# THE PRIMES: INFINITUDE, DENSITY AND SUBSTANCE

PETE L. CLARK

## 1. There are infinitely many primes

The title of this section is surely, along with the uniqueness of factorization, the most basic and important fact in number theory. The first recorded proof was by Euclid, and we gave it at the beginning of the course. There have since been (very!) many other proofs, many of which have their own merits and drawbacks. It is entirely natural to look for further proofs: in terms of the arithmetical function $\pi(n)$ which counts the number of primes $p \leq n$, Euclid's proof gives that

$$\lim_{n \to \infty} \pi(n) = \infty.$$

After the previous section we well know that one can ask for more, namely for the asymptotic behavior (if any) of $\pi(n)$. The asymptotic behavior is known – the celebrated **Prime Number Theorem**, coming up soon – but it admits no proof simple enough to be included in this course. So it is of interest to see what kind of bounds (if any!) we get from some of the proofs of the infinitude of primes we shall discuss.

1.1. **Euclid's proof.** We recall Euclid's proof. There is at least one prime, namely $p_1 = 2$, and if $p_1, \ldots, p_n$ are any $n$ primes, then consider

$$N_n = p_1 \cdots p_n + 1.$$

This number $N_n$ may or may not be prime, but being at least 3 it is divisible by some prime number $q$, and we cannot have $q = p_i$ for any $i$: if so $p_i | p_1 \cdots p_n$ and $p_i | N_n$ implies $p_i | 1$. Thus $q$ is a new prime, which means that given any set of $n$ distinct primes we can always find a new prime not in our set: therefore there are infinitely many primes.

Comments: (i) Euclid's proof is often said to be "indirect" or "by contradiction", but this is unwarranted: given any finite set of primes $p_1, \ldots, p_n$, it gives a perfectly definite procedure for constructing a new prime.

(ii) Indeed, if we define $E_1 = 2$, and having defined $E_1, \ldots, E_n$, we define $E_{n+1}$ to be the smallest prime divisor of $E_1 \cdots E_n + 1$, we get a sequence of distinct prime numbers, nowadays called the **Euclid sequence** (of course we could get a different sequence by taking $p_1$ to be a prime different from 2). The Euclid sequence begins

$$2, 3, 7, 43, 13, 53, 5, \ldots$$

Many more terms can be found on the *online handbook of integer sequences*. The obvious question – does every prime occur eventually in the Euclid sequence with $p_1 = 2$ (or in any Euclid sequence?) remains unanswered.

(iii) It is certainly a "classic" proof, but it is not "aesthetically perfect" (whatever that may mean). Namely, there is a moment when the reader wonders – hey, why are we multiplying together the known primes and adding one? One can address this by pointing out in advance the key fact that $\gcd(n, n+1) = 1$ for all $n$. Therefore if there were only finitely many primes $p_1, \ldots, p_r$, there would be an integer divisible by all of them, $N = p_1 \cdots p_r$, and then the fact that $\gcd(N, N+1) = 1$ leads to a contradiction. I do like this latter version better, but it is really just a rewording of Euclid's proof.[1]

(iv) Euclid's proof can be used to prove some further results. For instance:

**Theorem 1.** *Fix a positive integer $N > 2$. Then there are infinitely many primes $p$ which are* not *congruent to* $1 \pmod N$.

*Proof.* Take $p_1 = 2$, which is not congruent to $1 \pmod N$. Assume that $p_1, \ldots, p_n$ is a list of $n$ primes, none of which are $1 \pmod N$. Now consider the product

$$P_n := Np_1 \cdot \ldots \cdot p_n - 1.$$

$P_n \geq N - 1 \geq 2$, so it has a prime divisor. Also $P_n \equiv -1 \pmod N$. So if every prime divisor $q$ of $P_n$ were $1 \bmod N$, then so would $P_n$ be $1 \pmod N$ – which it isn't – therefore $P_n$ has at least one prime divisor $q$ which is not $1 \pmod N$. As above, clearly $q \neq p_i$ for any $i$, which completes the proof. □

In fact this argument can be adapted to prove the following generalization.

