2. Gerlits J. On a problem of S. Mrowka // Period. Math. Hund. 1973. V. 4 № 1. P. 71-79.
3. Marty R. On m-adic spaces // Acta Math. Hung. 1971. V. 22. № 3/4. P. 441-447.
4. Архангельский А. В., Пономарев В. И. Основы общей топологии в задачах и упражнениях. М.: Наука, 1974.
5. Александров П. С. Введение в теорию множеств и общую топологию. М.: Наука, 1977.
6. Чертанов Г. И. О непрерывных образах произведений разреженных бикомпактов // Сиб. мат. журн. 1988. Т 29. № 6. С. 167-175.

Сергей Арнольдович ИНЮТИН —
заведующий кафедрой высшей математики Сургутского государственного педагогического института,
кандидат технических наук, доцент

УДК 681.26

КОМПЬЮТЕРНАЯ МОДУЛЯРНАЯ АЛГЕБРА КВАДРАТИЧНОГО ДИАПАЗОНА И ОБЛАСТЬ ЕЕ ПРИЛОЖЕНИЯ

АННОТАЦИЯ. Приведена компьютерная модулярная алгебра с квадратичным диапазоном для элементов множества носителя - теоретическая база архитектурных решений для вычислительных систем с распараллеливанием на уровне машинных операций, и описана область ее применения.

The auther focuses upon the modular computer algebra with a square diapazon for a variable. This is the theoretical base for the computer systems with parallel machine operations.

Среди возможных видов рапараллеливания вычислительного процесса :
— на уровне задач,
— проблемных алгоритмов решения задач,
— машинных операций, используемых при выполнении проблемных алгоритмов, последний представляет интерес по следующим причинам. Распараллеливание выполнения машинных операций — достаточно универсальный метод увеличения быстродействия ЭВМ. Для описания арифметики и представления данных используются модулярные системы счисления. В этих системах при определенных ограничениях на величины диапазонов изменения операндов для мультипликативных операций достигается линейная временная сложность. Это недостижимо для позиционных, полиадических и полулогарифмических систем представления данных. Выигрыш в быстродействии становится особенно заметным при больших (многоразрядных) величинах операндов. Для оптимального применения модулярных систем в качестве арифметико- логической базы вычислительных устройств сами проблемные алгоритмы нуждаются в преобразовании их в «вычетную» форму с максимальным числом операций вычисления по модулю. После преобразования проблемные алгоритмы оптимальные, в смысле минимального количества немодульных операций, отображаются на модулярную аппаратную или программную арифметико-логичес-

кие базы соответствующих вычислительных средств: устройств или программное обеспечение, ориентированное на сетевое и класстерное многомашинное применение.

Параллельные машинные алгоритмы — резерв увеличения быстродействия электронно-вычислительных устройств [1, 4]. Сконструируем и опишем параллельную компьютерную алгебру с квадратичным диапазоном для ее элементов. Квадратичный диапазон, в отличии от исследованного в достаточной степени одинарного [1, 2, 3], не прменялся ранее для модулярных систем. Нами он выбран по причине более естественного способа реализации мультипликативных операций как в позиционных системах счисления , так и в модулярных.

Опишем множество — носитель алгебры и множество операций в ней.

Множество — носитель компьютерной алгебры — есть конечномерное метрическое пространство V-векторов с модулярными компонентами . Его можно задать следующим образом.

Элементы пространства есть векторы с модулярными компонентам:

$$\bar{a} = (\alpha_1,\ldots,\alpha_n) = ((\bar{a}\cdot\bar{e}_1),\ldots,(\bar{a}\cdot\bar{e}_n)),$$

или $\underline{a} = (\ a_1(\mathrm{mod}\, p_1^2), a_2(\mathrm{mod}\, p_2^2),\ldots,a_n(\mathrm{mod}\, p_n^2))$,

где $a \in p_1' \times \ldots \times p_n'$, — декартово произведение полных систем наименьших неотрицательных вычетов по квадратам взаимно-простых модулей,

$$\alpha_i \equiv |A|_{p^2_i} \in p'_i = \{0,\ldots,\ p^2{}_i - 1\}$$

или в другой записи $\alpha_i \equiv A(\mathrm{mod}\, p_i^2)$,

$(\bar{a}\cdot\bar{e}_i)$ — скалярное произведение векторов $\bar{a},\bar{e}_i$.

