Math 259: Introduction to Analytic Number Theory

Čebyšev (and von Mangoldt and Stirling)

Before investigating $\zeta(s)$ and $L(s,\chi)$ as functions of a complex variable, we give another elementary approach to estimating $\pi(x)$, due to Čebyšev. This method, unlike Euler's, produces upper and lower bounds on $\pi(x)$ that remain within a small constant factor as $x \to \infty$. These bounds $x/\log x \ll \pi(x) \ll x/\log x$ are sufficient for many theoretical and practical applications, which thus do not require the more advanced and subtle techniques that enter into the proof of the Prime Number Theorem. (The bounds are also close enough to let Čebyšev prove "Bertrand's Postulate": every interval $(x, 2x)$ with $x > 1$ contains a prime. See [HW 1996, p.343–4] for Erdös's simplification of Čebyšev's proof; this simplified proof is also on the Web: http://forum.swarthmore.edu/dr.math/problems/kuropatwa.4.3.97.html .) For us Čebyšev's method also has the advantage of introducing the von Mangoldt function and the Stirling approximation to $x!$, both of which will figure prominently in our future analysis.

It is well known[1] that for any prime p and positive integer x the exponent of p in $x!$ (a.k.a. the p-valuation of $x!$) is

$$c_p(x) := \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \cdots = \sum_{k=1}^{\infty} \left\lfloor \frac{x}{p^k} \right\rfloor,$$

the sum being finite because eventually $p^k > x$. It was Čebyšev's insight that one could extract information about $\pi(\cdot)$ from the resulting formula

$$x! = \prod_p p^{c_p(x)},$$

or equivalently

$$\log x! = \sum_p c_p(x) \log(p) = \sum_{n=1}^{\infty} \left\lfloor \frac{x}{n} \right\rfloor \Lambda(n), \tag{1}$$

where $\Lambda(n)$ is the *von Mangoldt function*

$$\Lambda(n) := \begin{cases} \log p, & \text{if } n = p^k \text{ for some positive integer } k \text{ and prime } p; \\ 0, & \text{otherwise.} \end{cases}$$

To make use of (1) we need to estimate

$$\log x! = \sum_{n=1}^{x} \log n$$

[1] If only thanks to the perennial problems along the lines of "how many zeros end 2003! ?".

for large x. We do this by in effect applying the first few steps of symmetrized Euler-Maclaurin summation, to find:

Lemma. *There exists a constant C such that*

$$\log x! = (x+\frac{1}{2})\log x - x + C + O(1/x) \tag{2}$$

holds for all positive integers x.

Proof: For any $\mathcal{C}^2$ function f we have (by integrating by parts twice)

$$\int_{-1/2}^{1/2} f(y)\,dy = f(0) + \frac{1}{2}\left[\int_{-1/2}^{0} f''(y)\big(y+\frac{1}{2}\big)^2\,dy + \int_{0}^{1/2} f''(y)\big(y-\frac{1}{2}\big)^2\,dy\right]$$
$$= f(0) + \frac{1}{2}\int_{-1/2}^{1/2} f''(y)\big\|y+\frac{1}{2}\big\|^2\,dy,$$

where $\|z\|$ is the distance from z to the nearest integer. Thus

$$\sum_{k=1}^{N} f(k) = \int_{1/2}^{N+\frac{1}{2}} f(y)\,dy + \frac{1}{2}\int_{\frac{1}{2}}^{N+\frac{1}{2}} f''(y)\big\|y+\frac{1}{2}\big\|^2\,dy.$$

Taking $f(y) = \log(y)$ and $N = x$ we thus have

$$\log x! = (x+\frac{1}{2})\log(x+\frac{1}{2}) + \frac{1}{2}\log 2 - x - \frac{1}{2}\int_{\frac{1}{2}}^{x+\frac{1}{2}} \big\|y+\frac{1}{2}\big\|^2\frac{dy}{y^2}.$$

