МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

**«Вятский государственный университет»**

**(ФГБОУ ВО «ВятГУ»)**

Факультет автоматики и вычислительной техники

Кафедра электронных вычислительных машин

Система остаточных классов

Отчет

Лабораторная работа №2 по дисциплине

«Основы информатики»

Выполнил студент группы ИВТб-11 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Жеребцов К. А./

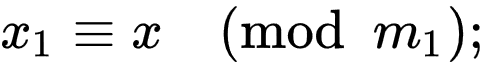
Проверил преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Исупов К. С./

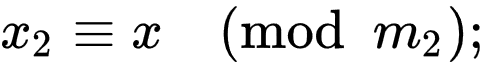
***Цель работы:*** изучить систему остаточных классов, основанную на понятии вычета и китайской теореме об остатках. Приобретение навыков выполнения операций в системе остаточных классов.

***Теория:***

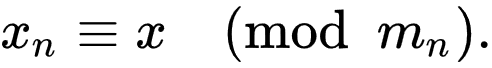
Система остаточных классов (СОК) — система счисления, основанная на модулярной арифметике.

Представление числа в системе остаточных классов основано на понятии вычета и китайской теореме об остатках. СОК определяется набором попарно взаимно простых модулей (m1,m2,…,mn). M=m1\*m2\*…\*mn, так, что каждому целому числу x из отрезка [0;M-1] ставится в соответствие набор вычетов (x1,x2,…,xn), где





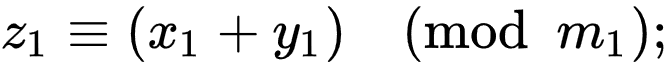


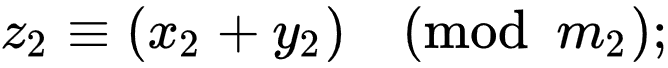


Преимущества системы остаточных классов:

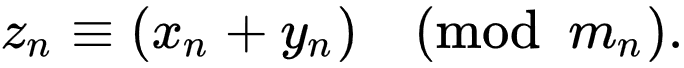
В СОК арифметические операции (сложение, вычитание, умножение, деление) выполняются покомпонентно, если про результат известно, что он является целочисленным и также лежит в [0;M-1].

Формула для сложения: (x1,x2,…,xn)+ (y1,y2,…,yn)= (z1,z2,…,zn), где









Аналогично выполняются вычитание, умножение и деление. Замечание: на деление накладываются дополнительные ограничения. Деление должно быть целочисленным, то есть делитель должен нацело делить делимое. Делитель должен быть взаимо-простым со всеми модулями базиса.

Недостатки системы остаточных классов:

1. отсутствие эффективных алгоритмов для сравнения чисел; обычно, сравнение осуществляется через перевод аргументов из СОК в систему счисления (полиадическую) со смешанными основаниями: 
2. медленные алгоритмы взаимного преобразования представления чисел из позиционной системы счисления в СОК и обратно;
3. сложные алгоритмы деления (когда результат не является целым);
4. трудность в обнаружении переполнения.

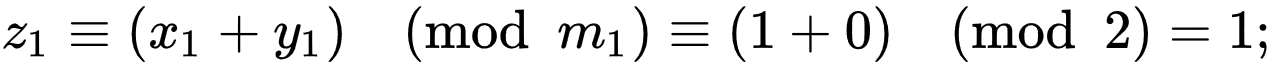
Пример:

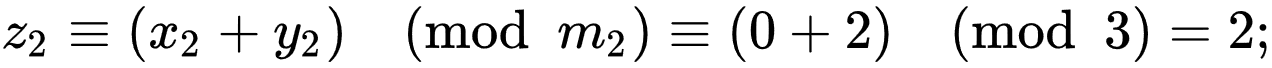
Рассмотрим СОК с базисом (2;3;5). В этом базисе можно взаимно-однозначно представить числа из промежутка от 0 до 29, так как M=2\*3\*5=30. Таблица соответствия чисел из позиционной системы счисления и системы остаточных классов:

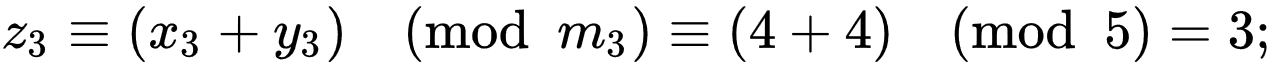
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| {\displaystyle 0=(0;0;0)} | {\displaystyle 1=(1;1;1)} | {\displaystyle 2=(0;2;2)} | {\displaystyle 3=(1;0;3)} | {\displaystyle 4=(0;1;4)} |
| {\displaystyle 5=(1;2;0)} | {\displaystyle 6=(0;0;1)} | {\displaystyle 7=(1;1;2)} | {\displaystyle 8=(0;2;3)} | {\displaystyle 9=(1;0;4)} |
| {\displaystyle 10=(0;1;0)} | {\displaystyle 11=(1;2;1)} | {\displaystyle 12=(0;0;2)} | {\displaystyle 13=(1;1;3)} | {\displaystyle 14=(0;2;4)} |
| {\displaystyle 15=(1;0;0)} | {\displaystyle 16=(0;1;1)} | {\displaystyle 17=(1;2;2)} | {\displaystyle 18=(0;0;3)} | {\displaystyle 19=(1;1;4)} |
| {\displaystyle 20=(0;2;0)} | {\displaystyle 21=(1;0;1)} | {\displaystyle 22=(0;1;2)} | {\displaystyle 23=(1;2;3)} | {\displaystyle 24=(0;0;4)} |
| {\displaystyle 25=(1;1;0)} | {\displaystyle 26=(0;2;1)} | {\displaystyle 27=(1;0;2)} | {\displaystyle 28=(0;1;3)} | {\displaystyle 29=(1;2;4)} |

