Общероссийский математический портал

Аль Халиди Аркан Мохаммед, Ш. Т. Ишмухаметов, Эффективное программирование процедуры вычисления НОД натуральных чисел, *Изв. вузов. Матем.*, 2020, номер 6, 3–8

DOI: <https://doi.org/10.26907/0021-3446-2020-6-3-8>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.23.180.231

26 апреля 2023 г., 12:43:18

АЛЬ ХАЛИДИ АРКАН МОХАММЕД, Ш.Т. ИШМУХАМЕТОВ

ЭФФЕКТИВНОЕ ПРОГРАММИРОВАНИЕ ПРОЦЕДУРЫ ВЫЧИСЛЕНИЯ НОД НАТУРАЛЬНЫХ ЧИСЕЛ

Аннотация. Изучается проблема ускорения вычисления наибольшего общего делителя натуральных чисел на основе аппроксимирующего k -арного алгоритма. Предложена схема реализации аппроксимирующего алгоритма, обеспечивающая значение коэффициента редукции рассматриваемых чисел A_i/B_i не меньше k , где $k = 2^s$ — регулируемый параметр вычисления, не превышающий размер машинного слова. Такой подход обеспечивает значительное преимущество нашего алгоритма по отношению к классическому алгоритму Евклида.

Ключевые слова: наибольший общий делитель, алгоритм Евклида, k -арный алгоритм, аппроксимирующий k -арный алгоритм.

УДК: 511.1

DOI: 10.26907/0021-3446-2020-6-3-8

Введение. Классический алгоритм Евклида используется для вычисления наибольшего общего делителя (НОД) пары заданных натуральных чисел A и B . Этот алгоритм является составной частью многих теоретико-числовых и криптографических алгоритмов. В частности, он используется в вычислениях в конечных полях и имеет важное приложение в современных системах типа Блокчейн [1]. Этот алгоритм работает с использованием рекуррентного соотношения $\text{НОД}(A; B) = \text{НОД}(B; A \bmod B)$. Это соотношение используется многократно до тех пор, пока остаток $A \bmod B$ не станет равным нулю, тогда аргумент B будет равен искомому НОД исходной пары натуральных чисел.

k -арный алгоритм Евклида был разработан в 1990 году Дж. Соренсоном ([2], [3]) и улучшен независимо друг от друга К. Вебером [4] и Т. Джебелеаном [5] в 1993 и 1995 годах. В основе этого алгоритма лежит теорема, доказанная Дж. Соренсоном. Пусть $\lceil r \rceil$ обозначает ближайшее целое число к числу r , полученное округлением вверх.

Теорема. Пусть целые числа $A > B > 0$ заданы, и k — положительное натуральное число, взаимно простое с A и B . Существуют целые числа x, y , удовлетворяющие соотношению $1 \leq x \leq \lceil \sqrt{k} \rceil, |y| \leq \lceil \sqrt{k} \rceil$ такие, что

$$Ax + By \equiv 0 \pmod{k}. \quad (1)$$

Полагая $C = (Ax + By)/k$, получим новую пару $(B; C)$, имеющую такой же НОД, что и $\text{НОД}(A; B)$, либо НОД, кратный $\text{НОД}(A; B)$. Посторонние множители, появляющиеся в

Поступила в редакцию 09.07.2019, после доработки 20.09.2019. Принята к публикации 25.09.2019.

Благодарности. Работа выполнена в рамках реализации программы развития Научно-образовательного математического центра Приволжского федерального округа, соглашение № 075-02-2020-1478.

НОД($B; C$) должны быть изъяты на последней стадии алгоритма путем дополнительного вычисления НОД исходных A и B с НОД, полученным как выход k -арного алгоритма.

Вычислив $C = (Ax + By)/k$, мы должны проверить условие $d = \text{НОД}(C; k) = 1$, и если оно не выполняется, поделим C на d .

