МАТЕМАТИКА

УДК 511.2

О ЧИСЛЕ ТОЧЕК НА ОДНОМ КЛАССЕ КРИВЫХ В КОЛЬЦЕ ВЫЧЕТОВ

В.И. Мурашко[1], **А.А. Печёнкин**[2]

[1]*Гомельский государственный университет им. Ф. Скорины*
[2]*Московский Физико-технический институт*

ON THE NUMBER OF POINTS ON ONE CLASS OF CURVES IN A RING OF RESIDUES

V.I. Murashka[1], **A.A. Piachonkin**[2]

[1]*F. Scorina Gomel State University*
[2]*Moscow Institute of Physics and Technology*

Найдено число точек на произвольной кривой вида $x^m \equiv y^k (mod\, n)$. Введено понятие *m/k-ичного вычета* (рационального степенного вычета). Найдено количество рациональных степенных вычетов по модулю произвольного натурального числа. В качестве следствия получен классический результат о количестве квадратичных вычетов по составному модулю.

Ключевые слова: *алгебраическая кривая*, *число точек на алгебраической кривой*, *степенной вычет*, *первообразный корень*, *индексы по модулю* 2^α.

The number of points on a curve $x^m \equiv y^k (mod\, n)$ is calculated. The concept of *m/k-power residue* (rational power residue) is introduced. Let *n* be a natural number. The number of rational power residues modulo *n* is calculated. As a corollary the classic result on the number of quadratic residues is obtained.

Keywords: algebraic curve, number of points on an algebraic curve, power residue, primitive root, indices modulo 2^α.

Введение

Во всей работе через *n*, *k* и *m* мы обозначаем некоторые натуральные числа. Напомним, что число *a* называется *m-ичным* (*степенным*) *вычетом* по модулю *n*, если разрешимо сравнение $x^m \equiv a\ (mod\, n)$. Первое систематическое изучение квадратичных вычетов было произведено К. Гауссом в его работе «Арифметические исследования», 1801, [1]. В 1996 году W. Stangl в работе [2] вычислил количество *квадратичных вычетов* по модулю *n*. В работе [3] была получена формула для числа *кубических вычетов* по модулю произвольного натупального числа. Наконец, в 2010 году М.А. Королёв в работе [4] предложил формулу для количества *m-ичных вычетов* по модулю *n*.

Заметим, что задача о числе степенных вычетов совпадает с задачей о количестве различных решений сравнения $x^m - y \equiv 0\ (mod\, n)$. Таким образом, в упомянутых выше работах рассматривался частный случай задачи о количестве различных решений сравнения

$$f(x_1,...,x_k) \equiv 0\ (mod\, n),$$

где $f(x_1,...,x_k)$ – многочлен от k переменных с целыми коэффициентами. Другим ярким примером данной задачи является задача о количестве точек на эллиптической кривой, оценка числа которых по простому модулю была дана Х. Хассе в 1936 году. Отметим также, что в работе [5] изучалось количество точек на модулярных гиперболах.

Ввиду этого, для $I = \{i_1,...,i_t\} \subseteq \{1,...,k\}$ через $R_{f,I}(n)$ (соотв. $R^*_{f,I}(n)$) обозначим количество комбинаций вычетов $(y_1,...,y_t)\ (mod\, n)$, таких что сравнение $f(x_1,...,x_k) \equiv 0 (mod\, n)$ имеет решение при $x_{i_1} \equiv y_1,...,x_{i_t} \equiv y_t\ (mod\, n)$ (соотв. таких, что $(y_j, n) = 1\ \ \forall j \in \{1,...,t\}$). Если $I = \{1,...,k\}$, то положим $R_{f,I}(n) = R_f(n)$ и $R^*_{f,I}(n) = R^*_f(n)$.

В данной работе нас будет интересовать число обобщённых степенных вычетов в смысле следующего определения:

Определение. *Число a является m / k-ичным вычетом по модулю n, если разрешимо сравнение вида* $x^m \equiv a^k (mod\, n)$.

Другими словами, задача о количестве m/k вычетов есть задача о числе различных значений, которые может принимать вторая координата точек на кривой $x^m - y^k \equiv 0 (mod\, n)$, то есть необходимо вычислить величину $R_{x^m - y^k, \{2\}}(n)$.

1 Мультипликативность основных функций

Напомним, что $(q_1,...,q_k)$ – НОД чисел $q_1,...,q_k$, $[q_1,...,q_k]$ – НОК чисел $q_1,...,q_k$.

***Теорема* 1.1.** *Пусть* $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ *– каноническое разложение числа n. Тогда функции* $R_{f,I}(n)$ *и* $R^*_{f,I}(n)$ *являются мультипликативными функциями, то есть справедливы следующие равенства*

$$R_{f,I}(n) = \prod_{i=1}^{k} R_{f,I}(p_i^{\alpha_i}),\ R^*_{f,I}(n) = \prod_{i=1}^{k} R^*_{f,I}(p_i^{\alpha_i}).$$

