Секция «Математическая логика, алгебра и теория чисел»

Об одном способе выбора коэффициентов в обобщенном бинарном алгоритме вычисления НОД и некоторых вероятностях сокращения

Научный руководитель – Ишмухаметов Шамиль Талгатович

Долгов Дмитрий Александрович
Аспирант
Казанский (Приволжский) федеральный университет, Институт вычислительной математики и информационных технологий, Казань, Россия
E-mail: DADolgoff@yandex.ru

Наибольший общий делитель (НОД, gcd) - базовая операция во многих криптографических алгоритмах. K-арный алгоритм [2,3] - один из наиболее быстрых алгоритмов вычисления НОД. Пусть $A > B > 0$ - 2 нечетных натуральных числа. Необходимо найти коэффициенты x, y, такие что выполняется $xA + yB = 0\ (mod\ k)$ для некоторого фиксированного целого k: $gcd(A, B) = gcd(B, |(xA + yB)/k|)$. Мы выбираем $k = 2^s$, получая обобщеннный бинарный алгоритм.

В [1] был предложен новый способ выбора коэффициентов x, y для обобщенного бинарного алгоритма, рассматриваемый в рамках статьи. Рассмотрим 1 итерацию, проанализировав сокращение A/C, где $C = (x * A + y * B)/2^s$.

Пусть X, Y - целочисленные дискретные случайные величины. $X, Y \in [2^n, 2^{n+1}]$, $n \in N$. Рассмотрим нечетную реализацию случайных величин X, Y. Пусть $\xi = max(X, Y),\ \nu = min(X, Y)$. Реализации ξ, ν представим в двоичном виде. На t позиции стоит 1 из 4 вариатов: $00, 01, 10$ или 11. $\#(\xi, \nu) = 2^{n-2} * (2^{n-1} - 1)$. $R_{i,j} = (\xi * \nu_t - \nu * \xi_t)/2^w$, $w \geq t$, на t позиции стоят i, j. R_{11L} - максимальное сокращение для бинарного алгоритма $\xi/((\xi - \nu)/2^v)$, $v \geq 1$.

Оценим вероятность, что бинарный алгоритм НОД имеет наибольшее сокращение для 2 n битных чисел. 10 обязательно встретиться в двоичном разложении нечетных реализаций ξ, ν. Если в разложении есть только 10, и 11 не лежит нигде кроме последнего разряда, то обозначим так: $\overline{000\overline{1}}10\overline{11}$. Исследование вероятностей позволит выявить классы чисел, на которых бинарный алгоритм дает наибольшее сокращение по сравнению с обобщенным бинарным алгоритмом.

Теорема 1.
$P((\frac{\xi}{R_{11L}} \geq \frac{\xi}{|R_{10}|}) \cap \overline{000\overline{1}}10\overline{11}) = 0,\ n \geq 5.$

Теорема 2.
$P(((\frac{\xi}{R_{11L}} \geq \frac{\xi}{|R_{10}|}) \cap (\frac{\xi}{R_{11L}} \geq \frac{\xi}{|R_{00}|})) \cap 00\overline{0\overline{1}}10\overline{11}) < \frac{1}{2^{n-2}},\ n > 3.$

Источники и литература

1) Dolgov D. GCD calculation in the search task of pseudoprime and strong pseudoprime numbers // Lobachevskii Journal of Mathematics, 37. 2016. No 1. pp. 733-738.
2) Sorrenson J. Two fast GCD Algorithms // J.Alg., 16. 1994. No 1. pp.110-144.
3) Weber K. The accelerated integer GCD algorithm // ACM Transacations of Math.Software, 21. 1995. No 1. pp. 1-12.