Bibliographie

[1] S. K. Gogia and I. S. Luthar, *The Brauer–Siegel theorem for algebraic function fields*, J. Reine Angew. Math. 299 (1978), 28–37.
[2] E. Inaba, *Number of divisor classes in algebraic function fields*, Proc. Japan Acad. 26 (1950), 1–4.
[3] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading 1970.
[4] R. E. MacRae, *On unique factorization in certain rings of algebraic functions*, J. Algebra 17 (1971), 243–261.
[5] M. L. Madan and D. J. Madden, *On the theory of congruence function fields*, Comm. Algebra 8 (17) (1980), 1687–1697.
[6] M. L. Madan and C. S. Queen, *Algebraic function fields of class number one*, Acta Arith. 20 (1972), 423–432.
[7] D. Mumford, *Abelian Varieties*, Tata Inst. of Fund. Res. Stud. in Math., Bombay, Oxford University Press, Bombay 1970.
[8] S. G. Vladut, *An exhaustion bound for algebraic-geometric codes*, Problemy Peredachi Informatsii 23 (1987), 28–41; = Problems Inform. Transmission 23 (1987), 22–38.
[9] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent, Variétés abéliennes et courbes algébriques*, Pub. Math. Univ. Strasbourg VII et VIII, Act. Sci. Ind. n° 1041 et 1064, Hermann & Cie, Paris 1948.
[10] – *Basic Number Theory*, Grundlehren Math. Wiss. 144, Springer, New York 1967.

EQUIPE C.N.R.S. "ARITHMÉTIQUE ET THÉORIE DE L'INFORMATION"
C.I.R.M.
Luminy Case 916
13288 Marseille Cedex 9, France
D.M.I.
ÉCOLE NORMALE SUPÉRIEURE
45, rue d'Ulm
75230 Paris Cedex 05, France

Reçu le 15.5.1989 (1932)

ACTA ARITHMETICA
LVI (1990)

On the splitting of primes in an arithmetic progression, II

by

M. Bhaskaran (Duncraig) and S. Venkataraman (Madras)

1. Introduction. Let k be a number field and suppose $p \in \mathbf{Q}$ is tamely ramified in k: $p = P_1^{e_1} P_2^{e_2} \dots P_r^{e_r}$, $p \nmid e_i$. In this paper we show that there exists a set of rational primes with positive density in an arithmetic progression whose splitting in k depends on the ramification indices and residue class degrees of the P_i's. This is an extension of the result in [1].

2. Some preliminary results

Lemma 1. *Let k be a number field and suppose K is the narrow class field of the normal closure $\bar{k}$. Let P be a prime in K and suppose $I = I(P|P \cap \mathbf{Q})$ is the inertia group of P over $\mathbf{Q}$. If Q is any prime unramified in K such that $\left[\frac{K/\mathbf{Q}}{Q}\right] \in I$, then $q = Q \cap \mathbf{Q}$ splits into positive principal prime divisors.* (This means that the prime ideals have generators whose images under all real embeddings of k are positive.)

This is proved for (Hilbert) class field in [4] (also in [2]).

This easily carries over to narrow class-fields.

Theorem A. *Let k be a normal number field in which a prime p ramifies with ramification index $e_p = p^r e'_p$, $p \nmid e'_p$. Let a be a primitive root modulo p^l. Then there is a t_0, $0 \leqslant t_0 \leqslant r$, with the following property: The set of primes $q \equiv a \pmod{p^l}$ which have degree $e'_p p^{t_0}$ and which split into positive principal prime ideals in k has positive density.*

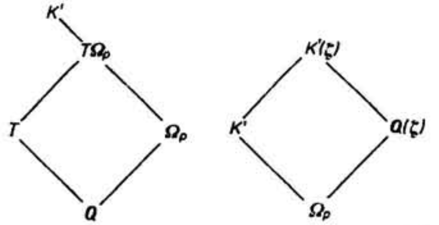
Proof. Let P be a prime ideal lying over p in the narrow class-field K of k. Let $I = I(P|p)$ be the inertia group of P over p and T the fixed field of the inertia group. Let V_1 be as usual,

$$V_1 = \{\sigma \in \mathrm{Gal}(K/\mathbf{Q}) |\ \sigma(\alpha) \equiv \alpha \pmod{P^2}\}.$$

Then V_1 is a normal subgroup of I and I/V_1 is cyclic. Let K' be the fixed field of V_1. Since V_1 is the p-Sylow subgroup of I, K'/T is a cyclic extension of degree e'_p. Let ζ denote a primitive p^l-th root of unity. Since T and $\mathbf{Q}(\zeta)$ are linearly disjoint,

$$\mathrm{Gal}(T(\zeta)/T) \cong \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}).$$

Let τ_a denote the automorphism such that $\tau_a(\zeta) = \zeta^a$, $\tau_a \in \mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$. Since τ_a generates $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$, $\tau_a|\Omega_p$ generates $\mathrm{Gal}(\Omega_p/\boldsymbol{Q})$ $(\Omega_p = K' \cap \boldsymbol{Q}(\zeta))$.



