New York Journal of Mathematics

New York J. Math. **21** (2015) 715–721.

A prime number theorem for finite Galois extensions

Andrew J. Hetzel and Eric B. Morgan

Abstract. Let F be an algebraic number field and let $\mathcal{P}_F(r)$ denote the number of nonassociated prime elements of absolute field norm less than or equal to r in the corresponding ring of integers. Using information about the absolute field norms of prime elements and Chebotarev's density theorem, we readily show that when F is a Galois extension of $\mathbb{Q}$, it is the case that $\mathcal{P}_F$ is asymptotic to $\frac{1}{h}\pi$, where π is the standard prime-counting function and h is the class number of F. Along the way, we pick up some well-known facts on the realizability of certain prime numbers in terms of those binary quadratic forms associated with the field norm over a ring of integers that is a unique factorization domain.

Contents

1. Introduction

Since the establishment of the prime number theorem (PNT) in 1896 by Jacques Hadamard [2] and Charles Jean de la Vallée-Poussin [8], mathematicians have sought to develop analogues of PNT in other venues where the notion of "prime element" is well-defined. In fact, analogues of PNT have been produced all the way from algebraic function fields in one variable over a finite field [3] to additive number systems [1] to geodesics on a compact surface with a Riemannian metric of curvature -1 [5]. However, for the classical context of rings of integers of algebraic number fields, the standard analogue of PNT, due to Edmund Landau [4], has been the "prime ideal theorem": in a ring of integers $\mathfrak{O}$ of an algebraic number field, the number of prime ideals of $\mathfrak{O}$ grows asymptotically as π, the standard prime-counting

Received July 16, 2015.

2010 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11D57, 11R11, 11R45.

Key words and phrases. Binary quadratic form, Chebotarev's density theorem, field norm, Galois extension, prime number theorem.

This work is based in part on the second-named author's master's research at Tennessee Tech University.

ISSN 1076-9803/2015

function. While such an analogue concerns prime elements in the context of the groups of divisors of such rings, it does not directly address prime elements in the rings themselves, that is, elements $\alpha \in \mathfrak{O}$ with the property that for all $\beta, \gamma \in \mathfrak{O}$, it is the case that $\alpha \,|\, \beta\gamma \to \alpha \,|\, \beta$ or $\alpha \,|\, \gamma$.

In this short note, we seek to partially remedy this issue by establishing a similar asymptotic result as in the prime ideal theorem for a function $\mathcal{P}_F(r)$ that counts the number of nonassociated prime *elements* of absolute field norm $\leq r$ in a given ring of integers $\mathfrak{O}$ of a finite Galois extension F of $\mathbb{Q}$. Most certainly, $\mathcal{P}_F(r)$ is bounded above by the number of prime ideals of $\mathfrak{O}$ of norm $\leq r$, where the norm of the prime ideal $\mathcal{P}$ of $\mathfrak{O}$ is defined to be the cardinality of the factor ring $\mathfrak{O}/\mathcal{P}$. However, our main theorem, Theorem 2.9, reveals that in fact $\mathcal{P}_F$ is asymptotic to $\frac{1}{h}\pi$, where h is the class number of F. Along the way, we pick up several well-known facts about field norms and certain binary quadratic forms.

2. Results

We begin with a proposition that provides the essential information on field norms for the achievement of the titular goal of this paper.

Proposition 2.1. *Let $F/\mathbb{Q}$ be a finite field extension with corresponding field norm N and let $\mathfrak{O}$ be the ring of integers of F. Let $\alpha \in \mathfrak{O}$. If $|N(\alpha)| = p$, where p is a prime, then α is a prime element of $\mathfrak{O}$. Conversely, if α is a prime element of $\mathfrak{O}$, then for some prime p, it must be the case that $|N(\alpha)| = p^m$, where m is a positive divisor of the degree of the normal closure of F over $\mathbb{Q}$. Moreover, if $F/\mathbb{Q}$ is itself a Galois extension, this p uniquely determines m and uniquely determines α up to conjugates, in the sense that if β is a prime element of $\mathfrak{O}$ such that $|N(\beta)| = p^r$ for some natural number r, then $r = m$ and β is a conjugate of α.*

