Exercise help set 2/2011 **Number Theory**

1. *Like this Eratosthenes finds all primes up to 400:*

   - Write 1-200.
   - Delete (strike thyrough) 1. It is no prime!
   - Leave 2. Delete 4, 6, 8, ie. all other even
   - Leave 3, Delete 6, ...ie. all other remaining multiples of 3. Half of them are deleted already.
   - 4 is away already. So are its multiples.
   - Leave 5. Delete 10 (gone already!) 15 (gone already!), ... Delete all remaining multiples of 5.
   - 6 is away already. So are its multiples.
   - Leave 7. Delete all other multiples of 7 like 14 (gone already!) 21 (gone already!),... !
   - 8 is away already. So are its multiples. The same applies to 9 and 10.
   - Leave 11, Delete all other multiples of 11 like 22 (gone already!) 33 (gone already!), ... $11 \times 11 = 121$, $13 \times 11 = 143$, and $17 \times 11 = 187$.
   - 12 is away already. So are its multiples.
   - Leave 13, Delete all other multiples of 13; only $13 \times 13 = 169$.
   - 14, 15, 16 are away already. So are their multiples.
   - Leave 17, poista 17×17.
   - Leave 19, poista 19×19.
   - 20 is away already. So are its multiples.
   - We have reached $\sqrt{4}00$, so no remaining number can be divisible,, since we would have detected the smallest factor already. Thye remaining numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 203, 209, 211, 217, 221, 223, 227, 229, 233, 239, 241, 247, 251, 253, 257, 259, 263, 269, 271, 277, 281, 283, 287, 289, 293, 299, 301, 307, 313, 217, 319, 323, 329, 331, 337, 341, 343, 347, 349, 353, 359, 361, 367, 371, 373, 377, 379, 383, 389, 391, 397 are the primes in 2...400.

2. ...

Every number is one of the following $3k$, $3k+1$, $3k+2$ depending on the remainder when dividing by 3. In the first set, only 3 is prime, the others are multiples of 3. The 2. set are what eewe want, and so are the third as well, since $3k+2 = 3(k+1)-1$. □

3. ...

(a, p) exists. Assume $d = (a, p)$. By definition, $d \mid a$ and $d \mid p$. If $d \neq 1$ then $d = p$, since p is prime. since $d \mid a$ and $d = p$, we have $p \mid a$. □.

4. ...

Assume $\sqrt[n]{a} \in \mathbb{Q}$ ie. $\sqrt[n]{a} = \frac{n}{m}$, where $k, m \in \mathbb{Z}$ and $m \neq 0$. Case 1: $k, m \neq 1$. The canonical decompostioions : $k = p_1 \dots p_\nu$, $m = q_1 \dots q_\mu$, give

$$\sqrt[n]{a} = \frac{p_1 \dots p_\nu}{q_1 \dots q_\mu},$$

and one can assume $p_i \neq q_j$ for all i, j

$$a(q_1 \dots q_\mu)^n = (p_1 \dots p_\nu)^n.$$

The left side is divisible by q_1, but the right side is not. Case 1 is impossible.

If $k = 1$ $\sqrt[n]{a} \in \mathbb{N}$. OK.

The case $k = 1$ is impossible essentially for the same reason as the first case.

5. *Use Eucdlid's method to find a sqequence of primes*

$$2, 2+1 = 3 \in \mathbb{P}, 2\cdot 3+1 = 7 \in \mathbb{P}, 2\cdot 3\cdot 7+1 = 43 \in \mathbb{P}, 2\cdot 3\cdot 7\cdot 43+1 = 1807 = 13\times 139,$$

where 13 and 139 are primes. Both are "new".

Ideas:

- All prime factors of $N_k = p_1 \dots p_k + 1$ differ from $p_1, \dots, p_k$
- So if we do not decompose $N_k = p_1 \dots p_k + 1$ but just simply define $N_1 = 2, N_2 = 3, \dots N_k = (N_1 \cdots N_k)+1$, then each N_k consits of noly of "new"primes, not dividing any previous Nj.
- How about finding more primes among the N_j ? Try:

$$2, 2+1 = 3 \in \mathbb{P}, 2\cdot 3+1 = 7 \in \mathbb{P}, 2\cdot 3\cdot 7+1 = 43 \in \mathbb{P}, 2\cdot 3\cdot 7\cdot 43+1 = 1807 = 13\times 139, 3263443,$$

  UUPPSS?
- The following. My calculator has only 10 digits.? Try Excel- notice

$$N_{k+1} = N_k \cdot (N_k - 1) + 1.$$

  Oh - I need 13 decimals — and thje next needs the double (WHY!) = 26 desimaalia,then 54, 108, 216 etc. How to identifiy such primes??????

