C3.8 Analytic Number Theory

Sheet 1 — MT24

This sheet covers asymptotic notation and elementary estimates on primes, and is aligned with the notes up to and including Section 2.

Section A

1. Prove the following.

   (i) $(\log X)^4 < X^{1/10}$ for all sufficiently large X;

   (ii) $e^{\sqrt{\log X}} = O_\varepsilon(X^\varepsilon)$ for all $\varepsilon > 0$ and $X \geqslant 1$;

   (iii) $X(1 + e^{-\sqrt{\log X}}) + X^{3/4}\sin X \sim X$.

   Solution: (i) By substituting $X = Y^{10}$ it is enough to show $10^4 \log^4 Y < Y$ for sufficiently large Y. Setting further $Y = e^Z$, it is sufficient yo show that $10^4 Z^4 < e^Z$ for sufficiently large Z. However by Taylor expansion, ignoring all terms except the fifth, we have $e^Z > Z^5/5!$ for positive Z. The claim now follows.

   (ii) We have $e^{\sqrt{\log X}} = X^{1/\sqrt{\log X}}$ and so certainly $e^{\sqrt{\log X}} < X^\varepsilon$ if $X \geqslant X_0(\varepsilon)$ is sufficiently large.

   (iii) First note that $|X^{3/4}\sin X| \leqslant X^{3/4} = o(X)$, so it suffices to show that $X(1 + e^{-\sqrt{\log X}}) \sim X$. Since $e^{-\sqrt{\log X}} \to 0$ as $X \to \infty$, this is immediate from the definition of $\sim$.

2. In the following exercise, $a(X), b(X)$ are positive functions tending to ∞ as $X \to \infty$. Say whether each of the following is true or false.

   (i) If $a(X) - b(X) \to 0$ then $a(X) \sim b(X)$.

   (ii) If $a(X) \sim b(X)$ then $a(X) - b(X) \to 0$.

   (iii) If $a(X) \sim b(X)$ and $a'(X) := \sum_{y \leqslant X} a(y)$, $b'(X) := \sum_{y \leqslant X} b(y)$ then $a'(X) \sim b'(X)$.

   (iv) The converse to (iii).

Ben Green: ben.green@maths.ox.ac.uk

Solution: (i) is true since $\left|\frac{a(X)}{b(X)} - 1\right| \leqslant \frac{|a(X)-b(X)|}{b(X)} \leqslant \frac{1}{b(X)}$ for sufficiently large X, and this tends to 0.

(ii) is false, as the example $a(X) = X$, $b(X) = X + 1$ shows.

(iii) Let $\varepsilon > 0$. Then, by the definition of what it means that $a(X) \sim b(X)$, there is some $X_0 = X_0(\varepsilon)$ such that $a(y) \geqslant (1-\varepsilon)b(y)$ for all $y \geqslant X_0$. It follows that if $X \geqslant X_0$ then

$$\begin{aligned}
a'(X) &= \sum_{y \leqslant X} a(y) \\
&= \sum_{y \leqslant X_0} a(y) + \sum_{X_0 \leqslant y \leqslant X} a(y) \\
&\geqslant \sum_{y \leqslant X_0} a(y) + (1-\varepsilon) \sum_{X_0 \leqslant y \leqslant X} b(y) \\
&\geqslant (1-\varepsilon) \sum_{X_0 \leqslant y \leqslant X} b(y) \\
&\geqslant (1-\varepsilon) b'(X) - \sum_{y \leqslant X_0} b(y)
\end{aligned}$$

If X is big enough, this is $> (1-2\varepsilon)b'(X)$. We have a similar inequality the other way around, and ε is arbitrary, so the result follows.

(iv) This is false; an example is to take $a(X) = X$ for all X, and $b(X) = X$ for all X except when X is a power of two, in which case take $b(X) = 2X$. (Remark: one may care to think about what happens if, additionally, $a(X)$ and $b(X)$ are monotonic).

Ben Green: ben.green@maths.ox.ac.uk

Section B

3. Prove the following.

   (i) There are infinitely many primes of the form $4k+3$.

   (ii) There are infinitely many primes of the form $4k+1$. (Hint: you may wish to prove that -1 is not a quadratic residue modulo any prime $3(\operatorname{mod} 4)$.)