Доказательство. Сначала докажем, что $R_{f,I}(n)$ является мультипликативной функцией. Рассмотрим сравнение

$$f(x_1,...,x_k) \equiv 0 (mod\ n). \qquad (1.1)$$

Предположим, что $n = n_1 \cdot n_2, \quad (n_1, n_2) = 1.$ Тогда каждому решению сравнения (1.1) по модулю *n* ставятся в соответствие решения аналогичных сравнений по модулям n_1 и n_2 соответственно. При этом, если какие-то координаты двух решений по модулю *n* совпадают, то очевидно, что эти же координаты совпадают у полученных решений и по модулю n_1, и по модулю n_2. Поэтому имеем

$$R_{f,I}(n) \le R_{f,I}(n_1) \cdot R_{f,I}(n_2).$$

С другой стороны, пусть $y_1,...,y_k$ – решение аналогичного (1.1) сравнению по модулю n_1, а $z_1,...,z_k$ – по модулю n_2. Так как *f* – многочлен, то из бинома Ньютона следует, что значения *f* по модулю *m* сравнимы на наборах, сравнимых по модулю *m* аргументов. Согласно Китайской теореме об остатках, найдется единственное решение $x_1,...,x_k$ сравнения (1.1), такое что

$$\begin{cases} x_1 \equiv y_1 (mod\ n_1) \\ x_1 \equiv z_1 (mod\ n_2) \end{cases} \cdots \begin{cases} x_k \equiv y_k (mod\ n_1) \\ x_k \equiv z_k (mod\ n_2). \end{cases}$$

Пусть у двух решений сравнения (1.1) Y_1 и Y_2 по модулю n_1 соответвующие координаты с индексами из *I* совпадают. Аналогично и для решений Z_1 и Z_2 по модулю n_2. Тогда из выше доказанного следует, что у соответсвующих решений X_1 и X_2 сравнения (1.1) по модулю *n* соответствующие координаты с индексами из *I* совпадают. Если же хотя бы одна из координат с индексами из *I* не совпадает у Y_1 и Y_2 или у Z_1 и Z_2, то координата с тем же индексом у X_1 и X_2 также не совпадает. Следовательно, имеем

$$R_{f,I}(n) \ge R_{f,I}(n_1) \cdot R_{f,I}(n_2).$$

Итак, $R_{f,I}(n) = R_{f,I}(n_1) \cdot R_{f,I}(n_2)$. Доказательство того факта, что $R^*_{f,I}(n)$ является мультипликативной функцией, проводится аналогично с учетом того факта, что $(x,n) = 1$ тогда и только тогда, когда $(x,n_1) = 1$ и $(x,n_2) = 1$. □

***Следствие* 1.1.** *Функции* $R_{f(x_1,...,x_k)}(n)$ *и* $R^*_{f(x_1,...,x_k)}(n)$ *являются мультипликативными.*

Доказательство. Следует из теоремы 1.1 при $I = \{1,...,k\}$. □

Через

$$s_{f(x)}(n) = R_{f(x)-y,\{2\}}(n)$$

будем обозначать число различных значений многочлена *f*(*x*) по модулю *n*. Аналогично через

$$s^*_{f(x)}(n) = R^*_{f(x)-y,\{2\}}(n)$$

будем обозначать число различных значений многочлена *f*(*x*) по модулю *n*, взаимно простых с *n*.

***Следствие* 1.2.** *Функции* $s_{f(x)}(n)$ *и* $s^*_{f(x)}(n)$ *являются мультипликативными.*

Доказательство. Следует из теоремы 1.1. □

2 Вычисление $R^*_{f,I}(p^\alpha)$

***Определение* 2.1** [6, гл. 6, с. 92–93]. *Первообразным корнем по модулю n называется число a, такое что порядок a равен* $\varphi(n)$. *Т. е.* $\forall b:$ $(b,n) = 1 \ \exists\ i \in \mathbb{N}:\ a^i \equiv b (mod\ n)$.

Теорема о существовании первообразного корня [6, гл. 6, с. 105]. *Первообразные корни существуют только по модулю* $2, 4, p^\alpha, 2p^\alpha$, *где p – любое нечётное простое.*

***Лемма* 2.1.** *Верны следующие тождества*

$$R_{im-jk}(n) = n \cdot (m,k,n) \qquad (2.1)$$

$$R_{im-jk,\{2\}}(n) = \frac{n \cdot (m,k,n)}{(m,n)}. \qquad (2.2)$$

Доказательство. Имеем

$$im \equiv jk (mod\ n). \qquad (2.3)$$

Пусть $d = (m,k,n), \quad m = m_1 \cdot d, \quad k = k_1 \cdot d.$ Тогда имеем

$$im \equiv jk (mod\ n) \Leftrightarrow im_1 \equiv jk_1 \left(mod\ \frac{n}{d} \right). \qquad (2.4)$$

Пусть $m' = \left(m_1, \frac{n}{d} \right), \quad m_1 = m'm_2.$ Тогда имеем

$$im_1 \equiv jk_1 \left(mod\ \frac{n}{d} \right) \Leftrightarrow im'm_2 \equiv jk \left(mod\ \frac{n}{d} \right).$$

Заметим, что левая часть последнего сравнения кратна m' и $\frac{n}{d}$ кратно m'. Так как по ранее предположенному $(k_1, m') = 1$ имеем, что $j = m' \cdot j_1.$ Тогда имеем

$$im'm_2 \equiv jk \left(mod\ \frac{n}{d} \right) \Leftrightarrow im_2 \equiv j_1 k_1 \left(mod\ \frac{n}{dm'} \right). \qquad (2.5)$$

Аналогичную операцию проделываем с k_1. В итоге, имеем

$$\begin{gathered} im_2 \equiv j_1 k_1 \left(mod\ \frac{n}{dm'} \right) \Leftrightarrow \\ \Leftrightarrow i_1 m_2 \equiv j_1 k_2 \left(mod\ \frac{n}{dm'k'} \right). \end{gathered} \qquad (2.6)$$

где $k' = \left(k_1, \frac{n}{dm'}\right)$, $k_1 = k' \cdot k_2$. Напомним хорошо известный факт: сравнение вида $ax \equiv b\,(mod\ n)$ всегда имеет единственное решение при $(a,n) = 1$. Из данного утверждения следует, что существует f – биекция из $\mathbb{Z}_q$ в $\mathbb{Z}_q$, $q = \frac{n}{dm'k'}$, такая что $tm_2 \equiv f(t)k_2\,(mod\ q)$. Значит, число решений сравнения (2.6) равно q.

