta' x^3+\gamma' x^2+\delta' x+\varepsilon'.$$

Let β, γ, and ε be as guaranteed by Lemma 6.4A. Then we have at least 4 distinct irreducibles $P_{1,i}$ $(1 \leqslant i \leqslant 4)$ of the form

$$P_{1,i} = x^6+\tau x^5+\alpha x^4+\beta x^3+\gamma x^2+\delta_i x+\varepsilon,$$

so that

$$M-x-P_{1,i} = x^4+(\beta'-\beta)x^3+(\gamma'-\gamma)x^2+(\delta'-\delta_i)x+\varepsilon'-\varepsilon$$
$$= x^4+bx^3+cx^2+d_i x+e.$$

From the set $\{d_i\}_{i=1}^4$, pick one d_k so that it does not equal any of the 3 numbers in Lemma 6.1 (1) and (2). Set $d = d_k$ and $P_1 = P_{1,k}$. $f(x) = M-x-P_1$ satisfies all hypotheses of Lemma 6.1 and hence Theorem 6.3 is true for $f(x)$. We have proved:

THEOREM 6.5A. *Let $q \geqslant 19$, odd, and suppose $p \neq 3$. Then the 3-primes problem is solved for all 6th degree polynomials over k_q.* ■

Case 2. $p = 3$. Here we need:

LEMMA 6.4B. *Let $p = 3$ and let τ, α, and γ' be given. If $q \geqslant 27$, then there exist coefficients β, γ, and ε such that there are at least 2 distinct irreducibles of the form*

$$x^6+\tau x^5+\alpha x^4+\beta x^3+\gamma x^2+\delta_i x+\varepsilon, \quad \text{and} \quad \gamma \neq \gamma'.$$

Proof. There are at most $q\cdot q\cdot(q-1)$ irreducibles which have 1st two coefficients τ and α and have γ' as the x^2-coefficient. By Corollary 3.11 there are at least $(q^4-q^3-q^2-q)/6$ irreducibles starting with τ and α. If we toss out all of the above-mentioned polynomials, our new lower bound is

$$\frac{(q^4-q^3-q^2-q)}{6}-(q^3-q^2) = \frac{q^4-7q^3+5q^2-q}{6}.$$

Now suppose that for every triple $(\beta, \gamma, \varepsilon)$, $\gamma \neq \gamma'$ and $\varepsilon \neq 0$, there is a unique irreducible, then we would have at most

$$1\cdot q\cdot(q-1)\cdot(q-1) = q^3-2q^2+q$$

irreducibles starting with τ and α and not having γ' in the x-slot.

Hence,

$$q^3-2q^2+q \geqslant \frac{q^4-7q^3+5q^2-q}{6} \Leftrightarrow q^4-13q^3+17q^2-7q \leqslant 0 \Rightarrow q \leqslant 11.$$

But we have assumed that $q \geqslant 27$. ■

Now suppose that $q \geqslant 27$ and again let

$$M-x = x^6+\tau x^5+(\alpha+1)x^4+\beta' x^3+\gamma' x^2+\delta' x+\varepsilon',$$

so that we have two distinct $P_{1,i}$ irreducibles so that

$$M-x-P_{1,i} = x^4+bx^3+cx^2+d_i x+e$$

where $c \neq 0$. Choose $d_k \neq \frac{b}{2} \cdot \left(c - \frac{b^2}{4}\right)$ (see Lemma 6.1), and set $P_1 = P_{1,k}$ and $d = d_k$. Now all hypotheses of Lemmas 6.1 (1) and (3) are satisfied, and again Theorem 6.3 holds. We can finally conclude

THEOREM 6.5. *Let q be odd and $q \geqslant 19$. Then every 6th degree polynomial over k_q is a 3-primes polynomial.* ■