At least this is known (Graham, Knuth & Patachnik):

- $N_5 = 1807$ is divisible.
- $N_6 = 3263443$ is prime.
- $N_7 = 10650056950807$ is divisible.
- $N_8 = 113423713055421844361000443$ is divisible.
- $N_9 = 1286493868327867174053714599836096154665325948519580 7$ is divisible.
- $N_{10} = 165506647324519964198468195444[45 digits]57240680891198813173764518544 3$ is divisible.
- $N_{11} = 27392450308603031423410234291 6[149 digits]73945464982838554150021392080$ is divisible.

  27392450308603031423410234291 6[149 digits]73945464982838554150021392080

WHY?.. USE Maxima!

```
(%i1)  e(n):= if n=1 then 2 else (e(n-1)-1)*e(n-1)+1$
(%i2)  e(2);
(%o2)  3

(%i3)  e(3);
(%o3)  7
```

```
(%i4)  e(4);
```
(%o4) 43

```
(%i5)  ifactors(%);
```
(%o5) [[43, 1]]

```
(%i6)  e(5);
```
(%o6) 1807

```
(%i7)  ifactors(%);
```
(%o7) [[13, 1], [139, 1]]

```
(%i8)  e(6);
```
(%o8) 3263443

```
(%i9)  ifactors(%);
```
(%o9) [[3263443, 1]]

```
(%i10) e(7);
```
(%o10) 10650056950807

```
(%i11) ifactors(%);
```
(%o11) [[547, 1], [607, 1], [1033, 1], [31051, 1]]

```
(%i12) e(8);
```
(%o12) 113423713055421844361000443

```
(%i13) ifactors(%);
```
(%o13) [[29881, 1], [67003, 1], [9119521, 1], [6212157481, 1]]

```
(%i14) e(9);
```
(%o14) 128649386832786717405371459983609615466532594851958 07

```
(%i15) ifactors(%);
```
(%o15) [[5295435634831, 1], [31401519357481261, 1], [77366930214021991992277, 1]]

```
(%i16) e(10);
```
(%o16) 16550664732451996419846819544 4[45*digits*]57240680891198813137645185443

```
(%i17) ifactors(%);
```
(%o17) [[181, 1], [1987, 1], [112374829138729, 1], [114152531605972711, 1], [3587438027224662415276 45

```
(%i18) e(11);
```
(%o18) 27392450308603031423410234291 6[149*digits*]73945464982838554150021392 0807

6. ..

a) Either p, $p+1$ is $p+2$ a multiple of 3 . If $p \in \mathbb{P}$ and $p+2 in \mathbb{P} > 3$, then $n+1$ is divisible by 3, so $n+4$ is divisible by 3.

b) Consider $d = (a, b) > 2$, so a and b arfe divisible by d:llä and so are all $an+b$. In order to be divisible by d:llä and prime, a number $an+b$ nust be d itself, so $an+b = d$. But $d \leq a, b$, so $n = 0$. The only possibiolity is a, if $a \in \mathbb{P}$.

7. *(There was a misprint. We find $C < 0$.)*
Begin by proving

$$-\log\left(1-\frac{1}{p}\right) \leq \frac{1}{p}+\frac{1}{p^2}. \tag{1}$$

ikn 2 ways.
Series expansion: For $0 < x < 1$, the terms in the series

$$\log(1-x) = \sum_{k=1}^{\infty} -\frac{x^n}{n}$$

are negative, so

$$\log(1-x) \geq \sum_{k=1}^{2} -\frac{x^n}{n} = -x-x^2$$

$$\textit{implying } -\log(1-x) \leq x+x^2.(\square)$$

By derivative: The derivative of $f(x) = \log(1+x)-x+x^2$ is $f'(x) = \frac{1}{1+x}-1+2x$, negative on $]-\frac{1}{2},0[$ (Solve $\frac{1}{1+x}-1+2x<0$). So f is declining, so $f(x) \geq f(0) = 0$, ie. $\log(1+x)-x+x^2 \geq 0$ so $\log(1+x) \geq x-x^2$ for all $x \in [-\frac{1}{2},0]$, same as $\log(1-x) \geq -x-(-x)^2 = -x-x^2$ for all $x \in [0,\frac{1}{2}]$. $(\square)$

