# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

## ПОВЫШЕНИЕ СКОРОСТИ ВЫПОЛНЕНИЯ ОПЕРАЦИИ МОДУЛЬНОГО ВОЗВЕДЕНИЯ В СТЕПЕНЬ МНОГОРАЗРЯДНЫХ ЧИСЕЛ

*Червяков Н.И., Лобес М.В.*

В статье рассмотрен алгоритм Монтгомери ускоренного модульного умножения многоразрядных чисел. Предложено адаптировать его для системы остаточных классов. Показано, что такая модификация алгоритма Монтгомери дает огромное преимущество по времени выполнения операции модульного умножения, а, следовательно, и операции модульного возведения в степень.

### Постановка задачи

В последние годы наблюдается повышенный интерес к методам и алгоритмам теории чисел, сложность реализации которых во многом зависит от входящих в них арифметических операций. Большинство из известных теоретико-числовых методов и алгоритмов содержат неоднократное выполнение операции модульного возведения в степень. При этом области, в которых эти методы и алгоритмы применяются, требуют обработки многоразрядных чисел [1]. Трудность состоит в том, что в рамках производительности современных вычислительных устройств, функционирующих в позиционной системе, реализация операции модульного возведения в степень многоразрядных чисел становится достаточно трудоемкой. Это объясняется необходимостью учета межразрядных переносов. Поэтому для того, чтобы значительно повысить производительность вычислительных устройств необходимо применение систем счисления, лишенных подобного недостатка [2].

В свете сказанного актуален переход к непозиционным системам счисления, наиболее перспективной из которых является система остаточных классов. Эта система обладает множеством неоспоримых преимуществ, в сравнении с позиционной системой, однако ее широкое применение сдерживается рядом причин [3]. Одна из них состоит в том, что при обработке многоразрядных чисел определенные трудности возникают при выполнении такой операции как модульное возведение в степень. Следовательно, для построения полноценной компьютерной арифметики на базе системы остаточных классов необходимо разработать эффективный алгоритм выполнения этой операции.

### Адаптация алгоритма ускоренного модульного умножения Монтгомери для системы остаточных классов

Так как классический алгоритм модульного возведения в степень сводится к ряду модульных умножений, то главным вопросом является разработка эффективного метода и алгоритма для выполнения этой операции. Трудность заключается в том, что операция модульного умножения по произвольному модулю предполагает реализацию операции деления, которая является достаточно сложной в любой, в том числе и в позиционной системе.

Одним из самых эффективных алгоритмов, известных в литературе и применяемых для ускорения операции модульного умножения, является алгоритм Монтгомери, основная идея которого заключается в преобразовании операндов в некоторые остатки и вычислении произведения этих остатков. Полученный результат умножения преобразуется назад к нормальному виду [4]. Такой подход выгоден, если необходимо вычислить ряд умножений в преобразованной сфере. Преимущество алгоритма Монтгомери состоит в том, что операция модульного умножения по произвольному модулю с помощью определенных преобразований заменяется рядом сложений и умножений по модулю, представляющему собой степень двойки. При этом трудоемкая операция деления заменяется несколькими битовыми операциями сдвига. Для того чтобы алгоритм Монтгомери подходил для практической реализации, удобнее всего выбрать двоичную систему счисления (см. рис. 1).

Результат модульного умножения после применения алгоритма получается в виде $S_{m+1} \equiv ABR^{-1} \bmod M$. Для того, чтобы привести его к нормальному виду нужно применить преобразование Монтгомери [4].

Так как алгоритм Монтгомери применяется в позиционной системе счисления, то, несмотря на преимущества, его применение не дает скачкообразного повышения скорости выполнения операции модульного умножения.

В алгоритме Монтгомери на каждом шаге используется младший коэффициент позиционного представления для вычисления $q_i$. Поэтому он может быть адаптирован для системы остаточных классов (см. рис. 2), если использовать обобщенную позиционную систему с аналогичным набором оснований. Пусть $p_1, p_2, ..., p_k$ – основания системы остаточных классов и $R = p_1 \cdot p_2 \cdot ... \cdot p_k$ диапазон.