Компоненты векторов $\bar{a}$ — есть вычеты по $\mathrm{mod}\, p_i^{\,2}$ некоторого числа $A \in \mathbf{N}$, принадлежащего множеству натуральных чисел. Если $A < \prod_1^n p_i^2$, то существует биективное отображение между множествами $\{\bar{a}\} \leftrightarrow \{A\}$.

Пространство - линейное:

$$\bar{c} = \mu\bar{a} + \nu\bar{b} = \left(\ldots,\left|\mu\alpha_i + \nu\beta_i\right|_{p_i^2},\ldots\right) \in \prod_{i=1}^n p_i' .$$

Определим скалярное произведение в этом векторном пространстве:

$$(\bar{a}\cdot\bar{b}) = \sum_{i=1}^n \alpha_i\beta_i,$$

скалярное произведение имеет следующие свойства:

$$(\bar{a}\cdot\bar{b}) \geq 0$$

$$(\bar{a}\cdot\bar{a}) = 0 \Leftrightarrow \bar{a} = (0,\ldots,0)$$

$$(\bar{a}\cdot\bar{b}) = (\bar{b}\cdot\bar{a})$$

$$((\bar{a}+\bar{c})\cdot\bar{b}) = (\bar{a}\cdot\bar{b}) + (\bar{c}\cdot\bar{b})$$

Определим характеристику вектора - его модуль: $(\bar{a}\cdot\bar{a}) = \sum_{i=1}^n \alpha_i^2 = \left|\bar{a}\right|^2$.

Скалярное произведение задает метрику, но не норму, так как $(\lambda\bar{a}\cdot\lambda\bar{a}) \leq \lambda^2(\bar{a}\cdot\bar{a})$.

Остаточное расстояние между векторами $\bar{a},\bar{b}$ (аналог расстояния Хэмминга) определим следующим образом :

$$\varpi(\bar{a}\cdot\bar{b}) = \sum_{i=1}^n \delta\left(\left|\alpha_i - \beta_i\right|_{p^2_i}\right),$$

где $\delta\left(\left|\alpha_i - \beta_i\right|_{p_i^2}\right) = \begin{cases} 1\bullet, \text{при } \alpha_i \neq \beta_i \\ 0\bullet, \text{при } \alpha_i = \beta_i \end{cases}$.

Остаточное расстояние есть метрика:

1. $\varpi(\bar{a},\bar{b}) \geq 0$,
2. $\varpi(\bar{a},\bar{b}) = \varpi(\bar{b},\bar{a})$,
3. $\varpi(\bar{a},\bar{b}) \leq \varpi(\bar{a},\bar{c}) + \varpi(\bar{c},\bar{b})$.

Так как модулярным кодированием между подмножеством целых чисел $[0,P^2-1]\subset \mathbf{N}$, где $P^2=\prod_{i=1}^{n} p^2{}_i$, и множеством векторов устанавливается биективное отображение, можно ввести классы эквивалентности на множестве модулярных векторов, зафиксировав модуль модулярного вектора. Отметим, что минимальное изменение вектора на единицу в смысле расстояния Ли, приводит к изменению квадрата модуля вектора на нечетное целое число.

Действительно $\left|\bar{a}\right|^2=\sum_{1}^{n}(\alpha_i^2)+2\alpha_j+1$, где $\alpha_i\in[0,...,p^2{}_i-1]$.

В модулярном векторном пространстве нормированные вектора только базисные, т. к. лишь для них $\left|\bar{e}_i\right|=1$.

Нулевой модуль имеется только у нулевого вектора. На единичном расстоянии по модулю от него отстоят только базисные вектора.

Ортонормированный базис n-мерного пространства, при $P^2=\prod_{i=1}^{n} p^2{}_i$ есть векторы $\bar{e}_i$, компонентами которых являются вычеты чисел (m_iP^2/p_i^2) по $\mathrm{mod}\,\mathrm{p}^2{}_i$, или

$$\bar{e}_i=(\overline{m_iP^2/p^2{}_i}),$$

где $m_i=\left|P^2/p^2{}_i\right|_{p^2{}_i}^{-1}$

Справедливы утверждения:

1. $(\bar{e}_i.\bar{e}_j)=0$,
2. $(\bar{e}_i.\bar{e}_i)=1$,
3. $p^2{}_i(\bar{e}_i)+(\overline{p^2{}_i})=p^2{}_i(\bar{1})$.

