

15

Комитет науки Министерства образования и науки  
Республики Казахстан  
РГП «Институт информационных и вычислительных технологий»  
КН МОН РК



25 лет  
Независимости  
Республики Казахстан



25 лет  
Институту  
информационных и  
вычислительных  
технологий

### **МАТЕРИАЛЫ**

Международной научной конференции  
«Информатика и прикладная математика»  
(«Computer science and Applied Mathematics»),  
посвященной 25-летию Независимости Республики Казахстан и  
25-летию Института информационных и  
вычислительных технологий

**I часть**

г. Алматы, 21-24 сентября 2016 года

**Алматы  
2016**

<b>Секция 1. СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И ТЕОРИИ УПРАВЛЕНИЯ</b>		<b>7</b>
<i>Altayeva A.B.</i>	Medical decision making diagnosis system integrating K-means and Naïve Bayes algorithms	8
<i>Ryskeldi M.M., Kelesbekov A.B.</i>	Multilayer soil freezing and swelling	13
<i>A. Sakabekov, Y. Auzhani</i>	Onedimensional nonlinear fourmoment system equations of Boltzmann with Maxwell-Auzhan boundary conditions	21
<i>Satybaldina A.N., Kalibekova G.B.</i>	Modeling of underground pipeline energy consumption taking into account uneven environmental temperature	27
<i>Thanos Stouraitis</i>	RNS-based RSA and ECC cryptography – basic operations, algorithms, and hardware	36
<i>Zumatov S.S.</i>	Program manifold's stability of automtic control systems by course of plane	37
<i>Айнакулов Ж.Ж., Кузьмин А.Г.</i>	Геоинформационное обеспечение агротехнологии точного земледелия на основе беспилотных летательных аппаратов (БПЛА)	47
<i>Амиргалиева Ж.Е., Арсланов М.З.</i>	Поиск с чередующимися окрестностями для задач дисперсии	54
<i>Арсланов М.З.</i>	О задаче раскроя на прямоугольники с двумя высотами	63
<i>Ахметова А.М., Нугманова С.А.</i>	Методы и алгоритмы перехода от позиционного представления к остаткам	66
<i>Бекмуратов Т.Ф., Мухамедиева Д.Т., Примова Х.А.</i>	Адаптивный алгоритм синтеза систем нечеткого вывода	76
<i>Бекмуратов Т.Ф., Мухамедиева Д.Т., Ниёзматова Н.А.</i>	Применение иммунного алгоритма для обучения нечеткой модели	85
<i>Джомартова Ш.А., Мазаков Т.Ж.</i>	Об одном способе исследования устойчивости интервальных линейных систем	93
<i>Домрачев А.А., Вусс Г.В.</i>	Основные подходы к формированию института международного электронного нотариата (соотнесение доверенных ИКТ-сервисов с рядом традиционных нотариальных действий)	105

# МЕТОДЫ И АЛГОРИТМЫ ПЕРЕХОДА ОТ ПОЗИЦИОННОГО ПРЕДСТАВЛЕНИЯ К ОСТАТКАМ

Ахметова А.М., Нугманова С.А.  
e-mail: [ardak\\_66@mail.ru](mailto:ardak_66@mail.ru), [nugm\\_s@mail.ru](mailto:nugm_s@mail.ru)

Институт информационных и вычислительных технологий КН МОН  
Казахстан

**Аннотация.** Система остаточных классов обладает одной особенностью, можно отнести к недостаткам этой системы: нельзя визуально определить величину представленного в СОК, а следовательно затруднительно и выполнение таких операций, как сравнение чисел, определение знака числа. Один из путей решения этой проблемы состоит в преобразовании чисел из СОК в позиционную систему счисления. В данной статье рассматривается алгоритм перехода от позиционного представления к остаточным

**Ключевые слова:** система остаточных классов, метод ортогональных Китайская теорема, базисы системы, диапазон, позиционная система, алгоритм, обратное позиционная система, преобразование.

