Harjoitukset 2 / 2011 RATKAISUT Lukuteoria

1. *Etsin Eratostheneen seulalla samantien kaikki lukua* 400 *pienemmät alkuluvut. (Tai ohjelmoi tietokoneesi etsimään paljon lisää.)*

- Kirjoita riviin kaikki luvut 1-200.
- Poista (viivaa yli) 1. Se ei ole alkuluku!
- Jätä 2, poista 4, 6, 8, eli kaikki muut parilliset
- Jätä 3, 6, ...eli kaikki muut jäljellä olevat 3:lla jaolliset. Joka toinen niistä onkin jo poissa!
- 4 on jo poistettu, samoin sen kaikki monikerrrat.
- Jätä 5, poista 10 (on jo poissa!) 15 (on jo poissa), ...eli poista kaikki muut jäljellä olevat viidellä jaolliset Useimmat niistä ovatkin jo poissa!
- 6 on jo poistettu, samoin sen kaikki monikerrrat.
- Jätä 7, poista muut 7:llä jaolliset: 14 (on jo poissa!) 21 (on jo poissa),... useimmat niistä ovatkin jo poissa!
- 8 on jo poistettu, samoin sen kaikki monikerrrat. Vastaava koskee lukuja 9 ja 10.
- Jätä 11, poista muut 11:llä jaolliset 22 (on jo poissa!) 33 (on jo poissa), ...eli kaikki jäljellä olevat 11:llä jaolliset eli $11 \times 11 = 121$, $13 \times 11 = 143$, ja $17 \times 11 = 187$.
- 12 on jo poistettu, samoin sen kaikki monikerrrat.
- Jätä 13, poista muut jäljellä olevat 13:llä jaolliset eli enää $13 \times 13 = 169$.
- 14, 15, 16 monikertoineen ovat jo poissa.
- Jätä 17, poista 17×17.
- Jätä 19, poista 19×19.
- 20 on jo poistettu, samoin sen kaikki monikerrrat.
- Koska on saavutettu $\sqrt{4}00$ ei mikään jäljellä oleva luku enää ole jaollinen, koska sen mahdollinen tekijä olisi jo huomattu. Jäljelle jääneet luvut 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 ovat siis alkuluvut väliltä 2...400.

2. *Näytä, että alkuluku* $p \neq 3$ *on muotoa* $p = 3k+1$ *tai* $p = 3k-1$, $(k \in \mathbb{N})$.

Jokainen luku on muotoa $3k$, $3k+1$ tai $3k+2$ sen mukaan onko jakojäännös 3:lla jaettaessa 0,1 vai 2. Ensin mainituista vain 3 on alkuluku, muut jaollisia 3:lla. Toiseen ryhmään kuuluvat ovat haluttua muotoa ja kolmannessa ryhmässä olevat ovat muotoa $3k + 2 = 3(k + 1) - 1$, joka sekin kelpaa. □

3. *Todista: Jos* p *on alkuluku ja* $a \in \mathbb{Z}$, *niin joko* $p \mid a$ *tai* $(a, p) = 1$.

Suurin yhteinen tekijä (a, p) on olemassa. Olkoon se $d = (a, p)$. Tietysti $d \mid a$ ja $d \mid p$. Jos d ei ole 1, niin $d = p$, koska alkuluvulla p ei ole muita positiivisia tekijöitä kuin 1 ja p. Koska $d \mid a$ ja $d = p$, niin $p \mid a$. □.

4. *Näytä, että jos* n *ja* a *ovat luonnollisia lukuja ja* $\sqrt[n]{a} \in \mathbb{Q}$, *niin* $\sqrt[n]{a} \in \mathbb{N}$ *ja siis esimerkiksi* $\sqrt[3]{10}$ *ei ole rationaaliluku.*

Idea on sama, jolla on tapana todistaa, ettei $\sqrt{2}$ ole rationaaliluku. Olkoon $\sqrt[n]{a} \in \mathbb{Q}$ eli $\sqrt[n]{a} = \frac{n}{m}$, missä $k, m \in \mathbb{Z}$ ja $m \neq 0$. Tutkitaan ensin tapaus, jossa $k, m \neq 1$. Hajotetaan k ja m tuloksi alkuluvuista: $k = p_1 \dots p_\nu$, $m = q_1 \dots q_\mu$, jolloin

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

ja tässä voi olettaa, että $p_i \neq q_j$ kaikilla i, j, sillä osamäärän voi supistaa, kunnes osoittajassa ja nimittäjässä on eri tekijät. Korotetaan puolittain potenssiin n ja kerrotaan nimittäjällä.

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

Vasen puoli on jaollinen luvulla q_1, mutta oikea puoli ei, sillä oikean puolen alkutekijät ovat luvut $p_1 \dots p_\nu$, josta mikään ei ole q_1. Ristiriita. Jäljelle jää tapaus, jossa joko k tai m on 1. Jälkimmäisessä tapauksessa $\sqrt[n]{a}$ on kokonaisluku, kuten väitettiin. Ensimmäinen tapaus on mahdoton, koska $\frac{1}{m} < 1 < \sqrt[n]{a}$.

5. *Etsitään Eukleideen klassisella menetelmällä alkulukuja.*

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

missä 13 ja 139 ovat alkulukuja (teht.1). Kumpikin on tietenkin aikaisemmin esiintymätön.

