IV-1. [**kettingbreukfactorisatie**]

(i) Implementeer het *Jacobisymbool* op efficiënte wijze; dit Jacobisymbool, dat we noteren met $\left(\frac{a}{m}\right)$. geeft voor elke oneven positieve m een functie die is gedefinieerd voor $a \in \mathbf{Z}$ door

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right),$$

als $m = p_1 \cdots p_k$, met p_i priem for $1 \leq i \leq k$, waar $(\frac{a}{p})$ voor een oneven priemgetal p het *Legendresymbool* is, gegeven door

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{als } a \text{ een kwadratische niet-rest is modulo } p; \\ 1 & \text{als } a \text{ een kwadratische rest is modulo } p; \\ 0 & \text{als } a \text{ deelbaar is door } p. \end{cases}$$

Maak gebruik van het feit dat de waarde van het Legendresymbool slechts afhangt van de restklasse van a modulo p, en ook multiplicatief is in de *teller*, dus $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$; dat laatste volgt uit het feit dat kwadraatresten precies de even machten zijn van een voortbrenger van de multiplicatieve groep modulo p. Gebruik ook de kwadratische reciprociteitswet, die impliceert dat voor oneven, positieve a, b met $\text{ggd}(a, b) = 1$

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

en de aanvullingswetten, die voor oneven b geven dat:

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \quad \text{en} \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

(ii) Implementeer het factorisatiealgoritme van Shanks; hiervoor wordt voor de kettingbreuk van $\sqrt{N}$ de rij (P_n, Q_n) bepaald voor $n \geq 0$, totdat Q_n een kwadraat R^2 is voor een even n waarvoor R niet al eerder als Q_j optrad. Zoals uitgelegd in **1.2.16** geeft zo'n Q_n mogelijk een factorisatie voor N uit $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n Q_n$. Om te voorkomen dat p_n uitgerekend moet worden, wordt zodra $Q_n = R^2$ gevonden is, niet verder gegaan met $(P_n + \sqrt{N})/Q_n$ maar met $(-P_n + \sqrt{N})/R$. Het blijkt dat zodra in de daaruit volgende rij (P'_k, Q'_k) twee opeenvolgende waarden P'_k, P'_{k+1} hetzelfde zijn, Q_{k+1} of, als Q_{k+1} even is, $Q_{k+1}/2$ een factor van N is.

(iii) Implementeer het kettingbreukfactorisatiealgoritme uit Toepassing **1.2.16**. Gebruik hierbij het Jacobisymbool om in de factorbasis geen overbodige priemgetallen op te nemen.