

费马曲线上的有理点

徐浪, 曹炜*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 当 $i \in \{1, 2, 3\}$ 时, 给出费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0$ ($\alpha \in F_q^*$) 上 F_{q^i} -有理点 $[u, v, w]$ 的具体形式及其个数公式 N . 当 $\alpha \in F_{q^2}^*$ 时, 给出 $P^2(F_{q^2})$ 上该费马曲线有理点个数的简单公式, 并得到了这些曲线上的有理点乘积 uvw 为 F_{q^i} 上立方数的充分条件.

关键词: 费马曲线; 有限域; 射影平面; 仿射平面; 有理点

中图分类号: O156

文献标志码: A

文章编号: 1001-5132 (2015) 03-0048-05

有限域上的方程与曲线是代数及有限域的重要研究对象, 在密码学中有重要的应用价值. 在文中用 F_q 表示含有 q 个元的有限域, 其中 $q = p^r$, $r \in \mathbb{Z}^+$, p 为素数, 用 F_q^* 表示 F_q 中非零元素之集. 设 F_{q^i} ($i = 1, 2, 3$) 上费马曲线

$$C: u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0, \alpha \in F_q^*, \quad (1)$$

用 N 表示 $P^2(F_{q^i})$ 上曲线 C 的 F_{q^i} -有理点的个数. 用 CF_{q^i} 表示 F_{q^i} 上所有元素的立方之集, 即 $CF_{q^i} = \{\alpha \in F_{q^i} \mid \exists \beta \in F_{q^i}, \text{s.t. } \alpha = \beta^3\}$.

关于有限域上费马曲线的有理点个数的估计, 有一些比较经典的结论. 1935 年, Hasse 和 Davenport 得到了 $A^2(F_p)$ 上费马曲线 $x^n + y^n = a$ ($a \in F_p^*, n \geq 2, n \mid p-1$) 的 F_p -有理点个数 N 的估计: $|N - p - 1| \leq (n-1)(n-2)\sqrt{p}$. Hasse 和 Weil 给出了射影平面上定义在 F_{q^i} 上的任意光滑不可约代数曲线 C_1 的 F_{q^i} -有理点个数 N 的估计: $|N - (q^i + 1)| \leq 2gq^{i/2}$, 其中 g 为曲线 C_1 的亏格. 随着研究的深入, 上界不断缩小, 尤其针对一些比较特殊的情况, 还可以给出有理点个数的具体公式. 1992 年, Wolfmann^[1] 给出了 F_{q^2} 上费马曲线 $\alpha x^{q+1} + \beta y^{q+1} + \delta z^{q+1} = 0$ ($\alpha, \beta, \delta \in F_{q^2}^*$) 的 F_{q^2} -有理点的个数公式. 2007 年, Moisio^[2] 利用 Kloosterman 和给出 $\alpha x^{q-1} + \beta y^{q-1} + \delta z^{q-1} = 0$ ($\alpha, \beta, \delta \in F_{q^i}^*, i = 2, 3$) 的 F_{q^i} -有理点的个数公式. 2009 年, Hou 等^[3] 通过

规定迹和范数的首一不可约多项式的个数给出了 F_{q^i} ($i = 2, 3$) 上费马曲线 $x^{q-1} + \alpha y^{q-1} = \beta$ ($\alpha, \beta \in F_{q^i}^*$) 的 F_{q^i} -有理点的个数公式. 2013 年, Voloch 等^[4] 研究 $P^2(F_{q^i})$ ($i = 1, 2, 3$) 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} = 0$ 和 $P^3(F_{q^2})$ 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$, 不仅得到了漂亮的个数公式, 而且给出了有理点的具体形式及乘积的相关性质.

笔者将进一步研究当 $i = 1, 2, 3$ 时, $P^2(F_{q^i})$ 上费马曲线(1)式的有理点具体形式及个数公式, 并找到解的乘积 uvw 为立方数的充分条件.