Алгоритм Монтгомери, адаптированный для системы остаточных классов, вычисляет значение $S$ так что

$$S \equiv ABR^{-1} \bmod M . \qquad (1)$$

На каждом этапе алгоритма вычисляется цифра обобщенной позиционной системы

$$q_i = \left| \left| s_i + a_i \;\; b_i \right|_{p_i} \;\; \left| \frac{1}{p_i - m_i} \right|_{p_i} \right|_{p_i} \qquad (2)$$

и цифры представления в системе остаточных классов

$$s_j = \left| \left| s_j + a_i \;\; b_j + q_i \;\; m_j \right|_{p_j} \;\; \left| 1/p_i \right|_{p_j} \right|_{p_j} . \qquad (3)$$

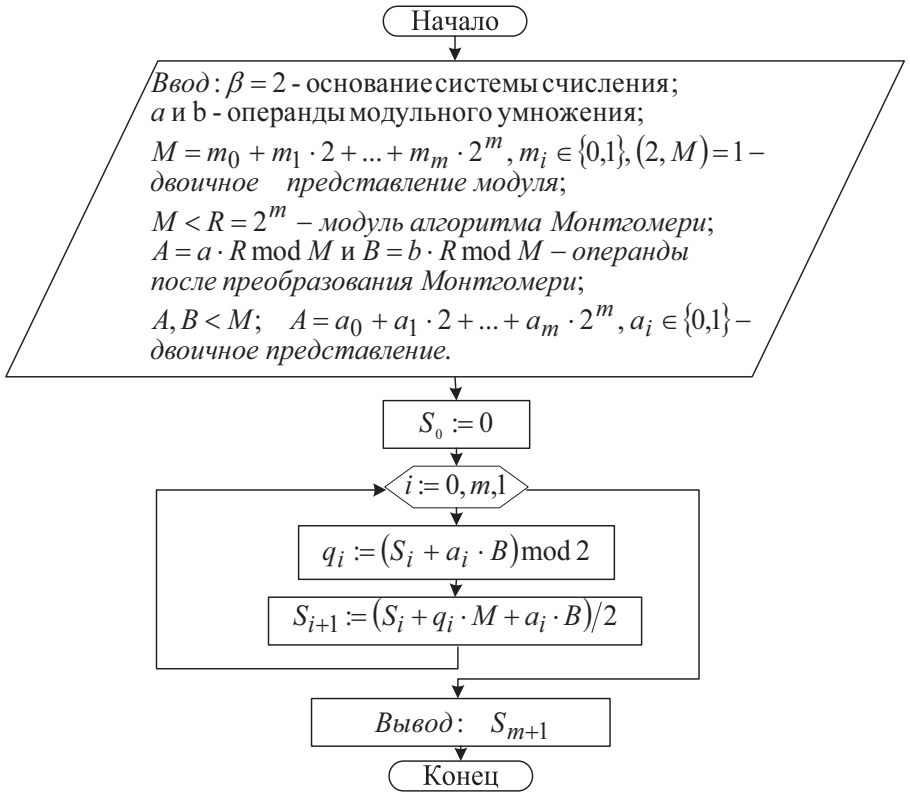


Рис. 1. Алгоритм Монтгомери для двоичной системы счисления

При этом значения $s_j$ вычисляются таким образом, что они являются кратными $p_j$.

Следовательно, если основания системы являются простыми числами, то деление $s_j$ на $p_j$ заменяется умножением на мультипликативную обратную величину.

Тогда из алгоритма имеем равенство

$$S = \cfrac{\cfrac{\cfrac{a_1 B + q_1 M}{p_1} + a_2 B + q_2 M}{p_2} + \ddots + a_{k-1} B + q_{k-1} M}{p_{k-1}} . \qquad (4)$$

Равенство (4) после приведения к общему знаменателю и группировки имеет вид

$$S = \frac{1}{R}((a_1 + a_2 p_1 + ... + a_k p_1 ... p_{k-1}) \;\; B + \\ + (q_1 + q_2 p_1 + ... + q_k p_1 ... p_{k-1}) \cdot M) \qquad (5)$$

или

$$S = \frac{1}{R} \;\; (A \cdot B + Q \cdot M) . \qquad (6)$$

Следовательно, так как

$$Q \cdot M \bmod M = 0, \quad (7)$$

то справедливо сравнение (1).

