Exercise set 2 **Number Theory**
Tuesday SEP 27 2011 at 4 pm. SHARP (!) **in MaD-302**

1. *Use Eratosthenes' sieve to find all primes under* 200

2. *Let* $p \neq 3$ *be a prime. Prove that*

$$p = 3k + 1 \quad \text{or} \quad p = 3k - 1 \quad \text{for some } k \in \mathbb{N}.$$

3. *Preove: if* p *is prime and* $a \in \mathbb{Z}$,*then either* $p \mid a$ *or* $(a, p) = 1$.

4. *Prove that if* n *and* a *are natural numbers and* $\sqrt[n]{a} \in \mathbb{Q}$, *then* $\sqrt[n]{a} \in \mathbb{N}$ *so for example* $\sqrt[3]{10}$ *is irrational.*

5. *in Euclid's classical proof, a prime outside* $\{p_1, p_2, \ldots, p_n\}$ *is found by considering prime factors of*

$$N_n = p_1 p_2 \cdots p_n + 1$$

. *Do this beginning with* $\{2\}$, *next being* $\{2, p_2\}$, *where in fact* $N_2 = 2 + 1 = 3$, *so* $p_2 = 3$ *since* N_2 *happens to be prime. Continue, until*

(1) *either, you have found 5 odd primes . (or more, if you like)*
(2) *ir:* N_p *is not a prime* $p_n \neq N_n$.

Idesas? Questions??

6. *a)* $3, 5$ *and* 7 *are a triple of primes:* $p, p + 2, p + 4$ *Why are there no others?*
b) leta, $b \in \mathbb{N}$ *and* $(a, b) \geq 2$. *prove that hte set* $A = \{an + b \mid n = 0, 1, 2, \ldots\}$ *contains at most one prime.*

7. *Prove htat there is a number* $C > 0$, *such tha rt for all* $k \geq 2$

$$\sum_{p \leq k, p \in \mathbb{P}} \frac{1}{p} \geq \log \log k + C, \tag{1}$$

so the series $\sum_{p \in \mathbb{P}} \frac{1}{p}$ *doverges. You may assume as known (lectures!) that*

$$\prod_{p \leq k, p \in \mathbb{P}} \frac{1}{1 - p^{-1}} \geq \sum_{n} \frac{1}{n} \geq \log k. \tag{2}$$

Take logarithms. Remember how to use them, and notice that

(1) $-\ln\left(1 - \frac{1}{p}\right) \leq \frac{1}{p} + \frac{1}{p^2}$, *(proof not required today, nut easy using series or tha fact that* $f(x) = \log(1 + x) - x + x^2$ *decreases on* $[-\frac{1}{2}, 0]$
(2) *the series* $\sum_p p^{-2}$ *converges.*

KÄÄNNÄ

8. *Calculate (at least some terms of)*

(1) $E_0 * E_0$
(2) $E * E_0$
(3) $E_0 * \Omega$
(4) $E * N_\alpha$
(5) $E * \sigma_{\frac{1}{2}}$
(6) $\mu * E * E_0$.

9. *Just read:*
Remember : Eukleideen algoritmi luvuille 126 and 35:

$$\begin{aligned} 126 &= 3 \cdot 35 + 21, \\ 35 &= 1 \cdot 21 + 14, \\ 21 &= 1 \cdot 14 + 7, \\ 14 &= 2 \cdot 7. \end{aligned}$$

s and t are found "backwards":

$$\begin{aligned} (126, 35) = 7 &= 21 - 1 \cdot 14, \\ &= 21 - (35 - 1 \cdot 21), \\ &= (126 - 3 \cdot 35) - (35 - (126 - 3 \cdot 35)), \\ &= 2 \cdot 126 - 7 \cdot 35. \end{aligned}$$

This is clumsy when large numbers on computers. Better:

Let ℓ, q_i , r_i be like in Eukleideen algoritm. try to find s_i and t_i such that $s_i r_0 + t_i r_1 = r_i$ for all $0 \le i \le \ell$.

Assume first, that such mumbers exist: Apply tis to indices $i-1$, i and $i+1$ and use Eukleideen algoritmin:

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= (s_{i-1} r_0 + t_{i-1} r_1) - q_i (s_i r_0 + t_i r_1) \\ &= (s_{i-1} - q_i s_i) r_0 + (t_{i-1} - q_i t_i) r_1. \end{aligned} \tag{3}$$

But $r_{i+1} = s_{i+1} r_0 + t_{i+1} r_1$. Choos the coefficients recursively:

$$\begin{aligned} s_{i+1} &= s_{i-1} - q_i s_i, \\ t_{i+1} &= t_{i-1} - q_i t_i. \end{aligned} \tag{4}$$

Then, by (3), if $s_k r_0 + t_k r_1 = r_k$ for $k = i-1$ and $k = i$ and the coefficients s_k and t_k are found by (4) then the equation $s_k r_0 + t_k r_1 = r_k$ is also satisfied for $k = i+1$. So, it is sufficient to find suitable initiala values. Such are

$$s_0 = 1, \quad t_0 = 0, \quad s_1 = 0, \quad t_1 = 1.$$

In the extended Euclidean algorithm, numbers ℓ, q_i, $r_i \in \mathbb{N}$, s_i, $t_i \in \mathbb{Z}$, $1 \le i \le \ell$, are found such that $0 \le r_{i-1} < r_i$, for $1 \le i \le \ell$, ja

$$\begin{cases} s_0 = 1, \quad t_0 = 0 \\ s_1 = 0, \quad t_1 = 1 \\ r_{i-1} = q_i r_i + r_{i+1} \\ s_{i-1} = q_i s_i + s_{i+1} \\ t_{i-1} = q_i t_i + t_{i+1} \end{cases} \tag{5}$$

Then $s_i r_0 + t_i r_1 = r_i$ *for all* $0 \leq i \leq \ell$ *amd* $r_\ell = (r_0, r_1)$.
Literature [**?**, §3.2], [**?**, §4.5.2].

ESIMERKKI. *The previous exaple in the extendend algorithm gives*

i	r_i	s_i	t_i
0	126	1	0
1	35	0	1
2	21	1	-3
3	14	-1	4
4	7	2	-7
5	0	-5	18

Riviltä $i = 4$ *saadaan*
$r_\ell = (r_0, r_1) = s_\ell r_0 + t_\ell r_1$, *eli*
$7 = (126, 35) = 2 \cdot 126 - 7 \cdot 35$.