1 预备知识

定义 1^[5] 设 $\alpha \in F_q^*$, 使得 $\alpha^r = 1$ 的最小的正整数 r 称为 α 在 F_q^* 上的乘法阶, 记为 $\text{ord}(\alpha) = \min\{r \in \mathbb{Z}^+ \mid \alpha^r = 1\}$.

定义 2^[6] 设 $f \in F_q[x]$ 是非零多项式, 假设 $f(0) \neq 0$, 使得 $f(x)$ 整除 $x^e - 1$ 的最小正整数 e 称为多项式 $f(x)$ 的阶, 记为 $\text{ord}(f) = \min\{e \in \mathbb{Z}^+ \mid f(x) \mid x^e - 1\}$. 若 $f(0) = 0$, 有 $f(x) = x^h g(x)$, 其中 $h \in \mathbb{N}$, $g \in F_q[x]$, $g(0) \neq 0$, 此时 $\text{ord}(f) = \text{ord}(g)$.

定义 3^[6] F, E 为有限域, F 有 q 个元, E 有 q^s 个元, $\forall \alpha \in E$, $\text{Tr}_{E/F}(\alpha)$, $N_{E/F}(\alpha)$ 分别为 α 从 E 到 F 上的迹与范数, 其中 $\text{Tr}_{E/F}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}}$, $N_{E/F}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{s-1}}$. 特别地, 当

收稿日期: 2014-12-21.

宁波大学学报(理工版)网址: <http://journal.lg.nbu.edu.cn/>

基金项目: 宁波市自然科学基金 (2014A610017).

第一作者: 徐浪 (1991-), 女, 湖北咸宁人, 在读硕士研究生, 主要研究方向: 数论与密码. E-mail: shuxuexulang@163.com

*通信作者: 曹炜 (1974-), 男, 湖北潜江人, 博士/副教授, 主要研究方向: 数论、有限域及其应用. E-mail: caowei@nbu.edu.cn

F 为 E 的素域时, $Tr_{E/F}(\alpha)$ 又称为绝对迹函数.

定义 4^[6] 函数 $\chi: F_q \rightarrow U$ 称为 F_q 上加法特征, 其中 U 是模为 1 的复数之集, $\chi(0)=1$, 且 $\forall \alpha, \beta \in F_q$ 满足 $\chi(\alpha+\beta)=\chi(\alpha)\chi(\beta)$. F_q 的典范加法特征为 $\chi_1(\alpha)=e^{\frac{2\pi i Tr_{F_q/F_p}(\alpha)}{p}}$, $\forall \alpha \in F_q$.

定义 5^[6] 函数 $\psi: F_q^* \rightarrow U$ 称为 F_q 上乘法特征, 其中 $\psi(1)=1$, 且 $\forall \alpha, \beta \in F_q^*$, 有 $\psi(\alpha\beta)=\psi(\alpha)\psi(\beta)$. F_q 的平方特征为 $\eta(\alpha)=(\alpha/q)$, $\forall \alpha \in F_q^*$, (α/q) 为勒让德符号, 补充定义 $\eta(0)=0$.

定义 6^[7] 设 F_q 为有限域, n 元组 $(a_1, \dots, a_n)$ 之集称为 n 维仿射平面, 其中 $a_i \in F_q$, 记 $A^n(F_q) = \{(a_1, \dots, a_n) | a_i \in F_q, i=1, 2, \dots, n\}$. 任意点 $P=(a_1, \dots, a_n) \in A^n(F_q)$, a_i 为点 P 的坐标, 点 P 称为 F_q -有理点.

定义 7^[7] 设 F_q 为有限域, 非零 $n+1$ 元组 $(a_0, a_1, \dots, a_n)$ 所在等价类之集称为 n 维射影平面, 记

$$P^n(F) = \{[a_0, a_1, \dots, a_n] | a_i \in F, i=0, 1, \dots, n\}.$$

$(a_0, a_1, \dots, a_n)$ 与 $(b_0, b_1, \dots, b_n)$ 等价 $\Leftrightarrow \exists k \in F_q^*$, s.t. $a_i = kb_i, i=0, 1, \dots, n$. a_i 为点 P 的齐次坐标, 点 P 称为 F_q -有理点.