Отметим, что уравнение $Ax + By \equiv 0 \pmod k$ эквивалентно уравнению $y \equiv -qx \pmod k$, где $q = AB^{-1} \pmod k$. Искомую пару x, y можно найти, перебирая значения x от 1 до $\lceil \sqrt{k} \rceil$ и вычисляя два значения $y \equiv -qx \pmod k$, принадлежащие интервалу $[-\lceil \sqrt{k} \rceil; \lceil \sqrt{k} \rceil]$. На следующей итерации рассматривается новая пара $(B; C)$. Более подробное описание k -арного алгоритма дано в основной работе Дж. Соренсона [3]. В статье [6] рассмотрен расширенный k -арный алгоритм, предназначенный для решения уравнения Безу и вычисления обратных по модулю элементов.

1. Аппроксимирующий k -арный алгоритм. В работе [7] и статье [8] Ш. Ишмухаметовым и Р. Рубцовой был разработан аппроксимирующий k -арный алгоритм, главное отличие которого состоит в том, что коэффициенты x и y ищутся не в интервале $[-\sqrt{k}; \sqrt{k}]$ как в алгоритме Соренсона, а значение x выбирается из интервала $[1; k]$, а y вычисляется так, чтобы обеспечить наилучшее приближение $Ax \approx -By$. Такой подход обеспечивает взаимное сокращение слагаемых в сумму $Ax + By$ и наименьшее возможное значение $|C| = (Ax + By)/k$, что уменьшает общее число итераций, оставляя общие расходы на вычисления в ходе одной итерации примерно равными классической схеме алгоритма Соренсона.

Дадим подробное теоретическое описание аппроксимирующего алгоритма и выполним его анализ. Отметим в первую очередь выбор параметра k . Его значение может быть выбрано произвольным, но, исходя из представления целых чисел, в компьютере лучше это значение выбрать равным степени двойки, тогда операции проверки чисел на четность, сокращение на k , деление на 2 будут выполняться эффективнее, чем при любых других значениях k . Выберем поэтому k равным небольшой степени двойки: $k = 2^s$.

На каждом шаге аппроксимирующего алгоритма на вход подаются нечетные натуральные числа A и B , вычисляется пара значений x и y такие, что выполняется формула (1) и вычисляется $C = (Ax + By)/k$. После этого проверяют, не равно ли C единице или нулю, и если нет, то переходят к новой итерации с парой (B, C) .

Главное отличие аппроксимирующего алгоритма от k -арного алгоритма Соренсона заключается в выборе целых чисел x и y . Рассмотрим процедуру поиска пары x и y более подробно.

2. Поиск пары (x, y) в аппроксимирующем k -арном алгоритме. Через r обозначим дробь A/B , а через q — положительное значение $AB^{-1} \pmod k$. Практическое вычисление параметра q выполняется как вычисление остатков $a = A \pmod k$, $b = B \pmod k$, обратного по модулю k элемента $b^{-1} \pmod k$, и вычисление произведения $ab^{-1} \pmod k$. Поскольку параметр k представляет собой степень двойки, вычисление a и b — это просто отделение от конца чисел A и B s разрядов в их бинарном представлении, где $k = 2^s$, поэтому самой накладной здесь является операция вычисления обратного по модулю 2^s элемента. Для ускорения можно использовать заранее вычисленные таблицы обратных элементов по модулю k . Если значение k слишком велико, то можно хранить таблицы по модулю меньшего значения 2^t , $t < s$, и найти значения обратных элементов по большему модулю с помощью подъема Гензеля. Эта процедура подробно описана в [6].

Из условия (1) получим $y \equiv -qx \pmod k$ или $y = -qx + ks$ для $s \in \mathbf{Z}$. Тогда

$$C = \left\lfloor \frac{Ax + By}{k} \right\rfloor = B \left\lfloor \frac{(A/B)x + y}{k} \right\rfloor = B \left\lfloor \frac{rx + (-qx + ks)}{k} \right\rfloor = B \left\lfloor \frac{(r - q)x}{k} + s \right\rfloor.$$

Обозначим через α' дробь $(r - q)/k$, и пусть $\alpha' = \alpha + ss$, где ss – ближайшее к α' целое число, $|\alpha| \leq 0.5$. Тогда

$$C = B|(\alpha + ss)x + s|. \quad (2)$$

Подберем подходящие x , $1 \leq x < k$, и $s \in \mathbf{Z}$ так, чтобы C в (2) приняло наименьшее значение. Для решения этой задачи будем использовать две возможные стратегии. Первая стратегия разработана в работе [8] и заключается в следующем.