**Theorem 2.** *Fix a positive integer $N > 2$, and let $H$ be a proper subgroup of $U(N) = (\mathbb{Z}/N\mathbb{Z})^\times$. There are infinitely many primes $p$ such that $p \pmod N \notin H$.*

The proof is left as an exercise. (Suggestion: fix $a \in \mathbb{Z}^+$, $1 < a < N$, such that $a \pmod N \notin H$. Take $P_0 = 2N - a$ and for $n \geq 1$, $P_n = 2N \prod_{i=1}^n p_i - a$.)

Remark: If $\varphi(N) = 2$ – that is, for $N = 3$, 4, or 6 – then $\pm 1$ gives a reduced residue system modulo $N$, so that any prime $p > N - 1$ which is not $1 \pmod N$ is necessarily $-1 \pmod N$. Thus the argument shows that there are infinitely many primes $p$ which are $-1 \pmod 3$, $-1 \pmod 4$ or $-1 \pmod 6$. This is of course a special case of Dirichlet's theorem.

Remark: Interestingly, one can also prove without too much trouble that there are infinitely many primes $p \equiv 1 \pmod N$: the proof uses cyclotomic polynomials.

**Theorem 3.** *For any field $F$, there are infinitely many irreducible polynomials over $F$, i.e., infinitely many irreducible elements in $F[T]$.*

*Proof.* Euclid's argument works here: take e.g. $p_1(t) = t$, and having produced $p_1(t), \ldots, p_r(t)$, consider the irreducible factors of $p_1(t) \cdots p_r(t) + 1$. □

Note that one can even conclude that there are infinitely many prime ideals in $F[t]$ – equivalently, there are infinitely many *monic* irreducible polynomials. When $F$ is infinite, the monic polynomials $t - a$ for $a \in F$ do the trick. When $F$ is

[1] I have heard this argument attributed to the great 19th century algebraist E. Kummer. For what little it's worth, I believe I came up with it myself as an undergraduate. Surely many others have had similar thoughts.

finite, we showed there are infinitely many irreducible polynomials, but there are only $\#F - 1$ different leading coefficients, so there must be infinitely many monic irreducible polynomials. It is interesting to think about why this argument does not work in an arbitrary PID.[2]

1.2. **Fermat numbers.** Another way to construe Euclid's proof is that it suffices to find an infinite sequence $n_i$ of pairwise coprime positive integers, because these integers must be divisible by different primes. The Euclid sequence is such a sequence. A more "natural" looking sequence is the following.

**Theorem 4.** *The Fermat numbers $F_n = 2^{2^n} + 1$ are pairwise coprime.*

*Proof.* We claim that for all $n \geq 1$ we have

$$F_n = \prod_{d=0}^{n-1} F_d + 2.$$

This certainly suffices, since if $p$ is some common prime divisor of $F_d$ (for any $d < n$) and $F_n$ then $p \mid F_n - 2$, hence $p \mid 2$, but all the Fermat numbers are odd. The claim itself can be established by induction; we leave it to the reader. □

1.3. **Mersenne numbers.** Recall that Fermat believed that all the Fermat numbers were prime, and this is not true, since e.g.

$$F_5 = 2^{2^5} + 1 = 641 \cdot 6700417,$$

and in fact there are no larger known prime Fermat numbers. Nevertheless the previous proof shows that there is something to Fermat's idea: namely, they are "almost" prime in the sense that no two of them have a common divisor. One then wonders whether one can devise a proof of the infinitude of the primes using the Mersenne numbers $2^p - 1$, despite the fact that it is unknown whether there are infinitely many Mersenne primes. This can indeed be done:

Let $p$ be a prime (e.g. $p = 2$, as usual) and $q$ a prime divisor of $2^p - 1$. Then $2^p \equiv 1 \pmod{q}$. In other words, $p$ is a multiple of the order of 2 in the cyclic group $(\mathbb{Z}/q\mathbb{Z})^\times$. Since $p$ is prime the order of 2 must be exactly $p$. But by Lagrange's theorem, the order of an element divides the order of the group, which is $\varphi(q) = q - 1$, so $p \mid q - 1$ and hence $p < q$. Thus we have produced a prime larger than the one we started with.