Число и вектор $\bar{a}$ в рассматриваемой модулярной системе связаны следующими соотношениями:

$$A=\sum_{1}^{n}(\bar{a}\cdot(\bar{e}_i))\cdot m_iP^2/p^2{}_i-rP^2,$$

$$A=(\bar{a}\cdot\bar{M})-rP^2,$$

где r - характеристика A, зависящая от выбора базиса,

$$\bar{M}=(...,m_iP^2/p^2{}_i,...).$$

Модулярная алгебра задается следующей сигнатурой

$$\langle V,+,-,\cdot,\times,/,\div\rangle,$$

где $V=p_1'\times\ldots\times p_n'$ — множество носитель, его свойства описаны .

Множество операций содержит:

$+,-$ — адитивные операции, покомпонентное сложение и вычитание по модулям системы,

$\cdot$ — покомпонентное умножение первого рода по модулям системы,

$\times$ — умножение второго рода,

$/$ — покомпонентный аналог операции деления нацело или умножения первого рода на обратный элемент [2],

$\div$ — аналог операции деления нацело или умножения второго рода на обратный элемент [2].

Для определения вышеперечисленных операций необходимо множество (в общем случае взаимно простых) n чисел $\{p_i\}$ — оснований модулярной системы.

Рассмотрим адитивные и мультипликативные бинарные векторные операции.

Адитивные покомпонентные операции определим следующим образом:

$$\bar{a}\pm\bar{b}=\left(...,\left|\alpha_i\pm\beta_i\right|_{p^2{}_i},....\right).$$

Определим векторное умножение в модулярной алгебре двумя способами. Модулярное умножение первого рода - есть покомпонентная операция, его результат - вектор вида:

$$\bar{a}\cdot\bar{b}=\left(...,\left|\alpha_i\cdot\beta_i\right|_{p^2_i},....\right),$$

в частности , для этого умножения $(\overline{m_i P^2 / p^2 i})\cdot(\overline{m_j P^2 / p^2 j})=0$.

Векторное умножение второго рода $\bar{a}\times\bar{b}$, вводится стандартным образом. Его результат — вектор, перпендикулярный векторам-сомножителям. Модуль результата равен произведению модулей на синус угла между ними.

Замечание 1. При n=3 для ортогональных векторов $(p^2 i-1,0,0)$, $(0,p^2 j-1,0)$ вектор произведения ортогонален к векторам сомножителям, а его модуль

$$\begin{vmatrix} p^2 i-1 & 0 \\ 0 & p^2 j-1 \end{vmatrix}=\left|(p^2 i-1)(p^2 j-1)\right|_{p^2 i p^2 j}=-p^2 i-p^2 j+1.$$

Вышеуказанное согласуется со способом введения непростых оснований модулярной системы.

Замечание 2. Модули векторов-произведений при двух видах векторных умножений не совпадают

$$\sum_{i=1}^{n}\left|\alpha_i\beta_i\right|^2_{p^2_i}\neq\sum_{i=1}^{n}\alpha_i^2\cdot\sum_{i=1}^{n}\beta_i^2-\left(\sum_{i=1}^{n}\alpha_i\beta_i\right)^2,$$

в частности, при n=2

$$\left|\alpha_1\beta_1\right|^2_{p^2_1}+\left|\alpha_2\beta_2\right|^2_{p^2_2}\neq(\alpha_2\beta_1-\alpha_1\beta_2)^2.$$

Соответственно, вводится операция формального деления первого рода:

$$\bar{a}/\bar{b}=\bar{a}\cdot\left|\bar{b}\right|^{-1}_{P^2}=\left(...,\left|\alpha_i\left|\beta_i\right|^{-1}_{p^2_i}\right|_{p^2_i},....\right),$$

где $|\bar{b}|^{-1}_{P^2}$ -обратный вектор, для него справедливо соотношение:

$$\left|\left|\bar{b}\right|^{-1}_{P^2}\cdot\bar{b}\right|_{P^2}=1$$

Обратный вектор определен для любого вектора из V без нулевых компонент.

Операция формального деления второго рода не вводится.

Дадим описание и формализацию области приложения указанной алгебры и методов выполнения машинных операций в ней. При этом необходимо учесть следующие моменты.

Ресурсы вычислительной техники постоянно совершенствуются и увеличиваются. Они не могут быть безграничны в принципе. Ряд математических задач, имеющих мощные приложения, требуют выполнение операций над числами во все больших диапазонах их изменений, причем результаты должны быть точными, без округлений.

Нижеприведенные определения используют понятие машинных ресурсов: машинный диапазон, объем памяти. Однако они инвариантны к типу компьютеров и могут быть конкретизированы для определенных ЭВМ. Определения дадим применительно к алгебраическим операциям над целыми числами.

