15

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

25 лет
Независимости
Республики Казахстан

IICT

25 ЛЕТ

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

Содержание

МЕТОДЫ И АЛГОРИТМЫ ПЕРЕХОДА ОТ ПОЗИЦИОННОГО ПРЕДСТАВЛЕНИЯ К ОСТАТКАМ

Ахметова А.М., Нугманова С.А.
e-mail: ardak_66@mail.ru, nugm_s@mail.ru

Институт информационных и вычислительных технологий КН МОН РК
Казахстан

Аннотация. *Система остаточных классов обладает одной особенностью, которую 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 базисов, Китайская теорема, базисы системы, диапазон, позиционная система, алгоритм, обобщенная 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. Свобода, 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 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 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 система остаточных классов, а следовательно затруднительно и выполнение таких операций, как сравнение чисел, определение знака числа. Один из путей решения этой проблемы состоит в преобразовании чисел от позиционного представления чисел к остаткам и обратно из системы остаочных 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 визуально

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 исследования 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 определившейся 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.

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

где $F_i(\alpha_i)$ - целочисленная функция вычета α_i по некоторому модулю, p_i – основание СОК, $|\ldots|_{p_i}$ - 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

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

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 преобра
ния, обеспечивающие получение характеристик, указывающих на принадлежность
ла, представленного в СОК, тому или иному интервалу диапазона представимых чис
Математической основой устройств первого типа является определение наим
ших неотрицательных вычетов, которые определяются свёртками исходного чис
каждому модулю. Для определения свёрток по каждому модулю необходимо пере
число из позиционной системы счисления в систему остаточных классов.

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

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

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

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

или

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

где $0 \le A_i \le N-1$.

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

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

Подставим (4) в (3), получим

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

Таким образом, для образования числа X в СОК требуется k констант, являю
ся степенями p_1 и $p_i - 1$ констант, соответствующих значениям A_i.

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

Рассмотренный метод является основой широкого выбора возможных аппарат
ных реализаций цифровых преобразователей ПСС – СОК, которые различаются меж
собой как по составу и количеству используемых элементов, так и по скорости пре
разования информации. Известные в литературе цифровые преобразователи ПСС
СОК, основанные на данном методе, анализ которых позволил сделать важные выво
о том, что одним из существенных недостатков подобных преобразователей являю
большие аппаратурные затраты при переводе чисел большой разрядности и низ
быстродействие. Повышенные требования, связанные с уменьшением аппаратурн
средств и увеличением скорости обработки информации, привели к необходимос
глубокого изучения вопросов разработки эффективных алгоритмов. Для решения э
задачи предлагаются два метода. Рассмотрим первый метод. Для этого докажем сле
ющую теорему, которая является основой нового метода преобразования чисел из П
в СОК как аппаратурными, 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

$$C_i \equiv N^i \left(mod\, P_j\right). \tag{6}$$

а P_j - простое число, r – число разрядов P_j (при j= 1, 2,…,r), то

$$X \equiv X_n \left(mod\, p_j\right) \text{ и } X_n < X \tag{7}$$

Доказательство. $C_0 = 1$, $C_1 = N^i \left(modP_j\right), \ldots C_k = N^k \left(modP_j\right)$. Далее, подставляя значения выражений (6) в выражение (7), и учитывая свойства сравнений, получим

$$X = A_k N^k + A_{k-1} N^{k-1} + \ldots + A_0 N^0 \equiv A_k C^k + A_{k-1} C^{k-1} + \ldots A_0 C^0 (modP_j) \equiv X_1 \tag{8}$$

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

$$X = \left(\ldots\left(A_k N + A_{k-1}\right) N + A_{k-2}\right) N + \ldots + A_1) N + A_0 \equiv X_1 modP_j = -\alpha_j modP_j$$

$$\left(A_k N + A_{k-1}\right) N \equiv X_k \left(modp_j\right),$$

$$\left(X_k modP_j + A_{k-2}\right) N \equiv X_{k-1} \left(modp_j\right) \tag{9}$$

$$\left(X_3 modP_j + A_1\right) N \equiv X_2 (modp_j),$$

$$\left(X_2 modP_j + A_0\right) \equiv X_1 modp_j = \alpha_j modp_j$$

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 аппаратурных 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 $p_1, p_2, \ldots, p_n$ попарно взаимно простые числа, $P = \prod_{i=1}^{n} P_i, m_1, m_2, \ldots, m_n$ подобраны так, что $\frac{P}{P_i} m_i \equiv 1 \left(modp_i\right)$, $A_0 = \sum_{i=1}^{n} \frac{P}{p_i} m_i a_i$, $i = 1,\ldots,n$. Тогда решение системы, $A \equiv \alpha_i \left(modP_i\right)$, $i = 1, \ldots n$ будет иметь вид: $A \equiv A_0 (modP)$.

