Частные Ферма и логарифмирование в мультипликативной группе кольца вычетов по примарному модулю

В. М. Сидельников

§1. Введение

Оценки сложности логарифмирования в мультипликативной группе кольца вычетов по $\mathrm{mod} m$, мультипликативной группе конечного поля $\mathbf{F}_q$, где $q = p^l$, p — простое число, или в группе точек эллиптической кривой над конечным полем имеют важное прикладное значение [1]. Методы их получения в общем случае достаточно сложны и не будут обсуждаться в настоящей работе.

В работе рассматривается следующая задача. Пусть m — целое число и $\xi \in (\mathbf{Z}/m\mathbf{Z})^*$ — элемент мультипликативной группы кольца $\mathbf{Z}/m\mathbf{Z}$ порядка n и a — элемент циклической группы, порожденной ξ. Рассмотрим уравнение

$$\xi^x \equiv a(\mathrm{mod} m),\ 0 \le x < n. \tag{1}$$

Корень этого уравнения, а именно число $x = \mathrm{ind}_\xi(a)$, обычно называют логарифмом или индексом элемента a по модулю m и основанию ξ, а саму задачу вычисления x — задачей логарифмирования в циклической группе $(\mathbf{Z}/m\mathbf{Z})^*$.

Предположительно сложность задачи логарифмирования для некоторых $m = p$ и ξ порядка n в $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{F}_p^*$, p — простое, при $\log n \sim c \log p$, $0 < c \le 1$, $p \to \infty$, (возможно и почти для всех) не является полиномиальной от длины записи числа p, например, в двоичной системе исчисления. Вместе с тем следует отметить, что для некоторых p задача логарифмирования в $\mathbf{F}_p^*$ является полиномиальной при любом допустимом n.

Например, пусть $p - 1 = \prod_{i=1}^k p_i^{\alpha_i}$. Как хорошо известно [1], задача логарифмирования в группы $\mathbf{F}_p^*$ при $n = p - 1$ может быть за число операций, которое полиномиально зависит от длины записи p, сведена к k задачам логарифмирования по $\mathrm{mod} p_i$. Таким образом, если все числа p_i являются "маленькими" ($p_i = O(\log p)$), то и вся задача логарифмирования становится полиномиальной от длины записи p.

В настоящей работе показано (теорема 2), что если $x = x_0 + x_1(p-1)$ — решение уравнения 1 при $m = p^\alpha$, $\alpha > 1$, и если одно из чисел x_0 или $x_1 \bmod p$ известно, то оставшееся число при $\alpha = const, p \to \infty$, может быть вычислено за число операций не выше $O(\log^3 p)$. Часть этого утверждения тривиальна, а именно та часть, где утверждается, что вычислить x_1 просто, зная x_0. Новой является другая часть утверждения — вычислить x_0 просто, если известно число $x_1 \bmod p$.

Основным аппаратом, который используется для получения указанного результата, являются теоретико-числовые функции $\Phi(a)$, носящие название частные Ферма, свойства которых похожи на свойства функции $\mathrm{ind}_\xi(a)$ в мультипликативной группе кольца вычетов, а именно, $\Phi(ab) \equiv \Phi(a) + \Phi(b) \bmod m$. Одним из основных результатов работы является "новое" "естественное" определение этих функций на элементах мультипликативной группы кольца вычетов по модулю m^2, несколько отличающееся от определения частных Ферма, введенных Ризелем [2]. В общем случае частные Ферма Ризеля является линейной комбинацией "новых" функций. Вместе с тем в важном частном случае $m = p^\alpha$ — примарное число, "новые" функции совпадают с функциями, введенными в [2].

В §2 настоящей работе введены функции частные Ферма $\Phi_i(a)$, $i = 1, \ldots u$, для произвольного целого положительного нечетного числа $m = \prod_{i=1}^u p_i^{\alpha_i}$. Рассматривается линейное пространство (модуль) $L(m)$ над кольцом $\mathbf{Z}/m\mathbf{Z}$, которое натянуто на u функций $\Phi_i(a)$. Каждая из $\Phi_i(a)$ гомоморфно отображают мультипликативную группу $(\mathbf{Z}/m^2\mathbf{Z})^*$ вычетов взаимно простых с m в аддитивную группу вычетов по $\mathrm{mod} m$. В случае $m = p$, где p — простое число, $u = 1$ и функция $\Phi_1(a) = \Phi(a)$ определяются соотношением

$$\Phi_1(a) \equiv \frac{a^{p-1} - 1}{p} (\mathrm{mod} p), \quad a \in (\mathbf{Z}/p^2\mathbf{Z})^*, \tag{2}$$

т.е. обычным образом (см. [2]). Показано, что для непримарного m ($u > 1$) функция частное Ферма, определенная в [2] для этого m, принадлежит пространству $L(m)$.