1.4. **Euler's first proof.** It is a remarkable fact that the formal identity

$$\prod_p (1 - \frac{1}{p})^{-1} = \sum_n \frac{1}{n}$$

– which amounts to unique factorization – immediately implies the infinitude of primes. Indeed, on the left hand side we have a possibly infinite product, and on the right-hand side we have an infinite sum. But the infinite sum is well-known to be divergent, hence the product must be divergent as well, but if it were a finite product it would certainly be convergent!

[2]For there are PID's with only finitely many prime ideals: e.g. the set of rational numbers whose reduced denominator is prime to 42 is a PID with exactly three prime ideals.

Many times in the course we have seen a rather unassuming bit of abstract algebra turned into a mighty number-theoretic weapon. This example shows that the same can be true of analysis.

1.5. **Chaitin's proof.** In his most recent book[3] the computer scientist Gregory Chaitin announces an "algorithmic information theory" proof of the infinitude of primes. He says: if there were only finitely many primes $p_1, \ldots, p_k$ then every positive integer $N$ could be written as

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

which is "too efficient" a way of representing all large integers $N$. Chaitin compares his proof with Euclid's proof and Euler's proof (with a grandiosity that I confess I find unjustified and unbecoming). But criticism is cheaper than understanding: can we at least make sense of his argument?

Let us try to estimate how many integers $n$, $1 \leq n \leq N$, could possibly be expressed in the form $p_1^{a_1} \cdots p_k^{a_k}$, i.e., as powers of a fixed set of $k$ primes. In order for this expression to be at most $N$, every exponent has to be much smaller than $N$: precisely we need $0 \leq a_i \leq \log_{p_i} N$; the latter quantity is at most $\log_2 N$, so there are at most $\log_2 N + 1$ choices for each exponent, or $(\log_2 N + 1)^k$ choices overall. But aha – this latter quantity is much smaller than $N$ when $N$ is itself large: it is indeed the case that the percentage of integers up to $N$ which we can express as a product of any $k$ primes tends to 0 as $N$ approaches infinity.

So Chaitin's proof is indeed correct and has a certain admirable directness to it.

1.6. **Another important proof.** However, the novelty of Chaitin's proof is less clear. Indeed, in many standard texts (including Hardy and Wright, which was first written in 1938), one finds the following argument, which is really a more sophisticated version of Chaitin's proof.

Again, we will fix $k$ and estimate the number of integers $1 \leq n \leq N$ which are divisible only by the first $k$ primes $p_1, \ldots, p_k$, but this time we use a clever trick: recall that $n$ can be written uniquely as $uv^2$ where $u$ is squarefree. The number of squarefree $u$'s – however large! – which are divisible only by the first $k$ primes is $2^k$ (for each $p_i$, we either choose to include it or not). On the other hand, $n = uv^2 \leq N$ implies that $v^2 \leq N$ and hence $v \leq N^{\frac{1}{2}}$. Hence the number of $n \leq N$ divisible only by the first $k$ primes is at most $2^k \sqrt{N}$. If there are $k$ primes less than or equal to $N$, we therefore have

$$2^k \sqrt{N} \geq N$$

or

$$k \geq \frac{\log_2(N)}{2}.$$

[3]Its title is *Meta Math! The Quest for Omega*.

1.7. **An algebraic number theory proof.** We now sketch a proof due to Lawrence Washington.