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

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

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

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

$$B_i=\frac{m_iP}{P_i}m_iP_i, i=1,\ldots,n \ ,$$

где

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

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

$$P_im_i\circ 1(mod\,P_i)$$

Тогда, по Китайской теореме, число

$$A=(\alpha_1,\alpha_2,\ldots\alpha_n)\equiv\sum_{i=1}^{n}\alpha_iB_i(modP)$$

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

$$A=\left|\sum_{i=1}^{n}\alpha_iB_i\right| \ P=\sum_{i=1}^{n}\alpha_iB_i-r_AP \qquad (4)$$

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

Пример. Пусть дана система оснований $P_1=2,P_2=3,P_3=5,P_4=7,P_5=11$, об диапазона $P=2\cdot3\cdot5\cdot7\cdot11=2310$. P = 2·3·5·7·11 перевести число A = (1,2,1,4.7) A = 2, 1, 4, 7) в позиционную систему.

Вычислим ортогональные базисы.

Для этого найдем величины P:

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

Ищем веса базисов:

$1155^{m_1}\circ 1(mod2), \ m_1\circ 1(mod2)$

$770^{m_2}\circ 1(mod3), m_2\circ 2(mod3)$

$462^{m_1} \circ 1 (mod 5)$, $m_3 \circ 3 (mod 5)$

$330^{m_4} \circ 1 (mod 7)$, $m_4 \circ 1 (mod 7)$

$210^{m_5} \circ 1 (mod 11)$, $m_5 \circ 1 (mod 11)$

Тогда получаем сами базисы:

$B_1 = m_1 \cdot P_1 = 1 \cdot 1155 = 1155$,

$B_2 = m_2 \cdot P_2 = 2 \cdot 770 = 1540$,

$B_3 = m_3 \cdot P_3 = 3 \cdot 462 = 1386$,

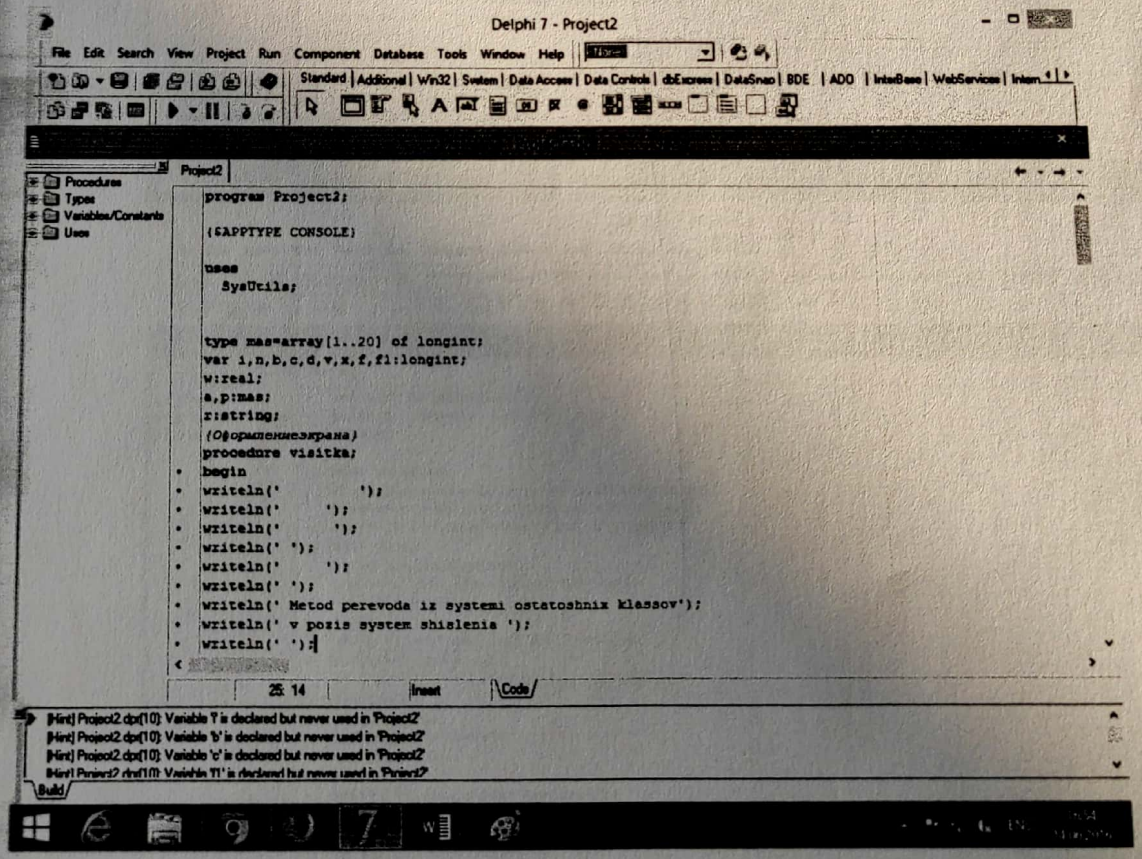
$B_4 = m_4 \cdot P_4 = 1 \cdot 330 = 330$,