The integral is

$$-\frac{1}{2}\int_{\frac{1}{2}}^{\infty} \big\|y+\frac{1}{2}\big\|^2\frac{dy}{y^2} \;+\; O(1/x),$$

and the other terms are

$$(x+\frac{1}{2})\log x - x + \frac{1}{2}(\log 2 + 1) + O(1/x),$$

from which (2) follows. □

[Stirling also determined the value of C (which turns out to be $\frac{1}{2}\log(2\pi)$, as we shall soon see), and extended (2) to an asymptotic series for $x!/((x/e)^x\sqrt{2\pi x}\,)$ in inverse powers of x. But for our purposes $\log x! = (x+\frac{1}{2})\log x - x + O(1)$ is more than enough. In fact, since for the time being we're really dealing with $\log\lfloor x\rfloor!$ and not $\log\Gamma(x+1)$, the best honest error term we can use is $O(\log x)$.]

Now let

$$\psi(x) := \sum_{1\le n\le x} \Lambda(n).$$

Then from (1) and (2) we have

$$\sum_{k=1}^{\infty} \psi(x/k) = (x+\frac{1}{2})\log x - x + O(1).$$

This certainly suggests that $\psi(x) \sim x$, and lets us prove upper and lower bounds on $\psi(x)$ proportional to x. For instance, since $x \geq 1 + \sum_{m=1}^{\infty} \lfloor x/2^m \rfloor$ for all $x \geq 1$, we have

$$\psi(x) \leq \log x! - \sum_{m=1}^{\infty} \log \left\lfloor \frac{x}{2^m} \right\rfloor !,$$

which yields

$$\psi(x) \leq \left[\sum_{m=1}^{\infty} \frac{m}{2^m} \log 2 \right] x + O(\log^2 x) = (2 \log 2)x + O(\log^2 x).$$

For a lower bound we can use the inequality

$$\psi(x) \geq \sum_{k=1}^{\infty} (-1)^{k-1} \psi(x/k) = \log \frac{x!}{(x/2)!^2} = (\log 2)x + O(\log x)$$

for an even integer $x = 2n$; This is essentially the same tactic of factoring $\binom{2n}{n}$ that Čebyšev used to prove $\pi(2x) > \pi(x)$.

It is true that we're ultimately interested in $\pi(x)$, not $\psi(x)$. But it is easy to get from one to the other. For one thing, the contribution to $\psi(x)$ of prime powers p^k with $k > 1$ is negligible — certainly less than $\sum_{k=2}^{\log_2 x} \lfloor x^{1/k} \rfloor \log x \ll x^{1/2} \log x$. The remaining sum, $\sum_{p \leq x} \log p$, can be expressed in terms of $\pi(x)$ and vice versa using partial summation, and we find:

$$\psi(x) = \log(x)\pi(x) - \int_2^x \pi(y) \frac{dy}{y} + O(x^{1/2} \log x),$$

$$\pi(x) = \frac{\psi(x)}{\log x} + \int_2^x \psi(y) \frac{dy}{y \log^2 y} + O(x^{1/2}).$$

It follows that the Prime Number Theorem $\pi(x) \sim x/\log x$ holds if and only if $\psi(x) \sim x$, and good error terms on one side imply good error terms on the other. It turns out that we can more readily get at $\psi(x)$ than at $\pi(x)$; for instance, $\psi(x)$ is quite well approximated by x, while the "right" estimate for $\pi(x)$ is not $x/\log x$ but $(x/\log x) + \int^x dy/\log^2 y$, i.e., the "logarithmic integral" $\int^x dy/\log y$. It is in the form $\psi(x) \sim x$ that we'll actually prove the Prime Number Theorem.

Exercises

On Čebyšev's method:

1. How many consecutive 0's are there at the end of the base-12 expansion of 2006!? Why did I choose 12 rather than any smaller base (including the default 10), and what other bases less than 100 would serve the same purpose?

