Solutions to Sheet 10.

Reminder: $\mathrm{Li}(n) := \int_2^n \frac{1}{\log t}\,\mathrm{d}t$.

Problem 1

This exercise tests your understanding of the Siegel-Walfiz theorem. Let's write down explicitely what it says.

Theorem 1 (Explicit Siegel-Walfisz)**.** *Let $A > 0$. There is a constant $K = K(A)$ and a constant c such that whenever $q < (\log x)^A$, we have the approximation (with K and c independent of q!!!)*

$$\left|\frac{x}{\varphi(q)} - \psi(x;q,a)\right| < Kx\mathrm{e}^{-c\sqrt{\log x}}.$$

It is a routine exercise in partial summation to obtain the corresponding statement for $\pi(x)$, which reads (with the same c)

Theorem 2 (Explicit Siegel-Walfisz for π)**.** *Let $A > 0$. There is a constant $K = K(A)$ and a constant c such that whenever $q < (\log x)^A$, we have the approximation (with K and c independent of q!!!)*

$$\left|\frac{\mathrm{Li}(x)}{\varphi(q)} - \pi(x;q,a)\right| < Kx\mathrm{e}^{-c\sqrt{\log x}}.$$

In particular, if q is large enough and we choose x such that $q < \log(x)^A$ (i.e., so large that we can apply Siegel-Walfisz), we have $Kx\mathrm{e}^{-c\sqrt{\log x}} < \frac{\mathrm{Li}(x)}{\varphi(q)} + 1$, so that $\pi(x;q,a) > 0$. The condition $q < (\log x)^A$ is equivalent to $\mathrm{e}^{q^{1/A}} < x$. As A may be chosen arbitrarily large, this implies that we have $\pi(x;q,a) > 0$ if $x \gg \mathrm{e}^{q^{\varepsilon}}$.

This bound might feel unsatisfying, because $\exp(q^{\varepsilon})$ is huge compared to q! We cannot do much better because the possibility of Siegel-Zeroes forces us to impose hard restrictions on the size of q compared to x. However, if the generalized Riemann hypothesis were true, we wouldn't have to worry about them. Perron's formula would the estimate

$$\psi(x,\chi) \ll (\log q)x^{\frac{1}{2}+\varepsilon}$$

and hence

$$\psi(x;q,a) = \frac{1}{\varphi(q)}\sum_{\chi}\sum_{n}\chi(n)\Lambda(n)n^{-s} = \frac{x}{\varphi(q)} + O((\log q)x^{1/2+\varepsilon}). \tag{1}$$

(I am not completely sure with the error term, but you might be able to work this out yourself. You will need the approximations

$$\frac{L'}{L}(s,\chi) = \begin{cases} O(1) & \mathrm{Re}\, s \geq 2 \\ O(\log q\,|s|) & \mathrm{Re}\, s \leq -\frac{1}{2} \text{ and } |s+m| > \frac{1}{4}\forall m \in \mathbb{N} \\ \sum_{|t-\mathrm{Im}\,\rho|\leq 1}\frac{1}{s-\rho} + O(\log(q(2+|t|))) & -\frac{1}{2} \leq \mathrm{Re}\, s \leq 2, \end{cases}$$

where the latter sums goes over the non-trivial zeroes of $L(s,\chi)$.) Anyways, we observe that the main term of (1) dominates the error if $q^{2+\varepsilon} < x$. This is the desired bound.

Problem 2

(a) Let's try partial summation in conjunction with Polya-Vinogradov.

$$\sum_{M<n\leq N} \chi(n)n^{-s} = N^{-s}\sum_{n\leq N}\chi(n) - M^{-s}\sum_{n\leq M}\chi(n) + s\int_M^N t^{-s-1}\sum_{M<n\leq t}\chi(n)\,\mathrm{d}t$$

Now Polya-Vinogradov gives that every sum can be bound by $O(q^{1/2}\log q)$. We obtain

$$\sum_{M<n\leq N}\chi(n)n^{-s} \ll M^{-\operatorname{Re}s}q^{\frac{1}{2}}\log q + |s|\int_M^N t^{-\operatorname{Re}s-1}q^{\frac{1}{2}}\log q\,\mathrm{d}t \ll \frac{|s|\,qM^{-\operatorname{Re}s}}{\operatorname{Re}s}.$$

Here we completed the integral and bounded $q^{\frac{1}{2}}\log q \ll q$. (This is not optimal, but it doesn't matter).

