Math 259: Introduction to Analytic Number Theory

Elementary approaches I: Variations on a theme of Euclid

Like much of mathematics, the history of the distribution of primes begins with Euclid:

Theorem (Euclid [IX, 20])**.** *There are infinitely many primes.*

Euclid's justly famed argument, while often presented as a proof by contradiction, is readily framed as an effective (albeit rather inefficient) construction:

Proof: Given primes $p_1, p_2, \ldots, p_n$, let $P_n = \prod_{k=1}^{n} p_n$, define $N_n = P_n + 1$, and let p_{n+1} be the smallest factor of N_n. Then p_{n+1} is a prime no larger than N_n and different from $p_1, \ldots, p_n$. Thus $\{p_k\}_{k>1}$ is an infinite sequence of distinct primes, Q.E.D.

This answers Yes to the first asymptotic question to ask about

$$\pi(x) := \#\{p \leq x : p \text{ is a positive prime}\} = \sum_{\substack{0<p<x \\ p \text{ prime}}} 1,$$

namely whether $\pi(x) \to \infty$ as $x \to \infty$. Moreover, the proof also gives an explicit upper bound on p_n, and thus a lower bound on $\pi(x)$.

Theorem. *For each integer $n > 0$, there are more than n primes $p < 2^{2^n}$. Equivalently, we have*[1]

$$\pi(x) > \log_2 \log_2 x$$

for all $x > 1$.

Proof: In the proof of Euclid's theorem, we may take $p_1 = 2$, and observe that

$$p_{n+1} \leq N_n = 1 + \prod_{k=1}^{n} p_n \leq 2 \prod_{k=1}^{n} p_n.$$

if equality were satisfied at each step we would have $p_n = 2^{2^{n-1}}$. Thus by induction we see that

$$p_n \leq 2^{2^{n-1}},$$

and of course the inequality is strict once $n > 1$. Therefore if $x \geq 2^{2^{n-1}}$ then $p_k < x$ for $k = 1, 2, \ldots, n$, and so $\pi(x) \geq n$, Q.E.D.

The $P_n + 1$ trick has been adapted to prove some special cases of Dirichlet's theorem on primes in arithmetic progression, which asserts that for coprime integers $q > 0$ and a there are infinitely many primes $p \equiv a \bmod q$. (We shall give the proof later in the course.) Of course the case 1 mod 2 is trivial given Euclid. For $-1 \bmod q$ with $q = 3, 4, 6$, start with $p_1 = q - 1$ and define $N_n = qP_n - 1$.

[1] Q: What sound does a drowning analytic number theorist make?
A: log log log log ... [R. Murty, via B. Mazur]

More generally, for any quadratic character χ there are infinitely many primes p with $\chi(p) = -1$; as a special case, given an odd prime q_0, there are infinitely many primes p which are quadratic nonresidues of q_0. [I'm particularly fond of this argument because I was able to adapt it as the punchline of my doctoral thesis; see [Elkies 1987].] The case of $\chi(p) = +1$ is only a bit trickier.[2] For instance, to prove Dirichlet for $(q, a) = (4, 1)$, let $p_1 = 5$ and $N_n = 4P_n^2 + 1$, and invoke Fermat's theorem on the prime factors of $x^2 + y^2$. Again this argument even yields an explicit lower bound on

$$\pi(x, 1 \bmod 4) := \#\{p \le x : p \text{ is a positive prime congruent to } 1 \bmod 4\},$$

namely[3]

$$\pi(x, 1 \bmod 4) > C \log\log x$$

for some positive constant C.

But Euclid's approach and its variations, however elegant, are not sufficient for our purposes. For one thing, numerical evidence suggests — and we shall soon prove — that $\log_2 \log_2 x$ is a gross underestimate on $\pi(x)$. For another, one cannot prove all cases of Dirichlet's theorem using only variations on the Euclid argument.[4] Our next elementary approaches will address at least the first deficiency.

Exercises

1. Let G be a subgroup of $(\mathbf{Z}/q\mathbf{Z})^*$ other than $(\mathbf{Z}/q\mathbf{Z})^*$ itself. Prove that there are infinitely many primes whose residue modulo q is not in G.