   Solution: (i) Basically the same as Euclid's proof. If $p_1, \ldots, p_N$ is all these primes except 3, consider $4p_1 \cdots p_N + 3$.

   (ii) If $-1 = x^2(\operatorname{mod} p)$ then $(-1)^{\frac{p-1}{2}} = x^{p-1} = 1(\operatorname{mod} p)$ (Fermat's Little Theorem) and so $p \equiv 1(\operatorname{mod} 4)$. Now let $p_1, \cdots, p_N$ be the complete list of primes $1(\operatorname{mod} 4)$ and consider $(2p_1 \cdots p_N)^2 + 1$.

4. We say that an arithmetic function is *multiplicative* if $f(ab) = f(a)f(b)$ whenever $(a,b) = 1$, and *completely multiplicative* if this holds without the coprimality restriction. For each of the functions $\Lambda, \mu, \phi, \tau, \sigma$, say with proof whether or not it is (a) multiplicative or (b) completely multiplicative.

   Solution: The function Λ is not multiplicative (and hence certainly not completely multiplicative). For example, $\Lambda(6) = 0 \neq \Lambda(2)\Lambda(3)$.

   The Möbius function μ is multiplicative (easy check from the definition). It is not completely multiplicative as, for example, $\mu(4) \neq \mu(2)^2$.

   The ϕ function is multiplicative. This follows from the Chinese remainder theorem: x is coprime to ab iff it is coprime to both a and b. It is not completely multiplicative since, for example, $\phi(4) = 2$, $\phi(2)^2 = 1$.

   The τ function is multiplicative, since if $n = ab$ and if $d \mid n$ then $d = ef$ with $e \mid a$ and $f \mid b$, and vice versa. It is not completely multiplicative since, for example, $\tau(4) = 3$ whilst $\tau(2)^2 = 4$.

   The σ function is multiplicative. One could observe, in fact, that if f is multiplicative then so is $g(n) := \sum_{d|n} f(d)$, and apply this fact to $f(d) = d$.

   (Remark: none of the functions is completely multiplicative. This illustrates the point that being merely multiplicative is a very natural condition on a function. One can mention the Liouville function as one of the more natural completely multiplicative functions.

Ben Green: ben.green@maths.ox.ac.uk

5. Show that there are arbitrarily large gaps between consecutive primes by

   (i) utilising the bounds on $\pi(x)$ shown in the course;

   (ii) considering the numbers $n! + 2, \dots, n! + n$.

   Which of the two approaches gives the better bound?

   Solution: The upper bound in the weak prime number theorem evidently implies that there are gaps of size $\gg \log n$ amongst the primes less than n. The construction implies that, among the primes less than $X = n!$, there are gaps of length $\sim n$. However, $n = o(\log X)$; indeed $n! > (n/2)^{n/2} > e^{cn \log n}$ for large n, so $n \ll \frac{\log X}{\log\log X}$.

6. Assuming the prime number theorem, show that $p_n \sim n \log n$, where p_n denotes the nth prime.

   Solution: Let $\delta > 0$ be small. By the prime number theorem and the fact that there are infinitely many primes, we have

$$n = \pi(p_n) > (1 - \frac{\delta}{2})\frac{p_n}{\log p_n}$$

when n is sufficiently large, thus

$$\limsup_{n\to\infty} \frac{p_n}{n \log p_n} \leqslant \frac{1}{1 - \frac{\delta}{2}} < 1 + \delta. \tag{1}$$

Suppose that $p_n \geqslant (1+\delta) n \log n$ for an infinite sequence of n. Then, since $t/\log t$ is an increasing function of t, we have

$$\frac{p_n}{n \log p_n} \geqslant \frac{(1+\delta)\log n}{\log(1+\delta) + \log n + \log\log n}.$$

Dividing top and bottom by $\log n$ we get

$$\frac{p_n}{n \log p_n} \geqslant \frac{(1+\delta)}{\frac{\log(1+\delta)}{\log n} + 1 + \frac{\log\log n}{\log n}}.$$

As $n \to \infty$ along any subsequence, the denominator tends to 1. Therefore by standard facts about limits we have

$$\limsup_{n\to\infty} \frac{p_n}{n \log p_n} \geqslant 1 + \delta,$$

contrary to (1).

The other direction is similar and is omitted.

Ben Green: ben.green@maths.ox.ac.uk

7. Denote by τ the divisor function.

   (i) Show that $\tau(n) \leqslant 2\sqrt{n}$.

