Yksinkertaisia jaollisuustestejä

Jukka Jylänki
jukkajyl@mail.student.oulu.fi

Matemaattisten tieteiden laitos
Oulun yliopisto
2007

Sisältö

1 Käsitteitä **3**

2 Kongruenssin ominaisuuksia **4**

3 Jaollisuustestejä **6**

4 Lähteet **11**

1 Käsitteitä

Käytetään merkintöjä

$$\begin{aligned}
&\mathbb{N} = \{0, 1, 2, \ldots\},\\
&\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\},\\
&\mathbb{Z}_+ = \{1, 2, \ldots\},\\
&\mathbb{Z}_{\geq 2} = \{2, 3, \ldots\}.
\end{aligned}$$

Määritelmä 1.1. *Jos luvuille $a, b \in \mathbb{Z}$ on olemassa $k \in \mathbb{Z}$, siten että $a = kb$, niin sanotaan, että b jakaa a:n, tai että b on a:n tekijä. Tällöin merkitään $b \mid a$.*

Määritelmä 1.2. *Luku $p \in \mathbb{Z}_{\geq 2}$ on **alkuluku**, jos sillä on vain triviaalit tekijät ± 1 ja $\pm p$. Käytetään merkintää*

$$\mathbb{P} = \{p : p > 1 \text{ on alkuluku}\}.$$

Määritelmä 1.3. *Jos luvuille $a, b \in \mathbb{Z}, m \in \mathbb{Z}_+$ on voimassa $m \mid (a - b)$, niin sanotaan, että a on kongruentti b:n kanssa modulo m ja merkitään $a \equiv b \pmod{m}$.*

Merkitään $[a]_m = \{x : x \equiv a \pmod{m}\}$. Lisäksi merkitään

$$\mathbb{Z}_m = \{[x]_m : 0 \leq x < m\}.$$

2 Kongruenssin ominaisuuksia

Tässä luvussa tarkastellaan joidenkin kongruenssiyhtälöiden ominaisuuksia.

Lause 2.1. *Kaikilla $a, b \in \mathbb{N}$ on olemassa sellaiset $u, v \in \mathbb{Z}$, että $syt(a, b) = ua + vb$.*

Todistus. Merkitään $\mathbb{S} = \{na+mb |\ n, m \in \mathbb{Z}, na+mb > 0\}$ ja olkoon d tämän joukon pienin alkio. Siis $d = ua + vb$ joillakin $u, v \in \mathbb{Z}$. Koska $a, b \in \mathbb{Z}$, niin $d \leq a$ ja $d \leq b$. Nyt jakoyhtälön nojalla on olemassa sellaiset $q, r \in \mathbb{N}, r < d$, että

$$a = qd + r.$$

Tällöin

$$a = q(ua + vb) + r,$$

josta ratkaisemalla r saadaan

$$r = (1 - qu)a + (-v)b.$$

Tästä esityksestä nähdään, että $r \in \mathbb{S}$. Koska d on joukon $\mathbb{S}$ pienin alkio ja $r < d$, niin $r = 0$ eli $d |\ a$. Samanlaisella päättelyllä saadaan $d|b$. Luku d on siis lukujen a ja b yhteinen tekijä. Jos jokin luku $d'|a$ ja $d' |\ b$, niin $d' |\ ua + vb = d$. Siten $d = syt(a, b)$ eli on olemassa sellaiset $u, v \in \mathbb{Z}$, että $syt(a, b) = ua + vb$. □

Lause 2.2. *Olkoot $a, b, c \in \mathbb{Z}$. Yhtälöllä $ax+by = c$ on ratkaisu $(x_0, y_0) \in \mathbb{Z}^2$, jos ja vain jos $syt(a, b) |\ c$.*

Todistus. Olkoon x_0 ja y_0 kokonaislukuja, joille $ax_0+by_0 = c$. Tällöin $syt(a, b)$ jakaa yhtälön vasemman puolen, joten se jakaa myös luvun c, eli $syt(a, b) |\ c$.

