МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ОДЕССКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. И.И. МЕЧНИКОВА

Аналитическая теория чисел

в задачах и теоремах

Варбанец С. П.

Одесса, 2013

Печатается по решению Ученого Совета ИМЭМ ОНУ

от 19 сентября 2013 года, протокол №1

составители: к. ф.-м. н. Варбанец С.П.

рецензенты: д. ф.-м. н. Леонов Ю.Г.

к. ф.-м. н. Покась С.М.

Оглавление

Введение

К. Гаусс был первым, кто стал применять простейшие тригонометрические суммы к решению задач теории чисел. В частности, используя свойства носящей его имя “Суммы Гаусса”, он построил одно из своих доказательств закона взаимности квадратических вычетов.

В дальнейшем, благодаря исследованиям Г.Вейля, Харди, Литтлвуда, ван де Корпута и И.М.Виноградова, тригонометрические суммы стали мощным средством решения многих важных и трудных задач теории чисел.

В этой главе мы рассмотрим некоторые применения тригонометрических сумм к задачам о распределении решений сравнений от двух переменных в неполной системе вычетов.

§1. Теорема И.М.Виноградова о распределении дробных долей многочлена.

Классическая теорема Виноградова – Поля, утверждает, что количество квадратичных вычетов по модулю p, расположенных на отрезке $[0, T]$, определяется асимптотической формулой

$$N(T) = \frac{1}{2}T + O\left(\sqrt{p}\log p\right)$$

допускает такую интерпретацию: $N(T)$ равно количеству дробных долей многочлена y^2/p, попавших в интервал $\left(0, \left(T + \frac{1}{2}\right)/p\right)$, когда y пробегает значения $1,2, \dots, p-1$.

Пусть $n \geq 11, T > 0$ −целое число,

$$f(x) = \alpha_{n+1}x^{n+1} + \alpha_n x^n + \cdots + \alpha_1 x^1 + \alpha_0$$

многочлен с вещественными коэффициентами, r одно из чисел $2,3,\dots,n+1$.

$$d_\tau = \frac{a}{q} + \frac{\theta}{q^2}, \qquad |\theta| \le 1,\ (a,q) = 1, 1 < q \le T^r$$

Положим

1. $q = T^\tau$, если $1 < q \le T$
2. $\tau = 1$ если $T < q \le T^{r-1}$
3. $q = T^{r-\tau}$, если $T^{r-1} < q \le T^r$,

$$l = log\,\frac{12n(n+1)}{\tau},\ \ \rho = \frac{\tau}{3n^2 l}$$

Имеет место следующая теорема, доказанная И.М.Виноградовым [9]

Теорема. Пусть m и T – целые положительные,

Тогда справедлива оценка

$$|S| < (8n)^{\frac{1}{2}nl} m^{\frac{2\rho}{\tau}} T^{1-\rho}.$$

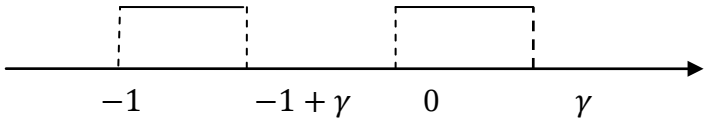
Используя этот результат, докажем теорему о распределении дробных долей многочлена:

Теорема. Пусть $A_T(\gamma)$ означает количество дробных долей $\{f(x)\}, x = 1,2,\dots,T$ попавших на полуинтервал $[0,\gamma), 0 \le \gamma < 1$.

Тогда

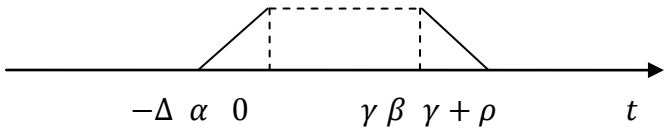
$$A_T(\gamma) = T_\gamma + O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau}{3n^2 l}}\right)$$

Доказательство. Обозначим через $\chi(t)$ характеристическую функцию полуинтервала $[0,\gamma)$ периодически с периодом I продолженную на всю вещественную ось



Возьмём параметр $0 < \Delta < \frac{1}{2}$ / более точно определим его позднее /.

Положим $\alpha = -\Delta/2$, $\rho = \gamma + \Delta/2$. Обозначим через $\psi(t)$ периодическую с периодом I функцию, определённую графиком:



Согласно лемме о стаканчиках Виноградова $\psi(t)$ разлагается в ряд Фурье

$$\psi(t) = \beta - \alpha + \sum_{m=1}^{\infty} (a_m \cos 2\pi mt + b_m \sin 2\pi mt),$$

$$|a_m| = O\left(\frac{1}{m}\right), \quad |b_m| = O\left(\frac{1}{m}\right),$$

$$|a_m| = O\left(\frac{1}{m^2\Delta}\right), \quad |b_m| = O\left(\frac{1}{m^2\Delta}\right).$$

Ясно, что

$$A_T(\gamma) = \sum_{x=1}^{T} \chi\big(f(x)\big)$$

Проведём исследование суммы, близкой к данной, обозначим её S

$$S = \sum_{x=1}^{T} \psi(\alpha_{n+1}x^{n+1} + \alpha_n x^n + \cdots + \alpha_1 x^1 + \alpha_0) = (\gamma + \Delta)T +$$

$$+ \sum_{x=1}^{T} \sum_{m=1}^{\infty} (a_m \cos 2\pi m f(x) + b_m \sin 2\pi m f(x)) =$$

$$= \gamma T + \Delta T + O\left(\sum_{m=1}^{\infty} max(|a_m|, |b_m|) \left|\sum_{x=1}^{T} e^{2\pi i m f(x)}\right|\right)$$

Введём некоторое δ /определим его позднее / и разобьем сумму на две суммы:

$$S_1 = \gamma T + \Delta T + O\left(\sum_{m>\delta} max(|a_m|, |b_m|) \left|\sum_{x=1}^{T} e^{2\pi i m f(x)}\right|\right) +$$

$$+ O\left(\sum_{m=1}^{\delta} max(|a_m|, |b_m|) \left|\sum_{x=1}^{T} e^{2\pi i m f(x)}\right|\right)$$

/к внутренней сумме применим приведенную выше теорему Виноградова /

$$\left|\sum_{x=1}^{T} e^{2\pi i m f(x)}\right| < (8n)^{\frac{1}{2}nl} m^{\frac{2\rho}{\tau}} T^{1-\rho}$$

$$S_x = \gamma T + \Delta T + O\left(\frac{T}{\Delta}\sum_{m>\delta}\frac{1}{m^2}\right) + O\left((8n)^{\frac{1}{2}nl} T^{1-\rho} \sum_{1\le m\le\delta}\frac{1}{m} m^{\frac{2\rho}{\tau}}\right) =$$

$$= \gamma T + \Delta T + O\left(\frac{T}{\Delta\delta}\right) + O\left((8n)^{\frac{1}{2}nl} T^{1-\rho}\delta^{\frac{2\rho}{\tau}}\right)$$

Возьмём

$$\delta = \frac{1}{\Delta^2}, \qquad \Delta = T^{-\frac{\rho\tau}{\tau-2\rho}}$$

После несложных операций получаем

$$O\left(\frac{T}{\Delta\delta}\right) = O(T\Delta) = O\left(T^{1-\frac{\rho\tau}{\tau-2\rho}}\right)$$

$$O\left((8n)^{\frac{1}{2}nl} T^{1-\rho-\frac{2\rho}{\tau}\frac{\rho\tau}{\tau-2\rho}}\right) = O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}\right)$$

$$S = \gamma T + O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}\right)$$

Обозначим через $\chi_1(t)$ характеристическую функцию интервала $(-\Delta, 0)$ периодически продолженную с периодом I на всю ось, через $\chi_2(t)$ обозначим характеристическую функцию интервала $(\gamma, \gamma+\Delta)$ периодически продолженную с периодом I на всю ось. Получаем

$$A_T(\gamma) = T_\gamma + O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}\right) +$$

$$+\theta_1 \sum_{x=1}^{T} \chi_1\big(f(x)\big) + \theta_2 \sum_{x=1}^{T} \chi_2\big(f(x)\big), \qquad |\theta_1| \le 1, |\theta_2| \le 1$$

Обозначим через $\psi_1(t)$ функцию, определённую на $(-2\Delta, 1-2\Delta)$

$$\psi_1(t) = \begin{cases} \frac{1}{\Delta}(t+2\Delta), & \text{если} -2\Delta \le t \le -\Delta, \\ 1, & \text{если} \quad -\Delta \le t \le 0 \\ -\frac{1}{\Delta}(t-\Delta), & \text{если} \quad 0 \le t \le \Delta \\ 0, & \text{если} \quad \Delta \le t \le 1-2\Delta \end{cases}$$

и периодически с периодом с периодом I продолженную на всю ось.