Очень важным свойством частных Ферма является невысокая сложность их вычисления. А именно, для вычисления функции $\Phi(a)(\bmod p)$ при $m = p$ достаточно вычислить a^{p-1} по модулю p^2 и разделить результат на p. Число модульных умножений, требуемых для этого, очевидно, не превосходит $O(\log p)$. Это же верно для всех m.

Следует отметить, что Ризелем в работе [2] для частных Ферма $\Phi(a) \equiv \frac{a^{\lambda(m)}-1}{m} (\bmod m)$, где m целое и $\lambda(m)$ – функция Кармайкла, получены интересные численные результаты для логарифмирования в кольце $(\mathbf{Z}/m\mathbf{Z})^*$ с помощью функции $\Phi(a)$ для некоторых конкретных m. Ю.В. Нестеренко [4] также получил некоторые важные и пока неопубликованные результаты о функции $\Phi(a)$, в частности, об определении функции частное Ферма в кольцах алгебраических чисел, а также об их периодах. Часть результатов настоящей работы была опубликована в [5].

Если разложить идеал (p) в произведение

$$(p) = \mathfrak{p}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{p}_u^{\alpha_u} \tag{3}$$

простых дивизоров из кольца целых чисел некоторого расширения $\mathbf{K}/\mathbf{Q}$ поля рациональных чисел $\mathbf{Q}$, то можно ввести u функций частных Ферма для этого расширения примерно так же как это сделано для кольца вычетов по $\bmod m$. Частично эта идея уже реализована в работе [4], где для произвольного идеала $\mathfrak{m}$ кольца целых $\mathbf{K}$ введена функция $\Phi(a, \mathbf{K}, \mathfrak{m})$, похожая на функцию Ферма Ризеля.

Если окажется, что

$$(p) = \mathfrak{p}_1^{\alpha}, \quad \alpha > 1, \tag{4}$$

то будет справедлив результат подобный утверждению теоремы 2. В этом случае роль кольца вычетов по $\mathrm{mod} p^\alpha$ займет кольцо вычетов по $\mathrm{mod}\mathfrak{p}^\alpha$, изоморфное кольцу вычетов по $\mathrm{mod}(f(x))^{\alpha_i}$, где $f(x)$ — некоторый неприводимый многочлен над $\mathbf{F}_p$.

Найти какое-либо расширение $\mathbf{K}/\mathbf{Q}$ поля $\mathbf{Q}$, для которого идеал (p) является разветвленным, не сложно и может быть, например, реализовано даже в некотором расширении $\mathbf{Q}$ степени два. Одним из кандидатов такого расширения является поле $\mathbf{Q}(\beta)$, где β — корень уравнения $x^2 + p$.

Естественным вопросом, на который хотелось бы ответить, является вопрос как использовать полученные результаты для упрощения логарифмирования в конечном простом поле? Как полагает автор прямо использовать функции Ферма не представляется возможным из-за того, что у этих функции в ядро обязательно входит мультипликативная группа $(\mathbf{Z}/m\mathbf{Z})^*$ кольца вычетов по $\mathrm{mod}m$, вернее подгруппа $(\mathbf{Z}/m^2\mathbf{Z})^*$ ей изоморфная (теорема 1). Поэтому например при $m = p$ следы интересующей нас группы $(\mathbf{Z}/p\mathbf{Z})^*$ в образе $\Phi_1(a)$ отсутствуют.

Поэтому естественно рассматривать m вида $m = m'pn$, $n|p-1$,. Для таких m у некоторых $\Phi_i(a)$ подгруппа $(\mathbf{Z}/m^2\mathbf{Z})^*$ порядка n не входит в ядро. Вместе с тем сказать в настоящее момент что либо окончательное о сложности логарифмирования в конечном простом поле автор не может.

Как думает автор, "новые" функции частные Ферма по существу вступят в игру при работе с кольцом вычетов по модулю $\mathfrak{M}$, где $\mathfrak{M}$ — некоторый идеал, лежащий над p.

