D-MATH
FS 2021
Prof. E. Kowalski

Solutions 2

Probabilistic Number Theory

1 a. Suppose that $n = p_1^{e_1} \cdots p_l^{e_l}$ with distinct primes $p_1, \ldots .p_l$ and $e_i \geq 1$. Then

$$\sum_{d \mid n} \Lambda(d) = \sum_{p^\nu \mid n} \log p = e_1 \log p_1 + \cdots + e_l \log p_l = \log n.$$

b. This is partial summation: We have

$$\begin{aligned}\sum_{n \leq x} \frac{\Lambda(n)}{n} &= \frac{1}{x} \sum_{n \leq x} \Lambda(n) - \int_1^x \left(\sum_{n \leq t} \Lambda(n) \right) \left(-\frac{1}{t^2} \right) dt \\ &= \frac{\psi(x)}{x} + \int_1^x \frac{\psi(t)}{t^2} \, dt.\end{aligned}$$

c.

$$\begin{aligned}\sum_{n \leq x} \frac{\Lambda(n)}{n} &= \frac{\psi(x)}{x} + \int_1^x \frac{\psi(t) - t}{t^2} \, dt + \int_1^x \frac{t}{t^2} \, dt \\ &= 1 + O\left(\frac{1}{(\log x)^2} \right) + \int_1^x \frac{\psi(t) - t}{t^2} \, dt + \log x.\end{aligned}$$

Since $\frac{\psi(t)-t}{t^2} = O\left(\frac{1}{t(\log t)^2} \right)$, the integral in A is absolutely convergent and we can write

$$\begin{aligned}\int_1^x \frac{\psi(t) - t}{t^2} \, dt &= \int_1^\infty \frac{\psi(t) - t}{t^2} \, dt + O\left(\int_x^\infty \frac{1}{t(\log t)^2} \, dt \right) \\ &= \int_1^\infty \frac{\psi(t) - t}{t^2} \, dt + O\left(\frac{1}{\log x} \right).\end{aligned}$$

Putting these together gives

$$\begin{aligned}\sum_{n \leq x} \frac{\Lambda(n)}{n} &= \log x + 1 + \int_1^\infty \frac{\psi(t) - t}{t^2} \, dt + O\left(\frac{1}{\log x} \right) \\ &= \log x + A + O\left(\frac{1}{\log x} \right)\end{aligned}$$

as claimed.

d. By using partial summation on c.) and the facts that

$$\int \frac{\log t}{t}\,dt = \frac{1}{2}(\log t)^2 + C \qquad \text{and} \qquad \int \frac{1}{t\log t}\,dt = \log\log t + C,$$

we see that

$$\begin{aligned}
\sum_{n\le x} \frac{\Lambda(n)\log n}{n} &= (\log x)\sum_{n\le x}\frac{\Lambda(n)}{n} - \int_1^x \frac{\sum_{n\le t}\frac{\Lambda(n)}{n}}{t}\,dt \\
&= \log x\left(\log x + A + O\left(\frac{1}{\log x}\right)\right) \\
&\quad - \int_1^x \frac{\log t}{t}\,dt - \int_1^x \frac{A}{t}\,dt + O\left(\int_1^x \frac{1}{t\log t}\,dt\right) \\
&= (\log x)^2 + A\log x - \frac{1}{2}(\log x)^2 - A\log x + O(\log\log x) \\
&= \frac{1}{2}(\log x)^2 + O(\log\log x)
\end{aligned}$$

as required.

e. We have

$$\sum_{n\le x}\frac{\log n}{n} = \sum_{n\le x}\frac{1}{n}\sum_{d\,|\,n}\Lambda(d) = \sum_{d\le x}\Lambda(d)\sum_{\substack{n\le x\\ n\equiv 0\,(d)}}\frac{1}{n} = \sum_{d\le x}\frac{\Lambda(d)}{d}\sum_{m\le x/d}\frac{1}{m}.$$

But

$$\sum_{m\le x/d}\frac{1}{m} = \log x - \log d + \gamma + O\left(\frac{d}{x}\right),$$

hence

$$\begin{aligned}
\sum_{n\le x}\frac{\log n}{n} &= (\log x)\sum_{d\le x}\frac{\Lambda(d)}{d} - \sum_{d\le x}\frac{\Lambda(d)\log d}{d} + \gamma\sum_{d\le x}\frac{\Lambda(d)}{d} \\
&\quad + O\left(\frac{1}{x}\sum_{d\le x}\Lambda(d)\right) \\
&= \log x\left(\log x + A + O\left(\frac{1}{\log x}\right)\right) - \frac{1}{2}(\log x)^2 \\
&\quad + O(\log\log x) + \gamma\log x + O(1) \\
&= \frac{1}{2}(\log x)^2 + (A+\gamma)\log x + O(\log\log x)
\end{aligned}$$

as claimed.

f. Note that $\frac{\log t}{t}$ is monotonically decreasing for $t \geq e$. Therefore, for any $n \geq 4$, we have

$$\int_n^{n+1} \frac{\log t}{t}\, dt \leq \frac{\log n}{n} \leq \int_{n-1}^{n} \frac{\log t}{t}\, dt.$$

Summing this over $4 \leq n \leq x$ gives

$$\begin{aligned}\frac{1}{2}(\log x)^2 - \frac{1}{2}(\log 4)^2 &= \int_4^x \frac{\log t}{t}\, dt \\ &\leq \sum_{4\leq n\leq x} \frac{\log n}{n} \\ &\leq \int_3^x \frac{\log t}{t}\, dt \\ &= \frac{1}{2}(\log x)^2 - \frac{1}{2}(\log 3)^2.\end{aligned}$$

Inserting the small values of n certainly gives

$$\sum_{n\leq x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + O(1).$$

Since we proved in e.) that

$$\sum_{n\leq x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + (A+\gamma)\log x + O(\log\log x),$$

this implies that $A = -\gamma$ and the remaining assertions follow. $\square$

2 a.