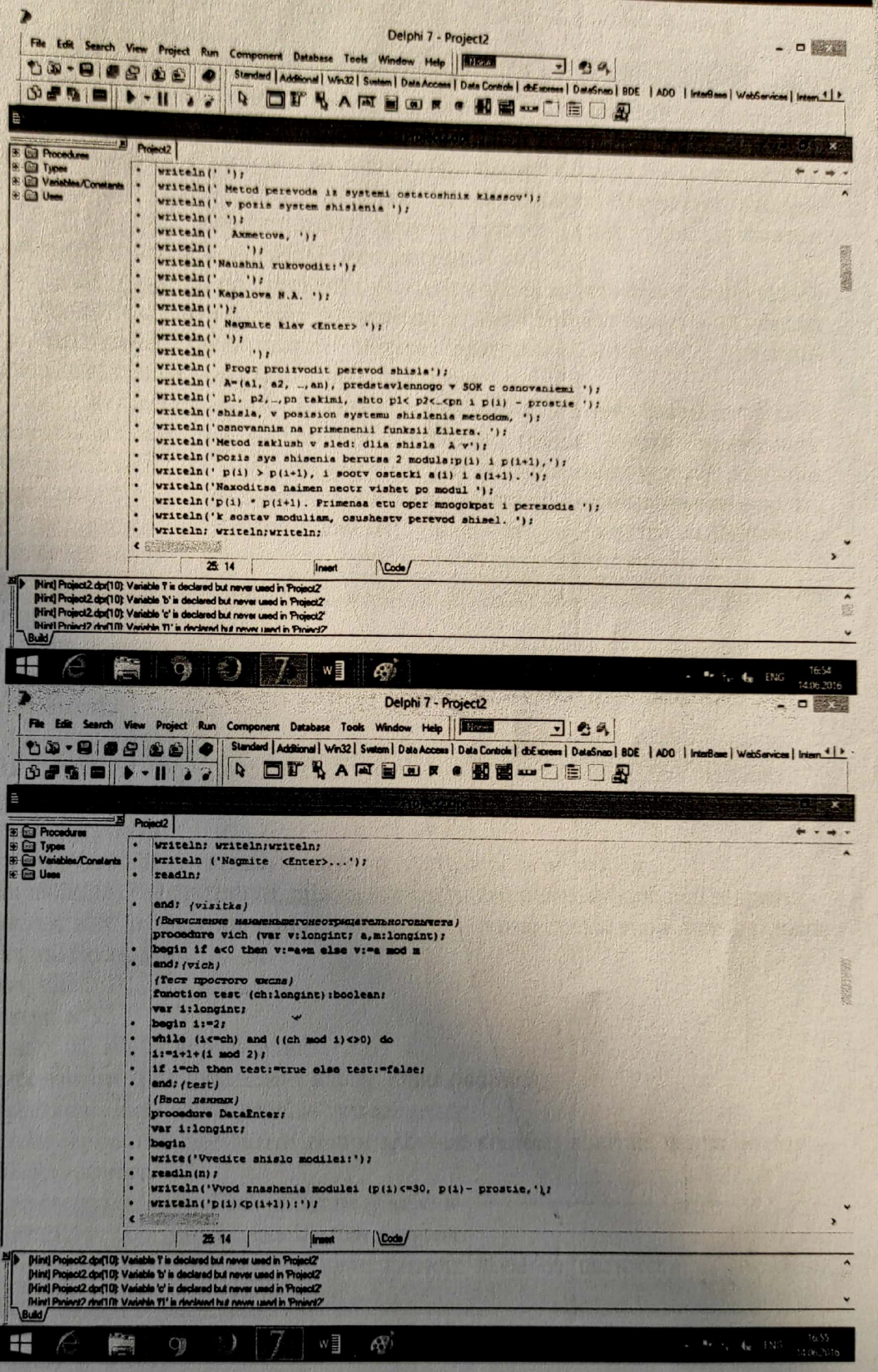
$B_5 = m_5 \cdot P_5 = 1 \cdot 210 = 210$