(2) main proof: Try to find C such that $C \in \mathbb{R}$, että for all $k \geq 2$:

$$\sum_{p\leq k, p\in\mathbb{P}} \frac{1}{p} \geq \log\log k + C. \tag{2}$$

Given in lecture:

$$\prod_{p\leq k, p\in\mathbb{P}} \frac{1}{1-p^{-1}} \geq \sum_{n} \frac{1}{n} \geq \log k. \tag{3}$$

take log on both sides. the right side becomes $\log\log k$. Lefti:

$$\log \prod_{p\leq k, p\in\mathbb{P}} \frac{1}{1-p^{-1}} = \sum_{p\leq k, p\in\mathbb{P}} -\log\left(1-\frac{1}{p}\right) \overset{(1)}{\leq} \sum_{p\leq k, p\in\mathbb{P}} \left(\frac{1}{p}+\frac{1}{p^2}\right) \leq \sum_{p\leq k, p\in\mathbb{P}} \frac{1}{p} + \sum_{p\in\mathbb{N}} \frac{1}{p^2}$$
$$\leq \sum_{p\leq k, p\in\mathbb{P}} \frac{1}{p} + \zeta(2).$$

Choose $C = -\sum_{p\in\mathbb{N}} \frac{1}{p^2} = -\zeta(2)$.

8. (1) *$E_0 * E_0 = E_0$, koska E_0 on konvoluutiokertolaskun ykkösalkio.*
(2) *$E * E_0 = E$, koska E_0 on konvoluutiokertolaskun ykkösalkio.*
(3) *$E_0 * \Omega = \Omega$, koska E_0 on konvoluutiokertolaskun ykkösalkio.*
(4) *$E * N_\alpha(n) = \sum_{d\,|\,n} E(n/d)N_\alpha(d) = \sum_{d\,|\,n} 1\cdot d^\alpha = \sum_{d\,|\,n} d^\alpha = \sigma_\alpha(n)$.*
(5) *$E * \sigma_{\frac{1}{2}}(n) = \sum_{d\,|\,n} E(n/d)\sigma_\alpha(d) = \sum_{d\,|\,n} \sigma_\alpha(d) = \sum_{d\,|\,n} \sum_{f\,|\,d} f^\alpha$ =??*
(6) *$E * \sigma_{\frac{1}{2}}(1) = \sum_{d\,|\,1} \sigma_\alpha(d) = \sum_{d=1} \sigma_\alpha(d) = \sigma_\alpha(1) = \sum_{f\,|\,1} f^\alpha = 1$, kuten on selvää siitäkin, että $E * \sigma_{\frac{1}{2}}$ on multiplikatiivinen.*
(7) *$\mu * E * E_0 = \mu * E = E_0$.*

9. .

Laajennetun Eukleideeen algoritmin oleellinen ominaisuus on, ettei laskun kaikkia vaiheita tarvitse tallettaa paluuta varten, vaan riittää pitää koneen muistiissa pair viimeistä riviä. Pitkässä laskussa säästyy olellinen määrä muistia.

Tehtäväpaperin laskut oli muuten laskettu Mathematicalla. Näin:

```
In:=
ClearAll[i,r, s, t, q];
i =.; Print[i, r[i], s[i], t[i]];
r[0] = 126; s[0] = 1; t[0] = 0;
r[1] = 35; s[1] = 0; t[1] = 1;
i = 0; Print[i, r[i], s[i], t[i]];
i = 1; Print[i, r[i], s[i], t[i]];
While[Not[r[i] == 0],
q[i] = Quotient[r[i - 1], r[i]];
r[i + 1] = Mod[r[i - 1], r[i]];
s[i + 1] = (s[i - 1] - q[i]*s[i]);
t[i + 1] = (t[i - 1] - q[i]*t[i]);
i = i + 1; Print[i, r[i], s[i], t[i]];
]
Out=
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
```