Получаем:

$$\sum_{x=1}^{T} \chi_1\big(f(x)\big) \le \sum_{x=1}^{T} \psi_1(\alpha_{n+1}x^{n+1} + \alpha_n x^n + \cdots + \alpha_1 x^1 + \alpha_0) =$$

$$= O(T\Delta) + O(8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}.$$

Аналогично:

$$\sum_{x=1}^{T} \chi_2\big(f(x)\big) \le \; O(T\Delta) + O(8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}.$$

И наконец, вспоминая, что $\Delta = T^{1-\frac{\tau\rho}{\tau-2\rho}}$, имеем

$$A_T(\gamma) = T_\gamma + O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau\rho}{\tau-2\rho}}\right)$$

Учтём теперь, что

$$\frac{\tau\rho}{\tau-2\rho} = \frac{\tau\frac{\tau}{3n^2l}}{\tau-2\frac{\tau}{3n^2l}} = \frac{\tau}{3n^2l-2} > \frac{\tau}{3n^2l}$$

Поэтому

$$A_T(\gamma) = T_\gamma + O\left((8n)^{\frac{1}{2}nl} T^{1-\frac{\tau}{3n^2l}}\right)$$

Доказанная теорема И.М. Виноградова о распределении дробных долей многочлена имеет непосредственное приложение к задаче о распределении решений сравнений вида

(1) $$y \equiv f(x)(mod\ p^k),$$

где p −простое число, а $f(x)$ −многочлен с целыми коэффициентами. Точнее задача ставится так: дано два числа $1 \le T_1 \le p^n$ и $1 \le T \le p^n$. Требуется определить количество решений сравнения (1), у которых $0 \le x \le T$, $0 \le y \le T_1$

Обозначим это количество через $A(T, T_1)$.

Вопрос о нахождении величины $A(T, T_1)$ редуцируется очевидно к вопросу о распределении дробных долей многочлена:

$A(T, T_1)$ равно количеству дробных долей $\{f(x)/p^n\}$, когда $x = 0,1, \dots, T$ попавших на отрезок $\left[0, {}^{T}/_{p^n}\right]$.

Приведём пример. Пусть дано сравнение

$$y \equiv ax^k (mod\ p^n),$$

$(a, p) = 1$, $k > n \ge 12$. Ограничиваясь рассмотрением второго случая теоремы И.М.Виноградова, что означает

$$p^{\frac{n}{k-1}} \le T < p^n,$$

получаем

$$A(T, T_1) = \frac{TT_1}{p^n} + O\left((8n)^{\frac{1}{2}klog\ 12(k-1)} T^{1-\frac{1}{3k^2 log\ 12(k-1)}}\right) \quad (2)$$

Для общего сравнения с двумя неизвестными

$$F(x, y) \equiv O(mod\ p^n) \quad (3)$$

Непосредственное применение теоремы Виноградова невозможно, так у нас нет явного представления y в виде многочлена от x.

Эту трудность мы можем обойти, используя p −адическое описание решений сравнения (3).

§2. Р −адические ряды в элементарной теории чисел.

Предметом наших дальнейших рассмотрений являются сравнения вида

(1) $$F\ (x, y) \equiv O(mod\ p^n),$$

где p −простое число.

Пусть T_1 и T_2 два натуральных числа, $1 \leq T_1 \leq p^n, 1 \leq T_2 \leq p^n$. Обозначим через $A(T_2, T_1)$ количество решений сравнения (1), у которых $0 \leq x \leq T_1$, $0 \leq y \leq T_2$.

Наша цель состоит в нахождении приближённой формулы для величины $A(T_2, T_1)$. Для достижения этой цели мы будем сводить задачу к теореме И.М.Виноградова p распределений дробных долей многочлена. Более точно, надо выразить y как многочлен от x /в смысле сравнимости по модулю p^n/. Для этого нужно разложить y в $p-$ адический ряд по степени x и ограничить достаточно большим количеством начальных членов разложения.

Приведём несколько примеров на эту мысль. Мы не будем употреблять терминологию $p-$ адического анализа, но наши рассуждения –элементаризированный $p-$ адический анализ.

Мы получаем результаты в форме, пригодной для использования в аналитической теории чисел.

I. Начнём с рассмотрения сравнения

(2) $$y^k - x \equiv 0(mod\ p^n),$$

здесь $p > 2 -$ простое, n и $k \geq 2$ −натуральные, $k|(p-1)$.

Решения (x, y), не сравнимые с $(0,0)$ по модулю p, назовём регулярными.

Лемма 1. Сравнение

$$y^n - x \equiv 0(mod\ p^n)$$

имеет точно $p^{n-1}(p-1)$ регулярных решений.

Д о к а з а т е л ь с т в о. Сравнение (2) в отношении регулярных решений эквивалентно сравнению

(2′) $$k \cdot ind\ y - ind\ x \equiv 0\big(mod\ p^{n-1}(p-1)\big),$$

/ здесь ind берётся относительно некоторого первообразного корня g по модулю p^n/.

Это сравнение разрешимо тогда и только тогда, когда $k|ind\ x$.

Среди чисел $0,1,\dots,p^{n-1}(p-1)-1$ имеется точно $\frac{p^n(p-1)}{k}$ кратных k. Значит есть точно $\frac{p^{n-1}(p-1)}{k}$ чисел $x_i, x_i \not\equiv 0(mod\ p)$, являющихся вычетами степени k по модулю p^n. Пусть x_i какой-то вычет степени k по модулю p^n, $(x_i, p) = 1$. Из сравнения

$$ind\ y - \frac{ind\ x}{k} \equiv 0\left(mod\ p^{n-1}\frac{p-1}{k}\right)$$

видно, что данному x_i будем соответствовать k решений сравнения (2), которые получаются из одного $y_{i,0}$ по формуле

$$y_{i,} = g^{f p^{n-1}\frac{p-1}{k}} \cdot y_{i,0}, \quad f = 0,1,\dots,k-1.$$

Итак, имеется $p^{n-1}\frac{p-1}{k} \cdot k = p^{n-1}(p-1)$ регулярных решений сравнения (2).

Покажем, как с помощью решений сравнения (2) при $n = 1$ можно описать все решения сравнения (2) для $n \geq 2$.

Пусть a_x какое-либо решение сравнения

$$y^k \equiv a_x(mod\ p^n)$$

/возможно с другим y/.

Лемма 2. Пусть $a_x, 1 \leq a_x \leq p-1$, вычет степени k по модулю p. Пусть $b_x^{(j)}, j = 0,1,\dots,k$, все корни сравнения

$$y^k \equiv a_x(mod\ p).$$

Для каждого $t_1, 0 \leq t_1 < p^{n-1}$, найдется единственное $t, 0 \leq t \leq p^{n-1}-1$,

такое, что $\left(b_x^{(j)} + pt_1\right)^k \equiv a_x + pt(mod\ p^n)$

Действительно, t однозначно определяется по модулю p^{n-1} в виде

$$t \equiv \frac{b_x^{(j)^k} - a_x}{p} + \frac{\left(b_x^{(j)} + pt_1\right)^k - b_x^{(j)^k}}{p} (mod\ p^{n-1}).$$

2. Пусть $q > 1 -$ натуральное, $a \equiv 1(mod\ q)$, но $a \not\equiv 1(mod\ q^2)$.

Рассмотрим сравнение

(3) $$xa^x \equiv y(mod\ q^n)$$

Лемма 3. Пусть $q = {p_1}^{\alpha_1} \dots {p_t}^{\alpha_t}$

Тогда при любом $n < \min(p_1, \dots, p_t)$ справедливо сравнение

$$a^x \equiv 1 + a_1 qx + a_2 q^2 x^2 + \dots + a_{n-1} q^{n-1} x^{n-1} (mod\ q^n),$$

где $(a_i, q) = 1, i = 1, \dots, n-1$.