(b) Note that in part a, we can choose N arbitrarily large (without changing the implicit constant in $\ll$!). Hence it makes sense to choose some $M > 2$ and split the sum $L(s,\chi) = \sum_{n\in\mathbb{N}}\chi(n)n^{-s}$ into the parts $n \leq M$ and $n > M$ and apply the result of part a for the latter sum. How large do we have to choose M in order to make this work? As $\operatorname{Re}s > 1-(\log q)^{-1}$ and $|\operatorname{Im}s| < q$ we find $|s| \ll q\operatorname{Re}s$. With part a, this gives

$$\sum_{M<n}\chi(n)n^{-s} \ll q^2M^{(\log q)^{-1}-1}.$$

If we choose $M = q^2$, this reduces to $\ll 1$, so let's see if the sum with terms $n < M$ is small enough. We trivially bound

$$\sum_{n<M}\chi(n)n^{-s} \ll \sum_{n<M} n^{(\log q)^{-1}}n^{-1} \ll \int_1^M t^{(\log q)^{-1}-1}\,\mathrm{d}t = \Big[(\log q)t^{(\log q)^{-1}}\Big]_1^M.$$

As $M = q^2$ and $(q^2)^{(\log q)^{-1}} = \mathrm{e}^{2(\log q)(\log q)^{-1}} = \mathrm{e}^2 \ll 1$, we are done.

(c) We will prove this with Cauchy's integral formula. Remember what it says:

$$L'(s,\chi) = \frac{1}{2\pi\mathrm{i}}\int_C \frac{L(z,\chi)}{(z-s)^2}\,\mathrm{d}z,$$

where C is some path convoluting s. We choose C to be the circle $\{z \mid |z-s| = (\log q)^{-1}\}$. This might cause us to leave the domain $\operatorname{Re}s > 1-(\log q)^{-1}$, however the bound of part b stays valid even if $\operatorname{Re}s > 1-2(\log q)^{-1}$. We get

$$L'(s,\chi) \ll \int_{|z-s|=(\log q)^{-1}} \frac{L(z,\chi)}{(z-s)^2}\,\mathrm{d}z \ll (\log q)^2.$$

Here we used $L(z,\chi) \ll \log q$ and $(s-z)^{-2} \ll (\log q)^2$, so the part in the integral is bounded by $O((\log q)^3)$. As we integrate over a path with length $O((\log q)^{-1})$, we obtain a bound with $O((\log q)^2)$, and we win.

Problem 3

Before solving this, we should maybe try to figure out why we would expect this result. Given some number n, we are supposed to evaluate the counting function

$$R(n) = \#\{p \leq n \mid n-p \text{ is square free}\}.$$

Naively, one might be think that

$$R(n) \approx \zeta(2)^{-1}\pi(n) = \prod_p (1-p^{-2})\pi(n),$$

as the propability of a random number to be square-free is (in a suitable sense) given by $\zeta(2)^{-1}$, and we inspect numbers (which seem random) in a set of cardinality $\pi(n)$. This heuristic is not too far off, but it is wrong! The main term of the asymptotic is clearly different.
To see what goes wrong, let q be any prime number. First assume that $q \nmid n$. What is the probability that q^2 divides $n-p$ for some prime $p \neq q$? Neither n nor p are divisible by q, so the residue classes of these numbers mod q^2 are invertible, and there are $\varphi(q^2)$ such residue classes. So the probability is given by $\varphi(q^2)^{-1}$. Now assume $q \mid n$. One quickly checks that q^2 cannot divide $n-p$ (unless $p = q$, but this case does not contribute much). Now we can explain the asymptotic: There are $\approx \mathrm{Li}(n)$ primes $\leq n$, and the probability for $n-p$ not being divisible by some prime q is given by $(1-\varphi(q^2)^{-1})$ if $q \nmid n$ and by 1 if $q \mid n$. As $n-p$ is square-free iff no square of a prime divides it, we should expect

$$R(n) \approx \prod_{q \nmid n} (1-\varphi(q^2)^{-1})\mathrm{Li}(n) = \prod_{q \nmid n} \left(1 - \frac{1}{q(q-1)}\right)^{-1} \mathrm{Li}(n),$$

and this is what we have to prove.

