Notes on Number Theory and Discrete Mathematics Print ISSN 1310–5132, Online ISSN 2367–8275 Vol. 24, 2018, No. 2, 55–62 DOI: 10.7546/nntdm.2018.24.2.55-62

Quotients of primes in an algebraic number ring

Brian D. Sittinger

Department of Mathematics, California State University Channel Islands 1 University Drive, Camarillo, CA 93010, United States e-mail: brian.sittinger@csuci.edu

Received: 23 June 2017

Accepted: 11 February 2018

Abstract: It has been established on many occasions that the set of quotients of prime numbers is dense in the set of positive real numbers. More recently, it has been proved that the set of quotients of primes in the Gaussian integers is dense in the complex plane. In this article, we not only extend this result to any imaginary quadratic number ring, but also prove that the set of quotients of primes in any real quadratic number ring is dense in the set of real numbers. To conclude, we show how to extend these results to an arbitrary algebraic number ring.

Keywords: Prime number, Prime ideal, Number ring.

2010 Mathematics Subject Classification: 11R04, 11R44, 11A41, 11N05.

1 Introduction

It is a standard fact from Real Analysis that \mathbb{Q} is a dense subset of \mathbb{R} . However, it is not as wellknown that the set of quotients of *prime* numbers is a dense subset of $\mathbb{R}_{>0}$. One of the earliest appearances of this fact is in Sierpiński's textbook on Number Theory [13]. This fact, along with a few variations of it, has been studied and explored in great detail through the years; see [1, 4, 6, 10, 15] for instance. These results are proved by using some variant of the Prime Number Theorem, which as a reminder we now state in its classic formulation below.

Proposition 1.1. If $\pi(x)$ denotes the number of prime numbers in \mathbb{N} less than or equal to some x > 0, then $\pi(x) \sim \frac{x}{\ln x}$. In other words, $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.

Recently, Garcia ([5]) established that the set of quotients of primes from the ring of *Gaussian* integers $\mathbb{Z}[i]$ is dense in \mathbb{C} by using a suitable generalization of the Prime Number Theorem to

 $\mathbb{Z}[i]$. We generalize his work by showing that the set of quotients of primes from any fixed imaginary quadratic ring is dense in \mathbb{C} . This method of proof also permits use to show with little effort that the set of quotients of primes belonging to a fixed congruence class of Gaussian integers is dense in \mathbb{C} .

After accomplishing this task, we turn our attention to real quadratic number rings, where we show that the set of quotients of primes from a given real quadratic ring is dense in \mathbb{R} . Finally, we show how to establish analogous density results for the set of quotients of primes from any algebraic number ring.

In this article, we refer to the prime numbers in \mathbb{N} as *rational primes*, in order to distinguish them from the prime elements in a given algebraic number ring.

2 Background on algebraic number rings

We first fix some notation for an algebraic number ring. For further details, check any textbook on Algebraic Number Theory, such as [9] and [16].

Let K denote an algebraic number field over \mathbb{Q} (that is, $[K : \mathbb{Q}] < \infty$) with \mathcal{O} being its corresponding number ring. In particular, a quadratic number field has the form $\mathbb{Q}(\sqrt{d})$ for any square-free integer d. Its ring of integers \mathcal{O} , called a *quadratic number ring*, is the set $\{a + b\omega : a, b \in \mathbb{Z}\}$, where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \mod 4\\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Although we do not necessarily have unique factorization into irreducible elements in \mathcal{O} , we do have unique factorization into prime *ideals* in \mathcal{O} . One way to 'measure' how far \mathcal{O} is from being a UFD is as follows: we set up an equivalence relation on the ideals in \mathcal{O} as follows: we say that two ideals a and b in \mathcal{O} are equivalent if there exist nonzero $\alpha, \beta \in \mathcal{O}$ such that $\langle \alpha \rangle \mathfrak{a} = \langle \beta \rangle \mathfrak{b}$. This equivalence partitions the ideals into disjoint ideal classes that form a finite abelian group called the *class group* of \mathcal{O} . Its cardinality is called the *class number* of \mathcal{O} and is denoted by h. For what we need, it should be noted that the trivial ideal class is the class of *principal* ideals, and thus \mathcal{O} is a UFD iff h = 1 (as all ideals in a UFD are principal). The trivial ideal class is of chief interest to us, because a generator of a principal prime ideal gives a prime element in \mathcal{O} .