Д о к а з а т е л ь с т в о. Имеем $a = 1 + uq, (u, q) = 1$.

Значит,

$$a^x = (1 + uq)^x \equiv 1 + uqC_x^1 + \dots + (uq)^{n-1} C_x^{n-1} (mod\ q^n).$$

Рассматривая $uqC_x^1 + \dots + (uq)^{n-1} C_x^{n-1}$

как многочлен относительно x и замечая, что коэффициент при

$x^l, l = 1, \dots, n-1$ имеет вид

$$\frac{(uq)^l}{l!} - \frac{\frac{l(l-1)}{2}(uq)^{l+1}}{(l+1)!} + \dots = q^l(a_l + qb_l)(mod\ q^n),$$

где $a_l \equiv \frac{u^l}{l!}(mod\ q^n)$, а потому $(a_l, q) = 1$, получаем утверждение леммы.

Замечание. Если $q = p^l, p -$ простое, $\alpha > 1$, то при $p < n < p^2$, имеет место сравнение

$$a^x \equiv 1 + a_1 F(1)x + a_2 F(2)x^2 + \dots + a_{n-1} F(n-1)x^{n-1} (mod\ q^n),$$

где $F(k) = g_1 g_2 \dots g_k$, а $\{g_i\} -$ периодическая последовательность периода p: $g_1 = p^\alpha, g_2 = p^\alpha, \dots g_{p-1} = p^\alpha, g_p = p^{\alpha-1}$.

Лемма 4. При x, пробегающем полную систему вычетов по модулю q^n, xa^x также пробегает такую систему.

Д о к а з а те л ь с т в о. Пусть

$$x_1 a^{x_1} \equiv x_2 a^{x_2} (mod\ q^n), 0 \leq x_2 < x_1 \leq q^n - 1.$$

Тогда $x_1 a^{x_1 - x_2} \equiv x_2 (mod\ q^n)$.

Но $a \equiv 1 (mod\ q)$.

Поэтому $x_1 \equiv x_2 (mod\ q)$, т.е. $x_1 - x_2 = qy_1$.

Мы имеем

$$x_1 a^{x_1 - x_2} = x_1 a^{qy_1} \equiv x_2 (mod\ q^n).$$

Однако, $a^2 \equiv 1 (mod\ q^2)$.

Значит, $x_1 \equiv x_2 (mod\ q^2)$.

Продолжая этот процесс n раз и учитывая, что $a^{q^{s-1}} \equiv 1 (mod\ q^s)$, получим утверждение леммы.

1. Рассмотрим теперь сравнение

$$(4) \qquad x^2 + y^2 \equiv 1 (mod\ p^n)$$

Мы будем следовать работе Л.П.Постниковой

Решения сравнения (4) разделим на две категории

I. Нерегулярные, в которых $y \equiv 1 (mod\ p)$ или $y \equiv -1 (mod\ p)$
II. Регулярные, в которых $y \not\equiv \pm 1 (mod\ p)$

Нас будут интересовать только регулярные решения.

Лемма 5. Пусть (x_0, y_0) какое-либо регулярное решение сравнения

$$(4') \qquad x^2 \equiv 1 - y^2 (mod\ p)$$

При любом $t, 0 \leq t \leq p^{n-1} - 1$, сравнение

$$(5) \qquad x^2 \equiv 1 - (y_0 + pt)^2 (mod\ p^n)$$

Имеет точно для несравнимых по модулю p^n решения.

Д о к а з а т е л ь с т в о. Возьмём $t, 0 \leq t \leq p^{n-1} - 1.$

и обозначим через $A = 1 - (y_0 + pt)^2$. Мы видим, что сравнение

$$x^2 \equiv A(mod\ p)$$

имеет решение /например, $x = x_0$/. Но по известной теореме теории чисел из этого следует, что сравнение

$$x^2 \equiv 1 - (y_0 + pt)^2 (mod\ p^n)$$

Имеет точно два решения. Лемма доказана.

Обозначим решения сравнения

$$x^2 \equiv 1 - (y_0 + pt)^2 (mod\ p^n), \text{т. е. } t = 0,$$

Через $x_1(0)$ и $x_2(0)$. Заметим, что $x_1(0)$ и $x_2(0)$ взаимно−просты с p. Вообще, через $x_1(t)$ и $x_2(t)$ будем обозначать решения сравнения (5).

Лемма 6. Обозначим

$$s = \left[\frac{p-1}{p-2} n\right]$$

Существует многочлен степени s

$$f(t) = \Phi_0(y_0) + p^{\lambda_1}\Phi_1(y_0)t + \cdots + p^{\lambda_s}\Phi_s(y_0)t^s,$$

у которого $\Phi_0(y_0), \Phi_1(y_0), \dots, \Phi_s(y_0)$ − целые числа, взаимно-простые с p, а $\lambda_1, \dots, \lambda_s$ −натуральные числа, удовлетворяющие неравенствам

$$\lambda_j \geq j\frac{p-1}{p-2},$$

Такой, что

$$x_1(t) \equiv x_1(0)f(t)(mod\ p^n),$$

$$x_2(t) \equiv x_2(0)f(t)(mod\ p^n).$$

Д о к а з а т е л ь с т в о. Пусть y_0' решение сравнения

$$\left(1-{y_0}^2\right){y_0}' \equiv 1(mod\ p^n)$$

/оно существует, ибо $y_0 \not\equiv \pm 1(mod\ p), \left(1-{y_0}^2, p\right) = 1/.$

Сравнение (5), очевидно, эквивалентно следующему

$$x^2 \equiv \left(1-{y_0}^2\right)(1-2y_0y_0'pt-{y_0}'p^2t^2)(mod\ p^n).$$

Будем предполагать, что $1 \le y_0' \le p^n - 1.$

Рассматривая $y_0, {y_0}'$ и w как вещественные числа, разложим

$$\Phi(w) = \sqrt{1-2y_0y_0'w-{y_0}'w^2}$$

в степенной ряд

$$\Phi(w) = \sum_{l=0}^{\infty} X_l(y_0, y_0')\, w^l,$$

где $X_l = X_l(y_0, y_0')$ −функция от y_0 и y_0'. Ясно, что $X_0 = 1, X_1 = -y_0y_0'.$

Далее, имеем

$$\frac{dlog\ \Phi(w)}{dw} = -\frac{1}{2}\cdot\frac{2y_0y_0' + 2{y_0}'w}{1-2y_0y_0'w-{y_0}'w^2} = -\frac{y_0y_0' + {y_0}'w}{1-2y_0y_0'w-{y_0}'w^2}$$

Приравнивая правые части, получаем

$$\sum_{l=0}^{\infty} l\, X_l\, w^{l-1}(1-2y_0y_0'w-{y_0}'w^2) + \sum_{l=0}^{\infty} X_l\, w^l(y_0y_0' + {y_0}'w) = 0.$$

Отсюда при $l = 1,2$ ...

$$X_{l+1}(l+1) - 2y_0y_0'l\, X_l - (l-1)X_{l-1}y_0' + y_0y_0'X_l + y_0'X_{l-1} = 0$$

$$X_{l+1}(l+1) = (2l-1)y_0y_0'X_l + (l-2)y_0'X_{l-1}.$$

Из этой формулы, исходя из X_0 и X_1 мы можем определить все X_{l+1}

Рассмотрим многочлен

$$\Phi_s(w) = \sum_{l=0}^{\infty} X_l\, w^l.$$

Докажем, что в многочлене

$$\Phi_s{}^2(w) - 1 + 2y_0y_0'w + y_0'w^2$$

отсутствуют все члены, содержащие w в степени от нулевой до $s-$ой включительно.

Действительно,

$$\Phi_s{}^2(w) - 1 + 2y_0y_0'w + y_0'w^2 =$$

$$= \left(\Phi_s(w) - \sqrt{1 - 2y_0y_0'w - y_0{}'w^2}\right)\left(\Phi_s(w) + \sqrt{1 - 2y_0y_0'w - y_0{}'w^2}\right)$$

Но разложение $\Phi_s(w) - \sqrt{1 - 2y_0y_0'w - y_0{}'w^2}$ в степенной ряд начинается со степени w^{s+1}, а разложение $\Phi_s(w) + \sqrt{1 - 2y_0y_0'w - y_0{}'w^2}$ начинается с нулевой степени w. Это и требуется.