Ищем правильную рациональную дробь m/n , аппроксимирующую модуль α :

$$m/n \approx |\alpha|, \text{ или } |\alpha| = m/n \pm \varepsilon,$$

для небольшого положительного ε . Накладываем ограничение на знаменатель дроби m/n не превышать k . Предположим, что $\alpha > 0$ (случай $\alpha < 0$ рассматривается аналогично). Тогда

$$C = B|(m/n \pm \varepsilon + ss)x + s|.$$

Полагая значение x равным n и $s = -m - ss \cdot n$, получим

$$C = B|\varepsilon n|.$$

Назовем соотношение B/C коэффициентом редукции и обозначим его буквой ρ_1 . Очевидно, чем больше ρ_1 , тем лучше сходимость алгоритма. По определению

$$\rho_1(A, B) = \frac{1}{\varepsilon n}. \quad (3)$$

Значение ε — это точность аппроксимации α рациональной дробью m/n . В статье [8] показано, что в классе рациональных дробей со знаменателем, ограниченным k , наилучшая дробь обеспечивает редукцию $\rho_1(A, B) > 2k/3$ при $|\alpha| > 1/k$. Здесь мы улучшим эту оценку.

3. Построение наилучшего приближения для действительного α . Наилучшее приближение обеспечивается использованием дробей Фарея. Дадим необходимые определения.

Определение 1. Пусть задана константа $C > 0$. Дробями Фарея называется совокупность правильных рациональных дробей со знаменателем, ограниченным C .

Определение 2. Пусть даны две рациональные дроби: $r_1 = m_1/n_1$ и $r_2 = m_2/n_2$. Медианой этих дробей называется дробь r , равная $(m_1 + m_2)/(n_1 + n_2)$. Медиана r удовлетворяет условию $r_1 < r < r_2$.

Пусть выбрана константа $k > 1$ и задано действительное число $\alpha \in (0; 1/2)$. Будем строить правильную дробь со знаменателем, меньшим k , обеспечивающей наилучшее приближение α . Предположим, что $\alpha > 1/(k - 1)$.

В качестве первого приближения возьмем пару соседних дробей вида $(1/(n + 1); 1/n)$, содержащую α . Сделаем индукционное предположение о том, что на шаге $i \geq 1$ найдены две правильные дроби:

$$r_1 = \frac{m_1}{n_1} < \alpha < r_2 = \frac{m_2}{n_2}.$$

Проверим условие $n_1 + n_2 \geq k$. Если оно выполнено, то завершаем вычисление, выбрав в качестве решения одну из дробей m_1/n_1 или m_2/n_2 .

Иначе, построим медиану $r = (m_1 + m_2)/(n_1 + n_2)$. Проверим условие $r \leq \alpha$. Если оно выполнено, то переходим к новому интервалу $(r_1; r)$, содержащему α . Иначе, перейдем к интервалу $(r; r_2)$. Переходим к шагу $i + 1$.

Процесс конечен, так как на каждой итерации происходит увеличение знаменателя одной из ограничивающих дробей.

Приведем пример построения дроби Фарея для $\alpha = 0.278$:

$$\alpha \in \left(\frac{1}{4}; \frac{1}{3}\right) \rightarrow \left(\frac{1}{4}; \frac{2}{7}\right) \rightarrow \left(\frac{3}{11}; \frac{2}{7}\right) = (0.272; 0.286).$$

Процедура заканчивается на третьем шаге, поскольку следующая медиана имеет знаменатель $n = 11 + 7 = 18 > k$. Наилучшим приближением для $\alpha = 0.278$ является дробь $3/11$, поскольку расстояние от левой границы до α равно примерно 0.006, а от α до правой границы равно 0.08. Однако с точки зрения производительности алгоритма такой выбор будет неверным. Действительно, коэффициент ρ_1 определен в (3), как величина обратная произведению расстояния на значение знаменателя. Для левой дроби $3/11$ это значение равно $1/(0.006 \cdot 11) \approx 15.2$. Для правой дроби $2/7$ значение $\rho_1 = 1/(0.008 \cdot 7) \approx 17.9$, значит, выбор правой границы является более эффективным.