   (ii) Find a formula for τ in terms of the prime factorisation of n.

   (iii) Using your formula from (ii), show that for any $\varepsilon > 0$ we have $\tau(n) < n^{\varepsilon}$ for sufficiently large n.

Solution: (i) If $d \mid n$ then n/d divides n, and at least one of these numbers is $\leqslant \sqrt{n}$.

(ii) If $n = p_1^{a_1} \cdots p_k^{a_k}$ then we have $\tau(n) = (a_1 + 1) \cdots (a_k + 1)$. (The set of divisors is precisely those $p_1^{b_1} \cdots p_k^{b_k}$ with $0 \leqslant b_i \leqslant a_i$ for all i.

(iii) If $p \geqslant 2^{1/\varepsilon}$ then we have $a + 1 \leqslant 2^a \leqslant p^{a\varepsilon}$ for all a. For smaller values of p we have $a + 1 \leqslant p^{a\varepsilon}$ provided that $a > r$, where $r = r(\varepsilon)$ is the smallest integer such that $2^{r\varepsilon} \geqslant r + 1$. Therefore

$$\tau(n) \leqslant n^{\varepsilon} \prod_{\substack{i : p_i < 2^{1/\varepsilon} \\ a_i \leqslant r}} (a_i + 1) \leqslant C_{\varepsilon} n^{\varepsilon},$$

where $C_{\varepsilon} = (r + 1)^{\pi(2^{1/\varepsilon})}$. For sufficiently large n, this is $< n^{2\varepsilon}$. Redefining ε to $\varepsilon/2$ gives the result.

Remark. Item (iii) here is a very useful and important bound in number theory called the *divisor bound.*

8. (i) Let X be an integer. Show that

$$\sum_{n \leqslant X} \log n = X \log X - X + O(\log X).$$

   (ii) Show that if X is an integer then

$$\sum_{p \leqslant X} \log p \Big(\Big\lfloor \frac{X}{p} \Big\rfloor + \Big\lfloor \frac{X}{p^2} \Big\rfloor + \dots \Big) = X \log X - X + O(\log X).$$

   (iii) Show that the contribution from the terms $\lfloor \frac{X}{p^k} \rfloor$ with $k \geqslant 2$ is $O(X)$.

   (iv) Deduce *Mertens' estimate*

$$\sum_{p \leqslant X} \frac{\log p}{p} = \log X + O(1).$$

   Explain why this remains valid even if X is not necessarily an integer.

Ben Green: ben.green@maths.ox.ac.uk

Solution: (i) The idea is to compare the sum $\sum_{n\leqslant X}\log n$ with the integral $\int_1^X \log t dt - X\log X - X$. Drawing a picture, and using the fact that log is monotonic and bounded by $\log X$ on the interval, the result follows. (We remark that this is a primitive form of Stirling's formula, since the LHS is $\log X!$.)

(ii) We claim that the LHS is $\log X!$, which suffices by part (i). If $X! = \prod p^{v_p(X)}$ then $\log X! = \sum_p v_p(X)\log p$, so it suffices to show that $v_p(X) = \lfloor X/p\rfloor + \lfloor X/p^2\rfloor + \dots$. This is Legendre's formula, as mentioned in lectures. It follows by taking the number of $n \leqslant X$ divisible by p (namely $\lfloor X/p\rfloor$), adding the number divisible by p^2, etc.

(iii) For fixed p,

$$\sum_{k\geqslant 2}\left\lfloor \frac{X}{p^k}\right\rfloor \leqslant \sum_{k\geqslant 2}\frac{X}{p^k} = \frac{X}{p(p-1)}$$

by summing the GP. Hence

$$\sum_p \log p \sum_{k\geqslant 2}\lfloor\frac{X}{p^k}\rfloor \leqslant X\sum_p \frac{\log p}{p(p-1)} \leqslant X\sum_m \frac{\log m}{m(m-1)} = O(X).$$

(iv) From what we have said so far we have

$$\sum_{p\leqslant X}\log p\left\lfloor\frac{X}{p}\right\rfloor = X\log X + O(X).$$

The error in removing the $\lfloor\cdot\rfloor$ is

$$\sum_{p\leqslant X}\log p\{X/p\} \leqslant \sum_{p\leqslant X}\log p$$

which, by the basic bounds on primes proved in the course, is $O(X)$.

