Lukuteorian alkeet
Kuudensien harjoitusten ratkaisuita

1. Kuinka monta primitiivistä juurta on modulossa 13? Määritä lisäksi primitiiviset juuret modulo 13.

2. Esitä koko redusoitu jäännössysteemi jonkin valitsemasi primitiivisen juuren avulla.

Ratkaisut. Selvitetään ensiksi luvun kaksi kertaluku $\mathrm{ord}_{13}\,2$. Kyseinen kertaluku jakaa luvun $13-1=12$, ja on siten jokin luvuista 1, 2, 3, 4, 6 ja 12. Varmasti $\mathrm{ord}_{13}2 \neq 1$, ja koska lisäksi

$$2^2 \equiv 4 \not\equiv 1, \quad 2^3 \equiv 8 \not\equiv 1, \quad 2^4 \equiv 16 \equiv 3 \not\equiv 1, \quad \text{ja} \quad 2^6 \equiv 64 \equiv 12 \not\equiv 1 \pmod{13},$$

on oltava $\mathrm{ord}_{13}2 = 12$ ja luku 2 on primitiivinen juuri modulo 13.

Nyt kaikki nollasta poikkeavat jäännösluokat saadaan esitettyä luvun 2 potensseina: Lasketaan ensin puuttuvat potenssit

$$2^5 \equiv 32 \equiv 6, \quad 2^7 \equiv 2^{5+2} \equiv 24 \equiv 11, \quad 2^8 \equiv 2^{7+1} \equiv 22 \equiv 9,$$
$$2^9 \equiv 2^{8+1} \equiv 18 \equiv 5, \quad 2^{10} \equiv 2^{9+1} \equiv 10, \quad 2^{11} \equiv 2^{10+1} \equiv 20 \equiv 7.$$

Nyt kysytyt esitykset ovat

$1 \equiv 2^{12}$	$5 \equiv 2^9$	$9 \equiv 2^8$
$2 \equiv 2^1$	$6 \equiv 2^5$	$10 \equiv 2^{10}$
$3 \equiv 2^4$	$7 \equiv 2^{11}$	$11 \equiv 2^7$
$4 \equiv 2^2$	$8 \equiv 2^3$	$12 \equiv 2^6$

Koska jokaisella $\alpha \in \{1, 2, \ldots, 12\}$ on potenssin 2^α kertaluku

$$\mathrm{ord}_{13}2^\alpha = \frac{\mathrm{ord}_{13}2}{(\alpha, \mathrm{ord}_{13}2)} = \frac{12}{(\alpha, 12)},$$

ovat primitiiviset juuret modulo 13 ne näistä potensseista, joille $(\alpha, 12) = 1$, eli

$$2^1 \equiv 2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11 \quad \text{ja} \quad 2^{11} \equiv 7.$$

3. Ratkaise yhtälö $x^2 \equiv 12 \pmod{13}$. (Vihje: esitä 12 primitiivisen juuren avulla, järkeile, miksi saat ottaa neliöjuuret yhtälöstä, ja viimeistele ratkaisu Lagrangen lauseella.)

Ratkaisu. Edellisestä tehtävästä tiedämme, että $12 \equiv 2^6 \pmod{13}$. Koska $(\pm 2^3)^2 = 2^6 \equiv 12 \pmod{13}$, on olemassa kaksi eri ratkaisua $x \equiv \pm 2^3 \equiv \pm 8 \pmod{13}$, eli ratkaisut $x \equiv 5$ ja $x \equiv 8 \pmod{13}$. Toisaalta Lagrangen lauseen nojalla ratkaisuita on enintään kaksi.

4. Olkoon $n = 47 \cdot 53$. Valitse jokin e RSA:n julkisen avaimen osaksi (ei, ei lukua 1, koska silloin salaus ei varsinaisesti salaisi), ja määritä loput RSA:n käytössä vaadittavat parametrit. Havainnollista lopulta järjestelmää kryptaamalla luku 28 ja sen jälkeen purkamalla kryptaus.

