INTRODUCTION TO NUMBER THEORY. (Fall 2015)

1. EXERCISES (Mo 7.9)

1. Prove using the definition of divisibility: if $a|b_j$ for $j = 1, \ldots, \ell$, then in $a|(b_1 + \ldots + b_\ell)$.

2. Prove the formula given in the lectures: if n ja m have the prime factorizations

$$n = \prod_{k=1}^{\infty} p_k^{\alpha_k} \quad \text{and} \quad m = \prod_{k=1}^{\infty} p_k^{\beta_k},$$

then the greatest common divisor (a, b) can be expressed in the form

$$(a, b) = \prod_{k=1}^{\infty} p_k^{\gamma_k}, \quad \text{where } \gamma_k = \min(\alpha_k, \beta_k).$$

3. Let a ja b be positiive integers with prime factorizations as in the previous exercise. Denote

$$h := \prod_{k=1}^{\infty} p_k^{\gamma_k}, \quad \text{where } \gamma_k = \max(\alpha_k, \beta_k).$$

Show that h is the unique integer with the properties:

(1) $a|h$ ja $b|h$, (2) jos $a|h'$ ja $b|h'$, niin $h|h'$, (3) $h \geq 1$.

This number is called the *smallest common multiple* of the numbers a and b, and it is often denoted by l.c.m(a, b).

4. Use the Euclidean algorithm

(i) to find the greatest common divisor of the numbers 2015 and 755.

(ii) to find the general solution (in integers) of the equation $276x + 1578y = 714$.

5. (i) Assume that $a_1, a_2, \ldots, a_n$ are integers that are not all zero. Show that there exists number $d = (a_1, \ldots, a_n)$ (the greatest common divisor of these numbers), which satisfies

(1) $d|a_j$ for all $1 \leq j \leq n$,

(2) if $d'|a_j$ for all $1 \leq j \leq n$, then $d'|d$,

(3) $d \geq 1$.

(ii) Deduce that the equation $a_1x_1 + \ldots a_nx_n = d$ is always solvable (in integers).

[Hint: The proof of Thm 1.5 generalizes as such and (ii) follows again as a corollary.]

6. Show that if $a \equiv b \pmod{m}$, then $(a, m) = (b, m)$.

7*. [This is so-called $*$-exercise. They give more challenge to afficinadoes. One gets extra bonus points from them, but possibly there is not enough time to cover them during the exercise hours.]

The idea of the present exercise os to clarify that unique decomposiion into primes is a non-trivial fact. Instead of natural numbers consider the set $\widetilde{\mathbf{N}} = \{4k+1 : k \geq 0\} = \{1, 5, 9, 13, \ldots\}$. Show first that it is closed under multiplication: if $n, m \in \widetilde{\mathbf{N}}$,then $nm \in \widetilde{\mathbf{N}}$. We define in a natural way that $p \geq 2$, $p \in \widetilde{\mathbf{N}}$, is a 'prime' if it cannot be represented as a product $p = nm$, where $n, m \geq 2$ ja $n, m \in \widetilde{\mathbf{N}}$. Verify that any element in $\widetilde{\mathbf{N}}$ is a product of 'primes'. However, show that there is $n \in \widetilde{\mathbf{N}}$, for which the 'prime' factorization' is not unique!!

Hints:

T.5: [The proof of Thm 1.5 generalizes as such and (ii) follows again as a corollary.]