Теперь заметим, что каждое значение i_1 в сравнении (2.6) однозначно задает значение i в сравнении (2.5), а каждому значению j_1 из сравнения (2.6) соответствует k' значений j_1 из сравнения (2.5). Следовательно, число решений сравнения (2.5) имеет вид $q \cdot k'$. Используя аналогичные соображения, получаем, что число решений сравнения (2.4) имеет вид $q \cdot k' \cdot m'$.

Далее, заметим, что каждому значению i_1 из сравнения (2.4) соответствует ровно d значений i из сравнения (2.3). Аналогично для j_1 и j. Следовательно, имеем

$$R_{im-jk}(n) = q \cdot k' \cdot m' \cdot d^2 = n \cdot d = n \cdot (m,k,n).$$

Если считать число возможных различных значений только для второй координаты, то по предыдущим рассуждениям имеем

$$R_{im-jk,\{2\}}(n) = q \cdot k' \cdot d = \frac{n}{m'} = \frac{n}{\left(\frac{m}{d}, \frac{n}{d}\right)} = \frac{n \cdot (m,k,n)}{(m,n)}. \square$$

***Теорема* 2.1.** *Пусть p – простое число и $\alpha \geq 1$. Тогда число решений сравнения $x^m - y^k \equiv 0\,(mod\ p^\alpha)$, взаимно простых с p, имеет следующий вид*

$$R^*_{x^m-y^k}(p^\alpha) =$$

$$= \begin{cases} \varphi(p^\alpha) \cdot (m,k,\varphi(p^\alpha)), & p \neq 2; \\ 2^{\alpha-1} \cdot (2 \cdot m, 2 \cdot k, 2^{\alpha-1}), & p = 2, m, k \vdots 2; \\ 2^{\alpha-1}, & \text{в противном случае.} \end{cases}$$

Доказательство. Рассмотрим два случая:

Случай 1. $p \neq 2$. Согласно *теореме о существовании первообразного корня*, существует *первообразный корень* по модулю p^α. Обозначим его через β. Так как мы рассматриваем взаимно простые с p решения сравнения $x^m - y^k \equiv 0\,(mod\ p^\alpha)$, можем произвести замены $x = \beta^i$, $y = \beta^j$. Тогда имеем

$$x^m - y^k \equiv 0\,(mod\ p^\alpha) \Leftrightarrow \beta^{im} \equiv \beta^{jk}\,(mod\ p^\alpha).$$

Из свойств первообразного корня имеем

$$\beta^{im} \equiv \beta^{jk}\,(mod\ p^\alpha) \Leftrightarrow im \equiv jk\,(mod\ \varphi(p^\alpha)).$$

Согласно тождеству (2.1) из леммы 2.1, число решений последнего сравнения – $\varphi(p^\alpha) \cdot (m,k,\varphi(p^\alpha))$. Следовательно, имеем

$$R^*_{x^m-y^k}(p^\alpha) = \varphi(p^\alpha) \cdot (m,k,\varphi(p^\alpha)).$$

Случай 2. $p = 2$. Пусть $\alpha = 1$. Тогда нетрудно видеть, что $\forall m,k \in \mathbb{N}$ имеем $R^*_{x^m-y^k}(2) = 1$.

Пусть $\alpha \geq 2$. Согласно [6, гл. 6, с. 102–104], любое нечётное число по модулю 2^α можно представить в виде $(-1)^q 5^\delta$, $q \in \mathbb{Z}_2$, $\delta \in \mathbb{Z}_{2^{\alpha-2}}$. Тогда наше сравнение сводится к виду

$$x^m - y^k \equiv 0\,(mod\ 2^\alpha) \Leftrightarrow$$

$$\Leftrightarrow (-1)^{mq_1} 5^{m\delta_1} \equiv (-1)^{kq_2} 5^{k\delta_2}\,(mod\ 2^\alpha).$$

Из свойств индексов по модулю 2 имеем

$$(-1)^{mq_1} 5^{m\delta_1} \equiv (-1)^{kq_2} 5^{k\delta_2}\,(mod\ 2^\alpha) \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} mq_1 \equiv kq_2\,(mod\ 2), & (2.7) \\ m\delta_1 \equiv k\delta_2\,(mod\ 2^{\alpha-2}). & (2.8) \end{cases}$$

Далее возможны следующие случаи:

$$2 \mid m,k, \quad (2.9)$$

$$2 \mid m, 2 \nmid k, \quad (2.10)$$

$$2 \nmid m, 2 \mid k \quad (2.11)$$

$$2 \nmid m,k. \quad (2.12)$$

Рассмотрим случай (2.9). Очевидно, что в этом случае сравнение (2.7) имеет 4 решения. Для подсчета числа решений сравнения (2.8) воспользуемся тождеством (2.1) из леммы 2.1 и получим $2^{\alpha-2} \cdot (m,k,2^{\alpha-2})$ решений. Следовательно, число решений исходного сравнения в данном случае имеет вид

$$R^*_{x^m-y^k}(2^\alpha) = 4 \cdot 2^{\alpha-2} \cdot (m,k,2^{\alpha-2}) = 2^\alpha \cdot (m,k,2^{\alpha-2}).$$