## 1 Анализ последних исследований и публикаций

Толчком к исследования в области непозиционных систем счисления послужили опубликованные в 1955-1957 гг работы чешских ученых М. Валаха и А. С. посвященные представлению чисел в виде совокупности не отрицательных вычетов по группе взаимно простых оснований, и определившейся в связи с этим представлением возможности выполнения рациональных операций без учета разрядных связей цифрами числа. Проведенные авторами настоящей исследования в этой новой системе счисления, названной системой остаточных классов, привели к созданию математики.

В процессе исследования возможностей системы остаточных классов удалось построить самокорректирующиеся коды пригодные для обнаружения и исправления ошибок возникающих не только при передаче информации, но и при арифметической обработке.

## 2 Постановка задачи

В настоящее время существует несколько алгоритмов, предназначенных для использования в области цифровой обработки сигналов. Здесь немалую роль играет система остаточных классов, основанная на элементарной теории чисел. Система остаточных классов обладает одной особенностью: нельзя визуально определить величину числа, представленного в системе остаточных классов, а следовательно затруднительно и выполнение таких операций, как сравнение чисел, определение знака числа. Одним из путей решения этой проблемы состоит в преобразовании чисел от позиционного представления чисел к остаткам и обратно из системы остаточных классов в позиционную систему счисления. Цель исследования – рассмотреть методы и алгоритмы перехода от позиционного представления к остаткам.

## 3 Основная часть

Перевод числа  $N$  из позиционной системы в систему остаточных классов может быть осуществлен с помощью набора констант, являющихся эквивалентами степеней (основание позиционной системы) в системе остаточных классов [1]. Нельзя визу-

определить величину числа, представленного в системе остаточных классов (СОК), а, следовательно, затруднительно и выполнение таких операций, как сравнение чисел, определение знака числа. Один из путей решения этой проблемы состоит в преобразовании чисел из позиционной системы в остаточную систему классов и обратно из СОК в позиционную систему счисления [2]. Оценим существующие способы перевода, как традиционные: методы перехода от позиционного представления к остаткам и обратно.

Обработка информации в цифровых устройствах, функционирующих в СОК, осуществляется с помощью модульных и немодульных операций. К модульным операциям относятся операции сложения, вычитания и умножения. Анализ применения арифметики СОК показывает, что их звенья имеют одинаковую структуру, типовым элементом которой является последовательность вида

#### 4 Анализ последних исследований и публикаций

Толчком к исследованиям в области непозиционных систем счисления послужили опубликованные в 1955-1957 гг работы чешских ученых М. Валаха и А. Свободы, посвященные представлению чисел в виде совокупности не отрицательных вычетов по группе взаимно простых оснований, и определившей в связи с этим представлением возможности выполнения рациональных операций без учета разрядных связей между цифрами числа. Проведенные авторами настоящей исследования в этой новой системе счисления, названной системой остаточных классов, привели к созданию машинной арифметики.

В процессе исследования возможностей системы остаточных классов удалось построить самокорректирующиеся коды пригодные для обнаружения и исправления ошибок возникающих не только при передаче информации, но и при ее арифметической обработке.

$$V = \left| \sum_{i=1}^K |F_i(\alpha_i)|_{p_i} \right|_{p_i} \quad (1)$$

где  $F_i(\alpha_i)$  - целочисленная функция вычета  $\alpha_i$  по некоторому модулю,  $p_i$  - основание СОК,  $|\dots|_{p_i}$  - операция определения наименьшего вычета по модулю  $p_i$

К немодульным операциям относятся операции, при которых значение того или иного результата разряда зависит от всех или нескольких разрядов исходного числа.

Устройства, реализующие немодульные операции, довольно чётко разделяются на 2 типа.

Примером устройства первого типа является устройство свёртки, обеспечивающее вычисление

$$V = \left| \sum_{i=1}^K |A_i Q_i|_{p_i} \right|_{p_i} \quad (2)$$

где  $A_i$  - значение  $i$ -го разряда исходного числа, представленного в позиционной системе счисления (ПСС);  $Q_i$  - весовой коэффициент.

