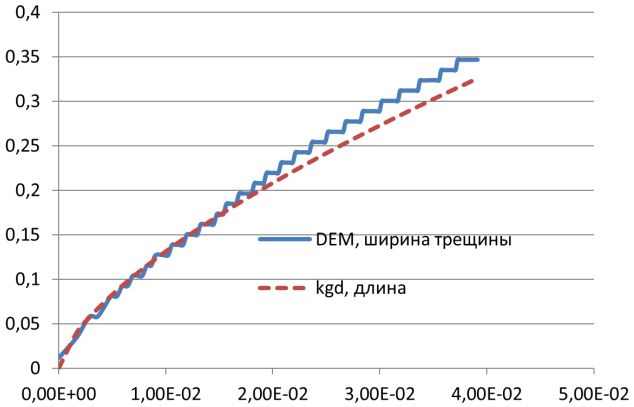

Рисунок 6 – Сравнение полудлины трещины, полученной численным решением DEM и моделью KGD

Заключение. В данной статье рассматривается алгоритм расчета геометрических параметров плоских гидравлических трещин основанный на основе сопряженной дискретно-элементной модели. Разработанная модель включает три компоненты для моделирования различных физических процессов, возникающих при ГРП, а также методику их сопряжения. Дискретно-элементная структура модели позволяет естественно включать возможность формирования трещин, осуществления течения жидкости по сети трещин и фильтрации через поры, с учетом напряженно-деформированного состояния пласта. Разработанная модель ориентирована на реализацию на системах массово-параллельной архитектуры, в том числе с использованием технологии GPGPU. Проведено сравнение геометрических параметров трещин, получаемых DEM-решателем и моделью KGD.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Fu, P. An explicitly coupled hydro-geomechanical model for simulating hydraulic fracturing in arbitrary discrete fracture networks / P. Fu, S. Johnson, C. Carrigan // International Journal for Numerical and Analytical Methods in Geomechanics. – 2012. – Vol. 37 – Is. 14 – P. 2278–2300.
2. Fu, P. Generalized displacement correlation method for estimating stress intensity factors / P. Fu, S. Johnson, R. Settgast, C. Carrigan // Engineering Fracture Mechanics – Vol. 88 – July 2012 – P. 90–107.
3. Gao, H. Numerical simulation of crack growth in an isotropic solid with randomized internal cohesive bonds / H. Gao, P. Klein // Journal of the Mechanics and Physics of Solids – Vol. 46 – Is. 2 – 1998 – P. 187–218.
4. Zhang, Z. A new quasi-continuum constitutive model for crack growth in an isotropic solid / Z. Zhang, X. Ge // European Journal of Mechanics - A/Solids – Vol. 24 – Is. 2 – 2005 – P. 243–252.
5. Zhao, G. Development of Micro-Macro Continuum-Discontinuum Coupled Numerical Method // Thesis, Ecole Polytechnique Fédérale de Lausanne – 2010.
6. Wang, S. Fully Coupled Thermal-Hydraulic-Mechanical Reservoir Simulation with Non-Isothermal Multiphase Compositional Modeling / S. Wang, J. Zhang, Z. Yang, C. Yin, Y. Wang, R. Zhang, Y. Wu // Society of Petroleum Engineers – SPE Reservoir Simulation Conference – 2017.
7. Sarmadivaleh, M. Numerical and experimental investigation of the interaction of natural and propagated hydraulic fracture / H. Fatahi, M. Hossain, M. Sarmadivaleh // Journal of Natural Gas Science and Engineering – Vol. 37 – 2017 – P. 409–424.
8. Экономидес, М. Унифицированный дизайн гидроразрыва пласта: от теории к практике / М. Экономидес, Р. Олни, П. Валько – Москва : Орса Пресс, 2004.

Материал поступил в редакцию 14.01.2018

KRASNOPROSHIN V.V., KONOVALOV O.L., CHAIKO V.V. Algorithm for calculating the geometric parameters of flat hydraulically induced fractures

This paper investigates the algorithm for calculating the geometry of flat fractures propagating under the pressure of pumping fluid. The conjugate discrete-element model and the corresponding numerical scheme are introduced. The comparison of the geometric parameters of the fractures obtained by numerical modeling and analytical model KGD is made.

УДК 581.3

Ивасьев С.В.