2. Since our upper and lower asymptotic bounds $\log 2, \log 4$ on $\psi(x)/x$ are within a factor of 2 of each other, they do not quite suffice to prove Bertrand's Postulate. But any improvement *would* prove that $\pi(2x) > \pi(x)$ for sufficiently

large x, from which the proof for all x follows by exhibiting a few suitably spaced primes. It turns out that better bounds are available starting from (1). For instance, show that $\psi(x) < (\frac{1}{2}\log 12)x + O(\log^2 x)$. Can you obtain Čebyšev's bounds of 0.9 and 1.1? In fact it is known that the upper and lower bounds can be brought arbitrarily close to 1, but alas the only known proof of that fact depends on the Prime Number Theorem!

To recover Bertrand's Postulate, one needs for once to convert all the $O(\cdot)$'s to explicit error estimates. One then obtains an explicit x_0 such that $\pi(2x) > \pi(x)$ for all $x \geq x_0$, which reduces Bertrand's Postulate to the finite computation of verifying $\pi(2x) > \pi(x)$ for each $x \in (1, x_0)$. This can be done by calculating a sequence of $O(\log x_0)$ primes $2, 3, 5, 7, 13, 23, \ldots, p$, each less than twice the previous prime, and with $p > x_0$. Once we prove the Prime Number Theorem it will follow that for each $\epsilon > 0$ there exists x_0 such that $\pi((1+\epsilon)x) > \pi(x)$ for all $x \geq x_0$.

3. Estimate $\log \prod (m^2 + n^2)$, where the product extends over all $(m, n) \in \mathbf{Z}^2$ such that $0 < m^2 + n^2 \leq x$. What is the exponent of a prime $p \leq x$ in this product? Using this information, how close can you come to the asymptotic formula $\pi(x, 1 \bmod 4) \sim \frac{1}{2}x/\log x$?

Bernoulli polynomials, Euler-Maclaurin summation, and efficient computation of $\zeta(s)$ and $L(s, \chi)$:

4. The *Bernoulli polynomials* $\mathrm{B}_n(x)$ are defined for $n = 0, 1, 2, 3, \ldots$ by the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \mathrm{B}_n(x)\frac{t^n}{n!}.$$

The *Bernoulli numbers* B_n are the rational numbers $\mathrm{B}_n(0)$, with generating function $t/(e^t - 1) = \sum_{n=0}^{\infty} B_n t^n/n!$. The first few Bernoulli polynomials are

$$\mathrm{B}_0(x) = 1, \quad \mathrm{B}_1(x) = x - \frac{1}{2}, \quad \mathrm{B}_2(x) = x^2 - x + \frac{1}{6},$$

$$\mathrm{B}_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, \quad \mathrm{B}_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}.$$

Show that in general $\mathrm{B}_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$ (= "$(B+x)^{[n]}$" mnemonically), that $\mathrm{B}_n'(x) = n\mathrm{B}_{n-1}(x)$, and that B_n $(n = 1, 2, 3, \ldots)$ is the unique polynomial such that $\mathrm{B}_n(x+1) - \mathrm{B}_n(x) = nx^{n-1}$ and $\int_0^1 \mathrm{B}_n(x)\,dx = 0$. Show that the Bernoulli number B_n vanishes for odd $n > 1$. What is $\mathrm{B}_n(x) + \mathrm{B}_n(x + \frac{1}{2})$?

5. Now let f be a $\mathcal{C}^n$ function on $[t, t+1]$. Prove that

$$f(t) = \int_t^{t+1} f(x)\,dx + \sum_{m=1}^{n} \frac{B_m}{m!}\big(f^{(m-1)}(t+1) - f^{(m-1)}(t)\big)$$

$$+ (-1)^{n+1} \int_t^{t+1} f^{(n)}(x)\frac{\mathrm{B}_n(x-t)}{n!}\,dx.$$

Therefore, if f is a $\mathcal{C}^n$ function on $[M,N]$ for some integers M,N then