Теперь рассмотрим случаи (2.10), (2.11), (2.12). Очевидно, что в каждом из этих случаев сравнение (2.7) имеет ровно 2 решения. Для подсчета числа решений сравнения (2.8) снова воспользуемся тождеством (2.1) леммы 2.1 и получим $2^{\alpha-2}$ решений, так как $(m,k,2^{\alpha-2}) = 1$. Следовательно, число решений исходного сравнения в данном случае имеет вид $2 \cdot 2^{\alpha-2} = 2^{\alpha-1}$. Объединяя все выше описанное, получаем формулу, которую и требовалось доказать. $\square$

***Теорема* 2.2.** *Пусть p – простое число и $\alpha \geq 1$. Тогда число таких y $(mod\ p^\alpha)$, таких что сравнение $x^m - y^k \equiv 0\,(mod\ p^\alpha)$, взаимно простых с p, разрешимо, имеет вид*

$$R^*_{x^m-y^k,\{2\}}(p^\alpha) =$$

$$= \begin{cases} \dfrac{\varphi(p^\alpha) \cdot (m,k,\varphi(p^\alpha))}{(m,\varphi(p^\alpha))}, & p \neq 2; \\ 1 & p = 2, \alpha = 1; \\ \dfrac{2^{\alpha-2}}{(m,2^{\alpha-2})}, & p = 2, \alpha \geq 2, 2 \mid m, 2 \nmid k; \\ \dfrac{2^{\alpha-1} \cdot (m,k,2^{\alpha-2})}{(m,2^{\alpha-2})}, & \text{в противном случае.} \end{cases}$$

Доказательство. Аналогично доказательству теоремы 2.1 с использованием тождества (2.2) из леммы 2.1. □

***Замечание* 2.1.** *Согласно ранее введённому определению, в теореме 2.2 было посчитано число m / k-ичных вычетов по модулю p^α, взаимно простых с p.*

***Замечание* 2.2.** *Пусть $q \in \mathbb{N}$. Тогда, вообще говоря, количества m / k-ичных и qm / qk-ичных вычетов по модулю n, взаимно простых с n, могут не совпадать. Пример: p – нечётное простое, $m = q = p, k = 1$. Тогда*

$$R^*_{x^m - y^k,\{2\}}(p^2) = p - 1 \neq p(p-1) = R^*_{x^{qm} - y^{qk},\{2\}}(p^2).$$

***Следствие* 2.1.** *Пусть p – простое число. Число m-ичных вычетов по модулю p^α, взаимно простых с p имеет вид*

$$s^*_{x^m}(p^\alpha) =$$

$$= \begin{cases} \dfrac{\varphi(p^\alpha)}{(m, \varphi(p^\alpha))}, & p \neq 2; \\ 2^{\alpha-1}, & p = 2, 2 \nmid m; \\ 2^{\alpha-2-t}, & p = 2, \alpha > t+1, t \in \mathbb{N} : 2^t \mid m, 2^{t+1} \nmid m; \\ 1, & \text{в противном случае.} \end{cases}$$

Доказательство. Напомним, что

$$s^*_{x^m}(p^\alpha) = R^*_{x^m - y,\{2\}}(p^\alpha).$$

Следовательно, выше приведенная формула является следствием из теоремы 2.2 при $n = 1$. □

3 Вычисление $R_{f,l}(p^\alpha)$

***Теорема* 3.1.** *Пусть p – простое число и $\alpha \geq 1$. Тогда число решений сравнения $x^m - y^k \equiv 0 (mod\ p^\alpha)$ имеет вид*

$$R_{x^m - y^k}(p^\alpha) = p^{2\alpha - \left[\frac{\alpha}{m}\right] - \left[\frac{\alpha}{k}\right]} +$$

$$+ \sum_{i \in A} R^*_{x^m - y^k}(p^{\alpha - i\cdot[m,k]}) \cdot p^{i\cdot[m,k]\left(2 - \frac{1}{m} - \frac{1}{k}\right)},$$

$$A = \left[0, \frac{\alpha}{[m,k]}\right) \cap \mathbb{Z}.$$

Доказательство. Возможны 2 случая:

1. $x^m \equiv y^k \equiv 0 (mod\ p^\alpha)$. Очевидно, что в этом случае имеем $x = p^{\left[\frac{\alpha}{m}\right]} x_1$, $y = p^{\left[\frac{\alpha}{k}\right]} y_1$. Значит, переменные x и y могут принимать $p^{\alpha - \left[\frac{\alpha}{m}\right]}$ и $p^{\alpha - \left[\frac{\alpha}{k}\right]}$ различных значений соответственно. Следовательно, число решений в данном случае имеет вид $p^{\alpha - \left[\frac{\alpha}{m}\right]} \cdot p^{\alpha - \left[\frac{\alpha}{k}\right]} = p^{2\alpha - \left[\frac{\alpha}{m}\right] - \left[\frac{\alpha}{k}\right]}$.