Let $R$ be a PID, with field of fractions $F$. Suppose $K$ is a finite-degree field extension of $F$ – in other words, there exists some positive integer $d$ and elements $x_1, \ldots, x_d$ of $K$ such that every element $x$ of $K$ can be written as $\alpha_1 x_1 + \ldots + \alpha_d x_d$ for $\alpha_i \in F$. In such a situation we can define a subset $R_L$ of $L$, which is the set of all elements $x$ of $L$ which satisfy a monic polynomial relation with coefficients in $R$: that is, for some $n \in \mathbb{Z}^+$,

$$x^n + r_{n-1}x^{n-1} + \ldots + r_1 x + r_0 = 0,$$

and $r_i \in R$ for all $i$. It can be shown that $R_L$ is a subring of $L$, called the **integral closure** of $R$ in $L$: see §2 of the Appendix on Integral Elements and Extensions. As an example, when $R = \mathbb{Z}$ and $D$ is a squarefree integer not congruent to 1 (mod 4), then taking $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{D})$, then the integral closure of $\mathbb{Z}$ in $L$ is our friend the quadratic ring $\mathbb{Z}[\sqrt{D}]$. Anyway, here is the result:

**Theorem 5.** *Suppose that a PID $R$, with quotient field $K$, has only finitely many prime ideals. Then for any finite-degree field extension $L$ of $K$, the integral closure $S$ of $R$ in $L$ is again a PID.*

This shows the infinitude of the primes in $\mathbb{Z}$, since we saw that $\mathbb{Z}[\sqrt{-5}]$ is *not* a PID!

The proof of Theorem 5 lies further up and further in the realm of algebraic number theory than we dare to tread in this course. But here is a sketch of a proof for the "slummers"[4]: the ring $S$ is a Dedekind domain, so for any nonzero prime ideal $\mathfrak{p}$ of $R$, $\mathfrak{p}S$ is a nontrivial finite product of powers of prime ideals. The distinct prime ideals $\mathcal{P}_i$ appearing in this factorization are precisely the prime ideals $\mathcal{P}$ *lying over* $\mathfrak{p}$, i.e., such that $\mathcal{P} \cap R = \mathfrak{p}$. This shows that the restriction map $\mathcal{P} \mapsto \mathcal{P} \cap R$ from prime ideals of $S$ to prime ideals of $R$ has finite fibers. Thus, since by assumption there are only finitely many prime ideals of $R$, there are only finitely many prime ideals of $S$. Finally, a Dedekind domain with only finitely many prime ideals is necessarily a PID, as can be shown using the Chinese Remainder Theorem.

This is a proof with a moral: we need to have infinitely many primes in order for number theory to be as complicated as it is.

1.8. **Furstenberg's proof.** The last proof we will give is perhaps the most remarkable one. In the 1955 issue of the American Mathematical Monthly there appeared the following article by Hillel Furstenberg, which we quote in its entirety:

"In this note we would like to offer an elementary 'topological' proof of the infinitude of the prime numbers. We introduce a topology into the space of integers $S$, by using the arithmetic progressions (from $-\infty$ to $+\infty$) as a basis. It is not difficult to verify that this actually yields a topological space. In fact under this topology $S$ may be shown to be normal and hence metrizable. Each arithmetic progression is closed as well as open, since its complement is the union of other arithmetic progressions (having the same difference). As a result the union of any finite number of arithmetic progressions is closed. Consider now the set $A = \cup A_p$,

[4]i.e., more advanced readers who are reading these notes

where $A_p$ consists of all multiples of $p$, and $p$ runs though the set of primes $\geq 2$. The only numbers not belonging to $A$ are $-1$ and $1$, and since the set $\{-1, 1\}$ is clearly not an open set, $A$ cannot be closed. Hence $A$ is not a finite union of closed sets which proves that there are an infinity of primes."