*Пример сложения:*

Сложим два числа 9 и 14 в базисе (2;3;5). Их представление в заданном базисе 9=(1;0;4) и 14=(0;2;4) (см. табличку выше). Воспользуемся формулой для сложения: (z1,z2,z3) =(1,0,4)+(0,2,4)



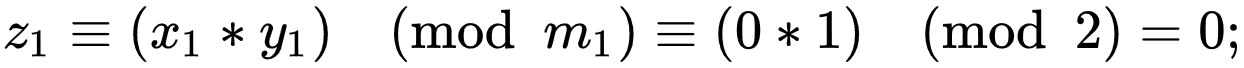


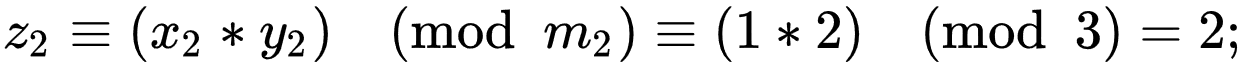


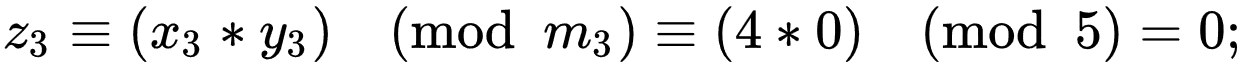
(z1,z2,z3) = (1,2,3) - по таблице убеждаемся, что результат равен 23.

*Пример умножения:*

Умножим два числа 4 и 5 в базисе (2;3;5). Их представление в заданном базисе 4=(0;1;4) и 5=(1;2;0) (см. табличку выше). Воспользуемся формулой для умножения: (z1,z2,z3)=(0,1,4)\*(1,2,0)







(z1,z2,z3) = (0,2,0) - по таблице убеждаемся, что результат равен 20.

Замечание: если бы мы умножали или складывали числа, которые дали в результате умножения число больше или равное M=30, то полученный результат RES = REAL(mod M), где REAL — результат операции в позиционной системе счисления.

***Задание:*** закрепить пройденный материал, выбрать свой набор модулей, рассчитать все необходимые константы и произвести необходимые операции.

***Решение:***

Рассмотрим СОК с базисом (2;3;7)}. В этом базисе можно взаимно-однозначно представить числа из промежутка от 0 до 42, так как M=2\*3\*7=42.

Целое число в СОК представляется в виде последовательности: X=(x1,x2,…,xn), где xi= X mod mi.

Таким образом,

X=8=(8 mod 2, 8 mod 3, 8 mod 7)=(0,2,1)

Y=10=(10 mod 2, 10 mod 3, 10 mod 7)=(0,1,3).

1. Выполним сложение

Z1=X+Y=(0+0 mod 2,2+1 mod 3,1+3 mod 7)=(0,0,4)

1. Выполним вычитание

Z2=X-Y=(0-0 mod 2, 2-1 mod 3, 1-3 mod 7)=(0,1,5)

Z4=Y-X=(0-0 mod 2, 1-2 mod 3 3-1 mod 7)=(0,2,2)

1. Выполним умножение

Z3=X\*Y=(0\*0 mod 2,2\*1 mod 3,1\*3 mod 7)=(0,2,3).

Если X\*Y=8\*10=80, а M=42, то Z3= 80 mod 42= 38=

=(38 mod 2, 38 mod 3,38 mod 7)=(0,2,3)

1. Выполним преобразование из СОК в позиционную систему:

M1=42/2=21 w1=21 mod 2 = 1

M2=42/3=14 w2=14 mod 3 = 2

M3=42/7=6 w3=6 mod 7 = 6

Z1=(0,0,4)=|0\*21\*1+0\*14\*2+4\*6\*6|42=144 mod 42=18

Z2=(0,1,5)=-|M-Z2|42=-|2-0,3-1,7-5|42=-|2,2,2|42=-|2\*21\*1+2\*14\*2+2\*6\*6|42=

=-(170 mod 42)=-2

Z3=(0,2,3)=|0\*21\*1+2\*14\*2+3\*6\*6|42=164 mod 42=38

Z4=(0,2,2)=|0\*21\*1+2\*14\*2+2\*6\*6|42=128 mod 42=2

***Вывод:***

В ходе лабораторной работы был закреплен пройденный материал, путем выбора своих модулей и выполнения всех необходимых операций, а именно нахождения всех констант, выполнения сложения, вычитания и умножения, перевода из позиционной системы счисления в систему остаточных классов и обратно.