МЕТОД ВЫСОКОВЕРОЯТНОСТНОГО ОПРЕДЕЛЕНИЯ ПРОСТЫХ МНОГОРАЗРЯДНЫХ ЧИСЕЛ НА ОСНОВЕ ВЕКТОРНО-МОДУЛЬНОГО УМНОЖЕНИЯ

Введение. Проблема принадлежности заданного натурального числа к классу простых или составных чисел является актуальной не только в математике, но и в компьютерных науках. Отличить простое число от составного, а также разложить последнее на простые множители, является одной из важнейших задач арифметики. Поиск больших простых чисел, например, необходим для обеспечения надежности систем шифрования информации с открытым ключом. Безопасность последних базируется на утверждении, что операция умножения двух больших простых чисел является односторонней функцией.

На сегодняшнее время проверка простоты числа осуществляется на основе вероятностных тестов Ферма, Соловей-Штрассена, Миллера-Рабина, которые отличаются большой вычислительной сложностью.

Обзор известных решений проверки чисел на простоту. Основной идеей теста Ферма проверки на простоту является использование теоремы Ферма, согласно которой, если n – простое, то для произвольного a, $1 \le a \le n - 1$ имеет место равенство $a^{n-1} \equiv 1 \pmod{n}$, иначе n не является простым [1].

В тесте на простоту Соловей-Штрассена используется критерий Эйлера: если n – простое, то $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ для всех значений a, которые взаимно простые с n. Следует отметить, что в данном подходе нужно проверять, будет ли $\left(\frac{a}{n}\right)$ квадратичным остатком, то есть вычислять символ Якоби [1], что приводит к временной сложности $O(n \cdot \log_2^2 n)$.

Тест Миллера-Рабина наиболее часто используется на практике и называется сильным тестом на простоту. Он базируется на следующем факте. Пусть n – нечетное простое число, причем $n - 1 = 2^s r$, где r – нечетное, s – некоторое натуральное число, a – натуральное число, взаимно простое с n, то есть НОД(a,n)=1. Тогда имеет место одно из равенств: $a^r \equiv 1 \pmod{n}$, или $a^{2^j r} \equiv -1 \pmod{n}$ для некоторого j, $0 \le j \le s - 1$ [2]. Учитывая, что в данном методе

Ивасьев Степан Владимирович, *к.т.н., старший преподаватель кафедры кибербезопасности Тернопольского национального экономического университета, E-mail: stepan.ivasiev@gmail.com*
Украина, ТНЭУ, 46000, г. Тернополь, ул. Львовская, 11.