Определение. Большой (многократный) компьютерный диапазон (**P**— числовой диапазон) — множество числовых величин, наибольшая из которых многократно превышает наибольшую величину из машинного диапазона типовой ЦВМ, как правило, более чем на несколько порядков.

Математические объекты в **P** — числовые величины (или числа) , над которыми выполняется набор соответствующих алгебраических операций. Числовые величины A задаются в векторной форме, где элементы векторов — цифры позиционного, полиаддического или модулярного представления. Множество — носитель компьютерной алгебры больших величин совпадает с полной системой вычетов по модулю P [3].

Алгебра (арифметика) большого диапазона формально определяется следующей сигнатурой:

$$\left(\langle P\rangle, \{+,-,\cdot,/\}, =, , <\right)$$

где $\langle P\rangle$ — полная система вычетов (в частности наименьших неотрицательных) по mod P,

$\{+,-,\cdot,/\}$ — множество операций , выполняемых над элементами большого диапазона,

$\{=,<\}$ — множество отношений над элементами множества – носителя.

В варианте модулярной системы для супремума большого диапазона справедливо

$$P = \prod_{i=1}^{n} p_i ,$$

где p_i — основание модулярной системы, они выбираются простыми вблизи супремума компьютерного диапазона типовой ЦВМ. Это позволяет элементы большого диапазона задавать модулярными векторами [3].

Целочисленный аналог этой алгебры в модулярном варианте с квадратичным диапазоном — есть модулярная компьютерная алгебра большого или многократного диапазона со специальными модулярными арифметическими операциями:

$$\left(\langle P^2\rangle, \Sigma_0, =, \mathrm{IS}, \mathrm{MJ}, \Sigma_1\right),$$

где $\langle P^2\rangle$ — полная система вычетов по mod,

$\Sigma_0 = \{+,-,\cdot,KP,-1,FD\}$ — множество модульных операций с покомпонентным распараллеливанием, включает операции: сложение, вычитание, умножение, каноническое представление KP, вычисление обратного элемента по модулю, формальное деление FD или умножение на обратный элемент [2].

$=$ — проверка отношения равенства, покомпонентная операция,

IS, MJ — вычисление двух функционалов (неточный след, модульное ядро), вычисляемых для выполнения операций второго множества [3],

$\Sigma_1 = \{\div, |\cdot|_F, <\}$ — множество немодульных операций включает: деление в общем случае, вычет по произвольному модулю $F < P$ и сравнение элементов большого диапазона по величине.

Эта компьютерная алгебра позволяет выполнить стандартные арифметические операции над целыми числами в большом (многократном) машинном диапазоне, сравнивать их по величине. Деление выполняется целочисленным, результат равен целой части частного от деления.

Между вышеуказанными компьютерными алгебрами существует изоморфизм. Сравнение их возможностей целесообразно проводить по скорости выполнения некоторых базовых операций, определяемых для множества проблемных алгоритмов для вариантов максимального распараллеливания на n –процессоров и для однопроцессорного вычислительного устройства или типовой ЦВМ [1,4].

Для решения вычислительных проблем теоретической физики, космогонии, криптосинтеза, анализа и ряда других необходимо выполнение вычислений в сверхбольших диапазонах, которые, с одной стороны, являются естественным обобщением больших диапазонов, с другой стороны, имеют принципиальное отличие от последних. Отличие заключается в том, что речь идет о вычислениях над математическими объектами, не имеющими числовой (векторной) записи, но в конечном счете числами. Явные числовые записи невозможно или нецелесообразно после вычислений (генерации) хранить по причине нехватки вычислительных ресурсов. Назовем эти математические объекты сверхбольшими числами.

Определение. Сверхбольшой (супербольшой) компьютерный диапазон (**Q** –диапазон) –есть множество числовых объектов (в конечном счете чисел) таких, что их

наибольшее значение значительно превышает максимальное значение числовой величины из большого компьютерного и ,тем более, типового машинного диапазона. Элементы **Q** –диапазона есть числовые объекты или сверхбольшие числа.

Особенность сверхбольшого диапазона в том, что оценки величин его элементов возможно получить лишь через алгоритмы их генерации. Это также отличает сверхбольшие числа от обычных чисел из машинного диапазона, а также чисел из больших диапазонов

Несмотря на отсутствие у числовых объектов из сверхбольшого диапазона **Q** числового (векторного) представления, над ними необходимо выполнять вычисления в алгебре с ограниченным числом операций. Работа с такими числовыми объектами возможна в вычетной арифметике посредством вычисления вычетов от результатов, получаемых на каждом шаге алгоритма генерации. При этом учитывается, что величины результата шага алгоритма не превышают супремума известного большого диапазона, работа в котором поддерживается имеющимися вычислительными средствами на модулярной или позиционной базах.