- If $p = 2$, then $2 = (\pm 1)^2 + (\pm 1)^2$ are the only 4 possibilities.
- Let now $p \equiv 1 \bmod 4$ and let $m := g^{\frac{p-1}{4}}$. In particular $m^4 \equiv 1$, so $m^2 \equiv \pm 1$. But $p-1$ is the minimun so that $g^{p-1} \equiv 1$, hence $m^2 \equiv -1 \bmod p$. If $p|(m^2+1)$, then $p|(m+i)(m-i)$ in $\mathbb{Z}[i]$. If p were irreducible, we'd have $p|(m+i)$ or $p|(m-i)$. But $\frac{m}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, hence p is irreducible in $\mathbb{Z}[i]$.
  There exist $a, b, c, d \in \mathbb{Z}$ so that $p = (a+ib)(c+id)$. Since $p \in \mathbb{Z}$, we have $p^2 = (a^2+b^2)^2$ and so $p = a^2 + b^2$.
  Moreover, the factorization $p = (a+ib)(c+id)$ is essentially unique in $\mathbb{Z}[i]$, hence
  $$p = (\pm a)^2 + (\pm b)^2 = (\pm b)^2 + (\pm a)^2$$
  are the only 8 possibilities
- If $p \equiv 3 \bmod 4$, then $r(p) = 0$, in particular p irreducible. That's because for all $a \in \mathbb{Z}$, $a^2 \equiv 0$ or $1 \bmod 4$. So a sum of two squares can be only $0, 1$ or $2 \bmod 4$.

- Let now $n = a^2 + b^2$ and $p \equiv 3 \bmod 4$ a divisor of n. Since $p|(a+ib)(a-ib)$ and p is irreducible in $\mathbb{Z}[i]$, we have that either $p|(a+ib)$ or $p|(a-ib)$, so $p|a$ and $p|b$ and so $p^2|n$.
  By induction, one sees that the exponent of p in n must be even.

Finally, from the identity $(a^2+b^2)(c^2+d^2) = (ac+bd)^2(ac-bd^2)$ one has that if n and m are representable as sum of two squares, then so is nm.

b. Let's verify the identity in the case $n = a^2 + b^2$ odd. Write

$$n = p_1^{r_1} \dots p_k^{r_k} q_1^{2n_1} \dots q_s^{2n_s},$$

where $p_i \equiv 1 \bmod 4$ and $q_i \equiv 3 \bmod 4$. Then

$$a + ib = q_1^{n_1} \dots q_s^{n_s} \prod_{i=1}^{k} (a_i + ib_i)^{r_i'} (a_i - ib_i)^{r_i''},$$

where $p_j = a_j^2 + b_j^2$ and $r_j = r_j' + r_j''$. Thus we have $r_j + 1$ possibilities for every j, so $\prod_{j=1}^{k}(r_j+1)$ possibilities in total, which became $4\prod_{j=1}^{k}(r_j+1)$ by counting the units.
If n is odd, we then get

$$\frac{r(n)}{4} = \begin{cases} \prod_{j=1}^{k}(r_j+1) & \text{if } n = p_1^{r_1} \dots p_k^{r_k} q_1^{2n_1} \dots q_s^{2n_s} \\ 0 & \text{if } n \text{ has only odd powers in the factor.} \end{cases}$$

On the other hand, if p is an odd prime, then

$$(\chi_4 * 1)(p^\ell) = \sum_{d|p^\ell} \chi_4(d) = \sum_{c=0}^{\ell} \chi_4(p^c) = \begin{cases} \ell + 1 & \text{if } p \equiv 1 \mod 4 \\ \begin{cases} 1 & \text{if } \ell \text{ is even} \\ 0 & \text{if } \ell \text{ is odd} \end{cases} & \text{if } p \equiv 3 \mod 4. \end{cases}$$

In both cases, we have $(\chi_4 * 1)(p^\ell) = \frac{r(p^\ell)}{4}$.

c. Since $|\chi_4(n)| \leq 1$ for every n,

$$\frac{r(n)}{4} = (\chi_4 * 1)(n) = \sum_{d|n} \chi_4(d) \leq \sum_{d|n} |\chi_4(d)| \leq \tau(n).$$

d. For every point of $\mathbb{Z}^2$, consider the square of side 1 with vertex on the below-left of p. The problem is to compute the sum of the areas of the unitary squares whose vertices on the below-left are inside the circle. This area is greater than the area of the circle of radius $\sqrt{x} - \sqrt{2}$, since the latter circle is contained in these squares. The are is also smaller that the area of the circle of radius $\sqrt{x} + \sqrt{2}$, which contains all these squares. Hnece

$$\pi(\sqrt{x} - \sqrt{2})^2 \leq \sum_{n \leq x} r(n) \leq \pi(\sqrt{x} + \sqrt{2})^2,$$

which implies the claim.

e. This simply follows by the fact that for every $z \geq 1$,

$$\frac{1}{N} \sum_{\substack{n \leq N \\ 1 \leq r(n) \leq z}} 1 \leq \frac{1}{N} \sum_{\substack{n \leq N \\ 1 \leq r(n)}} 1 \ll \frac{1}{N} \frac{N}{\sqrt{\log N}} \xrightarrow[N \to +\infty]{} 0.$$