Найдем теоретическую границу между двумя дробями, для которой значение коэффициента ρ_1 одинаково для левой и правой границ:

$$\left(\alpha - \frac{m_1}{n_1}\right) n_1 = \left(\frac{m_2}{n_2} - \alpha\right) n_2, \text{ или } n_1\alpha - m_1 = m_2 - \alpha n_2 \rightarrow \alpha = \frac{m_1 + m_2}{n_1 + n_2}.$$

Значит, точка равновесия между двумя дробями, на которой значения коэффициента редукции совпадают, равна медиане граничных точек. Оценим наименьшее (наихудшее) значение коэффициента редукции $\rho_1(\alpha)$ на интервале $(1/(k-1); 1/2)$. Предположим, что значение α находится между двумя соседними дробями m_1/n_1 и m_2/n_2 такими, что $n_1 + n_2 \geq k$.

Лемма 1. *Расстояние между соседними дробями Фарея m_1/n_1 и m_2/n_2 равно $1/(n_1 + n_2)$.*

Доказательство. Покажем по индукции, что на любом шаге построения приближения к числу α соседние дроби удовлетворяют условию леммы. Действительно, на первом шаге процедуры соседние дроби имеют вид $(1/(n+1); 1/n)$ и разность между ними равна $1/(n(n+1))$.

Предположим, что на шаге i соседние дроби m_1/n_1 и m_2/n_2 , содержавшие α , удовлетворяют условию леммы, т. е. выполняется $m_1n_2 - m_2n_1 = 1$. Следующий интервал, содержащий α , имеет вид $(m_1/n_1; (m_1 + m_2)/(n_1 + n_2))$ или $((m_1 + m_2)/(n_1 + n_2); m_2/n_2)$. Тогда

$$\frac{m_1 + m_2}{n_1 + n_2} - \frac{m_1}{n_1} = \frac{m_1n_1 + m_2n_1 - m_1n_1 - m_1n_2}{n_1(n_1 + n_2)} = \frac{1}{n_1(n_1 + n_2)}.$$

Аналогично, для правого интервала. □

Лемма 2. *Значение коэффициента редукции при приближении α , удовлетворяющего условию $|\alpha| \geq 1/k$ дробями Фарея со знаменателем, ограниченными $k-1$, больше или равно k .*

Доказательство. Точка равновесия между дробями m_1/n_1 и m_2/n_2 равна медиане r этих дробей. В наихудшем случае значение α совпадает с этой медианой и расстояние от нее до границ интервала равно согласно лемме 1 $d_1 = 1/n_1(n_1 + n_2)$ и $d_2 = 1/n_2(n_1 + n_2)$ соответственно. Соответствующие значения коэффициента редукции равны между собой:

$$\rho_1(\alpha) = 1/(n_1d_1) = 1/(n_2d_2) = n_1 + n_2 \geq k.$$

Последнее неравенство вытекает из того факта, что дроби m_1/n_1 и m_2/n_2 являются конечными в процедуре построения дробей Фарея, поэтому сумма их знаменателей больше или равна k . В частности, при $\alpha = 1/k$ значение $\rho_1(\alpha)$ равно k . □

При значениях $|\alpha| < 1/k$ ближайшей к $|\alpha|$ дробью Фарея будет дробь $1/(k-1)$, тогда, в наихудшем случае, когда $\alpha \approx 0$, расстояние до $1/(k-1)$ приближается к $1/(k-1)$, и

значение $\rho_1(\alpha)$ окажется близким к 1, что означает плохую сходимость алгоритма на этой итерации.

Чтобы сгладить негативные последствия подобных случаев, определим стратегию 2.

