Math-Net.Ru

Общероссийский математический портал

В. В. Астахов, О существовании и числе стационарных точек дискретного логарифма по основанию, отличному от первообразного корня, *Дискрет. матем.*, 2013, том 25, выпуск 4, 41–53

DOI: <https://doi.org/10.4213/dm1256>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 107.22.136.117

26 апреля 2023 г., 12:05:53

О существовании и числе стационарных точек дискретного логарифма по основанию, отличному от первообразного корня

© 2013 г. В. В. Астахов

В связи с атаками на системы цифровой подписи возникает задача решения уравнения $x \equiv R^{x+c} \pmod{p}$, p — простое. В данной работе рассматривается задача о числе и существовании решений (x, R) этого уравнения с ограничениями $0 < x < p$, $R \in Z_p^* \setminus \{1\}$, $\text{ord } R = d$, $d|p-1$, d — простое. Показано существование таких пар при фиксированном c при $d > \frac{\log_2 p}{\log_2 \log_2 p} \cdot (1 + \varepsilon(p, c))$, $\varepsilon(p, c) = o(1)$, $p \rightarrow \infty$. Также доказано, что решения существуют для всех c при $d > \log_2 p \cdot (1 + \varepsilon(p))$, $\varepsilon(p) = o(1)$, $p \rightarrow \infty$, а число таких решений не меньше $\left\lceil \frac{d-1}{2 \cdot (\log_2 p + \log_2 \log_2 p + 3)} \right\rceil$ для любых c , d и p .

1. Введение

Задачи подделки электронной подписи в схеме DSA, определяемой национальным стандартом США FIPS 186, и схеме, определяемой (не действующим в настоящее время) стандартом ГОСТ Р 34.10-94, сводятся к задаче нахождения решения сравнений $x \equiv C \cdot R^x \pmod{p}$ и $x \equiv R^x \pmod{p}$ соответственно (см. [2]) относительно таких x , что $0 < x < p$. Необходимое условие для стойкости схемы ГОСТ Р 34.10-94 было дано в работе [7] в виде вычислительной трудности задачи вычисления дискретного полулогарифма.

При замене параметра $s = r$ в [2] на $s = \alpha \cdot r$, где α — случайное число из множества $\{0, 1, \dots, p-1\}$, получим уравнение $x \equiv R^x \pmod{p}$ со случайным значением параметра R . Таким образом, возникает вопрос, когда подобное уравнение разрешимо при достаточно большом количестве значений R . Оценка этого числа может быть получена как отношение числа таких решений (x, R) уравнения $x \equiv R^x \pmod{p}$, что R имеет фиксированный простой порядок, и максимального числа решений уравнения $x \equiv R^x \pmod{p}$ при фиксированном R . В данной работе рассматривается первое уравнение в несколько более общем виде $x \equiv R^{x+c} \pmod{p}$.

Задачи такого рода изучались в теории чисел. Задача о существовании решения в виде пары чисел (x, R) , где $0 < x < p$, x и R — первообразные корни, а $c = 0$, равносильна задаче о существовании первообразного корня, взаимно простого с $p-1$, которая долгое время оставалась открытой проблемой. Она сформулирована, например, в книге Ги [3]. В 2003 году она была решена (см. [3], [5]), в дальнейшем были получены и некоторые оценки числа таких первообразных корней (см. [1], [4]). В 2011 году была получена оценка числа решений в парах (x, R) , где R уже мог быть

любым отличным от нуля по модулю p (см. [5]). В 2009 году при $c = 0$ было доказано (см. [1]) существование пар решений, в которых R имеет простой порядок по модулю p , больший корня из p . Стоит отметить, что случай, когда R имеет простой порядок, является очень важным именно для криптографических приложений, в частности, в схеме ГОСТ Р 34.10-94 R имеет порядок $d|p-1$, где d — простое число. В данной работе показано существование пар решений $x \equiv R^{x+c} \pmod{p}$, $1 < x < p$, $\text{ord } R = d$, d — простое, при фиксированном c

$$d > \frac{\log_2 p}{\log_2 \log_2 p} (1 + \varepsilon(p, c)), \quad \varepsilon(p, c) = o(1), \quad p \rightarrow \infty.$$

Также доказано существование решений для всех c при

$$d > \log_2 p \cdot (1 + \varepsilon(p)), \quad \varepsilon(p) = o(1), \quad p \rightarrow \infty.$$

Получено, что число таких решений не меньше

$$\left\lceil \frac{d-1}{2 \cdot (\log_2 p + \log_2 \log_2 p + 3)} \right\rceil$$

для любых c , d и p , d и p — простые.

Данные результаты связаны с распределением элементов некоторой циклической подгруппы H порядка d группы Z_p^* . В [6] высказывается гипотеза об их равномерном распределении при $\frac{|H|}{\log p} \rightarrow \infty$. Однако пока наилучшим остается результат [6], где данный факт доказан для $|H| \sim p^{\frac{c}{\log \log p}}$, откуда следует, что число решений системы $x \equiv R^{x+c} \pmod{p}$, $0 < x < p$, $R \in Z_p^* \setminus \{1\}$, $\text{ord } R = d$ при $d \sim p^{\frac{c}{\log \log p}}$ в парах (x, R) имеет вид $\varphi(d) + o(\varphi(d))$. Результаты настоящей работы затрагивают куда меньшие значения $|H| = d \sim \log p$.