2. $x^m \equiv y^k \not\equiv 0 (mod\ p^\alpha)$. Заметим, что степень p, на которую делятся x^m и y^k, одна и та же. В частности, она делится и на m, и на k, то есть имеет вид $i \cdot [m,k], 0 \leq i < \dfrac{\alpha}{[m,k]}$. Зафиксируем i и посчитаем число решений:

Пусть $x = p^{i\cdot\frac{[m,k]}{m}} \cdot x_1$, $y = p^{i\cdot\frac{[m,k]}{k}} \cdot y_1$, $(x_1, p) = 1$, $(y_1, p) = 1$ Тогда имеем

$$x^m \equiv y^k (mod\ p^\alpha) \Leftrightarrow x_1^m \equiv y_1^k (mod\ p^{\alpha - i\cdot[m,k]}). \quad (3.1)$$

Заметим, что каждое решение x_1 сравнения (3.1) запишется в виде $x_1 + u \cdot p^{\alpha - i\cdot[m,k]}$, $u \in \mathbb{Z}$, а решение y_1 – в виде $y_1 + t \cdot p^{\alpha - i\cdot[m,k]}, t \in \mathbb{Z}$. Тогда решение исходного сравнения для x запишется в виде

$$x = p^{i\cdot\frac{[m,k]}{m}} \cdot x_1 + u \cdot p^{\alpha - i\cdot[m,k] + \frac{i\cdot[m,k]}{m}}.$$

Заметим, что $\alpha - i\cdot[m,k] + \dfrac{i\cdot[m,k]}{m} > \dfrac{i\cdot[m,k]}{m}$, то есть наибольшая степень p, на которую делится x, равна $\dfrac{i\cdot[m,k]}{m}$, как и по предположению.

Предположим, что какие-то два решения

$$a_1 = p^{i\cdot\frac{[m,k]}{m}} \cdot x_1 + u_1 \cdot p^{\alpha - i\cdot[m,k] + \frac{i\cdot[m,k]}{m}}$$

и $$a_2 = p^{i\cdot\frac{[m,k]}{m}} \cdot x_2 + u_2 \cdot p^{\alpha - i\cdot[m,k] + \frac{i\cdot[m,k]}{m}}$$

сравнимы по модулю p^α. Тогда, согласно свойствам сравнений,

$$x_1 - x_2 \equiv p^{\alpha - i\cdot[m,k]} \cdot (u_2 - u_1) (mod\ p^{\alpha - i\cdot\frac{[m,k]}{m}}) \Rightarrow$$

$$\Rightarrow x_1 \equiv x_2 (mod\ p^{\alpha - i\cdot[m,k]}).$$

Последнее сравнение означает, что два рассмотренные нами решения a_1 и a_2 соответствуют одному и тому же решению сравнения $x_1^m \equiv y_1^k (mod\ p^{\alpha - i\cdot[m,k]})$. При этом выражение $u \cdot p^{\alpha - i\cdot[m,k] + \frac{i\cdot[m,k]}{m}}$ пробегает ровно $p^{i\cdot[m,k] - i\cdot\frac{[m,k]}{m}}$ значений по модулю p^α. Аналогичные рассуждения проводим с y.

В качестве следствия из данного рассуждения можно вывести, что каждому решению сравнения (3.1) соответствует ровно

$$p^{i\cdot[m,k]\left(1 - \frac{1}{m}\right)} \cdot p^{i\cdot[m,k]\left(1 - \frac{1}{k}\right)} = p^{i\cdot[m,k]\left(2 - \frac{1}{m} - \frac{1}{k}\right)}$$

решений исходного сравнения. Значит при заданном i число решений исходного сравнения равно $p^{i\cdot[m,k]\left(2 - \frac{1}{m} - \frac{1}{k}\right)} \cdot R^*_{x^m - y^k}(p^{\alpha - i\cdot[m,k]})$.

Суммируя по всевозможным значениям i и добавляя первый случай, получаем

$$R_{x^m - y^k}(p^\alpha) = p^{2\alpha - \left[\frac{\alpha}{m}\right] - \left[\frac{\alpha}{k}\right]} +$$

$$+ \sum_{i \in A} R^*_{x^m - y^k}(p^{\alpha - i\cdot[m,k]}) \cdot p^{i\cdot[m,k]\left(2 - \frac{1}{m} - \frac{1}{k}\right)},$$

$$A=\left[0,\frac{\alpha}{[m,k]}\right)\cap\mathbb{Z}. \qquad \square$$

***Следствие* 3.1.** *Пусть p – нечётное простое число и q – минимальное целое положительное число, такое что $q\equiv\alpha(mod[m,k])$. Тогда число решений сравнения $x^m-y^k\equiv 0(mod\ p^\alpha)$ имеет вид*

$$R_{x^m-y^k}(p^\alpha)=p^{2\alpha-\left[\frac{\alpha}{m}\right]-\left[\frac{\alpha}{k}\right]}+$$
$$+\frac{\varphi(p^\alpha)\cdot(m,k,\varphi(p^\alpha))\cdot\left(p^{(\alpha-q)\cdot\left(1-\frac{1}{m}-\frac{1}{k}\right)}-1\right)}{p^{[m,k]\cdot\left(1-\frac{1}{m}-\frac{1}{k}\right)}-1}+$$
$$+\varphi(p^\alpha)\cdot(m,k,\varphi(p^{\alpha-q}))\cdot p^{\left(1-\frac{1}{m}-\frac{1}{k}\right)}\cdot\begin{cases}0, & q=0;\\ 1, & \text{иначе.}\end{cases}$$

