***Дискретная Математика и Теоретическая Информатика (ДМиТИ)***

**Раздел II. Теория Чисел.**

Тема: Сравнение по модулю. Системы сравнений.

***Сравнение по модулю***

**Опр.1** *p****∈*** *-* простое, если *p = a\*b* ()⇒ (данная скобка означает ИЛИ).  
Лемма a\*b p (p-простое) ⇒

Теорема (Основная теорема арифметики)  
 Такое представление единственно с точностью до порядка множителей.  
(Любое положительное число может быть представлено в виде произведения простых чисел)  
  
Примеры:

**Опр.2**   
*a* сравнимо с *b* по модулю *m*, если

Утверждение.1 Свойства:  
(1) – транзитивность  
(2.1)   
(2.2)   
(2.3)

**Опр.3** **Класс вычетов** числа *a* по модулю *m* это

Утверждение.2 Классы вычетов чисел *a* и *b* по модулю *m* либо совпадают, либо не пересекаются.  
**Опр.4** (аналогично для «-» и «\*»).  
Опр.5   
Пример:

Теорема

Множество классов вычетов mod m с введёнными операциями являются коммутативным кольцом, то есть:  
(1) и – **коммутативность**  
(2) – **ассоциативность**  
(3) – **нейтральный элемент**  
(4) – **обратимый элемент**  
(5) – **ассоциативность**   
(6)   
(7)(8) (7)-(8) – **дистрибутивность**  
  
Теорема  
.

Теорема

Пример №1:

Вычислить 30/63 в кольце вычетов по модулю 92.

***Способ I.***  
Ответ:

***Способ II.***

И решаем с помощью РАЕ

|  |  |  |  |
| --- | --- | --- | --- |
| 92  63 |  | 0  1 | 1  0 |
| 29 | 1 | -1 | 1 |
| 5 | 2 | 3 | -2 |
| 4 | 5 | -16 | 11 |
| 1 | 1 | 19 | -13 |
| 0 | 4 | -92 | 63 |

Ответ:

***Системы сравнений***

Теорема КТО (Китайская теорема об остатках)

Пусть – попарно взаимно простые натуральные числа (т.е. при ) и . Тогда, каковы бы ни были целые числа , система сравнений

Имеет единственное решение , где , и

Пример №2:

Найти наименьшее натуральное число x, удовлетворяющее условиям:

*1-действие*

Упростили произведение модулей:

42 мы получили просто (3\*13+3)

*2-действие*

*3-действие*

сократили 15 и 12 на 3

*4-действие*

*. -* Ответ