Устройства свёртки широко используются в цифровых системах, функционирующих в СОК, представляющих существенную, а порой и основную часть оборудования, предназначенную для реализации ряда способов выполнения операций - перевода чисел из ПСС в СОК, деления произвольных чисел и некоторых других. Кроме того, такие устройства находят применение и в цифровых системах, функционирующих в ПСС.

Примером устройств второго типа является устройство позиционного преобразования, обеспечивающие получение характеристик, указывающих на принадлежность числа, представленного в СОК, тому или иному интервалу диапазона представимых чисел. Математической основой устройств первого типа является определение наименьших неотрицательных вычетов, которые определяются свёртками исходного числа по каждому модулю. Для определения свёрток по каждому модулю необходимо перевести число из позиционной системы счисления в систему остаточных классов.

Перевод числа в систему остаточных классов можно осуществить методом деления. Однако из-за операции деления техническая реализация такого метода не эффективна для машинного использования, кроме того, данный метод требует применения арифметического устройства в позиционной системе счисления.

Рассмотрим метод перевода числа из позиционной системы счисления в СОК, содержащий операции деления, называемый методом непосредственного суммирования модульных значений разрядов позиционного числа.

Пусть число  $X$  записано в позиционной системе счисления с основанием  $N$ , т.е.

$$X = A_k N^k + A_{k-1} N^{k-1} + \dots + A_0 N^0$$

или

$$X = \sum_{i=0}^k A_i N^i$$

где  $0 \leq A_i \leq N-1$ .

Представим степени основания  $N^i$  и коэффициенты  $A_i$  в системе остаточных классов с основаниями  $p_1, p_2, \dots, p_n$ , тогда

$$N^i = (B_1^{(i)}, B_2^{(i)}, \dots, B_n^{(i)}), \quad A^i = (A_1^{(i)}, A_2^{(i)}, \dots, A_n^{(i)}).$$

Подставим (4) в (3), получим

$$X = \left( \sum_{i=0}^{k-1} A_1^{(i)} B_1^{(i)} \bmod p_1, \sum_{i=0}^{k-1} A_2^{(i)} B_2^{(i)} \bmod p_2, \dots, \sum_{i=0}^{k-1} A_n^{(i)} B_n^{(i)} \bmod p_n \right)$$

Таким образом, для образования числа  $X$  в СОК требуется  $k$  констант, являющихся степенями  $p_i$  и  $p_i - 1$  констант, соответствующих значениям  $A_i$ .

Имея в памяти процессора массив из  $k + p_i - 1$  констант, весь перевод может быть осуществлён процессором, работающим в СОК.

Рассмотренный метод является основой широкого выбора возможных аппаратных реализаций цифровых преобразователей ПСС – СОК, которые различаются между собой как по составу и количеству используемых элементов, так и по скорости преобразования информации. Известные в литературе цифровые преобразователи ПСС – СОК, основанные на данном методе, анализ которых позволил сделать важные выводы о том, что одним из существенных недостатков подобных преобразователей являются большие аппаратные затраты при переводе чисел большой разрядности и низкое быстродействие. Повышенные требования, связанные с уменьшением аппаратных средств и увеличением скорости обработки информации, привели к необходимости глубокого изучения вопросов разработки эффективных алгоритмов. Для решения этой задачи предлагаются два метода. Рассмотрим первый метод. Для этого докажем следующую теорему, которая является основой нового метода преобразования чисел из ПСС в СОК как аппаратными, так и программными способами.