Доказательство. Исходя из формул теорем 2.1 и 3.1, имеем

$$R_{x^m-y^k}(p^\alpha)=p^{2\alpha-\left[\frac{\alpha}{m}\right]-\left[\frac{\alpha}{k}\right]}+$$
$$+\varphi(p^\alpha)\cdot(m,k,\varphi(p^\alpha))\cdot p^{0\cdot[m,k]\left(2-\frac{1}{m}-\frac{1}{k}\right)}+\ldots$$
$$+\varphi(p^q)\cdot(m,k,\varphi(p^q))\cdot p^{\frac{q}{[m,k]}\cdot[m,k]\left(2-\frac{1}{m}-\frac{1}{k}\right)}\cdot h,$$
$$h=\begin{cases}0, & q=0;\\ 1, & \text{иначе.}\end{cases}$$

Из формулы для функции Эйлера имеем, что $\varphi(p^{\alpha-j})\cdot p^j=\varphi(p^\alpha)$, если $\alpha-j>0$. Также, очевидно следующее неравенство: $(m,k,\varphi(p^\beta))=$ $=(m,k,\varphi(p^{[m,k]}))$, $\beta\geq[m,k]$. Используя два данных факта, имеем

$$R_{x^m-y^k}(p^\alpha)=p^{2\alpha-\left[\frac{\alpha}{m}\right]-\left[\frac{\alpha}{k}\right]}+\varphi(p^\alpha)\cdot(m,k,\varphi(p^\alpha))\times$$
$$\times\left(1+p^{[m,k]\left(1-\frac{1}{m}-\frac{1}{k}\right)}+\ldots+p^{(\alpha-q-[m,k])\cdot[m,k]\left(1-\frac{1}{m}-\frac{1}{k}\right)}\right)+$$
$$+\varphi(p^\alpha)\cdot(m,k,\varphi(p^q))\cdot p^{(\alpha-q)\left(1-\frac{1}{m}-\frac{1}{k}\right)}\cdot h.$$

Используя формулу для первых n членов геометрической прогрессии, получаем формулу, записанную в утверждении следствия. $\square$

***Теорема* 3.2.** *Пусть p – простое число и $\alpha\geq 1$. Тогда число таких y $(mod\ p^\alpha)$, таких что сравнение $x^m-y^k\equiv 0(mod\ p^\alpha)$ разрешимо, имеет вид*

$$R_{x^m-y^k,\{2\}}(p^\alpha)=p^{\alpha-\left[\frac{\alpha}{k}\right]}+$$
$$+\sum_{i\in A}R^*_{x^m-y^k,\{2\}}(p^{\alpha-i\cdot[m,k]})\cdot p^{i\cdot[m,k]\left(1-\frac{1}{k}\right)},$$
$$A=\left[0,\frac{\alpha}{[m,k]}\right)\cap\mathbb{Z}.$$

Доказательство. Аналогично доказательству теоремы 3.1. $\square$

***Следствие* 3.2.** *Пусть p – нечётное простое число и q – минимальное целое положительное число, такое что $q\equiv\alpha(mod[m,k])$. Тогда число таких y $(mod\ p^\alpha)$, таких что сравнение $x^m-y^k\equiv 0(mod\ p^\alpha)$ разрешимо, имеет вид*

$$R_{x^m-y^k,\{2\}}(p^\alpha)=p^{\alpha-\left[\frac{\alpha}{k}\right]}+$$
$$+\frac{\varphi(p^\alpha)\cdot(m,k,\varphi(p^\alpha))}{(m,\varphi(p^\alpha)}\cdot\frac{p^{-\frac{\alpha-q}{n}}-1}{p^{-\frac{[m,k]}{k}}-1}+$$
$$+\frac{\varphi(p^\alpha)\cdot(m,k,\varphi(p^q))}{(m,\varphi(p^q))}\cdot p^{-\frac{\alpha-q}{k}}\cdot\begin{cases}0, & q=0;\\ 1, & \text{иначе.}\end{cases}$$

Доказательство. Аналогично доказательству следствия 3.1. $\square$

***Замечание* 3.1.** *В теореме* 3.2 *нами было посчитано число m / k-ичных вычетов по модулю p^α.*

***Замечание* 3.1.** *Пусть $q\in\mathbb{N}$. Тогда, вообще говоря, количества m / k-ичных и qm / qk-ичных вычетов по модулю n могут не совпадать.*

***Следствие* 3.2.1.** *Пусть p – простое и $\alpha\geq 1$. Тогда число m-ичных вычетов по модулю p^α имеет вид*

$$s_{x^m}(p^\alpha)=\sum_{i=0}^{\left[\frac{\alpha}{m}\right]}s^*_{x^m}(p^{\alpha-i\cdot m})+\delta_m(\alpha),$$
$$\delta_m(\alpha)=\begin{cases}0, & \alpha\equiv 0(mod\ m);\\ 1, & \text{иначе.}\end{cases}$$

Доказательство. Напомним, что

$$s_{x^m}(p^\alpha)=R_{x^m-y,\{2\}}(p^\alpha).$$

Следовательно, выше приведенная формула является следствием из теоремы 3.2 при $n=1$. $\square$

***Следствие* 3.2.2.** *Пусть p – нечётное простое число и q – минимальное целое неотрицательное число, такое что $q\equiv\alpha(mod\ m)$. Тогда число m-ичных вычетов по модулю p^α имеет вид*

$$s_{x^m}(p^\alpha)=1+\frac{\varphi(p^\alpha)}{(m,\varphi(p^\alpha))}\cdot\frac{p^{-(\alpha-q)}-1}{p^{-m}-1}+$$
$$+\frac{\varphi(p^\alpha)}{(m,\varphi(p^q))}\cdot p^{-(\alpha-q)}\cdot\begin{cases}0, & q=0;\\ 1, & \text{иначе.}\end{cases}$$

Доказательство. Это утверждение вытекает из следствия 3.2 при $n=1$.