Сделаем несколько замечаний связанных с историей изучения функций частное Ферма. Около полутора столетия назад их рассматривал в своих работах Абель, который интересовался вопросом: может ли число $a^{p-1} - 1$ делится на p^2?. Эйзенштен (G. Eisenstein) установил, что функции $\Phi_1(a)$, определенной в (2), выполнено

$$\Phi_1(ab) \equiv \Phi_1(a) + \Phi_1(b) \bmod p \ \text{ и } \ \Phi_1(a + cp) \equiv \Phi_1(a) - c/a \bmod p.$$

Также рассматривались [7] функции $\Phi(a) \equiv \frac{a^{\varphi(m)}-1}{m} \bmod m$, которые являются естественным обобщением функций из (2) на непростые числа m, $m \in (\mathbf{Z}/m\mathbf{Z})^*$. Ризель [2] заменил функцию Эйлера $\varphi(m)$ в последнем равенстве на функцию Кармайкла $\lambda(m)$ — наименьшее общее кратное порядков элементов в $(\mathbf{Z}/m\mathbf{Z})^*$.

Видимо, не известно является ли для фиксированного a бесконечным число простых p, для которых $\Phi_1(a) \equiv 0 \bmod p$. Имеется многочисленные численные примеры таких пар Абеля (p, a). Как указано в [6] со ссылкой на [8], что для $a = 2$ имеется только две пары Абеля $(1093, 2)$ и $(3511, 2)$ при $p < 4 \times 10^{12}$.

Известны также неудачные попытки использовать частных Ферма для логарифмирования в конечном поле. Причина этого, как полагает автор, указана выше. Вместе с тем, возможно, определенные ниже обобщенные функции Ферма при подходящем выборе m, связанном некотором образом с

простым p, по модулю которого мы производим логарифмирование, могут оказаться полезными для решения нашей основной задачи. Как выбирать подобные m в настоящий момент не известно.

Автор ни коей мере не претендует на полноту изложения истории изучения функций частное Ферма.

§2. Определение функций частное Ферма и их свойства

Пусть $m = \prod_{i=1}^{u} p_i^{\alpha_i}$, $p_i > 2$, $\alpha_i > 0$ — каноническое разложение нечетного целого m, $a = a_0 + a_1 m$ — целое, взаимно простое с m, $0 < a_0 < m$, $\varphi(\cdot)$ — функция Эйлера. Рассмотрим $\mathbf{Z}(m) = (\mathbf{Z}/m\mathbf{Z})^*$ мультипликативную группу кольца $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$.

Как известно, [3], $|\mathbf{Z}(m)| = \varphi(m)$ и группа $\mathbf{Z}(m)$ изоморфна прямому произведению циклических подгрупп $\mathbf{Z}({p_i}^{\alpha_i})$ порядков $\varphi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i - 1}$, $i = 1, ..., u$.

Пусть $m_i = m p_i^{-\alpha_i}$ и $n_i, n_i \in \mathbf{Z}(m)$, — число, определенное условием $n_i^{-1} \equiv m_i \bmod p_j^{\alpha_j}$, $j = 1, \ldots, j-1, j+1, \ldots, u$, и $a \in \mathbf{Z}(m)$. Отметим, что $(n_i, m p_i^{-\alpha i}) = 1$. Легко также установить, что числа n_i можно выбрать так, чтобы

$$\sum_{j=0}^{u} n_i m_i = 1.$$

Далее будем полагать, что последнее равенство всегда выполнено.

Через $\vec{a}$ будем обозначать вектор $\vec{a} = (a_1, \ldots, a_u)$, $a_i \in \mathbf{Z}(p_i^{\alpha_i})$, определенный равенством

$$a \equiv \sum_{j=0}^{u} a_j n_j m_j \bmod m,$$

который будем рассматривать как образ элемента a в группе $\mathbf{Z}(p_1^{\alpha_1}) \times \ldots \times \mathbf{Z}(p_u^{\alpha_u})$. Будем коротко писать, что $a \sim \vec{a}$.

Циклическую подгруппу порядка $\varphi(p_i^{\alpha_i})$ группы $\mathbf{Z}(m)$, образованную элементами a, для которых вектор $\vec{a}$ имеет вид $\vec{a} = (1, \ldots, 1, a_i, 1, \ldots, 1)$, $a_i \in \mathbf{Z}(p_i^{\alpha_i})$, $(p_i^{\alpha_i}, a_i) = 1$, будем обозначать через $\mathbf{Z}^{(i)}(m)$, $i = 1, \ldots, u$.

Рассмотрим функцию

$$v_i(a) = v_i(\vec{a}) = a_i^{\varphi(p_i^{\alpha_i})} - 1. \tag{5}$$

Очевидно,

$$v_i(a) \equiv 0 \bmod p_i^{\alpha_i},$$

ибо $\varphi(p_i^{\alpha_i})$ — порядок группы $\mathbf{Z}(p_i^{\alpha_i})$ и поэтому $a_i^{\varphi(p_i^{\alpha_i})} = 1 + b p_i^{\alpha_i}$. Следовательно, число

$$v_i(a)v_i(b) = (v_i(ab) - v_i(a) - v_i(b)) \tag{6}$$

делится на $p_i^{2\alpha_i}$. Отсюда

$$v_i(ab) \equiv v_i(a) + v_i(b) \bmod p_i^{\alpha_i} \tag{7}$$

Так как $v_i(a + m^2) \equiv v_i(a) \bmod m^2$, то произведение ab в (7) можно рассматривать по $\bmod m^2$, что и будем делать в дальнейшем.