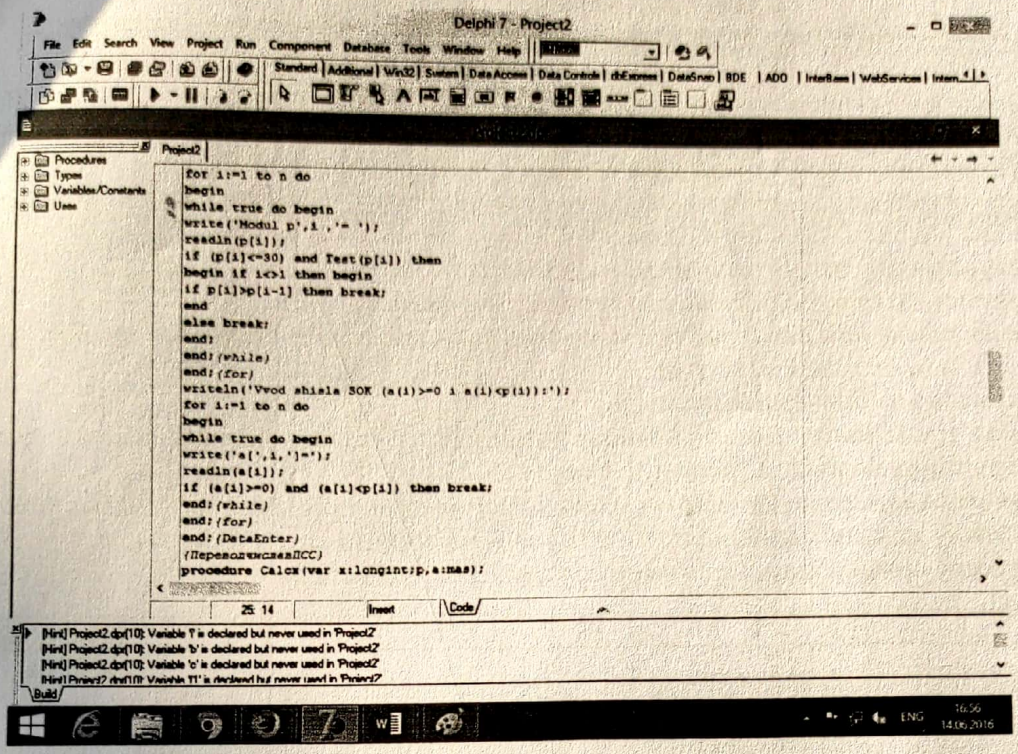
Вычислим величину числа A:

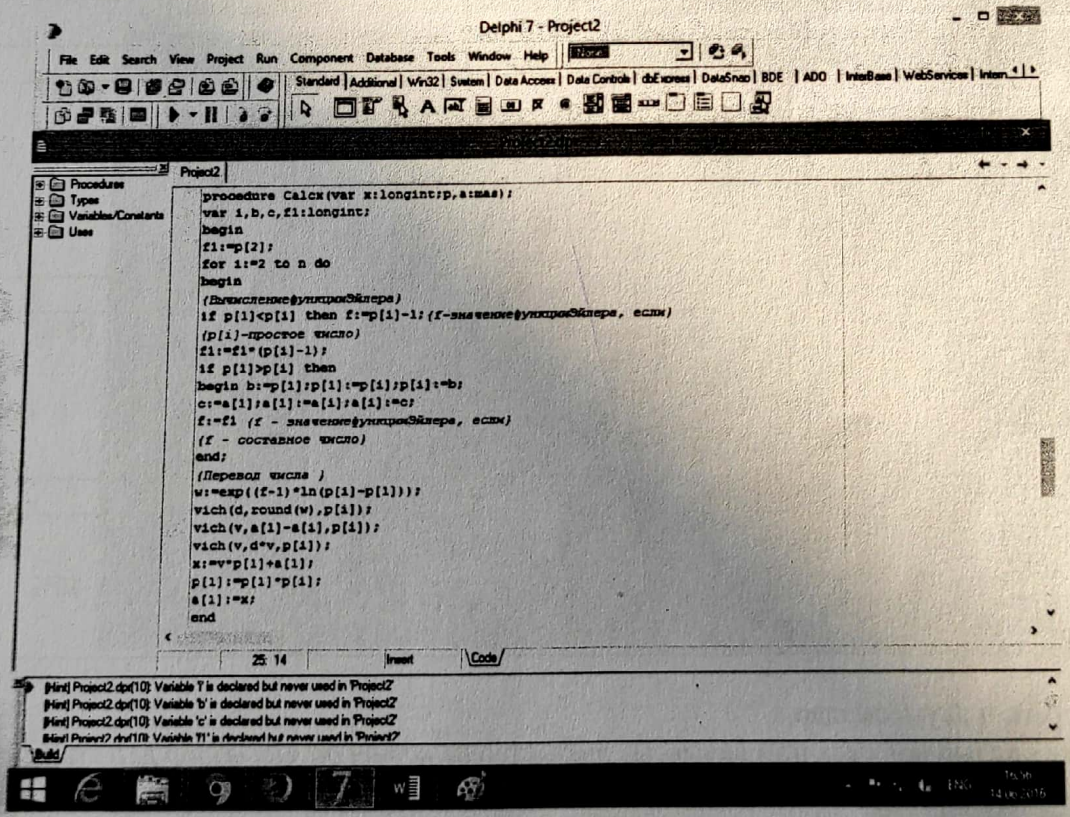
$$A = |1 \cdot 1155 + 2 \cdot 1540 + 1 \cdot 1386 + 4 \cdot 330 + 7 \cdot 210|_{2310} = |8411|_{2310} = 1481.$$

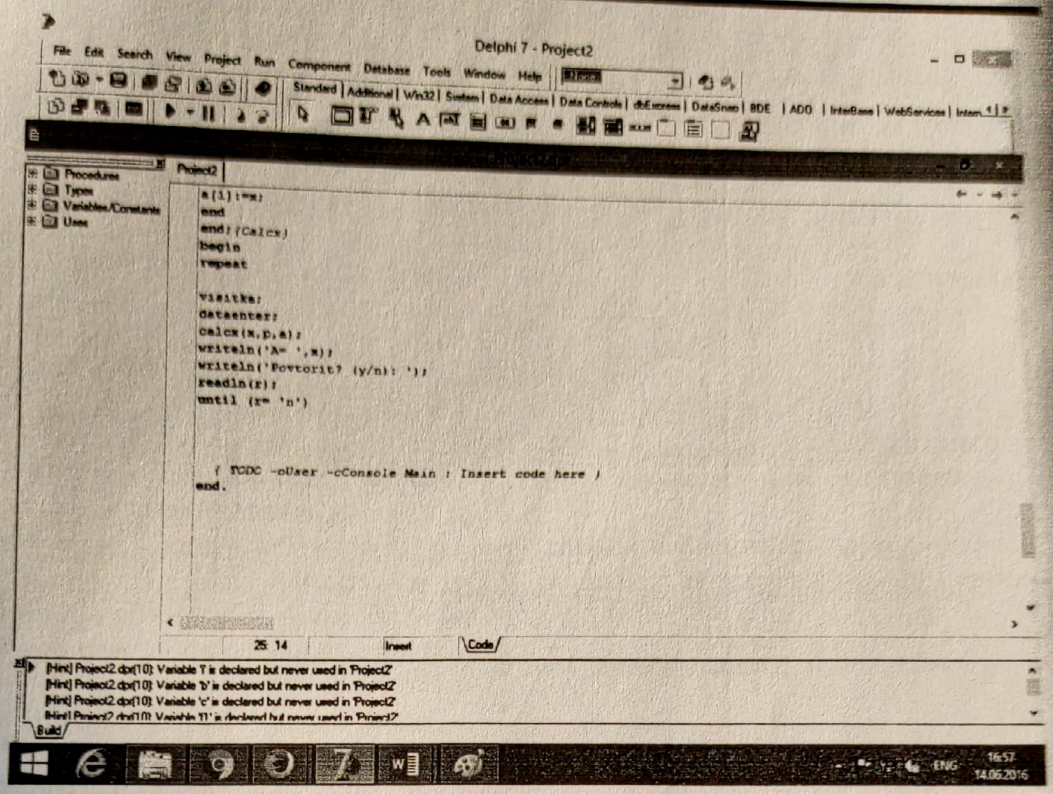
Получены результаты составленной программы перевода чисел из системы остаточных классов в позиционную систему.

