Домашнее задание на 31.01 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

№1 Пусть стороны треугольника $a, b, c \in \mathbb{Z}$. Выполняется т.Пифагора:

$$a^2 + b^2 = c^2$$

№2 Решим сравнения:

а) $19x \equiv 2(mod 88)$

Это равносильно:

$$19x - 2 = 88y \implies 19x - 88y = 2$$

Решим:

$$\begin{pmatrix} 19 & -88 & | & -2 \\ 1 & 0 & | & 0 \\ 0 & 1 & | & 0 \end{pmatrix} \implies \begin{pmatrix} 19 & 7 & | & -2 \\ 1 & 5 & | & 0 \\ 0 & 1 & | & 0 \end{pmatrix} \implies \begin{pmatrix} -2 & 7 & | & -2 \\ -14 & 5 & | & 0 \\ -3 & 1 & | & 0 \end{pmatrix}$$

$$\implies \begin{pmatrix} 2 & 1 & | & -2 \\ 14 & -37 & | & 0 \\ 3 & -8 & | & 0 \end{pmatrix} \implies \begin{pmatrix} 1 & 0 & | & -2 \\ -37 & 88 & | & 0 \\ -8 & 19 & | & 0 \end{pmatrix} \implies \begin{pmatrix} 1 & 0 & | & 0 \\ -37 & 88 & | & -74 \\ -8 & 19 & | & 16 \end{pmatrix}$$

$$\implies \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 88 \\ 19 \end{pmatrix} t + \begin{pmatrix} -74 \\ 16 \end{pmatrix} \implies x = 88t - 74 \quad t \in \mathbb{Z}$$

б) $102x \equiv 9(mod 165)$ Это эквивалентно:

$$102x - 165y = 9$$

Решим:

$$\begin{pmatrix} 102 & -165 & | & -9 \\ 1 & 0 & | & 0 \\ 0 & 1 & | & 0 \end{pmatrix} \implies \begin{pmatrix} -24 & 3 & | & -9 \\ 3 & -21 & | & 0 \\ -2 & 15 & | & 0 \end{pmatrix} \implies \begin{pmatrix} 0 & 3 & | & -9 \\ -165 & -21 & | & 0 \\ 118 & 15 & | & 0 \end{pmatrix}$$

$$\implies \begin{pmatrix} 3 & 0 & | & 0 \\ -21 & -165 & | & -63 \\ 15 & 118 & | & 45 \end{pmatrix} \implies \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -165 \\ 118 \end{pmatrix} t + \begin{pmatrix} -63 \\ 45 \end{pmatrix} \implies$$

$$\implies x = -165t - 63 \quad t \in \mathbb{Z}$$

№3 По теореме Ферма:

$$5^{p-1} = 1(mod\, p)$$

При этом:

$$5^{p^2} = 1(mod\, p)$$

Значит нужно, чтобы:

$$p - 1 \mid p^2 \implies p^2 \equiv 0(mod\, p - 1)$$

Т.к. p и $p - 1$ взаимно просты, то можно сократить на p:

$$p \equiv 0(mod\, p - 1) \implies 1 = (p - 1)t$$

При $t \neq 0$:

$$p = \frac{1 + t}{t} = \frac{1}{t} + 1 \implies t = 1, -1 \implies p = 2, 0$$

При $t = 0$:

$$1 = 0 \quad \emptyset$$

Ответ: 0 и 2

№4 Чтобы найти все основания a, для которых число $n = 15$ является псевдопростым, мы должны проверить условие:

$$a^{n-1} \equiv 1 \pmod{n}$$

где $n-1=14$. Таким образом, нам нужно проверить:

$$a^{14} \equiv 1 \pmod{15}$$

Сначала найдем все числа a, такие что $(a,15)=1$. Число 15 имеет делители 3 и 5, поэтому a не должно быть кратно 3 или 5. Таким образом, возможные значения a в пределах от 1 до 14:

$$a = 1, 2, 4, 7, 8, 11, 13, 14$$

Условие
$$a^{14} \equiv 1 \pmod{15}$$
По теореме Эйлера эквивалентно (т.к. $\varphi(15) = 8$, значит $a^8 = 1 \pmod{15}$):
$$a^6 \equiv 1 \pmod{15}$$

Теперь нам нужно проверить каждое значение a из списка $a = 2, 4, 7, 8, 11, 13, 14$ на выполнение условия $a^6 \equiv 1 \pmod{15}$.