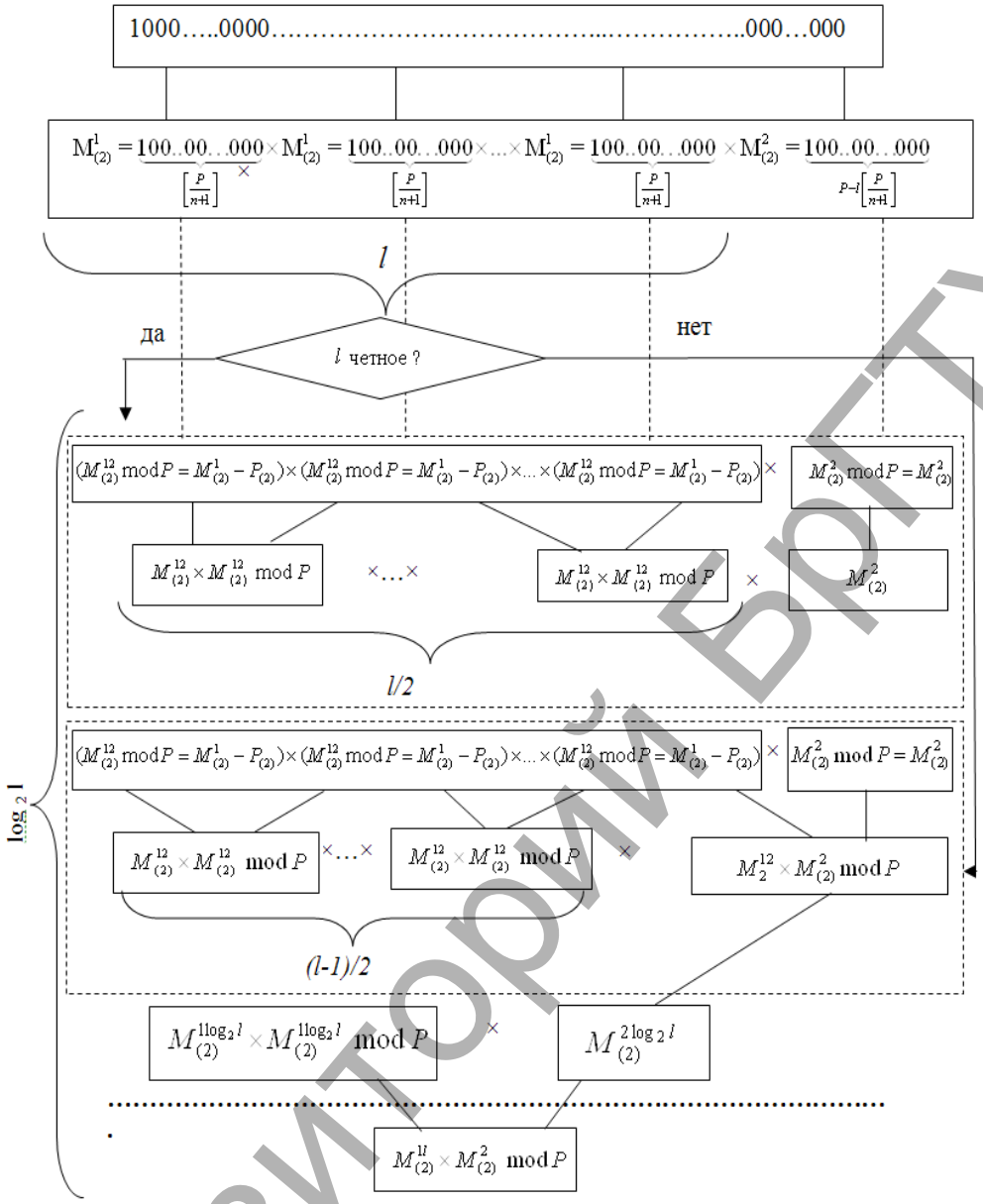

Рисунок 1 – Схема проверки многоразрядных чисел на простоту

используются операции модулярного экспоненциирования, это также приводит к значительной временной сложности.

Самый простой метод установления простоты числа был известен еще в древности и называется он решетом Эратосфена. Для реализации его нужно выписать в ряд числа от 2 до n. Первое число в ряду является простым. Из ряда вычеркиваются числа, которые кратным 2. Далее надо взять второе число, стоящее в ряду, и вычеркнуть все числа, кратные ему. И так далее нужно брать i-е число и вычеркивать кратные ему числа, пока не будет выполняться неравенство $i < \sqrt{n}$. Числа, которые останутся в ряду после операций вычеркивания, являются простыми.

Этот метод эффективен, если число n невелико (n<10.000.000.000). При этом его можно использовать не только для тестирования на простоту, но и для поиска простых чисел в указанном интервале, а также для решения задачи факторизации.

Метод проверки на простоту по использованию векторно-модульного алгоритма модулярного умножения в системе остаточных классов. Разработанный метод проверки чисел большой разрядности (ЧБР) на простоту основывается на фундаментальной математической основе малой теоремы Ферма и разработанного в [3] векторно-модульного алгоритма умножения в системе остаточных классов (СОК).

Пусть n – разрядное число P необходимо проверить на простоту. Для этого, согласно частному случаю теоремы Ферма, должно выполняться следующее соотношение:

$$m=2^P \bmod p=2. \quad (1)$$

Введем обозначение: $2^p = M_{(2)}$ и представим его в таком виде:

$$\underbrace{M(2)=100000\ldots00}_{P\text{- разрядов}}. \quad (2)$$

Соответственно, $p=\sum_{i=0}^{n-1} p_i 2^i$, где p_i=0,1, причем p>>n. Далее $M_{(2)}$ раскладывается в произведение двоичных чисел:

$$M(2)=\underbrace{100..00..00}_{\left[\frac{P}{n+1}\right]}\cdot\underbrace{100..00..00}_{\left[\frac{P}{n+1}\right]}\cdot\ldots\cdot\underbrace{100..00..00}_{\left[\frac{P}{n+1}\right]}\cdot\underbrace{100..00..00}_{P-l\left[\frac{P}{n+1}\right]}. \quad (3)$$

В (3) $l=\left\lceil \frac{p}{n+1} \right\rceil$ – количество одинаковых множителей в разложении $M_{(2)}$ с разрядностью n+1.

