Harjoitukset 8 Ratkaisut **Lukuteoria**
tiistai 8.11.2011 16.00-17.30 MaD-302

1. *Käy läpi leikkiesimerkki RSA-algoritmista.*

$p = 11$, $q = 13$, $m = pq = 143$. Salaajan avainluku $e = 77$.

a) Tulkinta-avainluku on $d = e^{-1} = 77^{-1} \in \mathbb{Z}^*_{\varphi(m)} = \mathbb{Z}^*_{(p-1)(q-1)} = \mathbb{Z}^*_{120}$. Ratkaistaan Eukleideen algoritmilla Diofantoksen yhtälö $d \cdot 77 + d' \cdot 120 = 1$. Tulos on $d = 53$. ($d' = -34$, mutta sitä ei tarvita jatkossa.)

b) Kryptataan ja julkaistaan sanoma 50: ULOS=$50^e = 50^{77} \pmod{143} = 85 (\in \mathbb{Z}^*_{143})$.

c) Tulkitaan kryptattu sanoma: SANOMA= $ULOS^{53} = 85^{53} \pmod{143}$. Lasketaan malliksi auki peräkkäisin neliöinnein $\pmod{145}$:

$$85^0 \equiv 1 \pmod{143}$$
$$85^1 \equiv 85 \pmod{143}$$
$$85^2 \equiv 75 \pmod{143}$$
$$85^4 \equiv 75^2 \equiv 48 \pmod{143}$$
$$85^8 \equiv 48^2 \equiv 16 \pmod{143}$$
$$85^{16} \equiv 16^2 \equiv 113 \pmod{143}$$
$$85^{32} \equiv 25^2 \equiv 42 \pmod{143}$$

Siis $85^{53} \equiv 85^{32} \cdot 85^{21} \equiv 85^{32} \cdot 85^{16} \cdot 85^4 \cdot 85^1 \equiv 42 \cdot 113 \cdot 48 \cdot 85 \equiv 50 \pmod{143}$. (SE TOIMII!)

d) Jos olisin alunperin tiennyt vain salausavaimen $e = 77$, en olisi voinut kryptata sanomaa. Tarvitaan myös luku m Näillä luvulla $e = 77$, $m = 143$ olisin toki osannut murtaa koodin tuntematta salaisia lukuja p, q. Olisin vain jakanut luvun $m = 143$ tekijöikseen 11 ja 13 ja laksenut luvun d kuten yllä. Tositilanteessa valitaan alkuluvut p ja q niin suuriksi, ettei tekijöihin jako onnistu nopeallakaan tietokoneella.

(**Wikipedia**: RSA keys are typically 1024–2048 bits long. Some experts believe that 1024-bit keys may become breakable in the near future (though this is disputed); few see any way that 4096-bit keys could be broken in the foreseeable future. Therefore, it is generally presumed that RSA is secure if n is sufficiently large. If n is 300 bits or shorter, it can be factored in a few hours on a personal computer, using software already freely available. Keys of 512 bits have been shown to be practically breakable in 1999 when RSA-155 was factored by using several hundred computers and are now factored in a few weeks using common hardware.[10] A theoretical hardware device named TWIRL and described by Shamir and Tromer in 2003 called into question the security of 1024 bit keys. It is currently recommended that n be at least 2048 bits long.)

2. *Ratkaisen liitteen 4 tehtävän 4.1.*

Olkoon p alkuluku siten, että $p \equiv 3 \pmod 4$ ja olkoon a neliönjäännös $\pmod p$. Osoitan, että alkion a neliöjuuri kunnassa $\mathbb{Z}_p$ on $c = a^{\frac{p+1}{4}}$ eli, että $a^{\frac{p+1}{2}} \equiv a \pmod p$:

Eulerin kriteerin (3.1) mukaan $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$. Yllä oletettin, että a on neliönjäännös $\pmod p$, joten $\left(\frac{a}{p}\right) = 1$. Siis $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, josta $a^{\frac{p-1}{2}} \equiv a^2 \pmod p$. □

