23 $p \pm 1$

Задача. Бобу продолжает разрабатывать программу генерации простых чисел $p > 2^{512}$ для криптосистемы RSA. Для защиты от некоторых методов факторизации модуля RSA требуется генерировать такие p, что числа $p \pm 1$ имеют максимально большие простые делители. Пусть

$$D(p) = \frac{p-1}{q_0} + \frac{p+1}{q_1},$$

где q_0 — максимальный простой делитель $p-1$, а q_1 — максимальный простой делитель $p+1$. Какое минимальное значение может принимать $D(p)$?

Решение. Докажем, что $D(p) \geq 10$.

Справедлив один из случаев: $p \equiv 1 \pmod 6$ или $p \equiv 5 \pmod 6$.

Пусть $p \equiv 1 \pmod 6$, т. е. $p = 6k + 1$. Если $k \neq q_0$, то $D(p) > (p-1)/q_0 \geq 12$. Если же $k = q_0$, то $(p+1)/q_1 \geq 4$. Действительно,

1) если $p + 1 = 2q_1$, то $q_1 = 1 + 3q_0$ — четное, противоречие;

2) если $p + 1 = 3q_1$, то $3(q_1 - 2q_0) = 2$, снова противоречие.

В целом, при $k = q_0$ справедлива оценка $D(p) \geq 6 + 4 = 10$.

Случай $p \equiv 5 \pmod 6$ рассматривается аналогично. □