2. О существовании решений с заданным порядком

Рассмотрим систему

$$x \equiv R^{c+x} \pmod{p}, \quad 1 < x < p, \quad R \in Z_p^* \setminus \{1\}. \quad (1)$$

Пусть $G \subset Z_p^*$ и G — циклическая подгруппа с образующим элементом g ; пусть порядок $|G| = d$. Заметим, что если d и p — простые, то $\text{ord } R = d$, $1 < R < p$, тогда и только тогда, когда $R \in \langle \xi^{\frac{p-1}{d}} \rangle$, $1 < R < p$, где ξ — первообразный корень по модулю p . Таким образом, задача о нахождении решений с фиксированным простым порядком R сводится к задаче нахождения решений, в которых R принадлежит фиксированной циклической подгруппе. В дальнейшем мы будем рассматривать задачу о существовании и количестве решений с $R \in G$.

Обозначим через $a \pmod{p}$ наименьший неотрицательный вычет a по модулю p , через $\mu(a, p)$ — наименьший по абсолютному значению вычет a по модулю p .

Положим $\rho_p(a_0, a_1) = |\mu(a_0 - a_1, p)|$. Нетрудно проверить, что $\rho_p(a_0, a_1)$ является метрикой. Заметим, что $\rho_p(a_0, a_1) \leq \frac{p-1}{2} < \frac{p}{2}$ для нечетного p , а также что $\rho_d(a_0, a_1) = \rho_d(p - a_0, p - a_1)$ для всех натуральных d и p .

Лемма 1. Пусть $d \mid p-1$ — простое, G — циклическая подгруппа Z_p^* с образующим g порядка d . Тогда количество таких решений (x, R) системы (1), что $R \in G$, равно количеству чисел $n_0 \in \{1, \dots, d-1\}$, для которых $d \nmid (g^{n_0} \pmod{p} + c)$.

Доказательство. Для $c = 0$ лемма была доказана в [1]; ее доказательство дословно переносится на случай $c \neq 0$. Приведем его здесь. Пара (x, R) — решение (1) с $R \in G$ тогда и только тогда, когда $R = g^{n_1}(\bmod p)$, $x = g^{n_0}(\bmod p)$,

$$n_1 \cdot (g^{n_0}(\bmod p) + c) \equiv n_0 (\bmod d), \quad 0 < n_1 < d, \quad 0 < n_0 < d.$$

Для каждого такого n_0 , что $d \nmid (g^{n_0}(\bmod p) + c)$, существует единственное n_1 , удовлетворяющее сравнению; если $d \mid (g^{n_0}(\bmod p) + c)$, то решений нет. Отсюда следует утверждение леммы. $\square$

Теорема 1. Пусть p — натуральное, G — циклическая подгруппа Z_p^* с образующим g простого порядка $d > 2$, $d \mid p - 1$, $(g - 1, p) = 1$ и $(\frac{d+1}{2})^{d-1} \geq p \cdot \frac{d-1}{2 \cdot d} + 1$. Тогда при $c \equiv 0 (\bmod d)$ существует такое решение (1), что $R \in G$.

Доказательство. Пусть

$$g_i = g^i(\bmod p), \quad 0 < g_i < p, \quad i \in Z.$$

Предположим противное: (1) не имеет таких решений (x, R) , что $R \in G$; тогда по Лемме 1

$$d \mid (g_i + c), \quad i = 1, \dots, d - 1. \quad (2)$$

Так как $c \equiv 0 (\bmod d)$, то из (2) следует, что $d \mid g_i$. Рассмотрим соотношение

$$g^d - 1 = (g - 1) \cdot (g^{d-1} + g^{d-2} + \dots + g + 1) \equiv 0 (\bmod p).$$

Из него и того, что $(g - 1, p) = 1$, имеем

$$g^{d-1} + g^{d-2} + \dots + g + 1 \equiv 0 (\bmod p).$$

Тогда

$$\sum_{i=1}^{d-1} g_i + 1 \equiv 0 (\bmod p), \quad \sum_{i=1}^{d-1} g_i + 1 \equiv 1 (\bmod d).$$

А так как $d \mid p - 1$, то

$$\sum_{i=1}^{d-1} g_i + 1 \equiv p (\bmod p \cdot d).$$

С другой стороны,

$$0 < \sum_{i=1}^{d-1} g_i + 1 \leq p \cdot d.$$

Далее, так как $(d, p) = 1$, то по китайской теореме об остатках имеем точное равенство:

$$\sum_{i=1}^{d-1} g_i + 1 = p. \quad (3)$$

Рассмотрим теперь все возможные линейные комбинации g_i с коэффициентами из множества $\{0, 1, 2, \dots, \frac{d-1}{2}\}$:

$$A = \left\{ \sum_{i=1}^{d-1} \alpha_i \cdot g_i \mid \alpha_i \in \left\{ 0, 1, 2, \dots, \frac{d-1}{2} \right\} \right\}.$$

Заметим, что $0 \leq x \leq (p-1) \cdot \frac{d-1}{2}, d \mid x$ для всех $x \in A$. Покажем, что $|A| = \left(\frac{d+1}{2}\right)^{d-1}$, или, другими словами, что все линейные комбинации различны. Предположим противное: пусть две комбинации совпадают. Сократим равные слагаемые в левой и правой частях:

$$\sum_{i=1}^{d-1} g_i \cdot \alpha_i = \sum_{i=1}^{d-1} g_i \cdot \beta_i, \quad \alpha_i \cdot \beta_i = 0, \quad i = 1, 2, \dots, d-1.$$

Пусть $\alpha_l > 0$ — максимальный из коэффициентов α_i, β_i этих комбинаций. Тогда $\beta_l = 0$ и

$$\sum_{i=1}^{d-1} g^i \cdot \alpha_i \equiv \sum_{i=1}^{d-1} g^i \cdot \beta_i \pmod{p},$$

а значит,

$$\alpha_l + \sum_{i=1, i \neq l}^{d-1} g^{i-l} \cdot \alpha_i \equiv \sum_{i=1}^{d-1} g^{i-l} \cdot \beta_i \pmod{p}.$$