引理 1^[3] 设 $f(x)=x^2+ax+b \in F_q[x]$, f 不可约当且仅当:

- (i) q 为奇数时, $\eta(a^2-4b)=-1$;
- (ii) q 为偶数时, $a \neq 0, Tr_{F_q/F_2}(b/a^2)=1$.

引理 2^[4] $i \in \{1, 2, 3\}$, $u, v, w \in F_{q^i}$, 若 $u^{q-1} + v^{q-1} + w^{q-1} = 0$, 则 uvw 为 F_{q^i} 上立方数.

引理 3^[4] $P^3(F_{q^2})$ 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$ 有理点形式如下:

(i) $[u_1, u_2, u_3, u_4]$, 其中 $u_i \in F_{q^2}$, 至少有一个非 0, 并且对 $\{1, 2, 3, 4\}$ 有置换 σ 使得:

$$u_{\sigma(1)}^{q-1} = -u_{\sigma(2)}^{q-1}, u_{\sigma(3)}^{q-1} = -u_{\sigma(4)}^{q-1}.$$

(ii) 当 $q \equiv 2 \pmod{3}$ 时, $[u_1, u_2, u_3, u_4]$, 其中恰有一个 u_i 为 0, 其余 3 个的 $q-1$ 次幂是不同的立方根.

(iii) 当 $q \equiv 0 \pmod{3}$ 时, $[u_1, u_2, u_3, u_4]$, 其中 $u_i \in F_q$, 并且恰有一个 u_i 为 0.

2 主要结论及其证明

定理 1 满足以下情形之一时, $CF_{q^i} = F_{q^i}$:

- (1) $q^i \equiv 2 \pmod{3}$;
- (2) $q^i \equiv 0 \pmod{3}$.

证明 当 $q^i \equiv 2 \pmod{3}$ 时, 设 $q^i - 1 = 3t + 1$, $t \in \mathbb{Z}$, 又 $\forall \alpha \in F_{q^i}^*$, $\alpha^{q^i-1} = 1$, 从而 $\alpha^{3t} \cdot \alpha = 1$, 即有 $\alpha^{3t} = \alpha^{-1}$, $\alpha^{-1} \in F_{q^i}^*$ 取遍 $F_{q^i}^*$ 中所有元, 易见 $F_{q^i}^*$ 中所有元为立方数; 当 $q^i \equiv 0 \pmod{3}$ 时, $\forall \alpha \in F_{q^i}$, $\alpha^{q^i} = \alpha$, 即有 $(\alpha^{q^i-1})^q = \alpha$, 而 $3|q$, 故 $F_{q^i}^*$ 中所有元亦为立方数.

当 $CF_{q^i} = F_{q^i}$ 时, F_{q^i} 上所有元均为立方数, 推广了引理 2, 有下面结论.

推论 1 满足以下情形之一时, $P^2(F_{q^i})$ 上费马曲线的有理点乘积为 F_{q^i} 立方数:

- (1) $q \equiv 2 \pmod{3}, i \equiv 1 \pmod{2}$;
- (2) $q \equiv 0 \pmod{3}, \forall i \in \mathbb{N}$.

定理 2 $P^2(F_{q^2})$ 上费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0 (\alpha \in F_{q^2}^*)$ 有理点形式如下:

(1) 当 $\alpha \equiv \pm 2 \pmod{p}$ 或 $e|q+1$ 时, $[cv^2, v, 1]$, 其中 $c \in F_{q^2}^*, f(v^{q-1})=0, \text{ord}(f)=e$,

$$f(x) = x^2 + \alpha x + 1 \in F_q[x];$$

(2) $[1, 0, d]$, 其中 d 满足 $d^{q-1} = -1$;

(3) 当 $\text{ord}(\alpha) | 2$ 时, $[0, 1, d_1], [d_2, 1, 0]$, 其中 d 满足 $d_i^{q-1} = -\alpha, i=1, 2$.

