Math 1580 – Problem Set 6 (a.k.a. a bunch of problems about $L(X)$). Due Friday Oct. 21, 4pm

Problem 1. Prove that the function $L(X) = e^{\sqrt{(\ln X)(\ln\ln X)}}$ is subexponential. In other words, show that

(a) For every positive constant α, no matter how large, $L(X) = \Omega\left((\ln X)^{\alpha}\right)$.
(b) For every positive constant β, no matter how small, $L(X) = \mathcal{O}(X^{\beta})$.

Problem 2. (a.k.a. more fun with logarithms than you ever had before.) This exercise asks you to verify an assertion in the proof of Corollary 3.44.

(a) Prove that there is a value of $\epsilon > 0$ such that

$$(\ln X)^{\epsilon} < \ln L(X) < (\ln X)^{1-\epsilon} \quad \text{for all } X > 10.$$

(b) Let $c > 0$, let $Y = L(X)^c$, and let $u = (\ln X) / (\ln Y)$. Prove that

$$u^{-u} = L(X)^{-\frac{1}{2c}(1+o(1))}.$$

Problem 3. Proposition 3.47 assumes that we choose random numbers a modulo N, compute $a^2 \pmod{N}$, and check whether the result is B-smooth. We can achieve better results if we take values for a of the form

$$a = \lfloor\sqrt{N}\rfloor + k \quad \text{for } 1 \le k \le K.$$

(For simplicity, you may treat K as a fixed integer, independent of N. More rigorously, it is necessary to take K equal to a power of $L(N)$, which has a small effect on the final answer.)

(a) Prove that $a^2 - N \le 2K\sqrt{N} + K^2$, so in particular $a^2 \pmod{N}$ is $\mathcal{O}(\sqrt{N})$.
(b) Prove that $L(\sqrt{N}) \approx L(N)^{1/\sqrt{2}}$ by showing that

$$\lim_{N\to\infty} \frac{\ln L(\sqrt{N})}{\ln L(N)^{1/\sqrt{2}}} = 1.$$

More generally, prove that in the same sense, $L(N^{1/r}) \approx L(N)^{1/\sqrt{r}}$ for any fixed $r > 0$.
(c) Re-prove Proposition 3.47 using this better choice of values for a. Set $B = L(N)^c$ and find the optimal value of c. Approximately how many relations are needed to factor N?

Problem 4. Illustrate the quadratic sieve, as was done in class and in Figure 3.3 (page 157), by sieving prime powers up to B on the values $F(T) = T^2 - N$ in the indicated range.

(a) Sieve $N = 493$ using prime powers up to $B = 11$ on the values from $F(23)$ to $F(38)$. Use the relations that you find to factor N.
(b) Extend the computations in (a) by using prime powers up to $B = 16$ and sieving values from $F(23)$ to $F(50)$. What additional values are sieved down to 1 and what additional relations do they yield?