Определение 1. *Функцию* $\Phi_i(a)$, $a \in \mathbf{Z}(m)$, $a \sim (a_1, \ldots, a_u)$,

$$\Phi_i(a) \equiv \Phi_i(\vec{a}) \equiv \frac{v_i(a) n_i m_i}{p_i^{\alpha_i}} \equiv \frac{(a_i^{\varphi(p_i^{\alpha_i})} - 1) n_i m_i}{p_i^{\alpha_i}} \bmod m \tag{8}$$

будем называть частным Ферма, отвечающим примарному показателю $p_i^{\alpha_i}$.

Несколько иначе функция $\Phi_i(a)$ может быть определена следующим образом. Пусть ω_i — гомоморфизм группы $\mathbf{Z}(m)$ на подгруппу $\mathbf{Z}^{(i)}(m)$. Тогда

$$\Phi_i(a) \equiv \frac{\omega_i(a^{\varphi(p_i^{\alpha_i})}) - 1}{p_i^{\alpha_i}} \equiv \frac{\omega_i(a)^{\varphi(p_i^{\alpha_i})} - 1}{p_i^{\alpha_i}} \bmod m. \tag{9}$$

Как вытекает из (7) имеет место равенство

$$\Phi_i(ab) \equiv \Phi_i(a) + \Phi_i(b) \bmod m, \tag{10}$$

где под ab понимается число, равное произведению чисел a и b (без приведения по модулю m).

Область определения $\Phi_i(a)$ естественно расширить на группу $\mathbf{Z}(m^2)$, положив

$$\Phi_i(a+bm) \equiv \Phi_i(a) + \varphi(p_i^{\alpha_i})a_i^{-1}bn_im_i \bmod m, \tag{11}$$

где $a \in \mathbf{Z}(m), b \in \mathbf{Z}/m\mathbf{Z}$ и a_i^{-1} — обратное к a_i число, вычисленное по $\mathrm{mod}p_i^{\alpha_i}$. Следует отметить, что правая часть в (11) вычисляется в соответствии с (8), ибо $\varphi(p_i^{\alpha_i})a_i^{-1}bn_im_i$ — это как раз та часть значения $\Phi_i(a+bm)$, которая отвечает b.

Для функции $\Phi_i(a)$, определённой соотношением (8), выполнено $\Phi_i(a+m^2) = \Phi_i(a)$, поэтому группа $\mathbf{Z}(m^2)$ является естественной областью её определения.

Как следует из (10), функция $\Phi_i(a)$ гомоморфно отображает мультипликативную группу $\mathbf{Z}(m^2)$ на некоторую подгруппу аддитивной группы кольца $\mathbf{Z}/m\mathbf{Z}$. Очевидно, что подгруппа порядка $\varphi(m^2)\varphi^{-1}(p_i^{2\alpha_i})$ группы, образованная всеми $a \sim \vec{a} = (a_1, \ldots, a_u)$, у которых $a_i = 1$, принадлежит ядру этого отображения.

Нашей дальнейшей целью является изучение линейного над $\mathbf{Z}/m\mathbf{Z}$ пространства $L(m)$, образованного множеством функций вида

$$\Phi(a) \equiv \sum_{i=0}^{u} b_i\Phi_i(a) \bmod m,$$

где коэффициенты b_i независимо пробегают элементы кольца $\mathbf{Z}/m\mathbf{Z}$.

Теорема 1. *Пусть* $\varphi(p_i^{2\alpha_i}) = p_i^{\alpha_i}\varphi(p_i^{\alpha_i}) = p_i^{2\alpha_i-1}(p-1)$ *и* $\mathbf{Z}^{(i)}(m^2, p_i^{2\alpha_i-1})$, $\mathbf{Z}^{(i)}(m^2, p-1)$ — *подгруппы группы* $\mathbf{Z}^{(i)}(m^2)$ *порядков* $p_i^{2\alpha_i-1}$ *и* $p-1$, *соответственно.*