3. *Muutan muotoon* $D^2 \equiv c \pmod m, \quad D = ax + b.$

a) $\pmod{10}$:

$$x^2 + 4x + 5 \equiv 0 \iff (x+2)^2 + 1 \equiv 0 \iff (x+2)^2 \equiv -1 \equiv 9.$$

b) $\pmod{10}$:

$$\begin{aligned} x^2 + 3x + 5 \equiv 0 \pmod{10} &\implies 4x^2 + 12x + 20 \equiv 0 \pmod{40} \\ &\iff (2x+3)^2 \equiv 29 \pmod{40}. \end{aligned}$$

c) $\pmod 9$:

$$x^2 + 3x + 5 \equiv 0 \overset{4 \in \mathbb{Z}_9^*}{\iff} 4x^2 + 12x + 20 \equiv 0 \iff (2x+3)^2 \equiv 9 - 20 \equiv 7.$$

d) $\pmod 9$:

$$\begin{aligned} 3x^2 + x + 5 \equiv 0 \pmod 9 &\iff 9x^2 + 3x + 15 \equiv 0 \pmod{27} \\ &\iff 4 \cdot 9x^2 + 4 \cdot 3x + 4 \cdot 15 \equiv 0 \pmod{27} \\ &\iff (6x+1)^2 - 1 + 60 \equiv 0 \pmod{27} \\ &\iff (6x+1)^2 + 5 \equiv 0 \pmod{27} \\ &\iff (6x+1)^2 \equiv -5 \equiv 22 \pmod{27} \end{aligned}$$

4. *Olkoon* p *pariton alkuluku ja* $(a,p) = (b,p) = 1$.

Jos kummallakaan kongruensseista $x^2 \equiv a \pmod p$ ja $x^2 \equiv b \pmod p$ ei ole ratkaisua, niin silloin $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, joten $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$ ja siis kongruenssilla $x^2 \equiv ab \pmod p$ on ratkaisu. □

5.

Lasketaan Legendren symbolit sen selvittämiseksi, mitkä annetuista kongruensseista ovat ratkeavia.

a) $\left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) \cdot (-1)^{\frac{7-1}{2}\frac{101-1}{2}} = \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) \cdot (-1)^{\frac{3-1}{2}\frac{7-1}{2}} = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$. Siis ei!

b) $\left(\frac{-7}{101}\right) = \left(\frac{-1}{101}\right) \cdot \left(\frac{7}{101}\right) = (-1)^{\frac{101-1}{2}} \left(\frac{7}{101}\right) = (-1)^{\frac{101-1}{2}} \left(\frac{101}{7}\right) \overset{a)}{=} -1$. Siis ei!

c) $x^2 \equiv 7 \pmod{303} \implies x^2 \equiv 7 \pmod{101}$. Siis a)-kohdan mukaan ei!

6. *Mille alkuluvuille* p *on kongruenssi* $x^2 \equiv -3 \pmod{3p}$ *ratkeava?*

Heti huomaa, että $p = 2$ kelpaa ja $p = 3$ ei kelpaa, onhan $3^2 = 9 \equiv 3 \equiv -3 \pmod 6$ eikä mikään neliö ole $\equiv -3 \pmod 9$. Muille alkuluvuille laskin näin:

$$\begin{aligned} x^2 \equiv -3 \pmod{3p} &\implies 3 \mid x^2 \implies 3 \mid x \implies x = 3y \quad (y \in \mathbb{Z}) \\ (3y)^2 \equiv -3 \pmod{3p} &\iff 3p \mid 9y^2 + 3 \iff p \mid 3y^2 + 1 \\ &\iff 3y^2 \equiv -1 \pmod p \\ &\iff y^2 = -(1/3) \in \mathbb{Z}_p, \end{aligned}$$

joka ratkeaa tasan silloin, kun $-(1/3) \in \mathbb{Z}_p$ on neliönjäännös, mikä taas viime kerran tehtävän mukaan on yhtäpitävää sen kanssa, että 3 on neliönjäänmös $\pmod p$., j se tapahtuu (laskemalla Legendren symboli!), kun p on muotoa $6n+1$.