Тогда

$$\begin{aligned} \alpha_l + \sum_{i=1, i \neq l}^{d-1} g_{(i-l) \bmod d} \cdot \alpha_i - \sum_{i=1}^{d-1} g_{(i-l) \bmod d} \cdot \beta_i &\equiv 0 \pmod{p}, \\ \alpha_l + \sum_{i=1, i \neq l}^{d-1} g_{(i-l) \bmod d} \cdot \alpha_i - \sum_{i=1}^{d-1} g_{(i-l) \bmod d} \cdot \beta_i &\equiv \alpha_l \pmod{d}, \end{aligned}$$

поэтому

$$\alpha_l + \sum_{i=1, i \neq l}^{d-1} g_{(i-l) \bmod d} \cdot \alpha_i - \sum_{i=1}^{d-1} g_{(i-l) \bmod d} \cdot \beta_i \equiv p \cdot \alpha_l \pmod{p \cdot d}.$$

С другой стороны,

$$-p \cdot \alpha_l < \alpha_l + \sum_{i=1, i \neq l}^{d-1} g_{(i-l) \bmod d} \cdot \alpha_i - \sum_{i=1}^{d-1} g_{(i-l) \bmod d} \cdot \beta_i < p \cdot \alpha_l$$

в силу равенства (3). Но в интервале $(-p \cdot \alpha_l, p \cdot \alpha_l)$ нет чисел, сравнимых с $p \cdot \alpha_l$ по модулю $p \cdot d$ (так как $\alpha_l \leq \frac{d-1}{2}$), а значит, наше предположение неверно, и все линейные комбинации различны. Так как среди чисел $0, 1, \dots, (p-1) \cdot \frac{d-1}{2}$ делящихся на d всего $(p-1) \cdot \frac{d-1}{2 \cdot d} + 1$, то

$$|A| = \left(\frac{d+1}{2}\right)^{d-1} \leq (p-1) \cdot \frac{d-1}{2 \cdot d} + 1 < p \cdot \frac{d-1}{2 \cdot d} + 1.$$

Получаем противоречие с условием, а значит, наше изначальное предположение было не верно и (1) имеет решение с $R \in G$. $\square$

Следующая лемма будет основной для всех дальнейших рассуждений.

Лемма 2. Пусть p — натуральное, $d > 2$ — простое и $d \mid p-1$.

(1) Пусть для натуральных чисел $k, q, h_0, h_1, \dots, h_k$ выполнены условия

$$\begin{aligned} (p, q) &= 1, \quad (p, h_i) = 1, \quad h_i \equiv h_0 \cdot q^i \pmod{p}, \\ h_i &\equiv h_1 \pmod{d}, \quad i = 1, \dots, k, \quad \rho_d(h_0, h_1) \neq 0, \\ \sum_{i=0}^{k-1} h_{i+u} &< \rho_d(h_0, h_1) \cdot p, \quad u \in \{0, 1\}. \end{aligned}$$

Тогда

$$\frac{\rho_d(h_0, h_1) \cdot p}{d} + 1 > C_k^{[\frac{k}{2}]}. \quad (4)$$

(2) Пусть для натуральных чисел $k, q, h_{-k}, h_{-k+1}, \dots, h_{-1}, h_0, h_1, \dots, h_k$ выполнены условия

$$\begin{aligned} k &\geq 2, \quad (p, q) = 1, \quad (p, h_i) = 1, \quad h_i \equiv h_0 \cdot q^i \pmod{p}, \\ h_{\pm i} &\equiv h_1 \pmod{d}, \quad i = 1, \dots, k, \quad \rho_d(h_0, h_1) \neq 0, \\ \sum_{i=0}^{k-1} h_{i+u} &< \rho_d(h_0, h_1) \cdot p, \quad u \in \{-k, -k+1, \dots, 1\}. \end{aligned}$$

Тогда

$$\frac{([\frac{d-1}{2 \cdot \rho_d(h_0, h_1)}] + 1)^k}{[\frac{d-1}{2 \cdot \rho_d(h_0, h_1)}] \cdot k} < \frac{(d-1) \cdot p}{2 \cdot d} + 1. \quad (5)$$

Доказательство. 1. Обозначим через B множество всех линейных комбинаций h_i с коэффициентами 0 или 1, в которых ровно $[\frac{k}{2}]$ коэффициентов равны 1:

$$A = \{h_{i_1} + h_{i_2} + \dots + h_{i_{[\frac{k}{2}]}} \mid 0 < i_1 < i_2 < \dots < i_{[\frac{k}{2}]} \leq k\}.$$

Покажем, что все такие суммы различны. Предположим противное. Пусть существуют две комбинации с равными суммами. Сократим все одинаковые слагаемые, останутся две равные суммы с равными числами слагаемых:

$$\sum_{\alpha=1}^l h_{i_\alpha} - \sum_{\alpha=1}^l h_{j_\alpha} \equiv 0 \pmod{p}.$$

И пусть $i_1 < i_2 < \dots < i_{k_0}, j_1 < j_2 < \dots < j_{k_0}, i_1 < j_1$. Тогда

$$\begin{aligned} \sum_{\alpha=1}^{k_0} h_{i_\alpha} - \sum_{\alpha=1}^{k_0} h_{j_\alpha} &\equiv 0 \pmod{p}, \\ q^{i_1} \cdot (h_0 + \sum_{\alpha=2}^{k_0} h_{i_\alpha - i_1} - \sum_{\alpha=1}^{k_0} h_{j_\alpha - i_1}) &\equiv 0 \pmod{p}. \end{aligned}$$

Значит,

$$h_0 + \sum_{\alpha=2}^{k_0} h_{i_\alpha - i_1} - \sum_{\alpha=1}^{k_0} h_{j_\alpha - i_1} \equiv 0 \pmod{p}.$$

