Number Theory I

D-MATH Prof. Dr. Emmanuel Kowalski

Solutions: Exercise Sheet 1

1. For a real number $x \ge 0$, we define

$$N(x) = |\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 \le x\}|$$

The goal of this exercise is to prove the estimate

$$N(x) = \pi x + O(x^{1/2}),$$

for $x \ge 1$ (recall that f(x) = O(g(x)) for $x \in X$ means that there exists a constant $c \ge 0$ such that $|f(x)| \le cg(x)$ for all $x \in X$).

1. Show that

$$N(x) \le \pi(\sqrt{x} + \sqrt{2})^2$$

for all $x \ge 0$. (Hint: interpret N(x) as the area of a certain union of squares of side 1, contained in a suitable disc.)

<u>Solution</u>: The value of N(x) is precisely the area of the union \mathcal{N} of unit squares $[a, a+1) \times [b, b+1)$ where $(a, b) \in \mathbb{Z}^2$ and $a^2 + b^2 \leq x$, or equivalently $||(a, b)|| \leq \sqrt{x}$ using the Euclidean metric. For each $(u, v) \in \mathcal{N}$, there exists $(a, b) \in \mathbb{Z}^2$ with $a^2 + b^2 \leq x$ and $(u, v) \in [a, a+1) \times [b, b+1)$. By the triangle inequality,

$$\begin{aligned} \|(u,v)\| &\leq \|(a,b)\| + \|(u-a,v-b)\| \\ &\leq \sqrt{x} + \|(1,1)\| \\ &\leq \sqrt{x} + \sqrt{2}. \end{aligned}$$

Thus \mathcal{N} is contained in the disc of radius $\sqrt{x} + \sqrt{2}$, so that $N(x) = \operatorname{Area}(\mathcal{N}) \leq \pi(\sqrt{x} + \sqrt{2})^2$.

2. Show that

$$N(x) \ge \pi(\sqrt{x} - \sqrt{2})^2$$

for all $x \ge 0$. (Hint: use a similar idea.)

Solution: As before, $N(x) = \operatorname{Area}(\mathcal{N})$. Let (u, v) be any point with $||(u, v)|| \le \sqrt{x} - \sqrt{2}$, and let (a, b) = (|u|, |v|). Then $(a, b) \in \mathbb{Z}^2$ and by the triangle inequality,

$$\|(a,b)\| \le \|(u,v)\| + \|(a-u,b-v)\|$$

$$\le \sqrt{x} - \sqrt{2} + \|(1,1)\|$$

$$= \sqrt{x} - \sqrt{2} + \sqrt{2} = \sqrt{x},$$

so \mathcal{N} contains the square with bottom-left corner (a, b). The point (u, v) is contained in this square and thus in \mathcal{N} , so \mathcal{N} contains the disc of radius $\sqrt{x} - \sqrt{2}$. Thus $N(x) = \operatorname{Area}(\mathcal{N}) \geq \pi(\sqrt{x} - \sqrt{2})^2$.

3. Conclude.

Solution: The bounds of the previous two parts show that

$$-2\sqrt{2}\sqrt{x} + 2 \le N(x) - \pi x \le 2\sqrt{2}\sqrt{x} + 2.$$

Thus for example $|N(x) - \pi x| \le 6\sqrt{x}$ for all $x \ge 1$, so that $N(x) = \pi x + O(x)$.

2. We order the primes in increasing order $(p_n)_{n\geq 1}$:

$$2 = p_1 < 3 = p_2 < 5 = p_3 < \cdots$$
.

The goal of the exercise is to show that there exist positive constants c_1^\prime and c_2^\prime such that

$$c_1' n \log(n) \le p_n \le c_2' n \log(n) \tag{1}$$

for all $n \ge 1$.

1. Show that

$$\lim_{n \to +\infty} \frac{\log(n)}{\log(p_n)} = 1$$

(Hint: observe first that $\pi(p_n) = n$, and then use Chebychev's estimate.) Solution: By Chebychev's estimate, there exist positive constants c_1 and c_2 such that

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

Note that $\pi(p_n) = n$, so applying this estimate to $x = p_n$ and taking logarithms we get that

$$\log c_1 + \log p_n - \log \log p_n \le \log n \le \log c_2 + \log p_n - \log \log p_n.$$

Dividing by $\log p_n$, we get

$$1 + \frac{\log c_1 - \log \log p_n}{\log p_n} \le \frac{\log n}{\log p_n} \le 1 + \frac{\log c_2 - \log \log p_n}{\log p_n}$$

Taking the limit as $n \to \infty$ (and thus as $p_n \to \infty$), we note that $\frac{\log c_1}{\log p_n} \to 0$, $\frac{\log c_2}{\log p_n} \to 0$, and $\frac{\log \log p_n}{\log p_n} \to 0$. Thus the limit of $\frac{\log n}{\log p_n}$ is bounded above and below by 1, so it must be 1.