Remarks: Furstenberg was born in 1935, so this ranks as one of the leading instances of undergraduate mathematics in the 20th century. He is now one of the leading mathematicians of our day. What is all the more remarkable is that this little argument serves as a preview of the rest of his mathematical career, which has concentrated on applying topological and dynamical methods ("ergodic theory") to the study of problems in number theory and combinatorics.

## 2. Bounds

Let us now go through some of these proofs and see what further information, if any, they yield on the function $\pi(n)$.

1. From Euclid's proof one can deduce that $\pi(n) \geq C \log\log n$. We omit the argument, especially since the same bound follows more readily from the Fermat numbers proof. Of course this is a horrible bound.

2. The Mersenne numbers proof gives, I believe, an even worse (iterated logarithmic) bound. I leave it to the reader to check this.

3. Euler's first proof does not immediately come with a bound attached to it. However, as we saw earlier in our study of the $\phi$ function, it really shows that

$$\prod_{i=1}^{r}(1 - \frac{1}{p_i})^{-1} > \sum_{i=1}^{r} \frac{1}{r} \geq C \log r.$$

After some work, one can deduce from this that

$$\sum_{i=1}^{n} \frac{1}{p_i} \geq C \log\log n,$$

whence the divergence of the prime reciprocals. We will not enter into the details.

4. Chatin's proof gives a lower bound on $\pi(n)$ which is between $\log\log n$ and $\log n$ (but much closer to $\log n$).

5. As we saw, one of the merits of the proof of §1.6 is that one easily deduces the bound $\pi(n) \geq \frac{\log_2 n}{2}$. (Of course, this is still almost a full exponential away from the truth.)

6. As we mentioned, knowing that the prime reciprocals diverge *suggests* that $\pi(n)$ is at worst only slightly smaller than $n$ itself. It *shows* that $\pi(n)$ is not bounded above by any power function $Cn^{\delta}$ for $\delta < 1$.

7. The last two proofs give no bounds whatsoever, not even implicitly. This seems to make them the worst, but there are situations in which one wants to separate out the problem of proving the infinitude of a set of numbers from the problem of

estimating its size, the latter problem being either not of interest or (more often) hopelessly out of current reach. In some sense all of the arguments except the last two are implicitly *trying to prove too much* in that they give lower bounds on $\pi(n)$. Trying to prove more than what you really want is often a very good technique in mathematics, but sometimes, when the problem is really hard, making sure that you are concentrating your efforts solely on the problem at hand is also a key idea. At any rate, there are many problems in analytic combinatorics for which Furstenberg-type existence proofs either were derived long before the explicit lower bounds (which require much more complicated machinery) or are, at present, the only proofs which are known.

I confess that I like Furstenberg's proof the best.

## 3. The density of the primes

All of the results of the previous section were *lower bounds* on $\pi(x)$. It is also of interest to give an upper bound on $\pi(x)$ beyond the "trivial" bound $\pi(x) \leq x$. The following gives such a result.

**Theorem 6.** *As $n \to \infty$, we have $\frac{\pi(n)}{n} \to 0$.*

If you like, this result expresses that the probability that a randomly chosen positive integer is prime is 0. We will come back to this idea after the proof, replacing "probability" by the more precise term *density*.

*Proof.* Let us first observe that there are at most $\frac{N}{2}$ primes in the interval $[1, N]$ since all but one of them must be odd. Similarly, since only one prime is divisible by 3, every prime $p > 6$ must be of the form $6k + 1$ or $6k + 5$, i.e., only 2 of the 6 residue classes mod 6 can contain more than one prime (in fact some of them, like 4, cannot contain any primes, but we don't need to worry about this), so that of the integers $n \leq N$, at most $\frac{2}{6}N + 6 + 2$ are primes.