Для модулярного экспоненциирования $2^p \bmod p$ с использованием метода, предложенного в [3], вычисляются остатки каждого из множителей уравнения (3) путем вычитания, то есть:

$$M_{(2)}^{12}=\underbrace{100..00\ldots000}_{\left[\frac{P}{n+1}\right]}-P_{(2)}; \quad (4)$$

$$M_{(2)}^{12}=\underbrace{100..00\ldots000}_{P-l\left[\frac{P}{n+1}\right]}-P_{(2)}=\underbrace{100..00\ldots000}_{P-l\left[\frac{P}{n+1}\right]}, \quad (5)$$

где $P_{(2)}$ – двоичное представление числа p.

В результате получается l остатков $M_{(2)}^{12}$ и 1 остаток $M_{(2)}^{2}$. Если l четное, то на следующем этапе группируются l остатков $M_{(2)}^{12}$ по 2, то есть квадраты $\left(M_{(2)}^{12}\right)^2$, и продолжаются вычисления $2^p \bmod p$, на каждом шагу которого выполняется поиск одного остатка, количество которых будет $log_2 l$ и столько же операций умножений.

В случае если l нечетное, то группируется l-1 остатков $M_{(2)}^{12}$ по 2, то есть $\left(M_{(2)}^{12}\right)^2$, и один $M_{(2)}^{12}\cdot M_{(2)}^{2}$. Для вычисления $2^p \bmod p$ нужно $log_2 l$ шагов, на каждом из которых проверяется четность и нечетность количества остатков. Такая процедура приводит к нахождению на каждом этапе двух остатков, общее количество которых $log_2 l$. Столько же будет операций умножений.

Итак, для нахождения $2^p \bmod p$ нужно $log_2 l$ описанных выше шагов, на каждом из которых происходит проверка на четность количества остатков. Такая процедура приводит к выполнению на каждом шагу двух операций модулярного умножения, которые можно выполнить векторно-модульным методом, описанным в [3, 4], с временной сложностью $O(2\ log_2 n)$.

По сравнению с известными, разработанный метод характеризуется высоким быстродействием и меньшей вычислительной сложностью, что позволяет эффективно применять его при проверке ЧБР на простоту.

На рисунке 1 представлена разработанная структурная схема предложенного алгоритма поразрядного разбиения при нахождении остатка ЧБР, который указывает на вероятную простоту числа.

Проведенные исследования показывают эффективность и высокую вероятность обнаружения простых чисел.

Блок-схема работы алгоритма проверки ЧБР на простоту представлена на рисунке 2.

Пошаговое выполнение предложенного алгоритма реализуется следующим образом:

1. Вход: n-разрядное число p.
2. Поиск разности $M_{(2)}^{2}=2^{n+1}-p$.
3. Поиск целой части от деления $l=p/n$ и $U=2^{p-l\cdot n+1}$.
4. Если l – четное, то вычисляется $res=(M_{(2)}^{2})^2 \bmod p$ и происходит побитовый сдвиг переменной l, то есть $l=l/2$. Если l – нечетное, тогда $l=l-1$, $U=(U\cdot M_{(2)}^{2}) \bmod p$.
5. Если l – четное, тогда $res=(res\cdot res) \bmod p$ и выполняется побитовый сдвиг переменной l, то есть $l=l/2$. Если l – нечетное, тогда $l=l-1$, $U=(U\cdot M_{(2)}^{2}) \bmod p$.
6. Если $l > 0$, то осуществляется переход на шаг 5.
7. Происходит операция модулярного умножения и присвоения $res=(res\cdot U) \bmod p$.
8. Если $res = 2$, то число вероятностно простое и алгоритм возвращает значение *true*, если же нет, то значение *false*.

В результате таких вычислений будет получено значение $2^p \bmod p$, и если оно равно 2, то p является простым числом.

Следует отметить, что очень редко встречаются числа, удовлетворяющие условию (1), но они не являются простыми. Нижняя граница совпадения при этом находится в соотношении 1:1000, а верхняя – 3:1000.

