Шинко Андрей

МИКОЗИ

Лабораторная работа №0

18.02

Вариант 4

№1

Найти остаток от деления $M = 5^{111}$ и $N = 16$

$$5^{111} \equiv 5 \cdot 5^{110} \equiv 5 \cdot 25^{55} \equiv [25 \equiv -7 \pmod{16}] \equiv$$

$$\equiv 5 \cdot (-7)^{55} = -35 \cdot 49^{27} \equiv -3 \cdot 1^{27} \equiv -3 \equiv$$

$$\equiv 13 \pmod{16}$$

$a \equiv b \pmod{m}$

$(a - b) = \vdots 4$

1. $a \pm c \equiv b \pm d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^t \equiv b^t \pmod{m}$

№2

Найти знач. ф-ии Эйлера $\varphi(n)$.

$n = 1562$

$$\varphi(1562) = \varphi(2 \cdot 11 \cdot 71) = (2-1)(11-1)(71-1) =$$

$$= 700.$$

$\varphi(m)$ – кол-во нат. чисел, $\leq m$ и взаимнопростые с m.

$\varphi(m) = |\mathbb{Z}_m^*|$

1. p-и простое $\Rightarrow \varphi(p^s) = p^s - p^{s-1}$
2. НОД $(a, b) = 1$ $\Rightarrow \varphi(a, b) = \varphi(a)\,\varphi(b)$

№3

Найти $a^{-1} \pmod n$, где $a=5$, $n=16$

$5^{-1} \pmod{16} \equiv \left[\varphi(16)=\varphi(2^4)=2^4-2^3=8\right] \equiv$

$\equiv 5^7 \equiv 5 \cdot 25^3 \equiv 5(-7)^3 \equiv -35\ 49 \equiv$

$\equiv -3 \cdot 1 \equiv 13 \pmod{16}$

Если $НОД(a,m)=1$, то

$a^{\varphi(m)} \equiv 1 \pmod m$

$a^{-1} \pmod m \equiv a^{\varphi(m)-1} \pmod m$

№4

С помощью расшир. алгор. Евклида найти $НОД(a,b)$, и x, y

$ax+by = НОД(a,b)$. Реш. должно быть несколько.

$a=34 \quad b=70$

I сп.

$НОД(34,70) = НОД(2,34) = НОД(\ 2) = 2$

$НОД(34,70) = 2$

$НОД(a,b) = НОД(b\%a, a)$

до тех пор пока $НОД(0,a)=a$

II сп.

$70 = 34 \cdot 2 + 2$

$34 = 2 \cdot 17 + 0$

$b = aq + r$

$x_0=0,\ x_1=1$

$y_0=1,\ y_1=0$

$x_i = x_{i-2} - q_{i-1} \cdot x_{i-1}$

$(-11-y)$

Тогда $-2 \cdot 34 + 1 \cdot 70 = 2$

$x_0=0,\ x_1=1$

$y_0=1,\ y_1=0$

$x_2 = 0 - 2 \cdot 1 = -2$

$x_3 = 1 - 17(-2) = 35$

$y_2 = 1 - 2 \cdot 0 = 1$

$y_3 = 0 - 17 \cdot 1 = -17$

Ответ: $x=-2,\ y=1,\ НОД=2$