SIEVE THEORY 2015, PROF. ZEEV RUDNICK
TAKE-HOME EXAM
DUE DATE: JULY 15, 2015

Instructions: The assignment should be delivered to my mailbox or sent via email (rudnick@post.tau.ac.il) by Wednesday, 15 July 2015 at latest.

Exercise 1. For $N \geq 1$, the Farey sequence of level N is defined to be all rationals in $(0, 1]$ which in reduced form have denominator at most N:

$$\mathcal{F}_N = \{\frac{a}{q} : \gcd(a, q) = 1,\ 1 \leq a \leq q \leq N\} .$$

For instance, $\mathcal{F}_5 = \{\frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$. Show that

$$\#\mathcal{F}_N = \frac{N^2}{2\zeta(2)} + O(N \log N) .$$

Hint: $\varphi(n) = n \sum_{d|n} \mu(d)/d$.

Exercise 2. Show that

$$\sum_{n \leq x} \Lambda(n)^2 = x \log x - x + o(x)$$

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

Exercise 3. A Carmichael number is a composite integer N for which $a^{N-1} = 1 \bmod N$ for all a coprime to N.

a) Show that if N is a Carmichael number, then N is odd, and that for all prime divisors $p \mid N$, we have $p - 1 \mid N - 1$ (this is a converse of Korselt's criterion).

b) Show that for $p > 3$, if p, $q := 2p - 1$ and $r := 3p - 2$ are all prime, then their product $N = pqr$ is a Carmichael number.

Exercise 4. Show that the number of integers $n \leq x$ so that n, $2n - 1$, $3n - 2$ are all primes, is at most $\ll x/(\log x)^3$.

Exercise 5. For a monic integer polynomial

$$f(t) = t^n + a_{n-1}t + \cdots + a_0$$

we define the height as $\mathrm{Ht}(f) = \max_j |a_j|$. We define

$$\mathcal{R}_n(N) = \{f(t) = t^n + a_{n-1}t + \cdots + a_0 : \mathrm{Ht}(f) \leq N; \text{reducible over } \mathbb{Q}\}$$

to be the set of <u>reducible</u> monic polynomial of degree n with integer coefficients, of height at most N. Show that for $n > 2$,

$$\#\mathcal{R}_n(N) \ll_n N^{n-\frac{1}{2}} \log N .$$

Hint: Use the large sieve in its n-dimensional form, where

$$\Omega_p = \{f \in \mathbb{F}_p[t], \deg f = n,\ \text{monic irreducible over } \mathbb{F}_p\} .$$