Number Theory for Computer Scientists 89-256
Question Sheet 1
Due March 22, 2001

Please feel free to e-mail me at `mschein@math.biu.ac.il` with any questions.

(1) Suppose that $a \equiv b \mod n$. Prove that $(a, n) = (b, n)$.
(2) Suppose that $n, m \in \mathbb{N}$ and their decompositions into prime factors are known: $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $m = q_1^{a_1} q_2^{a_2} \cdots q_s^{a_s}$. In terms of these decompositions, what is (m, n)? What is the least common multiple (lcm) of m and n? Prove that $(m, n) \cdot \operatorname{lcm}(m, n) = mn$.
(3) Let $a, b \in \mathbb{Z}$. The following algorithm computes their greatest common divisor without needing to know the prime factor decompositions of a and b. Prove that it indeed runs in finite time (in fact, in runs in polynomial time, but you are not asked to prove this) and always outputs the correct answer.
    - Step 1: Set $a_0 = a$ and $b_0 = b$.
    - Step 2: Replacing a_n and b_n by their absolute values if necessary, we may assume without loss of generality that $a_n, b_n \geq 0$. If $a_n = b_n$, then output $(a, b) = (a_n, b_n) = a_n$. Otherwise, switching a_n and b_n if necessary, assume $a_n > b_n \geq 0$ and proceed to the next step.
    - Step 3: Using the Euclidean algorithm for division, write $a_n = qb_n + r_n$, where $0 \leq r_n < b_n$.
    - Step 4: If $r_n = 0$, then output $(a, b) = (a_n, b_n) = b_n$.
    - Step 5: If $r_n \neq 0$, then set $a_{n+1} = b_n$ and $b_{n+1} = r_n$ and run Step 2 with a_{n+1}, b_{n+1}.
(4) Use the algorithm from the previous question to compute $(455, 1235)$.
(5) Consider the series $\{a_n\}_{n \geq 1}$ given by $a_1 = 1$, $a_2 = 11$, $a_3 = 111$, $a_4 = 1111$, etc. In other words, a_n is the number whose representation in base 10 is given by n consecutive ones. Prove that a_n is never a perfect square if $n > 1$.
(6) Let $p \in \mathbb{N}$ be such that p and $p^2 + 2$ are both prime. Prove that $p = 3$.
(7) Let $\{a_n\}$ be the sequence defined recursively as follows: $a_1 = 0, a_2 = 1$, and if $n \geq 3$ then a_n is obtained by concatenating the base 10 representations of a_n and a_{n-1}. For instance, $a_3 = 10$, $a_4 = 101$, $a_5 = 10110$, $a_6 = 10110101$, etc. Prove that $a_n \equiv 0 \mod 11$ if and only if $n \equiv 1 \mod 6$.
(8) Let $p > 3$ be prime. Prove that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & : p \equiv 1 \mod 6 \\ -1 & : p \equiv 5 \mod 6. \end{cases}$$

(9) Let p be an odd prime and assume $p \neq 5$. Prove that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & : p \equiv \pm 1 \mod 10 \\ -1 & : p \equiv \pm 3 \mod 10. \end{cases}$$

(10) Let $n, a, b \in \mathbb{N}$. Prove that if $b|a$, then $(n^b - 1)|(n^a - 1)$.

(11) Prove that $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$. Does this remain true if we replace 2 by an arbitrary natural number?