3 Quotients of primes in an imaginary quadratic ring

In this section, we extend the density result for the Gaussian integers [5] to any imaginary quadratic number ring \mathcal{O} . To do this, we use the following 'angular' prime number theorem of Kubilius [8] and Hecke [2]. It states that any sector $\{z \in \mathbb{C} : \theta_1 < \arg z < \theta_2\}$ in the complex plane contains prime elements of arbitrarily large magnitude.

Proposition 3.1. Let \mathcal{O} be an imaginary quadratic number ring. Fix $0 \leq \theta_1 < \theta_2 \leq 2\pi$ and x > 0, and let $\Pi(x; \theta_1, \theta_2)$ denote the number of prime elements $\rho \in \mathcal{O}$ satisfying $|\rho|^2 \leq x$ and $\theta_1 < \arg \rho < \theta_2$. Then,

$$\Pi(x;\theta_1,\theta_2) \sim \frac{g(\theta_2 - \theta_1)}{2\pi h} \cdot \frac{x}{\ln x},$$

where g denotes the number of units in \mathcal{O} .

The presence of h in this prime number formula signifies that we are looking at the principal ideal class. Moreover, the significance of g follows from the fact that a generator of a principal ideal is unique up to multiplication by a unit in O.

A consequence of this proposition we will use is that if 0 < a < b, then for all sufficiently large real x, an annular sector

$$\{z \in \mathbb{C} : ax < |z|^2 < bx \text{ and } \theta_1 < \arg z < \theta_2\},\$$

contains a prime element in \mathcal{O} . This follows from straightforward calculus:

$$\lim_{x \to \infty} [\Pi(bx; \theta_1, \theta_2) - \Pi(ax; \theta_1, \theta_2)] = \lim_{x \to \infty} \Pi(bx; \theta_1, \theta_2) \left[1 - \frac{\Pi(ax; \theta_1, \theta_2)}{\Pi(bx; \theta_1, \theta_2)} \right]$$
$$= \lim_{x \to \infty} \Pi(bx; \theta_1, \theta_2) \left[1 - \frac{ax \ln(bx)}{bx \ln(ax)} \right]$$
$$= \left(1 - \frac{a}{b} \right) \lim_{x \to \infty} \Pi(bx; \theta_1, \theta_2)$$
$$= \infty.$$

Now, we state the desired variant of a prime number theorem to deduce the desired density result for any imaginary quadratic number ring.

Theorem 3.2. The set of quotients of primes in an imaginary quadratic ring O is dense in the complex plane.

Proof. It suffices to show that any annular sector

$$\{ z \in \mathbb{C} : \psi_1 < \arg z < \psi_2, \, 0 < r < |z| < R \}$$

contains a quotient of prime numbers in \mathcal{O} .

Fixing $\theta \in (0, 2\pi]$, since

$$\lim_{x \to \infty} \left[\Pi\left(\frac{x}{r^2}; 0, \theta\right) - \Pi\left(\frac{x}{R^2}; 0, \theta\right) \right] = \infty,$$

there exists $x_0 > 0$ such that

$$\Pi\left(\frac{x}{r^2}; 0, \theta\right) - \Pi\left(\frac{x}{R^2}; 0, \theta\right) \ge 2 \text{ for all } x \ge x_0.$$

Moreover, since the angular prime number theorem implies that there are infinitely many prime numbers in \mathcal{O} in the sector (ψ_1, ψ_2) , there exists a prime number π_1 in the sector (ψ_1, ψ_2) with sufficiently large magnitude $(|\pi_1|^2 > x_0)$ such that

$$\Pi\left(\frac{|\pi_1|^2}{r^2}; 0, \xi\right) - \Pi\left(\frac{|\pi_1|^2}{R^2}; 0, \xi\right) \ge 2,$$

where $\xi = \min\{\psi_2 - \arg(\pi_1), \arg(\pi_1) - \psi_1\}.$

Next, the inequality in the last assertion implies that there exists a prime number π_2 satisfying $\frac{|\pi_1|}{R} < |\pi_2| < \frac{|\pi_1|}{r}$ and $0 < \arg(\pi_2) < \xi$.