Finally, if X is now allowed to be an arbitrary positive real number then replace X with $\lfloor X\rfloor$ and apply the estimate. The sum $\sum_{p\leqslant X}\frac{\log p}{p}$ is unchanged, while the right hand side is $\log\lfloor X\rfloor + O(1) = \log X + \log(1+\frac{\lfloor X\rfloor}{X}) + O(1) = \log X + O(1)$.

Remark. One may use more sophisticated tools such as the Euler-Maclaurin summation formula to get better approximations to $\sum_{n\leqslant X}\log n$, and this leads to the more precise forms of Stirling's formula.

Ben Green: ben.green@maths.ox.ac.uk

Section C

9. Prove the second Mertens estimate: we have

$$\sum_{p\leqslant X}\frac{1}{p} = \log\log X + O(1).$$

(Hint: Write $F(y) = \sum_{p\leqslant y}\frac{\log p}{p}$ and consider $\int_2^x F(y)w(y)dy$ for an appropriate weight function w.)

Deduce that there are constants $c_1, c_2 > 0$ such that

$$\frac{c_1}{\log X} \leqslant \prod_{p\leqslant X}(1-\frac{1}{p}) \leqslant \frac{c_2}{\log X}.$$

Solution: We take the hint (this technique is called "partial summation"). By exchanging the order of summation we have

$$\int_2^x F(y)w(y)dy = \sum_{p\leqslant x}\frac{\log p}{p}\int_p^x w(y)dy.$$

We wish to chose $w(y)$ so that the integral is $\frac{1}{\log p}$. Differentiating both sides suggests $-w(p) = -\frac{1}{p\log^2 p}$, so we set $w(y) = \frac{1}{y\log^2 y}$. Then

$$\int_p^x w(y)dy = \frac{1}{\log p} - \frac{1}{\log x}.$$

Therefore we obtain

$$\sum_{p\leqslant X}\frac{1}{p} = \frac{1}{\log X}\sum_{p\leqslant X}\frac{\log p}{p} + \int_2^X \frac{F(y)}{y\log^2 y}dy.$$

By the previous exercise, the first term on the right is $1+O(\frac{1}{\log X})$. Also by the previous exercise, the second term is $\int_2^X \frac{dy}{y\log y} + O(\int_2^X \frac{dy}{y\log^2 y})$, which is $O(1)$ plus $\int_2^X \frac{dy}{y\log y}$. This integral is, by substituting $y = e^t$, seen to be $\log\log X + O(1)$.

Proof of the last part: this follows quickly from the observation that $1-\frac{1}{p} = \exp(-\frac{1}{p} + O(\frac{1}{p^2}))$ and the previous part.

Remark. In both cases more precise results are available via a more careful analysis (involving the prime number theorem). Specifically

$$\sum_{p\leqslant X}\frac{1}{p} = \log\log X + c_0 + o(1)$$

for some c_0 and

$$\prod_{p \leqslant X} \big(1 - \frac{1}{p}\big) = (e^{-\gamma} + o(1)) \frac{1}{\log X}.$$

10. Let p_n denote the nth prime.

(i) Is it the case that, for sufficiently large n, the sequence $p_{n+1} - p_n$ is strictly increasing?

(ii) Is it the case that, for sufficiently large n, the sequence $p_{n+1} - p_n$ is nondecreasing?

Solution: (i) Answer: no. If the sequence is strictly speaking then $p_{n+1} - p_n > n - c$ for sufficiently large n, which means that p_n grows quadratically. This is contrary to the asymptotic $p_n \sim n \log n$ obtained in an earlier question.

(ii) Answer: also no. Suppose that this is so. Suppose that $p_{n+i+1} - p_{n+i} = m$ for $i = 0, 1, \dots, m-1$. If $m \geqslant 3$ then there is an integer m, $1 < m' < m$, coprime to m. The numbers p_{n+i} then run through a complete set of residue classes modulo m' and so in particular at least one of these numbers is composite, contrary to assumption. It follows that

$$p_{n+\sum_{m=3}^{M} m} \geqslant p_n + \sum_{m=3}^{M} m^2,$$

i.e. $p_{n+CM^2} \geqslant p_N + C'M^3$, much bigger that the actual growth of p_n.

Ben Green: ben.green@maths.ox.ac.uk