Proof. Let $\alpha \in \mathfrak{O}$ and suppose that $|N(\alpha)| = p$ for some prime p. Note that $|N(\alpha)| = |\mathfrak{O}/\alpha\mathfrak{O}|$ and that $\alpha\mathfrak{O} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \cdots \mathcal{P}_s^{e_s}$, where $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_s$ are distinct prime ideals of $\mathfrak{O}$ and the e_i's are natural numbers. But then $p = \Pi_{i=1}^{s} |\mathfrak{O}/\mathcal{P}_i^{e_i}|$, whence $s = 1$ and $e_1 = 1$. Therefore, α is a prime element of $\mathfrak{O}$.

The "conversely" statement follows from basic information concerning inertial degrees within Galois extensions and the "moreover" statement follows from the fact that any two principal prime ideals of $\mathfrak{O}$ the lie above the same prime p must be Galois conjugates of each other. □

We pause briefly in the next several results to consider the special situation of Galois extensions of prime degree, particularly where the corresponding ring of integers is a unique factorization domain. In this context, Corollary 2.2 below reveals that the prime elements of such a ring of integers may be completely characterized in terms of the absolute value of the associated field norm.

Corollary 2.2. *Let $F/\mathbb{Q}$ be a Galois extension of prime degree with corresponding field norm N and let $\mathfrak{O}$ be the ring of integers of F. Let $\alpha \in \mathfrak{O}$. If α is a prime element of $\mathfrak{O}$, then one of the following must hold:*

(1) *$|N(\alpha)|$ is prime.*
(2) *$\alpha = pu$, where u is a unit of $\mathfrak{O}$ and p is a prime not of the form $|N(\beta)|$ for some $\beta \in \mathfrak{O}$.*

If $\mathfrak{O}$ is further assumed to be a unique factorization domain, then the converse is true, as well.

Proof. Put $q = [F : \mathbb{Q}]$. For the forward direction, by Proposition 2.1, it suffices to show that if α is a prime element of $\mathfrak{O}$ such that $|N(\alpha)| = p^q$, where p is prime, then $\alpha = pu$, where u is a unit of $\mathfrak{O}$, and p is not of the form $|N(\beta)|$ for some $\beta \in \mathfrak{O}$. Let α be such an element. Since the inertial degree of p in $\mathfrak{O}$ must be q, it follows that p is inert in $\mathfrak{O}$. As such, $p\mathfrak{O} = \alpha\mathfrak{O}$, and we have that $\alpha = pu$, where u is a unit of $\mathfrak{O}$. Moreover, if $p = |N(\beta)|$ for some $\beta \in \mathfrak{O}$, then the above proposition asserts that β would be a prime element of $\mathfrak{O}$. But then the inertial degree of p in $\mathfrak{O}$ would be 1 and not q.

For the converse, assume further that $\mathfrak{O}$ is a unique factorization domain. By the above proposition, it suffices to show that if $\alpha \in \mathfrak{O}$ meets condition (2) of the corollary, then α is a prime element of $\mathfrak{O}$. Suppose that α is such an element. If α is not prime, then by the assumption on $\mathfrak{O}$, it is reducible. Moreover, $\alpha = \pi_1\pi_2 \cdots \pi_s$, where each π_i is prime and $s \geq 2$. Then $\pm p^q = N(\alpha) = \Pi_{i=1}^{s} N(\pi_i)$. By the first part of the corollary, it must be the case that, for any given π_i, either $|N(\pi_i)| = p$ or $\pi_i = pu$ for some unit u in $\mathfrak{O}$. However, if $\pi_i = pu$ for some unit u in $\mathfrak{O}$, then $N(\pi_i) = \pm p^q$, whence $s = 1$. Thus, for each $i = 1, 2, \ldots, s$, we must have that $|N(\pi_i)| = p$, a contradiction to the hypothesis on p given in condition (2). Therefore, α must be a prime element of $\mathfrak{O}$. □

In the further specialized circumstance of rings of integers that are unique factorization domains in quadratic extensions over $\mathbb{Q}$, Proposition 2.3 shows that for almost all prime numbers, the property of being a quadratic residue is sufficient to guarantee that the prime number is of the first type indicated in Corollary 2.2. For the sake of generality, Proposition 2.3 is couched in terms of "prime integers", which are simply prime elements in the ring $\mathbb{Z}$.

