

УДК 681.3.06

Г.З. Халимов

Харьковский национальный университет радиоэлектроники, Харьков

УСЛОВИЯ СУЩЕСТВОВАНИЯ НЕТРИВИАЛЬНЫХ КРИВЫХ ГУРВИЦА

Представлены условия существования нетривиальных кривых Гурвица обобщенного вида и построения обычных кривых в конечном поле.

Ключевые слова: криптография, алгеброгеометрические методы, кривые Гурвица.

Введение

Алгебраические кривые как проективные многообразия нашли применение при решении ряда задач в кодировании и криптографии. Примерами являются традиционные исследования по эллиптическим кривым в криптографии цифровой подписи или по максимальным кривым для задач универсального хеширования и помехоустойчивого кодирования.

Кривые Гурвица имеют большую библиографию. Основные результаты представлены в работах F. Torges, среди которых можно выделить [1, 2], а также P. Carbonne, T. Neocq [3], R. Pellikan, P. Beelen [4, 5], и автора статьи [6 – 9]. Направлениями исследований являются определение параметров и условий существования кривых Гурвица.

В работе [1] введено определение обобщенных кривых Гурвица и установлен морфизм между обобщенными кривыми Гурвица и Ферма. Здесь же определены условия максимальности для обычных кривых Гурвица и обобщенных кривых при ограничении на выбор показателей степени кривой.

Связь между кривыми Гурвица и Ферма представлена P. Carbonne, T. Neocq в [3].

В работе [4] предложена техника построения кривых на основе формального полинома и определен класс кривых Гурвица, как обобщение кватрики Клейна.

В работе [5] приведены соотношения для рода кривой. Результаты исследований по максимальным кривым Гурвица, условия максимальности обобщенных кривых со снятием ограничений на показатели степени кривой представлены в [6].

Максимальная кривая Гурвица с третьим значением рода описана в [7].

В [8, 9] получены в общем виде оценки для числа точек кривых Гурвица.

Целью статьи является определение условия существования и построения нетривиальных кривых Гурвица в конечном поле.

В разделе 1 приводятся основные результаты по кривым Гурвица в конечном поле.

В разделе 2 представлены теоремы существования и построения нетривиальных кривых Гурвица.

1. Основные результаты по кривым Гурвица в конечном поле

Кривые Гурвица H_n определяются выражением

$$X^n Y + Y^n Z + XZ^n = 0 \quad (1)$$

и имеют частные производные вида:

$$\begin{aligned} F_X &= nX^{n-1}Y + Z^n; \\ F_Y &= nY^{n-1}Z + X^n; \\ F_Z &= nZ^{n-1}X + Y^n. \end{aligned} \quad (2)$$

Несингулярность кривых Гурвица над F_q определяется условиями вида [10]:

- 1) n и q должны быть взаимно простыми;
- 2) $\gcd(n^2 - n + 1, q) = 1$.

Для вычисления рода кривой Гурвица H_n используем выражение рода для кривой вида

$$X^a + X^b Y^c + Y^d = 0. \quad (3)$$

В работе [4] (замечание 4.3) доказывается, что для несингулярной модели кривой (2) справедливо

$$g \leq 1 + \frac{1}{2} \left\{ \begin{aligned} &|ac + bd - ad| - \gcd(a - b, c) - \\ &-\gcd(b, c - d) - \gcd(a, d) \end{aligned} \right\}. \quad (4)$$

Если характеристика поля F_q не делит $\gcd(a - b, c), \gcd(b, c - d), \gcd(a, d)$ и $ac + bd - ad$ тогда справедливо равенство.

В силу соотношения (4) для кривой Гурвица H_n выражение для рода имеет следующий вид

$$g = \frac{n^2 - n}{2}. \quad (5)$$

Существует обобщение кривых Гурвица $H_{n,\ell}$ которое имеет вид [1]

$$X^n Y^\ell + Y^n Z^\ell + X^\ell Z^n = 0, \quad (6)$$

где $n \geq \ell \geq 2$, $\Delta(n, \ell) = n^2 - n\ell + \ell^2 \geq 2$ и частные производные

$$\begin{aligned} F_X &= nX^{n-1}Y^\ell + \ell X^{\ell-1}Z^n; \\ F_Y &= nY^{n-1}Z^\ell + \ell X^n Y^{\ell-1}; \\ F_Z &= nZ^{n-1}X^\ell + \ell Y^n Z^{\ell-1}. \end{aligned} \quad (7)$$

Несингулярность кривых Гурвица $H_{n,\ell}$ над F_q определяется условием [1]:

$$\gcd \Delta(n, \ell), \text{char } F_q = 1. \quad (8)$$

Род кривой $H_{n,\ell}$, как следует из (4) и отмечается в [5] равен

$$g = \frac{n^2 - n\ell + \ell^2 + 2 - 3 \gcd(n, \ell)}{2}. \quad (9)$$

Следующая теорема определяет оценку числа точек кривой Гурвица в проективном пространстве P^2 для конечного поля.