Кроме этого на каждом этапе алгоритма с помощью операции расширения системы оснований вычисляется остаток $s_i$ по основанию $p_i$. Для определения цифры $s_i$ по основанию $p_i$ предложен метод расширения системы оснований на основе представления ортогональных базисов в обобщенной позиционной системе.

На основе алгоритма Монтгомери, адаптированного для системы остаточных классов, и классического алгоритма модульного возведения в степень может быть разработан алгоритм модульного возведения в степень многоразрядных чисел. Для этого результат каждого модульного умножения необходимо использовать как один или оба (в случае возведения в квадрат) операнда последующего модульного умножения.

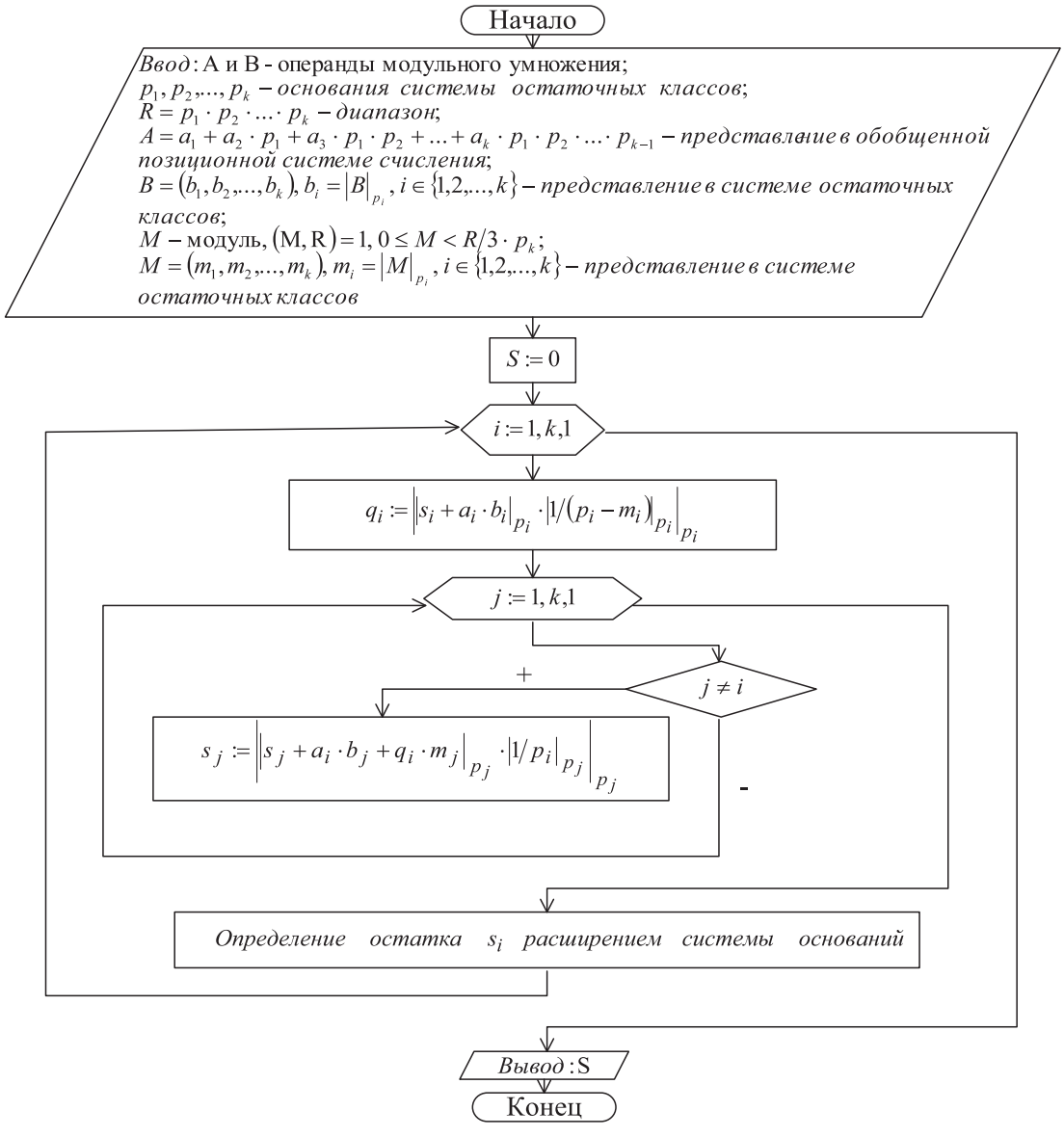


Рис. 2. Алгоритм Монтгомери, адаптированный для системы остаточных классов

## Сравнительная оценка основного алгоритма Монтгомери, адаптированного для системы остаточных классов

Преобразование Монтгомери, выполняемое в начале и в конце алгоритма, может не оцениваться, так его сложность при большом количестве модульных умножений практически не влияет на преимущество, даваемое непосредственно алгоритмом Монтгомери. Так же можно не оценивать преобразования операндов и результата из позиционной системы в систему остаточных классов и обратно, так как разработанный алгоритм модульного умножения рассчитан на применение в специализированном вычислительном устройстве, целиком работающем в системе остаточных классов.

Сравнительная оценка может быть выполнена по двум критериям: по общему количеству битовых операций, выполняемых в алгоритме и по количеству битовых операций, определяющих время реализации алгоритма.

Оценка общего количества битовых операций, выполняемых в алгоритмах в зависимости от разрядностей операндов (см. таблицу 1), показывает, что основной алгоритм Монтгомери содержит в среднем в 1,2 раза меньше битовых операций.