Proposition 2.3. *Let $\mathfrak{O}$ be the ring of integers of a quadratic algebraic number field with radicand D and p be a (possibly negative) prime integer such that $(p, D) = 1$.*

(a) *If $p = N(\alpha)$ for some $\alpha \in \mathfrak{O}$, then p is a quadratic residue modulo $|D|$.*
(b) *If $D \equiv 3 \pmod 4$ and p is an odd prime for which $p = N(\alpha)$ for some $\alpha \in \mathfrak{O}$, then p is a quadratic residue modulo $4|D|$.*

If $\mathfrak{O}$ is further assumed to be a unique factorization domain and p a (possibly negative) prime integer such that $|p| > |D|$, then we have the following:

(c) *If* $D \equiv 1 \pmod 4$ *and* p *is a quadratic residue modulo* $|D|$*, then* $|p| = |N(\alpha)|$ *for some* $\alpha \in \mathfrak{O}$*.*
(d) *If* $D \equiv 2 \pmod 4$ *and* p *is a quadratic residue modulo* $4|D|$*, then* $|p| = |N(\alpha)|$ *for some* $\alpha \in \mathfrak{O}$*.*
(e) *If* $D \equiv 3 \pmod 4$ *and* p *is a quadratic residue modulo* $4|D|$*, then* $|p| = |N(\alpha)|$ *for some* $\alpha \in \mathfrak{O}$*.*

Proof. (a),(b) Straightforward.

(c) Observe that quadratic reciprocity guarantees that D is a quadratic residue modulo $|p|$. As such, p is not a prime element of $\mathfrak{O}$. Since $\mathfrak{O}$ is a unique factorization domain, p is reducible, whence there exist nonunits $\alpha, \beta \in \mathfrak{O}$ such that $p = \alpha\beta$. But then $p^2 = N(p) = N(\alpha)N(\beta)$, and the result follows.

(d),(e) These proofs are similar to the proof of part (c). □

From Proposition 2.3, we readily obtain a well-known result concerning the representability of certain prime numbers in terms of particular binary quadratic forms.

Corollary 2.4. *Let* p *be a prime. Then we have the following:*

(a) $p = a^2 + b^2$ *for some* $a, b \in \mathbb{Z}$ *if and only if either* $p = 2$ *or* p *is a quadratic residue modulo* 4*.*
(b) $p = a^2 + 2b^2$ *for some* $a, b \in \mathbb{Z}$ *if and only if either* $p = 2$ *or* $p \equiv 1, 3 \pmod 8$*.*
(c) *For each of* $D = 3, 7, 11, 19, 43, 67, 163$*, we have that*

$$p = a^2 + ab + \frac{1+D}{4}b^2$$

for some $a, b \in \mathbb{Z}$ *if and only if either* $p = D$ *or* p *is a quadratic residue modulo* D*.*

Proof. Note that the (positive definite) binary quadratic forms indicated in the statement of the corollary correspond to the norms on $\mathfrak{O}_F$, where $F = \mathbb{Q}(\sqrt{D})$ with $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$, respectively. Moreover, it is well-known that each such ring of integers is a unique factorization domain (in fact, these are all the quadratic rings of integers with negative radicand that are unique factorization domains). Therefore, save a straightforward check that $|D|$ (or 2 in the case of $D = -1$), and all primes $p < |D|$ that are quadratic residues modulo $|D|$ (or $4|D|$ in the case of $D = -1$) are representable by the corresponding binary form, all parts except (b) follow from Proposition 2.3. The equivalence in (b), however, is well-known. □

We return now to the major goal of this paper, the asymptotics of the prime-counting function for finite Galois extensions of $\mathbb{Q}$. To this end, we provide the appropriate notation below.

Notation 2.5. Let $\mathfrak{O}_F$ be the ring of integers of an algebraic number field F and N the field norm for F. Let r be a positive real number. Then

$$\mathcal{P}_F(r) = |\{[\alpha] \mid \alpha \text{ is a prime element of } \mathfrak{O}_F \text{ and } |N(\alpha)| \leq r\}|$$

where the indicated equivalence class is determined by the associates equivalence relation. Less formally, $\mathcal{P}_F(r)$ will denote the number of nonassociated prime elements α of $\mathfrak{O}_F$ for which $|N(\alpha)| \leq r$.