Теорема 1 [9]. Пусть кривая

$$X^n Y^\ell + Y^n Z^\ell + X^\ell Z^n = 0$$

определена в P^2 над конечным полем F_q и является несингулярной. Пусть

$$\gcd(n, \ell, q-1) = c > 1$$

$$\text{и } \gcd(n^2 - n\ell + \ell^2, c(q-1)) = c^2 d,$$

тогда оценка для числа точек кривой Гурвица имеет вид

$$N = tc^2 d + 3, \quad (10)$$

где $0 \leq t \leq q-1$.

Частные результаты по кривым Гурвица представлены следствиями 1 – 3 [9].

Следствие 1. Если

$$\gcd(n^2 - n\ell + \ell^2, q-1) = 1$$

и

$$\gcd(n, \ell) = 1,$$

то число точек несингулярной кривой Гурвица $H_{n,\ell}$ будет равно

$$N = q + 2. \quad (11)$$

Следствие 2. Если

$$\gcd(n^2 - n\ell + \ell^2, q-1) = 1$$

и

$$\gcd(n, \ell) = c,$$

то число точек несингулярной кривой Гурвица $H_{n,\ell}$ будет равно

$$N = tc^2 + 3. \quad (12)$$

Следствие 3. Пусть

$$\gcd(n^2 - n\ell + \ell^2, q-1) = d$$

и

$$\gcd(n, \ell) = 1,$$

тогда число точек несингулярной кривой Гурвица $H_{n,\ell}$ будет равно

$$N = td + 3. \quad (13)$$

Справедлива следующая лемма.

Лемма 1 [9]. Пусть $n, \ell > 0$ есть целые взаимно простые числа,

$$\gcd(n, \ell) = 1$$

и

$$\Delta(n, \ell) = n^2 - n\ell + \ell^2.$$

Тогда делителями $\Delta(n, \ell)$ являются или простой делитель равный 3, или простые делители $d > 3$, или степенные делители d^e , с условием $d \equiv 1 \pmod 6$.

Кривые с числом точек $N \neq q+2$ будем называть нетривиальными.

2. Теоремы существования и построения нетривиальных кривых Гурвица

Следующая теорема определяет существование нетривиальных кривых Гурвица $H_{n,\ell}$, для случая

$$\gcd(n^2 - n\ell + \ell^2, q-1) = d$$

и

$$\gcd(n, \ell) = 1.$$

Теорема 2. Пусть задано конечное поле F_q и $n, \ell > 0$, $\gcd(n, \ell) = 1$. Нетривиальная кривая Гурвица $H_{n,\ell}$

$$X^n Y^\ell + Y^n Z^\ell + X^\ell Z^n = 0$$

существует, если

$$\gcd(n^2 - n\ell + \ell^2, q-1)$$

содержит делители $d_i^e > 3$ такие, что $d_i \equiv 1 \pmod 6$, а также делитель равный 3, где $e \geq 1$.

Доказательство. В силу следствия 3 существует нетривиальная кривая Гурвица с числом точек

$$N = t \gcd(n^2 - n\ell + \ell^2, q-1) + 3,$$

если

$$\gcd(n^2 - n\ell + \ell^2, q-1) = d > 1.$$

Как следует из леммы 4, параметр

$$\Delta(n, \ell) = n^2 - n\ell + \ell^2$$

имеет только делители d_i^e , $d_i > 3$ и $d_i \equiv 1 \pmod 6$, где $e \geq 1$ и делитель равный 3, следовательно, $q-1$ в разложении так же содержит делители этого подмножества.

Замечание 1.

1. Условия теоремы 2 определяют требования к показателям степеней нетривиальной кривой Гурвица и отмечается, что порядок поля в разложении должен иметь делители со свойством

$$d_i \equiv 1 \pmod 6$$

или равный 3.

2. Важное значение имеет решение обратной задачи, как по делителям порядка поля F_q построить все нетривиальные кривые Гурвица, то есть найти показатели $n, \ell > 0$.

Следующая теорема является новой и определяет правило построения обычных нетривиальных кривых H_n .

