ІНФОРМАТИКА ТА МЕТОДИКА ЇЇ ВИКЛАДАННЯ

УДК 512.624.95

Рябухо О.М., Турка Т.В.

[1] *кандидат фізико-математичних наук, доцент, КДМТУ*

[2] *кандидат фізико-математичних наук, доцент кафедри алгебри, ДВНЗ «ДДПУ»*

e-mail: ren_elena@mail.ru, tvturka@gmail.com

ЗАСТОСУВАННЯ ПЕРЕСТАНОВОЧНИХ ПОЛІНОМІВ В КРИПТОГРАФІЇ

В роботі подано огляд результатів про перестановочні многочлени, тобто про такі многочлени, для яких відповідні поліноміальні функції є перестановками множини елементів скінченного поля F_q. Побудовані приклади перестановочних многочленів, описані перспективи застосування перестановочних двучленів в криптографії.

Ключові слова: *перестановочні многочлени, скінченні поля, криптографічні протоколи.*

Вступ

В сучасному інформаційному суспільстві засоби захисту інформації та способи його зламу розвиваються постійно. Цей розвиток навряд чи буде колись завершено у зв'язку з постійним збільшенням обчислювальної можливості сучасних комп'ютерів.

Однією з основних задач, розв'язуваних в криптографії, є задача посилки повідомлення по незахищеному каналу зв'язку. Традиційний спосіб розв'язання даної задачі полягає у використанні схеми шифрування з відкритим ключем, ідея якої ґрунтується на використанні публічної функції для шифрування повідомлень, що пересилаються, та секретної функції для розшифровки повідомлень. Криптостійкість таких схем заснована на припущенні про велику обчислювальну складність задачі обернення функції шифрування без знання секрету, на основі якого дана функція була побудована.

При побудові криптографічних систем широке застосування одержали так звані перестановочні многочлени скінченних полів F_q, які індукують перестановки елементів скінченного поля F_q і, відтак, відповідають елементам симетричної группи S_q, тобто групи всіх підстановок на множині з q елементів.

Перестановочними многочленами називаються многочлени, функції яких є бієкцією над аналізованим кільцем (полем). Перспектива використання перестановочних многочленів у криптографічних схемах з відкритим ключем, як кандидатів на роль функції шифрування, є одним із головних стимулів розвитку теорії таких многочленів. Математичні елементи теорії перестановочних многочленів над скінченними полями і індукованими ними групами підстановок знаходить застосування при побудові блочних криптосистем для перестановки інформаційних блоків повідомлень, які передаються.

В даний момент у самому поширеному криптографічному протоколі RSA з відкритим ключем в якості шифруючих функцій використовуються одночлени. Використання більш складних перестановочних многочленів може підвищити криптостійкість такого протоколу. Тому задача дослідження питання про властивості перестановочних многочленів над скінченими полями, і питання можливості їх застосування в криптографії є надзвичайно важливою і актуальною.

Перестановочні многочлени над скінченними полями

Означення 1. *Многочлен $f \in F_q[x]$ називається перестановочним многочленом поля F_q, якщо відповідна йому поліноміальна функція $f : F_q \to F_q$, яка відображає елементи $c \in F_q$ в елементи $f(c) \in F_q$ є перестановкою елементів поля F_q.*

Вперше перестановочні многочлени згадуються в роботах Ерміта і Діксона [1], [2], де розглядалися прості скінченні поля.

Теорема 1. *(Критерій Ерміта). Нехай p — характеристика поля F_q. Тоді многочлен $f \in F_q[x]$ є перестановочним многочленом поля F_q тоді і тільки тоді, коли виконуються наступні дві умови:*

1) *многочлен f має рівно один корінь в F_q;*

2) *для кожного цілого t такого, що $1 \leqslant t \leqslant q-2$ і $t \not\equiv 0 (\mathrm{mod}\ p)$, результат зведення многочлена $f(x)^t$ за модулем $x^q - x$ має степінь $d \leqslant q-2$.*

Очевидно, що якщо многочлен $f \in F_q[x]$ є перестановочним многочленом поля F_q, то умова 2) теореми1. виконується і без обмеження $t \not\equiv 0 (\mathrm{mod}\ p)$. Умова ж 1) може бути замінена іншою, наприклад, як в наступній теоремі.