Notation 2.6. Let $\mathfrak{O}_F$ be the ring of integers of an algebraic number field F over $\mathbb{Q}$ and N the field norm for F. Let r be a positive real number. Then $\mathcal{A}_F(r)$ will denote the number of primes p such that $|N(\alpha)| = p \leq r$ for some $\alpha \in \mathfrak{O}_F$, and $\mathcal{B}_F(r)$ will denote the number of primes p such that $|N(\alpha)| = p^m \leq r$, where $m > 1$, for some prime element $\alpha \in \mathfrak{O}_F$.

Exploiting the information on prime elements given in Proposition 2.1, Proposition 2.7 below provides some useful bounds on the $\mathcal{P}_F$ function.

Proposition 2.7. *Let $F/\mathbb{Q}$ be a Galois extension of degree n. Then there exists a positive constant C such that for all $r > 0$,*

$$n\,[\mathcal{A}_F(r) - C] \leq \mathcal{P}_F(r) \leq n\,[\mathcal{A}_F(r) + \mathcal{B}_F(r)]$$

Proof. Let α be a prime element of $\mathfrak{O}_F$ such that $|N(\alpha)| \leq r$. By Proposition 2.1, it must be the case that $|N(\alpha)| = p^m$ for some prime p and positive divisor m of n. Moreover, this p uniquely determines m and uniquely determines α up to conjugates. Since there are at most n pairwise nonassociated conjugates of α, we have that $\mathcal{P}_F(r) \leq n[\mathcal{A}_F(r) + \mathcal{B}_F(r)]$.

Now, also by Proposition 2.1, if p is a prime for which there exists $\alpha \in \mathfrak{O}_F$ such that $|N(\alpha)| = p$, then α is a prime element of $\mathfrak{O}_F$. Moreover, since $F/\mathbb{Q}$ is a Galois extension, such a p is either ramified or completely split as a product of exactly n principal prime ideals in $\mathfrak{O}_F$. Note that there are only finitely many primes that are ramified in F (in particular, p is ramified in F if and only if $p \,|\, \Delta_F$, where Δ_F is the discriminant of F). Put C equal to the number of ramified primes p for which $|N(\alpha)| = p$ for some $\alpha \in \mathfrak{O}_F$, so that for any r, the quantity $\mathcal{A}_F(r) - C$ is a lower bound on the number of primes $p \leq r$ that completely split as a product of n principal prime ideals in $\mathfrak{O}_F$. The inequality $n\,[\mathcal{A}_F(r) - C] \leq \mathcal{P}_F(r)$ now follows. □

One of the critical pieces of information that we will need for our main theorem is Chebotarev's density theorem [7], which we record below. While Chebotarev's density theorem was originally couched in terms of Dirichlet density, it is important to note that it is equally as valid for natural density (see [6, p. 31]). This fact allows for its utility here.

Chebotarev's Density Theorem. *Let $F/\mathbb{Q}$ be a finite Galois extension with Galois group G. Then for any conjugacy class C of G, the (natural) density of the set of primes p for which the Frobenius automorphism $\sigma_p \in C$ is $|C|/|G|$.*

Thanks to Chebotarev's density theorem, we may now give an asymptotic result for the $\mathcal{A}_F$ function in terms of the standard prime-counting function π and, consequently, the desired asymptotic result for the $\mathcal{P}_F$ function.

Proposition 2.8. *Let $F/\mathbb{Q}$ be a Galois extension of degree n. Then*

$$\mathcal{A}_F \sim \frac{1}{nh}\pi,$$

where h is the class number of F.

Proof. Let K be the Hilbert class field of F and let $\mathfrak{O}_F$ be the ring of integers of F. Note that K is Galois over $\mathbb{Q}$ of degree nh. Let $S(r)$ be the number of primes $p \leq r$ that completely split in K. Observe that if σ_p is the Frobenius automorphism for the prime p, then p is completely split in K if and only if σ_p is an element of the trivial conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$. As such, Chebotarev's density theorem implies that $S \sim \frac{1}{nh}\pi$.