7. *Ratkaisut lineaarisiin Diofantoksen yhtälöihin yksi ratkaisu löydetään esimerkiksi Eukleideen algoritmilla. Loput saa kaavalla (1) $x_k = x_0 + kb$ ja (2) $y_k = y_0 - ka$.*

a) $3x + 2y = 1 \qquad (1 + 2k; -1 - 3k)$
b) $3x - 2y = 1 \qquad (1 + 2k; 1 + 3k)$
c) $6x + 4y = 2 \qquad (1 + 2k; -1 - 3k)$
d) $17x - 43y = 100 \qquad (16 + 43k; 4 + 17k)$
e) $110x - 174y = 18 \qquad (-3 + 87k; -2 + 55k)$

8. *Ol. a, b, $c > 0$, $(a, b) = 1$. Tutkitaan, onko $ax + by = c$:lle positiivilukuratkaisuja.*

a) Oletetaan lisäksi $ab < c$. Osoitetaan, että on olemassa positiivinen ratkaisu. Koska $(a, b) = 1$ niin on olemassa jokin ratkaisu (x_0, y_0) ja muut ratkaisut ovat (x_k, y_k), missä (1) $x_k = x_0 + kb$ ja (2) $y_k = y_0 - ka$. Valitaan mahdollisimman pieni k, jolla $x_k > 0$ vielä toteutuu, jolloin (1) mukaisesti $0 \leq x_k (= x_0 + kb) \leq b$. Tällöin

$$y_k = \frac{c - ax_k}{b} > \frac{ab - ax_k}{b} \geq \frac{ab - ab}{b} = .$$

b) Oletetaan $a + b > c$. Osoitetaan, että ei ole olemassa positiivista ratkaisua. Jos olisi a, b, x, $y > 0$, niin olisi a, b, x, $y \geq 1$, koska kaikki ovat kokonaislukuja. Silloin $c = ax + by \geq a + b$ vastoin oletusta. □

9. *Määrää kaikki primitiiviset Pythagoraan kolmikot (x, y, z), joilla $y = 40$. Määrää myös ei-primitiiviset.*

Primitiiviset ((x,y,z)=1) Pythagoraan kolmikot $(x; y; z)$, missä y parillinen (NÄIN!), ovat tasan kolmikot $(a^2 - b^2; 2ab; a^2 + b^2)$; missä $a > b > 0$, $(a, b) = 1$ ja a:lla ja b:llä eri pariteetti. Tehtävässä on $2ab = y = 40$ eli $ab = 20 = 2^2 \cdot 5$. Siis $a \in \{1, 2, 4, 5, 10, 20\}$ jolloin samassa järjestyksessä $b \in \{20, 10, 5, 4, 2, 1\}$. Koska $a > b$, tulevat kysymykseen vain 3 viimeistä vaihtoehtoa, mutta myös $(10; 2)$ karsiutuu, koska on oltava $(a, b) = 1$. Jäljelle jääneissä pareissa $(a; b) = 5; 4)$ ja $(20; 1)$ on a:lla ja b:llä eri pariteettikin, joten ne kelpaavat ja antavat kolmikot $(x; y; z) = (a^2 - b^2; 2ab; a^2 + b^2) = (\mathbf{9}; \mathbf{40}; \mathbf{41})$ ja $(\mathbf{399}; \mathbf{40}; \mathbf{401})$.

