О некоторых свойствах групп алгебр с параметрами

Ю. А. Ишматова

Группы алгебр с параметрами являются основным объектом в ряде криптографических стандартов республики Узбекистан. В работе исследуется ряд свойств таких групп, существенных с точки зрения криптографии. Доказывается критерий обратимости элемента, вычисляется порядок группы, а также устанавливается связь возведения в степень с возведением в степень в мультипликативных группах колец вычетов.

Ключевые слова: алгебры с параметром, криптографический стандарт, возведение в степень.

1. Введение

Алгебры с параметрами были введены в 1974 году в работах П. Ф. Хасанова [3, 4] для решения задач анализа линейных электрических цепей. При выработке криптографических стандартов республики Узбекистан алгебры с параметрами были выбраны в качестве основного объекта алгоритма вычисления электронной подписи [6], а также одного из объектов алгоритма симметричного шифрования [7]. В работах, посвященных анализу предложенных стандартов [8], формулировались некоторые утверждения о свойствах групп алгебр с параметрами, в том числе критерий обратимости элемента и формула для вычисления порядка группы, однако доказательств сформулированных утверждений в открытых источниках найти не удалось. Кроме того, вопросы сложности решения задачи дискретного логарифмирования в группах алгебр с параметрами и сложности возведения в степень в алгебрах с параметрами не исследовались на формальном уровне.

В данной работе приводятся доказательства критерия обратимости элемента алгебры с параметрами (теорема 1) и формулы для вычисления порядка группы (теорема 2). Теорема 3 устанавливает связь между возведением в степень в группах алгебр с параметрами (при значениях параметра, отвечающих стандарту вычисления электронной подписи) и возведением в степень в мультипликативных группах колец вычетов. Показывается, что сложность решения задач дискретного логарифмирования и возведения в степень в этих группах эквивалентны.

Автор выражает глубокую благодарность научному руководителю н.с. А. В. Галатенко за постановки задач и внимание к работе.

2. Основные понятия и результаты

Пусть $n \in \mathbb{N}$, $R \in \mathbb{Z}_n$. Рассмотрим двуместную операцию $\circledR$: $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, называемую умножением с параметром R и определенную следующим соотношением: $\forall a, b \in \mathbb{Z}_n, a \circledR b = (a + b + abR) \pmod n$. Несложно увидеть, что введенная операция является коммутативной и ассоциативной, а элемент 0 является нейтральным. Множество Z_n с введенной операцией будем называть алгеброй с параметром R. Строго говоря, введенный объект зависит от двух параметров — n и R, однако мы будем следовать терминологии работ [3, 4, 6, 7] и исключать первый параметр из названия.

Заметим, что в случае, когда $R = 0$, алгебра с параметром R превращается в группу по сложению кольца вычетов $\mathbb{Z}_n$. Задача дискретного логарифмирования в такой группе эквивалентна делению, то есть легко разрешима. В дальнейшем мы будем считать, что $R \neq 0$. Кроме того, будем считать, что $n > 1$ (в противном случае задача вырождается).

Для верификации электронной подписи необходима обратимость некоторых элементов, участвующих в алгоритме. Как следствие, становится важной задача проверки обратимости элемента. Приведем критерий обратимости относительно операции умножения с параметром R. Для того, чтобы различать обращение в алгебре с параметром

от обращения в $\mathbb{Z}_n$, операцию взятия обратного элемента для умножения с параметром будем обозначать $\backslash -1$.

Теорема 1. *Пусть $n \in \mathbb{N}, R \in \mathbb{Z}_n$, $a \in \mathbb{Z}_n$. Элемент a является обратимым относительно умножения с параметром R тогда и только тогда, когда $1+R*a$ обратим по умножению в $\mathbb{Z}_n$. В этом случае обратный элемент вычисляется по формуле $a^{\backslash -1} = -a(1 + R * a)^{-1} \pmod n$.*

Следствие 1. *Сложность решения задачи проверки обратимости элемента в алгебре с параметром R превосходит сложность решения задачи проверки обратимости по умножению элемента в $\mathbb{Z}_n$ не более, чем на константу.*

Легко увидеть, что подмножество обратимых элементов алгебры с параметром образует группу относительно умножения с параметром R.