Кроме того,

$$h_0 + \sum_{\alpha=2}^{k_0} h_{i_\alpha-i_1} - \sum_{\alpha=1}^{k_0} h_{j_\alpha-i_1} \equiv h_0 - h_1 \pmod{d},$$

$$h_0 + \sum_{\alpha=2}^{k_0} h_{i_\alpha-i_1} - \sum_{\alpha=1}^{k_0} h_{j_\alpha-i_1} \equiv (h_0 - h_1) \cdot p \equiv \pm \rho_d(h_0, h_1) \cdot p \pmod{p \cdot d}.$$

С другой стороны,

$$-\rho_d(h_0, h_1) \cdot p < h_0 + \sum_{\alpha=2}^{k_0} h_{i_\alpha-i_1} - \sum_{\alpha=1}^{k_0} h_{j_\alpha-i_1} < \rho_d(h_0, h_1) \cdot p,$$

и $\rho_d(h_0, h_1) \cdot p < \frac{d \cdot p}{2}$, получаем противоречие. Теперь заметим, что каждая линейная комбинация не превышает $\rho_d(h_0, h_1) \cdot p$ и что все они сравнимы по модулю d . Все эти линейные комбинации различны, и их $C_k^{[\frac{k}{2}]}$, откуда получаем требуемое неравенство. $\square$

2. Рассмотрим теперь все возможные линейные комбинации h_i с коэффициентами из множества $\{0, 1, 2, \dots, [\frac{d-1}{2 \cdot \rho_d(h_0, h_1)}]\}$ и выделим множества комбинаций с суммой коэффициентов, равной некоторому числу ζ :

$$C = \left\{ \sum_{i=1}^k \alpha_i \cdot h_i \mid \alpha_i \in \left\{ 0, 1, 2, \dots, \left[\frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right] \right\} \right\},$$

$$C_\zeta = \left\{ \sum_{i=1}^k \alpha_i \cdot h_i \mid \alpha_i \in \left\{ 0, 1, 2, \dots, \left[\frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right] \right\}, \sum_{i=1}^k \alpha_i = \zeta \right\}.$$

Заметим, что $0 \leq x \leq p \cdot [\frac{d-1}{2 \cdot \rho_d(h_0, h_1)}] \cdot \rho_d(h_0, h_1) - 1 \leq \frac{p \cdot (d-1)}{2} - 1$ для любого x из C . Покажем, что для любого ζ все элементы C_ζ различны. Предположим противное: пусть две комбинации совпадают. Сократим равные слагаемые в левой и правой частях:

$$\sum_{i=1}^k \alpha_i \cdot h_i = \sum_{i=1}^k \beta_i \cdot h_i, \quad \alpha_i \cdot \beta_i = 0, \quad i = 1, 2, \dots, k,$$

пусть α_l — максимальный из коэффициентов α_i, β_i этих комбинаций. Тогда $\beta_l = 0$ и

$$\sum_{i=1}^k h_i \cdot \alpha_i \equiv \sum_{i=1}^k h_i \cdot \beta_i \pmod{p},$$

а значит,

$$\alpha_l \cdot h_0 + \sum_{i=1, i \neq l}^k h_{i-l} \cdot \alpha_i - \sum_{i=1}^k h_{i-l} \cdot \beta_i \equiv 0 \pmod{p},$$

$$\alpha_l \cdot h_0 + \sum_{i=1, i \neq l}^k h_{i-l} \cdot \alpha_i - \sum_{i=1}^k h_{i-l} \cdot \beta_i \equiv \alpha_l \cdot (h_0 - h_1) \pmod{d},$$

следовательно,

$$\alpha_l \cdot h_0 + \sum_{i=1, i \neq l}^k h_{i-l} \cdot \alpha_i - \sum_{i=1}^k h_{i-l} \cdot \beta_i \equiv p \cdot \alpha_l \cdot (h_0 - h_1) \equiv \pm p \cdot \alpha_l \cdot \rho_d(h_0, h_1) \pmod{p \cdot d}.$$

С другой стороны,

$$-p \cdot \alpha_l \cdot \rho_d(h_0, h_1) < \alpha_l \cdot h_0 + \sum_{i=1, i \neq l}^k h_{i-l} \cdot \alpha_i - \sum_{i=1}^k h_{i-l} \cdot \beta_i < p \cdot \alpha_l \cdot \rho_d(h_0, h_1).$$

Но так как $\alpha_l \cdot \rho_d(h_0, h_1) \leq \frac{d-1}{2}$, то в интервале $(-p \cdot \alpha_l \cdot \rho_d(h_0, h_1), p \cdot \alpha_l \cdot \rho_d(h_0, h_1))$ нет чисел, сравнимых с

$$p \cdot \alpha_l \cdot \rho_d(h_0, h_1) \pmod{p \cdot d},$$

а значит, наше предположение неверно, и все элементы C_ζ различны. Заметим, что $\sum_{\zeta=0}^{\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor \cdot k} |C_\zeta| = |C| = \left(\left(\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor + 1 \right)^k \right)$. Так как при $k \geq 2$ в каждом множестве C_ζ , $0 < \zeta < \left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor \cdot k$, есть хотя бы 2 комбинации, то найдется множество с числом элементов $|C_{\zeta_0}| \geq \frac{\left(\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor + 1 \right)^k - 2}{\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor \cdot k - 1} \geq \frac{\left(\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor + 1 \right)^k}{\left\lfloor \frac{d-1}{2 \cdot \rho_d(h_0, h_1)} \right\rfloor \cdot k}$ (второе неравенство следует из того, что отношение в левой его части не меньше 2), с другой стороны, элементы C_{ζ_0} различны, совпадают по модулю d и не превосходят $\frac{p \cdot (d-1)}{2}$. Отсюда получаем требуемое неравенство. $\square$