2. Using again Chebychev's estimate, prove (1). <u>Solution</u>: Since $\lim_{n\to\infty} \frac{\log n}{\log p_n} = 1$, there exist constants d_1 and d_2 such that for all $n \ge 1$,

$$d_1 \le \frac{\log n}{\log p_n} \le d_2$$

or equivalently

$$\frac{1}{d_2}\log n \le \log p_n \le \frac{1}{d_1}\log n.$$
(2)

Applying Chebychev's estimate to $x = p_n$, we get that

$$c_1 \frac{p_n}{\log p_n} \le n \le c_2 \frac{p_n}{\log p_n}$$
$$\Rightarrow c_1 p_n \le n \log p_n \le c_2 p_n$$

The left inequality combined with (2) implies that $c_1 p_n \leq n \log p_n \leq \frac{1}{d_1} n \log n$, so that $p_n \leq \frac{1}{c_1 d_1} n \log n$. By the same logic on the other side, $\frac{1}{c_2 d_2} n \log n \leq p_n$. Taking $c'_1 = \frac{1}{c_2 d_2}$ and $c'_2 = \frac{1}{c_1 d_1}$ completes the proof of (1).

3. Prove that

$$\sum_{p \le x} \frac{1}{p} \to +\infty$$

More precisely, how large can you get the partial sums

$$\sum_{p \le x} \frac{1}{p}$$

to be as $x \to +\infty$? Solution: Write

$$\sum_{p \le x} \frac{1}{p} = \sum_{n \le \pi(x)} \frac{1}{p_n}$$

$$\ge \frac{1}{c'_2} \sum_{n \le \pi(x)} \frac{1}{n \log n}, \text{ by part (2)}$$

$$\ge \frac{1}{c'_2} \int_2^{\pi(x)-1} \frac{1}{u \log u} du$$

$$= \frac{1}{c'_2} \left(\log \log(\pi(x) - 1) - \log \log 2) \right)$$

$$\ge \frac{1}{2c'_2} \left(\log \log\left(\frac{c_1 x}{\log x}\right) - \log \log 2 \right)$$

using that $\log \log(n-1) \geq \frac{1}{2} \log \log n$ for all $n \geq 1$ and Chebyshev's estimate. This in turn is larger than (for example) $\frac{1}{4c'_2} \log \log x$ for large enough x. Since $\log \log x \to \infty$, so does $\sum_{p \leq x} \frac{1}{p}$.

If instead of using the upper bound $p_n \leq c'_2 n \log n$, we used the lower bound $p_n \geq c'_1 n \log n$, and applied the same argument, we can show that $\sum_{p \leq x} \frac{1}{p} \leq d \log \log x$ for some constant d. Thus $\sum_{p \leq x} \frac{1}{p}$ grows on the order of $\log \log x$.

3. We define the von Mangoldt function $\Lambda(n)$ for integers $n \ge 1$ by

$$\Lambda(n) = \begin{cases} \log(p) & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \ge 1\\ 0 & \text{otherwise.} \end{cases}$$

1. Show that for $n \ge 1$, we have

$$\sum_{k=1}^{n} \Lambda(k) = O(n).$$

(Hint: split the sum into the sums over primes, squares of primes, etc, and use Chebychev's estimate.)

<u>Solution</u>: The von Mangoldt function $\Lambda(k)$ is supported on prime powers, so

$$\sum_{k=1}^{n} \Lambda(k) = \sum_{p^{j} \le n} \log p$$
$$= \sum_{p \le n} \log p \left\lfloor \frac{\log n}{\log p} \right\rfloor$$
$$\leq \sum_{p \le n} \log n$$
$$= \pi(n) \log n \le c_{2} \frac{n}{\log n} \log n = c_{2}n,$$

where the last line follows from Chebychev's estimate. Thus $\sum_{k=1}^{n} \Lambda(k) = O(n)$. 2. Show that for any integer $n \ge 1$, we have

$$\sum_{k=1}^{n} \log(k) = \sum_{\substack{p,j \\ p^{j} \le n}} \left\lfloor \frac{n}{p^{j}} \right\rfloor \log(p) = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \Lambda(k).$$

