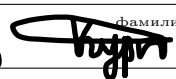


Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Омский государственный технический университет»

Факультет информационных технологий и компьютерных систем
Кафедра «Прикладная математика и фундаментальная информатика»

Индивидуальная работа
по дисциплине «Теория чисел»

Студента	Курпенова Куата Ибраимовича
	<small>фамилия, имя, отчество полностью</small>
Курс	2, группа ФИТ-212
Направление	02.03.02 Прикладная математика и фундаментальная информатика
	<small>код, наименование</small>
Руководитель	доц., канд. физ.-мат. наук
	<small>должность, ученая степень, звание</small>
	Белим С. Ю.
	<small>фамилия, инициалы</small>
Выполнил	04.01.23 
	<small>дата, подпись студента</small>

Омск 2022

Задание 1

Вычислите значение символа Лежандра: $\frac{111}{541}$.

Решение

$$\frac{111}{541} \equiv \frac{97}{111} \equiv \frac{14}{97} \equiv \frac{2 \cdot 7}{97} \equiv \frac{7}{97} \equiv \frac{6}{97} \equiv \frac{3}{7} \equiv -\frac{1}{3} \equiv -1$$

Ответ

Символ Лежандра равен -1.

Задание 2

Вычислите значение символа Лежандра с помощью критерия Эйлера: $\frac{11}{37}$.

Решение

$$\frac{11}{37} \equiv 11^{\frac{37-1}{2}} (mod 37) \equiv 11^{12} (mod 37)$$

$$11^{12} \equiv 1 (mod 37)$$

$$11^{12} - 1 \equiv 0 (mod 37)$$

$$(11^6 + 1)(11^6 - 1) \equiv 0 (mod 37)$$

$$11^2 \equiv 121 (mod 37) \equiv 10 (mod 37) \equiv -1 (mod 37)$$

$$(-1)^3 mod(37) \equiv -1 (mod(37))$$

$$11^{12} \equiv 1 (mod 37)$$

$$11^{12} (mod 37) \equiv 313842837672 (mod 37) \equiv 1 (mod 37)$$

Ответ

Символ Лежандра равен 1.

Задание 3

Решите сравнение: $x^2 \equiv 5 (mod 29)$.

Решение

Рассмотрим символ Лежандра, так как 29 - простое число.

$$\frac{5}{29} \equiv (-1)^{\frac{5-1}{2} \cdot \frac{29-1}{2}} \frac{29}{5} \equiv \frac{4}{5} \equiv (-1)^{\frac{4-1}{2} \cdot \frac{5-1}{2}} \frac{5}{4} \equiv \frac{1}{4} \equiv 1$$
$$5 \in Q_{29}$$

$$1 \equiv \frac{5}{29} \equiv 5^{\frac{29-1}{2}} (mod 29)$$

$$1 \equiv 5^{14} (mod 29)$$

$$5^{14} \equiv 1 (mod 29)$$

$$5^{14} - 1 \equiv 0 (mod 29)$$

$$(5^7 - 1)(5^7 + 1) \equiv 0 (mod 29)$$

$$5^3 \equiv 125 (mod 29) \equiv 9 (mod 29)$$

$$5^4 \equiv 625 (mod 29) \equiv 16 (mod 29)$$

$$5^7 \equiv 9 \cdot 16 \equiv 144 (mod 29) \equiv 28 (mod 29) \equiv -1 (mod 29)$$

Возьмём квадратичный невычет по модулю 29:

$$\frac{2}{29} \equiv 2^{\frac{29-1}{2}} (mod 29) \equiv 2^{14} (mod 29)$$

$$-1 \equiv 2^{14} (mod 29)$$

$$2^{14} \cdot 5^7 \equiv 1 (mod 29)$$

$$2^{14} \cdot 5^8 \equiv 5 (mod 29)$$

$$x \equiv \pm(5^4 \cdot 2^7) (mod 29)$$

Ответ

$$x \equiv \begin{cases} 11 (mod 29) \\ 18 (mod 29) \end{cases}$$