Oletetaan sitten, että $syt(a, b) |\ c$. Edellisen lauseen nojalla on olemassa sellaiset $u, v \in \mathbb{Z}$, että

$$ua + vb = syt(a, b).$$

Kertomalla tämä yhtälö puolittain luvulla $k = \frac{c}{syt(a,b)} \in \mathbb{Z}$ saadaan yhtälö

$$uka + vkb = c.$$

Merkitään $x_0 = uk \in \mathbb{Z}$ ja $y_0 = vk \in \mathbb{Z}$, jolloin $ax_0 + by_0 = c$. □

Lause 2.3. *Olkoon $a, b \in \mathbb{Z}$. Kongruenssilla $ax \equiv b \pmod{m}$ on kokonaislukuratkaisu, jos ja vain jos $syt(a, m) |\ b$. Jos x_0 on eräs ratkaisu, niin kaikki ratkaisut ovat muotoa $x_0 + k \cdot \frac{m}{syt(a,m)}$.*

Todistus. Yhtälö $ax \equiv b \pmod{m}$ voidaan kongruenssin määritelmän nojalla esittää yhtäpitävästi muodossa $ax - km = b$ eräällä luvulla $k \in \mathbb{Z}$. Lauseen 2.2 nojalla ratkeava, jos ja vain jos $syt(a, m) \mid b$.

Oletetaan nyt, että x_0 on kongruenssin jokin ratkaisu. Todistetaan, että kaikki ratkaisut x_k ovat muotoa $x_k = x_0 + k \cdot \frac{m}{syt(a,m)}$, missä $k \in \mathbb{Z}$. Yhtälöt $ax_0 \equiv b \pmod{m}$ ja $ax_k \equiv b \pmod{m}$ voidaan esittää muodoissa $ax_0 - b = k_1 m$ ja $ax_k - b = k_2 m$ eräille luvuille $k_1 \in \mathbb{Z}$ ja $k_2 \in \mathbb{Z}$. Vähentämällä nämä yhtälöt puolittain toisistaan saadaan

$$a(x_k - x_0) = m(k_2 - k_1)$$

ja jakamalla edelleen luvulla $d := syt(a, m)$ saadaan yhtälö

$$\frac{a}{d}(x_k - x_0) = \frac{m}{d}(k_2 - k_1).$$

Tässä $syt(\frac{a}{d}, \frac{m}{d}) = 1$, joten $\frac{m}{d} \mid (x_k - x_0)$ ja tällöin $x_k - x_0 = k \cdot \frac{m}{d}$ jollakin $k \in \mathbb{Z}$. Siis mielivaltaiselle ratkaisulle x_k saadaan esitys

$$x_k = x_0 + k\frac{m}{syt(a, m)}, k \in \mathbb{Z}.$$

□

Määritelmä 2.4. *Merkitään $\mathbb{Z}$-kertoimisten polynomien joukkoa symbolilla $\mathbb{Z}[x]$. Jos polynomeille $f(x), g(x) \in \mathbb{Z}[x]$ on voimassa $f(x_0) \equiv g(x_0) \pmod{m}$ kaikilla $x_0 \in \mathbb{Z}$, niin sanotaan, että polynomit $f(x)$ ja $g(x)$* ***ovat kongruentteja modulo m*** *ja merkitään $f(x) \equiv g(x) \pmod{m}$.*

Määritelmä 2.5. *Polynomin $f(x) \in \mathbb{Z}[x]$* ***nollakohta modulo m*** *on luku x_0, jolla $f(x_0) \equiv 0 \pmod{m}$.*

Lause 2.6. *Jos $f(x)$ on astetta k oleva polynomi ja x_0 on sen nollakohta modulo m, niin*

$$f(x) \equiv (x - x_0)g(x) \pmod{m}$$

jollakin astetta $k - 1$ olevalla polynomilla $g(x)$.

Todistus. Olkoon $f(x)$ astetta k oleva polynomi ja $f(x_0) \equiv 0 \pmod{m}$. Merkitään $h(x) = f(x) - f(x_0)$. Nyt $h(x_0) = f(x_0) - f(x_0)$ eli $(x - x_0)$ on $h(x)$:n tekijä. Tällöin $h(x) = (x - x_0)g(x)$, missä $g(x)$ on astetta $k - 1$. Siis $f(x) \equiv f(x) - f(x_0) = h(x) = (x - x_0)g(x) \pmod{m}$. □