We now turn to the case $n = 5$. We must first develop an appropriate analogue to Lemma 6.1. Let $\gamma \in k_{q^j}$ and let $f(x) = x^5+bx^4+cx^3+dx^2+ex+g \in k_q[x]$ where we shall now assume in addition to oddness that $p \neq 5$. First suppose that $f(x)-\gamma$ had two multiple roots each of multiplicity 2, i.e., $f(x)-\gamma = (x-\alpha_1)^2(x-\alpha_2)^2(x-\alpha_3)$. Letting $s = \alpha_1+\alpha_2$ and $P = \alpha_1\alpha_2$, it is easy to multiply out and write

$$f(x) = x^5-(\alpha_3+2s)x^4+(2\alpha_3 s+s^2+2P)x^3- \\ -(\alpha_3 s^2+2\alpha_3 P+2Ps)x^2+(2\alpha_3 Ps+P^2)x-\alpha_3 P^2.$$

We eliminate α_3 using $-b = \alpha_3+2s$ and substitute throughout. A result of this is that $c = -2bs-3s^2+2P$, which we solve for $2P$ and then substitute throughout. We now obtain

$$(*) \qquad d = 5s^3+6bs^2+(c+2b^2)s+bc.$$

Since $p \neq 5$, this is a cubic equation in s which has 3 roots, call them s_1, s_2, and s_3. We also have obtained the expression

$$(**) \qquad e = -\tfrac{15}{4}s^4-4bs^3+(-\tfrac{1}{2}c-b^2)s^2+c^4/4 = \varphi(s).$$

Let us call the expression on the right-hand side $\varphi(s)$.

Further, the second derivative $f''(x) = \big(f(x)-\gamma\big)'' = 20x^3+12bx^2+6cx+2d$ has 3 roots, say β_1, β_2, and β_3. If β_1, say, were also a root of $f'(x) = 5x^4+4bx^3+3cx^2+2dx+e$, then we would have $e = -(5\beta_1^4+4b\beta_1^3+3c\beta_1^2+2d\beta_1)$.

Suppose now that we do not allow the coefficient e to take on any of the 6 values $\varphi(s_i)$, $i = 1, 2, 3$ or $-(5\beta_i^4+4b\beta_i^3+3c\beta_i^2+2d\beta_i)$ for $i = 1, 2, 3$. Then $f'(x) = \big(f(x)-\gamma\big)'$ has 4 distinct roots, and all must give rise to distinct values of $f(x)$ (if α_1, α_2 are two such roots and $f(\alpha_1) = f(\alpha_2)$, then setting $\gamma = f(\alpha_1)$, we see that both α_1 and α_2 are multiple roots of $f(x)-\gamma$, which is impossible by our choice of the coefficient e). We have proved:

LEMMA 6.6. *Let $f(x) = x^5+bx^4+cx^3+dx^2+ex+g \in k_q[x]$ where q is odd and not a power of 5, and let $\gamma \in k_{q^j}$ for some j. Let $\{s_i\}_{i=1}^3$ be the roots of (*) and let $\{\beta_i\}_{i=1}^3$ be the roots of $f''(x)$. Assume that the coefficient e satisfies $e \neq \varphi(s_i)$ (φ defined in (**) above), $i = 1, 2, 3$ and $e \neq -(5\beta_i^4+4b\beta_i^3+3c\beta_i^2+2d\beta_i)$, $i = 1, 2, 3$. Then $f(x)-\gamma$ has at most one multiple root of multiplicity 2, and $f(x)$ satisfies the hypotheses of Theorem 5.1.* ■

COROLLARY 6.7. *Let $f(x)$ satisfy the hypotheses of Lemma 6.6. Let P be a finite prime of $k_q(t)$ which ramifies in E and let $\mathfrak{p}$ be any prime in E over P. Then the inertial group $I_{\mathfrak{p}}$ is generated by a single transposition.*