Теорема 2. Пусть p — натуральное, c — целое, G — циклическая подгруппа Z_p^* с образующим g простого порядка $d > 2$, $d \mid p-1$, $(g-1, p) = 1$ и выполнено одно из двух условий:

$$(1) \quad d \mid c+1,$$

$$(2) \quad d \nmid c+1 \text{ и}$$

$$\frac{\left(\left\lfloor \frac{d-1}{2 \cdot \rho_d(-c, 1)} \right\rfloor + 1 \right)^{d-1}}{\left\lfloor \frac{d-1}{2 \cdot \rho_d(-c, 1)} \right\rfloor \cdot (d-1)} \geq \frac{(d-1) \cdot p}{2 \cdot d} + 1.$$

Тогда существует такое решение (x, R) системы (1), что $R \in G$.

Доказательство. Заметим, что в случае $d \mid c$ Теорема 2 следует из Теоремы 1, так как числа d и p удовлетворяют её условиям. Пусть теперь $c_0 = c \pmod{d}$, $c_0 \neq 0$. Пусть снова

$$g_i = g^i \pmod{p}, \quad 0 < g_i < p, \quad i \in Z.$$

Предположим, что решения (x, R) с $R \in G$ не существует. Тогда по Лемме 1

$$d \mid (g_{n_0} + c), \quad n_0 \in \{1, \dots, d-1\},$$

а значит,

$$g_i \equiv -c_0 \pmod{d}, \quad i = 1, \dots, d-1,$$

и в силу условия $(g-1, p) = 1$

$$\sum_{i=1}^{d-1} g_i + 1 \equiv 0 \pmod{p}.$$

Далее, так как

$$\sum_{i=1}^{d-1} g_i + 1 \equiv c_0 + 1 \pmod{d},$$

то

$$\sum_{i=1}^{d-1} g_i + 1 \equiv (c_0 + 1) \cdot p \pmod{p \cdot d}.$$

При этом

$$0 < \sum_{i=1}^{d-1} g_i + 1 < p \cdot d.$$

Отсюда при $c_0 = d - 1$ сразу получаем противоречие, и первый пункт доказан, а при остальных значениях c_0 имеем

$$\sum_{i=1}^{d-1} g_i + 1 = (c_0 + 1) \cdot p. \quad (6)$$

Заметим, что из (6) непосредственно следует равенство

$$\sum_{i=1}^{d-1} (p - g_i) - 1 = (d - 2 - c_0) \cdot p, \quad (7)$$

или

$$\sum_{i=0}^{d-1} (p - g_i) = (d - c_0 - 1) \cdot p.$$

Таким образом, для чисел $g_i^{(1)} = g_i$ и $g_i^{(2)} = p - g_i$ выполнены условия

$$0 < g_i^{(a)} < p,$$

$$g_i^{(a)} \equiv g_1^{(a)} \pmod{d}, \quad i = 1, \dots, d-1, \quad a \in \{1, 2\};$$

$$0 < \rho_d(g_0^{(a)}, g_1^{(a)}) = \rho_d(1, -c) \in \{c_0 + 1, d - (c_0 + 1)\},$$

а при некотором $a' \in \{1, 2\}$

$$\sum_{i=0}^{d-1} g_i^{(a')} = \rho_d(-c, 1) \cdot p.$$

Тогда при $u = -(d-1), -(d-2), \dots, 1$

$$\sum_{i=0}^{d-2} g_{i+u}^{(a')} < \sum_{i=0}^{d-1} g_{i+u}^{(a')} = \sum_{i=0}^{d-1} g_i^{(a')} = \rho_d(-c, 1) \cdot p = \rho_d(g_0^{(a')}, g_1^{(a')}) \cdot p.$$

Первое равенство верно в силу того, что $g_i^{(a')}$ периодичны с периодом d , поэтому сумма любых d подряд идущих элементов одинакова. А значит, при $k = d-1, q = g$ и числах $h_i = g_i^{(a')}$ выполнены условия п. 2 Леммы 2. $\square$.

Следствие 1. Если p — натуральное, G — циклическая подгруппа Z_p^* с образующим g простого порядка $d > 2, d \mid p-1, (g-1, p) = 1, c_0 = c \pmod{d}, 0 \leq c_0 < d$, то каждое из следующих условий является достаточным для существования такого решения (x, R) системы (1), что $R \in G$:

$$(1) \ c_0 = d - 1,$$

$$(2) \ c_0 = d - 2,$$

$$(3) \ c_0 = 0, d \geq \frac{\log_2 p - 1}{\log_2 \log_2 p - \log_2 \log_2 \log_2 p - 1} + 1,$$

$$(4) \ d > \log_2 p - \frac{1}{2} \cdot \log_2 \log_2 p + \log_2(\min(c_0 + 1, d - 2 - c_0)) + 3, 0 < c_0 < d - 2.$$

Доказательство. 1. Было получено в ходе доказательства Теоремы 2.

2. Пусть $c_0 = d - 2$. Если решений (x, R) с $R \in G$ не существует, то в силу (7)

$$\sum_{i=1}^{d-1} (p - g_i) - 1 = 0,$$

однако при $d > 2$ в левой части есть хотя бы два положительных слагаемых, а значит, равенство невозможно.

