УДК 511.1

ПСЕВДОЕДИНИЦЫ В РАСШИРЕНИИ МУЛЬТИПЛИКАТИВНОЙ ГРУППЫ ПО МОДУЛЮ КРИПТОСИСТЕМЫ RSA

PSEUDOUNITS IN ETH EXPANSION OF A MULTIPLICATIVE GROUP MODULO RSA CRYPTOSYSTEM

[1]Ульянов М.В., д-р. техн. наук, проф.

[1]Национальный исследовательский университет Высшая школа экономики

[2]Сметанин Ю.Г., д-р. физ.-мат. наук, г.н.с.

[2]Вычислительный центр РАН им. А.А. Дородницына

Аннотация

В статье рассматривается расширение до полной системы вычетов мультипликативной группы, порожденной составным модулем, соответствующим модулю в криптосистеме RSA. Вводится понятие псевдоединицы по модулю RSA и исследуются свойства псевдоединиц. Приводится формула для вычисления псевдоединиц по модулю RSA. Данная статья имеет теоретический характер, однако описанные в ней свойства псевдоединиц полезны в современных информационных технологиях при построении и анализе криптостойкости модифицированных схем цифровой подписи и обеспечении информационной безопасности и отказоустойчивости информационных и инфо-коммуникационных систем.

Ключевые слова: группы, системы вычетов, RSA, китайская теорема об остатках, псевдоединицы.

Abstract

Expansion of a multiplicative group modulo composite number in RSA cryptosystem up to the complete residual system is considered. A notion of pseudounit is proposed. Properties of pseudounits are investigated. A formula for pseudounits modulo RSA is presented.

Keywords: groups, residual systems, RSA, Chinese residue system, pseudounits.

1. Введение

Вопросы построения и анализа криптосистем с открытым ключом и схем электронной подписи, основанных на теоретико-числовых методах, привели к расширению интереса к свойствам сравнений по модулю составного числа. В классической теории чисел этот вопрос не относился к числу вопросов, вызывающих наибольший интерес, и авторам не удалось найти опубликованных результатов о числе решений степенных уравнений в кольцах по модулю составного числа. В связи с этим в статье рассматривается расширение мультипликативной группы, порожденной составным модулем, соответствующим модулю в криптосистеме RSA, до полной системы вычетов. Элементы этого расширения обладают рядом особенностей, но основной является наличие чисел, обладающих свойствами единицы. Изучению особенностей этого расширения, введению понятия псевдоединицы в расширении группы по модулю RSA и исследованию свойств псевдоединиц и посвящена настоящая статья.

2. Обозначения и терминология

Далее в тексте статьи авторы используют следующие, как общепринятые в теории чисел [1], так и оригинальные обозначения; рассматриваются только неотрицательные целые числа:

$Z_+ = N \cup \{0\}$ — множество неотрицательных целых чисел;

$n = p \cdot q$ — модуль криптосистемы RSA [2], p, q — простые нечетные числа;

$\varphi(n) = (p-1)\cdot(q-1)$ — функция Эйлера для $n = p \cdot q$;

$a \bmod_m = r$ — неотрицательный остаток от деления: $a = k \cdot m + r, 0 \le r \le m-1$;

$a \equiv b (\bmod m)$ — символ сравнения (К.Ф. Гаусс): числа a, b принадлежат одному классу эквивалентности по модулю m, т.е. $a \bmod_m = b \bmod_m$;

$a = [\alpha, \beta]_{p,q}$ — представление числа a в системе счисления в остатках [3] по модулям p и q, при этом $\alpha = a \bmod_p, \beta = a \bmod_q$;

НОД(a,b) — наибольший общий делитель a и b;

$*_{\bmod_n}$ — операция умножения по модулю n: $a \left(*_{\bmod_n}\right) b = (a \cdot b) \bmod_n$

$Z_n^* = \{z \mid z \in Z_+, z < n, \text{НОД}(z,n) = 1\}$ — множество чисел, меньших и взаимно простых с n;

$Z_n = \{z \mid z \in Z_+, z < n, \}$ — расширение Z_n^* до полной системы вычетов по модулю n.

$\left\langle Z_n^*, *_{\bmod_n} \right\rangle$ — алгебраическая структура — мультипликативная группа вычетов по модулю n. Исторически эта структура также обозначается через $\mathbf{Z}_n^*$ (в жирном начертании), и далее под $\mathbf{Z}_n^*$ авторы понимают именно мультипликативную группу;

$a^{-1} (\bmod n)$ — элемент, обратный к a в группе $\mathbf{Z}_n^*$;

$\left\langle Z_n, *_{\bmod_n} \right\rangle$ — алгебраическая структура, определенная на полной системе вычетов по модулю n. Мы будем обозначать эту структуру через $\mathbf{Z}_n$, по аналогии с $\mathbf{Z}_n^*$. Заметим, что $\mathbf{Z}_n$ уже не является группой, поскольку содержит числа, кратные p и q, для которых не существует обратных элементов в Z_n. Структура $\mathbf{Z}_n$ с операцией умножения по модулю n является моноидом и содержит делители нуля.