Solution: Writing $n! = \prod_p p^{v_p(n)}$ and recalling the identity that

$$v_p(n) = \sum_{p^j \le n} \left\lfloor \frac{n}{p^j} \right\rfloor,$$

we have

$$\sum_{k=1}^{n} \log k = \log(n)$$
$$= \log\left(\prod_{p} p^{v_p(n)}\right)$$
$$= \sum_{p \le n} v_p(n) \log p$$
$$= \sum_{p^j \le n} \left\lfloor \frac{n}{p^j} \right\rfloor \log p,$$

as desired. For the second equality, note that Λ is supported on prime powers and is precisely log p when k is a power of p, so this follows by the definition of Λ . 3. Show that

$$\sum_{k=1}^{n} \log(k) = n \log(n) + O(n)$$

for $n \ge 1$. (Hint: compare the sum with an integral.) Solution: We have

$$\int_{2}^{n} \log(u) du \leq \sum_{k=1}^{n} \log k \leq \int_{1}^{n} \log(u) du + \log(n+1)$$

$$\Rightarrow (u \log(u) - u|_{2}^{n} \leq \sum_{k=1}^{n} \log k \leq (u \log(u) - u|_{1}^{n} + \log(n+1))$$

$$\Rightarrow n \log n - n - 2 \log 2 + 2 \leq \sum_{k=1}^{n} \log k \leq n \log n - n + 1 + \log(n+1).$$

The upper and lower bounds combined imply that $\left|\sum_{k=1}^{n} \log k - n \log n\right| = O(n)$, as desired.

4. Deduce that

$$\sum_{k=1}^{n} \frac{\Lambda(k)}{k} = \log(n) + O(1)$$

for $n \ge 1$, and that

$$\sum_{p \le n} \frac{\log(p)}{p} = \log(n) + O(1).$$

(Hint: for the first, combine (1), (2) and (3) and $0 \le x - \lfloor x \rfloor \le 1$; for the second, show that the contribution to the first sum of squares and higher powers of primes is bounded.)

Solution: Note first that

$$\frac{1}{n}\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \Lambda(k) = \frac{1}{n}\sum_{k=1}^{n} \log k, \text{ by part (2)}$$
$$= \frac{1}{n}(n\log n + O(n)), \text{ by part (3)}$$
$$= \log n + O(1).$$

The sum we want to evaluate is, however, slightly different. Instead, we have

$$\sum_{k=1}^{n} \frac{\Lambda(k)}{k} = \frac{1}{n} \sum_{k=1}^{n} \frac{n}{k} \Lambda(k)$$
$$= \frac{1}{n} \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \Lambda(k) + \frac{1}{n} \sum_{k=1}^{n} \left(\frac{n}{k} - \left\lfloor \frac{n}{k} \right\rfloor \right) \Lambda(k)$$
$$= \log n + O(1) + O\left(\frac{1}{n} \sum_{k=1}^{n} \Lambda(k)\right),$$

since $\frac{n}{k} - \lfloor \frac{n}{k} \rfloor \leq 1$. Applying part (1) to the final term completes the argument. For the second sum, along with the first result for this question, it suffices to show that

$$\sum_{\substack{p^j \le n \\ j \ge 2}} \frac{\log p}{p^j} = O(1).$$

Summing first over j via geometric series, we have

$$\sum_{p \le n} \log p \sum_{j \ge 2}^{\log_p(n)} \frac{1}{p^j} \le \sum_{p \le n} \log p \sum_{j \ge 2} \frac{1}{p^j}$$
$$= \sum_{p \le n} \log p \frac{1}{p(p-1)}$$
$$\le \sum_{k=1}^{\infty} \frac{\log k}{k^2},$$

noting that for each prime $p, \frac{\log p}{p(p-1)} \leq \frac{\log(p-1)}{(p-1)^2}$, and that we only increase the sum by further extending to all integers k. But the sum over k is convergent (as seen for example by comparing $\frac{\log k}{k^2}$ to $\frac{1}{k^{3/2}}$), so it is bounded by a constant and thus O(1), as desired.

4. (Optional but recommended) Using a computer, make a table of sums of three and four squares, and try to make suitable guesses or conjectures concerning the numbers that appear, which ones don't, and how many times an integer n might be a sum of three or four squares.

Due date: 30/09/2024