Функция $\Phi_i(a)$ *гомоморфно отображает группу* $\mathbf{Z}^{(i)}(m^2)$ *на подгруппу порядка* $p_i^{\alpha_i}$ *аддитивной группы* $\mathbf{Z}(m)$, *образованную числами* $jm_i = jmp_i^{-\alpha_i}, j = 0, \ldots, p_i^{\alpha_i} - 1$. *Ядром этого отображения в подгруппе* $\mathbf{Z}^{(i)}(m^2)$ *является подгруппа* $\tilde{\mathbf{Z}}^{(i)}(p^{\alpha_i})$ *порядка* $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}g_i$, *образованная числами* $a^{p_i^{\alpha_i}}$, $a \in \mathbf{Z}^{(i)}(m^2)$, *т.е. подгруппа группы* $\mathbf{Z}^{(i)}(m^2)$ *изоморфная мультипликативной группе* $\mathbf{Z}^{(i)}(m)$.

Доказательство. Элемент a группы $\mathbf{Z}(m^2)$ представим в виде $a = a_1s_ip_i^{2\alpha_i} + a_2\hat{n}_im^2p_i^{-2\alpha_i}$, где $s_ip_i^{2\alpha_i} = 1 \bmod m^2p_i^{-2\alpha_i}$, $\hat{n}_im^2p_i^{-2\alpha_i} \equiv 1 \bmod p_i^{2\alpha_i}$, $a_1 \in \mathbf{Z}(m^2p_i^{-2\alpha_i}), a_2 \in \mathbf{Z}(p_i^{2\alpha_i})$, $s_ip_i^{2\alpha_i} + \hat{n}_im^2p_i^{-2\alpha_i} = 1$. Как легко видеть, $a^x \equiv [a_1^x]_1s_ip_i^{2\alpha_i} + [a_2^x]_2\hat{n}_im^2p_i^{-2\alpha_i} \bmod m^2$, где $[y]_j$, $j = 1, 2$, — вычет числа y по модулю $m^2p_i^{-2\alpha_i}$ и $p_i^{2\alpha_i}$, соответственно. Отсюда при $a = s_ip_i^{2\alpha_i} + a_2\hat{n}_im^2p_i^{-2\alpha_i} \in \mathbf{Z}^{(i)}(m^2)$ получим

$$a^{\varphi(p_i^{\alpha_i})} = s_ip_i^{2\alpha_i} + [a_2^{\varphi(p_i^{\alpha_i})}]_2\hat{n}_im^2p_i^{-2\alpha_i}). \tag{12}$$

Следовательно,

$$\Phi_i(a) \equiv \frac{s_ip_i^{2\alpha_i} + (1+lp_i^{\alpha_i})\hat{n}_im^2p_i^{-2\alpha_i} - 1}{p_i^{\alpha_i}} \equiv l\hat{n}_im^2p_i^{-2\alpha_i} \equiv jmp_i^{-\alpha_i} \bmod m,\ j \equiv l\hat{n}_imp_i^{-\alpha_i} \bmod p_i^{\alpha_i}$$

в виду того, что функция $[a_2^{\varphi(p_i^{\alpha_i})}]_2$ отображает циклическую группу $\mathbf{Z}(p_i^{2\alpha_i})$ на подгруппу порядка $p_i^{\alpha_i}$, элементы которой имеют вид $1 + lp_i^{\alpha_i} \bmod p_i^{2\alpha_i}$ [3].

Таким образом, функция $\Phi_i(x)$ отображает группу $\mathbf{Z}^{(i)}(m^2)$ на подгруппу порядка $p_i^{\alpha_i}$ аддитивной группы кольца $\mathbf{Z}/m\mathbf{Z}$. Ядром этого отображения является подгруппа $\tilde{\mathbf{Z}}^{(i)}(m^2)$ чисел вида $c = a^{p_i^{\alpha_i}}$, $a \in \mathbf{Z}^{(i)}(m^2)$ в виду того, что $\varphi(p_i^{2\alpha_i}) = \varphi(p_i^{\alpha_i})p_i^{\alpha_i}$, и, следовательно,

$$\Phi_i(c) \equiv \Phi_i(a^{p_i^{\alpha_i}}) \equiv \frac{(a_i^{\varphi(p_i^{2\alpha_i})} - 1)n_im_i}{p_i^{\alpha_i}} \equiv \frac{(1+lp_i^{2\alpha_i} - 1)n_im_i}{p_i^{\alpha_i}} \equiv 0 \bmod m.$$

