Homework 7

Due **Saturday**, October 30

Written Part

5. In problem 1 we computed square roots using Sage's built in functionality. But if $p \equiv 3 \mod 4$, there is actually an easy algorithm! So fix $p \equiv 3 \mod 4$ and let $a \in \mathbb{F}_p^*$ have a square root mod p. Give a $\mathcal{O}(\log p)$ algorithm to compute a square root of a modulo p, and prove its correctness. (*Hint: You can do this in a single exponentiation!*)

   Proof. We will show that if $p \equiv 3 \mod 4$ and $a \in \mathbb{F}_p^*$. Then $a^{\frac{p+1}{4}}$ is a square root of a. To see this, compute:

$$\begin{aligned}\left(a^{\frac{p+1}{4}}\right)^2 &= a^{\frac{p+1}{2}} \\ &= a^{\frac{p-1}{2}+1} \\ &= a^{\frac{p-1}{2}} \cdot a \\ &\equiv a \mod p\end{aligned}$$

   where in the last step we observe that since a has a square root, we know $a^{\frac{p-1}{2}} \equiv 1 \mod p$ by Euler's Criterion (HW5 Problem 8a). Therefore, the algorithm for computing the square root of a is merely using fast powering to compute $a^{\frac{p+1}{4}}$. $\square$

6. Let $L(X) = e^{\sqrt{\ln x \ln \ln x}}$. Prove that $L(X)$ is subexponential (in the number of bits of X) by proving:

   (a) $L(X) = \mathcal{O}(X^\beta)$ for every $\beta > 0$.

   Proof. Let $\beta > 0$. We compute:

$$\begin{aligned}\lim_{x\to\infty} \frac{e^{\sqrt{\ln x \ln\ln x}}}{x^\beta} &= \lim_{x\to\infty} \frac{e^{\sqrt{\ln x \ln\ln x}}}{e^{\beta \ln x}} \\ &= \lim_{x\to\infty} e^{\sqrt{\ln x \ln\ln x} - \beta \ln x}.\end{aligned}$$

   We will show that the exponent converges to $-\infty$ so that the limit converges to 0. For simplicity, we make the substitution $k = \ln x$, and note that $x \to \infty$ if and only if $k \to \infty$. Then we are computing:

$$\lim_{k\to\infty} \sqrt{k \ln k} - \beta k = -\infty,$$

   It suffices to show that the second term grows faster, that is:

$$\lim_{k\to\infty} \frac{\beta k}{\sqrt{k \ln k}} = \lim_{k\to\infty} \frac{\beta\sqrt{k}}{\sqrt{\ln k}} = \infty,$$

   which is true as polynomial growth is faster than logarithmic growth. $\square$

   (b) $L(X) = \Omega((\ln X)^\alpha)$ for every $\alpha > 0$.

Proof. In class we showed that if $f(x) = e^{\sqrt{\ln x}}$ then $f(x) = \Omega((\ln x)^\alpha)$ for every $\beta > 0$. It therefore suffice to show that $L(x) = \Omega(f(x))$. Notice that if $x > e^e$, then $\ln\ln(x) > \ln\ln(e^e) = \ln(e) = 1$, so that $\ln x \ln\ln x > \ln x$. In particular, we may conclude that for all such x:

$$L(x) = e^{\sqrt{\ln x \ln\ln x}} > e^{\sqrt{\ln x}} = f(x),$$

so that $L(x) = \Omega(f(x))$, completing the proof.

For completeness we include the proof that $f(x) = \Omega((\ln x)^\alpha)$ for every $\beta > 0$. Using the Taylor series for e^t, we see that:

$$f(x) = \sum_{n=0}^{\infty} \frac{(\ln x)^n}{n!}.$$

For any $N > 0$, let T_N be the N'th taylor polynomial:

$$T_N(x) = \sum_{n=0}^{N} \frac{(\ln x)^n}{n!}.$$

Since $\frac{(\ln x)^n}{n!} > 0$ for $x > 1$, we see that $f(x) > T_N(x)$ for $x > 1$. In particular, $f(x) = \Omega(T_N(x))$ for any N. Fix any $\alpha > 0$ and fix $N > \alpha$. We are done if we can show:

$$\lim_{x\to\infty} \frac{(\ln x)^\alpha}{T_N(x)} < \infty.$$

For simplicity, we make the substitution $k = \ln x$. Then $k \to \infty$ if and only if $x \to \infty$, so it suffices to show that:

$$\lim_{k\to\infty} \frac{k^\alpha}{1 + k + k^2/2 + \cdots + k^N/N!} = 0.$$

But this is clear as the denominator is a polynomial of degree greater than the numerator. $\square$

7. Optimizing the various parts of our sieve factorization algorithm one can show that we can factor N in about $\mathcal{O}(L(N))$, which is subexponential! Let's see how good this is. For simplicity, suppose it takes about $L(N)$ computations to factor N, and we have a computer than can run a billion computations in a second. How long would it take to factor N of the following orders. (Put your answer in seconds, days, years...whatever is appropriate. Also if you do your computations on cocalc turn that part in too so the grader can see).