Теорема 3. Пусть задано конечное поле F_q . Делители порядка поля $q-1$ есть числа p_1, p_2, \dots, p_k и $p_i \equiv 1 \pmod 6$, для $\forall i$ кроме, может быть одного делителя равного 3. Степень n нетривиальной кривой Гурвица $X^n Y + Y^n Z + XZ^n = 0$ определяется выражением

$$n = n_1 P_1 + n_2 P_2 + \dots + n_k P_k \pmod{p_1 \cdot p_2 \cdot \dots \cdot p_k}; \quad (14)$$

$$P_i = b_i \prod_{\substack{s=1 \\ s \neq i}}^k p_s \equiv 1 \pmod{p_i}, \quad (15)$$

где n_1, n_2, \dots, n_k – образующие элементы мультипликативных подгрупп 6-го и 2-го порядков по модулям p_1, p_2, \dots, p_k , а b_i – целые числа.

В силу следствия 3, для существования нетривиальной кривой Гурвица H_n необходимо, чтобы

$$\gcd(n^2 - n + 1, (q-1)) = p_1 p_2 \dots p_k$$

и по теореме 2 $p_i \equiv 1 \pmod 6$ для $\forall i$, кроме, может быть одного делителя равного 3.

Как следует из леммы 1, для каждого делителя

$$p_1, p_2, \dots, p_k$$

в силу

$$\gcd(n^2 - n + 1, (q-1)) = p_1 p_2 \dots p_k,$$

является справедливым

$$n^2 - n + 1 \equiv 0 \pmod{p_i}$$

или

$$n_i^2 - n_i + 1 \equiv 0 \pmod{p_i},$$

где $n \equiv n_i \pmod{p_i}$.

Вычисления по модулям p_i приводятся к вычислениям в конечном поле F_{p_i} . Пусть α – образующий элемент поля F_{p_i} , тогда $n_i = \alpha^s$ является элементом подполя 6-го порядка $s = \frac{p_i - 1}{6}$, если $p_i \equiv 1 \pmod 6$ или 2-го порядка, если делитель равен 3 (по лемме 1).

Таким образом, для делителей p_1, p_2, \dots, p_k , можно сформировать набор образующих элементов мультипликативных подгрупп 6-го и 2-го порядков n_1, n_2, \dots, n_k , которые в свою очередь, являются ос-

татками от деления $n \equiv n_i \pmod{p_i}$. Для нахождения искомого значения n по остаткам, используем известную китайскую теорему об остатках. Таким образом, выражение для степени n кривой Гурвица удовлетворяющей условиям теоремы определяется соотношениями (14) и (15).

Доказательство теоремы является конструктивным. Следующие примеры демонстрируют её действие.

Пример 1. Пусть задано конечное поле F_q . Делители порядка поля $q-1$ есть числа $p_1 = 3, p_2 = 43$. Построить нетривиальную кривую Гурвица H_n .

Решение. Так как $p_1 = 3$, можно построить мультипликативную подгруппу 2-го порядка, с образующим элементом $n_1 = 2$. Делитель $p_2 = 43$ и $p_2 \equiv 1 \pmod 6$. Образующий элемент подгруппы 6-го порядка есть $n_2 = 7$.

Действительно,

$$n_2^3 = 7^3 \equiv -1 \pmod{43}.$$

Найдём по формуле (15) решения для параметров P_1 и P_2 , которые имеют следующий вид:

$$P_1 = b_1 p_2 = b_1 43 = 1 \cdot 43 = 43 \equiv 1 \pmod 3$$

и

$$P_2 = b_2 p_1 = b_2 3 = 29 \cdot 3 = 87 \equiv 1 \pmod{43}.$$

По формуле (14) получим значение n

$$\begin{aligned} n &= n_1 P_1 + n_2 P_2 \pmod{p_1 p_2} = \\ &= 2 \cdot 43 + 7 \cdot 87 \equiv 50 \pmod{129}. \end{aligned}$$

Кривая Гурвица

$$X^{50} Y + Y^{50} Z + XZ^{50} = 0$$

определенная над полем F_q является нетривиальной, так как

$$n^2 - n + 1 = 50^2 - 50 + 1 = 3 \cdot 19 \cdot 43$$

и

$$\gcd(n^2 - n + 1, (q-1)) = 3 \cdot 43.$$

Это решение не является единственным. Так для делителя $p_2 = 43$ существует ещё один образующий элемент подгруппы 6-го порядка, а именно, $n'_2 = 37$.

По формуле (14) имеем

$$\begin{aligned} n &= n_1 P_1 + n'_2 P_2 \pmod{p_1 p_2} = \\ &= 2 \cdot 43 + 37 \cdot 87 \equiv 80 \pmod{129}. \end{aligned}$$

Кривая Гурвица

$$X^{80} Y + Y^{80} Z + XZ^{80} = 0$$

определенная над полем F_q также является нетривиальной, и разложение для параметра

$$\Delta(n, \ell = 1)$$

имеет следующий вид

$$n^2 - n + 1 = 80^2 - 80 + 1 = 3 \cdot 7^2 \cdot 43.$$

Данный пример показывает, что по теореме 3 может быть построено столько кривых Гурвица

$$X^n Y + Y^n Z + XZ^n = 0,$$

сколько имеется образующих элементов мультипликативных подгрупп 2-го и 6-го порядков для делителей числа $q-1$. Следующее утверждение определяет это число.