From this, it now follows that
$$r < \left|\frac{\pi_1}{\pi_2}\right| < R$$
 and $\psi_1 < \arg\left(\frac{\pi_1}{\pi_2}\right) < \psi_2$.

4 Quotients of Gaussian primes, revisited

Recall that the ring of *Gaussian integers* $\mathbb{Z}[i]$ is the set of integers in the field $\mathbb{Q}(i)$ and have the form a + bi where $a, b \in \mathbb{Z}$. This set is well-known to be a UFD with units $\pm 1, \pm i$. It can be shown (see [9] or [16]) that a nonzero Gaussian integer is a prime if and only if it is an associate of p (namely $\pm p$ and $\pm pi$) for some rational prime $p \equiv 3 \mod 4$, or it is of the form $a + bi \in \mathbb{Z}[i]$ where $a^2 + b^2$ is a rational prime. We refer to these primes as *Gaussian primes*.

Note that the proof of Theorem 3.2 applied to $\mathbb{Z}[i]$ does not rely on a specific type of a Gaussian prime, while the proof in [5] fixes the Gaussian prime in the denominator be a rational prime congruent to 3 mod 4. Although this latter idea simplifies the density proof a bit with regards to the argument of the prime, it does not allow for the denominator to be an associate of a Gaussian prime that is not a rational prime.

We exploit this distinction to show how flexible the techniques from our previous density proof is, as we can modify it to give a Gaussian integer analogue of the following fact [14]:

Proposition 4.1. Fix $a, b, m, n \in \mathbb{N}$ such that gcd(a, m) = gcd(b, n) = 1. Then,

$$\left\{\frac{p}{q}: p, q \text{ prime in } \mathbb{Z}, p \equiv a \text{ mod } m, \text{ and } q \equiv b \text{ mod } n\right\}$$

is dense in \mathbb{R} .

To state and prove this generalization, we note that the Gaussian integers have a notion of congruence as well. Fix $\gamma \in \mathbb{Z}[i]$; for $\alpha, \beta \in \mathbb{Z}[i]$ we write $\alpha \equiv \beta \mod \gamma$ iff $\gamma \mid (\beta - \alpha)$. With this notation, we can now state the following 'Dirichlet' variant of the prime number theorem [7].

Proposition 4.2. Fix $0 \le \theta_1 < \theta_2 \le 2\pi$ and x > 0, and let $\Pi(x; \theta_1, \theta_2; \beta, \gamma)$ denote the number of Gaussian primes $\rho \equiv \beta \mod \gamma$ satisfying $\theta_1 < \arg \rho < \theta_2$ and $|\rho|^2 \le x$. Then,

$$\Pi(x;\theta_1,\theta_2;\beta,\gamma) \sim \frac{4(\theta_2-\theta_1)}{2\pi\phi(\gamma)} \cdot \frac{x}{\ln x},$$

where $\phi(\gamma)$ denotes the number of invertible congruence classes modulo γ .

It should be noted that this proposition asserts that the Gaussian primes are equidistributed both by argument and by congruence class. Moreover, the ϕ function above is an extension of the Euler phi function to $\mathbb{Z}[i]$.

By adapting the proof of Theorem 3.2 with this variation of the prime number theorem, we immediately obtain the following result.

Theorem 4.3. Fix $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}[i]$ such that $gcd(\beta_1, \gamma_1) = gcd(\beta_2, \gamma_2) = 1$. Then, the set of quotients

$$\left\{\frac{\pi_1}{\pi_2}: \pi_1, \pi_2 \text{ are Gaussian primes}, \pi_1 \equiv \beta_1 \text{ mod } \gamma_1, \text{ and } \pi_2 \equiv \beta_2 \text{ mod } \gamma_2\right\}$$

is dense in \mathbb{C} .