Now, the Hilbert class field K has the property that a prime ideal $\mathcal{P}$ of $\mathfrak{O}_F$ is principal if and only if $\mathcal{P}$ splits completely in K. Furthermore, observe that an unramified prime p (in F) is counted by the $\mathcal{A}_F$ function if and only if p splits completely in F as a product of principal prime ideals of $\mathfrak{O}_F$. Thus, if C is equal to the number of ramified primes in F, then $\mathcal{A}_F(r) - C \leq S(r)$. Now, assume p is completely split in K. Then the inertial degree of p in $K/\mathbb{Q}$ must be 1, and so the inertial degree of any prime factor of p in F in K/F must also be 1. As such, since K/F is unramified, it must be the case that any prime factor of p in F is completely split in K, whence any prime factor of p in F must be principal. Combined with the fact that the inertial degree of p in $F/\mathbb{Q}$ is also necessarily 1, it follows that p is a prime counted by the $\mathcal{A}_F$ function. In particular, $S(r) \leq \mathcal{A}_F(r)$. Therefore, $\mathcal{A}_F \sim S \sim \frac{1}{nh}\pi$. □

Theorem 2.9. *Let $F/\mathbb{Q}$ be a finite Galois extension. Then*

$$\mathcal{P}_F \sim \frac{1}{h}\pi,$$

where h is the class number of F.

Proof. By Propositions 2.7 and 2.8, it suffices to show that $\mathcal{B}_F = o(\pi)$. However, by Proposition 2.1, it follows that $\mathcal{B}_F(r) \leq \pi(\sqrt{r})$ for all $r > 1$. Since the prime number theorem itself guarantees that

$$\lim_{r\to\infty} \pi(\sqrt{r})/\pi(r) = 0,$$

it must be the case that $\mathcal{B}_F = o(\pi)$, and the proof is complete. □

Acknowledgement. We wish to express our gratitude to the referee for his expert suggestions that greatly improved the quality of this paper.

References

[1] Forman, William; Shapiro, Harold N. Abstract prime number theorems. *Comm. Pure Appl. Math.* **7** (1954), 587–619. MR0063396 (16,114e), Zbl 0057.28404, doi: 10.1002/cpa.3160070308.

[2] Hadamard, J. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France* **24** (1896), 199–220. MR1504264, JFM 27.0154.01.

[3] Kruse, Margret; Stichtenoth, Henning. Ein Analogon zum Primzahlsatz für algebraische Funktionenkörper. *Manuscripta Math.* **69** (1990), no. 3, 219–221. MR1078353 (91j:11101), Zbl 0723.11059, doi: 10.1007/BF02567920.

[4] Landau, Edmund. Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes. *Math. Ann.* **56** (1903), no. 4, 645–670. MR1511191, JFM 34.0228.03, doi: 10.1007/BF01444310.

[5] Margulis, G. A. Certain applications of ergodic theory to the investigation of manifolds of negative curvature. *Funkcional. Anal. i Priložen.* **3** (1969), no. 4, 89–90. MR0257933 (41 #2582), Zbl 0207.20305, doi: 10.1007/BF01076325.

[6] Stevenhagen, P.; Lenstra, H. W., Jr. Chebotarëv and his density theorem. *Math. Intelligencer* **18** (1996), no. 2, 26–37. MR1395088 (97e:11144), Zbl 0885.11005, doi: 10.1007/BF03027290.

[7] Tschebotareff, N. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.* **95** (1926), no. 1, 191–228. MR1512273, JFM 51.0149.04, doi: 10.1007/BF01206606.

[8] de la Vallée-Poussin, Ch. J. Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles* **21** (1896), 183–256. JFM 27.0155.03.

(Andrew J. Hetzel) Department of Mathematics, Tennessee Tech University, Cookeville, TN 38505, USA
ahetzel@tntech.edu

(Eric B. Morgan) Department of Mathematics, Tennessee Tech University, Cookeville, TN 38505, USA
emorgan@tntech.edu

This paper is available via http://nyjm.albany.edu/j/2015/21-31.html.