Теорема 2. *Нехай поле F_q має характеристику p. Тоді многочлен $f \in F_q[x]$ є перестановочним многочленом поля F_q тоді і тільки тоді, коли виконуються наступні умови:*

1) *многочлен* $f(x)^{q-1}(\mathrm{mod}\ (x^q - x))$ *має степінь* $q-1$;

2) *для довільного цілого* t, *де* $1 \leqslant t \leqslant q-2$ *і* $t \not\equiv 0(\mathrm{mod}\ p)$, *многочлен* $f(x)^t(\mathrm{mod}\ (x^q - x))$ *має степінь* $d \leqslant q-2$.

Декілька простих прикладів перестановочних многочленів можна отримати за допомогою наступних елементарних результатів. Спочатку вкажемо приклади перестановочних многочленів над будь-якими полями F_q.

Теорема 3.

1) *Кожний лінійний многочлен над полем* F_q *є перестановочним многочленом поля* F_q;

2) *одночлен* x^n *є перестрановочним многочленом поля* F_q *тоді і тільки тоді, коли* $\mathrm{НСД}(n, q-1) = 1$.

Доведення.

1) Лінійний многочлен має вид $ax + b$. За критерієм Ерміта він є перестановочним.

2) Одночлен x^n є перестановочним многочленом поля F_q тоді і тільки тоді, коли відображення $f : c \to c^n$, де $c \in F_q$ є відображення «на», а це має місце тоді і тільки тоді, коли $\mathrm{НСД}(n, q-1) = 1$. □

Теорема 4. *Нехай* F_q *— поле характеристики* p. *Тоді* p*-многочлен*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in F_q[x]$$

є перестановочним многочленом поля F_q *тоді і тільки тоді, коли многочлен* $L(x)$ *має в полі* F_q *единий корінь, рівний 0.*

Доведення. Функція $L : c \to L(c)$, де $c \in F_q$ є лінійним оператором в F_q (який розглядається як векторний простір над полем F_p). Тоді відображення L є взаємно однозначним тоді і тільки тоді, коли многочлен $L(x)$ має в полі F_q єдиний корінь, який дорівнює 0. □

Інші приклади перестановочних многочленів можна отримати, якщо скористатися тим, що множина перестановочних многочленів замкнена відносно операції композиції (тобто, якщо $f(x)$ і $g(x)$ — перестановочні многочлени поля F_q, то $f(g(x))$ також є перестановочним многочленом поля F_q.) Клас перестановочних многочленів, який одержуємо при цьому описується наступною теоремою.

Теорема 5. *Нехай* F_q *— скінченне поле,* $r \in N$, $\mathrm{НСД}(r, q-1) = 1$ *і нехай* s *— додатній дільник числа* $q-1$. *Нехай далі,* $g(x) \in F_q[x]$ *— такий*

многочлен над полем F_q, *що многочлен* $g(x^s)$ *не має ненульових коренів в полі* F_q. *Тоді многочлен* $f(x) = x^r(g(x^s))^{(q-1)/s}$ *є перестановочним многочленом поля* F_q.

