Семинар

1) Образуют ли числа $2^0, 2^1, 2^2, \ldots, 2^{12}$ полную систему вычетов по модулю 13?

2) Вычислить:
$\varphi(7^3)$, $\varphi(8!)$, $\varphi(240240)$

3) Решить сравнения:

$13x \equiv 10 \mod 15$

$16x \equiv 7 \mod 26$

$12x \equiv 18 \mod 22$

$12x \equiv 8 \mod 24$

4. Доказать, что уравнение $3x^2 + 2 = y^2$ неразрешимо в целых числах

5 Доказать, что если p - простое, то: $(p-1)! \equiv -1 \mod p$

$$\varphi(7^3) = 7^3 - 7^2 = 7^2(7-1) = 7^2 \cdot 6 = 496$$
$$= 294$$

$$\varphi(p^n) = p^n - p^{n-1}$$

$$\varphi(8!) = \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot \overset{2\cdot 3}{6} \cdot 7 \cdot 8) =$$

$$= \varphi(2 \cdot 2^2 \cdot 2 \cdot 2^3 \cdot 3^2 \cdot 5 \cdot 7) = \varphi(2^7 \cdot 3^2 \cdot 5 \cdot 7) =$$

$$= \varphi(2^7)\varphi(3^2)\varphi(5)\varphi(7) = (2^7 - 2^6)(3^2 - 3)$$

$$4 \cdot 6 =$$

$$\varphi(240240) = \varphi(240 \cdot 1001)$$

$$p = 1001$$

$$a^{p-1} \equiv 1 \mod p$$

$$\alpha a < p \qquad 2 \ldots [\sqrt{1001}]$$

$$\varphi(240\cdot 1001) = \varphi(240\cdot 11\cdot 91) =$$

$$= \varphi(240\cdot 11\cdot 7\cdot 13) = \varphi(240)\cdot\varphi(11)\varphi(7)\varphi(13)$$

$$= \varphi(3\cdot 2^4\cdot 5)\cdot(10)\cdot(6)\cdot(12) = 2\cdot 4\cdot 10\cdot 6\cdot 12\,(2^4-2^3)$$

$$\underbrace{2\cdot 4}_{8}\qquad \underbrace{8\cdot 10}_{80}\qquad \underbrace{80\cdot 6}_{480}\qquad 480\cdot 12$$

$$= 5760\cdot 8 = 46080$$

✓ $13x \equiv 10 \mod 15$

$13x - 10 \equiv 0 \mod 15$

$13x - 10 = 15\cdot k$

$x = 5\cdot y$

$13\cdot 5y \equiv 10 \mod 15$

✓ $13\cdot 5y - 10 = 15\cdot k$

✓ $13y - 2 = 3k$

✓ $13y \equiv 2 \mod 3$

$\text{NOD}(13,3) = 1$

$y \equiv 2 \mod 3$

$y = 3n + 2$

$x = 5 \cdot y = 5(3n+2) = \underbrace{15n+10}, \quad x_0 = 10$

$13(15n+10) \equiv 10 \bmod 15$

$n=0 \quad 130-10=120=15\cdot 8$

$n=1$

$13(15+10) = 13\cdot 25 = 325 \equiv 10 \bmod 15$

$325-10 = \underbrace{315} \equiv 0 \bmod 15$

$315 = 21\cdot 15$

$n=-1$

$13(15\cdot(-1)+10) = 13(-5) = -65$

$-65-10 \equiv 0 \bmod 15 \quad -75 \equiv 0 \bmod 15$

$16x \equiv 7 \bmod 26$

$НОД(16,26) = НОД(16,10) = НОД(6,10) = НОД(6,4$

$= НОД(2,4) = НОД(2,2) = 2$

$НОД(16,26)=2$

Если

$\overset{16}{\overset{\shortparallel}{a}}x \equiv 8 \bmod \overset{26}{\overset{\shortparallel}{m}}$ и

$НОД(a,m) = d$, то $\underline{d \mid 8}$ $\quad \underbrace{2 \nmid 7},$

<u>Нет решений.</u>

✓ $12x \equiv 18 \mod 22$ $\qquad x = 7$

$12 \cdot 7 - 18 \equiv 0 \mod 22$

$84 - 18 = 66 = 22 \cdot 3$

$12x - 18 = 22 \cdot k$

$6x - 9 = 11k$

$6x \equiv 9 \mod 11 \quad \cdot 3$

✓ $2x \equiv 3 \mod 11$

$HOD(11, 2) = HOD(11 - 2\cdot 5, 2) = HOD(1, 2) = HOD(1, 1)$

$11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 2\cdot 5$

$2 = 1 \cdot 1 + 1 \qquad 1 = 2 - 1 \cdot 1$

$1 = 1 \cdot 1 + 0 \qquad 1 = 2 - 1 \cdot (11 - 2 \cdot 5)$

$1 = 2 - 1 \cdot 11 + 2 \cdot 5 =$

$1 = 2 \cdot 6 - 1 \cdot 11 \Rightarrow 3 = 2 \cdot 3 \cdot 6 - 3 \cdot 11$

$2 \cdot 3 \cdot 6 - 3 = 3 \cdot 11$

$2 \cdot 18 \equiv 3 \mod 11$

$x = 18 \mod 11 = 7$

$2x \equiv 3 \mod 11$

$2^{10} \equiv 1 \mod 11$

$x = 2^9 \cdot 3 \mod 11$

$2^4 \cdot 2^4 \cdot 2 \cdot 3 \equiv 5 \cdot 5 \cdot 2 \cdot 3 \equiv 3 \cdot 2 \cdot 3 \equiv 18 \equiv 7$

$x \equiv 7 \mod 11$

$2 \cdot 7 \equiv 3 \mod 11$

$HOD(12, 22) = 2$

$x_0 = 7$

$x_0 + \frac{m}{d} = 7 + 11 = 18$

$12 \cdot 18 - 18 \equiv 0 \mod 22$

$18 \cdot 11 \equiv 0 \mod 22$

$12x \equiv 8 \mod 24$

НОД$(12, 24) = 12 \Rightarrow 12 | 8$ - ложь.

Доказать, что уравнение

$3x^2 + 2 = y^2$ неразрешимо

в целых числах

Если $3x^2 + 2 = y^2 \quad \exists\, x, y \in \mathbb{Z}$

тогда $\forall m \quad 3x^2 + 2 \equiv y^2 \mod m$

$m = 2 \qquad 3x^2 + 2 \equiv y^2 \mod 2$

$m = 3$

Квадраты числа по модулю 3 дают в остатке либо 0, либо 1

Если $x^2 \equiv 0 \mod 3$

$3 \cdot 0 + 2 \equiv 2 \mod 3 \equiv y^2 \mod 3$ - ложь

Если $x^2 \equiv 1 \mod 3$

$3 \cdot 1 + 2 = 5 \equiv 2 \mod 3 \equiv y^2 \mod 3$ ложь