5 Quotients of primes in a real quadratic number ring

In this section, suppose that \mathcal{O} is a real quadratic number ring. These rings are quite different than their imaginary counterparts. First, since a real quadratic number ring is a subset of \mathbb{R} , we will be stating a density statement in \mathbb{R} instead of \mathbb{C} . Secondly, a real quadratic number ring has *infinitely* many units. Fortunately, any such unit can be written in the form $\pm \eta^k$ for some integer k and fixed unit $\eta \in \mathcal{O}$ called a *fundamental unit* of \mathcal{O} . Without loss of generality, we may assume that $\eta > 1$.

There is a Prime Number Theorem for real quadratic number rings that dates back to the work of Hecke [2], but we will use the following refinement of Rademacher [12]. To state the theorem, we use the following definition: we say that $\alpha \in \mathcal{O}$ is *totally positive* if both α and its conjugate α' are positive. (Recall that for any $a, b \in \mathbb{Q}$, the conjugate of $a + b\sqrt{d}$ equals $a - b\sqrt{d}$.)

Proposition 5.1. Let \mathcal{O} be a real quadratic number ring. Fix x > 0, and let $\Pi(x)$ denote the number of totally positive prime elements $\rho \in \mathcal{O}$ satisfying $0 < \rho \leq x$. Then, we have

$$\Pi(x) \sim \frac{1}{2h\ln\eta} \int_2^x \int_2^x \frac{du\,dv}{\ln(uv)}.$$

It should be noted that the double integral is asymptotically equal to $\frac{x^2}{\ln(x^2)}$ [3]. By letting $x \to \infty$, this theorem shows that there are infinitely many totally positive prime elements in \mathcal{O} . Now, we use this result to readily establish the density of quotients of primes in \mathcal{O} .

Theorem 5.2. The set of quotients of primes in a real quadratic number ring \mathcal{O} is dense in \mathbb{R} .

Proof. We need to show that any given interval (a, b) contains a quotient of primes in \mathcal{O} . Assume without loss of generality that a, b > 0. Then it follows directly from Proposition 5.1 that

$$\lim_{x \to \infty} (\Pi(bx) - \Pi(ax)) = \infty.$$

This implies that for all sufficiently large x, there exists a prime $\pi_1 \in \mathcal{O}$ such that $ax < \pi_1 < bx$. Then, since there exist primes in \mathcal{O} with arbitrarily large magnitude by Proposition 5.1, let $x = \pi_2$ for some prime $\pi_2 \in \mathcal{O}$. This immediately yields $a < \frac{\pi_1}{\pi_2} < b$, as required.

Remark: An alternate proof suggested in private conversation with Garcia uses previous quotient set density theorems and bypasses the use of Proposition 5.1. As a trade-off, it does not allow for the possibility of using non-rational prime numbers to establish the density result and ultimately does not generalize to an arbitrary algebraic number ring. It relies on the following fact [9]:

Given a real quadratic number field $\mathbb{Q}(\sqrt{d})$ with d > 0 and square-free, an odd rational prime p remains prime in \mathcal{O} iff d is not a square modulo p.

By fixing d, this condition gives a set of congruences that p satisfies in terms of d. Pick one such congruence condition; by Dirichlet's Theorem on Arithmetic Progressions, there are infinitely many such primes. Applying Proposition 4.1 to this congruence condition yields Theorem 5.2.

6 Quotients of primes in an algebraic number ring

Now, suppose that K is an algebraic number field of degree n over \mathbb{Q} with ring of integers \mathcal{O} . Before proceeding further, we need to fix some more notation. Let n = s + 2t and r = s + t - 1, where s denotes the number of real embeddings and s denotes the number of pairs of complex embeddings of K. For an element $\omega \in \mathcal{O}$, let $\omega^{(j)}$ denote the image of ω under the *j*th embedding of K into Minkowski space $L_{s,t} = \mathbb{R}^s \times \mathbb{C}^t$ with j = 1, 2, ..., s + t. Without loss of generality, assume that the trivial real and complex embeddings give the first and (s + 1)-th entries of the ordered tuples in $L_{s,t}$.

Now, we are able to state a version of Mitsui's generalized Prime Number Theorem [11] suitable for our purpose.