In fact this simple reasoning can be carried much farther, using what we know about the $\varphi$ function. Namely, for any positive integer $d$, if $\gcd(a, d) > 1$ there is at most one prime $p \equiv a \pmod{d}$.[5] In other words, only $\varphi(d)$ out of $d$ congruence classes mod $d$ can contain more than one prime, so at most $(\frac{\varphi(d)}{d})N + d + \varphi(d)$ of the integers $1 \leq n \leq N$ can possibly be prime. (Here we are adding $d$ once to take care of the one prime that might exist in each congruence class and adding $d$ a second time to take care of the fact that since $N$ need not be a multiple of $d$, so the "partial congruence class" at the end may contain a higher frequency of primes than $\varphi(d)/d$, but of course no more than $\varphi(d)$ of primes overall.) But we know, thank goodness, that for every $\epsilon > 0$, there exists a $d$ such that $\frac{\varphi(d)}{d} < \epsilon$, and choosing this $d$ we find that the number of primes $n \leq N$ is at most

$$\frac{\pi(N)}{N} \leq \frac{\epsilon N + d + \varphi(d)}{N} = \epsilon + \frac{d + \varphi(d)}{N}.$$

This approaches $\epsilon$ as $N \to \infty$, so is, say, less than $2\epsilon$ for all sufficiently large $N$. □

Remark: Reflecting on the proof, something slightly strange has happened: we showed that $\varphi(d)/d$ got arbitrarily small by evaluating at $d = p_1 \cdots p_r$, the product

[5]Recall this is true because if $x \equiv a \pmod{d}$, $\gcd(a, d) \mid d \mid x - a$, and $gcd(a, d) \mid a$, so $\gcd(a, d)|x$.)

of the first $r$ primes. Thus, in order to show that the primes are relatively sparse, we used the fact that there are infinitely many of them!

In fact, by similarly elementary reasoning, one can prove a more explicit result, that $\pi(n) \leq \frac{Cn}{\log \log n}$. Before moving on to discuss some similar and stronger statements about the order of magnitude of $\pi(n)$, let us digress a bit on the notion of density of a set of integers.

Definition: A subset $A$ of the positive integers is said to have **density** $\delta(A) = \alpha$ if

$$\lim_{N \to \infty} \frac{\#\{1 \leq n \leq N \mid n \in A\}}{N} = \alpha.$$

We have encountered this notion before: recently we claimed (based on something less than a rigorous proof) that the density of squarefree integers is $\frac{6}{\pi^2}$. Notice that we have just shown that the primes have density zero. Here are some further examples:

Example 1: For any positive integers $a$ and $N$, the density of the set of positive integers $x \equiv a \pmod N$ is $\frac{1}{N}$. In particular, the set of all positive integers whose last decimal digit is 1 has density $\frac{1}{10}$.

Example 2: Any finite set has density zero.

Example 3: For any $k > 1$, the set of $k$th powers $n^k$ has density 0.

Example 4: In fact the set of all *proper powers*, i.e., positive integers of the form $n^k$ with $k > 1$, has density zero.

Example 5: The set $A$ of all positive integers whose *first* decimal digit is 1 does not have a density: that is, the limit does not exist. To see this, let $C(N)$ be the number of positive integers $1 \leq n \leq N$ with first digit 1. For any $k \geq 1$, $C(2 \cdot 10^k - 1) \geq \frac{1}{2}(2 \cdot 10^k - 1)$, since all of the integers from $10^k$ to $2 \cdot 10^k - 1$ begin with 1, and this is half of all integers less than $2 \cdot 10^k - 1$. On the other hand, none of the integers from $2 \cdot 10^k$ to $10^{k+1} - 1$ begin with 1, and this is $\frac{8}{10}$ of the integers less than or equal to $10^{k+1} - 1$, so $C(10^{k+1} - 1) \leq \frac{2}{10}(10^{k+1} - 1)$. Thus $C(N)/N$ does not tend to any limiting value.

Because of this definition it is common to discuss also the upper density $\overline{\delta}(A)$ and the lower density $\underline{\delta}(A)$: in the above definition replace lim by lim inf (resp. lim *sup*), the point being that these two quantities exist for any set, and a set $A$ has a density if $\underline{\delta} = \overline{\delta}$. Note that if $\overline{\delta}(A) = 0$, then necessarily $\delta(A)$ exists and equals 0.

