# Peatükk 8

# Pollardi $p-1$ algoritm

Vaatleme Pollardi $p-1$ algoritmi (teada aastast 1974), mis on efektiivne teatud struktuuriga suurte täisarvude jaoks.

**Algoritm 8.0.1 (Pollardi $p-1$ algoritm)** *Sisendid: paaritu täisarv $n$, mida tahame faktoriseerida, ning tõke $B$.*

```
1  funct pollard(n, B) ≡
2    a := 2
3    for j := 2 to B do a := a^j mod n od
4    d := gcd(a − 1, n)
5    if 1 < d < n
6      then
7            pollard := d
8       else
9            pollard := don't know
10   fi.
```

Kirjeldame algoritmi tööd. Oletame, et $p$ on arvu $n$ algarvuline jagaja ning suvalise algarvu astme $q \mid p-1$ korral $q \leq B$. Sel juhul $(p-1) \mid B!$. Pärast **for** tsüklit (samm 3) $a \equiv 2^{B!} \pmod{n}$ ning seega ka $a \equiv 2^{B!} \pmod{p}$, kuna $p \mid n$. Kuna $2^{p-1} \equiv 1 \pmod{p}$ (Fermat' väike teoreem) ning $(p-1) \mid B!$, siis pärast **for** tsüklit ka $a \equiv 1 \pmod{p}$, seega $p \mid (a-1)$, millest ning faktist $p \mid n$ tuleneb, et $p \mid d = \gcd(a-1, n)$, kus algarv $d$ on arvu $n$ mittetriviaalne tegur (kui muidugi $a \neq 1$). Teades mittetriviaalset tegurit $d$, üritame edasi faktoriseerida arve $d$ ning $\frac{n}{d}$ (juhul kui on tegu kordarvudega).

**Näide 8.0.2** *Olgu $n = 157707008441$, ning $B = 180$. Algoritmi rakendades saame $a = 11620221425$, ning $d = 135979$. Arvu $n$ algarvudeks lahutuseks saame $n = 135979 \times 115979$. Antud juhul algoritm töötab, kuna arvul $135978$ on "väikesed" algarvulised tegurid: $135978 = 2 \times 3 \times 131 \times 173$. Seega võttes $B \geq 173$, saame, et $135978 \mid B!$, nagu soovitud.*

Algoritmi 8.0.1 jooksul tehakse $B-1$ modulaarset astendamist, iga neist võtab maksimaalselt $2\log B$ modulaarset korrutamist, kasutades tuntud algoritmi. Suurima ühisteguri saame leida ajas $O((\log n)^3)$, seega Pollardi $(p-1)$-algoritmi keerukus on $O(B\log B\cdot(\log n)^2+(\log n)^3)$. Kui $B=O((\log n)^i)$ mingi fikseeritud täisarvu $i$ korral, siis on algoritm polünomiaalne, ent samas arvu $B$ sellise valiku korral on õnnestumise tõenäosus väga väike. Arvu $B$ väärtuse drastiline suurendamine (näiteks suuruseni $\sqrt{n}$) suurendaks õnnestumise tõenäosust, kuid sel juhul ei tööta algoritm enam kiiremini kui täielik läbijagamine.

Seega on Pollardi $p-1$ algoritmi edukaks kasutamiseks vajalik arvu $n$ sellise algarvulise teguri $p$ olemasolu, mille korral arvu $(p-1)$ algarvulised tegurid oleksid "väikesed". Kasutades kordarvuteste saab triviaalselt genereerida sellise RSA moodul $n=pq$, mille faktoriseerimine $p-1$ algoritmi abil ei ole ökonoomne: tuleb leida suured algarvud $p_1$ ja $q_1$, nii et ka $p=2p_1+1$ ja $q=2p_1+1$ on algarvud.

Lenstra poolt 1980-ndatel avastatud võimsam elliptiliste kõverate algoritm on $p-1$ algoritmi üldistus. Märgime ilma antud algoritmi süvenemata, et elliptiliste kõveratel põhinev algoritm on edukas laiemal skaalal — nimelt juhul kui arvule $p$ piisavalt "lähedal" täisarvul (lähedus kõigub ja sõltub otseselt Hasse-Weili teoreemist) on ainult "väikesed" algarvulised tegurid. Kui $p-1$ meetod sõltub võrdustest rühmas $\mathbb{Z}_p$, siis Lenstra elliptiliste kõverate algoritm baseerub võrdustel rühmades $E(GF(p))$ erinevate elliptiliste kõverate puhul.