Доведення. Покажемо, що многочлен задовольняє умовам теореми 1. Умова 1) виконується очевидно. Щоб довести умову 2) покладемо $t \in Z$, $1 \leqslant t \leqslant q-2$ і припустимо спочатку, що t не ділиться на s. Відмітимо, що $f(x)^t$ представляє собою суму членів, показники степенів яких мають вид $rt + ms$, де $m \in Z$ і $m \geqslant 0$. Так як НСД$(r, s) = 1$, ці показники степеня не діляться на s і, значить не діляться на $q-1$. Тоді степінь многочлена $f(x)^t (\mathrm{mod}\ (x^q - x))$ не перевищує $q-2$. Якщо t ділиться на s, наприклад $t = ks$, де $k \in N$, то

$$f(x)^t = x^{rt}(g(x^s))^{(q-1)k}$$

Якщо припустити $h(x) = x^{rt}$, то так як $g(c^s) \neq 0$ для всіх $c \in F_q$, ми отримуємо, що $f(c)^t = h(c)$; крім того, $f(0)^t = h(0)$. Тоді

$$f(x)^t \equiv x^{rt} (\mathrm{mod}\ (x^q - x))$$

і так як rt не ділиться на $q-1$, многочлен $f(x)^t (\mathrm{mod}\ (x^q - x))$ є многочленом степеня не більшого ніж $q-2$. □

Із зауваження зробленого після теореми 4, зокрема, випливає, що якщо $f \in F_q[x]$ — перестановочний многочлен поля F_q і $b, c, d \in F_q$, $c \neq 0$, то $f_1(x) = cf(x+b) + d$ також є перестановочним многочленом поля F_q. Вибираючи відповідним чином константи b, c, d можна отримати многочлен $f_1(x)$ в нормованій формі. Останнє означає, що $f_1(x)$ є нормованим многочленом і при цьому $f_1(0) = 0$, і якщо степінь n многочлена $f_1(x)$ не ділиться на характеристику поля F_q, то коефіцієнт при x^{n-1} дорівнює 0. Таким чином, можна обмежитися вивченням нормованих перестановочних многочленов. Користуючись критерієм Ерміта, можна отримати всі нормовані перестановочні многочлени довільного фіксованого степеня.

Скористаємося другим критерієм для перевірки перестановочності многочленів. Візьмемо конкретні приклади: чи є перестановочними многочлени $x^4 + 1$, $x^3 - 2x$ над полем F_3?

Для доведення скористаємося критерієм перестановочності, який був сформульований у теоремі 2.. Розглянемо степені многочленів:

$$deg((x^4+1)^2 (\mathrm{mod}\ (x^3 - x))) = deg(3x^2 + 1) = 2,$$

$$deg((x^3 - 2x)^2 (\mathrm{mod}\ (x^3 - x))) = deg(x^2) = 2,$$

Умова 1) теореми 2 виконуються.

Перевіримо другу умову: $t = 1$

$$deg((x^4 + 1)(\text{mod } (x^3 - x))) = deg(x^2 + 1) = 2,$$

$$deg((x^3 - 2x)^2(\text{mod } (x^3 - x))) = deg(-x) = 1,$$

Умова 2) виконується тільки для многочлена $x^3 - 2x$. Значить многочлен $x^3 - 2x$ над полем F_3 є перестановочним. Многочлен $x^4 + 1$ над полем F_3 — неперестановочний.

Отже, множина перестановочних многочленів F_q, степінь яких менше q, утворюють групу відносно операції композиції. Ця група ізоморфна симметричній групі S_q, тобто групі всіх перестановок на множині з q елементів.

Таким чином, симетричну групу S_q, перестановок і її підгрупи можна подати у вигляді груп перестановочних многочленів.

Одержаний результат сформулюємо:

Теорема 6. *Якщо $q > 2$, то многочлен x^{q-2} разом з лінійними многочленами над полем F_q породжує симетричну групу підстановок S_q.*

Застосування перестановочних двучленів в криптографії

В сучасних криптосистемах, а саме у самому поширеному криптографічному протоколі RSA з відкритим ключем в якості шифруючих функцій використовуються одночлени. Використання більш складних перестановочних многочленів може підвищити криптостійкість такого протоколу. На сьогодні задача дослідження питання про властивості перестановачних многочленів над скінченими полями, і питання можливості їх застосування в криптографії є надзвичайно важливою і актуальною.