3 Jaollisuustestejä

Suoraviivainen tapa testata luvun n jaollisuutta on jakaa lukua n alkuluvuilla p, joille $p^2 \leq n$, kunnes tekijä löytyy tai kaikki luvut on kokeiltu. Pienille luvuille (esimerkiksi $\leq 2^{32}$) tämä soveltuu hyvin, sillä $\sqrt{2^{32}} = 2^{16} = 65536$, jota pienempiä alkulukuja on vain 6542 kappaletta. Suurin tällä hetkellä tunnettu alkuluku on $2^{32582657} - 1$ [PrimeA]. Jos yritettäisiin suoraviivaisesti todistaa tämä alkuluvuksi, tarvittaisiin $\approx 2^{16291329}$ jakojäännösoperaatiota. Tämän hetken nopeimmat pöytäkoneet ovat noin 37 GFlopsin luokkaa [TomsHardware07]. Siltikin laskenta veisi $2^{16291269} \approx 10^{4904161}$ vuotta, mikä on noin $10^{4904061}$ kertaa se aika, johon mennessä kaikki universumin mustat aukot ovat menettäneet vetovoimansa ja protoniytimet hajonneet [Holtz]. Jotain muuta pitäisi keksiä.

Tarkastellaan seuraavaksi muutamia alkulukuja koskevia tuloksia. Näiden avulla saadaan erilaisia jaollisuustestejä.

Lause 3.1 (**Lagrange**). *Jos $p \in \mathbb{P}$ ja $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, missä $a_n \not\equiv 0 \pmod{p}$, niin polynomilla $f(x)$ on korkeintaan n erillistä nollakohtaa modulo p.*

Todistus. Todistetaan induktiolla polynomin asteen n suhteen.

Alkuaskel. $n = 1$:

$$a_0 + a_1x \equiv 0 \pmod{p}$$

$syt(a_1, p) = 1$, joten lauseen 2.3 nojalla kongruenssi on ratkeava ja kaikki ratkaisut ovat muotoa

$$x_0 + k \cdot \frac{p}{syt(a_1, p)} = x_0 + k \cdot p \equiv x_0 \pmod{p}$$

eli ratkaisu on yksikäsitteinen modulo p.

Induktioaskel.

Induktio-oletus: Muotoa $a_0 + a_1x + \ldots + a_kx^k \equiv 0 \pmod{p}$ olevilla kongruenssiyhtälöillä on korkeintaan k erillistä ratkaisua modulo p.

Induktioväite: Muotoa $b_0 + b_1x + \ldots + b_{k+1}x^{k+1} \equiv 0 \pmod{p}$ olevilla kongruenssiyhtälöillä on korkeintaan $k + 1$ erillistä ratkaisua modulo p.

Todistus: Olkoon $f(x) \in \mathbb{Z}[x]$ astetta $k + 1$ oleva polynomi. Tehdään vastaoletus: yhtälöllä $f(x) \equiv 0 \pmod{p}$ on ainakin $k + 2$ erillistä ratkaisua $x_1, x_2, \ldots, x_{k+2}$. Lauseen 2.6 nojalla

$$f(x) \equiv (x - x_1)g(x) \pmod{p}$$

jollakin astetta k olevalla polynomilla $g(x) \in \mathbb{Z}[x]$. Induktio-oletuksen mukaan polynomilla $g(x)$ on korkeintaan k erillistä nollakohtaa modulo p, joten kongruenssiyhtälön oikean puolen lausekkeella on korkeintaan $k+1$ erillistä nollakohtaa modulo p ($\mathbb{Z}_p$ on kunta, joten nollakohtien määrä ei kasva lasketttaessa $(x - x_1)g(x)$). Vastaoletuksen mukaan kongruenssiyhtälön vasemman puolen lausekkeella on ainakin $k + 2$ erillistä nollakohtaa modulo p. Siten $f(x_i) \equiv 0 \pmod{p}$ ja $(x_i - x_1)g(x_i) \not\equiv 0 \pmod{p}$ jollakin $i = 2, \ldots, k + 2$, mikä on ristiriidassa polynomien kongruenssin määritelmän kanssa. Siten vastaoletus on väärä ja $f(x)$:llä on korkeintaan $k+1$ erillistä nollakohtaa modulo p.