Proof. Clearly, we have $R(n) = \sum_{p \leq n} \mu^2(n-p)$. A standard trick to deal with μ^2 is writing it as $\mu(k) = \sum_{d^2 \mid k} \mu(d)$. Applying this gives

$$R(n) = \sum_{p \leq n} \mu^2(n-p) = \sum_{p \leq n} \sum_{d^2 \mid n-p} \mu(d) = \sum_{d \leq \sqrt{n}} \mu(d) \sum_{p \leq n,\ p \equiv n \bmod d^2} 1.$$

This is now basically an issue of counting primes in an arithmetic progression! Hence it really smells like Siegel-Walfisz, but this is not applicable right away. One issue is that we can only apply Siegel-Walfisz if $(d,n) = 1$. But restricting to those d does not really affect our main term, as whenever $(d,n) > 1$ there is at most one prime number in that arithmetic progression, and the contribution of those is bounded by $\omega(n) \ll n^{\varepsilon}$. Furthermore, and more seriously, Siegel-Walfisz is only applicable if d is small compared to n, more precisely, only if $d < (\log n)^A$. But again, we can elementarily bound the terms with $d > (\log n)^A$. Given some d, the amount of numbers $< n$ congruent to n mod d^2 can be bounded by $\ll \frac{n}{d^2}$. We obtain

$$R(n) = \sum_{d \leq (\log n)^A,\ (d,n)=1} \psi(n; n, d^2) + O\left(\sum_{(\log n)^A < d < \sqrt{n}} \frac{n}{d^2}\right) + O(\sqrt{n}),$$

and the O-terms can be bound by $\ll \frac{n}{(\log n)^A}$. Also, we can now apply Siegel-Walfisz! We find

$$R(n) = \sum_{d \leq (\log n)^A,\ (d,n)=1} \frac{1}{\varphi(d^2)} \mathrm{Li}(n) + O\left(\frac{n}{(\log n)^A}\right).$$

The sum can be completed, as $\varphi(d^2) \gg \frac{d^2}{\log\log d} \gg d^{2-\varepsilon}$, so that

$$\sum_{d > (\log n)^A} \frac{1}{\varphi(d^2)} \ll \frac{1}{(\log n)^{A(1-\varepsilon)}}.$$

This allows us to conclude (for any A, not the choice we made before)

$$R(n) = \sum_{d \in \mathbb{N},\ (d,n)=1} \frac{1}{\varphi(d^2)} \mathrm{Li}(n) + O_A\left(\frac{n}{(\log n)^A}\right) = \prod_{p \nmid n} \left(1 - \frac{1}{\varphi(p^2)}\right) \mathrm{Li}(n) + O_A\left(\frac{n}{(\log n)^A}\right).$$

Problem 4

We follow the hint. Let $n \equiv 3 \mod 4$, write it as $n = 4k+3$. Now

$$\frac{4}{n} - \frac{1}{k+1} = \frac{4}{n} - \frac{4}{n+1} = \frac{4}{n(n+1)} = \frac{4}{(4k+3)(4k+4)} = \frac{1}{(4k+3)(k+1)}.$$

This shows that there is a solution for every $n \equiv 3 \mod 4$. One also quickly verifies that if $\frac{4}{n} = \frac{1}{a} + \frac{1}{b}$, then $\frac{4}{mn} = \frac{1}{ma} + \frac{1}{mb}$. Also, there is a solution whenever n is even. Hence we really only have to show that almost all numbers have a prime divisor $\equiv 3 \mod 4$.

Now we can use (5.15). The numbers having only prime factors congruent 1 mod 4 is a subset of the numbers that can be written as a sum of two squares, and by (5.15), the number of sums of two squares up to x is bound by $O(\frac{x}{\sqrt{\log x}}) = o(x)$.

Max von Consbruch, email: s6mavonc@uni-bonn.de. Date: January 10, 2023