Kaikki Pythagoraan kolmikot $(x; y; z)$, missä y parillinen (NÄIN!), ovat tasan kolmikot $(k(a^2 - b^2); 2kab; k(a^2 + b^2))$; missä $a > b > 0$, $(a, b) = 1$ ja a:lla ja b:llä eri pariteetti. Tehtävässä on $2kab = y = 40$,joten $kab = 20 = 2^2 \cdot 5$ ja siis $ab \in \{1, 2, 4, 5, 10, 20\}$. Tapaus $ab = 20$ on käsitelty. Muut käsitellään samalla tavalla:

$ab = 10$ Siis $a \in \{1, 2, 5, 10\}$ jolloin samassa järjestyksessä $b \in \{10, 5, 2, 1\}$. Koska $a > b$, tulevat kysymykseen vain 2 viimeistä vaihtoehtoa, $(a; b) = (5; 2)$ ja $(10; 1)$, joissa on oikea parieetti ja syt, ja saadaan, muistaen, että tässä $k = 2$, $(x; y; z) = (2(a^2 - b^2); 4ab; 2(a^2 + b^2)) = (\mathbf{42}; \mathbf{40}; \mathbf{58})$ ja $(\mathbf{198}; \mathbf{40}; \mathbf{202})$.

$ab = 5$ Siis $a \in \{1, 5\}$ jolloin samassa järjestyksessä $b \in \{5, 1\}$. Koska $a > b$, tulee kysymykseen vain 1. vaihtoehto, $(a; b) = (5; 1)$, jossa on oikea parieetti ja syt, ja saadaan, muistaen, että tässä $k = 4$, $(x; y; z) = (4(a^2 - b^2); 8ab; 4(a^2 + b^2)) = (\mathbf{96}; \mathbf{40}; \mathbf{58})$.

$ab = 4$ Siis $a \in \{1, 2, 4\}$ jolloin samassa järjestyksessä $b \in \{4, 2, 1\}$. Koska $a > b$, tulee kysymykseen vain 1. vaihtoehto, $(a; b) = (4; 1)$, jossa on oikea parieetti ja syt, ja saadaan, muistaen, että tässä $k = 5$, $(x; y; z) = (5(a^2 - b^2); 10ab; 5(a^2 + b^2)) = (\mathbf{75}; \mathbf{40}; \mathbf{85})$.

$ab = 2$ Siis $a \in \{1, 2\}$ jolloin samassa järjestyksessä $b \in \{2, 1\}$. Koska $a > b$, tulee kysymykseen vain 1. vaihtoehto, $(a; b) = (2; 1)$, jossa on oikea parieetti ja syt, ja saadaan, muistaen, että tässä $k = 10$, $(x; y; z) = (10(a^2 - b^2); 20ab; 10(a^2 + b^2)) = (\mathbf{30}; \mathbf{40}; \mathbf{50})$.

$ab = 1$ Siis $a = b = 1$. Koska pitää olla $a > b$, tämä vaihtoehto ei toteudu.

10. *Osoita, että Pythagoraan kolmikossa (x, y, z) aina vähintään yksi luvuista on jaollinen 3:lla ja samoin 4:lla ja 5:llä.*

a) Vähintään yksi luvuista x, y, z on jaollinen 3:lla: Jos ei x eikä z ole jollinen 3:lla, niin $x \equiv \pm 1 \pmod 3$ ja $z \equiv \pm 1 \pmod 3$, jolloin $x^2 \equiv 1 \pmod 3$ ja $z^2 \equiv 1 \pmod 3$ ja siis $y^2 = z^2 - x^2 \equiv 1 - 1 = 0 \pmod 3$.

b) vähintään yksi luvuista x, y, z on jaollinen 4:lla: Riittää tutkia primitiivisiä ratkaisuja. Jos x on parillinen, niin $x = 2ab$, missä a:lla ja b:lla on eri pariteetti, siis toinen on parillinen, jolloin $4 \mid x$.

c) vähintään yksi luvuista x, y, z on jaollinen 5:llä: Riittää osoittaa, että tulo xyz on jaollinen 5:llä. Riittää tutkia primitiivisiä ratkaisuja. Ratkaisukaavan mukaan

$$xyz = 2ab(a^2 - b^2)(a^2 + b^2) = 2ab(a^4 - b^4) = 2(a^5 b - ab^5).$$

Fermat'n pienen lauseen mukaan $a^5 = a \pmod 5$ ja samoin $b^5 = b \pmod 5$, joten $xyz \equiv 2(ab - ab) = 0 \pmod 5$. (Samalla tavoin voisi todistaa jaollisuuden 3:lla.)