D_n — подмножество чисел множества $Z_n \setminus \{0\}$, не входящих в группу $\mathbf{Z}_n^*$. Очевидно, что эти числа имеют вид $a = kp, k \in \{1, \ldots, q-1\}$ или $a = lq, l \in \{1, \ldots, p-1\}$ и являются делителями нуля в $\mathbf{Z}_n$. Собственно говоря, множество D_n и есть расширение множества Z_n^* до $Z_n \setminus \{0\}$.

3. Особенности моноида $\mathbf{Z}_n$ при $n = p \cdot q$

Моноид $\mathbf{Z}_n$ при $n = p \cdot q$ является основной структурой, на которой действует криптосистема RSA. В соответствии с теоремой Эйлера $\forall a \in Z_n^* \; a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, и, следовательно $a^{\varphi(n)+1} \equiv a (\mathrm{mod}\, n)$, а если $a < n$, то $a^{\varphi(n)+1} \bmod_n = a$, что и обеспечивает работоспособность RSA в том случае, если $a \in Z_n^*$. Однако основное (в смысле криптосистемы RSA) свойство расширения множества Z_n^* состоит в том, что криптосистема работает для любых чисел из Z_n.

Утверждение 1.

$$\forall a \in Z_n \; a^{\varphi(n)+1} \bmod_n = a. \tag{1}$$

Приведем доказательство этого утверждения, содержащееся в [2]:

Доказательство

Полагая $1 \le a < n$, и учитывая, что $\varphi(n) = (p-1) \cdot (q-1)$, имеем

$$a^{\varphi(n)+1} = a \cdot a^{\varphi(n)} = a \cdot a^{(p-1)\cdot(q-1)},$$

и, следовательно, применяя теорему Эйлера отдельно для числа p, получаем

$$a^{\varphi(n)+1} (\mathrm{mod}\, p) \equiv a \cdot \left(a^{(p-1)}\right)^{(q-1)} (\mathrm{mod}\, p) \equiv a \cdot 1^{(q-1)} (\mathrm{mod}\, p) \equiv a (\mathrm{mod}\, p), \tag{2}$$

аналогично, для числа q:

$$a^{\varphi(n)+1} (\mathrm{mod}\, q) \equiv a (\mathrm{mod}\, q). \tag{3}$$

В силу китайской теоремы об остатках из (2) и (3) следует, что

$$\forall a \in Z_n \;\; a^{\varphi(n)+1} \equiv a (\mathrm{mod}\, p \cdot q) \Rightarrow a^{\varphi(n)+1} \bmod_{p \cdot q} = a,$$

и, поскольку $p \cdot q = n$, то (1) доказано.

Конец доказательства.

4. Понятие псевдоединицы в расширении $\mathbf{Z}_n^*$

Отметим одну интересную особенность моноида $\mathbf{Z}_n$ с носителем $Z_n = Z_n^* \cup D_n \cup \{0\}$ при $n = p \cdot q$, т.е. для модуля криптосистемы RSA. Очевидно, что при $a \notin Z_n^*$, т.е. при $a \in D_n$ или при $a = 0$ теорема Эйлера не справедлива, следовательно, мы имеем

$$a^{\varphi(n)} \bmod_n = x.$$

Очевидно, что $x \in Z_n$, однако значение x может быть как равно нулю или единице, так и принадлежать группе $\mathbf{Z}_n^*$, или же быть элементом из множества D_n. Теорема Эйлера не отвечает на этот вопрос.

Утверждение 2.

$$\forall a \in D_n \; a^{\varphi(n)} \bmod_n = x \Rightarrow x \in D_n . \tag{4}$$

Доказательство

Докажем, что $x \neq 1$. В предположении, что $x = 1$, положим $a = kp$ и, подставляя в (4), получаем

$$(k \cdot p)^{\varphi(n)} = r \cdot p \cdot q + 1 \Rightarrow (k \cdot p)^{\varphi(n)} - r \cdot p \cdot q = 1,$$

но слева $\left((k \cdot p)^{\varphi(n)} - r \cdot p \cdot q\right) \bmod_p = 0$, в то время как справа $1 \bmod_p = 1$, следовательно $x \neq 1$. Другая возможность для $a \in D_n$ — значения $a = lq$ рассматривается аналогично.