Для защищенности от атак методом «грубой силы» необходимо, чтобы размер группы, в которой производятся вычисления, был достаточно большим. Порядок группы алгебры с параметром вычисляется в следующей теореме.

Теорема 2. *Пусть $n \in \mathbb{N}$, $n = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$, где $k \in \mathbb{N}$, p_i — простые числа, $\alpha_i \in \mathbb{N}, i = 1, \ldots, k$. Пусть $R \in \mathbb{Z}_n$, $R \neq 0 \pmod n$. Пусть $\Phi(R, n)$ — порядок группы алгебры с параметром R. Тогда справедливо следующее равенство:*

$$\Phi(R,n) = \prod_{\{p_j | (R,p_j) \neq 1\}} p_j^{\alpha_j} \prod_{\{p_k | (R,p_k) = 1\}} p_k^{\alpha_k}(1 - \frac{1}{p_k}).$$

Из теоремы 2 следует, что порядок группы алгебры с параметром R не меньше порядка мультипликативной группы $\mathbb{Z}_n$.

Основной операцией в стандарте вычисления электронной подписи является возведение в степень в алгебре с параметром. Возведение элемента a в степень k с параметром обозначим через $a^{\backslash k}$. Теорема 3 устанавливает связь возведения в степень в $\mathbb{Z}_n$ и в алгебрах с параметрами.

Теорема 3. *Пусть $n \in \mathbb{N}$, $R \in \mathbb{Z}_n$, $R \neq 0 \pmod n$, причем R и n взаимно просты. Пусть $t, u \in \mathbb{N}$. Тогда для любых элементов a и b, принадлежащих $\mathbb{Z}_n$, справедливы следующие равенства:*

$$a^{\backslash t} = ((1 + R * a)^t - 1)/R \pmod n,$$
$$b^u = R * (((b-1)/R)^{\backslash u}) + 1 \pmod n.$$

Следствие 2. *Пусть $n \in \mathbb{N}$, $R \in \mathbb{Z}_n$, $R \neq 0 \pmod n$, причем R и n взаимно просты. Тогда сложности решения задач дискретного логарифмирования и возведения в степень в кольце вычетов по модулю n и в алгебре с параметром R эквивалентны.*

Учитывая следствие и верхнюю для числа умножений при возведении в степень [5], получаем, что асимптотическая сложность возведения в степень с параметрами для взаимно простых R и n асимптотически не превосходит $\log n$.

3. Вспомогательные утверждения

Приведенные в данном разделе леммы предназначены для доказательства теоремы 2; теорема 1 доказывается независимо, поэтому использование в доказательстве лемм теоремы 1 является корректным.

Лемма 1. *Пусть $n \in \mathbb{N}$, $R \in \mathbb{Z}_n$, $R \neq 0$, R и n взаимно просты. Пусть $M = \{(1 + Ra) \pmod n | a \in \mathbb{Z}_n\}$. Тогда число обратимых элементов по модулю n в M и в $\mathbb{Z}_n$ совпадает.*

Доказательство. Несложно увидеть, что отображение $f(a) = 1 + R * a \pmod n$ является биекцией в $\mathbb{Z}_n$. Действительно, в силу взаимной простоты R обратим в $\mathbb{Z}_n$, и умножение на R — биекция. Сложение с единицей также биекция. Таким образом M и $\mathbb{Z}_n$ совпадают как множества. Следовательно, число обратимых элементов в M и $\mathbb{Z}_n$ совпадает. Лемма доказана.

Лемма 2. *Пусть $n \in \mathbb{N}$, $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, где $k \in \mathbb{N}$, p_i — простые числа, $\alpha_i \in \mathbb{N}, i = 1, \ldots, k$. Пусть $R \in \mathbb{Z}_n$, $R \neq 0$, R и n взаимно просты.*

Тогда

$$\Phi(R,n)=\prod_{i=1}^{k}p_i^{\alpha_i}(1-\frac{1}{p_i}).$$

Доказательство. В силу леммы 1, число обратимых элементов в алгебре с параметром R и в $\mathbb{Z}_n$ совпадает. Число обратимых элементов в $\mathbb{Z}_n$ может быть вычислено с помощью функции Эйлера φ [1, Гл. 2, § 4], совпадающей с функцией Φ из условия леммы.

