1 Discussion

We are interested in the relationship between prime numbers and numbers which can be written as sum $a^2 + b^2$ of two squares. It is a classic result of elementary number theory, known as *Fermat's theorem on sums of two squares*, that an odd prime number p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$ (that is, it is one more than a multiple of 4). (See the other document which contains an elementary proof of Fermat's theorem, as well as of a classification of all numbers of whether they can be written as a sum of two squares or not.) It is a rather challenging fact of number theory (from Chebotarev's density theorem or Dirichlet's theorem) that "half" (in some technical sense) of all prime numbers are of the form $p \equiv 1 \pmod 4$, with the other half being of the form $p \equiv 3 \pmod 4$. It follows that half of all prime numbers can be written as a sum of two squares.

It turns out that this makes prime numbers unusual in tending to be a sum of two squares. Naively, if you ignore collisions of the form $a^2 + b^2 = c^2 + d^2$, one expects that roughly half (more precisely, $\pi/8$) of all numbers can be written as a sum of two squares; but in reality the proportion of numbers of that form approaches zero for large numbers, whereas for primes the ratio remains one half.

Formally speaking, if we randomly pick an integer in the range from 1 to n (where n is large), the probability that the chosen number is a sum of two squares is

$$\frac{K}{\sqrt{\log n}}$$

where $K = 0.7642\ldots$ is the Landau-Ramanujan constant. (This result was proven by Landau in 1908, and independently found by Ramanujan. The proof is not readily available to me so I do not know its difficulty.) However, the chance that a random such number is a sum of two squares increases to $1/2$ if we condition on the number being a prime number.

Conversely, we know from the prime number theorem (proven 1896) that for a random number in the range 1 to n, the probability it is prime is

$$\frac{1}{\log n},$$

but (combining the above results) if we condition it on being a sum of two squares then the probability increases to

$$\frac{1}{2K\sqrt{\log n}}.$$

So in either direction we see that prime numbers and sums of two squares are "correlated", in a sense.

The goal of this document is to give an elementary proof (of my own invention, except for the first lemma) that the density of sums of two squares is asymptotically zero, which is a weaker version of the result due to Landau. Along the way we will prove several other interesting results. Formally, the *density* $\rho(S)$ of a set S of positive integers is defined as

$$\rho(S) = \lim_{n\to\infty} \frac{|S \cap \{1, 2, \ldots, n\}|}{n}$$

provided that limit exists. For example, the density of the even numbers is $1/2$, and the density of the perfect squares is zero.

Let $p_1, p_2, \ldots$ be the prime numbers. Let $q_1, q_2, \ldots$ be the prime numbers which satisfy $q_i \equiv 1 \pmod 4$. Let $r_1, r_2, \ldots$ be the prime numbers which satisfy $r_i \equiv 3 \pmod 4$.

2 Lemmas

Lemma 1.

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

Proof. This proof is due to Erdős.

Suppose otherwise, and let k be so large that

$$\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}.$$

Now let n be an arbitrary integer and consider the set $\{1, \ldots, n\}$. In this set, the number of numbers divisible by p_i for some $i > k$ is at most

$$\sum_{i>k} \frac{n}{p_i} < \frac{n}{2}.$$

The other numbers are divisible only by primes p_i with $i \leq k$, so such numbers can be written in the form

$$p_1^{a_1} \cdots p_k^{a_k},$$

where clearly $0 \leq a_i < \log n$. Therefore the number of numbers of such form is at most $(\log n)^k$, so for all n we have

$$n = |\{1, \ldots, n\}| \leq (\log n)^k + \frac{n}{2}.$$

However in the limit for large n this is less than n, a contradiction. □

Lemma 2. *Consider a sequence $a_1, \ldots$ with $a_i \geq 2$. Then*

$$\sum \frac{1}{a_i} \to \infty \qquad \text{if and only if} \qquad \prod \left(1 - \frac{1}{a_i}\right) = 0.$$

Proof. Let x be the product, and consider

$$\begin{aligned} \log(x) &= \sum \log\left(1 - \frac{1}{a_i}\right) \\ &= -\sum \left(\frac{1}{a_i} + \frac{1}{2a_i^2} + \frac{1}{3a_i^3} + \cdots\right). \end{aligned}$$

Therefore

$$-\sum \left(\frac{2}{a_i}\right) \leq \log(x) \leq -\sum \left(\frac{1}{a_i}\right),$$

so $\log(x)$ diverges to $-\infty$ if and only if $\sum \frac{1}{a_i} \to \infty$. □

Lemma 3. *Let P_k be the set of numbers with at most k prime divisors (not necessarily distinct, so $4 \in P_2$ but $4 \notin P_1$). Then $\rho(P_k) = 0$ for all k.*

Proof. We induct on k; the case $P_0 = \{1\}$ is immediate. Now consider arbitrary $k > 0$, and suppose otherwise that $\rho(P_k) = \alpha > 0$.

Let n be so large that

$$\prod_{i<n} \left(1 - \frac{1}{p_i}\right) < \alpha,$$

which is possible because the infinite product is zero.

For any $a \in P_k$ we can uniquely write $a = bc$ where b is only divisible by prime divisors at most p_n, and c is only divisible by prime divisors greater than p_n. Note that only finitely many different b are possible across all $a \in P_k$ (because b has at most k prime divisors, each of which has one of n different possible values).