$\star$

Группа $\tilde{\mathbf{Z}}^{(i)}(p_i^{\alpha_i})$, образованная элементами вида $c = a^{p_i^{\alpha_i}}, a \in \mathbf{Z}^{(i)}(m^2)$, изоморфна группе $\mathbf{Z}(p_i^{\alpha_i})$. Отметим, что координата $c_i = a' + a''p_i^{\alpha_i}$, $a' \in \mathbf{Z}(p_i^{\alpha_i})$ ее элемента $\vec{c} \sim c$ имеет вид

$$c_i = a' + a'\Phi_i(a')p_i^{\alpha_i},\ a' \in \mathbf{Z}(p_i^{\alpha_i}). \tag{13}$$

Действительно, в этом случае

$$a^{p_i^{\alpha_i}} = s_ip_i^{2\alpha_i} + [a_i^{p_i^{\alpha_i}}]_2\hat{n}_im_i^2p_i^{-2\alpha_i},\ a_i \in \mathbf{Z}(p_i^{2\alpha_i})$$

и, как нетрудно вычислить,

$$[a_i^{p_i^{\alpha_i}}]_2 = [(a' + a''p_i^{\alpha_i})^{p_i^{\alpha_i}}]_2 = a'\Phi(a')p_i^{\alpha_i} + a'.$$

Отсюда и из определения функции $\Phi(a)$ следует, что все $c = a^{p_i^{\alpha_i}}$, $a \in \mathbf{Z}^{(i)}(m^2)$ имеют вид

$$c = s_i p_i^{\alpha_i} + (a' + a'\Phi(a')p_i^{\alpha_i})\hat{n}_i m^2 p_i^{-2\alpha_i},\ a' \in \mathbf{Z}(p^{\alpha_i}). \tag{14}$$

Функцию Ферма $\Phi(x)$ обычно определяют соотношением

$$\Phi(a) \equiv \frac{a^{\lambda(m)} - 1}{m} \bmod m, \tag{15}$$

где $\lambda(m)$ — наименьшее общее кратное порядков элементов группы $\mathbf{Z}(m)$ (функция Кармайкла). Очевидно, она обладает свойством аналогичным (10), т.е. гомоморфно отображает мультипликативную группу $\mathbf{Z}(m^2)$ в аддитивную группу $\mathbf{Z}/m\mathbf{Z}$. Имеем

$$a = \prod_{j=0}^{u} \omega_i(a) \quad \text{и} \quad \Phi_i(\omega_j(a)) = 0,\ i \neq j,\ \Phi_i(\omega_i(a)) = \Phi_i(a).$$

Поэтому с учетом (9)

$$\Phi(a) = \sum_{j=0}^{u} \Phi(\omega_j(a)) = \sum_{j=0}^{u} \frac{(a_j^{\lambda(m)} - 1)n_j m_j}{p_i^{\alpha_i}} =$$

$$= \sum_{j=0}^{u} \Phi_j(a^{\lambda(m)p_j^{-\alpha_j}}) = \sum_{j=0}^{u} \lambda(m) p_j^{-\alpha_j} \Phi_j(a).$$

Таким образом, функция $\Phi(x)$ принадлежит пространству $L(m)$.

§3. Примеры возможного использования функций $\Phi_i(a)$ для вычисления индексов элементов в группе $\mathbf{Z}(m)$

Пример 1. $m = p$ — простое число.

В этом случае $u = 1$ и, следовательно, существует только одна функция частное Ферма $\Phi_1(a)$.

Как следует из теоремы 1, подгруппа $\tilde{\mathbf{Z}}(p) \triangleleft \mathbf{Z}(p^2)$, изоморфная мультипликативной группе $\mathbf{Z}(p)$ конечного простого поля $\mathbf{F}_p$, отображается функцией $\Phi_1(a)$ в 0.

Из (13) следует, что элементы $a \in \tilde{\mathbf{Z}}(p)$ имеют вид

$$a = a' + a'\Phi_1(a')p,\ a' \in \mathbf{Z}(p). \tag{16}$$

В рассматриваемом случае, видимо, функцию $\Phi_1(a)$ прямо невозможно использовать для вычисления индексов элементов в группе $\mathbf{Z}(p)$. Вместе с тем функция $\mathrm{ind}_\xi(a)$ (корень уравнения $\xi^x \equiv a \bmod p$) может быть вычислена с сложностью $O(\log p)$ с помощью функции $\Phi_1(a)$ и некоторой другой числовой функции $\Gamma_p(a)$, к определению которой мы переходим.

Группа $\mathbf{Z}(p^2)$ порядка $\varphi(p^2) = p(p-1)$ является прямым произведением групп $\tilde{\mathbf{Z}}(p) \triangleleft \mathbf{Z}(p^2)$ и $\hat{\mathbf{Z}}(p) \triangleleft \mathbf{Z}(p^2)$ порядков $p-1$ и p. Группа $\tilde{\mathbf{Z}}(p)$ изоморфна мультипликативной группе конечного поля $\mathbf{Z}/p\mathbf{Z}$, а ее элементы имеют вид (16). Группа $\hat{\mathbf{Z}}(p)$ изоморфна аддитивной группе конечного поля $\mathbf{Z}/p\mathbf{Z}$, а ее элементы имеют вид $1 + ap$, $a \in \mathbf{Z}/p\mathbf{Z}$.