1. Для $a=2$:

$$2^6 = 64 \quad \Rightarrow \quad 64 \mod 15 = 4 \quad \Rightarrow \quad 2^6 \equiv 4 \pmod{15} \quad \text{(не подходит)}.$$

2. Для $a=4$:

$$4^6 = (4^2)^3 = 16^3 \equiv 1^3 \equiv 1 \pmod{15} \quad \text{(подходит)}.$$

3. Для $a=7$:
$$7^6 = (7^2)^3 = 49^3 \equiv 4^3 \pmod{15}.$$

Теперь вычислим 4^3:

$$4^3 = 64 \quad \Rightarrow \quad 64 \mod 15 = 4 \quad \Rightarrow \quad 7^6 \equiv 4 \pmod{15} \quad \text{(не подходит)}.$$

4. Для $a = 8$:
$$8^6 = (8^2)^3 = 64^3 \equiv 4^3 \pmod{15}.$$

Как и в предыдущем случае:

$$4^3 = 64 \quad \Rightarrow \quad 64 \mod 15 = 4 \quad \Rightarrow \quad 8^6 \equiv 4 \pmod{15} \quad \text{(не подходит)}.$$

5. Для $a = 11$:

$$11^6 = (11^2)^3 = 121^3 \equiv 1^3 \equiv 1 \pmod{15} \quad \text{(подходит)}.$$

6. Для $a = 13$:

$$13^6 = (13^2)^3 = 169^3 \equiv 4^3 \pmod{15}.$$

Как и ранее:

$$4^3 = 64 \quad \Rightarrow \quad 64 \mod 15 = 4 \quad \Rightarrow \quad 13^6 \equiv 4 \pmod{15} \quad \text{(не подходит)}.$$

7. Для $a = 14$:

$$14^6 = (-1)^6 \equiv 1 \pmod{15} \quad \text{(подходит)}.$$

Ответ: $4, 11, 14$

№5 $\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 1 \pmod{13} \end{cases}$ Это равносильно:

$$\begin{cases} x - 2 = 11k \\ x - 1 = 13p \end{cases} \quad , \quad k, p \in \mathbb{Z}$$

Следовательно,

$$x = 11k + 2 = 13p + 1 \implies 11k - 13p = -1$$

Решим диафантово уравнение:

$$\begin{pmatrix} 11 & -13 & | & 1 \\ 1 & 0 & | & 0 \\ 0 & 1 & | & 0 \end{pmatrix} \implies \begin{pmatrix} -2 & -13 & | & 1 \\ 1 & 0 & | & 0 \\ 1 & 1 & | & 0 \end{pmatrix} \implies \begin{pmatrix} -2 & 1 & | & 1 \\ 1 & -7 & | & 0 \\ 1 & -6 & | & 0 \end{pmatrix}$$

$$\implies \begin{pmatrix} 0 & 1 & | & 1 \\ -13 & -7 & | & 0 \\ -11 & -6 & | & 0 \end{pmatrix} \implies \begin{pmatrix} 1 & 0 & | & 0 \\ -7 & -13 & | & 7 \\ -6 & -11 & | & 6 \end{pmatrix} \implies \begin{pmatrix} k \\ p \end{pmatrix} = \begin{pmatrix} -13 \\ -11 \end{pmatrix} t + \begin{pmatrix} 7 \\ 6 \end{pmatrix}$$

Получаем:

$$\begin{cases} x = 11 \cdot (-13t + 7) + 2 \\ x = 13 \cdot (-11t + 6) + 1 \end{cases} \implies \begin{cases} x = -143t + 79 \\ x = -143t + 79 \end{cases} \implies x = -143t + 79 \quad t \in \mathbb{Z}$$

Ответ: $x = -143t + 79 \quad t \in \mathbb{Z} \Leftrightarrow x \equiv 79 \pmod{-143}$