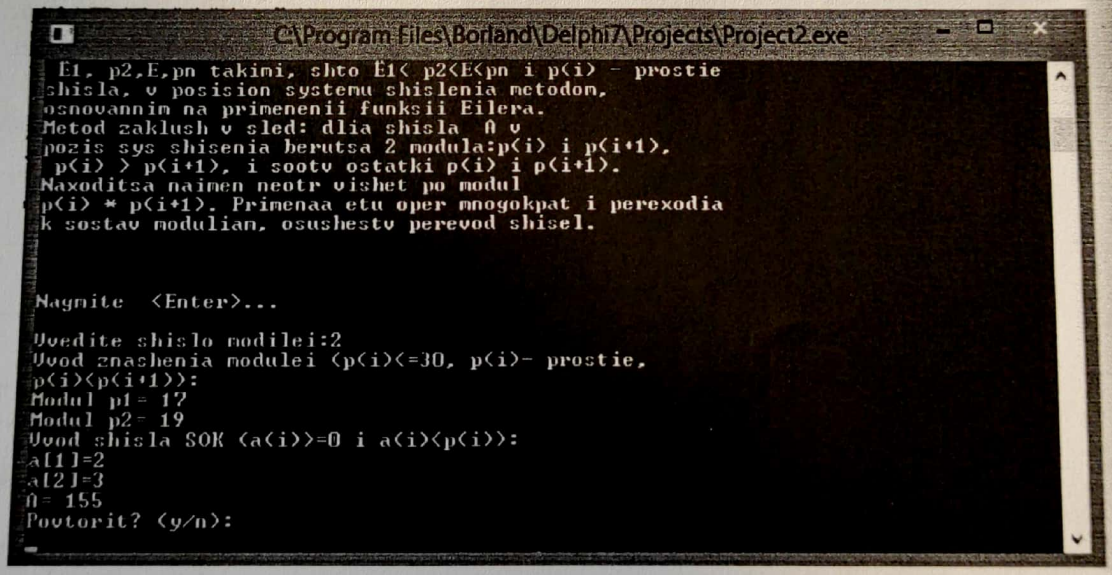


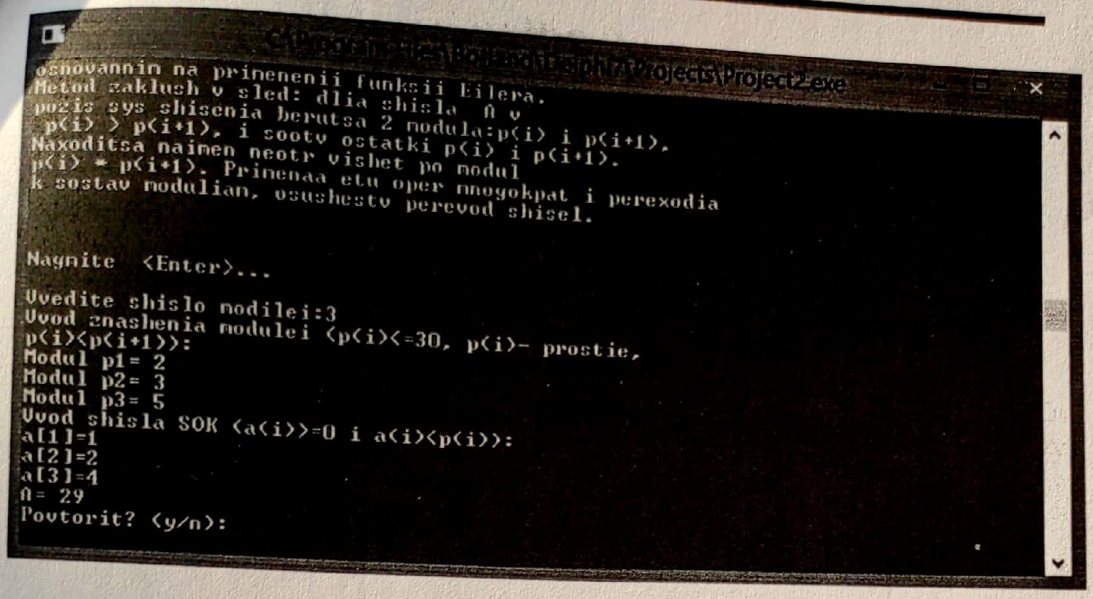












Список литературы

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.