***Лемма* 3.1.** *Пусть p – простое число. Тогда число решений сравнения $x^m\equiv 1(mod\ p^\alpha)$ имеет вид*

$$R_{x^m-1}(p^\alpha)=$$
$$=\begin{cases}(m,\varphi(p^\alpha)), & p\neq 2;\\ 2^{t+1}, & \alpha\geq 2, t>0: 2^t\mid m, 2^{t+1}\nmid m;\\ 1, & \text{в противном случае.}\end{cases}$$

Доказательство. Расссмотрим случай нечётного p. Очевидно, что решениями являются только x, взаимно простые с p. Тогда, согласно теореме о существовании первообразного корня, существует первообразный корень β по модулю p^α и решение x можно представить в виде β^i. Тогда имеем

$$x^m \equiv 1 (mod\ p^\alpha) \Leftrightarrow \beta^{i\cdot m} \equiv \beta^{\varphi(p^\alpha)} (mod\ p^\alpha) \Leftrightarrow$$
$$\Leftrightarrow m \cdot i \equiv 0 (mod\ \varphi(p^\alpha)).$$

Хорошо известно, что последнее сравнение имеет ровно $(m, \varphi(p^\alpha))$ решений.

Теперь рассмотрим случай $p = 2$. Если $\alpha = 1$, то очевидно, что $\forall \quad m \in \mathbb{N} \quad R_{x^m-1}(2^1) = 1$. Теперь рассмотрим случай $\alpha \geq 2$. Аналогично случаю нечётного p нетрудно заметить, что любое решение сравнения $x^m \equiv 1 (mod\ 2^\alpha)$ является нечётным. Тогда, согласно свойствам индексов по модулю 2^α, x представим в виде $(-1)^\gamma \cdot 5^\delta$. Тогда имеем

$$x^m \equiv 1 (mod\ 2^\alpha) \Leftrightarrow$$
$$\Leftrightarrow (-1)^{m\cdot\gamma} \cdot 5^{m\cdot\delta} \equiv (-1)^0 \cdot 5^0 (mod\ 2^\alpha) \Leftrightarrow$$
$$\Leftrightarrow \begin{cases} m \cdot \gamma \equiv 0 (mod\ 2), & (3.2) \\ m \cdot \delta \equiv 0 (mod\ 2^{\alpha-2}). & (3.3) \end{cases}$$

Если $2 \nmid m$, то очевидно, что сравнения (3.2) и (3.3) имеют ровно по одному решению. Это означает, что в этом случае $R_{x^m-1}(2^\alpha) = 1$.

Если же $2 \mid m$, то очевидно, что сравнение (3.2) имеет 2 решения, а сравнение (3.3) имеет $(m, 2^{\alpha-2})$ решений. Следовательно, в этом случае имеем, что $R_{x^m-1}(2^\alpha) = 2 \cdot (m, 2^{\alpha-2}) = 2^{t+1}$, где $t \in \mathbb{N}: \ 2^t \mid m$, но $2^{t+1} \nmid m$. □

***Следствие* 3.2.3** [4, Королев, лемма 2, с. 132]. *Пусть p – простое число, $\alpha \geq 1$ и t – максимальное целое число, такое что $\alpha - t \cdot m \geq 1$. Тогда число m-ичных вычетов по модулю p^α имеет вид*

$$s_{x^m}(p^\alpha) = \frac{\varphi(p^\alpha)}{R_{x^m-1}(p^\alpha)} + ... + \frac{\varphi(p^{\alpha-t\cdot m})}{R_{x^m-1}(p^{\alpha-t\cdot m})} + 1.$$

Доказательство. Следует из следствий 3.2.1 и 2.1, а также леммы 3.1. □

***Следствие* 3.2.4** [2, Stangl]. *Пусть $n = 2^t p_1^{d_1} ... p_k^{d_k}$. Тогда число квадратичных вычетов по модулю n имеет следующий вид*

$$s_{x^2}(n) = \left[\frac{2^{t-1}+5}{3}\right] \prod_{i=1}^{k} \left[\frac{p_i^{d_i+1} + 2p_i + 2}{2(p_i+1)}\right].$$

Доказательство. Согласно следствию 1.2, функция $s_{x^2}(n)$ является мультипликативной. Поэтому достаточно рассмотреть $s_{x^2}(p^\alpha)$, где p – простое.

Пусть p – нечётное и α – чётное. Тогда, согласно следствию 3.2.2, имеем

$$s_{x^2}(p^\alpha) = 1 + \frac{p^\alpha - p^{\alpha-1}}{2} \cdot \frac{p^{-\alpha}-1}{p^{-2}-1} =$$
$$= \frac{2(1-p)(1+p) + (p^\alpha - p^{\alpha-1})(p^{-\alpha+2} - p^2)}{2(1-p^2)} =$$
$$= \frac{2(1-p)(1+p) + (1-p)(-p^{-1})(p^2 - p^{\alpha+2})}{2(1-p^2)} =$$
$$= \frac{2+2p-p+p^{\alpha+1}}{2(p+1)} = \frac{p^{\alpha+1}+p+2}{2(p+1)}.$$