Ratkaisu. Lasketaan ensin

$$\varphi(n) = \varphi(47 \cdot 53) = 46 \cdot 52 = 2 \cdot 23 \cdot 2 \cdot 2 \cdot 13 = 2^3 \cdot 13 \cdot 23 = 2392.$$

Luvun e täytyy olla yhteistekijätön luvun 2392 kanssa. Luvun 2392 tekijöihinjaosta nähdään, että esimerkiksi luku $e = 11$ kelpaa. Nyt luku d on ratkaistava kongruenssiyhtälöstä

$$de \equiv 1 \pmod{\varphi(n)},$$

tai käytännöllisemmin Diofantosin yhtälöstä

$$11d - 2392x = 1.$$

Ratkaistaan d Eukleideen algoritmilla: ensinnäkin

$$2392 = 217 \cdot 11 + 5, \quad \text{ja} \quad 11 = 2 \cdot 5 + 1,$$

eli

$$1 = 11 - 2 \cdot 5 = 11 - 2\,(2392 - 217 \cdot 11) = 435 \cdot 11 - 2 \cdot 2392,$$

eli $d = 435$ kelpaa.

Nyt siis julkinen avain on $(n, e) = (47 \cdot 53, 11) = (2491, 11)$, ja salainen avain on $(p, q, \varphi(n), d) = (47, 53, 2392, 435)$.

Nyt viestin $w = 28$ salaus tapahtuu laskemalla

$$\begin{aligned} w' \equiv w^e \equiv 28^{11} \equiv 28^{1+2+8} &\equiv 28 \cdot 784 \cdot 2027 \\ &\equiv 21952 \cdot 2027 \equiv 44496704 \equiv 2462 \pmod{2491} \end{aligned}$$

Viestin purkaminen tapahtuu laskemalla

$$\begin{aligned} w'^d \equiv 2462^{435} &\equiv -29^{1+2+16+32+128+256} \equiv -29 \cdot 841 \cdot 2217 \cdot 346 \cdot 1976 \cdot 1179 \\ &\equiv -24389 \cdot 767082 \cdot 2329704 \equiv -1970 \cdot 2345 \cdot 619 \equiv -4619650 \cdot 619 \\ &\equiv -1336 \cdot 619 \equiv -826984 \equiv -2463 \equiv 28 \pmod{2491}. \end{aligned}$$

5. Olkoon $n = 16637$. Määritä sen alkutekijät p ja q.

Ratkaisu. Olkaamme toiveikkaita ja kokeilkaamme, onko kyseessä lauseen 42 kuvailema tilanne: lasketaan

$$t = \lceil \sqrt{n} \rceil = \lceil \sqrt{16637} \rceil = 129,$$

ja

$$r = \sqrt{t^2 - n} = \sqrt{129^2 - 16637} = \sqrt{4} = 2.$$

Nyt huomataan, että

$$n = t^2 - \left(t^2 - n\right) = t^2 - r^2 = (t + r)\,(t - r) = (129 + 2)\,(129 - 2) = 131 \cdot 127.$$

6. Olkoon RSA:n julkinen avain $(n, e) = (16637, 11)$. Määritä loput parametrit, eli murra systeemi.

Ratkaisu. Edellisestä tehtävästä tiedämme, että luvun n tekijöihinjako on $131 \cdot 127$. Siis voimme laskea

$$\varphi(n) = 130 \cdot 126 = 16380,$$

ja nyt oleellinen salainen eksponentti d voidaan ratkaista Diofantosin yhtälöstä

$$11d - 16380x = 1,$$

mikä on jälleen tehtävissä Eukleideen algoritmilla: lasketaan

$$16380 = 1489 \cdot 11 + 1.$$

Tästä seuraa, että

$$\begin{aligned} 1 = 16380 + (-1489) \cdot 11 = 16380 \cdot (-10) + (16380 - 1489) \cdot 11 \\ = 16380 \cdot (-10) + 14891 \cdot 11. \end{aligned}$$

Ja nyt huomaammekin, että $d = 14891$ kelpaa.