Первообразный корень $\xi \in \mathbf{Z}(p)$, $0 < \xi < p$, будем рассматривать как элемент группы $\mathbf{Z}(p^2)$. Представим его в виде $\xi = cd, c = \xi + \xi\Phi_1(\xi)p \in \tilde{\mathbf{Z}}(p-1)$, $d = 1 + \Theta(\xi)p \in \hat{\mathbf{Z}}(p)$. Функции $\Phi_1(\xi)$ и $\Theta(\xi)$, как следует из их определения, связаны соотношением

$$\xi\Phi_1(\xi) + \Theta(\xi) \equiv 0 \bmod p. \tag{17}$$

Пусть ξ — первообразный элемент поля $\mathbf{F}_p$ и $\xi^x \equiv a \bmod p$, $0 \leq x < p-1$. Функцию $\Gamma_p(a)$, $\Gamma_p(a) \in \mathbf{Z}/p\mathbf{Z}$, определим соотношением

$$\xi^x \equiv a + \Gamma_p(a)p \bmod p^2,\ 0 < a < p,\ 0 \leq x < p-1,\ a \equiv \xi^x \bmod p.$$

Имеем

$$\xi^x \equiv a + \Gamma_p(a)p \equiv (a + a\Phi_1(a)p)(1 + x\Theta(\xi)p) \equiv a + (a\Phi_1(a) + ax\Theta(\xi))p \bmod p^2,\ 0 \leq x < p-1$$

Откуда

$$a\Phi_1(a) + ax\Theta(\xi) \equiv \Gamma_p(a) \bmod p.$$

Следовательно, с учетом (17)

$$\Phi_1(a) - a\xi x\Phi(\xi) \equiv \Gamma_p(a) \bmod p. \tag{18}$$

или

$$x \equiv \mathrm{ind}_\xi(a) \equiv \frac{\Phi_1(a) - \Gamma_p(a)}{a\xi\Phi_1(\xi)} \bmod p, \tag{19}$$

если $\Phi_1(\xi) \not\equiv 0 \bmod p$.

Таким образом, при $\Phi_1(\xi) \not\equiv 0 \bmod p$ сложность вычисления функций $\mathrm{ind}_\xi(a)$ и $\Gamma_p(a)$ примерно одинакова.

Пример 2. $m = p^\alpha,\ \alpha > 1$.

В этом случае также имеется только одна функция $\Phi_1(a)$ $(u = 1)$.

Пусть $x = x_0 + x_1(p-1),\ 0 \le x_0 < p-1,\ 0 \le x_1 < p^{\alpha-1}$, — решение уравнения (1) при $n = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Предположим, что число x_1 известно. В этом случае уравнение (1) может быть записано в виде

$$\xi^{x_0} \equiv a\xi^{-x_1 p} \equiv a' + a'\Gamma_p(a') + a_2p^2 + \ldots (\mathrm{mod} p^2),\ 0 \le x_0 < p-1. \tag{20}$$

Так как $\alpha > 1$, то мы сможем вычислить функцию $\Gamma_p(a'),\ a' \in \mathbf{Z}(p)$, где $a' + \Gamma_p(a')p \equiv a \bmod p^2$.

Результаты из примера **1.** (равенство (19)) позволяют в этом случае найти x_0 с полиномиальной сложностью от длины записи числа p в том случае, когда $\Phi_1(\xi) \neq 0$.

Как полагает автор, правдоподобно утверждение: $\Phi_0(\xi) \neq 0$, если порядок элемента ξ достаточно большой, скажем, больше или равен $c\log p$, где c — некоторая постоянная.

Следует заметить, что достаточно знать x_1 по $\mathrm{mod} p$, ибо в этом случае мы можем найти решение 1 при $\alpha = 2$, а затем при $\alpha > 2$ "поднять" его в группу $\mathbf{Z}(p^\alpha)$. Последняя операция осуществляется при $\alpha = const,\ p \to \infty$, за число операций не выше $O(\log^3 p)$.

Верно и обратное: если $x = x_0 + x_1(p-1),\ 0 \le x_0 < p-1,\ 0 \le x_1 < p^{\alpha-1}$, — решение уравнения 1 при $n = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$ и число x_0 известно, то число x_1 может быть определено с полиномиальной сложностью.