Перечислим возможные задачи вычислений в сверхбольших диапазонах:

— сравнение числовых объектов по величине на больше, меньше или равно:

$A = A'$, $A > A'$;

— вычисление разности:

$A - A' = |A - A'|_F$ при $A / A' > 1$, $A - A' < F$

$A' - A = |A' - A|_F$ при $A' / A > 1$, $A' - A < F$

— вычисление модуля разности величин числовых объектов при $A - A' > F$:

$|A - A'|_F$ или $|A' - A|_F$

— вычисление вычета от величины числового объекта по некоторому модулю F, принадлежащиму большому диапазону : $|A|_F$.

Алгебра числовых объектов из сверхбольшого диапазона задается следующей сигнатурой:

$$(\langle Q \rangle , \{-, |\cdot|_F\}, =, <)$$

где $\langle Q \rangle$ — множество-носитель алгебры сверхбольшого диапазона есть множество последовательностей вычетов от числовых результатов, получаемых на этапах вычислительных алгоритмов (вычислимых функций) генерации числовых объектов.

На множество алгоритмов генерации числовых объектов накладываются ограничения :

— единственность результата алгоритма,

— многошаговость алгоритма, причем критерии останова могут задаваться извне количеством шагов или проверяться на каждом шаге сравнением с константой, результатом предыдущих шагов,

— конечностью степени вложенности алгебраических формул,

— идемпотентности операции вычисления вычета по одному модулю:

$$\left|\varphi\left(|A_{n-1}|_F\right)\right|_F = \left|\ldots\left|\varphi\left(\ldots\left|\varphi\left(|A_0|_F\right)\right|_F\right)\right|_F\ldots\right|_F$$

— ограниченностью результата шага относительно входных величин шага алгоритма:

$$0 \le A_i < F, \quad 0 \le \varphi(A_i) = A_{i+1} < F^2$$

— монотонностью возрастания на каждом шаге величины непредставимого числа:

$$A_0 < \varphi(A_1) < \ldots < \varphi(A_i) < \varphi(A_{i+1}) < \ldots < A_n = \varphi(A_{n-1})$$

— повторяемости операций на каждом шаге алгоритма.

В общем случае на шаге алгоритма генерации набор операций из алгебры большого диапазона произволен, хотя меньшую временную сложность будут иметь распараллелевыев модулярной алгебре большого диапазона кольцевые операции из Σ_0.

Вышеперечисленные условия довольно сильно сужают класс возможных алгоритмов, но не делают его пустым. В частности, вышеперечисленным ограничениям удовлетворяют вычислительные задачи тестирования чисел на простоту следующего вида:

$$\left|a^M \pm c\right|_F = \left\| \left(\left\| \ldots \left|a\right|_F^{m_0} \right|_F^{\ldots m_n} \right\|_F \right)^{\frac{M}{m_0 \ldots m_n}} \right\|_F \pm \left|c\right|_F \Bigg|_F ,$$

где m_i — целочисленные делители M, величины M, F — большие числа, для F неизвестно каноническое разложение, в частности, оно может быть простым.

На каждом шаге такого алгоритма результат его работы представим в виде:

$$A_{i+1} = \varphi\left(\left|A_i\right|_F\right) = N_{i+1}F + \left|A_{i+1}\right|_F .$$

Определим алгебраические операции и отношения равенства, неравенства в этой алгебре.

В дальнейшем под P_i будем понимать мультипликативный модуль модулярной системы, в частности, квадратичный , для которого $P_i = D_i^2$. Процедура вычисления разности двух сверхбольших чисел опирается на следующее утверждение.

Теорема. Пусть $A \,/\, A' > 1$ и $\Delta = A - A' < F < P_1 < \ldots < P_n$,
тогда $\forall P \in \{P_1,\ldots,P_n\}$ $\left\|A\right|_P - \left|A'\right|_P\Big|_P = \Delta - \text{const}$.