Induktioperiaatteen nojalla muotoa $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, n \in \mathbb{Z}_+$, olevilla polynomeilla on korkeintaan n erillistä nollakohtaa modulo p. □

Esimerkki 3.2. *Onko $n = 8$ alkuluku? Olkoon $f(x) = 2x + 4$. Haetaan ratkaisuja $f(x) \equiv 0 \pmod{8}$. Nyt*

$$f(2) = 2 \cdot 2 + 4 = 8 \equiv 0 \pmod{8} \text{ ja}$$

$$f(6) = 2 \cdot 6 + 4 = 16 \equiv 0 \pmod{8}$$

$2 \not\equiv 6 \pmod{8}$, joten Lagrangen lausetta käänteisesti soveltamalla havaitaan, että $n = 8$ ei ole alkuluku.

Käytetään merkintää $\mathbb{Z}_m^* = \{[a]_m \in \mathbb{Z}_m : a \neq 0 \text{ ja } syt(a, m) = 1\}$. Lisäksi merkitään $\phi(m) = |\mathbb{Z}_m^*|$.

Lause 3.3 (Euler). *Jos $m \in \mathbb{Z}_+$ ja $syt(a, m) = 1$, niin $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Todistus. Joukko $(\mathbb{Z}_m^*, *)$ on ryhmä [Niemenmaa, Myllylä, Tirilä 2006]. Kuvaus $\tau_a(a_i) = aa_i$, missä $a, a_i \in \mathbb{Z}_m^*$ on bijektio $\mathbb{Z}_m^* \mapsto \mathbb{Z}_m^*$ [Matala-Aho 2006]. Siten

$$a_1a_2 \ldots a_{\phi(m)} \equiv aa_1aa_2 \ldots aa_{\phi(m)} \pmod{m},$$

joten saadaan kongruenssiyhtälö

$$a_1a_2 \ldots a_{\phi(m)} \equiv a^{\phi(m)}a_1a_2 \ldots a_{\phi(m)} \pmod{m}.$$

Koska $syt(a_1a_2 \ldots a_{\phi(m)}, m) = 1$, voidaan kongruenssiyhtälö jakaa puolittain tulolla $a_1a_2 \ldots a_{\phi(m)}$, joten

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

□

Seuraus 3.4 (Fermat). *Jos $p \in \mathbb{P}$, niin $a^{p-1} \equiv 1 \pmod{p}$ kaikilla $0 < a < p$*
.

Todistus. Jos $p \in \mathbb{P}$, niin $\phi(p) = p - 1$. □

Fermat'n lause on samanhenkinen Lagrangen lauseen kanssa siinä mielessä, että sillä voidaan osoittaa luku yhdistetyksi, mutta ei jaottomaksi.

Esimerkki 3.5. *Onko $n = 133$ alkuluku?*
Valitaan $a = 2$. Tällöin

$$2^{133-1} \equiv 64 \pmod{133}, \textit{ joten}$$

Fermat'n lauseen nojalla n ei voi olla alkuluku.

Fermat'n lausetta algoritminomaisesti sovellettaessa voi käydä niin, että kaikki kokeiltavat kantaluvut toteuttavat lauseen kongruenssin. Valitettavasti tästä ei voida tehdä johtopäätöstä, että luku olisi alkuluku, kuten seuraava esimerkki osoittaa.

Esimerkki 3.6. *Olkoon $n = 5 \cdot 13 \cdot 17 = 1105$. Valittiinpa kantaluvuksi a mikä luku tahansa, niin huomataan että $a^{1104} \equiv 1 \pmod{1105}$, vaikka n ei ole alkuluku [Anderson, Bell 1997]. Tällaisia yhdistettyjä lukuja, joita Fermat'n lause ei voi todistaa yhdistetyksi, sanotaan Carmichaelin luvuiksi.*

Lause 3.7. *Luku $n \in \mathbb{Z}_+$ on alkuluku, jos ja vain jos $\phi(n) = n - 1$.*

Todistus. Oletetaan ensin, että $p \in \mathbb{P}$. Tällöin $\phi(p) = p - 1$.
Olkoon sitten $n \in \mathbb{Z}_+ \setminus \mathbb{P}$. Tällöin luvulla n on ei-triviaali tekijä $a < n$, joten $\phi(n) \leq n - 2$. □

Lause 3.8 (Lucas). *Jos $n \in \mathbb{Z}_+$ ja on olemassa $a \in \mathbb{Z}$ siten, että*

$$a^{n-1} \equiv 1 \pmod{n}$$

ja

$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$$

kaikilla $p \in \mathbb{P}$, joilla $p \mid n - 1$, niin n on alkuluku.