证明 假设 $u, v \in F_{q^2}^*$, 满足:

$$u^{q-1} + \alpha v^{q-1} + 1 = 0, \alpha \in F_{q^2}^*,$$

可得:

$$1 = ((-u)^{q-1})^{q+1} = (\alpha v^{q^2-q} + 1)(\alpha v^{q-1} + 1) = \alpha^2 + \alpha v^{q-1} + \alpha v^{1-q} + 1.$$

从而 $v^{2q-2} + \alpha v^{q-1} + 1 = 0$, 即 v^{q-1} 为 $f(x) = x^2 + \alpha x + 1 \in F_q[x]$ 在 F_{q^2} 上的解.

(i) 当 $\alpha \equiv \pm 2 \pmod{p}$ 时, $v^{q-1} = \pm 1, v \in F_{q^2}^*$;

(ii) 当 $\alpha \not\equiv \pm 2 \pmod{p}$ 时, 设 $\text{ord}(f)=e$, 则 $x^2 + \alpha x + 1 | x^e - 1$, 有 $(v^{q-1})^e = 1$, 而 $v \in F_{q^2}^*$, 故可得 $(q-1)e | q^2 - 1$, 即 $e | q+1$.

当 $v \in F_{q^2}^*$ 满足 $u^{q-1} + \alpha v^{q-1} + 1 = 0$ 时, 有 $u^{q-1} = v^{2q-2}, u = cv^2, c \in F_{q^2}^*$.

假设 $uvw = 0$, 若 $v = 0$, 则 $u^{q-1} + 1 = 0, u \in F_{q^2}^*$; 若 $w = 0$, 则 $u^{q-1} + \alpha = 0$, 而 $u \in F_{q^2}^*$, 故 $(-\alpha)^{q+1} = \alpha^{q+1} = \alpha^2 = 1$, 则有 $\text{ord}(\alpha) | 2$; 若 $u = 0$, 同理可得.

由此可得有理点的形式.

定理 3 $P^2(F_{q^2})$ 上费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0 (\alpha \in F_{q^2}^*)$ 有理点个数 N 满足:

当 $\alpha \not\equiv \pm 2 \pmod{p}$,

$$N = \begin{cases} (q-1)^2 + 3(q-1) \text{ if} \\ e | q+1, \text{ord}(2\alpha^{-1}) | 2, p=3, \\ (q-1)^2 + (q-1) \text{ if} \\ e | q+1, \text{ord}(2\alpha^{-1}) | 2, p \neq 3, \\ 2(q-1)^2 + 3(q-1) \text{ if} \\ e | q+1, \text{ord}(\alpha) | 2, p \neq 3, \\ 2(q-1)^2 + (q-1) \text{ if} \\ e | q+1, \text{ord}(\alpha), \text{ord}(2\alpha^{-1}) \neq 1, 2, \\ 3(q-1) \text{ if} \\ e \nmid q+1, \text{ord}(\alpha) | 2, \\ q-1 \text{ if} \\ e \nmid q+1, \text{ord}(\alpha) \neq 1, 2. \end{cases}$$

当 $\alpha \equiv \pm 2 \pmod{p}$ 时,

$$N = \begin{cases} (q-1)^2 + 3(q-1) \text{ if } p=3, \\ (q-1)^2 + (q-1) \text{ if } p \neq 3. \end{cases}$$

证明 考虑 $f(x) = x^2 + \alpha x + 1$ 在 F_{q^2} 上解的重数问题.

(i) 当 $p \neq 2$ 时, $f'(x) = 2x + \alpha$, $f(x)$ 有重因式 $\Leftrightarrow f'(x) | f(x) \Leftrightarrow f(-2^{-1}\alpha) = 0$. 其中 2^{-1} 为 2 的逆元, 此时有 $2^2 = \alpha^2$, 即 $\text{ord}(2\alpha^{-1}) | 2$.

