[P12] (Lower bound on number of primes). Let $\pi(n)$ be the number of primes smaller than or equal to n. The prime number theorem says that $\pi(n) \simeq \frac{n}{\ln n}$. Here, the task is to find a simple proof for the slightly weaker statement

$$\pi(n) \geq \frac{n}{2 \log n}.$$

(We use ln for the natural logarithm and log for the logarithm with base 2.)

(1) The *Chebyshev function* is $\psi(n) := \sum_{p \leq n} (\log p) \lfloor \frac{\log n}{\log p} \rfloor$, where the sum over all primes p smaller than or equal to n. Prove the two estimates

$$\pi(n) \log n \geq \psi(n) \geq \sum_{p \leq n} (\max\{k \,|\, p^k \leq n\}) \log p.$$

(2) Assume now that n is even. What is the largest prime that can divide the *central binomial coefficient* $\binom{n}{n/2}$? Use the answer to show that

$$\sum_{p \leq n} (\max\{k \,|\, p^k \leq n\}) \log p \geq \log \binom{n}{n/2}.$$

(3) Write out the definition for $\binom{n}{n/2}$. By canceling appropriate terms, the defining fraction can be brought into the form "a power of 2" times "a number greater than one". Use this approach to show that $\log \binom{n}{n/2} > \frac{n}{2}$. This concludes the proof.

(4) We have seen in the lecture that if $n_1 = p_1 q_1$ and $n_2 = p_2 q_2$ share a prime, the keys can be factored using Euclid's algorithm. Assume Alice creates a 2048 bit key by randomly choosing numbers between 1 and 2^{1024} until she has found two primes p, q. What is the expected number of draws required for this? Show that the probability of two such keys sharing a factor is considerably smaller than one over the number of hydrogen particles in the universe (by any plausible-looking estimate the Internet provides). (6)

[P13] Show that the integers a_i that specify a rational number s/r in the continued fraction expansion also appear in Euclid's algorithm when computing the greatest common divisor of s and r. (Note that this implies that the c.f.e. of a rational terminates and does so after logarithmically many steps). (2)