3. По Теореме 1 достаточно показать, что при заданных условиях

$$\left(\frac{d+1}{2}\right)^{d-1} \geq p \cdot \frac{d-1}{2 \cdot d} + 1. \quad (8)$$

Так как $d \mid p - 1, d > 2, d$ — простое, то $d \mid \frac{p-1}{2}$ и

$$p \cdot \frac{d-1}{2 \cdot d} + 1 = \frac{p}{2} - \frac{p}{2 \cdot d} + 1 \leq \frac{p}{2}.$$

Так как левая часть неравенства (8) возрастает с ростом d , то оно будет верно при всех $d \geq d_0$, где d_0 определяется равенством

$$\left(\frac{d_0+1}{2}\right)^{d_0-1} = \frac{p}{2} \Leftrightarrow (\log_2(d_0+1) - 1) \cdot (d_0 - 1) = \log_2 p - 1.$$

Отсюда следует, что $d_0 \geq \frac{\log_2 p}{\log_2 \log_2 p}$, иначе получаем противоречие :

$$(\log_2(d_0+1) - 1) \cdot (d_0 - 1) < \log_2 \left(\frac{\log_2 p + 1}{2}\right) \cdot \left(\frac{\log_2 p}{\log_2 \log_2 p} - 1\right) < \log_2 p - 1.$$

Значит,

$$d_0 = \frac{\log_2 p - 1}{\log_2(d_0+1) - 1} + 1 \leq \frac{\log_2 p - 1}{\log_2 \log_2 p - \log_2 \log_2 \log_2 p - 1} + 1,$$

что завершает доказательство п. 3.

4. Если в самом конце доказательства Теоремы 2 для тех же значений параметров применить п. 1 вместо п. 2 из Леммы 2, то получим, что для простых нечетных d , удовлетворяющих неравенству

$$C_{d-1}^{\frac{d-1}{2}} \geq \frac{\rho_d(1, -c_0) \cdot p}{d} + 1 = \frac{\min(c_0 + 1, d - c_0 - 1) \cdot p}{d} + 1, \quad (9)$$

утверждение верно. Покажем, что это неравенство выполняется, если

$$d > \log_2 p - \frac{1}{2} \cdot \log_2 \log_2 p + \log_2(\min c_0 + 1, d - 2 - c_0) + 3.$$

Для начала заметим, что $d \geq 5$, а значит, $2^{d-1.5} > d \cdot \sqrt{d-1}$. Учитывая что

$$\begin{aligned} C_{d-1}^{\frac{d-1}{2}} &= \frac{(d-1)!}{\left(\frac{d-1}{2}\right)! \left(\frac{d-1}{2}\right)!} = \prod_{i=1}^{\frac{d-1}{2}} \frac{(2 \cdot i - 1) \cdot 2 \cdot i}{i \cdot i} = \\ &= \prod_{i=1}^{\frac{d-1}{2}} 4 \cdot \left(1 - \frac{1}{2 \cdot i}\right) \geq 2^{d-1} \cdot \frac{1}{2} \cdot \prod_{i=2}^{\frac{d-1}{2}} \sqrt{1 - \frac{1}{i}} \geq \frac{2^{d-1.5}}{\sqrt{d-1}}, \end{aligned} \quad (10)$$

имеем:

$$\begin{aligned} C_{d-1}^{\frac{d-1}{2}} \cdot d - d &> 2^{d-1.5} \frac{d}{\sqrt{d-1}} - d = \\ &= 2^{d-1.5} \cdot \sqrt{d-1} + \frac{2^{d-1.5}}{\sqrt{d-1}} - d > 2^{d-1.5} \cdot \sqrt{d-1} > \\ &> p \cdot \min(c_0 + 1, d - c_0 - 1) \cdot \frac{2\sqrt{2(d-1)}}{\sqrt{\log_2 p}} > p \cdot \min(c_0 + 1, d - c_0 - 1). \end{aligned}$$

Отсюда следует (9), а значит, п. 4 Следствия 1 также доказан.

Замечание 1. Пусть $p = \frac{d^d - 1}{d - 1} = d^{d-1} + d^{d-2} + \dots + 1$, тогда d — корень d -й степени из 1 по модулю p . Тогда для мультипликативной циклической группы $\langle d \rangle$ имеем $d^i \pmod{p} = d^i \cdot d, i = 1, \dots, d-1$, таким образом, по Лемме 1 при $R \in \langle d \rangle$ решений (1) нет. С другой стороны, $d > \frac{\log_2 p}{\log_2 \log_2 p}$.

Заметим, что

$$\frac{\log_2 p - 1}{\log_2 \log_2 p - \log_2 \log_2 \log_2 p - 1} + 1 = \frac{\log_2 p}{\log_2 \log_2 p} + \varepsilon(p), \quad \varepsilon(p) = o\left(\frac{\log_2 p}{\log_2 \log_2 p}\right), p \rightarrow \infty.$$

Таким образом, как видно из Замечания 1, оценка снизу параметра d из п. 3 Следствия 1 имеет наилучший главный член при $p \rightarrow \infty$.

3. О числе решений

Теперь получим оценку снизу числа решений (1) из данной циклической подгруппы. Итак, пусть $d(p)$ — минимальное натуральное число, большее 2 и такое, что $C_{d(p)}^{\lfloor \frac{d(p)}{2} \rfloor} > p$. Заметим, что из (10) подстановкой можно получить, что если $d_0 \geq \log_2 p + \log_2 \log_2 p + 2$, то $C_{d_0}^{\lfloor \frac{d_0}{2} \rfloor} > p$, а значит, $d(p) < \log_2 p + \log_2 \log_2 p + 3$.

Теорема 3. Пусть p — натуральное, G — циклическая подгруппа Z_p^* с образующим g простого порядка $d > 2, d \mid p-1, (g-1, p) = 1$. Тогда существует не менее $\left\lfloor \frac{d-1}{2 \cdot d(p)} \right\rfloor$ таких решений (x, R) системы (1), что $R \in G$.