В силу рекуррентного соотношения для X_l коэффициенты многочлена $\Phi_s(w)$ суть рациональные числа. Поэтому и коэффициенты многочлена

$$\Phi_s{}^2(w) - 1 + 2y_0y_0'w + y_0'w^2$$

суть рациональные числа.

Коэффициенты многочлена

$$\Phi_s{}^2(pt) - 1 + 2y_0y_0'pt + y_0{}'p^2t^2$$

также рациональные числа. В этом разложении нет членов с $t^0, t^1, \dots, t^s$.

Представим коэффициент при t^j в многочлене

$$\Phi_s(pt) = \sum_{j=0}^{s} X_j\, p^j t^j$$

в виде

$$X_j p^j = p^{\lambda_j}\frac{c_j}{d_j},$$

где c_j и d_jвзаимно просты с p. Оценим снизу величину λ_j.

Докажем, что $j!X_j$ есть целое число. Для $j = 0$ и $j = 1$ это очевидно из вида X_0 и X_1. Пусть это доказано для $l = 0,1,..,j$.

Докажем для $l = j + 1$. Мы имеем рекуррентное соотношение

$$X_{j+1} = \frac{2j-1}{j+1} y_0 y_0' X_j + \frac{j-2}{j+1} y_0' X_{j-1}$$

Отсюда следует, что

$$(j+1)!X_{j+1} = (2j-1)y_0 y_0' j!X_j + (j-2)j y_0'(j-1)!X_{j-1}$$

и поскольку $j!X_j$ и $(j-1)!X_{j-1}$ целые числа, то и $(j+1)!X_{j+1}$ целое число. Отсюда

$$\nu_p(X_j) \geq -\nu_p(j!), \quad \lambda_j = \nu_p(X_j p^j) \geq j - \nu_p(j!).$$

Но $\nu_p(j!) = \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \cdots$

Поэтому

$$\lambda_j \geq j - \left[\frac{j}{p}\right] - \left[\frac{j}{p^2}\right] - \cdots \geq j - \frac{j}{p} - \frac{j}{p^2} - \cdots = j\frac{p-2}{p-1}$$

В многочлене

$$\Phi_s{}^2(pt) - 1 + 2y_0 y_0' pt + y_0{}' p^2 t^2$$

Коэффициент при x_j, где $j \geq s+1$, делится /хотя это и дробное число / на p в степени не меньшей

$$\min_{i_1+i_2=j} (\lambda_{i_1}, \lambda_{i_2})$$

Но

$$\min_{i_1+i_2=j} (\lambda_{i_1}, \lambda_{i_2}) \geq \frac{p-2}{p-1}(i_1+i_2) = j\frac{p-2}{p-1} \geq \left[j\frac{p-2}{p-1}\right].$$

Значит все коэффициенты многочлена

$$\Phi_s{}^2(pt) - 1 + 2y_0 y_0' pt + y_0{}' p^2 t^2$$

делятся на p в степени не меньшей

$$\left[\frac{p-2}{p-1}(s+1)\right] \geq \left[\frac{p-2}{p-1}\cdot\frac{p-1}{p-2}n\right] = n.$$

Обозначим через $e_j, j = 0,1, \ldots, s$, корень сравнения

$$e_j d_j \equiv c_j (mod\ p^n)$$

/коэффициенты e_jзависят от y_0/. Ясно, что $\left(e_j, p\right) = 1$.

Обозначим

$$f(t) = \sum_{j=0}^{s} p^{\lambda_j} e_j t^j$$

При любом целом $0 \leq t \leq p^{n-1} - 1$

$$f^2(t) \equiv 1 - 2y_0 y_0' pt - {y_0}' p^2 t^2 (mod\ p^n).$$

При $i = 1,2$:

$$\left(x_i(0) f(t)\right)^2 \equiv (1 - y^2)(1 + 2y_0 y_0' pt + {y_0}' p^2 t^2)(mod\ p^n)$$

или

$$\left(x_i(0) f(t)\right)^2 \equiv 1 - (y_0 + pt)^2 (mod\ p^n)$$

Таким образом, $x_i(0)f(t)$ удовлетворяет сравнение (5), но очевидно, что $x_1(0)f(t)$ и $x_2(0)f(t)$ равные решения этого сравнения. Но сравнение (5) имеет всего два решения. Поэтому

$$x_1(t) \equiv x_1(0) f(t) (mod\ p^n)$$

$$x_2(t) \equiv x_2(0) f(t) (mod\ p^n)$$

Лемма доказана.

Лемма 7. Пусть $p > 3$ −простое. В обозначениях леммы 6 мы имели

$$X_0 = 1,\ \ X_1 = -y_0 y_0',\ \ \ X_2 = -\frac{y_0'}{2}({y_0}^2 y_0' + 1);$$

$$X_{j+1} = \frac{2j-1}{j+1} y_0 y_0' X_j + \frac{j-2}{j+1} y_0' X_{j-1}$$

Введём величины $Y_j, j = 2,3, \ldots$

$$Y_2 = 0, Y_3 = 1, Y_{j+1} = \frac{2j-1}{j+1} y_0 y_0' Y_j + \frac{j-2}{j+1} Y_{j-1}$$

Для $j = 3,4, \ldots$, введём определитель

$$\Delta_j = \begin{vmatrix} X_{j-1} & X_j \\ Y_{j-1} & Y_j \end{vmatrix},$$

Очевидно,

$$\Delta_3 = \begin{vmatrix} X_2 & X_3 \\ 0 & 1 \end{vmatrix} = X_2 = -\frac{y_0'}{2}({y_0}^2 y_0' + 1).$$

Заметим, что $\nu_p(\Delta_3) = 0$ при $p > 2$.

Действительно, величина y_0' была определена нами из сравнения

$$y_0'(1 - y_0^2) \equiv 1 (mod\ p^n)$$

Значит,

$${y_0}^2 y_0' + 1 \equiv y_0' (mod\ p^n),$$

$$\Delta_3 = X_2 \equiv -\frac{{y_0'}^2}{2} (mod\ p^n).$$

Так, как $(y_0', p) = 1$, то наше предложение доказано. Отсюда, между прочим, следует, что $\Delta_3 \neq 0$.

Имеем при $j \geq 3$

$$\Delta_j = \begin{vmatrix} X_{j-1} & X_j \\ Y_{j-1} & Y_j \end{vmatrix} = \begin{vmatrix} X_{j-1} & \frac{2j-3}{j} y_0 y_0' X_{j-1} + \frac{j-3}{j} y_0' X_{j-2} \\ Y_{j-1} & \frac{2j-3}{j} y_0 y_0' Y_{j-1} + \frac{j-3}{j} y_0' Y_{j-2} \end{vmatrix} =$$

$$= \frac{j-3}{j} y_0' \begin{vmatrix} X_{j-1} & X_{j-2} \\ Y_{j-1} & Y_{j-2} \end{vmatrix} = -\frac{j-3}{j} y_0' \Delta_{j-1}.$$

Повторяя это рассуждение, получаем при $j \geq k + 3$

$$\Delta_j = (-y_0')^k \cdot \frac{(j-3)(j-4) \ldots \big(j-(k+2)\big)}{j(j-1) \ldots \big(j-(k-1)\big)} \Delta_{j-k}$$

Бери $k = j - 3$, получаем

$$\Delta_j = (-y_0')^{j-3} \cdot \frac{(j-3)!}{j(j-1)\dots 4}\Delta_3 = (-y_0')^{j-3} \cdot \frac{6}{j(j-1)(j-2)}\Delta_3.$$

Или

$$(6) \qquad j\,(j-1)(j-2)\begin{vmatrix} X_{j-1}p^{j-1} & X_j p^j \\ Y_{j-1}p^{j-1} & Y_j p^j \end{vmatrix} = (-y_0')^{j-3} 6\Delta_3 p^{2j-1}.$$

Обозначим

$$Y_j p^j = p^{\mu_j}\frac{f_j}{g_j},$$

где $(f_j, p) = 1$ и $(g_j, p) = 1$.