Theorem 6.1. Fix $0 \le \theta_1 < \theta_2 \le 2\pi$, and let $\Pi(Y; \theta_1, \theta_2)$ denote the number of prime elements $\omega \in \mathcal{O}$ satisfying $|\omega^{(j)}| \le Y$ for each j = 1, ..., s + t and $\theta_1 < \arg(\omega^{(k)}) < \theta_2$ for each k = s + 1, ..., s + t. Then, for all $Y \ge 3$, we have

$$\Pi(Y;\theta_1,\theta_2) \sim \left(\frac{\theta_2 - \theta_1}{2\pi}\right)^t \frac{g}{2^s h R} \int_{[2,Y]^s \times [2,Y^2]^t} \frac{dx_1 \dots dx_{s+t}}{\ln(x_1 \dots x_{s+t})},$$

where g is the number of roots of unity in K, and R is the regulator of K.

Remark: In the case of a real quadratic number ring (s = 2 and t = 0), this result reduces to Proposition 5.1, and in the case of an imaginary quadratic number ring (s = 0 and t = 1), this result reduces to Proposition 3.1.

By [3], the multiple integral is asymptotically equal to $\frac{Y^n}{\ln(Y^n)}$. Then, by letting $Y \to \infty$, this theorem shows that there are infinitely many prime elements in \mathcal{O} satisfying the desired angular constraints.

Now, we use this result to readily establish the density of quotients of primes in any algebraic number ring O. With this theorem, and using the techniques of proof from the imaginary and real quadratic number rings (Theorems 3.2 and 5.2), we are now able to prove the main result of this paper.

Theorem 6.2. Let K be an algebraic number field over \mathbb{Q} with ring of integers \mathcal{O} . If $K \subseteq \mathbb{R}$, then any quotient set of prime elements in \mathcal{O} is dense in \mathbb{R} . Otherwise, if $\mathbb{R} \subsetneq K \subseteq \mathbb{C}$, then any quotient set of prime elements in \mathcal{O} is dense in \mathbb{C} .

Proof: First, assume that $K \subseteq \mathbb{R}$. We need to show that there exist a quotient of prime elements in \mathcal{O} in any interval (a, b). Without loss of generality, assume that a > 0. Then it follows directly from the generalized Prime Number Theorem that

$$\lim_{x \to \infty} (\Pi(bx; 0, 2\pi) - \Pi(ax; 0, 2\pi)) = \infty.$$

By considering the first copy of \mathbb{R} in $L_{s,t}$, the last assertion implies that for all sufficiently large x, there exists a prime $\pi_1 \in \mathcal{O}$ such that $ax < \pi_1 < bx$. Next, since there exist primes in \mathcal{O}

with arbitrarily large magnitude by the generalized Prime Number Theorem, let $x = \pi_2$ for some prime $\pi_2 \in \mathcal{O}$. This immediately yields $a < \frac{\pi_1}{\pi_2} < b$, as required.

Next, assume that $\mathbb{R} \subsetneq K \subseteq \mathbb{C}$. It suffices to show that any annular sector $\{z \in \mathbb{C} : \psi_1 < \arg z < \psi_2, 0 < r < |z| < R\}$ contains a quotient of prime numbers in \mathcal{O} . It follows from the generalized Prime Number Theorem that

$$\lim_{x \to \infty} \left[\Pi\left(\frac{x}{r}; \psi_1, \psi_2\right) - \Pi\left(\frac{x}{R}; \psi_1, \psi_2\right) \right] = \infty.$$

Then, there exists $x_0 > 0$ such that

$$\Pi\left(\frac{x}{r};\psi_1,\psi_2\right) - \Pi\left(\frac{x}{R};\psi_1,\psi_2\right) \ge 2 \text{ for all } x \ge x_0.$$

Moreover, since the generalized Prime Number Theorem implies that there are infinitely many prime numbers $\omega \in \mathcal{O}$ satisfying $\theta_1 < \arg(\omega^{(k)}) < \theta_2$ for each k = s + 1, ..., s + t, there exists a prime $\pi_1 \in \mathcal{O}$ satisfying $\arg(\pi_1^{(k)}) \in (0, \xi)$ for each k = s + 1, ..., s + t with sufficiently large magnitude $(|\pi_1| > x_0)$ such that

$$\Pi\left(\frac{|\pi_1|}{r}; 0, \xi\right) - \Pi\left(\frac{|\pi_1|}{R}; 0, \xi\right) \ge 2,$$