Доказательство. Обозначим через $r - 1$ число решений (x, R) с $R \in G$. Допустим, что $r \leq \left\lfloor \frac{d-1}{2 \cdot d(p)} \right\rfloor$. Пусть $g_i = g^i \pmod{p}$, $i \in Z$. Заметим, что последовательность $\{g_i\}$ периодична с периодом d . Из Леммы 1 получаем, что все числа g_i , $i = 1, 2, \dots, d-1$, кроме каких-то $r - 1$, сравнимы с $(-c)$ по модулю d . Добавляя к ним g_0 , получаем, что не более r чисел не сравнимы с $(-c)$ по модулю d . Пусть опять $c_0 \equiv c \pmod{d}$, $0 \leq c_0 \leq d-1$.

Случай 1: среди чисел g_i , $i = 0, \dots, d-1$, нашлось такое g_l , что $\rho_d(g_l, -c_0) \geq d(p)$. Рассмотрим матрицу размером $d(p) \times (d-1)$, заданную набором её элементов:

$$\gamma_{i,j} = g_{l+i \cdot j}, \quad i \in \{1, \dots, d(p)\}, \quad j \in \{1, \dots, d-1\}.$$

В силу простоты d в каждом столбце и в каждой строке все индексы у g различны по модулю d . Всего строк $d(p)$, а значит, каждое число в матрице встречается не более $d(p)$ раз. Всего есть не более r чисел среди g_i , не сравнимых с $(-c)$ по модулю d , при этом g_l в матрице нет, а значит, в матрице их число не превосходит $(r-1) \cdot d(p)$, поэтому есть $d-1 - (r-1) \cdot d(p)$ столбцов, в которых все числа сравнимы с $(-c)$ по модулю p . Заметим, что $(r-1) \cdot d(p) < d-1$, а значит, существует такое t , что все числа в t -м столбце сравнимы с $(-c)$ по модулю d . Заметим, что

$$\sum_{i=0}^{d(p)-1} g_{l+d(p) \cdot (t+u)} < d(p) \cdot p \leq \rho_d(g_l, g_{l+t}) \cdot p, \quad u \in \{0, 1\}.$$

Остается применить п. 1 Леммы 2 с $k = d(p)$, $q = g_t$, $h_i = g_{l+i \cdot t}$ и получить неравенство

$$C_{d(p)}^{\left[\frac{d(p)}{2}\right]} < \frac{\rho_d(g_l, g_{l+t}) \cdot p}{d} + 1 \leq \frac{(d-1) \cdot p}{2 \cdot d} + 1 \leq p,$$

противоречащее выбору $d(p)$.

Случай 2: $\rho_d(g_i, -c_0) < d(p)$ для любого i . Покажем, что и в этом случае приходим к противоречию. Для этого заметим, что

$$\begin{aligned} \sum_{i=0}^{d-1} g_i &\equiv 0 \pmod{p}, \\ \sum_{i=0}^{d-1} g_i &\equiv \sum_{i=0}^{d-1} (g_i + c_0) \equiv x \pmod{d}, \quad 0 \leq x < d, \\ \rho_d(x, 0) &\leq \sum_{i=0}^{d-1} (\rho_d(g_i, -c_0)) < r \cdot d(p). \end{aligned}$$

А значит,

$$\sum_{i=0}^{d-1} g_i \equiv x \cdot p \pmod{p \cdot d};$$

в силу того, что левая часть этого сравнения лежит в интервале $(0, p \cdot d)$,

$$\sum_{i=0}^{d-1} g_i = x \cdot p, \quad \sum_{i=0}^{d-1} (p - g_i) = (d - x) \cdot p.$$

Пусть $g_i^{(1)} = g_i, c^{(1)} = c_0, g_i^{(2)} = p - g_i, c^{(2)} = 1 - c_0$.

Так как $\rho_d(x, 0)$ равняется или x , или $d - x$, то существует такое $a \in \{1, 2\}$, что $\sum_{i=0}^{d-1} g_i^{(a)} = \rho_d(x, 0) \cdot p$. С одной стороны, $\rho_d(x, 0) > 0$, с другой стороны, $\rho_d(0, x) \leq \sum_{i=0}^{d-1} \rho_d(g_i^{(a)}, -c^{(a)})$, а значит, найдется такое i_0 , что $\rho_d(g_{i_0}^{(a)}, -c^{(a)}) > 0$. Пусть $\max_i (\rho_d(g_i^{(a)}, -c^{(a)})) = M > 0$. И пусть

$$I = \left\{ i \mid \rho_d(g_i^{(a)}, -c^{(a)}) = M, i \in \{0, \dots, d-1\} \right\},$$

$$I_0 = \left\{ i \mid 0 < \rho_d(g_i^{(a)}, -c^{(a)}) < M, i \in \{0, \dots, d-1\} \right\},$$

$$S = \sum_{i \in I} g_i^{(a)}.$$

Заметим, что $|I| + |I_0| \leq r, S \leq |I| \cdot (p - 1)$. По принципу Дирихле найдется такой индекс l , что $l \in I, g_l^{(a)} \leq \frac{S}{|I|}$. Далее,

$$\begin{aligned} \rho_d(0, x) &\leq \sum_{i=0}^{d-1} \rho_d(g_i^{(a)}, -c^{(a)}) = \sum_{i \in I} \rho_d(g_i^{(a)}, -c^{(a)}) + \sum_{i \in I_0} \rho_d(g_i^{(a)}, -c^{(a)}) \leq \\ &\leq |I| \cdot M + |I_0| \cdot (M - 1) \leq r \cdot M - (r - |I|). \end{aligned}$$

Тогда рассмотрим матрицу размером $d(p) \times (d-1)$, заданную набором её элементов:

$$\gamma_{i,j} = g_{l+i \cdot j}^{(a)}, \quad i \in \{1, \dots, d(p)\}, \quad j \in \{1, \dots, d-1\}.$$

