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 |
|  | фамилия, имя, отчество полностью |
| Курс | 2 Группа ФИТ-212 |
| Направление | 02.03.02 Фундаментальная информатика |
|  | и информационные технологии |
|  | код, наименование |
| Руководитель | доц., канд. пед. наук, доцент |
|  | должность, ученая степень, звание |
|  | Белим С.Ю. |
|  | фамилия, инициалы |
| Выполнил |  |
|  | дата, подпись студента |
| баллы |  |
|  | дата, подпись руководителя |

Омск-2022

**Вариант 10**

**Задание 1**

Найти остаток от деления на 50

**Решение:**

(

НОД (3, 50) = 1, тогда по теореме Эйлера

,

НОД(5, 20) = 5

5\*

**Задание 2**

Решить сравнения а) 47х2(mod127), б) 12х18(mod42), в) 24х6(mod80)

**Решение:**

а) 47х2(mod127)

НОД(127, 47) = 1

б) 12х18(mod42)

НОД(42, 12) = 6

в) 24х6(mod80)

НОД(80, 24) = 8, 6 8 → сравнение неразрешимо

**Задание 3**

Решить систему сравнений

**Решение:**

{2, 3, 5} – попарно взаимно просты

НОК (2, 3, 5, 6, 15) = 30

Внедрим подсистему, которую можно решить с помощь китайской теоремы об остатках

**Задание 4**

Пусть в прямоугольном треугольнике длины сторон выражаются целыми числами. Докажите, что длина одной из трех сторон делится на 5.

**Решение:**

Пусть ни одно из чисел не делится на 5 => каждый квадрат сравним с ±1mod5 (1, 4, 9, 16). Но равенство ±1±1≡±1mod5 невозможно.

**Задание 5**

Вычислить над кольцом вычетов по модулю 675 с помощью алгоритма Руффини – Горнера значение многочлена в точке и найти неполное частное от деления многочлена на .

**Решение**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3 | 1 | -1 | 0 | 6 | 15 | 45 |
| 1 | 2 | 6 | 24 | 87 | 306 |

неполное частное от деления многочлена на