where $\xi = \min\{\psi_2 - \arg(\pi_1), \arg(\pi_1) - \psi_1)\}.$

Next, by considering the first copy of \mathbb{C} in $L_{s,t}$, the inequality in the last assertion implies that there exists a prime $\pi_2 \in \mathcal{O}$ satisfying $\frac{|\pi_1|}{R} < |\pi_2| < \frac{|\pi_1|}{r}$ and $0 < \arg(\pi_2) < \xi$. From this, it now follows that $r < \left|\frac{\pi_1}{\pi_2}\right| < R$ and $\psi_1 < \arg\left(\frac{\pi_1}{\pi_2}\right) < \psi_2$.

7 Concluding remarks

A unifying thread through the proofs of the density theorems presented here is having a suitable version of a prime number theorem around to permit us to establish the desired results. The existence of such theorems is rather remarkable in itself and are key results belonging to both analytic and algebraic number theory.

The curious reader may wonder whether there exist congruence class analogues for quotients of primes in quadratic number rings other than $\mathbb{Z}[i]$. This is indeed the case at least when these are UFDs, and the reader is encouraged to find and state the appropriate versions of the prime number theorem to establish these results; they can be found in [2], [8], and [12].

As for another open question, one can try to formulate and establish analogous density results for the noncommutative ring of Hurwitz quaternions

$$H = \left\{ a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\},\$$

and try to prove that $\{\pi_1\pi_2^{-1} : \pi_1, \pi_2 \in H \text{ are prime}\}\$ is dense in \mathbb{H} , the set of quaternions over \mathbb{R} .

References

- Brown, B., Dairyko, M., Garcia, S., Lutz, B., & Someck, M. (2014) Four Quotient Set Gems, *Amer. Math. Monthly*, 121, 590–598.
- [2] Hecke, E. (1920) Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen II, *Math. Zeitschr.* 6, 11–51.
- [3] Hinz, J. (1981) On the Theorem of Barban and Davenport–Halberstam in Algebraic Number Fields., J. Number Theory, 13 (4), 463–484.
- [4] Garcia, S., Selhorst-Jones, V., Ponce, D., & Simon, N. (2011) Quotient Sets and Diophantine Equations, *Amer. Math. Monthly*, 118, 704–711.
- [5] Garcia, S. (2013) Quotients of Gaussian Primes, Amer. Math. Monthly, 120, 851–853.
- [6] Hobby, D. & Silberger, D. (1993) Quotients of primes, Amer. Math. Monthly, 100, 50–52.
- [7] Kubilius, J. (1950) The distribution of Gaussian primes in sectors and contours, *Leningrad*. Gos. Univ. Uč. Zap, Cer. Mat. Nauk, 137 (19), 40–52.
- [8] Kubilius, J. (1952) On some problems of the geometry of prime numbers, *Mat. Sbornik N.S.*, 31 (73), 507–542.
- [9] Marcus, D. (1995) *Number Fields (2nd ed.)*, Springer-Verlag.
- [10] Micholson, A. (2012) Quotients of primes in arithmetic progressions, *Notes on Number Theory and Discrete Mathematics*, 18 (2), 56–57.
- [11] Mitsui, T. (1956) Generaized Prime Number Theorem, Jap. J. Math., 26, 1–42.
- [12] Rademacher, H. (1935) Über die Anzahl der Primzahlen eines reell-quadratischen Zahlkörpers, deren Konjugierten unterhalb gegebener Grenzen liegen, Acta Arith., 1, 67–77.
- [13] Sierpiński, W. (1988) *Elementary Theory of Numbers (2nd ed.)*, North-Holland, Amsterdam.
- [14] Sittinger, B. (2017) A Note on the Density of Quotients of Primes in Arithmetic Progressions, *Notes on Number Theory and Discrete Mathematics*, 23 (1), 99–100.
- [15] Starni, P. (1995) Answers to two questions concerning quotients of primes, Amer. Math. Monthly, 102, 347–349.
- [16] Stewart, I. & Tall, D. (2001) Algebraic Number Theory and Fermat's Last Theorem (3rd ed.), AK Peters/CRC Press.