Whenever $b > 1$, c must have fewer than k prime divisors, so by induction the density of the subset of P_k with $b > 1$ must be zero. Therefore the density of the subset of P_k with $b = 1$ is α, which is to say that the density of numbers with at most k prime divisors all of which are greater than p_n is α. However n was chosen so that the density of numbers with no prime divisors less than or equal to p_n is less than α, a contradiction. □

In our document giving a proof of Fermat's theorem, we discussed the Gaussian integers, which are the complex numbers of the form $a + bi$ where a and b are integers. We need to recall a few of those facts here for the following lemma. We define the norm of a Gaussian integer $\gamma = a + bi$ by

$$N(\gamma) = \gamma\overline{\gamma} = a^2 + b^2$$

where $\overline{\gamma} = a - bi$ is the complex conjugate. The norm is multiplicative, so $N(\lambda\mu) = N(\lambda)N(\mu)$. The Gaussian integers, like the integers, are a *unique factorization domain*, which means that each Gaussian integer can be uniquely factored into primes up to factors of units, which are the numbers $\pm 1, \pm i$ with norm one. The primes in the Gaussian integers are not the same as in the ordinary integers; whenever $N(\gamma)$ is prime in the integers, γ is prime in the Gaussian integers (the converse is not true).

Recall that q_j is the jth (integer) prime of the form $q_j \equiv 1 \pmod 4$. From Fermat's theorem we know that for each j there exists a_j, b_j such that $q_j = a_j^2 + b_j^2 = N(a_j + b_j i)$. (The choice of a_j, b_j can be made unique if we require $0 < a_j < b_j$.) Let $\gamma_j = a_j + b_j i$.

Lemma 4. *Let Q be the set of numbers all of whose prime divisors are in the q_j. Then $\rho(Q) = 0$.*

Proof. Suppose otherwise, that $\rho(Q) = \alpha > 0$. Let k be an integer so large that $k > 16/\alpha$.

Since $\rho(P_k) = 0$, therefore $\rho(Q \setminus P_k) = \alpha$.

For large n, the set $\{1, \ldots, n\}$ contains more than $\alpha n/2$ elements of $Q \setminus P_k$. Consider one such element $x \in Q \setminus P_k$, $1 \le x \le n$. We can factor

$$x = q_1^{a_1} \cdots q_\ell^{a_\ell} = \gamma_1^{a_1}\overline{\gamma_1}^{a_1} \cdots \gamma_\ell^{a_\ell}\overline{\gamma_\ell}^{a_\ell}.$$

Recall that each of the $\gamma_j, \overline{\gamma_j}$ is a prime in the Gaussian integers (because $N(\gamma_j) = N(\overline{\gamma_j}) = q_j$), so the latter expression is the prime factorization of x in the Gaussian integers. Note that $\sum a_j > k$ because $x \notin P_k$.

Consider integers b_j with $0 \leq b_j \leq a_j$, and define a Gaussian integer λ in terms of the b_j as

$$\lambda(b_1, \ldots, b_\ell) = \gamma_1^{b_1}\overline{\gamma_1}^{a_1 - b_1} \cdots \gamma_\ell^{b_\ell}\overline{\gamma_\ell}^{a_\ell - b_\ell},$$

so that $x = \lambda(\mathbf{b})\overline{\lambda(\mathbf{b})} = N(\lambda(\mathbf{b}))$.

The λ are all distinct because they have different prime factorizations from each other, and the Gaussian integers have unique prime factorization. So each such $\lambda = c + di$ gives a different pair of integers (c, d) satisfying $x = c^2 + d^2$. There are $\prod(1 + a_j) > \sum a_j > k$ ways of choosing the exponents b_j for a given x. Since there are more than $\alpha n/2$ choices of such x in the range $1 \leq x \leq n$, and more than k ways of choosing distinct pairs (c, d) with $x = c^2 + d^2$, that makes at least $k\alpha n/2 > 8n$ distinct pairs of integers (c, d) with $c^2 + d^2 \leq n$. However, we must have $|c| \leq \sqrt{n}$ and $|d| \leq \sqrt{n}$, so there are only on the order of $4(\sqrt{n})^2 = 4n$ distinct pairs of integers small enough. For large n this is a contradiction. □

3 Main results

The only explanations I have seen for the following result invoke Lemma 1 and Dirichlet's theorem, which implies that the q_i, r_i are equally frequent asymptotically. Such explanation is unsatisfactory because it is not a complete proof and it invokes a very difficult piece of mathematics (Dirichlet's theorem). In contrast the following proof only uses the elementary math we have introduced here and in the proof of Fermat's theorem.

I don't know of a proof that $\sum \frac{1}{q_i} \to \infty$.

Theorem 5.

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

Proof.

$$0 = \rho(Q) = \frac{1}{2} \prod \left(1 - \frac{1}{r_i}\right).$$

□

Theorem 6. *Let S be the set of numbers of the form $a^2 + b^2$. Then $\rho(S) = 0$.*

Proof. Recall from Fermat's theorem that S is the set of numbers x such that each r_i appears an even number of times in the prime factorization of x. The density of numbers not divisible by r_i is $1 - (1/r_i)$; the density of numbers divisibe by r_i^2 but not r_i^3 is $(1/r_i)^2 - (1/r_i)^3$, and so on. So therefore

$$\begin{aligned}
\rho(S) &= \prod \left(1 - \frac{1}{r_i} + \frac{1}{r_i^2} - \frac{1}{r_i^3} + \cdots\right) \\
&= \prod \frac{1}{1 + \frac{1}{r_i}} \\
\frac{1}{\rho(S)} &= \prod \left(1 + \frac{1}{r_i}\right) \\
&\geq \sum \frac{1}{r_i} \to \infty
\end{aligned}$$

so we must have $\rho(S) = 0$. $\square$