Вычисление коэффициентов k-арной редукции с помощью расширенного k-арного алгоритма

Еникеев Разиль Радиович

Старший преподаватель

Институт вычислительной математики и информационных технологий

Казанский (Приволжский) федеральный университет, Казань, Россия

E-mail: renikeev@kpfu.ru

Научный руководитель *— Ишмухаметов Шамиль Талгатович*

Вычисление наибольшего общего делителя (НОД) применяется в методах факторизации, компьютерной арифметики и в криптографических алгоритмах [2].

Алгоритм Евклида на каждой итерации вычисляет остаток от деления, поэтому применение этого метода для длинных чисел не эффективно ввиду вычислительной затратности операции деления. Для преодоления этой проблемы были разработаны различные методы поиска НОД. Одним из таких является k-арный алгоритм, разработанный Соренсоном (Sorenson). В этом методе выбирается $k > 1$, обычно для ускорения алгоритма в качестве k используется $k = 2^{2m}$. Для вычисления НОД чисел u, v применяется k-арная редукция: вычисляются значения a, b (коэффициенты редукции), удовлетворяющие двум условиям $au + bv \equiv 0 \pmod{k}$ и $a, |b| < \sqrt{k}$. Далее вычисляем $t = |au + bv| / k$ благодаря выполненному первому условию, где новое значение удовлетворяет неравенству $t < 2u/\sqrt{k}$ ввиду второго. Соренсон для нахождения коэффициентов a, b предлагал применять предвычисленные таблицы, что ограничивало максимальное значение k. Джебелеан (Jebelean) и Вебер (Weber) независимо друг от друга предложили вычислять коэффициенты с помощью расширенного алгоритма Евклида, что позволило использовать большие значения k.

В данной работе предлагается способ вычисления коэффициентов k-арной редукции с помощью расширенного k-арного алгоритма (РКА), что во время их вычисления позволяет избавиться от операций деления.

РКА вычисляет коэффициенты Безу x, y, удовлетворяющие соотношению $ux + by = \text{НОД}(u, v)$. Для предлагаемого в работе алгоритма подходит только метод, выполняющийся за один проход и описанный в [1]. Пусть $u_1 = u$, $u_2 = v$, $x_1 = 1$, $x_2 = 0$, $y_1 = 0$, $y_2 = 1$,

тогда выполняются равенства

$$u_1 = ux_1 + vy_1,$$
$$u_2 = ux_2 + vy_2.$$

Пусть $u_i = (a_i u_{i-2} + b_i u_{i-1})/k$ — результат редукции на i-й итерации. Тогда удовлетворяющие условию $u_i = ux_i + vy_i$ коэффициенты можно вычислить с помощью формул $x_i = (a_i x_{i-2} + b_i x_{i-1})/k$ и $y_i = (a_i y_{i-2} + b_i y_{i-1})/k$.

Для $x_3 = a_3/k$, $y_3 = b_3/k$ имеем

$$u_3 = ux_3 + vy_3 = (ua_3 + vb_3)/k,$$

то есть получаем, что числители x_3 и y_3 являются коэффициентами редукции. Коэффициенты $x_4 = (a_4 x_2 + b_4 x_3)/k = b_4 a_3/k^2$, $y_4 = (a_4 y_2 + b_4 y_3)/k = (a_4 + b_4 b_3/k)/k = (a_4 k + b_4 b_3)/k^2$. Обозначим числители в x_i и y_i как x'_i и y'_i соответственно, тогда выполняется равенство

$$u_4 = (ux'_4 + vy'_4)/k^2.$$

Получаем, что x'_4 и y'_4 являются коэффициентами редукции для u, v при $k' = k^2$ (k' используется для избегания двусмысленности). Продолжим подобные рассуждения и получим, что $u_i = (ux'_i + vy'_i)/k^{i-2}$. Таким образом, получаем алгоритм вычисления коэффициентов редукции через РКА. Коэффициенты же a_i и b_i можно вычислить с помощью предвычисленных таблиц, как первоначально предлагалось Соренсоном.

Преимуществом предложенного алгоритма является отсутствие операций деления в алгоритме.

Литература

1. Еникеев Р. Р. Нахождение коэффициентов Безу с помощью расширенного обобщенного бинарного алгоритма // Материалы XVI Международной конференции имени А.Ф. Терпугова, 2017. - С. 284-291.
2. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел. Казань: Казанский университет, 2011.