# 1 Discussion

Let $p_1, p_2, \ldots$ be the prime numbers. Let $q_1, q_2, \ldots$ be the prime numbers which satisfy $q_j \equiv 1 \pmod 4$ (that is, it is one more than a multiple of 4). Let $r_1, r_2, \ldots$ be the prime numbers which satisfy $r_j \equiv 3 \pmod 4$.

Previously we gave a simple and elementary proof due to Erdős that the sum of the reciprocals $\frac{1}{p_j}$ of the primes diverges to infinity, and used this to prove a stronger result that the sum of $\frac{1}{r_j}$ also diverges to infinity. We know from non-elementary facts of number theory that approximately "half" of all prime numbers are of the form $p \equiv 1 \pmod 4$, with the other half satisfying $p \equiv 3 \pmod 4$, so assuming that the two types are distributed similarly we would expect that $\sum \frac{1}{q_j}$ and $\sum \frac{1}{r_j}$ should each be about half of $\sum \frac{1}{p_j} \to \infty$, so should diverge themselves.

We were able to prove that $\sum \frac{1}{r_j} \to \infty$ in an elementary way by relating the distribution of the $r_j$ to numbers which are of the form $a^2+b^2 = (a+bi)(a-bi)$ and using a counting argument to show that such numbers are relatively rare (specifically, they have asymptotically zero density). However this proof cannot be modified to show that $\sum \frac{1}{q_j} \to \infty$, even though the two results seem superficially very similar to each other.

Here we give a direct demonstration that $\sum \frac{1}{q_j} \to \infty$ by applying Erdős' proof to primes in the ring $\mathbb{Z}[i]$ of Gaussian integers. (See the previous writeups for an introduction to basic properties of the Gaussian integers.) This proof depends on the relationship between primes in $\mathbb{Z}[i]$ and primes in the integers $\mathbb{Z}$, and therefore depends on Fermat's theorem on sums of two squares (see also our writeup of a proof of this fact).

# 2 Proof

We review the essential facts of primes in the Gaussian integers.

1. Both $\mathbb{Z}$ and $\mathbb{Z}[i]$ are *unique factorization domains*, meaning that each number can be uniquely factored into a product of primes, up to units. A *unit* is a divisor of 1 (which are $\pm 1$ in $\mathbb{Z}$ and $\pm 1, \pm i$ in $\mathbb{Z}[i]$). If $a = bu$ where $u$ is a unit then we say $a$ and $b$ are *associates.*

2. *Ramified primes*: 2 is prime in $\mathbb{Z}$, and $1 + i$ and its associates $(\pm 1 \pm i)$ are prime in $\mathbb{Z}[i]$.

3. *Split primes*: for each $j$, $q_j$ is prime in $\mathbb{Z}$, and $q_j$ factors as $q_j = \alpha\beta$ for some two primes $\alpha, \beta$ in $\mathbb{Z}[i]$. In fact $\beta = \overline{\alpha}$.

4. *Inert primes*: for each $j$, $r_j$ is prime in $\mathbb{Z}$ and $\mathbb{Z}[i]$.

5. This is a complete list of the primes in $\mathbb{Z}$ and $\mathbb{Z}[i]$ up to associates. (Certainly this is a complete list of the primes in $\mathbb{Z}$. To see that this includes every prime of $\mathbb{Z}[i]$, suppose $\alpha$ is prime in $\mathbb{Z}[i]$. Now consider $N(\alpha) = \alpha\overline{\alpha}$, an integer. $N(\alpha)$ can be factored in $\mathbb{Z}$ into primes, and then using the above three cases each prime in $\mathbb{Z}$ can be further factored into primes in $\mathbb{Z}[i]$. By unique factorization in $\mathbb{Z}[i]$ therefore $\alpha$ must be one of those primes listed above.)

The analysis of the relationship between the primes in one ring and a ring containing it is a central aspect of algebraic number theory.

Previously we defined a concept of asymptotic density of subsets of the integers. Similarly, if $S$ is a subset of $\mathbb{Z}[i]$ define the *density* $\rho(S)$ as

$$\rho(S) = \lim_{n\to\infty} \frac{|\{\alpha \in S \mid N(\alpha) < n\}|}{|\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) < n\}|}$$

provided the limit exists.

Now we proceed with our proof.

**Theorem 1.**

$$\sum \frac{1}{q_j} \to \infty$$

*Proof.* Let $S$ be the set of Gaussian integers $a + bi$ such that $a$ and $b$ are relatively prime (in particular, $a$ and $b$ are nonzero).

The density of $S$ is the proportion of pairs $(a, b)$ which are relatively prime, which is

$$\rho(S) = \prod \left(1 - \frac{1}{p_j^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

The computation justifying this is found in our previous writeups. (In any case, we only need that this number is positive, which can be verified directly by taking the logarithm and observing that $\sum \frac{1}{p_j^2} < \sum \frac{1}{j^2} = \frac{\pi^2}{6}$ converges by the integral test.)

For each $j$, let $q_j = \gamma_j \overline{\gamma_j}$ be the factorization of $q_j$ into primes in $\mathbb{Z}[i]$.

If an integer $c > 1$ divides $a + bi$ then $c$ divides both $a$ and $b$, so in particular none of the elements of $S$ are divisible by any of the $r_j$. Therefore the prime factors of the elements of $S$ are only $1 + i$ and the $\gamma_j$ and $\overline{\gamma_j}$.

Let $S_k$ be the subset of $S$ consisting of those numbers whose prime factors are among $1 + i$ and the $\gamma_j, \overline{\gamma_j}$ with $j < k$. Then for each $\alpha \in S_k$,

$$\alpha = u(1 + i)^{a_0} \gamma_1^{a_1} \overline{\gamma_1}^{b_1} \cdots \gamma_k^{a_k} \overline{\gamma_k}^{b_k},$$

where $u \in \{1, -1, i, -i\}$ is a unit. Taking the norm of both sides, we find that if $N(\alpha) < n$ then each $a_j, b_j \leq \log n$, so $\rho(S_k) = 0$. (More specifically, the asymptotic density is bounded by $(\log n)^{2k+1}/n^2$.)

Now the density in $\mathbb{Z}[i]$ of multiples of an integer $c$ is $\frac{1}{c^2}$, so with $q_j = \gamma_j \overline{\gamma_j}$ the density of multiples of $\gamma_j$ must be $\frac{1}{q_j}$ (similarly for $\overline{\gamma_j}$). Therefore for every $k$ the density of $S \setminus S_k$ must be at least

$$\rho(S \setminus S_k) \leq \sum_{j \geq k} \frac{2}{q_j}.$$

Since $\rho(S) = \frac{6}{\pi^2} > 0$ and $\rho(S_k) = 0$, therefore

$$\sum_{j \geq k} \frac{1}{q_j} \geq \frac{1}{2} \rho(S)$$

for every $k$, so the sum $\sum \frac{1}{q_j}$ must diverge to infinity. □