Proof. See Corollary 6.2. ■

We now proceed exactly as above to compute the error terms E_1 and E_2 (see Definition 5.10) for the case $n = 5$. We have now that the sum of the degrees of the ramified primes is less than or equal to 4, and all have the same m-values (see Definition 5.16) associated with the group $\langle(ab)\rangle$. The ∞-prime has ramification index 5, so its m-value is associated with the group generated by a 5-cycle. Going to the character table for S_5 (see, e.g., [13], p. 265),

$$E_1 = \frac{1}{n}\left(\sum_{\chi \neq \chi_0} |\chi(\sigma)|\left(\left(\sum_{P \text{ ramified}} \big(n_e - m_e(P)\big)\deg P\right) - 2n_e\right)\right)\sqrt{q}$$

$$\geqslant \frac{1}{5}\big((4-3)4+(4-0)1-2(4)\big)+ \\ +\big((6-3)4+(6-2)1-2(6)\big)+ \\ +\big((4-1)4+(4-0)1-2(4)\big)+ \\ +\big((1-0)4+(1-1)1-2(1)\big)\sqrt{q}$$

$$= \frac{1}{5}\big((4+4-8)+(12+4-12)+(12+4-8)+(4+0-2)\big)\sqrt{q}$$

$$= \frac{1}{5}(0+4+8+2)\sqrt{q} = \frac{14}{5}\sqrt{q}.$$

The error E_2 is small again, for just as in the case $n = 4$, no finite prime can contribute. This follows simply from observing that were a finite prime to contribute, $D_{\mathfrak{p}}$ would have to contain a 5-cycle and a normal 2-cycle, which is impossible (easy check). Hence, only the ∞-prime can contribute, and as just preceding Theorem 5.11, we have $E_2 \leqslant 1$.

Now by Theorem 5.11, we have

$$N_5 \geqslant (q+1)/5-\tfrac{14}{5}\sqrt{q}-1,$$

and the right-hand side is strictly positive provided

$$q+1-5 > 14\sqrt{q} \Leftrightarrow q^2-8q+16 > 196q$$

$$\Leftrightarrow q^2-204q+16 > 0 \Rightarrow q > \frac{204+\sqrt{(204)^2-64}}{2} = 203.92.$$

We hawe proved:

THEOREM 6.8. *Let $f(x)$ satisfy the hypotheses of Lemma 6.6. Then there exists an $\omega \in k_q$ such that $f(x)-\omega$ is irreducible provided $q \geqslant 207$, q is odd, and $p \neq 5$.* ■

We wish to use this theorem to obtain a solution to the 3-primes problem for 7th degree polynomials provided q is as in the theorem. Just as before, we need now, given an arbitrary polynomial M of deg 7 over k_q, to guarantee the existence of a 7th degree irreducible P_1 such that $M-x-P_1 = f(x)$ satisfies the hypotheses of Lemma 6.6.

We need the following:

LEMMA 6.9. *Let τ and α be fixed. If $q \geqslant 43$ and is odd, then there exist coefficients β, γ, δ and η such that there are at least 7 distinct irreducibles of the form*

$$x^7+\tau x^6+\alpha x^5+\beta x^4+\gamma x^3+\delta x^2+\varepsilon_i x+\eta.$$

Proof. Suppose not, then for each quadruple $(\beta, \gamma, \delta, \eta)$, we would have at most 6 irreducibles of the desired form. By Corollary 3.11 we would then have that

$$(q^5-q^3)/7 \leqslant 6q^3(q-1) \quad \text{(observe } \eta \neq 0\text{)}$$

$$\Leftrightarrow q^5-q^3 \leqslant 42q^4-42q^3 \Leftrightarrow q^5-42q^4+41q^3 \leqslant 0 \Rightarrow q < 42.$$

This is a contradiction. ∎

Now suppose that $q \geqslant 207$ and $p \neq 5$ and that

$$M-x = x^7+\tau x^6+(\alpha+1)x^5+\beta' x^4+\gamma' x^3+\delta' x^2+\varepsilon' x+\eta'.$$