**Теорема.** Пусть число  $X$  записано в позиционной системе счисления с основанием  $N$  и если

$$X_n = \sum_{i=0}^r A_i^{(n)} C_i^{(n)}$$

где

$$C_i \equiv N^i \pmod{P_j}. \quad (6)$$

$P_j$  - простое число,  $r$  - число разрядов  $P_j$  (при  $j=1, 2, \dots, r$ ), то

$$X \equiv X_n \pmod{P_j} \text{ и } X_n < X \quad (7)$$

Доказательство.  $C_0 = 1$ ,  $C_1 = N^1 \pmod{P_j}$ ,  $\dots$ ,  $C_k = N^k \pmod{P_j}$ . Далее, подставляя значения выражений (6) в выражение (7), и учитывая свойства сравнений, получим

$$X = A_k N^k + A_{k-1} N^{k-1} + \dots + A_0 N^0 \equiv A_k C^k + A_{k-1} C^{k-1} + \dots + A_0 C^0 \pmod{P_j} \equiv X_1 \quad (8)$$

Рассмотрим второй метод, который нашёл широкое применение в литературе. Назовём его методом последовательного умножения и суммирования. Суть метода состоит в следующем. Пусть число записано в виде (3). Иначе это выражение можно записать

$$X = (\dots (A_k N + A_{k-1}) N + A_{k-2}) N + \dots + A_1) N + A_0 \equiv X_1 \pmod{P_j} = -\alpha_j \pmod{P_j}$$

$$(A_k N + A_{k-1}) N \equiv X_k \pmod{P_j},$$

$$(X_k \pmod{P_j} + A_{k-2}) N \equiv X_{k-1} \pmod{P_j} \quad (9)$$

$$(X_3 \pmod{P_j} + A_1) N \equiv X_2 \pmod{P_j},$$

$$(X_2 \pmod{P_j} + A_0) \equiv X_1 \pmod{P_j} = \alpha_j \pmod{P_j}$$

Т.е. значение числа  $X$  в СОК по модулю  $P_j$  образуется путём умножения старшего разряда на основание системы счисления  $N$ , затем суммирования полученного результата со значением следующего разряда по модулю  $P_j$ , затем умножения полученного результата на основание  $N$  по модулю  $P_j$ , а так последовательные умножения и суммирования по модулю производятся до тех пор, пока при суммировании не будет добавлено значение младшего разряда.

Следует отметить, что рассмотренный метод позволяет реализовать весьма экономичные, в смысле аппаратных затрат, цифровые устройства преобразования информации.

Метод восстановления числа по его остаткам был найден еще в Китае две тыс. лет назад. Основой этого метода является теорема, названная, поэтому Китайской теоремой об остатках (КТО).

**Теорема.** Пусть  $p_1, p_2, \dots, p_n$  попарно взаимно простые числа,

$$P = \prod_{i=1}^n p_i, m_1, m_2, \dots, m_n \text{ подобраны так, что } \frac{P}{p_i} m_i \equiv 1 \pmod{p_i}, A_0 = \sum_{i=1}^n \frac{P}{p_i} m_i a_i, i = 1, \dots, n.$$

Тогда решение системы,  $A \equiv \alpha_i \pmod{p_i}, i = 1, \dots, n$  будет иметь вид:  $A \equiv A_0 \pmod{P}$ .

Эта теорема лежит в основе метода ортогональных базисов при переводе из системы остаточных классов в позиционную систему счисления.

Пусть основания системы остаточных классов  $p_1, p_2, \dots, p_n$ .

$P = \prod_{i=1}^n P_i$  объем диапазона системы. С выбором системы определяются основные константы – базисы,  $B_i, i = 1, \dots, n$ . Задача перевода числа  $A = (\alpha_1, \alpha_2, \dots)$  в ПСС заключается в определении таких чисел  $M_i, i = 1, \dots, n$  чтобы  $A = \sum_{i=1}^n M_i B_i$  однозначного определения  $M_i$  на базисы системы  $B_i$  накладывается ряд ограничений. Показывается, что таким свойством обладают базисы  $B_1 = (1, 0, 0, \dots, 0, 0), B_2 = (0, 1, 0, \dots, 0, 0), \dots, B_n = (0, 0, 0, \dots, 0, 1)$ , называются ортогональными [3].