4. Стратегия вычисления C при малых значениях $|\alpha|$. При малых значениях $|\alpha|$ стратегия 1 дает сбой, ухудшающий эффективность аппроксимирующего алгоритма, поэтому будем здесь использовать стратегию 2. Теперь мы не станем выполнять аппроксимацию α дробью m/n , а определим $x = 1$, $s = -ss$, $y = -q - ss \cdot k$, тогда $C = B|\alpha|$, и коэффициент редукции $\rho_2(\alpha) = B/C$ примет значение

$$\rho_2(\alpha) = \frac{1}{|\alpha|}.$$

При уменьшении $|\alpha|$ значение $\rho_2(\alpha)$ увеличивается, а значение $\rho_1(\alpha)$ уменьшается. Найдем точку равновесия, когда эти значения совпадают (для простоты предположим, что $\alpha > 0$). Учтем, что при $\alpha < 1/(k-1)$ $\varepsilon = 1/(k-1) - \alpha$ и $m/n = 1/(k-1)$:

$$\rho_1(A, B) = \rho_2(A, B) \rightarrow \varepsilon n = \alpha \rightarrow (1/(k-1) - \alpha)(k-1) = \alpha,$$

откуда $\alpha = 1/k$. Значит, стратегия 2 дает лучшую сходимость при $|\alpha| < 1/k$. При $|\alpha| = 1/k$ обе стратегии дают одинаковое значение коэффициента редукции $\rho(A, B) = k$.

5. Заключение. Нами разработана схема реализации аппроксимирующего k -арного алгоритма, позволяющая обеспечивать значение коэффициента редукции A_i/B_i на шаге алгоритма, не меньше k , где $k = 2^s$ — регулируемый параметр алгоритма, не превышающий размер машинного слова. Это позволяет достигнуть эффективность алгоритма вычисления наибольшего общего делителя пар натуральных чисел, многократно превышающую эффективность стандартного алгоритма Евклида вычисления НОД, для которого среднее значение коэффициента редукции находится в интервале от 2 до 3.

ЛИТЕРАТУРА

- [1] Latypov R., Stolov E., Ishmukhametov S., Vlasov I., Galiev A., Prokopyev N. ARCHAIN: A Novel Blockchain Based Archival System//2-d World Conf. on Smart Trends in Systems. Security and Sustainability, October 2018, London, UK.
- [2] Sorenson J. *The k-ary GCD Algorithm*, Univ. Wisconsin-Madison, Techn. Report, 1–20 (1990).
- [3] Sorrenson J. *Two fast GCD Algorithms*, J.Alg. **16** (1), 110–144 (1994).
- [4] Weber K. *The accelerated integer GCD algorithm*, ACM Trans. Math. Software, **21** (1), 1–12 (1995).
- [5] Jebelean T. *A Generalization of the Binary GCD Algorithm*, Proc. of Intern. Symp. on Symb. and Algebr. Comp. (ISSAC'93), 111–116 (1993).
- [6] Ишмухаметов Ш.Т., Мубараков Б.Г., Аль-Анни Маад Камаль, *Вычисление коэффициентов Безу для k-арного алгоритма нахождения НОД*, Изв. вузов. Матем., №11, 30–38 (2017).
- [7] Ishmukhametov S.T., Rubtsova R.G. *A fast algorithm for counting GCD of natural numbers*, Proc. of intern.conf. Algebra, Anal. and Geometry, Kazan, KFU (2016).
- [8] Ishmukhametov S.T. *An approximating k-ary GCD Algorithm*, Lobachevskii J. Math., **37** (6), 722–728 (2016).

Аркан Мохаммед Аль Халиди

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: Arkan3538@gmail.com

Шамиль Талгатович Ишмухаметов

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: Shamil.Ishmukhametov@kpfu.ru

Al Halidi Arkan Mohammed and Sh.T. Ishmukhametov

An effective programming of GCD Algorithms for natural numbers

Abstract. We study the problem of acceleration of GCD algorithms for natural numbers based on the approximating k -ary algorithm. We suggest a new scheme of the algorithm implementation ensuring the value of the reduction coefficient $\rho = A_i/B_i$ at a stage of the procedure equal or exceeding k where k is a regulating parameter of computation not exceeding the size a computer word. This ensures a significant advantage of our algorithm against the classical Euclidean algorithm.

Keywords: greatest common divisor, Euclidian GCD Algorithm, k -ary Algorithm, approximating k -ary Algorithm.

Arkan Mohammed Al Halidi

*Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,*

e-mail: Arkan3538@gmail.com

Shamil' Talgatovich Ishmukhametov

*Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,*

e-mail: Shamil.Ishmukhametov@kpfu.ru