Let $(\beta, \gamma, \delta, \eta)$ be as guaranteed by Lemma 6.9, then we have at least 7 distinct irreducibles $P_{1,i}$ $(1 \leqslant i \leqslant 7)$ of the form

$$P_{1,i} = x^7+\tau x^6+\alpha x^5+\beta x^4+\gamma x^3+\delta x^2+\varepsilon_i x+\eta,$$

so that

$$M-x-P_{1,i} = x^5+(\beta'-\beta)x^4+(\gamma'-\gamma)x^3+(\delta'-\delta)x^2+(\varepsilon'-\varepsilon_i)x+(\eta'-\eta)$$
$$= x^5+bx^4+cx^3+dx^2+e_i x+g.$$

From the set $\{e_i\}_{i=1}^7$ select one e_k which is not equal to any of the 6 numbers in Lemma 6.6. Set $e = e_k$ and $P_1 = P_{1,k}$. Now $f(x) = M-x-P_1$ satisfies all hypotheses of Lemma 6.6, and so Theorem 6.8 applies, $f(x)-\omega$ is irreducible, and we have written $M = P_1+(f(x)-\omega)+(x+\omega)$. Thus,

THEOREM 6.10. *Let $q \geqslant 207$, q odd, and $p \neq 5$. Then every 7th degree polynomial over k_q is a 3-primes polynomial.* ∎

If we now use the fact that q_7 as in the Hayes Theorem is 479 (see [5] or [11]), and that there is no power of 5 between 207 and 479, we may conclude:

COROLLARY 6.11. *Let $q \geqslant 207$ and odd. Then every 7th degree polynomial over k_q is a 3-primes polynomial.* ∎

Finally, we remark that for the case $n = 6$, we obtain $E_1 \geqslant (44/6)\sqrt{q}$, so that $q \geqslant 44^2 = 1936$, which far exceeds the Hayes bound of $q \geqslant 137$ for 8th degree polynomials. Hence the techniques of Sections 5 and 6 fail to give us useful results for all $n \geqslant 6$.

7. Completing the solution for 6th degree polynomials. In Section 6 we proved that every polynomial of degree 6 over k_q is a 3-primes polynomial provided that q is odd and greater than or equal to 19. To finish the problem for odd q, we have left to check the cases $q = 3, 5, 7, 9, 11, 13, 17$. For this we turn to the computer and analyze 4th degree polynomials over these fields. The idea, as usual, is: starting with arbitrary M of degree 6, subtract off P_1 of degree 6 with appropriate first and second coefficient so that $M-P_1$ is (monic) of degree 4. We then show that we can obtain P_2 of degree 4 with appropriate 1st, 2nd, *and* 3rd coefficient so that $M-P_1-P_2$ is monic and linear, hence irreducible.

Hence we wish now to study the distribution of 4th degree irreducibles with respect to their 1st *three* coefficients. Because q is odd, we may always translate by $\tau/4$ and hence it suffices to study polynomials with trace = 0. We are interested in the question: given some fixed element $\alpha \in k_q$, what is the distribution of 3rd coefficients of irreducibles with 1st coefficient 0 and 2nd coefficient α? We first observe that this distribution depends only on the quadratic nature of α.

LEMMA 7.1. *Let $k_q = \{\beta_i\}_{i=1}^q$. Suppose that there are $n(\alpha, \beta_i)$ irreducible 4th degree polynomials with trace = 0, 1st coefficient α, and 2nd coefficient β_i. If α_1 and α_2 have the same quadratic character, then $\{n(\alpha_1, \beta_i)\}_{i=1}^q = \{n(\alpha_2, \beta_i)\}_{i=1}^q$.*