Тогда в случае ортогональных базисов  $M_i = \alpha_i, i = 1, \dots, n$ . Ортогональные базисы определяются по формуле

$$B_i = \frac{m_i P}{P_i} m_i P, i = 1, \dots, n,$$

где

$$P_i = \frac{P}{P_1 \cdot P_2 \cdot \dots \cdot P_{i-1} \cdot P_{i+1} \cdot \dots \cdot P_n}$$

$m_i$  – целые положительные числа, которые называются весами базисов, определяют из сравнений

$$P_i m_i \equiv 1 \pmod{P_i}$$

Тогда, по Китайской теореме, число

$$A = (\alpha_1, \alpha_2, \dots, \alpha_n) \equiv \sum_{i=1}^n \alpha_i B_i \pmod{P}$$

Таким образом, если найдены ортогональные базисы для системы оснований для перевода числа  $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$  достаточно вычислить  $\sum_{i=1}^n \alpha_i B_i$  и ввести сумму в диапазон  $[0; P)$  вычитанием величины, кратной  $P$ , т.е.

$$\tilde{A} = \left| \sum_{i=1}^n \alpha_i B_i \right| \pmod{P} = \sum_{i=1}^n \alpha_i B_i - r_A P \quad (4)$$

Где  $r_A$  – ранг числа  $A$ , показывающий сколько раз надо вычесть величину  $P$  из полученного числа, чтобы вернуть его в диапазон.

Пример. Пусть дана система оснований  $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7, P_5 = 11$ , с диапазоном  $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$ .  $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$  перевести число  $A = (1, 2, 1, 4, 7)$   $A = (2, 1, 4, 7)$  в позиционную систему.

Вычислим ортогональные базисы.

Для этого найдем величины  $P_i$ :

$$P_1 = \frac{P}{P_1} = 1155, P_2 = \frac{P}{P_2} = 770, P_3 = \frac{P}{P_3} = 462, P_4 = \frac{P}{P_4} = 330, P_5 = \frac{P}{P_5} = 210$$

Ищем веса базисов:

$$1155 m_1 \equiv 1 \pmod{2}, m_1 \equiv 1 \pmod{2}$$

$$770 m_2 \equiv 1 \pmod{3}, m_2 \equiv 2 \pmod{3}$$





```
Project2
* writeln(' ');
* writeln(' Metod perevoda iz sistemi ostatoshnix klassov ');
* writeln(' v pozis system shislenia ');
* writeln(' ');
* writeln(' Axmetova, ');
* writeln(' ');
* writeln(' Naushni rukovodit: ');
* writeln(' ');
* writeln(' Kapalova N.A. ');
* writeln(' ');
* writeln(' Nagmite klav <Enter> ');
* writeln(' ');
* writeln(' ');
* writeln(' Progr proizvodit perevod shisla ');
* writeln(' A=(a1, a2, ..., an), predstavlenno v SOR c osnovaniami ');
* writeln(' p1, p2, ..., pn takimi, shto p1 < p2 < ... < pn i p(i) - prostie ');
* writeln(' shisla, v pozision systemu shislenia metodom, ');
* writeln(' osnovannik na primeneni funktsii Eilera. ');
* writeln(' Metod zakluch v sled: dlia shisla A v ');
* writeln(' pozis sys shislenia berutsa 2 modula: p(1) i p(i+1), ');
* writeln(' p(i) > p(i-1), i sootv ostatki a(i) i a(i+1). ');
* writeln(' Naxoditsa naimen neotr vishet po modul ');
* writeln(' p(i) * p(i+1). Primenaa etu oper mnogokpat i perehodia ');
* writeln(' k sostav moduliam, osushestv perevod shisel. ');
* writeln(' ');
* writeln: writeln: writeln:

```

[Hint] Project2.dpr(10): Variable 'i' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'b' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'c' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'T' is declared but never used in Project2

```
Project2
* writeln: writeln: writeln:
* writeln(' Nagmite <Enter>... ');
* readln;

end; (vishitka)
(Вывисление на экраны монитора результатов вычисления)
procedure vich (var v:longint; a,m:longint);
begin if a<0 then v:=a*m else v:=a mod m
end; (vich)
(Тест простого числа)
function test (ch:longint):boolean;
var i:longint;
begin i:=2;
while (i<=ch) and ((ch mod i)<>0) do
i:=i+1+(i mod 2);
if i=ch then test:=true else test:=false;
end; (test)
(Ввод данных)
procedure DataEnter;
var i:longint;
begin
write('Vvedite shislo modilei:');
readln(m);
writeln('Vvod znashenia modula: (p(1)<=30, p(1)- prostie, ');
writeln('p(1) < p(i+1): ');

```

[Hint] Project2.dpr(10): Variable 'i' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'b' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'c' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'T' is declared but never used in Project2



```
Delphi 7 - Project2  
File Edit Search View Project Run Component Database Tools Window Help  
Standard | Additional | Win32 | System | Data Access | Data Controls | dbExpress | DataSnap | BDE | ADO | InterBase | WebServices | Inter...  
Project2  
Procedures  
Types  
Variables/Constants  
Uses  
a(1):=x;  
end  
end; (CalcX)  
begin  
repeat  
  
vishka;  
datacenter;  
calcX(N,p,a);  
writeln('A= ',x);  
writeln('Povtorit? (y/n): ');  
readln(r);  
until (r = 'n')  
  
{ TDDC -oUser -cConsole Main : Insert code here }  
end.  
25 14 Insert \Code/  
[Hint] Project2.dpr(10): Variable 'r' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'b' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 'c' is declared but never used in Project2  
[Hint] Project2.dpr(10): Variable 't1' is declared but never used in Project2  
Build  
16:57 14.06.2016
```

C:\Program Files\Borland\Delphi7\Projects\Project2.exe  
Ei, p2,E,pn takimi, shcho Ei< p2<E<pn i p(i) - prostie  
shisla, v posision systemu shislenia metodom,  
osnovannim na primenenii funktsii Eilera.  
Metod zaklush v sled: dlia shisla n v  
pozis sys shislenia berutsa 2 modula:p(i) i p(i+1),  
p(i) > p(i+1), i sootv ostatki p(i) i p(i+1).  
Naxoditsa naimen neotr vishet po modul  
p(i) \* p(i+1). Primena etu oper mnogokpat i perexodia  
k sostav modulian, osushestv perevod shisel.  
  
Nagnite <Enter>...  
Vvedite shislo modilei:2  
Vvod znachenia modulei (p(i)<=30, p(i)- prostie,  
p(i)<p(i+1)):  
Modul p1= 17  
Modul p2= 19  
Vvod shisla SOK (a(i))=0 i a(i)<p(i)):  
a11=2  
a12=3  
n= 155  
Povtorit? (y/n):

```

osnovannin na prinenenii funktsii Eilera.
Metod zakluch v sled: dlia shisla n v
pozis sys shislenia berutsa 2 modula: p(i) i p(i+1).
p(i) > p(i+1), i sooto ostatki p(i) i p(i+1).
Naxoditsa naimen neotr vishet po modul
p(i) * p(i+1). Prinena etu oper mnogokrat i perexodia
k sostav modulian, osushesto perevod shisel.

Nagnite <Enter>...

Uvedite shislo modilei:3
Uvod znashenia modulei (p(i)<=30, p(i)- prostie,
p(i)<p(i+1)):
Modul p1= 2
Modul p2= 3
Modul p3= 5
Uvod shisla SOK (a(i))=0 i a(i)<p(i)):
a[1]=1
a[2]=2
a[3]=4
n= 29
Povtorit? (y/n):
    
```

### Список литературы

1. Бухштаб А. А. Теория чисел – М: Наука, 1975 г.
2. Айерленд К. Классическое введение в современную теорию чисел. М: Мир, 1987.
3. Акушинский И. Л., Юдицкий Д. И. Машинная арифметика в остаточных классах. – М. Советское радио, 1968.
4. Червяков Н. И. Применение системы остаточных классов в цифровых системах обработки и передачи информации. – Ставрополь: СВВиУС, 1984.