Example 6: If $A_1, \ldots, A_k$ are finitely many sets having densities $\alpha_1, \ldots, \alpha_k$, respectively, then the upper density of $A_1 \cup \ldots \cup A_k$ is at most $\alpha_1 + \ldots + \alpha_k$. If $A_1, \ldots, A_k$ are pairwise disjoint, then the density of $A_1 \cup \ldots \cup A_k$ exists and is exactly $\alpha_1 + \ldots + \alpha_k$. (In fact it is enough if the pairwise intersections $A_i \cap A_j$ all have density zero.)

Density versus probability: Why have we backed off from using the word "probability"? Because ever since the work of the great early twentieth century Russian mathematician Kolmogorov, mathematicians have been trained to use the word "probability" only in the measure-theoretic sense, or, in plainer language, for the following situation: we have a set $S$ (the "sample space") and a function which associates to each reasonable subset $E$ (an "event") a number $P(E)$, $0 \leq P(E) \leq 1$, and satisfying the axiom of **countable additivity**: if $\{E_i\}_{i=1}^{\infty}$ is a sequence of events which are strongly mutually exclusive (i.e., $E_i \cap E_j = \emptyset$ for all $i \neq j$), then

$$P(\bigcup_i E_i) = \sum_{i=1}^{\infty} P(E_i).$$

Our density function $\delta$ satisfies finite additivity but not countable additivity: indeed, if we took $A_i$ to be the singleton set $\{i\}$, then certainly $\delta(A_i) = 0$ for all $i$ but the union of all the $A_i$'s are the positive integers themselves, so have density 1. This is the problem: for a probability *measure* we cannot have (countably!) infinitely many sets of measure zero adding up to a set of positive measure, but this happens for densities.

A similar problem occurs in our "proof" that the squarefree integers have density $\frac{6}{\pi^2}$. The set $S_{p^2}$ of integers which are *not* multiples of $p^2$ has density $1 - \frac{1}{p^2}$, and it is indeed true that these sets are "finitely independent" in the sense that the intersection of any finite number of them has density equal to the product of the densities of the component sets:

$$\delta(S_{p_1} \cap \ldots \cap S_{p_n}) = \prod_{i=1}^{n} (1 - \frac{1}{p^2}).$$

## 4. Substance

Let us define a subset $S$ of the positive integers to be **substantial** if $\sum_{n \in S} \frac{1}{n} = \infty$.

Example 0: Obviously a finite set is not substantial.

Example 1: The set $\mathbb{Z}^+$ is substantial: the harmonic series diverges.

Example 2: If $S$ and $T$ are two sets with finite symmetric difference – that is, there are only finitely many elements that are in $S$ and not $T$ or in $T$ but not $S$ – then $S$ is substantial iff $T$ is substantial.

Example 3: For any subset $S$ of $\mathbb{Z}^+$, at least one of $S$ and its complementary subset $S' = \mathbb{Z}^+ \setminus S$ is substantial, since

$$\sum_{n \in S} \frac{1}{n} + \sum_{n \in S'} \frac{1}{n} = \sum_{n \in \mathbb{Z}^+} \frac{1}{n} = \infty.$$

So there are "plenty" of substantial subsets. It is certainly possible for both $S$ and $S'$ to be substantial: take, e.g. the set of even numbers (or any $S$ with $0 < \delta(S) < 1$: see below).

Example 4: For any fixed $k > 1$, the set of all perfect $k$th powers is not substantial: by (e.g.) the Integral Test, $\sum_{n=1}^{\infty} \frac{1}{n^k} < \infty$.

Example 5: The set of integers whose first decimal digit is 1 is substantial.

Example 6: Indeed any set $S$ with positive upper density is substantial. This is elementary but rather tricky to show, and is left as a (harder) exercise.