Таблица 1. Оценка общего количества битовых операций алгоритмов

| Разрядность операндов | Общее число битовых операций, выполняемых в алгоритме | | $\approx\left(\frac{O_{M+C}}{O_M}\right)$ |
|---|---|---|---|
| | Монтгомери $(O_M)$ | Монтгомери + СОК $(O'_{M+C})$ | |
| 8 | 208 | 310 | 1,5 |
| 16 | 800 | 1128 | 1,4 |
| 32 | 3136 | 3896 | 1,2 |
| 64 | 12416 | 13640 | 1,1 |
| 128 | 49408 | 54928 | 1,1 |
| 256 | 197120 | 217964 | 1,1 |
| 512 | 787456 | 856304 | 1,1 |
| 1024 | 3147776 | 3374377 | 1,1 |

Оценка количества битовых операций, определяющих время реализации алгоритмов (см. таблицу 2) показывает, что применение алгоритма Монтгомери, адаптированного для системы остаточных классов, дает огромное преимущество по времени выполнения операции модульного умножения, причем оно возрастает с ростом разрядностей операндов.

Таблица 2. Оценка количества битовых операций, определяющих время реализации алгоритмов

| Разрядность операндов | Число битовых операций, определяющих время реализации алгоритма | | $\approx\left(\frac{O_M}{O'_{M+C}}\right)$ |
|---|---|---|---|
| | Монтгомери $(O_M)$ | Монтгомери + СОК $(O'_{M+C})$ | |
| 8 | 208 | 256 | 0,8 |
| 16 | 800 | 739 | 1,1 |
| 32 | 3136 | 1658 | 1,9 |
| 64 | 12416 | 3839 | 3,2 |
| 128 | 49408 | 10852 | 4,6 |
| 256 | 197120 | 31167 | 6,3 |
| 512 | 787456 | 89572 | 8,8 |
| 1024 | 3147776 | 269236 | 11,7 |

## Выводы

Сравнительная оценка показала, что по вычислительной сложности (количеству битовых операций) алгоритм Монтгомери, адаптированный для системы остаточных классов, незначительно уступает основному алгоритму Монтгомери. Однако за счет малой разрядности оснований системы остаточных классов и параллельной структуры вычислений разработанный метод и алгоритм дает существенный выигрыш по времени реализации операции модульного умножения, причем этот выигрыш растет с ростом разрядностей операндов.