Докажем, что $x \notin Z_n^*$. Предположим, что $a = kp$ и $x \in Z_n^*$, тогда в силу теоремы Эйлера

$$x^{\varphi(n)} \bmod_n = 1 \Rightarrow (k \cdot p)^{\varphi(n) \cdot \varphi(n)} = r \cdot p \cdot q + 1,$$

невозможность этого доказывается аналогично случаю $x = 1$, точно также проводится и доказательство для значений a вида lq.

Остаются два случая: $x = 0$ или $x \in D_n$. Случай $x = 0$ невозможен, поскольку при $a = kp$ значение $k < q$, а при $a = lq$ значение $l < p$, и, следовательно, $a^{\varphi(n)}$ не делится нацело на $n = p \cdot q$, поскольку p и q — простые нечетные числа. Следовательно $x \in D_n$.

Конец доказательства.

Таким образом, для $a \in D_n$ $a^{\varphi(n)} \bmod_n = x$, и в силу утверждения 2 значение $x \in D_n$, но с другой стороны выполняется свойство RSA: $a^{\varphi(n)+1} \bmod_n = a$, что приводит к равенству

$$(a \cdot x) \bmod_n = a, x \in D_n , \tag{5}$$

причем нас интересует значение x, порожденное условием

$$x = a^{\varphi(n)} \bmod_n . \tag{6}$$

Определение

Значения x, обладающие свойством единицы в силу (5), и порожденные соотношением (6), сами при этом не равные единице, и принадлежащие расширению группы $\mathbf{Z}_n^*$ до моноида $\mathbf{Z}_n$, мы будем называть далее *псевдоединицами* по модулю криптосистемы RSA.

Конец определения.

5. Постановка задачи

Таким образом, *объектом исследования* в настоящей статье является алгебраическая структура, состоящая из множества Z_n и операции умножения по модулю n — $\mathbf{Z}_n = \left\langle Z_n, * \bmod_n \right\rangle$. *Предметом* исследования являются псевдоединицы в структуре $\mathbf{Z}_n$.

Авторы ставят перед собой следующие задачи:

1. Определить число псевдоединиц в $\mathbf{Z}_n$.

2. Указать способ вычисления значений этих псевдоединиц.

3. Исследовать свойства псевдоединиц.

6. Исследование псевдоединиц по модулю криптосистемы RSA

Прежде всего отметим, что при $a \bmod_n = 0$ любое значение x удовлетворяет равенству (5), а значение $x = 0$ удовлетворяет и условию (6). Таким образом, $x = 0$ при $a \bmod_n = 0$ является вырожденной псевдоединицей и далее рассматриваться не будет.

Рассмотрим далее значения $x \in D_n$. Предположим, что $a = kp$ и подставим это значение в (5) при $n = p \cdot q$

$$(kp \cdot x) \bmod_{p \cdot q} = kp \quad \Rightarrow \quad kp \cdot x = m \cdot pq + kp \Rightarrow x = \frac{mq}{k} + 1, \tag{7}$$

Поскольку $x \in Z_n$, т.е. является целым, то в (7) число m должно иметь вид $m = r \cdot k$, и, следовательно, x представим в виде $x = rq + 1$, т.е.

$$x \bmod_q = 1. \tag{8}$$

Поскольку $x \in D_n$ по утверждению 2, и x не может быть кратен q в силу (8), то $x \bmod_p = 0$, поскольку числа не кратные q в D_n имеют вид $k \cdot p$. Таким образом, для $a = kp$ псевдоединица x представима в системе счисления в остатках по p и q в виде:

$$x = [0,1]_{p,q}. \tag{9}$$

Обозначим певдоединицу для значений a вида kp через 1_p. Рассуждая аналогично при $a = lq$, из D_n получаем представление псевдоединицы для элементов из D_n вида lq:

$$x = [1,0]_{p,q} \tag{10}$$

и вводим соответствующее обозначение — 1_q.

Легко видеть, что в D_n существует ровно две псевдоединицы — 1_p и 1_q.

