Lecture 1

January 8, 2018

1 Primes

A prime number p is a positive integer which cannot be written as ab for some positive integers $a,\ b > 1$. A prime p also have the property that if $p \mid ab$, then $p \mid a$ or $p \mid b$. This is a special property of the integers about which you will learn in *Algebraic Number Theory* course. One of the central questions in analytic number theory concerns counting primes. Euclid proved that there are infinitely many primes. Do you know that proof? He assumes that this is not so, therefore all the primes in the world form a finite set. Let us assume that this set is

$$\{p_1, p_2, \ldots, p_k\}.$$

Then Euclid forms the number $N = p_1 p_2 \cdots p_k + 1$. Because we have added 1 to the product $p_1 \cdots p_k$, the number N cannot be a multiple of p_1. Or of p_2. Or of any of $p_1, \ldots, p_k$. However, since N is a positive integer, it must be a product of some primes. This is the fundamental theorem of arithmetic. Anyone of those primes dividing N is a prime number not in the set $\{p_1, p_2, \ldots, p_k\}$. This shows that the set of primes is infinite.

Problem 1. *Let p_k be the kth prime. Deduce from Euclid's proof that*

$$p_k \leq 2^{2^{k-1}} \qquad \textit{holds for all} \qquad k \geq 1.$$

So, now that we know that there are infinitely many primes, how do we count them? One way is to let x be any positive number, and count the number of primes $p \leq x$. This number is called $\pi(x)$. Thus,

$$\pi(x) = \sum_{p \leq x} 1.$$

Problem 2. *What is $\pi(100)$?*

2 Chebyshev's estimates

In 1896, de la Vallée Poussin and Hadamard proved independently the *Prime Number Theorem.* That is, they showed that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

The result had been conjectured by Gauss.

Earlier, Chebyshev had established that

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x}$$

for all $x \ge 10$, where $c_1 = \log(2^{1/2}3^{1/3}5^{1/5}/30^{1/30})$ and $c_2 = 6c_1/5$. Here, we prove something weaker by a method which is easier than Chebyshev's. The following proof is due to Erdős.

Theorem 1. *For $x \ge 2$,*

$$\left(\frac{3\log 2}{8}\right)\frac{x}{\log x} < \pi(x) < (6\log 2)\frac{x}{\log x}.$$

We shall need the following lemma.

Lemma 1. *Let p be a prime and $e_p(n!)$ be the exponent at which p appears in $n!$. Then*

$$e_p(n!) = \sum_{k\ge 0} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Proof. Induction on n. The formula is clearly true if $n = 1$ (for all p). Assume that it holds for n and write $n+1 = p^u m$, where $p \nmid m$. Then, by the induction hypothesis,

$$e_p((n+1)!) = e_p(n!) + u = \sum_{k=1}^{u} \left(\left\lfloor \frac{n}{p^k} \right\rfloor + 1 \right) + \sum_{k>u} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

All is left to note is that

$$\left\lfloor \frac{n+1}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^k} \right\rfloor + 1 \quad \text{if } 1 \le k \le u \quad \text{and} \quad \left\lfloor \frac{n+1}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^k} \right\rfloor \quad \text{if } k > u.$$

□

Proof of Theorem 1. We first prove the lower bound on $\pi(x)$. We start with the observation that

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \Big| \prod_{p<2n} p^{r_p} \tag{1}$$

if $n > 1$, where r_p is that positive integer such that $p^{r_p} \leq 2n < p^{r_p+1}$. Indeed, to prove divisibility (1) note that the exponent at which p appears in the binomial coefficient $\binom{2n}{n}$ equals

$$e_p((2n)!) - e_p((n!)^2) \quad = \quad e_p((2n)!) - 2e_p(n!) = \sum_{k\geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Divisibility relation (1) follows now by observing that $\lfloor 2y \rfloor - 2\lfloor y \rfloor \in \{0, 1\}$ holds for all real numbers y (when is it zero and when is it 1?) together with the fact that when $k > r_p$, we have $p^k > 2n$, therefore $\lfloor 2n/p^k \rfloor = 0$ for such values of k.

