Извлечение квадратного корня по простому модулю

Алгоритм:

`input:` $3 \leqslant p$ — простое, $1 \leqslant a < p$
`output:` $1 \leqslant x < p$ такой, что $x^2 = a$ или -1, если $\nexists x$

1. Если $a^{\frac{p-1}{2}} \neq 1$ вернуть $x = -1$
2. Пока корень не найден:
3. $\quad i$ `:= random [1..`$p-1$`]`
4. $\quad T(x)$ `:=` $(x+i)^{\frac{p-1}{2}} - 1 \mod (x^2 - a) = b \cdot x + c$ (многочлены от x)
5. $\quad$ Если $b \neq 0$, то вернуть $x = c \cdot b^{-1} = c \cdot b^{p-2}$

Доказательство корректности:

1. По простому модулю p у каждого числа от 1 до $p-1$ или нет корней, или ровно два квадратных корня.
   Пусть $a^2 = b^2 \mod p \Rightarrow (a-b)(a+b) = 0 \mod p \Rightarrow a = b \vee a = -b$
2. $\sqrt{1} \mod p = \pm 1$
3. Всего квадратов $p-1$: $1^2, 2^2, \ldots, (p-1)^2 \Rightarrow$ корней всего тоже $p-1$. У каждого числа 2 или 0 корней $\Rightarrow$ квадратный корень по модулю p существует ровно у $\frac{p-1}{2}$ чисел от 1 до $p-1$.
4. Группа ненулевых остатков по простому модулю циклична. Иначе говоря, существует первообразная, такое z: $z^0, z^1, \ldots, z^{p-2}$ — различные числа от 1 до $p-1$. Док-во существования первообразной: пусть d_a — порядок a, $d_a = x, d_b = y \Rightarrow d_{ab} = lcm(x, y)$. Если lcm всех равно t, то мы имеем уравнение $x^t = 1$ с $p-1$ решениями, значит, $t \geq p-1$
5. Для любого $x = 1 \ldots p-1 \quad \exists t$: $z^t = p$. Если t четно, то $x^{\frac{p-1}{2}} = (z^{\frac{t}{2}})^{p-1} = 1$, иначе $x^{\frac{p-1}{2}} = (z^{\frac{t-1}{2}})^{p-1} \cdot z^{\frac{p-1}{2}} = -1$ (т.к. $z^{\frac{p-1}{2}}$ — корень из 1).
6. $a^{\frac{p-1}{2}} = \sqrt{1} = \pm 1$. Пусть $\exists x$: $x^2 = a$, тогда $a^{\frac{p-1}{2}} = x^{p-1} = 1$. Таких a, что $a^{\frac{p-1}{2}} = -1$, ровно $\frac{p-1}{2}$. Квадратный корень не существует ровно для $\frac{p-1}{2}$ чисел. Значит, для всех a: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = 1$ квадратный корень существует (символ Лежандра равен 1).
7. **Самое интересное:**
   Пусть $z^2 = a \mod p$. Корнями многочлена $Q(x) = x^2 - a$ являются z и $-z$. Рассмотрим многочлен от x по модулю p: $P(x) = (x+i)^{\frac{p-1}{2}} - 1$. Корнями его являются числа вида $z - i$, где z — квадратичный вычет. Здесь i — фиксированное число (см. алгоритм). Если ровно одно из двух чисел z и $-z$ является корнем многочлена $P(x)$, то $T(x) = P(x) \mod Q(x) = x \pm z$. Если и z, и $-z$ являются корнями $P(x)$, то $T(x) = 0$. Если оба не являются, то $T(x) = \texttt{const} \neq 0$.

Оценка сложности:

1. Правильное i мы выбираем с вероятностью $\frac{1}{2}$.

2. Вычисление вероятности: $x^2 = (-x)^2 = a$, нам нужно такое i, что (символ Лежандра) $\binom{x+i}{p} \neq \binom{-x+i}{p}$. Значит, что $\binom{(x+i)/(x-i)}{p} = -1$. $\frac{x+i}{x-i} = \frac{x+j}{x-j} \Leftrightarrow (x+i)(x-j) = (x+j)(x-i) \Leftrightarrow x^2 + ix - jx - ij = x^2 - ix + jx - ij \Leftrightarrow 2ix = 2jx \Leftrightarrow i = j$, значит $i \to \binom{(x+i)/(x-i)}{p}$ — биекция для любого фиксированного x. Поскольку не вычетов ровно половина всех чисел, вероятность выбора удачного i равна $\frac{1}{2}$.
3. $T(x)$ мы вычисляем быстрым возведением в степень за $O(\log p)$.
4. b^{p-2} мы также вычисляем быстрым возведением в степень за $O(\log p)$.

Вывод: матожидание времени работы $= O(\log p)$.