Now $T \cap \Omega_p = \boldsymbol{Q}$. Let σ_1 be an embedding of $T\Omega_p$ which restricts to identity on T and equals $\tau_a|\Omega_p$ on Ω_p. Then σ_1 generates $\mathrm{Gal}(T\Omega_p/T)$. There is a generator σ_p of $\mathrm{Gal}(K'/T)$ which restricts to σ_1. Now choose an embedding σ of $K'(\zeta)$ which restricts to σ_p on K' and to τ_a on $\boldsymbol{Q}(\zeta)$. Then $\sigma \in \mathrm{Gal}(K'(\zeta)/\boldsymbol{Q})$. The set of primes Q in T which have degree one over $\boldsymbol{Q}$ has density one. So the set (say) A of degree 1 primes in T which have σ as Frobenius automorphism has positive density. Now we have to prove that the primes $Q \in A$ are such that $q = Q \cap \boldsymbol{Q}$ satisfy the condition $q \equiv a \pmod{p^l}$. This follows from the fact that the Frobenius automorphism of q in $\boldsymbol{Q}(\zeta)$ is τ_a. Now suppose U is a prime in K' lying over $Q \in A$. Then $\left[\frac{K/Q}{U}\right]$ restricts to σ_p. So the order of the Frobenius automorphism $O\left(\left[\frac{K/Q}{U}\right]\right)$ (= degree of U over $Q \cap \boldsymbol{Q}$) is divisible by e_p. But since $Q \cap \boldsymbol{Q}$ splits completely into positive principal prime factors in k and Q has degree 1 over $\boldsymbol{Q}$, the degree of $q = Q \cap \boldsymbol{Q}$ is $O\left(\left[\frac{K/Q}{U}\right]\right) = e'_p p^t$, $0 \leqslant t \leqslant r$. Since there are only finitely many values of t and q's have positive density, there is a t_0 for which the corresponding q's have positive density.

Remark 1. If k_0 is a field such that k is its normal closure, then the primes of positive density in the above theorem have principal prime ideal factors in k_0. This follows from Lemma 1.

Main theorem

THEOREM 1. *Suppose p is an odd rational prime which is tamely ramified in a number field k: $p = P_1^{e_1} P_2^{e_2} \ldots P_s^{e_s}$, $p \nmid e_i$, where P_i $(i = 1, \ldots, s)$ are prime ideals of k of residue class degree f_i. Then there exists an infinite set of rational primes q of positive density in the arithmetic progression $a \pmod{p^l}$ (a being a primitive root $\bmod p^l$) which split in the following manner:*

$$q = \prod_{i=1}^{s} \prod_{j=1}^{f_i} Q_{ij}$$

where each Q_{ij} is of degree e_i and is a positive principal prime ideal.

Proof. Since p is tamely ramified in k it is tamely ramified in $\bar{k}$. It is tamely ramified in K too. Therefore, with notation as in the previous lemma, we see that $V_1 = \{1\}$ and $I(P|p)$ is cyclic and $K = K'$. Let Q be a prime in A and $\mathfrak{M}$ a prime in K lying over Q. Then the Frobenius automorphism of $\mathfrak{M}$ with respect to Q is the generator of the inertia group $I(P|p)$. Consider $\mathfrak{M} \cap \bar{k} = \mathfrak{B}$. Then the Frobenius automorphism of $\mathfrak{B}$ over $\mathfrak{B} \cap \boldsymbol{Q}$ is the generator of the inertia group $I(\mathfrak{P}|\mathfrak{P} \cap \boldsymbol{Q})$, where $\mathfrak{P} = P \cap \bar{k}$. Fix a $q = Q \cap \boldsymbol{Q}$, $Q \in A$. Then the decomposition group of $\mathfrak{B}$ over q = Inertia group of $\mathfrak{P}$ over p, i.e., $D(\mathfrak{B}|\mathfrak{B} \cap \boldsymbol{Q}) = I(\mathfrak{P}|p)$. Let $f(\mathfrak{a}|\boldsymbol{Q})$ denote the residue class degree of a prime ideal $\mathfrak{a}$ in k over $\boldsymbol{Q}$. Then

$$f(\mathfrak{B} \cap k|\boldsymbol{Q}) = \left|\frac{D(\mathfrak{B}|q)}{D(\mathfrak{B}|\mathfrak{B} \cap k)}\right| = \left|\frac{I(\mathfrak{P}|p)}{I(\mathfrak{P}|\mathfrak{P} \cap k)}\right|$$

since

$$D(\mathfrak{B}|\mathfrak{B} \cap k) = D(\mathfrak{B}|q) \cap \mathrm{Gal}(\bar{k}/k) = I(\mathfrak{P}|p) \cap \mathrm{Gal}(\bar{k}/k) = I(\mathfrak{P}|\mathfrak{P} \cap k).$$