Divisibility relation (1) certainly gives that

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

On the other hand, since

$$(1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$$

and since

$$\binom{2n}{n} \geq \binom{2n}{k} \qquad \text{holds for all } k = 0, 1, \ldots, 2n,$$

we get that

$$\binom{2n}{n} > \frac{2^{2n}}{2n+1}.$$

By induction, one checks that

$$\frac{2^{2n}}{2n+1} > 2^n \qquad \text{holds for all } n \geq 3.$$

Hence, if $n \geq 3$, we have

$$2^n < \frac{2^{2n}}{2n+1} < \binom{2n}{n} < (2n)^{\pi(2n)},$$

which after taking logarithms becomes

$$\pi(2n) > \frac{\log(2^n)}{\log 2n} = \frac{\log 2}{2} \cdot \frac{2n}{\log(2n)}.$$

Assume now that $x \geq 8$. Let n be that positive integer such that $2n \leq x < 2n+2$. Note that $n \geq 3$. Further, we have $2n > x - 2 \geq 3x/4$ (because $x \geq 8$). The function $y \mapsto y/\log y$ is increasing for $y > e$ (to see this, study the sign of its derivative!) and certainly $3x/4 \geq 6 > e$ for $x \geq 8$. Putting together all the above we get that if $x \geq 8$, then

$$\pi(x) \geq \pi(2n) \geq \frac{\log 2}{2} \cdot \frac{2n}{\log(2n)} \geq \frac{\log 2}{2} \cdot \frac{3x/4}{\log(3x/4)} > \frac{3\log 2}{8} \cdot \frac{x}{\log x},$$

which is the desired lower bound for $x \geq 8$. You should now check by yourself that it also holds for $x \in [2, 8)$.

We now turn to the upper bound. Note that

$$\prod_{n<p\leq 2n} p \Big| \binom{2n}{n}.$$

Thus,

$$\prod_{n<p\leq 2n} p < (1+1)^{2n} = 2^{2n},$$

which after taking logarithms leads to

$$\pi(2n)\log n - \pi(n)(\log(n/2) + \log 2) < 2n \log 2.$$

Hence,

$$\pi(2n)\log n - \pi(n)\log(n/2) < 2n\log 2 + \pi(n)\log 2 \leq (3\log 2)n, \qquad (2)$$

where we used the obvious fact that $\pi(n) \leq n$. Put $f(n) = \pi(2n)\log n$ and notice that the inequality (2) above is

$$f(n) - f(n/2) < (3\log 2)n.$$

Let $n = 2^i$ for $i = k, k-1, \ldots, 2$. We then have

$$\begin{aligned} f(2^k) - f(2^{k-1}) &< (3\log 2)\, 2^k \\ f(2^{k-1}) - f(2^{k-2}) &< (3\log 2)\, 2^{k-1} \\ &\vdots \\ f(4) - f(2) &< (3\log 2)\, 4 \end{aligned} \qquad (3)$$

Summing up inequalities (3), we get

$$\begin{aligned}\pi(2^{k+1})\log(2^k) &= f(2^{k+1}) = (3\log 2)(4+8+\ldots+2^k)+f(2)\\ &= (3\log 2)(4+8+\ldots+2^k)+\pi(4)\log 2\\ &< (3\log 2)(1+4+8+\ldots+2^k)\\ &< (3\log 2)\,2^{k+1},\end{aligned}$$

so

$$\pi(2^{k+1}) < (6\log 2)\left(\frac{2^k}{\log(2^k)}\right).$$

Now given $x \geq 2$, choose $k \geq 1$ such that $2^k \leq x < 2^{k+1}$. If $x \geq 4$, then $k \geq 2$ so $2^k \geq 4 > e$. Thus, $2^k/\log(2^k) \leq x/\log x$ whenever $x \geq 4$. We thus get that

$$\pi(x) \leq \pi(2^{k+1}) < (6\log 2)\left(\frac{2^k}{\log(2^k)}\right) < (6\log 2)\frac{x}{\log x}$$

for $x \geq 4$. You should also check that the claimed inequality holds for all $x \in [2,4)$.

3 Homework

Problem 3. *Show that if 2^n+1 is prime then n is a power of 2.*

Problem 4. *Show that if 2^n-1 is prime then n is prime.*

Problem 5. *A positive integer n is pseudoprime to base 2 if n is composite and the congruence $2^{n-1} \equiv 1 \pmod{n}$ holds. Let $F_n = 2^{2^n}+1$ be the nth Fermat number. Show that if $k \leq n_1 < n_2 < \ldots < n_s \leq 2^k$, then $F_{n_1}\cdot\cdots\cdot F_{n_s}$ is either a prime or a base 2 pseudoprime. Deduce that there are infinitely many base 2 pseudoprimes.*

Problem 6. *Show that $(n-1)! \equiv -1 \pmod{n}$ if n is prime and $n \mid (n-1)!$ if $n > 4$ is composite. Use this to prove that*

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{1+\sum_{j=2}^{m}\left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j}\right\rfloor\right\rfloor}\right\rfloor^{1/n}\right\rfloor.$$

Problem 7. *Prove that*

$$\operatorname{lcm}[1,2,,\ldots,n] \geq 2^n$$

holds for all $n \geq 9$.