2. Exhibit an explicit value of C such that $\pi(x, 1 \bmod 4) > C \log\log x$ for all $x > 1$.

3. Use cyclotomic polynomials to show more generally that for any q_0, prime or not, there exist infinitely many primes congruent to 1 mod q_0. [Attributed to Euler in [Dickson 1919, Ch.XVIII], a chapter which gives much more information on the history of work on the distribution of primes up to about 1900. Note that $4P_n^2 + 1$ is the fourth cyclotomic polynomial evaluated at $2P_n$.] Show that again the number of such primes $< x$ grows at least as fast as some multiple of $\log\log x$.

4. Show that there are infinitely many primes congruent to 4 mod 5, once more with a $\log\log$ lower bound.

5. [A much later proof of the infinitude of primes that curiously gives the same bound $\pi(x) > \log_2 \log_2(x)$.] Recall that the m-th Fermat number F_m is defined by $F_m = 2^{2^m} + 1$ $(m = 0, 1, 2, \ldots)$. Prove that F_m and $F_{m'}$ are relatively prime

[2] But enough so that a problem from a recent Qualifying Exam for our graduate students asked to prove that there are infinitely many primes congruent to 1 mod 4.

[3] Even a drowning analytic number theorist knows that $\log\log$ and $\log_2 \log_2$ are asymptotically within a constant factor of each other. What is that factor?

[4] This is <u>not</u> a theorem, of course. How could one even define "variation of the Euclid argument" rigorously? But a Euclid-style argument for the infinitude of primes congruent to 2 mod 5 or mod 7 would already be quite impressive.

unless $m = m'$. Conclude that there are at least n primes $p \leq F_{n-1}$, and thus that $\pi(x) > \log_2 \log_2 x$.

Digression

Even a piece of mathematics as venerable as Euclid's proof of the infinitude of primes can continue to suggest very difficult problems. For instance, let p_n be the n-th prime, and let[5] $P_n = \prod_{i=1}^{n} p_i$. We know that $P_n + 1$ must contain a new prime factor, which cannot be p_{n+1} once $n > 1$ (if only because $P_n - 1$ must also contain a new prime factor). Does it happen infinitely often that p_{n+1} is a factor of $P_n + 1$? [This is the case for $n = 1$, 7, 232, 430, and no other $n < 5000$.] What of the primality of $P_n + 1$ itself? It is well-known that $P_n + 1$ is prime for $n = 1, 2, 3, 4, 5$, but $P_6 + 1 = 30031 = 59 \cdot 509$. Only fifteen $n > 5$ have been found for which $P_n + 1$ is prime, of which the smallest is 11 and the largest is 13494.[6] Again it is not known whether this happens infinitely often. Likewise for the primality of $P_n - 1$ and its divisibility by p_{n+1}. For another variation, define $q_1 = 2$ and, for $n > 0$, let q_{n+1} be the smallest prime factor of $(\prod_{i=1}^{n} q_i) + 1$. The sequence $\{q_n\}_{n=1}^{\infty}$ starts

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, \ldots$$

For instance, $q_5 = 13$ because $2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$. Is this "Euclid-Mullin sequence" [Sloane, A000945] a permutation of the sequence of primes? Probably yes, but proving this will likely be intractable for the foreseeable future. The same is true for the infinitude of primes of the form $P_n \pm 1$, and of n such that $p_{n+1} | P_n \pm 1$.

It should not even be obvious that one should expect that these four sets are all infinite. The heuristics supporting this expectation rely on results on the distribution of primes that we shall develop in the next few weeks.

References

[Dickson 1919] Dickson, L.E.: *History of the Theory of Numbers, Vol. I: Divisibility and Primality.* Washington: Carnegie Inst., 1919.

[Euclid] Euclid, *Elements.*

[Elkies 1987] Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over **Q**, *Invent. Math.* **89** (1987), 561–568; See also: Supersingular primes for elliptic curves over real number fields, *Compositio Math.* **72** (1989), 165–172.

[Sloane] Sloane, N.J.A.: *On-Line Encyclopedia of Integer Sequences.*
`http://www.research.att.com/~njas/sequences`

[5] By analogy with the "factorial" $n! = \prod_{i=1}^{n} i$, this P_n is sometimes called the n-th "primorial".

[6] Sequence A014545 in [Sloane], where the primality of $P_{13494} + 1$ is attributed to Arlin Anderson, Oct.20, 2000. For the analogous question concerning $P_n - 1$, see Sequence A055704 and A006794.