Here, if $\mathfrak{P} \cap k = P_1$, then $f(\mathfrak{B} \cap k|q) = e_1$. Consider now $\sigma(\mathfrak{B})$. Since

$$D(\sigma(\mathfrak{B})|q) = \sigma D(\mathfrak{B}|q)\sigma^{-1} = \sigma I(\mathfrak{P}|p)\sigma^{-1} = I(\sigma(\mathfrak{P})|p),$$

if $\sigma(\mathfrak{P}) \cap k$ is P_i, then

$$f(\sigma(\mathfrak{B}) \cap k|q) = e_i.$$

Let

$$H = \mathrm{Gal}(\bar{k}/k) \quad \text{and} \quad \Phi = \Phi(\mathfrak{B}|q) = \left[\frac{\bar{k}/\boldsymbol{Q}}{\mathfrak{B}}\right].$$

Consider the orbits of the cosets of H in G under the action of Φ:

$$\{Hg_1, Hg_1\Phi, \ldots, Hg_1\Phi^{m_1-1}\},$$
$$\{Hg_2, Hg_2\Phi, \ldots, Hg_2\Phi^{m_2-1}\}, \ldots, \{Hg_n, \ldots, Hg_n\Phi^{m_n-1}\}.$$

We know that q splits as $q = \mathfrak{B}_1 \ldots \mathfrak{B}_n$ in k where $\mathfrak{B}_i = g_i(\mathfrak{B}) \cap k$ and $m_i = f(\mathfrak{B}_i|q)$ (cf. [3], Theorem 33). Now, choose $\sigma_1, \sigma_2, \ldots, \sigma_s$ such that $\sigma_i(\mathfrak{P}) \cap k = P_i$. For a fixed i, let $\sigma_i(\mathfrak{P}) = \hat{\mathfrak{P}}$ and $\sigma_i(\mathfrak{B}) = \hat{\mathfrak{B}}$. We know that $f(\hat{\mathfrak{B}} \cap k|\boldsymbol{Q}) = e_i$. Let us consider

$$\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}.$$

Since

$$\left|\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)}\right| = \left|\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}\right| \left|\frac{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}{D(\hat{\mathfrak{B}}|q)}\right|,$$

$$\frac{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}{D(\hat{\mathfrak{B}}|q)} \cong \frac{D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}{D(\hat{\mathfrak{B}}|q) \cap D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)} = \frac{D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}{D(\hat{\mathfrak{B}}|\hat{\mathfrak{B}} \cap k)},$$

it follows that

$$\left|\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}\right| = \left|\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)}\right| \div \left|\frac{D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}{D(\hat{\mathfrak{B}}|\hat{\mathfrak{B}} \cap k)}\right| = f(\hat{\mathfrak{P}} \cap k|q) = f_i.$$

Let $\tau_1, \ldots, \tau_{f_i}$ be a set of coset representatives of

$$\frac{D(\hat{\mathfrak{P}}|p)}{D(\hat{\mathfrak{B}}|q)D(\hat{\mathfrak{P}}|\hat{\mathfrak{P}} \cap k)}.$$

Consider the f_i orbits

$$\{H\tau_1\sigma_i, H\tau_1\sigma_i\Phi, \dots, H\tau_1\sigma_i\Phi^{e_i-1}\},$$
$$\{H\tau_2\sigma_i, H\tau_2\sigma_i\Phi, \dots, H\tau_2\sigma_i\Phi^{e_i-1}\}, \dots, \{H\tau_{f_i}\sigma_i, \dots, H\tau_{f_i}\sigma_i\Phi^{e_i-1}\}.$$

We claim that they are distinct. Suppose $H\tau_u\sigma_i = H\tau_v\sigma_i\Phi^j$. Then

$$\tau_u\sigma_i = h\tau_v\sigma_i\Phi^j$$

which means

$$\tau_u\sigma_i\Phi^{-j}\sigma_i^{-1}\tau_v^{-1} = \tau_u\tau_v^{-1}(\tau_v\sigma_i\Phi^{-j}\sigma_i^{-1}\tau_v^{-1}) = h.$$

But $\tau_v\sigma_i\Phi^{-j}\sigma_i^{-1}\tau_v^{-1} \in D(\mathfrak{B}|q)$ since $D(\mathfrak{B}|q)$ is normal in $D(\mathfrak{P}|p)$. So τ_u and τ_v are in the same coset, contradicting our choice of τ_i's. Notice that $\tau_u\sigma_i\Phi^j(\mathfrak{P}) = \sigma_i(\mathfrak{P}) = \mathfrak{P}$. So the primes corresponding to these orbits will have degree e_i.