Аналогично неравенству $\lambda_j \geq j\frac{p-2}{p-1}$ мы можем доказать неравенство

$\mu_j \geq j\frac{p-2}{p-1}$.

Теперь, так как $\nu_p\big(6(-y_0')^{j-3}\Delta_3\big) = 0$, то вынося из первой строчки определителя в $(*)$ $p^{min(\lambda_j,\lambda_{j-1})}$, а из второй строчки $p^{min(\mu_j,\mu_{j-1})}$, заключаем, что

$$min\big(\lambda_j, \lambda_{j-1}\big) + min\big(\mu_j, \mu_{j-1}\big) \leq 2j - 1.$$

Но

$$\mu_j \geq j\frac{p-2}{p-1} > (j-1)\frac{p-2}{p-1},$$

$$\mu_j \geq (j-1)\frac{p-2}{p-1},$$

и, следовательно,

$$(j-1)\frac{p-2}{p-1} + min\big(\lambda_j, \lambda_{j-1}\big) \leq 2j - 1.$$

Это и требовалось доказать.

Упражнение. Проведите аналогичное исследование для сравнения

$$ax^3 + y^3 \equiv 1(mod\ p^n), (a, p) = 1, p = 6k - 1.$$

§3. Задачи на неполную систему вычетов по модулю, равному степени простого числа.

Мы видели, что задача на неполную систему вычетов для сравнений вида

$$(1) \qquad F(x,y) \equiv 0(mod\ p^n),$$

Когда сравнение разрешено относительно одной из переменных, решается непосредственным применением теоремы о распределении дробных долей многочлена. Если же сравнение не разрешено относительно одной переменных, то для приведения задачи к удобному для нас виду надо пользоваться разложениями, которыми мы занимались в предыдущем параграфе. Мы в качестве примеров рассмотрим решение двух задач.

I. Пусть p – простое число, $k|(p-1), k \geq 2; a_x$ – вычет степени k по модулю p. Рассмотрим сравнение

$$(2) \qquad y^k \equiv a_x + pt(mod\ p^n)$$

Обозначим через $B(T_1, T_2, a_x)$ количество решений сравнения под условием $0 \leq y \leq T, 0 \leq t \leq T_1$.

Теорема. При дополнительных условиях

$$p \geq 3, \qquad n \geq k-1, \qquad n \geq 12, \quad p^3 \leq T \leq p^n, \qquad 1 \leq T_1 \leq p^{n-1}$$

Для $B(T_1, T_2, a_x)$ справедлива асимптотическая формула

$$B(T_1, T_2, a_x) = \frac{TT_1k}{p^n} + O\left((8k)^{3klog\ n}\left(\frac{T}{p}\right)^{1-\frac{1}{12k^2nlog\ n}}\right)$$

С абсолютной постоянной в символе “O”.

Д о к а з а т е л ь с т в о. Мы сначала будем считать, что T имеет специальный вид $T = pu - 1, 1 \leq u \leq p^{n-1}$.

Докажем, что для $B(pu-1,T_1,a_x)$ верна формула

$$B(pu-1,T_1,a_x)=\frac{uT_1k}{p^{n-1}}+O\left((8k)^{3klog\,n}(u)^{1-\frac{1}{12k^2nlog\,n}}\right)$$

Обозначим $b_x^{(j)}, j=1,\dots,k$, корни сравнения $y^k\equiv a_x(p)$.

По-прежнему будем считать, что $1\le a_x\le p-1,\ 1\le b_x^{(j)}\le p-1$.

Для каждого $t_1, 0\le t_1\le p^{n-1}-1$, найдется единственное t,

$0\le t\le p^{n-1}-1$, такое, что

$$\left(b_x^{(j)}+pt_1\right)^k\equiv a_x+pt(mod\,p^n)$$

Поэтому количество решений сравнения

$$y^k\equiv a_x+pt(mod\,p^n)$$

с $0\le t_1\le u-1, 0\le t\le T_1$.

Следовательно $B(pu-1,T_1,a_x)$ равно количеству дробных долей

$$\left\{\frac{\left(b_x^{(j)}+pt_1\right)^k-b_x^{(j)k}}{p^n}+\frac{b_x^{(j)}-a_x}{p^n}\right\}$$

Попавших на отрезок $\left[0,\frac{T_1}{p^{n-1}}\right]$, когда $j=1,2,..,k;\ t_1=0,\dots,u-1$.

Если обозначить через $\chi(t)$ характеристическую функцию отрезка $\left[0,\frac{T_1}{p^{n-1}}\right]$, то имеем

$$B(pu-1,T_1,a_x)=\sum_{j=1}^{k}\sum_{t_1=0}^{u-1}\chi\left(\left\{\frac{\left(b_x^{(j)}+pt_1\right)^k-b_x^{(j)k}}{p^n}+\frac{b_x^{(j)}-a_x}{p^n}\right\}\right).$$

К сумме

$$\sum_{t_1=0}^{u-1}\chi\left(\left\{\frac{\left(b_x^{(j)}+pt_1\right)^k-b_x^{(j)k}}{p^n}+\frac{b_x^{(j)}-a_x}{p^n}\right\}\right)$$

можно применить теорему И.М.Виноградова о распределении дробных долей многочлена. Мы ведём оценку по коэффициенту при ${t_1}^k$. Этот коэффициент равен $p^{-(n-k)}$. Мы применяем первый случай оценки.

Здесь

$p^{n-k} \le u \le p^{n-1}, \tau = (n-k)\cdot\frac{\log n}{\log u},\ l = \log\frac{12k(k-1)}{\tau}.$

Поэтому

$$\sum_{t_1=0}^{u-1} \chi\left(\left\{\frac{\left(b_x^{(j)}+pt_1\right)^k - b_x^{(j)k}}{p^n} + \frac{b_x^{(j)}-a_x}{p^n}\right\}\right) =$$

$$= \frac{uT_1}{p^{n-1}} + O\left((8k)^{\frac{1}{2}kl}u^{1-\frac{\tau}{3k^2l}}\right).$$

Поскольку оценка в символе "O" равномерная относительно j, то имеем

$$B(pu-1, T_1, a_x) = \frac{uT_1k}{p^{n-1}} + O\left((8k)^{\frac{1}{2}kl}u^{1-\frac{\tau}{3n^2l}}\right)$$

Так как

$$\frac{1}{n-1} \le \frac{n-k}{n-1} \le \tau \le 1; \log 12k(k-1) \le l \le \log 12k(k-1)(n-1).$$

То получаем

$$B(pu-1, T_1, a_x) = \frac{uT_1k}{p^{n-1}} + O\left((8k)^{3klog\,n}u^{1-\frac{\tau}{3k^2\log n}}\right)$$

Пусть теперь $T = pu - r, 1 \le r \le p$

Поскольку в сравнении

$$\left(b_x^{(j)} + pt_1\right) \equiv a_x + pt(mod\ p^n).$$

каждому $y = b_x^{(j)} + pt_1$ соответствует не более одного значения t,то

$$B(T, T_1, a_x) = B(pu-1, T_1, a_x) + O(p),$$

где $u = \frac{T_1r}{p}$.

Значит,

$$B(T,T_1,a_x)=\frac{TT_1k}{p^n}+\frac{rT_1k}{p^n}+O(p)+$$

$$+O\left((8k)^{3klog\,n}\left(\frac{r+T}{p}\right)^{1-\frac{\tau}{12k^2n\log n}}\right)$$

Но так как $r\le p\le T$, то $T+r\le 2T$,

$$\frac{rT_1k}{p^n}=O(k)=O((8k)^{3klog\,n})$$

В силу $T\ge p^3$, следует $\frac{T}{p}\ge p^2$

$$\left(\frac{T}{p}\right)^{1-\frac{\tau}{12k^2n\log n}}\ge p^{2\left(1-\frac{\tau}{12k^2n\log n}\right)}\ge p$$

Итак,

$$B(T,T_1,a_x)=\frac{TT_1k}{p^n}+O\left((8k)^{3klog\,n}\left(\frac{T}{p}\right)^{1-\frac{\tau}{12k^2n\log n}}\right)$$

2. Обозначим через $A(T,T_1)$ количество решений сравнения

$$x^2+y^2\equiv 1(mod\,p^n),$$

таких, что $y\not\equiv\pm1(mod\,p)$ и для которых $0\le x\le T$, а $0\le y\le T_1-1$.