Todistus. Ehdosta $a^{n-1} \equiv 1 \pmod{n}$ seuraa, että $syt(a, n) = 1$, joten $ord_n a \mid (n-1)$. Jos $p \in \mathbb{P}$ ja $p \mid (n-1)$, niin oletuksen mukaan $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n} \Rightarrow ord_n a \nmid \frac{n-1}{p}$. Siis $ord_n a \mid (n-1)$, mutta $ord_n a \nmid \frac{n-1}{p}$ millään alkuluvulla $p \mid n-1$. Tällöin on oltava $ord_n a = n - 1$. Siis ryhmässä $\mathbb{Z}_n^*$ on alkio a, jonka kertaluku on $n - 1$. Alkion kertaluku jakaa ryhmän kertaluvun [Niemenmaa, Myllylä, Tirilä 2006], joten $\phi(n) = n - 1$ ja edellisestä lauseesta seuraa, että n on alkuluku. □

Esimerkki 3.9. *Onko $n = 199$ alkuluku? Nyt on voimassa*

$$n - 1 = 198 = 2 \cdot 3^2 \cdot 11,$$

ja lisäksi

$$3^{198} \equiv 1 \pmod{199},$$
$$3^{\frac{198}{2}} \equiv 198 \not\equiv 1 \pmod{199},$$
$$3^{\frac{198}{3}} \equiv 106 \not\equiv 1 \pmod{199},$$
$$3^{\frac{198}{11}} \equiv 125 \not\equiv 1 \pmod{199}.$$

Siten [3]:n kertaluku ryhmässä Z^*_{199} on 198, mikä on mahdollista vain kun Z^*_{199}:n kertaluku on 198. Siis 199 on alkuluku. Tämä on Lucasin lauseen idea.

Määritelmä 3.10. *Olkoon $n \in \mathbb{Z}_+$ ja $n - 1 = 2^k w$, missä w on pariton ja $k \geq 1$. Olkoon $b \in \mathbb{Z}_+$ sellainen, että $syt(b, n) = 1$. Luvun n sanotaan läpäisevän **Millerin testin** kannassa b, jos joko*

$$\textbf{(a)}\ b^w \equiv 1 \pmod{n}$$

tai

$$\textbf{(b)}\ b^{2^i w} \equiv -1 \pmod{n} \text{jollakin } i \in \mathbb{Z}, 0 \leq i \leq k - 1.$$

Lause 3.11. *Kaikki alkuluvut $p > 2$ läpäisevät Millerin testin missä tahansa kannassa $b < p$.*

Todistus. Olkoon $p-1 = 2^e w$, missä w on pariton. Olkoon $a \in \mathbb{Z}, syt(a, p) = 1$. Merkitään

$$b_k := a^{2^{e-k}w}, k = 0, 1, 2, ..., e.$$

Jos **(a)**-ehto toteutuu, niin p läpäisi testin. Jos ei, niin $b_e = a^w \not\equiv 1 \pmod{p}$. Olkoon j pienin indeksi, jolla $b_j \not\equiv 1 \pmod{p}$. Tällöin $b_{j-1} \equiv 1 \pmod{p}$. Nyt $j \neq 0$, koska $b_0 = a^{p-1} \equiv 1 \pmod{p}$, ja

$$b_j^2 = b_{j-1} \equiv 1 \pmod{p}$$

Toisen asteen kongruenssiyhtälön $b_j^2 \equiv 1 \pmod{p}$ mahdollisia ratkaisuja ovat $b_j \equiv 1$ tai $b_j \equiv -1 \pmod{p}$. Modulo p on alkuluku, joten Lagrangen lauseesta seuraa, että muita ratkaisuja ei ole. Lisäksi ensimmäinen vaihtoehto $b_j \equiv 1 \pmod{p}$ ei käy luvun j määrittelyn takia. Siten on oltava $b_j \equiv -1 \pmod{p}$, eli **(b)**-ehto toteutuu ja p läpäisi testin. □

Esimerkki 3.12. *Tarkastellaan lukua* $n = 91 = 7 \cdot 13$. *Käymällä läpi kaikki tätä pienemmät* 91*:n kanssa keskenään jaottomat luvut saadaan seuraava tulos:*