Перестановочні двучлени є одними з простих за формою многочленів, але при цьому їх властивості погано вивчені. На сьогодняшний день не існує критерію, який дозволяв би будувати випадкові перестановочні двучлени, немає достатньо великих серій таких двучленів, а також відсутні точні оцінки кількості перестановочних двучленів.

В роботі [4] досліджуються перестановочні многочлени у формі $x^r h(x^{(q-1)/d})$ над скінченними полями F_q, де $d|(q-1)$, і був отриманий критерій перестановочного многочлена у такій формі. Цей критерій був згодом спрощено у роботах [6], [7] до приведеного нижче.

Теорема 7. *Нехай d, $r > 0$, $d|(q-1)$ та $h(x) \in F_q x$.*

Тоді $f(x) = x^r h(x^{(q-1)/d})$ є перестановачним многочленом в F_q тоді і тільки тоді, коли виконуються дві умови:

1) $\gcd(r, (q-1)/d) = 1$;

2) $x^r h(x^{(q-1)/d})$ *є бієкцією над* μ_d, *де* μ_d — *множина коренів степеня* d *із одиниці в скінченому полі* F_q.

У разі малих значень d, критерій теореми 1 є ефективним, так як може бути перевірений за час $O(d^2 \log\ p)$.

У роботі [4] також було доведено, що вся множина таких многочленів у скінченому полі F_q утворює групу, порядок якої приведений нижче:

$$N_{d,q} = d! \left(\frac{q-1}{d}\right)^d \phi\left(\frac{q-1}{d}\right)$$

де $\phi(n)$ — функція Ейлера.

Будь-який перестановочний двучлен $\alpha x^n + \beta x^m$, де $n < m$ можна подати у вигляді $x^n h(x^{(q-1)/d})$, де $d = \gcd(q-1,\ m-n)$ та $h(x) = \alpha + \beta x^{d(m-n)/(q-1)}$. Це значить, що теорема 1 також може бути застосована і до двучлена, і, у випадку малих значень d, така перевірка являється ефективною.

У роботі [5] доведено, що, якщо двучлен $\alpha x^n + \beta x^m$ є перестановачним над простим полем F_q, то $\gcd(m-n,\ p-1) > \sqrt{p} - 1$ і із цього слід, що $d < \sqrt{p} + 1$.

Теорема 8. *Якщо* $x^n + \alpha x^m$ — *перестановачний двучлен над простим полем* F_q, *тоді* $\gcd(m-n,\ p-1) > \sqrt{p} - 1$.

У роботі [5] висувається гіпотеза, що $d < 2 \log p$, перевірено експериментально для усіх значень p до 10000. Перераховані в данній роботі перестановочні двучлени для усіх простих скінчених полів F_q, де $p < 15000$, також узгоджуються з цією гіпотезою. У випадку виконання гіпотези, задача перевірки перестановочності для будь-якого двучлена може бути розв'язання ефективно за час $O(\log^3 p)$, якщо реалізувати критерій теореми 7.

Многочлени у формі $x^r f(x^{(q-1)/d})$ замкнуті відносно операції композиції для фіксованого d. Із цього слідує, що многочлен обернений до перестановочного многочлена у формі $x^r f(x^{(q-1)/d})$ також можна подати у такій формі, так як обернений многочлен циклічної групи, породженої даної перестановочним многочленом відносно операції композиції. На основі цього можна зробити висновок, що кількість членів у зворотному многочлені не перевищує числа d. Ефективний спосіб обчислення коефіцієнтів зворотного многочлена отриманий в роботі [8] і складність його складає $O(d^2 \log p)$.