Proof. For any i, let $\{t_{ij}\}_{j=1}^{4n(\alpha_1,\beta_i)}$ be the collection (possibly empty) of elements of k_{q^4} which have minimum polynomial over k_q of the form $x^4+a_1x^2+\beta_i x+\ldots$ If $\alpha_2 = a^2\alpha_1$ $(a \in k_q)$, then $\{a^{-1}t_{ij}\}_{j=1}^{4n(\alpha_1,\beta_i)}$ is exactly the collection with minimum polynomial of the form $x^4+a_2x^2+a^3\beta_i x+\ldots$ Hence,

$$n(\alpha_1, \beta_i) = n(\alpha_2, a^3\beta_i).$$

Since multiplying by a^3 is an automorphism of k_q, we are done. ∎

We now turn to the computer and obtain the following information on the distribution of 3rd coefficients of 4th degree irreducibles. We observe that except for the first number in each set (which represents the # of polynomials with 3rd coefficient = 0), the *order* of entries depends on the particular 2nd coefficient, but by the lemma the *set* of entries does not.

The table on p. 362 tells us, for example, that over k_3, if the 2nd coefficient $\alpha = 0$, then there are no irreducibles with third coefficient $\beta = 0$, one with $\beta = 1$, and one with $\beta = 2$. If $\alpha = 1$ (the only quadratic residue),

Table 1

The distribution of linear term coefficients for 4th degree irreducible polynomials with trace = 0 for $q = 3, 5, 7, 9, 11, 13, 17$

q	2nd coefficient = 0	2nd coefficient quadratic residue	2nd coefficient non-quadratic residue
3	$0+1+1=2$	$1+1+1=3$	$1+0+0=1$
5	$2+1+1+1+1=6$	$1+1+2+2+1=7$	$1+2+0+0+2=5$
7	$0+3+3+0++0+3+3=12$	$2+2+1+1+1+1+2=10$	$2+1+2+3+3+2+1=14$
9	$4+2+2+2++2+2+2++2+2=20$	$2+2+2+2+2+2+2+2++2=18$	$2+1+1+4+1+4+4+4++1=22$
11	$0+3+3+3++3+3+3++3+3+3++3=30$	$3+1+5+2+3+4+4+3++2+5+1=33$	$3+2+3+3+1+3+3+1++3+3+2=27$
13	$6+6+0+0++3+6+3++3+6+3++0+0+6==42$	$3+4+4+5+3+3+2+2++3+3+5+4+4=45$	$3+3+4+1+4+2+4+4++2+4+1+4+3=39$
17	$8+4+4+4++4+4+4++4+4+4++4+4+4++4+4+4++4=72$	$4+4+4+4+2+6+7+3++2+2+3+7+6+2+4++4+4=68$	$4+3+4+4+4+3+6+6++6+6+6+6+3+4+4++4+3=76$

then there is one irreducible for each β, and if $\alpha = 2$ (the only quadratic non-residue), then there is one with $\beta = 0$, and no others.

Observe also that the total in each row is predicted by Corollary 3.8. For example, since -1 and 2 are both quadratic non-residues mod 3, that result predicts

$$\frac{(q^2-1)}{4} = \frac{(9-1)}{4} = 2$$

irreducibles with $\alpha = 0$,

$$\frac{(q^2+q)}{4} = \frac{(9+3)}{4} = 3$$

for $\alpha = 1$, and

$$\frac{(q^2-q-2)}{4} = \frac{(9-3-2)}{4} = 1$$

for $\alpha = 2$.

We now go about completing the solution of the 3-primes problem for 6th degree polynomials over odd fields.

First let us suppose that $p \neq 3$.

We observe in Corollary 3.11 that if the characteristic of the field is not 2 or 3, then the orthogonal geometric techniques guarantee us that given τ and $\alpha \in k_q$, there exist at least $(q^4-q^2-2q-2)/6$ irreducible polynomials of degree 6 with 1st coefficient $= \tau$ and 2nd coefficient $= \alpha$. We now make use of this fact to dispose of the cases $q = 17, 13, 11, 7,$ and 5.