Luku 91 *läpäisee Millerin testin kannoissa*

$$L := \{1, 9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90\}.$$

Näitä lukuja sanotaan ***valehtelijoiksi*** *luvulle* 91. *Missään muussa kannassa luku* 91 *ei läpäise Millerin testiä. Tällaisia kantoja on* $\phi(91) - |L| = 72 - 18 = 54$ *kappaletta, ja niitä sanotaan* ***todistajiksi*** *luvun 91 jaollisuudelle. Erityisesti huomataan, että* $\frac{18}{72} = \frac{1}{4}$. *Tähän havaintoon perustuu Miller-Rabinin algoritmi.*

Lause 3.13 (**Rabin**). *Olkoon* $n \in \mathbb{Z}_+$ *pariton. Valitaan satunnaisesti* k *lukua* b_1, b_2, ..., b_k, $0 < b_i < n$ *ja* $syt(b_i, n) = 1$. *Jos* n *on yhdistetty, niin todennäköisyys että* n *läpäisee Millerin testin jokaisessa kannassa* b_i *on pienempi kuin* $(\frac{1}{4})^k$.

Todistus. [Rabin 1980]. □

Laskennallisissa sovelluksissa alkulukujen nopea generointi on käytännöllisempää kuin taulukoiden säilyttäminen[PrimeB]. Vaikka Miller-Rabinin testi antaa "vain"probabilistisen arvion siitä, onko luku alkuluku, niin tämä arvio on kuitenkin erittäin hyvä ja testi kokonaisuudessaan on todella nopea. Esimerkiksi kryptografisia sovelluksia varten etsittäessä sopivan kokoisia (suuruusluokkaa 1024-2048 bittiä) alkulukuja, vaikkapa 10:n kantaluvun kokeileminen alkulukuehdokasta kohden vie häviävän pienen ajan ja tämän jälkeen todennäköisyys, että testi antoi väärän tuloksen on $\frac{1}{4^{10}} \approx 0.954 \cdot 10^{-6}$. Tehokkaan algoritmista tekee se, että yhden todistajan löytämisen jälkeen ehdokas tiedetään varmasti yhdistetyksi ja käytännössä tämä tapahtuu todennäköisesti jo jollakin ensimmäisistä ajoista [Menezes, van Oorschot, Vanstone 1996]. Jos halutaan etsiä alkulukuja joltakin lukuväliltä, niin Miller-Rabinin testiä voidaan käyttää erittäin nopeaan todennäköisten alkulukuehdokkaiden hakemiseen ja sitten käyttää jotain determinististä testiä [Agrawal, Kayal, Saxena 2002] ehdokkaiden jaottomuuden varmistamiseksi.

4 Lähteet

Agrawal, M., Kayal, N., Saxena, N. 2004. PRIMES is in P. Annals of Mathematics 160 (2004), no. 2, s. 781-793.
Saatavilla http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf.

Anderson, J., Bell, J. 1997. Number Theory with Applications. Prentice Hall. s. 24-97, 175-204, 272-279.

Holtz, B. Human Knowledge - Foundations and Limits.
http://humanknowledge.net/SocialScience/Futurology/Timeline.html.
Viitattu 2007/03/06.

Matala-Aho, T. 2006. Lukuteoria 1 Luentorunko. Oulun yliopisto. s. 29.

Menezes, A., Van Oorschot, P., Vanstone, S. 1996. Handbook of Applied Cryptography. CRC Press. Kappale 4.
Saatavilla http://www.cacr.math.uwaterloo.ca/hac/about/chap4.pdf.

Myllylä, K. Niemenmaa, M. Tirilä, J-M. 2006. Algebra 1 Luentorunko. Oulun yliopisto. s. 12.

PrimeA. 2007. The Prime Database: The List of Largest Known Primes Home Page.
http://primes.utm.edu/primes/. Viitattu 2007/03/04.

PrimeB. 2007. The Prime Database: What is the longest list of primes?
http://primes.utm.edu/notes/faq/LongestList.html. Viitattu 2007/04/01.

Rabin, M. 1980. Probabilistic Algorithm for Testing Primality. Journal of Number Theory, Volume 12, 1980, 128-138.

Tom's Hardware. 2007. CPU Performance Comparison Charts.
http://www23.tomshardware.com/cpu.html?modelx=33&model1=430&model2=464&chart=159. Viitattu 2007/03/06.