В роботі [9] був запропонований спосіб побудови перестановочних двучленів над скінченними полями, що дає можливість побудувати модельний криптографічний протокол з використанням двучленів в якості шифруючих

функцій, аналогічний криптографічному протоколу RSA. Для перестановочних двучленів $ax^n + bx^m$ в [9] було доведено, що такий протокол буде ненадійним, тому що сам вид функції шифрування дозволяє факторизувати модуль, за яким виконується обчислення, і через це протокол стає ненадійним. Що стосується використання в якости функциї шифрування більш складних многочленів, залишається відкритим. В [10] описаний алгоритм переліку, досліджені властивості перестановочних многочленів малої довжини над простими скінченними полями, сформульовані гіпотези про класифікацію перестановочних многочленів, які містять не більше п'яти членів.

Висновки

Перестановочні многочлени над скінченними полями и кільцями Z/nZ залишаються кандидатами на застосування їх в якості функцій шифрування тому, що обчислення коефіцієнтів зворотного перестановочного многочлена є обчислювально складною задачею. Перестановочні двучлени є одними з простих за формою многочленів, але їх використання в якості функції шифрування в протоколі RSA робить його ненадійним. Можливо підійдуть для використання перестановочні трьохчлени, але для випадку сильних простих чисел клас перестановочних трьохчленів сильно обмежений. Крім того поки що не існує критерію, який дозволяв би будувати випадкові перестановочні многочлени, немає достатньо великих серій таких многочленів, а також відсутні точні оцінки кількості таких многочленів.

Література

1. *Hermite Ch.* Sur les Fonctions de Sept Lettres // C.R. Acad. Sci. Paris. 1905. P. 750–757.
2. *Dickson L. E.* The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Finite Field Permute the Elements of the Field? // The American Mathematical Monthly. 1988. Vol. 95. P. 243–246.
3. *Lidl R., Mullen G. L.* When does a polynomial over a finite field permute the elemenls of the field? — The American Mathematical Monthly. 1988, Vol. 95. P. 243–246.
4. *Wan D., Lidl R.* Permutation polynomials of the form $x^n f(x^{(q-1)/d})$ and their group structure? // Monatshefte fur Mathematik. 1991. Vol. 112 N 2. P. 149–163.
5. *Masuda A. M., Zieve M. E.* Permutation Binomials over Finite Fields // Transactions of the American Mathematical Sosiety. 2009. Vol. 361. N 8. P. 4169–4180.

6. *Akbary A., Wang Q.* On polynomials of the form $x^n f(x^{(q-1)/d})$ // Internationnal Journal of Mathematics and Mathematical Scienes. 2007. Vol. 1. 7 pp.
7. *Zieve M. E.* On some permutation polynomials over F_q of the form $x^n f(x^{(q-1)/d})$ // Proc. of the American Mathematical Sosiety. 2009. Vol. 137. N 7. P. 2209–2216.
8. *Wang Q.* On Inverse Permutation Polinomials // Finite Fields and Their Applications. 2009. Vol. 15 N 2. P. 207–213.
9. *Васильев Н. Н., Рыбалкин М. А.* Перестановачные двучлены и группы, порождение ими // Записки научных семинаров ПОМИ. 2011. № 387. С. 83–101.
10. *Рыбалкин М. А.* Перестановочные многочлены малой длины над простыми конечными полями // Информационно-управляющие системы. 2014. № 5(72). С. 103–109.
11. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. Т.1. Пер. с англ. — М.: Мир, 1988. — 430 с.

Ryabukho Olena M., Turka Tetiana V.
FSBEI HE, «Kerch State Marine Technological University», Kerch;
Donbas State Teachers' Training University, Slovians'k, Ukraine.

Application permutation polynomials in cryptography

This paper provides an overview of the results of permutation polynomials over finite fields, ie these polynomials for which corresponding polynomial functions are permutations of the set of elements of finite fields F_q. An example of permutation polynomials described prospects of permutation polynomials in cryptography.

Keywords: *permutation polynomials, finite fields, cryptographic protocols.*