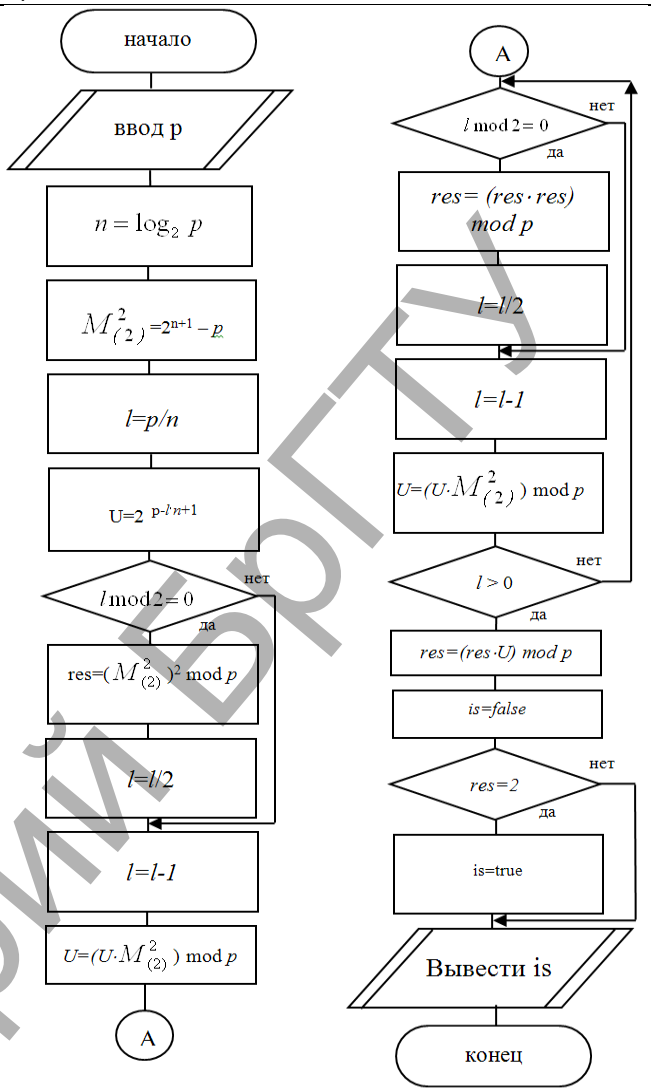

Рисунок 2 – Блок-схема проверки n-разрядных чисел на простоту

В таблице 1 представлены результаты экспериментального исследования распределения чисел, которые удовлетворяют условию (1) и являются составными.

Таблица 1 – Распределение составных чисел, которые удовлетворяют условию $2^p \bmod p=2$

Номер по порядку	Диапазон чисел	Составные числа P, которые удовлетворяют условию $2^p \bmod p = 2$
1	[1..1000]	341
2	[1000..2000]	1105
3	[1000..2000]	1387
4	[1000..2000]	1729
5	[2000..3000]	2047

Заключение. Разработан высоковероятностный метод проверки на простоту многоразрядных чисел, который, в отличие от известных, характеризуется меньшей вычислительной сложностью и сложностью реализации алгоритма. Представлены структурная схема и блок-схема алгоритма для реализации предложенного метода. Исследованы случаи исключений из принятого условия, количество которых свидетельствует о высокой вероятности обнаружения простого числа.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань: Казан. ун., 2011. – 190 с.
2. Venturi, D. Lecture Notes on Algorithmic Number Theory / D. Venturi. – New-York, Berlin: Springer-Verlag, 2009. – 217 p.
3. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D.Kozaczko, M.Kasianchuk, I.Yakymenko, S.Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015). - Warsaw, Poland. – V.1, September – 2015. – P.161–163.
4. Kasianchuk, M. Efficient methods for modular multiplication through the use of Rademacher – Krestenson TNB/ M. Kasianchuk, I. Yakymenko, Ya. Nykolaychuk, S. Ivasiev // Modern Problems of RadioEngineering, Telecommunications and ComputerScience (TCSET–2014): proceedingsofthe XI–th International Conference – L'viv–Slavske. – 2014. – P. 93–94.

Материал поступил в редакцию 14.01.2018

IVASIEV S.V. Method of high-probabilistic determination of simple multi-discharge numbers based on vector-module multiplication

The test for checking on the simplicity of multidigit numbers with using the method of vector and modular multiplication, which is characterized by high performance and low computational complexity in comparison with known is designed in this article. The block diagram of algorithm operation and its gradually implementation is presented.