В силу простоты d в каждом столбце и в каждой строке все индексы $u \cdot g^{(a)}$ различны по модулю d . Всего строк $d(p)$, а значит, каждое число в матрице встречается не более $d(p)$ раз. Всего есть r чисел среди $g_i^{(a)}$, не сравнимых с $(-c^{(a)})$ по модулю p , а значит, в матрице их число не превосходит $r \cdot d(p)$, поэтому есть $d-1-r \cdot d(p)$ столбцов, в которых все числа сравнимы с $(-c^{(a)})$ по модулю p . Сумма всех $g_i^{(a)}$, сравнимых с $(-c^{(a)})$ по модулю p , не превосходит $\rho_d(x, 0) \cdot p - S$, а значит, сумма чисел во всех столбцах, в которых все числа сравнимы с $-c^{(a)}$ по модулю p , не превосходит $(\rho_d(x, 0) \cdot p - S) \cdot d(p)$, поэтому существует такое t , что сумма элементов t -го столбца не больше

$$\begin{aligned} &\frac{(\rho_d(x, 0) \cdot p - S) \cdot d(p)}{d - r \cdot d(p) - 1} < \frac{((r \cdot M - (r - |I|)) \cdot p - S) \cdot d(p)}{r \cdot d(p)} = \\ &= M \cdot p - \frac{(r - |I|) \cdot p + S}{r} < M \cdot p - \frac{(r - |I|) \cdot \frac{S}{|I|} + S}{r} = M \cdot p - \frac{S}{|I|}. \end{aligned}$$

Следовательно, $\sum_{i=0}^{d(p)} g_{l+i \cdot t}^{(a)} \leq M \cdot p$. Тогда

$$\sum_{i=0}^{d(p)-1} g_{l+t \cdot (i+u)}^{(a)} < \sum_{i=0}^{d(p)} g_{l+t \cdot i}^{(a)} \leq M \cdot p \leq \rho_d(g_l^{(a)}, g_{l+t}^{(a)}) \cdot p, \quad u \in \{0, 1\}.$$

Остается применить п. 1 Леммы 2 с $k = d(p), q = g_t, h_i = g_{l+i \cdot t}^{(a)}$ и получить неравенство

$$C_{\frac{d(p)}{d(p)}}^{[\frac{d(p)}{2}]} < \frac{\rho_d(g_l^{(a)}, g_{l+t}^{(a)}) \cdot p}{d} + 1 \leq \frac{(d-1) \cdot p}{2 \cdot d} + 1 \leq p,$$

противоречащее выбору $d(p)$. $\square$

Следствие 2. Если p — натуральное, G — циклическая подгруппа Z_p^* с образующим g простого порядка $d > 2, d \mid p-1, (g-1, p) = 1$, то для таких c , что $\rho_d(1, -c) \geq d(p)$, существует не менее $\left\lfloor \frac{d-1}{d(p)} \right\rfloor$ таких решений (x, R) системы (1) с $R \in G$.

Доказательство. Пусть $r-1$ — число решений (x, R) с $R \in G$. Допустим, что $r \leq \left\lfloor \frac{d-1}{d(p)} \right\rfloor$. Пусть $g_i = g^i \pmod{p}, i \in Z$. Последовательность $\{g_i\}$ периодична с периодом d . Из Леммы 1 получаем, что все, кроме $r-1$, чисел $g_i, i = 1, 2, \dots, d-1$, сравнимы с $(-c)$ по модулю d . Добавляя к ним g_0 , получаем, что не более r чисел не сравнимы с $(-c)$ по модулю d . Пусть опять $c_0 = c \pmod{d}$.

Так как $g_0 = g^0 \pmod{p} = 1, \rho_d(g_0, -c_0) \geq d(p)$ и $(r-1) \cdot d(p) < d-1$, то выполнены условия случая 1 из доказательства Теоремы 3 с $l = 0$. Поэтому, повторяя рассуждения из Теоремы 3, приходим к противоречию. $\square$

Список литературы

1. Черепнев М. А., Некоторые эффективные оценки для числа решений задачи Бризолеса. В сб.: *Современные проблемы математики и механики. Математика*, 4, № 3. МГУ, Москва, 2009, с. 125–129.
2. Гашков С. Б., Применко Э. А., Черепнев М. А., *Криптографические методы защиты информации. Учебн. пособие*. «Академия», Москва, 2010.
3. Guy R. K., *Unsolved Problems in Number Theory. (2-nd edition)*. Springer-Verlag, New York - Berlin, 1981.
3. Campbell M. E., *On fixed points for discrete logarithms*, Master Thesis. Univ. of California at Berkeley, 2003.
4. Гречников Е. А., Двусторонние оценки числа неподвижных точек дискретного логарифма. *Вестник МГУ. Серия 1. Математика, Механика* (2012), № 3 3–8.
5. Bourgain J., Konyagin S., Shparlinski I., Distribution of elements of cosets of small subgroups and applications. *Int. Math. Res. Notices* (2012) **9**, 1968–2009.
5. Levin M., Pomerance C., Soundararajan K., Fixed points for discrete logarithms. *Algorithmic Number Theory Symposium IX* (2010) 6–15.
6. Montgomery H., Vaughan R., Wooley T., Some remarks on Gauss sums associated to k -th powers. *Math. Proc. Cambr. Phil. Soc.* (1995) **118**, 21–33.
6. Bourgain J., Multilinear exponential sums in prime fields under optimal entropy condition on the sources. *Geom. and Funct. Anal.* (2008) **18**, 1477–1522.
7. Варновский Н. П., Стойкость схем электронной подписи в модели с защищенным модулем. *Дискрет. матем.* (2008) **20**, №3, 147–159.

Статья поступила 18.06.2013.