We start with an arbitrary

$$M = x^6+\tau x^5+(\alpha+1)x^4+\beta x^3+\gamma x^2+\delta x+\varepsilon.$$

Let $\mathscr{P} = \{$6th degree irreducibles with 1st coefficient $= \tau$ and 2nd coefficient $= \alpha\}$, so we know

$$\#\mathscr{P} \geqslant \frac{q^4-q^2-2q-2}{6}.$$

Hence there must exist a $\beta' \in k_q$ such that if $\mathscr{P}' = \{P(x) \in \mathscr{P} \mid P(x)$ has 3rd coefficient $= \beta'\}$, then

$$\#\mathscr{P}' \geqslant \frac{q^4-q^2-2q-2}{6q}.$$

Let $\mathscr{M} = \{M-P_1 \mid P_1 \in \mathscr{P}'\}$, i.e., $\mathscr{M}$ is some collection of polynomials of the form

$$x^4+(\beta-\beta')x^3+ax^2+bx+c \quad \text{for some } a, b, c \in k_q, \text{ and } \#\mathscr{M} = \#\mathscr{P}'.$$

We now look at the separate cases:

1. $q = 17$. Table 1, after translation by $(\beta-\beta')/4$ (Proposition 2.3), shows that for arbitrary a and $b \in k_{17}$, there exists an irreducible P_2 of the form $x^4+(\beta-\beta')x^3+ax^2+bx+c$ for some c. Hence we may pick *any* $P_1 \in \mathscr{P}'$ and then $M-P_1-P_2$ is (monic) linear.

2. $q = 13$. The table shows that after translation by $(\beta-\beta')/4$, there is a single value a_0 and 4 distinct values b_1, b_2, b_3, b_4 such that there is *no* irreducible of the form

$$x^4+(\beta-\beta')x^3+a_0x^2+b_ix+\ldots$$

But in $\mathscr{M}$ there could be *at most* $1\cdot4\cdot(q-1) = 48$ polynomials of this form, whereas $\#\mathscr{M} \geqslant 363$, so we may pick a $P_1 \in \mathscr{P}'$ *not* of the above form, and now there is an appropriate P_2 of degree 4 such that $M-P_1-P_2$ is (monic) linear.

3. $q = 11$. The table shows that a single value a_0 paired with a single value b_0 which must be avoided. But there are at most $q-1 = 10$ such

elements of $\mathscr{M}$, and $\#\mathscr{M} \geqslant 219$. Hence we may pick $P_1 \in \mathscr{P}'$ not having a_0 and b_0 as quadratic and linear coefficients respectively, and so there exists an appropriate irreducible P_2 such that $M-P_1-P_2$ is linear.

4. $q = 7$. Just as in the above two cases, $1 \cdot 3 \cdot (q-1) = 18$ polynonomials at most must be avoided, but $\#\mathscr{M} \geqslant 55$.

5. $q = 5$. Here it is close but still okay. There are 2 quadratic coefficients each paired with two linear coefficients which must be avoided, so there are at most $2 \cdot 2 \cdot (q-1) = 16$ elements of $\mathscr{M}$ which are bad, but $\#\mathscr{M} \geqslant 19$.

We now turn to the case $p = 3$.

6th degree irreducibles distribute themselves differently over fields of characteristic 3. However, we showed in Corollary 3.11 that the minimum number of irreducibles with prescribed 1st and 2nd coefficients was $(q^4-q^3-q^2-q)/6$.

1. $q = 9$. The table shows that there are no "holes" in 4th degree irreducibles over k_9, so the existence of a single 6th degree irreducible with prescribed 1st and 2nd coefficients suffices (as in the case $q = 17$ above). Since we certainly have this, we are done.

2. $q = 3$. The techniques used above fail in this case because there are too many "holes" in the 4th degree irreducibles over k_3. Instead, we return to the computer and look at the distribution of 6th degree irreducibles over k_3.