УДК 581.3

Касянчук М.Н.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИИ УМНОЖЕНИЯ В ТРЁХМОДУЛЬНОЙ СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Введение. В настоящее время всё больше внимания уделяется разработке алгоритмов распараллеливания процессов выполнения арифметических операций [1], объёмы которых и значения соответствующих чисел растут значительными темпами. Особенно это касается асимметричной криптографии (криптосистемы RSA, Рабина, Эль-Гамаля, алгоритмов электронной цифровой подписи, шифрования на эллиптических кривых [2]), кодирования информации [3], обработки изображений, других задач теории чисел, дискретной и прикладной математики. Использующаяся на данный момент двоичная система исчисления имеет строго последовательную структуру, что ограничивает её возможности при параллельной обработке информации. Для этих целей целесообразно применять непозиционные системы исчисления, одной из которых является система остаточных классов (СОК) [4]. Хотя она тоже не лишена недостатков, главными из которых являются трудности при выполнении операций деления и сравнения, однако её успешно можно использовать для распараллеливания процессов при сложении, умножении и возведении в степень многоразрядных чисел.

Теоретические основы системы остаточных классов, её совершенной и модифицированной совершенной форм. Теоретической основой СОК является теория чисел [5]. Любое целое десятичное число N представляется в СОК в виде набора (b_1, b_2, … , b_s) наименьших положительных остатков от деления этого числа на фиксированные натуральные попарно взаимно простые числа (модули) p_1, p_2, … , p_s ($b_i=N \bmod p_i$), где s – количество модулей. При этом должно выполняться неравенство $0 \le N < P-1$, где $P=\prod_{i=1}^{s} p_i$ – число, которое определяет условие переполнения разрядности вычислений. Арифметические операции (сложение, умножение, возведение в степень) выполняются отдельно по каждому малоразрядному модулю, после чего полученные результаты преобразуются в десятичную систему исчисления с помощью китайской теоремы об остатках:

$$N=\left(\sum_{i=1}^{s} b_i B_i\right) \bmod P, \qquad (1)$$

где $B_i=M_i m_i$, $M_i=\dfrac{P}{p_i}$, $m_i=M_i^{-1} \bmod p_i$.

Нахождение обратных элементов по модулю характеризуется значительной вычислительной сложностью и в теории чисел реализуется полным перебором возможных вариантов, с помощью алгоритма Евклида или теоремы Эйлера [6]. В работе [7] описана совершенная форма (СФ) СОК, в которой выполняется условие $M_i \bmod p_i = 1$, что позволяет избежать процедуры поиска обратного элемента и умножения в (1) на базисные числа m_i. Выражение (1) в этом случае упрощается:

$$N=\left(\sum_{i=1}^{s} b_i M_i\right) \bmod P. \qquad (2)$$

Однако в этом случае $p_1=2$, $p_2=3$ и остальные значения p_i быстро увеличиваются, что неприемлемо при необходимости использования модулей приблизительно одинаковой разрядности.

В [8] предложена модифицированная совершенная форма (МСФ) СОК, в которой $M_i \bmod p_i = \pm 1$, что также исключает выполнение операции поиска обратного элемента. Вычисления (1) происходят согласно формуле

$$N=\left(\sum_{i=1}^{s} b_i m_i M_i\right) \bmod P, \qquad (3)$$

где $m_i=\pm 1$.

В [9] представлены теоретические основы построения трёхмодульной МСФ СОК. Однако в настоящее время отсутствуют экспериментальные исследования выполнения арифметических операций, в частности, умножения в СОК и её МСФ, что и составляет цель настоящей работы.

Экспериментальные исследования программной реализации системы остаточных классов и ее модифицированной совершенной формы. Для программной реализации операции умножения в СОК и МСФ СОК был выбран высокоуровневый язык программирования общего назначения Python, который ориентирован на повышение производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объём полезных функций. Код в Python организовывается в функции и классы, которые могут объединяться в модули (они, в свою очередь, могут быть объединены в пакеты). Пример ввода входных параметров представлен на рисунке 1.

Результаты размещаются в файл с расширением .csv, имя которого записано в последней строчке главного окна и включает в себя все входные параметры.

Касянчук Михаил Николаевич, *к.ф.-м.н., доцент, доцент кафедры компьютерной инженерии Тернопольского национального экономического университета, e-mail: kasyanchuk@ukr.net.*
Украина, ТНЭУ, 46000, г. Тернополь, ул. Львовская, 11.