The converse does not hold. Indeed, we saw above that the primes have zero density, but we will now establish the following:

**Theorem 7.** *The sum $\sum_p \frac{1}{p}$ of the prime reciprocals is infinite.*

*Proof.* (Erdős) Seeking a contradiction, we suppose that the series converges: then there exists an $k$ such that

$$\sum_{p > p_k} \frac{1}{p} < \frac{1}{2}.$$

However, the number of integers $1 \leq n \leq N$ which are divisible by $p_{k+1}$ is at most $\frac{N}{p_{k+1}}$; similarly for $p_{k+2}$, $p_{k+3}$, so that overall the number of integers which are divisible by any $p > p_k$ is at most

$$\frac{N}{p_{k+1}} + \frac{N}{p_{k+2}} + \ldots = N \sum_{p > p_k} \frac{1}{p} = \frac{N}{2}.$$

But this says that for any $N$, at least half of all positive integers are divisible by one of the first $k$ primes, which the argument of §1.6 showed not to be the case. □

Remarks: Maybe this is the best "elementary" proof of the infinitude of the primes. Aside from being an elegant and interesting argument, it is a quantum leap beyond the previous results: since for any $k \geq 2$, $\sum_n \frac{1}{n^k}$ converges, it shows that there are, in some sense, many more primes than perfect squares. In fact it implies that there is no $\delta < 1$ and constant $C$ such that $\pi(n) \leq Cn^{\delta}$ for all $n$, so that if $\pi(n)$ is well-behaved enough to have a "true order of magnitude" than its true order is rather close to $n$ itself.

A striking substance-theoretic result that we will not be able to prove here:

**Theorem 8.** *(Brun) The set $\mathcal{T}$ of "twin primes" – i.e., primes $p$ for which at least one of $p-2$ and $p+2$ is prime – is insubstantial.*

In a sense, this is disappointing, because we do not know whether $\mathcal{T}$ is infinite, whereas if $\mathcal{T}$ had turned out to be substantial we would immediately know that infinitely many twin primes exist! Nevertheless a fair amount of work has been devoted (for some reason) to calculating **Brun's sum**

$$\sum_{n \in \mathcal{T}} \frac{1}{n} \approx 1.902\ldots.$$

In particular Tom Nicely has done extensive computations of Brun's sum. His work got some unexpected publicity in the mid 1990's when his calculations led to the

recognition of the infamous "Pentium bug", a design flaw in many of the Intel microprocessors.[6]

The last word on density versus substance: In 1972 Endre Szemerédi proved – by elementary combinatorial means – the sensational result that any subset $S$ of positive upper density contains arbitrarily long arithmetic progressions, a vast generalization of a famous theorem of van der Waerden (on "colorings") which was conjectured by Erdős and Turan in 1936.[7] Unfortunately this great theorem does not apply to the primes, which have zero density.

However, Erdős and Turan made the much more ambitious conjecture that any substantial subset should contain arbitrarily long arithmetic progressions. Thus, when Green and Tao proved in 2002 that there *are* arbitrarily long arithmetic progressions in the primes, they verified a very special case of this conjecture. Doubtless many mathematicians are now reconsidering the Erdős-Turan conjecture with renewed seriousness.

[6]The PC I bought in 1994 (my freshman year of college) had such a bug. The Intel corporation reassured consumers that the bug would be of no practical consequence unless they were doing substantial floating point arithmetic. Wonderful...

[7]Several other mathematicians have devoted major parts of their career to bringing more sophisticated technology to bear on this problem, obtaining quantitative improvements of Szemerédi's theorem. Notably Timothy Gowers received the Fields Medal in 1998 for his work in this area. One must wonder whether the fact that Szemerédi did not receive the Fields Medal for his spectacular result is an instance of the prejudice against combinatorial mathematics in the mainstream mathematical community. (The extent of this prejudice also renders the plot of the movie "Good Will Hunting" somewhat implausible.)