Number Theory for Computer Scientists 89-256
Question Sheet 3
Due May 3, 2011 // 29 Nisan 5771

(1) Prove that for every integer $1 \leq n \leq 512$ there exists a prime number p such that $n < p \leq 2n$.
Hint: One of the primes 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631 always works.

(2) Suppose that Alice uses the Rabin encryption protocol with public key $n = 4757$. Suppose she agrees with Bob that he only sends messages m whose first two and last two digits are equal when m is written in base 2. Suppose Bob sends the encrypted message 1935. Decrypt.

(3) Recall that $\theta(x) = \sum_{p \leq x} \ln p$. You may assume it known that there exist constants $C_1, C_2 > 0$ such that $C_1 x < \theta(x) < C_2 x$ for all $x \geq 1$. (In class we proved that C_2 exists and that we may take $C_2 = 2 \ln 2$.) Deduce the following weak version of Bertrand's postulate: there exists a constant $B > 1$ such that for all $n \geq 1$ there is a prime number p such that $n < p \leq Bn$.

(4) Let $n = 768283049$. The solutions of the congruence $x^2 \equiv 27468081 \mod n$ are:

$$\begin{aligned} x &\equiv 5241 \mod n \\ x &\equiv 16929093 \mod n \\ x &\equiv 751353956 \mod n \\ x &\equiv 768277808 \mod n. \end{aligned}$$

Find the factorization of n into primes.

חג פסח כשר ושמח!