Лемма 3. *Пусть* $n\in\mathbb{N}$, $n=\prod\limits_{i=1}^{k}p_i^{\alpha_i}$, *где* $k\in\mathbb{N}$, p_i — *простые числа,* $\alpha_i\in\mathbb{N}, i=1,\ldots,k$. *Пусть* $R\in\mathbb{Z}_n$, $R=\prod\limits_{i=1}^{k}p_i^{\alpha_{i'}}$, $\alpha_{i'}\in\mathbb{N}, i=1,\ldots,k$. *Тогда* $\Phi(R,n)=n$.

Доказательство. В силу теоремы 1, элемент a из алгебры с параметром R обратим тогда и только тогда, когда элемент $1+R*a$ взаимно прост с n. Взаимная простота с n эквивалентна взаимной простоте с каждым простым делителем n. Но так как по условию все простые делители n делят R, то для любого элемента a из $\mathbb{Z}_n$ элемент $1+R*a$ равен 1 по модулю каждого простого делителя n. Следовательно все n элементов алгебры с параметром R обратимы.

Лемма 4. *Пусть* $n\in\mathbb{N}$, $n=n_1*n_2$, $n_1,n_2\in\mathbb{N}$, $n_1,n_2>1$, n_1 *и* n_2 *взаимно просты. Пусть* $R\in\mathbb{Z}_n$. *Тогда справедливо следующее равенство:*

$$\Phi(R,n)=\Phi(R\pmod{n_1},n_1)*\Phi(R\pmod{n_2},n_2).$$

Доказательство. Пусть элемент a принадлежит алгебре с параметром R и является обратимым. Из теоремы 1 следует, что $1+R*a$ и n взаимно просты. Так как n_1 и n_2 — делители n, $1+R*a$ взаимно прост с n_1 и n_2, откуда следует обратимость элементов $a\pmod{n_1}$ в алгебре с параметром $R\pmod{n_1}$ по модулю n_1 и в алгебре с параметром $R\pmod{n_2}$ по модулю n_2. Так как n_1 и n_2 взаимно просты, в силу китайской теоремы об остатках [2, Гл. 1, § 3], разным элементам a при этом будут соответствовать различные пары $(a\pmod{n_1}, a\pmod{n_2})$. Следовательно множество обратимых элементов алгебры

с параметром R инъективно вкладывается в множество пар обратимых элементов алгебр с параметрами $R \pmod{n_1}$ и $R \pmod{n_2}$ по соответствующим модулям.

Покажем, что рассмотренная инъекция является сюръекцией. Предположим, существует пара (a_1, a_2), причем a_1 обратим в алгебре с параметром $R \pmod{n_1}$ по модулю n_1, a_2 обратим в алгебре с параметром $R \pmod{n_2}$ по модулю n_2, и (a_1, a_2) не является образом обратимого элемента алгебры с параметром R по модулю n. Так как n_1 и n_2 взаимно просты, в силу китайской теоремы об остатках, существует элемент $a \in \mathbb{Z}_n$, такой что $a = a_1 \pmod{n_1}$, $a = a_2 \pmod{n_2}$. По предположению, a не является обратимым в алгебре с параметром R. Из теоремы 1 следует, что у $(1 + Ra)$ и n есть простой общий делитель p. Так как $n = n_1 * n_2$, p делит n_1 или n_2. Без ограничения общности p делит n_1. Следовательно, $1 + Ra = 1 + Ra_1 \pmod{n_1}$ и n_1 не являются взаимно простыми, что противоречит обратимости a_1.

Таким образом, построенное соответствие является биекцией.

4. Доказательства теорем

Доказательство теоремы 1

Необходимость. Пусть d — наибольший общий делитель n и $1 + R * a$, $d > 1$. Предположим, существует такое $b \in \mathbb{Z}_n$, что $a + b * (1 + R * a) = 0 \pmod{n}$. Рассмотрим это соотношение по модулю d. Получаем $a + 0 = 0 \pmod{d}$. Следовательно, $a = 0 \pmod{d}$. Из условия $1 + R * a = 0 \pmod{d}$ и равенства $a = 0 \pmod{d}$ получаем соотношение $1 = 0 \pmod{d}$. Противоречие.