(ii) 当 $p=2$ 时, $f'(x) = \alpha$, $\gcd(f(x), f'(x)) = 1$, $f(x)$ 无重因式.

结合定理 2, 我们给出以下 3 个条件:

(a) $\alpha \equiv \pm 2 \pmod{p}$ 或者 $e | q+1$;

(b) $\text{ord}(2\alpha^{-1}) | 2$;

(c) $\text{ord}(\alpha) | 2$.

(a) 成立时, 若 $\alpha \equiv \pm 2 \pmod{p}$, $f(x)$ 以 ± 1 为解, $v^{q-1} = \pm 1$, 若 $e | q+1$ 也有 $v \in F_{q^2}^*$; (b) 成立时, $f(x)$ 有重解; (c) 成立时, $d_i^{q-1} = -\alpha$, $d_i \in F_{q^2}^*$.

此时解的个数公式 N 便可得到(表 1).

表 1 有理点个数分布

分类情况	有理点个数 N
(a)和(b)成立, (c)成立	$(q-1)^2 + 3(q-1)$
(a)和(b)成立, (c)不成立	$(q-1)^2 + (q-1)$
(a)和(c)成立, (b)不成立	$2(q-1)^2 + 3(q-1)$
(a)成立, (b)和(c)不成立	$2(q-1)^2 + (q-1)$
(a)不成立, (c)成立	$3(q-1)$
(a)不成立, (c)不成立	$q-1$

注 1 当 $\alpha \equiv \pm 2 \pmod{p}$ 时, 由于 $\alpha \in F_q^*$, 则 $p \neq 2$, 且(b)成立; 当(b)和(c)都成立时, 有 $p=3$.

推论 2^[4] $P^2(F_{q^2})$ 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} = 0$ 有理点个数 N 满足:

$$N = \begin{cases} 3(q-1) \text{ if } q \equiv 1 \pmod{3}, \\ 3(q-1) + (q-1)^2 \text{ if } q \equiv 0 \pmod{3}, \\ 3(q-1) + 2(q-1)^2 \text{ if } q \equiv 2 \pmod{3}. \end{cases} \quad (2)$$

证明 在定理 3 中, 令 $\alpha=1$, 此时(c)必成立.

(i) $q \equiv 1 \pmod{3}$ 时, (a)和(b)均不成立; (ii) $q \equiv 0 \pmod{3}$ 时, $\alpha \equiv -2 \pmod{p}$, (a)和(b)成立; (iii) $q \equiv 2 \pmod{3}$ 时, $e | q+1$, (a)成立, (b)不成立. 由此可得(2)式.

推论 3 $P^2(F_{q^2})$ 上费马曲线 $u^{q-1} \pm 2v^{q-1} + w^{q-1} = 0$ 的有理点形式如下:

(1) 当 $p=2$ 时, $[1, v, w]$, 其中 $w \in F_q^*$, $v \in F_{q^2}$;

(2) 当 $\alpha=2$ 时, $[cv^2, v, 1]$, $v^{q-1} = -1$, $c \in F_q^*$; 当 $\alpha=-2$ 时, $[u, v, 1]$, $u, v \in F_q^*$;

(3) $[1, 0, d]$, 其中 $d^{q-1} = -1$;

(4) 当 $p=3$ 时, $[d_1, 1, 0]$, $[0, 1, d_2]$, 其中 $d_i^{q-1} = \mp 2, i=1, 2$.

