Näide Legendre'i/Jacobi sümboli leidmisest

1. Leiame algarvude 5237 ja 7901 jaoks Legendre'i sümboli $\left(\frac{5237}{7901}\right)$ väärtuse kahel eri viisil.

a) Esiteks, kasutame Legendre'i sümboli omadusi, Gaussi ruutvastavusseadust ja algteguriteks lahutamist:

$$\left(\frac{5237}{7901}\right) = \left(\frac{7901}{5237}\right) = \left(\frac{2664}{5237}\right) = \left(\frac{2^3 \cdot 3^2 \cdot 37}{5237}\right) = \left(\frac{2}{5237}\right)\left(\frac{37}{5237}\right),$$

sest $7901 \equiv 1 \pmod 4$ ja $7901 \equiv 2664 \pmod{5237}$. Kuna $5237 \equiv 5 \equiv -3 \pmod 8$, siis

$$\left(\frac{2}{5237}\right) = -1.$$

Faktide $37, 5237 \in \mathbb{P}$, $37 \equiv 1 \pmod 4$ ja $5237 \equiv 20 \pmod{37}$ tõttu

$$\left(\frac{37}{5237}\right) = \left(\frac{5237}{37}\right) = \left(\frac{20}{37}\right) = \left(\frac{2^2 \cdot 5}{37}\right) = \left(\frac{5}{37}\right).$$

Kuna $5, 37 \in \mathbb{P}$, $5 \equiv 1 \pmod 4$, $37 \equiv 2 \pmod 5$ ja $5 \equiv -3 \pmod 8$, siis

$$\left(\frac{37}{5237}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Järelikult

$$\left(\frac{5237}{7901}\right) = \left(\frac{2}{5237}\right)\left(\frac{37}{5237}\right) = (-1)^2 = 1.$$

b) Gaussi ruutvastavusseaduse rakendamine vaid Legendre'i sümbolite abil on keeruline, sest iga kord tuleb veenduda, et mõlemad Legendre'i sümbolis esinevad arvud on algarvud. Sellest kontrollist vabanemiseks võib vahepealsetes etappides ja üldse Jacobi sümboli väärtuste leidmisel kasutada Jacobi sümbolit, mille korral tuleb uurida vaid paarituks arvuks olemist. Seetõttu on enne Gaussi ruutvastavusseaduse rakendamist vaja eraldada välja kõik "lugejas" sisalduvad kahe astmed. Protsess näeb välja selline:

$$\left(\frac{5237}{7901}\right) = \left(\frac{7901}{5237}\right) = \left(\frac{2664}{5237}\right) = \left(\frac{2^3 \cdot 333}{5237}\right) = \left(\frac{2}{5237}\right)\left(\frac{333}{5237}\right).$$

Eelnevast teame, et $\left(\frac{2}{5237}\right) = -1$. Kuna 333 ja 5237 on paaritud arvud, $333 \equiv 1 \pmod 4$ ja $5237 \equiv 20 \pmod{37}$, siis

$$\left(\frac{333}{5237}\right) = \left(\frac{5237}{333}\right) = \left(\frac{20}{333}\right) = \left(\frac{2^2 \cdot 5}{333}\right) = \left(\frac{5}{333}\right).$$

Jälle, $5 \equiv 1 \pmod 4$ ning 3, 5 ja 333 on paaritud, seega

$$\left(\frac{333}{5237}\right) = \left(\frac{5}{333}\right) = \left(\frac{333}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Järelikult

$$\left(\frac{5237}{7901}\right) = \left(\frac{2}{5237}\right)\left(\frac{333}{5237}\right) = (-1)^2 = 1.$$