To complete the proof we have to show that any coset $H\sigma$ is of the form $H\tau_k\sigma_i\Phi^j$ for some i.

Suppose $\sigma(\mathfrak{P}) \cap k = P_i = \sigma_i(\mathfrak{P}) \cap k$. Then there exists $h \in \mathrm{Gal}(\bar{k}/k)$ such that

$$h\sigma(\mathfrak{P}) = \sigma_i(\mathfrak{P}), \quad \text{i.e.} \quad \sigma_i^{-1}h\sigma(\mathfrak{P}) = \mathfrak{P}.$$

Therefore

$$\sigma_i^{-1}h\sigma = \tau, \quad \tau \in D(\mathfrak{P}|p),$$

which means

$$h\sigma = \sigma_i\tau = \sigma_i\tau\sigma_i^{-1}\sigma_i.$$

Now $\sigma_i\tau\sigma_i^{-1} \in D(\mathfrak{P}|p)$. Therefore there is an h' such that

$$\sigma_i\tau\sigma_i^{-1} = h'\sigma_i\Phi^w\sigma_i^{-1}\tau_k$$

which means $h\sigma = h'\sigma_i\Phi^w\sigma_i^{-1}\tau_k\sigma_i = h'\tau_k\sigma_i\Phi^s\sigma_i^{-1}\sigma_i$ (since $D(\mathfrak{B}|q)$ is normal in $D(\mathfrak{P}|p)) = h'\tau_k\sigma_i\Phi^s$. Hence

$$H\sigma = H\tau_k\sigma_i\Phi^s.$$

This completes the proof.

Acknowledgement. This paper was prepared during a short visit of the first author to the Institute of Mathematical Sciences at Madras. He wishes to thank the institute for its hospitality. The authors thank Dr. R. Balasubramanian for the interest shown in this work.

References

[1] M. Bhaskaran, *On the splitting of primes in an arithmetic progression I*, J. Madras Univ., B, 51 (1988), 170–172.
[2] — *Some applications of Tchebotarev density theorem*, Proc. Ramanujan Centennial Inter. Conf., Annamalainagar 1987, 77–84.
[3] D. A. Marcus, *Number Fields*, Universitext, Springer, 1977.
[4] C. J. Parry, *On a problem of Schinzel concerning principal divisors in arithmetic progressions*, Acta Arith. 19 (1971), 215–227.

48, Nalpa Way
Duncraig 6023
Western Australia
THE INSTITUTE OF MATHEMATICAL SCIENCES
Madras–600 113
India

Received on 29.5.1989 (1939)

ACTA ARITHMETICA
LVI (1990)

Polynomials with high multiplicity

by

Francesco Amoroso (Pisa)

0. Introduction. Let S be a non-empty finite subset of C^n. Following Waldschmidt (see [W2], § 1.3e)) we define $\omega_M(S)$ as the minimum degree of an algebraic hypersurface having a singularity of order $\geqslant M$ at any point of S. We are looking for inequalities between $\omega_1(S)$ and $\omega_M(S)$, $M > 1$. Trivially, we have

$$\frac{1}{M}\omega_M(S) \leqslant \omega_1(S). \tag{1}$$

In the opposite sense, using powerful tools from complex analysis, Waldschmidt proved

$$\frac{1}{n}\omega_1(S) \leqslant \frac{1}{M}\omega_M(S) \tag{2}$$

(see [W2], § 7.5b)). The last inequality follows from Bombieri–Skoda's existence theorem, which in turn derives from some L^2-estimates and from existence theorems for the operator $\bar{\partial}$, due to Hörmander.

Weaker results of the following kind:

$$\frac{1}{c_n}\omega_1(S) \leqslant \frac{1}{M}\omega_M(S) \tag{2'}$$

where c_n is some constant greater than n, were obtained by Masser and Wüstholz independently (see [M] and [Wu]).

More recently, using deep arguments from projective geometry, Esnault and Viehweg (see [E–V]) have obtained the following improvement of (2):

$$\frac{\omega_1(S)+1}{n} \leqslant \frac{1}{M}\omega_M(S) \quad \text{for } n > 1.$$

A conjecture of J. P. Demailly asserts that one should have

$$\frac{\omega_1(S)+n-1}{n} \leqslant \frac{1}{M}\omega_M(S) \quad \text{for } n \geqslant 1.$$

In this paper we give some results of the type (2′) in the ring $\boldsymbol{Z}[x_1, \dots, x_n]$ with explicit bounds for the height of the polynomials.