Достаточность. Пусть элемент $1 + R * a$ взаимно прост с n. Тогда $1 + R * a$ обратим в $\mathbb{Z}_n$ и определено значение $b = -a(1 + R * a)^{-1} \pmod{n}$. Покажем, что $a \circledR b = 0 \pmod{n}$. В силу коммутативности умножения с параметром R это эквивалентно тому, что $b = a^{\backslash -1}$. В силу обратимости $1 + R * a$ достаточно показать, что $(1 + R * a)(a \circledR b) = 0 \pmod{n}$. Воспользовавшись опреелением умножения с параметром R, получаем следующую цепочку равенств: $(1 + R * a)(a \circledR b) = (1 + R * a)(a - a(1 + R * a)^{-1} - aRa(1 + R * a)^{-1}) = (1 + R * a) * a - a - aRa = 0 \pmod{n}$.

Доказательство теоремы 2

Разложим n в произведение n_1 и n_2, где n_1 соответствует всем простым делителям из НОД (R, n), n_2 — остальным простым делителям. Если n_1 равно 1, утверждение теоремы непосредственно вытекает из леммы 2, если n_2 равно 1 — из леммы 3.

Пусть $n_1, n_2 \neq 1$. В силу леммы 4, $\Phi(R, n) = \Phi(R \pmod{n_1}, n_1) * \Phi(R \pmod{n_2}, n_2)$. По лемме 2 $\Phi(R \pmod{n_2}, n_2) = \prod\limits_{\{p_k | (R, p_k) = 1\}} p_k^{\alpha_k}(1 - \frac{1}{p_k})$. По лемме 3 $\Phi(R \pmod{n_1}, n_1) = \prod\limits_{\{p_j | (R, p_j) \neq 1\}} p_j^{\alpha_j}$.

Доказательство теоремы 3

Так как R и n взаимно просты, элемент R обратим по модулю n, и все выражения корректно определены.

Докажем первое утверждение индукцией по показателю степени. При $t = 1$ утверждение является очевидно верным. Пусть утверждение верно для $t = k$. Покажем, что оно также верно при $t = k + 1$. Действительно, $a^{\backslash(k+1)} = a \circledR a^{\backslash k} \pmod{n}$. По инуктивному предположению, $a^{\backslash(k+1)} = a \circledR ((1 + R * a)^k - 1)/R = a + ((1 + R * a)^k - 1)/R + a((1 + R * a)^k - 1) = a(1 + ((1 + R * a)^k - 1)) + ((1 + R * a)^k - 1)/R \pmod{n}$. Сократив единицы во втором сомножителе первого слагаемого и сложив дроби, получаем следующее равенство: $a^{\backslash(k+1)} = (aR(1 + R * a)^k + (1 + R * a)^k - 1)/R = ((1 + R * a)^{k+1} - 1)/R \pmod{n}$.

Докажем второе утверждение. Пусть $u \in \mathbb{N}$. Выпишем первое утверждение для $a = (b - 1)/R \pmod{n}$. Получим следующее равенство: $((b - 1)/R)^{\backslash u} = ((1 + R * (b - 1)/R)^u - 1)/R \pmod{n}$. Упростив правую часть и разрешив соотношение относительно b^u, получим равенство из утверждения 2.

Список литературы

[1] Виноградов И. М. Основы теории чисел. М.-Л.: Гостехиздат, 1952.

[2] Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001.

[3] Хасанов П. Ф. Модели и алгебры схем цепей и систем / Дисс. на соиск. уч. ст. д. техн. наук. Ташкент, ТашПИБ, 1975. С. 144–250.

[4] Хасанов П. Ф. Фигурно-точечные модели и диаопределители матриц. Ташкент: Укитувчи, 1975.

[5] Brauer A. On addition chains // Bull. Amer. Math. Soc. 45. 1939. P. 736–739.

[6] O'z DSt 1092:2009. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Узбекское агентство стандартизации, метрологии и сертификации. Ташкент, 2009. http://nh.unicon.uz/detail.php?actn=1&id=2206

[7] O'z DSt 1105:2009. Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных. Узбекское агентство стандартизации, метрологии и сертификации. Ташкент, 2009. http://nh.unicon.uz/detail.php?actn=1&id=2207

[8] Xasanov X. P. Takomillashgan diamatricalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari (на узбекском языке). Ташкент: ФТМТМ, 2008.