   (a) $N \approx 2^{100}$. 0.027802429905024805 seconds.

   (b) $N \approx 2^{250}$. 159.2147074064945 minutes.

   (c) $N \approx 2^{500}$. 1130.0731911459704 years.

   (d) $N \approx 2^{1000}$. 5.553235322322046 trillion years.

Recall the function $\Psi(X, B) = \#\{n \leq X : n \text{ is } B\text{-smooth}\}$. In class we stated the following claim about the growth of Ψ in certain cases

Theorem 1 ([HPS] Theorem 3.43)**.** *Suppose there exists some* $0 < \varepsilon < 1/2$ *such that:*

$$(\ln X)^{\varepsilon} < \ln B < (\ln X)^{1-\varepsilon}.$$

Let u *be the ratio* $\ln X / \ln B$*. Then the number of* B*-smooth numbers less than* X *satisfies:*

$$\Psi(X, B) \approx X u^{-u}.$$

(Note, here $\approx$ can be taken to mean that their difference is a function whose limit as X goes to infinity is 0, although in the book they have something slightly more precise). This had the following Corollary, which is more useful for our analyis.

Corollary 1 ([HPS] Corollary 3.45)**.** *Let* $0 < c < 1$*. Then:*

$$\Psi(X, L(X)^{c})) \approx X \cdot L(X)^{(-1/2c)}.$$

8. Prove Corollary 1 using Theorem 1. In particular, prove the following two steps.
   (a) Show that there exists some $0 < \varepsilon < 1/2$ with

   $$(\ln X)^{\varepsilon} < \ln(L(X)^{c}) < (\ln X)^{1-\varepsilon}.$$

   Proof. Making the subsitution $k = \ln X$ we'd like to show that:

   $$k^{\varepsilon} < c\sqrt{k \ln k} < k^{1-\varepsilon},$$

   for k large enough. Let $\delta = 1/2 - \varepsilon$. Then this means showing:

   $$k^{1/2} k^{-\delta} < k^{1/2} c \sqrt{\ln k} < k^{1/2} k^{\delta},$$

   and since k is positive we can cancel the $k^{1/2}$ and therefore show that:

   $$k^{-\delta} < c\sqrt{\ln k} < k^{\delta}.$$

   for any $\delta > 0$, $0 < c < 1$, and k large enough. Since the left side approaches 0 as $k \to \infty$, the left inequality is clear. The right inequality follows from the observation that polynomial growth is faster than logarithmic. □

   (b) Let $u = \ln X / \ln(L(X)^{c})$. Show that:

   $$u^{-u} \approx L(X)^{-1/2c}.$$

   Then leverage that $\approx$ is transitive to deduce the corollary.
   (*Hint*: Write $u^{-u} = L(X)^{\frac{-1}{2c}(1+f(X))}$ for some function $f(X)$ such that $\lim_{X\to\infty} f(X) = 0$. In fact, this is the definition of $\approx$ given in the book!).

   Proof. Note that $\ln(L(X)^{c}) = c \ln L(X)$. To try to keep our heads on straight we make the simplifying substitution $k = \ln X$. With this and the first sentence in mind we compute:

   $$u = \frac{k}{c\sqrt{k \ln k}} = \frac{1}{c}\sqrt{\frac{k^2}{k \ln k}} = \frac{1}{c}\sqrt{\frac{k}{\ln k}}.$$

Therefore:

$$u^{-u} = \left(\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right)^{-\frac{1}{c}\sqrt{\frac{k}{\ln k}}} = e^{\ln\left(\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right)\cdot\left(-\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right)},$$

where in the last step we use that $t = e^{\ln t}$ for any t. Let's focus for a moment on the exponent.

$$\begin{aligned}
\ln\left(\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right)\cdot\left(-\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right) &= (1/2\ln k - \ln c - 1/2\ln\ln k)\cdot\left(-\frac{1}{c}\sqrt{\frac{k}{\ln k}}\right)\\
&= \frac{-1}{2c}(\ln k)\left(1 - 2\frac{\ln c}{\ln k} - \frac{\ln\ln k}{\ln k}\right)\sqrt{\frac{k}{\ln k}}\\
&= \frac{-1}{2c}\sqrt{k\ln k}(1+f(k)),
\end{aligned}$$

where $f(k) = -(2\frac{\ln c - \ln\ln k}{\ln k})$ goes to 0 as $k \to \infty$. Therefore, substituing back in for $X = e^k$ we see that:

$$u^{-u} = e^{-\frac{1}{2c}\sqrt{\ln X\ln\ln X}(1+f(2^x))} = L(X)^{-\frac{1}{2c}(1+f(\ln x))},$$

where $f(\ln x) \to 0$ as $x \to \infty$, giving the result! $\square$