当 $p \neq 2$ 且 $q \equiv 2 \pmod{3}$ 时, uvw 为 F_{q^2} 上立方数, 且有理点个数 N 满足:

$$N = \begin{cases} q^2(q-1) \text{ if } p=2, \\ (q-1)^2 + (q-1) \text{ if } p \neq 2, 3, \\ (q-1)^2 + 3(q-1) \text{ if } p=3. \end{cases}$$

定理 4 $P^2(F_{q^2})$ 上费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0$ ($\alpha \in F_{q^2}^*$) 有理点个数 N 满足:

$$N = \begin{cases} (q-1)^2(1 + \eta(\alpha^{2q} - 2^2\alpha^{q-1})) \text{ if } q \equiv 1(2), \\ (q-1)^2(1 + \chi_1(\alpha^{q-1} / \alpha^{2q})) \text{ if } q \equiv 0(2). \end{cases}$$

证明 假设 $u, v, w \in F_{q^2}^*$, 由定理 2 可得:

$$1 = ((-u)^{q-1})^{q+1} = (\alpha v^{q-1} + 1)^{q+1} = (\alpha v^{q-1} + 1)^q.$$

$$(\alpha v^{q-1} + 1) = \alpha^{q+1} + \alpha v^{q-1} + \alpha^q v^{q^2-q} + 1,$$

得到 $v^{2q-2} + \alpha^q v^{q-1} + \alpha^{q-1} = 0$, v^{q-1} 为 $f(x) = x^2 + \alpha^q x + \alpha^{q-1} \in F_{q^2}[x]$ 在 F_{q^2} 上的解.

由引理 1 可知: $f(x)$ 在 F_{q^2} 上有解 $\Leftrightarrow f(x)$ 在 F_{q^2} 上可约 $\Leftrightarrow$ 以下情形之一成立:

(i) q 为奇时, $\eta(\alpha^{2q} - 2^2\alpha^{q-1}) = 1, 0$, η 为 F_{q^2} 上平方特征;

(ii) q 为偶时, $\text{Tr}_{F_{q^2}/F_2}(\alpha^{q-1} / \alpha^{2q}) = 0$, 即 $\chi_1(\alpha^{q-1} / \alpha^{2q}) = 1$, χ_1 为 F_{q^2} 上典型加法特征.

下面考虑 $f(x)$ 在 F_{q^2} 上解的重数问题, $f(x)$ 无重因式 $\Leftrightarrow (f(x), f'(x)) = 1$, 而此时 $\deg f(x) = 2$, 故 $f(x)$ 有重因式 $\Leftrightarrow f'(x) | f(x)$.

(a) q 为奇数时, 若 $f(x)$ 有重因式, 则有 $f'(x) = 2x + \alpha^{q+1} | f(x)$, 即 $f(-2^{-1}\alpha^{q+1}) = 0$, 可得到 $\alpha^{q+1} = 2^2$, 此时 $\alpha^{2q} = 2^2 \alpha^{q-1}$; 若 $f(x)$ 无重因式, 则 $\alpha^{q+1} \neq 2^2$.

(b) q 为偶数时, $f'(x) = \alpha^{q+1}$, 必有 $(f(x), f'(x)) = 1$, 此时 $f(x)$ 无重因式.

由此可得个数公式.

定理 5^[4] $P^3(F_{q^3})$ 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$ 有理点个数 N 满足:

$$N = \begin{cases} 3(q-1)^4 + 3(q-1)^3 + 6(q-1) \text{ if} \\ \quad q \equiv 1 \pmod{6}, \\ 3(q-1)^4 + 3(q-1)^3 + 8(q-1)^2 + 6(q-1) \text{ if} \\ \quad q \equiv 5 \pmod{6}, \\ 3(q-1)^4 + 3(q-1)^3 + 4(q-1)^2 + 6(q-1) \text{ if} \\ \quad q \equiv 0 \pmod{3}, \\ (3q+1)(q-1)^3 + 6(q-1) \text{ if} \\ \quad q \equiv 4 \pmod{6}, \\ (3q+1)(q-1)^3 + 8(q-1)^2 + 6(q-1) \text{ if} \\ \quad q \equiv 2 \pmod{6}. \end{cases} \quad (3)$$

证明 考察

$$S = \{[u, v, w, x] \in P^3(F_{q^3}) \mid u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0\},$$

