БАЛТИЙСКИЙ НАУЧНО-ИНЖЕНЕРНЫЙ КОНКУРС 2019
Санкт-Петербург, 4-7 февраля 2019

О числе точек на кривой в кольце вычетов

«Математика»

Печёнкин Александр Алексеевич, Муравко Вячеслав Игоревич (научный руководитель, Старший преподаватель), место выполнения работы: В школе

Общая задача. Пусть f(x,y)- функция от двух переменных с целыми коэффициентами. Найти или оценить число решений уравнения f(x,y)=0 (mod n). В ходе исследования общей задачи, была поставлена также следующая задача: Задача. Пусть f(x) – некоторая арифметическая функция. Найти или оценить количество возможных значений функции f(x) по произвольному модулю n. Сфера использования - Широкое применение в современной криптографии.

В работе был использован методы теории сравнений по модулю n.

Полностью приведён алгоритм подсчета количества возможных значений функции f(x)=x^m по модулю n для любого m, из которого было получено следствие на формулу Стангла о числе квадратичных вычетов. Полностью приведён алгоритм подсчета количества возможных значений функции f(x)=ax^2+bx+c по модулю n. В качестве следствий получены решения некоторых уравнений вида s_(f(x)) (n)=a, где a из (n,n-1,ф(n)). Найдено условие, при котором функция P(x)=ax^3+bx^2+cx+d имеет менее чем n значений по модулю n.

В работе исследовано число возможных значений некоторых арифметических функций по произвольному модулю. Возможные пути развития задачи: 1.Исследование количества решений уравнения g(y)-f(x)=0 (mod n), где g(y) и f(x) -многочлены степени 2 и выше. 2. Продолжение исследования количества возможных значений функции f(x) по модулю n, где f(x) - многочлен степени 4 и выше от x.

Список литературы:

1. Stangl, Walter D. Counting Squares in Z_n– Mathematics Magazine T.69 (4): 285-289
2. S. Finch, P. Sebah. Squares and cubes modulo n. arXiv:math/0604465v3 [math.NT] 25 Mar 2016