Действительно, очевидно, в этом случае решение сводится к решению уравнения в подгруппе $\mathbf{Z}(p^\alpha, p^{\alpha-1})$, порядка $p^{\alpha-1}$ подгруппы группы $\mathbf{Z}(p^\alpha)$. Группа $\mathbf{Z}(p^\alpha, p^{\alpha-1})$ образована числами $1 + jp(\mathrm{mod} p^\alpha)$ и решение в ней уравнения

$$(1 + jp)^x = 1 + bp(\mathrm{mod} p^\alpha)$$

тривиально: достаточно его решить при $\alpha = 2$, а затем поднять его в группы $\mathbf{Z}(p^\alpha, p^3), \ldots$ $\ldots, \mathbf{Z}(p^\alpha, p^{\alpha-1})$. Все это можно, очевидно, сделать при $\alpha = const, p \to \infty$, за число операций не выше $O(\log^3 p)$.

Таким образом, доказана теорема

Теорема 2 *Пусть $x = x_0 + x_1(p-1)$ — решение уравнения 1 при $m = p^\alpha,\ \alpha > 1$. Если одно из чисел x_0 или $x_1 \bmod p$, то оставшееся число при $\alpha = const,\ p \to \infty$, может быть вычислено за число операций не выше $O(\log^3 p)$.*

Пример 3. $m = \prod_{i=1}^u p_i^{\alpha_i},\ p_i > 2,\ (\varphi(p_i^{\alpha_i}), n) = n,\ i = 1, ..., u$. Мы рассматриваем уравнение (1), где n — порядок группы порожденной элементом ξ — является простым числом. Также будем полагать, что выписанное разложение m на примарные множители известно.

Следует отметить, что если $m = m'm''$ и $(m', m'') = 1$, то уравнение (1) распадается в два уравнения по $\mathrm{mod} m'$ и $\mathrm{mod} m''$. Делается это следующим образом.

Пусть $\xi = \xi' n'm' + \xi'' n''m'',\ a = a'n'm' + a''n''m'',\ n''m'' \bmod m' \equiv 1 \equiv n'm' \bmod m'',\ n'm' + n''m'' = 1$. Тогда $\xi^x = \xi'^x n'm' + \xi''^x n''m'' = a'n'm' + a''n''m''$ и, следовательно, (1) эквивалентно двум уравнениям $\xi'^x \equiv a' \bmod m''$ и $\xi''^x \equiv a'' \bmod m'$. В частности, если порядок ξ' по $\mathrm{mod} m''$ равен 1, то первое уравнение не несет информации о x, и поэтому уравнение (1) в этом случае эквивалентно последнему из выписанных уравнений. Если порядки ξ' и ξ'' по $\bmod m''$ и $\bmod m'$ равны n, то каждое из последних двух уравнений эквивалентны исходному (1) в том смысле, что решение каждого из них совпадает с x.

Таким образом, если $(\varphi(m'), n) = 1$, то решение (1) сводится к решению аналогичного уравнения с $m = m''$ и если разложение m на m' и m'' известно, то это сведение осуществляется не более, чем за $O(\log^2 m)$ операций: необходимо только вычислить ξ и a по $\mathrm{mod} m''$. Поэтому мы изначально и предполагаем, что $(\varphi(p_i^{\alpha_i}), n) = n$.

Литература

[1] Odlyzko A.M. Discrete logarithms in finite fields and their cryptography significance. Adv. in Cryptology. Computer Science, V.209, Springer-Verlag, N.Y., $234-314$.

[2] Reisel H. Same soluble cases of the discrete logarithm problem. BIT, $28, 4, 1988, 839-851$.

[3] И.М. Виноградов, Основы теории чисел. М. Наука. 1981.

[4] Ю.В. Нестеренко, Частные Ферма в кольцах алгебраических чисел. Рукопись, 1996г.

[5] В.М. Сидельников, Частные Ферма и логарифмирование в конечном простом поле. Материалы межд. научных чтений по аналитической теории чисел и приложениям. 3-6 февраля 1997 г., МГУ, стр. 28-30.

[6] Saton T., Araki K., Ferma Quantients and Polynomial Time Discrete Log Algorithms for Anomalous Elliptic Curves. Commentarii math. uniersitatis Sancti Pauli, Vol. 47, No 1, 1988, pp. 81-92.

[7] Lerch M., Zur Theorie des Fermatschen Quantienten $\frac{a^{p-1}-1}{p} = q(a)$. Math. Ann. 60, 471-490, 1905.

[8] Ribenboim P.,The new book of prime number records. 3rd ed. Berlin-Heidelberg-New-York, Springer, 1995.