Теперь пусть p – нечётное и α – нечётное. Тогда из следствия 3.2.2 имеем

$$s_{x^2}(p^\alpha) = 1 + \frac{p^\alpha - p^{\alpha-1}}{2} \cdot \frac{p^{-\alpha+1}-1}{p^{-2}-1} + \frac{p^\alpha - p^{\alpha-1}}{2} \cdot p^{-\alpha+1} =$$
$$= \frac{2(1-p)(1+p) + (1-p)(-p^{-1})(p^3 - p^{\alpha+2})}{2(1-p^2)} +$$
$$+ \frac{p-1}{2} = \frac{2+2p+p^{\alpha+1}-p^2+p^2-1}{2(p+1)} = \frac{p^{\alpha+1}+2p+1}{2(p+1)}.$$

Пусть $p = 2, \ 2 \nmid \alpha$. Тогда из следствий 3.2.1 и 2.1 имеем, что

$$s_{x^2}(2^\alpha) = \sum_{i=0}^{\left[\frac{\alpha}{2}\right]} s^*_{x^2}(2^{\alpha-2\cdot i}) =$$
$$= 2^{\alpha-4} + 2^{\alpha-5} + ... + 2^3 + 2 + 1 + 1 =$$
$$= \frac{2 \cdot (4^{\frac{\alpha-3}{2}+1} - 1)}{4-1} + 1 = \frac{2^{\alpha-1}+4}{3}$$

Теперь пусть $p = 2, \ 2 \nmid \alpha$. Тогда из следствий 3.2.1 и 2.1, имеем, что

$$s_{x^2}(2^\alpha) = \sum_{i=0}^{\left[\frac{\alpha}{2}\right]} s^*_{x^2}(2^{\alpha-2\cdot i}) =$$
$$= 2^{\alpha-3} + 2^{\alpha-5} + ... + 2^2 + 1 + 1 + 1 =$$
$$= \frac{4^{\frac{\alpha-3}{2}+1} - 1}{4-1} + 2 = \frac{2^{\alpha-1}+5}{3}.$$

Учитывая, что полученные дроби целые числа и то, что добавление к числителю этих дробей, положительного числа, меньшего знаменателя, не изменит целую часть этих дробей, получим формулу Стангла. □

***Следствие* 3.2.5** [3, Finch, Sebah, с. 12]. *Пусть p – простое число. Тогда число кубических вычетов по модулю p^α имеет вид*

$$s_{x^3}(p^\alpha) = \frac{3^{\alpha+1}+10}{13}, \text{ если } p = 3 \text{ и } \alpha \equiv 0 (mod\ 3);$$

$$s_{x^3}(p^\alpha) = \frac{3^{\alpha+1}+30}{13}, \text{ если } p = 3 \text{ и } \alpha \equiv 1 (mod\ 3);$$

$$s_{x^3}(p^\alpha) = \frac{3^{\alpha+1}+12}{13}, \text{ если } p = 3 \text{ и } \alpha \equiv 2 (mod\ 3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+p+1}{p^2+p+1},\ \text{если}\ p\equiv 1(mod\,3)\ \text{и}\ \alpha\equiv 0(mod\,3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+p^2+p}{p^2+p+1},\ \text{если}\ p\equiv 1(mod\,3)\ \text{и}\ \alpha\equiv 1(mod\,3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+p^2+1}{p^2+p+1},\ \text{если}\ p\equiv 1(mod\,3)\ \text{и}\ \alpha\equiv 2(mod\,3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+2p^2+3p+3}{3(p^2+p+1)},\ \text{если}\ p\equiv 2(mod\,3)\ \text{и}\ \alpha\equiv 0(mod\,3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+3p^2+3p+2}{3(p^2+p+1)},\ \text{если}\ p\equiv 2(mod\,3)\ \text{и}\ \alpha\equiv 1(mod\,3);$$

$$s_{x^3}(p^\alpha)=\frac{p^{\alpha+2}+3p^2+2p+3}{3(p^2+p+1)},\ \text{если}\ p\equiv 2(mod\,3)\ \text{и}\ \alpha\equiv 2(mod\,3).$$

Доказательство. Аналогично следствию 3.2.4 рассматриваем все возможные случаи и считаем геометрические прогрессии. □

ЛИТЕРАТУРА

1. *Гаусс*, *К.Ф.* Труды по теории чисел / К.Ф. Гаусс; общая редакция академика И.М. Виноградова, комментарии члена-корр. АН СССР Б.Н. Делоне. – М.: Изд-во АН СССР, 1959. – 297 с.

2. *Stangl*, *W.* Counting squares in $\mathbb{Z}_n$ / W. Stangl // Mathematics Magazine. – 1996. – Vol. 69, № 4. – P. 285–289.

3. *Finch*, *S.* Squares and cubes modulo *n* / S. Finch, P. Sebah. – Mode of access: arXiv.org e-Print archive: https://arxiv.org/abs/math/0604465v3 [math.NT]. – Date of access: 25.03.2016.

4. *Korolev*, *M.A.* On the average number of power residues modulo a composite number / M.A. Korolev // Izvestiya: Mathematics. – 2010. – Vol. 74 (6) – P. 1225–1255.

5. *Eichhorn*, *D.* Sums and differences of the coordinates of points on modular hyperbolas / D. Eichhorn, M. Khan, A. Stein // Combinatorial number theory. – 2009. – P. 17–38.

6. *Виноградов*, *И.М.* Основы теории чисел / И.М. Виноградов. – М.-Л., Гостехиздат, 1952. – 178 с.

Поступила в редакцию 21.06.2020.