Ajatuksia:

- Lukujen $N_k = p_1 \dots p_k + 1$ kaikki alkutekijät ovat joka tapauksessa muita kuin luvut $p_1, \dots, p_k$
- Jos siis emme hajoitakaan lukua $N_k = p_1 \dots p_k + 1$ alkutekijöihin, vaan muodostamme lukujonon $N_1 = 2, N_2 = 3, \dots N_k = (N_1 \cdots N_k) + 1$, niin kukin N_k sisältää tekijöinään vain sellaisia alkulukuja, joita ei ole aikaisemmissa.
- Tämähän on ihan kiintoisa jono. Onkohan siinä enää ollenkaan alkulukuja 43:n jälkeen. Kokeillaan laskimella

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

  Onko jaollinen?
- Seuraava luku? Laskimen teho loppui. Siirrytään Excel-ohjelmaan huomaten, että

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

  Ei auta - tarvittaisiin 13 desimaalia — ja seuraava on suuruusluokkaa edellisen neliö, siis 26 desimaalia, sitten 54, 108, 216 jne. Kuka osaa testata tämmöisten lukujen jaollisuutta? (Asiaan palataan.)

  Itse asiassa tiedetään mm. seuraavaa (”Graham, Knuth & Patachnik”ja ”Lehtonen!”):
  - $N_5 = 1807$ on jaollinen.
  - $N_6 = 3263443$on alkulukuon alkulukuon alkulukuon alkuluku.
  - $N_7 = 10650056950807$ on jaollinen.
  - $N_8 = 113423713055421844361000443$ on jaollinen.
  - $N_9 = 12864938683278671740537145998360961546653259485195807$ on jaollinen.

– $N_{10} = 1655066473245199641984681954 44[45digits]57240680891198813173764518544 3$ on jaollinen.
– $N_{11} = 27392450308603031423410234291 6[149digits]73945464982838554150021392080$ on jaollinen.

Todistus Maxima- ohjemalla se onnistuu:

```
(%i1)  e(n):= if n=1 then 2 else (e(n-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) 12864938683278671740537145998360961546653259485195807
(%i15) ifactors(%);
(%o15) [[5295435634831, 1], [31401519357481261, 1], [77366930214021991992277, 1]]
(%i16) e(10);
(%o16) 1655066473245199641984681954 44[45digits]57240680891198813173764518544 3
(%i17) ifactors(%);
(%o17) [[181, 1], [1987, 1], [112374829138729, 1], [114152531605972711, 1], [3587438027224662
```

```
(%i18) e(11);
(%o18) 27392450308603031423410234291 6[149digits]7394546498283855415002139208 07
```

6. *a) Miksi ei voi olla luonnollista lukua $p > 3$, jolle luvut p, $p+2$ ja $p+4$ ovat alkulukuja? b) Olkoot $a, b \in \mathbb{N}$ ja $(a,b) \geq 2$. Osoita, että joukossa $A = \{an+b \mid n = 0,1,2,\dots\}$ on korkeintaan yksi alkuluku.*

a) Joko p, $p+1$ tai $p+2$ on jaollinen 3:lla. Jos p ja $p+2$ ovat alkulukuja > 3, niin siis $n+1$ on jaollinen 3:lla, jolloin myös $n+4$ jaollinen 3:lla.

b) Olkoon $d = (a,b) > 2$, jolloin a ja b ovat jaollisia d:llä ja samoin siis jokainen $an+b$. Ollakseen jaollinen d:llä ja samalla alkuluku on luvun $an+b$ oltava itse d, siis $an+b = d$. Mutta $d \leq a, b$, joten ainoa mahdollisuus on, että $n = 0$, joten joukon ainoa alkuluku on a, kun a sattuu olemaan alkuluku, muuten ei mikään.

7. *(Tehtävässä oli virhe. Löydetään negatiivinen C.)*
Todistetaan aluksi (vaikka ei pyydetty) molemmin tavoin, että

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

Sarjan avulla: Kun $0 < x < 1$, niin sarjan

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

termit ovat negatiivisia, joten

$$\log(1-x) \geq \sum_{k=1}^{2} -\frac{x^n}{n} = -x - x^2$$
$$\text{eli } -\log(1-x) \leq x + x^2. (\square)$$

Derivaatan avulla: Funktion $f(x) = \log(1+x) - x + x^2$ derivaatta on $f'(x) = \frac{1}{1+x} - 1 + 2x$, joka on negatiivinen välillä $]-\frac{1}{2}, 0[$ (Ratkaise epäyhtälö $\frac{1}{1+x} - 1 + 2x < 0$ esim. kertomalla ensin nimittäjä pois). Siten f on vähenevä, joten $f(x) \geq f(0) = 0$, ts. $\log(1+x) - x + x^2 \geq 0$ eli $\log(1+x) \geq x - x^2$ kaikille $x \in [-\frac{1}{2}, 0]$, mikä on samaa kuin $\log(1-x) \geq -x - (-x)^2 = -x - x^2$ kaikille $x \in [0, \frac{1}{2}]$. $(\square)$

(2) Päätodistus: Pitää osoittaa, että on olemassa sellainen vakio $C \in \mathbb{R}$, että kaikilla $k \geq 2$ pätee epäyhtälö

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

Luennolta tiedetään, että

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

Otetaan puolittain logaritmit. Oikea puoli on sen jälkeen $\log\log k$. *Lasketaan vasen puoli:*

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

Vakioksi C *kelapaa siis* $-\sum_{p\in\mathbb{N}} \frac{1}{p^2}$ *eli* $-\zeta(2)$.

8. *Laske konvoluutiot — ainakin arvo kohdassa 1.*
   (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