Теорема. Пусть p −простое, $n\ge 13$,

$$1\le T\le p^n,\quad p^{\frac{4n+13}{6}}\le T_1\le p^n.$$

Для величины $A(T,T_1)$ имеем следующее асимптотическое выражение

$$A(T,T_1)=\frac{TT_1}{p^n}\cdot\frac{p-(-1)^{\frac{p-1}{2}}-2}{p}+O\left((12n)^{3nlog\,27n}(T_1)^{1-\frac{\tau}{48n^3\log n}}p^{\frac{\tau}{48n^3\log n}}\right)$$

с абсолютной постоянной в символе "O".

Д о к а з а т е л ь с т в о. Мы сначала будем предполагать, что

$T_1=pu-1$. Мы будем использовать p −адический ряд для корня x

сравнения

$$x^2 + (y_0 + pt)^2 \equiv 1(mod\ p)$$

Ясно, что $A(T, T_1)$ равно количеству дробных долей

$$\left\{x_i(0)\frac{\Phi_0(y_0) + p^{\lambda_1}\Phi_1(y_0)t + \cdots + p^{\lambda_s}\Phi_s(y_0)t^s}{p^n}\right\}$$

когда $i = 1,2,$ а y_0 пробегает все решения сравнения

$$x_0^2 \equiv 1 - y_0^2(mod\ p), y_0 \not\equiv \pm 1(mod\ p),$$

/всего $\frac{p-(-1)^{\frac{p-1}{2}}}{2} - 1$ значений /, а $t = 0,1, \dots, u-1$, попавших на отрезок $\left[0, \frac{T}{p^n}\right]$

Пусть $\chi(t)$ характеристическая функция отрезка $\left[0, \frac{T}{p^n}\right]$ периодически с периодом I, продолженная на всю вещественную ось.

Очевидно, что

$$A(T, pu-1) =$$

$$= \sum_{i=1}^{2}\sum_{y_0}\sum_{t=0}^{u-1}\chi\left(\frac{x_i(0)\left(\Phi_0(y_0) + p^{\lambda_1}\Phi_1(y_0)t + \cdots + p^{\lambda_s}\Phi_s(y_0)t^s\right)}{p^n}\right)$$

К внутренней сумме применим теорему И.М.Виноградова о распределении дробных долей многочлена.

Поскольку $s = \left[\frac{p-1}{p-2}n\right]$, то $s \geq n \geq \frac{2n-1}{3}$

Оценку будем вести по коэффициенту при $t^{\left[\frac{2n-1}{3}\right]}$ или при $t^{\left[\frac{2n-1}{3}\right]-1}$

Мы знаем, что

$$\min\left(\lambda_{\left[\frac{2n-1}{3}\right]}, \lambda_{\left[\frac{2n-1}{3}\right]-1}\right) \leq \frac{2n-1}{3} + \frac{\frac{2n-1}{3}-1}{p-1} \leq \frac{2n-1}{3} + \frac{\frac{2n-1}{3}-1}{2} = n-1$$

За α_r /в теореме И.М.Виноградова / берём коэффициент при t^j, где j равно тому из номеров $\left[\frac{2n-1}{3}\right]$ или $\left[\frac{2n-1}{3} - 1\right]$, для которого $\lambda_j \leq n-1$.

Итак,

$$2n-7 \le j \le \frac{2n-1}{3},$$

$$\frac{2n-7}{3} \cdot \frac{p-2}{p-1} \le \lambda_j \le n-1$$

Или

$$\frac{2n-7}{6} \le \lambda_j \le n-1$$

Так, как $(x_i(0), p) = 1$ и $\left(\Phi_j(y_0), p\right) = 1$, то коэффициент при t^j имеет вид несократимой дроби

$$\frac{x_l(0)\Phi_j(y_0)}{p^{n-\lambda_j}}, 1 \le n-\lambda_j \le \frac{4n+7}{6}$$

В силу $p^n \ge T_1 \ge p^{\frac{4n+13}{6}}$, имеем $p^{n-1} \ge u \ge p^{\frac{4n+7}{6}} \ge p^{n-\lambda_j}$

Выберем τ из условия $p^{n-\lambda_j} = u^\tau$.

Поскольку $u^\tau \le u$, то $\tau \le 1$. С другой стороны

$$p \le u^\tau, \qquad p \le p^{(n-1)\tau}, \qquad \frac{1}{n-1} \le \tau \le 1$$

Положим $l = \log \frac{12s(s-1)}{\tau}$

Имеем $\log 27n^2(n-1) \ge l \ge \log 12n(n-1)$

Отсюда

$$A(T, pu-1) = \sum_{i=1}^{2} \sum_{y_0} \left(\frac{uT}{p^n} + O\left((8s)^{\frac{1}{2}sl} u^{1-\frac{\tau}{3s^2 l}} \right) \right).$$

Оценки в символе "O" равномерные относительно y_0 и i. Поэтом

$$A(T, pu-1) = \frac{Tu\left(p - (-1)^{\frac{p-1}{2}} - 2\right)}{p^n} +$$

$$+O\left((8s)^{\frac{1}{2}slog27n^2(n-1)} pu^{1-\frac{\tau}{3s^2 log27n^2(n-1)}} \right)$$

Далее, так как $s \le \frac{3}{2}n$, то

$$A(T, pu-1) = \frac{Tu\left(p-(-1)^{\frac{p-1}{2}}-2\right)}{p^n} +$$

$$+O\left((12n)^{nlog27n^2(n-1)}\, pu^{1-\frac{\tau}{16n^3logn^3}}\right)$$

Пусть $T_1 = pu + r$, $1 \le r \le p$. Каждому $y \not\equiv \pm 1 (mod\ p)$ может соответствовать не более двух решений сравнения

$$x^2 + y^2 \equiv 1 (mod\ p^n)$$

Поэтому

$$A(T, T_1) = A(T, pu-1) + O(p) = \frac{Tu\left(p-(-1)^{\frac{p-1}{2}}-2\right)}{p^n} + O(p) =$$

$$+O\left((12n)^{3nlog27n^3}\, u^{1-\frac{\tau}{48n^3logn}}\right) = \frac{TT_1}{p^n}\cdot\frac{p-(-1)^{\frac{p-1}{2}}-2}{p} + O\left(\frac{T}{p^n}p\right) +$$

$$+ + O\left((12n)^{3nlog27n}\left(\frac{T_1}{p}\right)^{1-\frac{\tau}{48n^3logn}}\right)$$

Итак,

$$A(T, T_1) = \frac{TT_1}{p^n}\cdot\frac{p-(-1)^{\frac{p-1}{2}}-2}{p} + O\left((12n)^{3nlog27n}\, {T_1}^{1-\frac{\tau}{48n^3logn}} p^{\frac{\tau}{48n^3logn}}\right)$$

Теорема доказана.

Упражнение. Используя пример 2 предыдущего параграфа, найдите асимптотическую формулу для количества решений сравнения

$$ax^3 + y^3 \equiv 1 (mod\ p^n), \qquad (a, p) = 1, \qquad p = 6k - 1.$$

§4. Применение метода Л.Морделла к задаче на непролную систему вычетов по модулю $\mathbf{p^n}$.

Пусть p −простое число, $\xi = (\xi_1, \dots, \xi_m)$ −целочисленный $m-$ мерный вектор и пусть $f(\xi) -$ полином от ξ с целыми коэффициентами.

Пусть $l = (l_1, \dots, l_m)$ $m-$ мерный вектор с условием

$$0 \le l_1 < p^n, \dots, 0 \le (l_m) < p^n,$$

в дальнейшем будем обозначать это так $0 \le (l) < p^n$.

Обозначим через N'_m число решений сравнения

$$(1) \quad f(\xi) \equiv 0 (mod\ p^n), \qquad 0 \le (\xi) < (l), \qquad \text{т.е} \ \ 0 \le \xi_i < l_i,$$

а через N_m число решений сравнения

$$(2) \qquad f(x) \equiv 0 (mod\ p^n),\ 0 \le (x) < p^n.$$

Наша цель состоит в оценке числа N'_m через N_m.

Решение этой задаче основано на исследованиях Л.Морделле.

