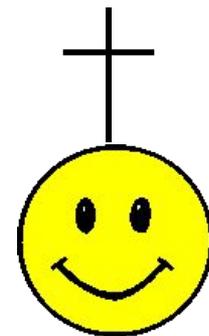




УРОК 2



Классы вычетов

n=5k+2 $n^4 - n$

2	14
7	2394
12	20724
17	83504
22	234234
27	531414
32	1048544
37	1874124
42	3111654
47	4879634
52	7311564
57	10555944
62	14776274
67	20151054
72	26873784
77	35152964

n=5k+3

$n^4 - n$

3	78
8	4088
13	28548
18	104958
23	279818
28	614628
33	1185888
38	2085098
43	3418758
48	5308368
53	7890428
58	11316438
63	15752898
68	21381308
73	28398168
78	37014978

Классом вычетов по модулю m называют множество чисел, дающих одинаковые остатки при делении на m .

Класс вычетов определяется любым его представителем.

Сравнения по модулю m .

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b \pmod{m}$$

T1.

Число a сравнимо с b по модулю m тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b(\text{mod } m)$$

T2. Рефлексивность отношения сравнимости.

$$a \equiv a(\text{mod } m)$$

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b(\text{mod } m)$$

ТЗ. Симметричность отношения сравнимости:

$$a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$$

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b(\text{mod } m)$$

T4. Транзитивность отношения сравнимости :

$$a \equiv b(\text{mod } m) \wedge b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m)$$

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b(\text{mod } m)$$

T5. Если $a \equiv b(\text{mod } m)$ и k -произвольное целое число, то

$$ka \equiv kb(\text{mod } m)$$

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b \pmod{m}$$

Т8.

$$a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow$$

$$\left. \begin{array}{l} a - c \equiv b - d \pmod{m} \\ a + c \equiv b + d \pmod{m} \end{array} \right\}$$

Т 9. К обеим частям сравнения можно прибавить или вычесть одно и то же число

Определение.

Числа a и b называют сравнимыми по модулю m , если их разность делится на m

$$a - b \square m \Rightarrow a \equiv b(\text{mod } m)$$

Т.13 В любой части сравнения можно отбросить или добавить слагаемое, кратное модулю.

$$a \equiv b(\text{mod } m) \Rightarrow a + km \equiv b(\text{mod } m)$$