Применение алгоритма Монтгомери, адаптированного для системы остаточных классов, позволяет время выполнения операции модульного воз-

ведения в степень 1024 разрядными операндами уменьшить в 17,5 раз.

### Литература


1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. – 328 с.
2. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. – 440 с.
3. Галушкин А.И., Червяков Н.И. Нейрокомпьютеры в остаточных классах. М.: Радиотехника, 2003. – 270 с.
4. Червяков Н.И., Лобес М.В. Модульное возведение в степень // Материалы III МНТК «Инфокоммуникационные технологии в науке, производстве и образовании». Ставрополь: Изд. СевКавГТУ, 2008. Ч. III. – С. 204-210.


УДК 681.128.56

# МОДЕЛИРОВАНИЕ КОЭФФИЦИЕНТА ПРЕЛОМЛЕНИЯ В ЛИНЕЙНОМ И НЕЛИНЕЙНОМ РЕЖИМАХ ДЛЯ НАНОСТРУКТУРНОГО СИТАЛЛА

*Султанов А.Х., Виноградова И.Л., Салихов А.И.*

Проведено математическое моделирование коэффициента преломления в линейном и нелинейном режимах мощностей для наноструктурного ситалла. Аналитический метод основан на модели движения напряженного осциллятора, подвергающегося действию внешней световой волны. Показано, что нелинейный режим движения сопровождается самовоздействием, а также возможной генерацией второй и третьей гармоник. Оценена погрешность метода, которая составляет 3-4 %. Найден коэффициент нелинейной жесткости для наноструктурного ситалла. Анализ зависимостей, определяющих изменение показателя преломления от интенсивности вводимого излучения, показало наличие трех характерных участков – задержанный нелинейный режим, скачкообразный рост и пологий почти линейный рост показателя преломления.

### Введение

Механическое нагружение, как известно, приводит к смещению потенциала межатомного взаимодействия [1], что вызывает изменение макроскопических свойств твердого тела в сравнении с его ненагруженным состоянием [2-3]. Данный эффект связан с различием в колебательной динамике ансамбля нелинейных осцилляторов, которые выступают элементами этой динамической системы и являются физической моделью твердого тела. В этой связи представляется интересным провести анализ поведения отдельного возбужденного осциллятора, нагруженного действием внешней силы. Подобного рода исследования, направленные на изучение динамики перераспределения кинетической и потенциальной энергии осциллятора, нагруженного постоянной внешней силой, представлены в [4-5]. В настоящей работе проводится исследование движения нагруженного нелинейного осциллятора под влиянием некоторого дополнительного периодического воздействия. А именно – моделируется эффект переизлучения поля оптическим электроном, движение которого искажено из-за внутреннего механического напряжения в веществе, внешнего светового поля для случая линейного и кубично нелинейного режимов мощностей. Это в свою очередь позволит получить коэффициенты, характеризующие макроскопические оптические свойства напряженного твердого тела – коэффициенты затухания и преломления. Согласование результатов приближенно-аналитического, численно-компьютерного решений и эксперимента приводят к заключению о правильности проведённых расчетов.

### Модель нагруженного осциллятора

Нагруженный осциллятор является моделью оптических (переизлучающих) электронов, находящихся в составе атомов или молекул, расположенных по границам зерен кристаллита. Если рассматривается кристаллит в традиционно квазиравновесном состоянии, то пограничено-зеренное искажение кристаллической решетки является небольшим [1], объем границ мал в сравнении с объемом зерен [3], и действие нагруженного осциллятора является достаточно малым в общей реакции вещества. Иначе обстоит дело для объемных нанокристаллических материалов (НКМ), которые являются существенно неравновесными веществами ввиду максимального объема: в процессе механической обработки кристаллита, применяемой для получения нанокристаллического материала, например, интенсивной пластической деформации (ИПД) [3], появляются зародыши (домены) с более мелким размером зерна по отношению к изначальному (или крупнозернистому) состоянию. С повышением степени деформации объем этих доменов увеличивается, постепенно захватывая все вещество. При этом даже еще в неравномерном по размеру зерна веществе вновь