Мы имеем

$$(3) \qquad p^{(m+1)n} N'_m = \sum_{u=0}^{p^n-1} \sum_{(t)=0}^{p^n-1} \sum_{(x)=0}^{p^n-1} \sum_{(\xi)}^{(l)} e^{2\pi i \frac{4f(2)+t-(x-\xi)}{p^n}},$$

где $t\ m-$ мерный вектор, а $t \cdot (x-\xi)$ есть скалярное произведение векторов t и $(x-\xi$.

Действительно, в силу соотношения

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{ax}{q}} = \begin{cases} q, \text{если } a \vdots q, \\ 0, \text{если } a \nmid q, \end{cases}$$

Суммирование по t и u даёт нуль, за исключением того случая, когда $x = \xi, f(\xi) \equiv 0 (mod\ p^n)$

Предположим теперь, что мы имеем оценки тригонометрических сумм, независящие от t:

$$(4) \qquad \left|\sum_{u}\sum_{(x)} e^{2\pi i\frac{uf(x)+t\cdot x}{p^n}}\right| \le E_m^{(r)},$$

где r означает число ненулевых координат вектора t

Мы докажем, что

$$(5) \qquad N'_m = l_1,\dots,l_m p^{-nm}N_m + \theta_m^{(m)}E_m^{(m)}p^{-n}(\log p^n)^m + R_m,$$

где

$$(6) \quad R_m = \sum_{r=1}^{m-1}\sum_{i_1,\dots,i_{m-r}} \theta_m^{(r)} l_{i_1},\dots,l_{i_{m-r}}E_m^{(r)}p^{(r-m-1)n}(\log p^n)^r, \left|\theta_m^{(r)}\right| < 1.$$

В самом деле, если в (3) все координаты t равны нулю, то такому t соответствует член $l_1,\dots,l_m p^n N_m$.

Пусть теперь r координат вектора t, например, $t_1,\dots,t_r$, отличны от нуля. Суммируя в (3) по ξ, получим выражение

$$(7) \quad l_{r+1},\dots,l_m \sum_{u}\sum_{(x)}\sum_{(t)}^{*} e^{2\pi i\frac{uf(x)+t\cdot x}{p^n}} \cdot \frac{1-e^{-2\pi i\frac{l_1 t_1}{p^n}}}{1-e^{-2\pi i\frac{t_1}{p^n}}} \dots \frac{1-e^{-2\pi i\frac{l_r t_r}{p^n}}}{1-e^{-2\pi i\frac{t_r}{p^n}}},$$

где $*$ означает, что суммирование ведётся только по $t_1,\dots,t_r$, причём $t_1,\dots,t_r \neq 0$.

Выражение (7) по абсолютной величине меньше, чем

$$l_{r+1},\dots,l_m \sum_{(t)}^{*} E_m^{(r)}\left(\sin\frac{\pi t_1}{p^n}\dots\sin\frac{\pi t_r}{p^n}\right)^{-1} < l_{r+1},\dots,l_m E_m^{(r)}p^{2n}(\log p^n)^r$$

Суммируя теперь по r и учитывая комбинации различных наборов из r индексов, получим соотношения (5) и (6).

Замечание 1. Величина $E_m^{(r)}$ получается более точной, если оценки суммирования по x в (4) находятся в зависимости от u.

Следуя также отметить, что если некоторые из l_i кратны p^{n-1}, то в выражении (7) можно считать, что при суммировании по соответствующему t_i оно принимает значения, взаимно простые с p, и значит в (4) оценка ведётся по всем значениям t_i, и взаимно простых с p. Этим фактом мы в дальнейшем воспользуемся.

Замечание 2. Из вывода формул (5) и (6) видно, что они остаются справедливыми, если на сравнения (1) и (2) накладываются некоторые дополнительные ограничения, общие для этих сравнений. Например, решения ищутся в классе векторов ξ и x, все координаты которых взаимно простых с p.

Применим теперь полученные результаты к задаче о распределении решений сравнения

$$(8)\quad \begin{matrix} ax^3 + y^3 \equiv 1 (mod\ p^n),\ \ (a,p) = 1, \quad p = 6k - 1, \\ 0 \le x < T_1, \quad 0 \le y < T_2. \end{matrix}$$

Решение ищется в классе пар чисел (x, y), для которых $(y, p) = 1$.

Аналогично тому, как было сделано в примере 3 второго параграфа этой главы, можно показать, что все решения сравнения описываются так

$$x = x_0 + pt, y = y(0)\varphi(t),$$

где x_0 пробегает все числа $0,1,\dots,p-1$, за исключением одного, для которого $ax_0{}^3 \equiv 1(mod\ p)$, а $\varphi(t)$ многочлен с целыми коэффициентами

$$\varphi(t) = a_0 + a_1 p^{\lambda_1} t + \cdots + a_s p^{\lambda_s} t^s,$$

причём

$$\lambda_i \ge i\frac{p-2}{p-1} > 0, \qquad i = 4,5,\dots,s;$$

а $y(0)$ −решение сравнения $ax^3 + y^3 \equiv 1(mod\ p^n)$.

Но тогда наша задача эквивалентна задаче о распределении решений сравнения вида

$$(9)\quad \begin{matrix} y \equiv y(0)\varphi(t)(mod\ p^n) \\ 0 \le y \le T_2, \quad 0 \le t < \left[\frac{T_1}{p}\right] = Q. \end{matrix}$$

Поэтому, если для каждого фиксированного x_0 удастся найти распределение решений сравнения (9), не зависящее от x_0, то и задача о распределении решений сравнения (8) будет решена.

Мы для удобства заменим t на x в (9) и тогда имеем

$$(10)\quad f(x, y) = y(0)\varphi(t) - y.$$

Итак, решается задача

$$(11)\quad f(x,y)\equiv 0(mod\ p^n),\qquad 0\le x<Q,\qquad 0\le y\le T_2,\qquad (y,p)=1.$$

Будем сначала считать, что $T_2=kp^{n-1},\ 0<k\le p$.

В силу формул (5) и (6) имеем

$$(12)\quad N'_{\theta,T_2}=\frac{QT_2}{p^{2n}}N+\theta E_2^{(2)}p^{-n}(\log p^n)^2+R_2,\qquad |\theta|\le 1,$$

где

$$(13)\quad R_2=\theta' E_2^{(1)}(Q+T_2)p^{-2n}\log p^n,\quad |\theta'|\le 1.$$

Здесь N'_{θ,T_2} −число решений сравнения (11), а N −число решений сравнения

$$(14)\quad y\equiv y(0)\left(a_0+a_1p^{\lambda_1}x+\cdots+a_sp^{\lambda_s}x^s\right)(mod\ p^n),\quad (y,p)=1.$$

Из оценки показателей λ_i видно, что $\varphi(x)$ по модулю p есть многочлен степени не выше 3, и , следовательно, сравнение $\varphi(x)\equiv 0(p)$ имеет не более трёх решений.

Отсюда следует, что при $x=0,1,\dots,p^n-1$ многочлен $\varphi(x)$ не более $3p^{n-1}$ раз принимает значения, кратные p.

Далее, сравнение

$$f(x,y)\equiv 0(mod\ p^n)$$

имеет ровно p^nрешений, ибо при каждом значении x величина y определяется однозначно, причём не более $3p^{n-1}$ раз y будет кратно p. Таким образом, имеем

$$N=p^n+O(p^{n-1})$$

с абсолютной постоянной в символе "O".

Для получения оценок $E_2^{(1)}$ и $E_2^{(2)}$ воспользуемся теоремой:

Теорема. Пусть $f(x)=a_1x+\cdots+a_kx^k-$ многочлен с целыми коэффициентами и пусть m −наибольшее целое, такое, что

$$(a_m,p)=1.$$

Тогда, если $1\le m<p$, то имеет место оценка

$$\left|\sum_{x=1}^{p^n} e^{2\pi i\frac{f(x)}{p^n}}\right| \le m^n p^{n\left(1-\frac{1}{m}\right)}$$

Д о к а з а т е л ь с т в о. Для $n = 1$ утверждение теоремы было доказано Карлицем и Утиямой на основе доказанной А.Вейлем гипотезы Римана для алгебраических кривых над конечным полем. Это доказательство довольно сложное и мы его воспроизводить не будем.