В системе счисления в остатках для двух модулей существует красивая формула перевода в обычное представление [3]:

$$[\alpha, \beta]_{p,q} \equiv \left(p \cdot p^{-1}(\bmod q) \cdot \beta + q \cdot q^{-1}(\bmod p) \cdot \alpha\right)(\bmod p \cdot q) \tag{11}$$

Поскольку псевдоединицы имеют представление (9) и (10), т.е. $\alpha \in \{0,1\}$, $\beta \in \{0,1\}$ и

$$p \cdot p^{-1}(\bmod q) < p \cdot q, \text{ и } q \cdot q^{-1}(\bmod p) < p \cdot q,$$

то (11) эквивалентно

$$[\alpha, \beta]_{p,q} = p \cdot p^{-1}(\bmod q) \cdot \beta + q \cdot q^{-1}(\bmod p) \cdot \alpha.$$

С учетом (9) и (10) мы получили явные формулы для вычисления значений псевдоединиц:

$$1_p = [0,1]_{p,q} = p \cdot p^{-1} (\mathrm{mod}\, q),$$

$$1_q = [1,0]_{p,q} = q \cdot q^{-1} (\mathrm{mod}\, p). \qquad (12)$$

Отметим, что помимо указанных свойств, псевдоединицы обладают также свойством, характерным для обычной единицы ($1^2 = 1$):

$$(1_p)^2 \bmod_{p \cdot q} = 1_p, \quad (1_q)^2 \bmod_{p \cdot q} = 1_q,$$

так и особыми свойствами, характерными только для псевдоединиц:

$$(1_p \cdot 1_q) \bmod_{p \cdot q} = 0,$$

т.е. псевдоединицы являются делителями нуля, и

$$(1_p + 1_q) \bmod_{p \cdot q} = 1 \Rightarrow 1_p + 1_q = p \cdot q + 1,$$

последнее равенство справедливо в силу того, что и $1_p < pq$ и $1_q < pq$.

6. Числовой пример

Рассмотрим модуль RSA $n = p \cdot q$, образованный простыми числами $p = 7, q = 11$. При этом $\varphi(n) = (p-1) \cdot (q-1) = 6 \cdot 10 = 60$. Вычислим псевдоединицы для данного модуля RSA по формулам (12):

$$1_7 = [0,1]_{7,11} = 7 \cdot 7^{-1} (\mathrm{mod}\, 11) = 7 \cdot 8 = 56,$$

$$1_{11} = [1,0]_{7,11} = 11 \cdot 11^{-1} (\mathrm{mod}\, 7) = 11 \cdot 2 = 22.$$

Фрагмент расчета по формуле (1) для чисел из Z_n приведен в таблице 1. Строки, выделенные жирным начертанием соответствуют элементам из D_n, и иллюстрируют равенство (5).

Табл. 1. Псевдоединицы для модуля RSA $p = 7, q = 11$.

a	$a \bmod_7$	$a \bmod_{11}$	$a^{60} \bmod_{77}$	$a^{61} \bmod_{77}$
0	0	0	0	0
1	1	1	1	1
2	2	2	1	2
3	3	3	1	3
4	4	4	1	4
5	5	5	1	5
6	6	6	1	6
7	**0**	**7**	**56**	**7**
8	1	8	1	8
9	2	9	1	9
10	3	10	1	10
11	**4**	**0**	**22**	**11**
12	5	1	1	12
13	6	2	1	13
14	**0**	**3**	**56**	**14**
15	1	4	1	15
16	2	5	1	16

17	3	6	1	17
18	4	7	1	18
19	5	8	1	19
20	6	9	1	20
21	**0**	**10**	**56**	**21**
22	**1**	**0**	**22**	**22**
23	2	1	1	23
24	3	2	1	24

7. Заключение

Таким образом, в статье введено понятие псевдоединицы в расширении мультипликативной группы по модулю криптосистемы RSA, дано определение псевдоединицы, показано, что при модуле вида $n = p \cdot q$ имеется всего две псевдоединицы — 1_p и 1_q. Указана формула для прямого вычисления значений псевдоединц и исследованы их свойства.

Данная статья имеет теоретический характер, однако описанные в ней свойства псевдоединиц полезны в современных информационных технологиях при построении и анализе криптостойкости модифицированных схем цифровой подписи и обеспечении информационной безопасности и отказоустойчивости информационных и инфо-коммуникационных систем. В частности, псевдоединицы играют важную роль в реконструкции закодированной информации при возникновении ее искажений. Конкретные приложения полученных результатов в современных информационных и инфо-коммуникационных технологиях представляют предмет дальнейших исследований авторов.

Библиографический список

1. Манин Ю. И., Панчишкин А. А. Введение в теорию чисел. — М.: ВИНИТИ, 1990. — Т. 49. — 341 с. — (Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления».).

2. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. — М.: МЦНМО, 1999. — 960 с., 263 ил.

3. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел. Пер. с англ./ Под ред. Ю.В. Линника. Изд 2-е. — М.: Книжный дом «ЛИБРОКОМ», 2010. — 176 с.