$$\sum_{n=M}^{N-1} f(n) = \int_M^N f(x)\,dx + \sum_{m=1}^{n} \frac{B_m}{m!}\big(f^{(m-1)}(N) - f^{(m-1)}(M)\big) + (-1)^{n+1}\int_M^N f^{(n)}(x)\frac{\mathrm{B}_n(x-\lfloor x\rfloor)}{n!}\,dx;$$

and if f is $\mathcal{C}^n$ on $[M,\infty)$ then

$$\sum_{n=M}^{\infty} f(n) = \int_M^\infty f(x)\,dx - \sum_{m=1}^{n} \frac{B_m}{m!} f^{(m-1)}(M) + (-1)^{n+1}\int_M^\infty f^{(n)}(x)\frac{\mathrm{B}_n(x-\lfloor x\rfloor)}{n!}\,dx, \tag{3}$$

provided the integrals converge and each $f^{(m-1)}(N)\to 0$ as $N\to\infty$. This is a rigorous form of the "Euler-Maclaurin formula"

$$\sum_{n=M}^{\infty} f(n) = \int_M^\infty f(x)\,dx - \sum_{m=1}^{\infty} \frac{B_m}{m!} f^{(m-1)}(M),$$

which rarely converges (can you find any nonzero f for which it *does* converge?), but is often useful as an asymptotic series. For instance, show that for any $s>1$ one can efficiently compute $\zeta(s)$ to within $\exp(-N)$ in time $N^{O(1)}$ by taking $f(x)=x^{-s}$ in (3) and choosing M,n appropriately. Do the same for $L(s,\chi)$ where χ is any nontrivial Dirichlet character and $s>0$. For instance, one can compute Catalan's constant

$$G = L(2,\chi_4) = 1 - \frac{1}{3^2} + \frac{1}{5^2} - \frac{1}{7^2} + - \cdots = .915965594177219015054 6\ldots$$

in this way.

We could also use (3) to obtain the analytic continuation of $\zeta(s)$ and $L(s,\chi)$ to the half-plane $\sigma > 1-n$, and thus to the whole complex plane since n is arbitrary. But this is a less satisfactory approach than using the functional equation which relates $L(s,\chi)$ to $L(1-s,\overline{\chi})$ and thus achieves the analytic continuation to $\mathbf{C}$ in one step.

More about $\psi(x)$:

6. Show that

$$\sum_{p\le x}\log p = \psi(x) - \psi(x^{1/2}) - \psi(x^{1/3}) - \psi(x^{1/5}) + \psi(x^{1/6}) \cdots = \sum_{k=1}^{\infty}\mu(k)\psi(x^{1/k}),$$

where μ is the *Möbius function* taking the product of $r\ge 0$ *distinct* primes to $(-1)^r$ and any non-square-free integer to 0.

Finally, another elementary approach to estimating $\pi(x)$ that gets within a constant of the Prime Number Theorem:

7. Let $P(u)$ be any nonzero polynomial of degree d with integer coefficients; then

$$\int_0^1 f(u)^{2n}\,du \geq 1/\mathrm{lcm}(1,2,\ldots,2dn+1) = \exp(-\psi(2dn+1)).$$

Thus

$$\psi(2dn+1) < 2n \log \min_{0<u<1} 1/|P(u)|.$$

For instance, taking $f(u) = u - u^2$ we find (at least for $4|x$) that $\psi(x) < x \log 4$. This is essentially the same (why?) as Čebyšev's trick of factoring $\binom{2n}{n}$, but suggests different sources of improvement; try $f(u) = (u-u^2)(1-2u)$ for example. [Unfortunately here the upper bound cannot be brought down to $1+\epsilon$; see [Montgomery 1994, Chapter 10] — thanks to Madhav Nori for bringing this to my attention.]

References

[HW 1996] Hardy, G.H., Wright, E.M.: *An Introduction to the Theory of Numbers*, 5th ed. Oxford: Clarendon Press, 1988 [AB 9.88.10 / QA241.H37].

[Montgomery 1994] Montgomery, H.L.: *Ten lectures on the interface between analytic number theory and harmonic analysis.* Providence: AMS, 1994 [AB 9.94.9].