Доказательство. Вычисления в модулярной арифметике с модулем P дают вектор, соответствующий вычетам сверхбольшого числа по сомножителям модулю P. Так как разность чисел есть константа по всем модулям, превышающим величину их разности, имеем:

$$A = N\,P + \left|A\right|_P , \quad A' = N'\,P + \left|A'\right|_P ,$$

$$\Delta = A - A' = (N - N')\,P + \left|A\right|_P - \left|A'\right|_P ,$$

$$\left|\Delta\right|_P = \left|A - A'\right|_P = \left|A\right|_P - \left|A'\right|_P + \left|N - N'\right| P - k\,P =$$

$$= \left|A\right|_P - \left|A'\right|_P + (011)\,P .$$

Замечание 1. Выполнение равенств теоремы является необходимым условием $\Delta < F$.

Замечание 2. Справедлив следующий алгоритм.

Пусть $\Delta < F < P = \prod_{i=1}^{n} p_i$. Здесь P одно из чисел множества.

$\{P_1,\ldots,P_n\}$

Вычислим $\left\{\left|\Delta\right|_{P/p_i}\right\}, \left\{\left|\Delta\right|_{P/p_i p_j}\right\}, \ldots$.

Минимальное значение $P/p_i \ldots p_l$, при котором $\left|\Delta\right|_{P/p_i \ldots p_l} = \left|\Delta\right|_P$ дает верхнюю оценку F.

Для проверки равенства сверхбольших чисел первым этапом является оценка отношения $A \,/\, A'$ и сравнение с единицей. Для этого применимы стандартные методы. В общем случае условие $\left|A\right|_F = \left|A'\right|_F$ является необходимым для равенства. Его можно усилить, если $F \in \{F_1, F_2, \ldots\}$ где $(F_i, F_j) = 1$.

Для проверки равенства сверхбольших чисел поступим следующим образом. Пусть выполнен первый этап, установлено, что $A \,/\, A'$ близко к единице. Оценим разность величин двух сверхбольших чисел $|A - A'| < F$. Выберем

$\ldots P_{-i} < \ldots < P_{-1} < F < P_1 < \ldots < P_i < \ldots$.

Теорема. Необходимое и достаточное условие равенства двух сверхбольших чисел $A = A'$ при наличии верхней оценки F их разности есть $|A - A'|_P = 0$, где

$P \in \{\ldots P_{-i}, \ldots, P_{-1}, P_1, \ldots, P_i, \ldots\}$.

Доказательство. Пусть $A = A'$, следовательно $A - A' = 0$. Равенство справедливо при операциях по любым модулям.

Пусть $|A - A'|_P = 0$, следовательно $A - A' = k\,P$, где P как меньше, так и больше грубой оценки супремума разности двух числовых объектов. Следовательно, $k = 0$, т. е. $A = A'$.

Следствие 1. Можно выбирать $P_i = P \,/\, (p_1 \ldots p_i)$ и т. д.

Следствие 2. Оценка P_i может быть более грубой, чем F, но в вычислительном плане вычисления по модулю P_i предпочтительнее, т. к. распараллеливаются.

В алгебре сверхбольшого диапазона для выполнения введенных операций и проверки отношений можно предложить следующий алгоритм.

Алгоритм.

1. Оценивается величина $A \,/\, A'$ сравнением с единицей.
2. Оценивается величина $A - A'$ с возможной степенью точности F.
3. Вычисляется величина $\left\| |A|_{P_i} - |A'|_{P_i} \right|_{P_i}$ посредством вычисления по mod P_i.

При этом:

— уточняется F.

4. Проверяется равенство $A = A'$.

Замечание1. При необходимости вычислений по mod F эта модульная операция реализуется посредством операций из Σ_1, Σ_0, при внешних операциях по mod P или mod P^2.

Замечание 2. Операция вычисления по mod F, где F - простое, для алгебры свербольшого диапазона является базовой и должна выполняться наиболее эффективно [5].

ЛИТЕРАТУРА

1. Коляда А. А. Модулярные структуры конвейерной обработки цифровой информации. Минск : Изд-во «Университетское». 1992. 368 с.

2. Инютин С. А. Метод вычисления обратного элемента в конечном поле // Научные труды СурГУ. Вып. I. Сургут: Сев.-Сиб. рег.кн.из-во. 1995. С. 102-107.

3. Inutin S. A. The Computer Parallel Modular Algebra. // Transaction of PARA-96. Denmark: Springer. 1996. P. 156-161.

4. Aho A. V. The Desing and Analysis of Computer Algorithms. Addison-Wecley Publ. Company. 1979. 346 p.

5. Munro I. The Computational Complexity of Algebraic and Numeric Problems // American Elsevier. New-York. 1986. № 7. P. 28-40.