Для $n \ge 2$ проведём доказательство методом математической индукции.

Имеем

$$\sum_{x=1}^{p^n} e^{2\pi i\frac{f(x)}{p^n}} = \sum_{y=0}^{p^{n-1}-1}\sum_{z=0}^{p-1} e^{2\pi i\frac{f\left(y+p^{n-1}z\right)}{p^n}} =$$

$$= \sum_{y=0}^{p^{n-1}-1}\sum_{z=0}^{p-1} e^{2\pi i\frac{f(y)+p^{n-1}zf'(y)}{p^n}}$$

Если теперь $f'(y) \not\equiv 0(mod\ p)$, то суммирование по z даёт нуль. Поэтому , если $\alpha_1, \dots, \alpha_l$ −все корни сравнения $f'(y) \equiv 0(p)$, то имеем

$$\left|\sum_{x=1}^{p^n} e^{2\pi i\frac{f(x)}{p^n}}\right| = \left|\sum_{j=1}^{l}\sum_{x\not\equiv\alpha_j(p)}^{p^n} e^{2\pi i\frac{f(x)}{p^n}}\right| \le$$

$$\le l\max_{1\le j\le l}\left|\sum_{y=1}^{p^{n-1}} e^{2\pi i\frac{f(\alpha_i+py)}{p^n}}\right| = l\max_{1\le j\le l}\left|\sum_{x=1}^{p^{n-1}} e^{2\pi i\frac{f(\alpha_i+py)-f(\alpha_i)}{p^n}}\right| =$$

$$= l\max_{1\le j\le l}\left|\sum_{x=1}^{p^{n-1}} e^{2\pi i\frac{g_j(x)}{p^{n-\mu_j}}}\right|,$$

где p^{μ_j} −наивысшая степень p, делящая все коэффициенты

$f\left(\alpha_j + py\right) - f\left(\alpha_j\right)$, а через $g_j(x)$ обозначен многочлен

$$f\left(\alpha_j + py\right) - f\left(\alpha_j\right) = p^{\mu_j} g_j(x)$$

Очевидно, $f^{(m)}(\alpha_j) \not\equiv 0(p)$, а поэтому $1 \le \mu_j \le m$. Легко также заметить, что $0 \le l \le m$.

Поэтому имеем

$$\left|\sum_{x=1}^{p^n} e^{2\pi i\frac{f(x)}{p^n}}\right| \le \max_{1\le j\le l} p^{\mu_j-1}\left|\sum_{x=1}^{p^{n-\mu_j}} e^{2\pi i\frac{g_j(x)}{p^{n-\mu_j}}}\right| \le$$

$$\le \max_{1\le j\le l} p^{\mu_j\left(1-\frac{1}{m}\right)}\left|\sum_{x=1}^{p^{n-\mu_j}} e^{2\pi i\frac{g_j(x)}{p^{n-\mu_j}}}\right|$$

причём многочлен $g_j(x)$ удовлетворяет всем условиям теоремы с тем же значением m.

Применяя теперь индукцию, получим

$$\left|\sum_{x=1}^{p^n} e^{2\pi i\frac{f(x)}{p^n}}\right| \le \max_{1\le j\le l} l^{n-\mu_j}\ p^{\mu_j\left(1-\frac{1}{m}\right)}\ p^{(n-\mu_j)\left(1-\frac{1}{m}\right)} \le$$

$$\le\ l^n\ p^{n\left(1-\frac{1}{m}\right)} \le\ m^n\ p^{n\left(1-\frac{1}{m}\right)}$$

Переходим к оценке $E_2^{(2)}$. Имеем

$$\left|E_2^{(r)}\right| = \left|\sum_{u=0}^{p^n-1}\sum_{x,y=0}^{p^n-1} e^{2\pi i\left(u\frac{y(0)\varphi(x)-y}{p^n}+\frac{t_1x+t_2y}{p^n}\right)}\right| =$$

$$= \left|\sum_u\sum_y e^{2\pi i\frac{t_2-u}{p^n}y}\sum_x e^{2\pi i\frac{uy(0)\varphi(x)-t_1x}{p^n}}\right|$$

Откуда

$$E_2^{(r)} \le \sum_u\left|\sum_y e^{2\pi i\frac{t_2-u}{p^n}y}\right|\cdot\left|\sum_x e^{2\pi i\frac{uy(0)\varphi(x)-t_1x}{p^n}}\right|$$

Сумма $\sum_y e^{2\pi i\frac{t_2-u}{p^n}y}$ равна нулю, за исключением только одного случая $u = t_2$, когда она равна p^n.

Если теперь воспользоваться замечанием I, то найдём, что суммирование по u ведётся лишь по числам, взаимно простыми с p.

При этих условиях к сумме

$$\sum_x e^{2\pi i \frac{uy(0)\varphi(x)-t_1 x}{p^n}}$$

применима доказанная выше теорема, причём $m \leq 3$.

Итак, имеем

$$E_2^{(r)} \leq p^n \cdot 3^n p^{\frac{2}{3}n} = 3^n p^{\frac{5}{3}n}, r = 1,2$$

Отсюда получаем

$$(15) \quad N'_{\theta,T_2} = \frac{QT_2}{p^n} + O\left(\frac{QT_2}{p^{n+1}}\right) + O\left(3^n p^{\frac{5}{3}n} (\log p^n)^2\right) +$$

$$+O\left(3^n \frac{Q+T_2}{p^{\frac{1}{5}n}} \log p^n\right)$$

Пусть теперь

$$kp^{n-1} < T_2 < (k+1)p^{n-1}$$

Тогда очевидно

$$N'_{\theta,kp^{n-1}} \leq N'_{\theta,T_2} \leq N'_{\theta,(k+1)p^{n-1}}$$

Отсюда следует, что

$$N'_{\theta,T_2} = \frac{QT_2}{p^n} + O\left(\frac{QT_2}{p^n k}\right) + O\left(3^n p^{\frac{2}{3}n} (\log p^n)^2\right) +$$

$$+O\left(3^n \frac{Q+T_2}{p^{\frac{1}{n}n}} \log p^n\right)$$

Или

$$(16) \quad N'_{\theta,T_2} = \frac{QT_2}{p^n} + O\left(\frac{QT_2}{p^n} \cdot \frac{1}{k}\right) + O\left(e^{2n} p^{\frac{2}{3}n} (\log p)^2\right)$$

С абсолютной постоянной в символах "O".

Обозначим теперь через $A(T_1, T_2)$ число решений сравнения (8)

Тогда, учитывая равномерность оценки (16) относительно x_0, получим

Теорема. Пусть

$$p^{n-1} < T_2 < p^n$$

Тогда имеет место асимптотическая формула

$$A(T_1, T_2) = \frac{T_1 T_2}{p^n} \cdot \frac{p-1}{p} + O\left(\frac{T_1}{p}\right) + O\left(e^{2n} p^{\frac{2}{3}n} (\log p)^2\right).$$

Упражнение. Найдите асимптотическую формулу для числа решений сравнения

$$x^2 + y^2 \equiv 1 (mod p^n), \qquad 1 \le x_1 \le T_1, 1 \le y_2 \le T_2,$$

используя метод Л.Морделла.

Список литературы

1. И.М. Виноградов, Метод тригонометрических сумм в теории чисел, Москва, «Наука», 1971.
2. Г. Дэвенпорт, Мультипликативная теория чисел, Москва, «Наука», 1971.
3. А.Е. Ингам, Распределение простых чисел, Москва, Главная редакция общетехнической литературы и номографии, 1936.
4. А.А. Карацуба, Основы аналитической теории чисел, Главная редакция физико-математической литературы изд-ва «Наука», 1975.
5. Х. Монтгомери, Мультипликативная теория чисел, Москва, «Мир», 1974.
6. К. Прахар, Распределение простых чисел, Москва, «Мир», 1967.
7. Е.К. Титчмарш, Теория дзета-функции Римана, Москва, ИЛ, 1953.
8. Хуа Ло-кен, Метод тригонометрических сумм и его применения в теории чисел, Москва, «Мир», 1964.
9. К. Чандрасекхаран, Арифметические функции, Москва, «Мир», 1975.
10. Н.Г. Чудаков, Введение в теорию L-функций Дирихле, Москва, Гостехиздат, 1947.