Утверждение 1. Число нетривиальных кривых Гурвица

$$X^n Y + Y^n Z + XZ^n = 0$$

над полем F_q таких, что

$$\gcd(n^2 - n + 1, (q-1)) = p_1 p_2 \dots p_k$$

и

$$p_i \equiv 1 \pmod{6}$$

для всех i , кроме, может быть одного делителя равного 3 равно $N = 2^k$, если среди делителей p_i нет делителя 3 и равно $N = 2^{k-1}$, если среди делителей p_i есть делитель 3.

Доказательство очевидно.

Замечание 2.

1. Построенные в примере 1 кривые Гурвица H_n с $n = 50$ и $n = 80$ имеют одинаковое число точек (см. теорему 2, следствие 3) и разные значения рода (см. выражение (5)).

2. Может не существовать кривой Гурвица H_n для которой параметр $n^2 - n + 1$ имел бы только заданный набор делителей и не имел бы других делителей. Такие кривые Гурвица являются избыточными по роду.

Выводы

1. Определены условия существования нетривиальных кривых Гурвица обобщенного вида (теорема 2).

2. Получено решение задачи, построения обычных нетривиальных кривых Гурвица по делителям порядка поля F_q (теорема 3).

3. Представлен практический алгоритм построения обычных нетривиальных кривых Гурвица в конечном поле, который определяется из конструктивного доказательства теоремы 3 (см. также пример 1).

Список литературы

1. Torres F. Plan maximal curves / F. Torres // *Acta Arith.* – 2001. – 98(2). – P. 165-179.
2. Cossidente A. Curves of large genus covered by the Hermitian curve / A. Cossidente, G. Korchm'aros, F. Torres // *Comm. Algebra.* – 2000. – 28(10). – P. 4707-4728.
3. Carbonne P. Decomposition de la Jacobienne sur les corps finis / P. Carbonne, T. Henocq // *Bull. Polish Acad. Sci. Math.* – 1994. – 42(3). – P. 207-215.
4. Pellikan R. The Klein quartic, the Fano plan and curves representing design. In *Codes, Curves and Signals: Common Threads in Communications*, (A. Vardy Ed.) / R. Pellikan // *Kluwer Acad. Publ., Dordrecht.* – 1998. – P. 9-20.
5. Beelen P. The Newton polygon of plane curves with many rational points / P. Beelen, R. Pellikan // *Designs, Codes and Cryptography.* – 2000. – 21. – P. 41-67.
6. Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Г.З. Халимов // *Прикладная радиоэлектроника.* – Х.: ХНУРЭ, 2010. – Т. 9, вып. 3. – С. 365-369.
7. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Г.З. Халимов // *Материалы XI Международной научно-практической конференции «Информационная безопасность», Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С.144-146.*
8. Халимов Г.З. Оценка параметров кривых Гурвица для целей универсального хеширования / Г.З. Халимов // *Сб. трудов Первой международной научно-технической конференции «Компьютерные науки и технологии». – Белгород, Россия, 8-10 октября 2009. – Ч. 2. – С.118-121.*
9. Халимов Г.З. Оценка числа решений уравнения Гурвица в конечном поле / Г.З. Халимов // *Радиоэлектроника, информатика, управление.* – Запорожье: ЗНТУ, 2010. – № 2 (23). – (в ред.).
10. Hoholdt N. Algebraic geometry codes / N. Hoholdt, J.H. van Lint, R. Pellican // *In the Handbook of Coding Theory.* – Elsevier, Amsterdam, 1998. – Vol. 1. – P. 871-961 (V.S. Pless, W.C. Huffman and R.A. Brualdi Eds).

Поступила в редколлегию 26.08.2010

Рецензент: д-р техн. наук, проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники, Харьков.

УМОВИ ІСНУВАННЯ НЕТРИВІАЛЬНИХ КРИВИХ ГУРВИЦА

Г.З. Халімов

Представлено умови існування нетривіальних кривих Гурвіца узагальненого вигляду і побудови звичайних кривих в кінцевому полі.

Ключові слова: криптографія, алгеброгеометричні методи, криві Гурвіца.

TERMS OF EXISTENCE OF UNBANAL CURVES OF HURVITZ

G.Z. Khalimov

Present existence condition the unconventional Hurvitz curves generalized view and construction common curves in Galois field.

Keywords: cryptography, algebro-geometric methods, curves of Hurvitz.