The computer confirms the following:

FACT 1. For every τ, α, $\beta \in k_3$, there are at least 2 distinct γ_1 and $\gamma_2 \in k_3$ such that $x^6+\tau x^5+\alpha x^4+\beta x^3+\gamma_i x^2+\delta x+\varepsilon$ is irreducible for some δ and ε *except* for the case $\tau = 0$, $\alpha = 1$, $\beta = 0$, in which case only $\gamma = 2$ gives rise to irreducibles. In this last case there are 3 irreducibles: x^6+x^4+2x+1, $x^6+x^4+2x^2+x+2$, and $x^6+x^4+2x^2+2x+2$.

We also have:

FACT 2. The 8 cubic irreducibles over k_3 are x^3+2x+1, x^3+2x+2; x^3+x^2+2, x^3+x^2+x+2, x^3+x^2+2x+1; x^3+2x^2+1, x^3+2x^2+x+1, x^3+2x^2+2x+2.

We now solve the problem for k_3:

Case 1. M (our given 6th degree polynomial) is *not* of the form $x^6+x^4+x^3+2x^2+ax+b$. Select irreducible P_1 such that

$$M-P_1 = x^3+\gamma' x^2+\delta' x+\varepsilon'$$

where $\gamma' \neq 0$ (possible since there are two choices for the appropriate quadratic term of P_1 — see Fact 1). Now select P_2 from the 6 possibilities in Fact 2 so that $M-P_1-P_2 = x+\varepsilon''$.

Case 2. $M = x^6+x^4+x^3+2x^2+ax+b$. Select P_1 from the 3 irreducibles listed in Fact 1 so that P_1 has a as linear coefficient. Hence $M-P_1 = x^3+b'$. Let $P_2 = x^3+2x+1$, then $M-P_1-P_2 = x+b''$.

We can finally conclude:

THEOREM 7.2. *If q is odd, then every 6th degree polynomial over k_q is a 3-primes polynomial.* ∎

If we now combine Theorem 2.5, Theorem 4.1, Theorem 4.4, Theorem 6.5, Corollary 6.11, and Theorem 7.2, we have finally a proof of Theorem 1.1, which was our goal.

References

[1] E. Artin, *Geometric algebra*, Interscience Publishers, New York 1957.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. 5 (1959), pp. 417–423.

[3] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York 1966.

[4] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), pp. 255–271.

[5] G. Effinger, *A Goldbach problem for polynomials over finite fields*, Ph. D. thesis, University of Massachusetts, 1981.

[6] A. Fröhlich, ed., *Algebraic number fields*, Academic Press, London 1977.

[7] L. J. Goldstein, *Analytic number theory*, Prentice-Hall, Englewood Cliffs, N. J., 1971.

[8] D. R. Hayes, *The distribution of irreducibles in* GF[q, x], Trans. Amer. Math. Soc. 117 (1965), pp. 101–127.

[9] — *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11 (1966), pp. 461–488.

[10] — *The Galois group of x^n+x-t*, Duke Math. Journ. 40 (1973), pp. 459–461.

[11] — and G. Effinger, *Analytic additive number theory over finite fields*, in preparation.

[12] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

[13] D. E. Littlewood, *The theory of group characters*, Clarendon Press, Oxford 1950.

[14] J. S. Lomont, *Applications of finite groups*, Academic Press, New York 1959.

[15] P. Samuel, *Algebraic theory of numbers*, Hermann, Paris 1970.

[16] J. P. Serre, *Linear representations of finite groups*, Springer-Verlag, Berlin–Heidelberg–New York 1977.

[17] — *Local fields*, Springer-Verlag, Berlin–Heidelberg–New York 1979.

[18] A. Weil, *Sur les courbes algebriques et les variétés qui s'en deduisent*, Hermann, Paris 1948.

UNIVERSITY OF MASSACHUSETTS AT AMHERST AND BATES COLLEGE
Lewiston, Maine, USA

Received on 3.6.1981 (1256)