可将其分解为:

$$S_0 = \{[u, v, w] \in P^2(F_{q^3}) \mid u^{q-1} + v^{q-1} + w^{q-1} = 0\},$$

$$S_1 = \{(u, v, w) \in A^3(F_{q^3}) \mid u^{q-1} + v^{q-1} + w^{q-1} + 1 = 0\}.$$

S_0 的个数 N_0 由引理 3 可得, S_1 可按有 0, 1, 2 个坐标为 0 分为 3 种情况, 记相应个数为 N_{10} , N_{11} , N_{12} . 主要考察 N_{10} , 即 $uvw \neq 0$, 由引理 3 可知:

$$u^{q-1} = -v^{q-1}, w^{q-1} = -1, \quad (4)$$

$$u^{q-1} = -w^{q-1}, v^{q-1} = -1, \quad (5)$$

$$w^{q-1} = -v^{q-1}, u^{q-1} = -1. \quad (6)$$

记方程 (4), (5), (6) 的解集为 A_1, A_2, A_3 . 此时

$$N_{10} = |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 A_2| - |A_2 A_3| - |A_1 A_3| + |A_1 A_2 A_3|.$$

q 为奇时,

$$|A_i| = |\{(u, v, w) \mid u^{q-1} = -v^{q-1}, w^{q-1} = -1\}| =$$

$$(q-1)(q^2-1)(q-1), i=1, 2, 3,$$

$$|A_i A_j| = |\{(u, v, w) \mid u^{q-1} = -1, v^{q-1} = -1,$$

$$w^{q-1} = -1\}| = (q-1)^3, i \neq j,$$

$A_1 A_2 A_3 = \emptyset, |A_1 A_2 A_3| = 0$, 故

$$N_{10} = 3(q-1)(q^2-1) \cdot (q-1) - C_3^2 (q-1)^3 + 0 = 3q(q-1)^3.$$

q 为偶时, 同理可得: $N_{10} = (3q+1)(q-1)^3$. 而 $N = N_0 + N_{10} + N_{11} + N_{12}$, 其值分布见表 2.

表 2 有理点个数分布

q	N_0	N_0	N_{11}	N_{12}
$q \equiv 0 \pmod{3}$	$3(q-1) + (q-1)^2$	$3q(q-1)^3$	$3(q-1)^2$	$3(q-1)$
$q \equiv 1 \pmod{6}$	$3(q-1)$	$3q(q-1)^3$	0	$3(q-1)$
$q \equiv 5 \pmod{6}$	$3(q-1) + 2(q-1)^2$	$3q(q-1)^3$	$C_3^1 \cdot 2(q-1)^2$	$3(q-1)$
$q \equiv 4 \pmod{6}$	$3(q-1)$	$(3q+1)(q-1)^3$	0	$3(q-1)$
$q \equiv 2 \pmod{6}$	$3(q-1) + 2(q-1)^2(3q+1)(q-1)^3$	$C_3^1 \cdot 2(q-1)^2$	$3(q-1)$	

由此可得个数(3)式.

定理 6 $P^2(F_{q^3})$ 上费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0$ ($\alpha^3 = 1, \alpha \in F_q$) 有理点形式如下:

(1) 当 $q \equiv 1 \pmod{3}$ 时, $[u, c\beta^{-1}u^{q+1}, 1]$, 其中 $c \in F_q^*$, $T(u) = 0, u \neq 0$;

(2) 当 $q \equiv 1 \pmod{3}$ 时, $[u, c\beta^{-1}u^{-q}, 1]$, 其中 $c \in F_q^*$, 并且 $T(1/u) = 0, u \neq 0$;

(3) 当 $q \equiv 4 \pmod{6}$ 时, $[u, 0, 1], [0, 1, d_1], [d_2, 1, 0]$, 其中 $u \in F_q^*$, $d_i^{q-1} = \alpha, i=1, 2$.

其中 $T(x) = x^{q^2} + x^q + x$, $\alpha = \beta^{q-1}$.

有理点的个数 N 满足:

$$N = \begin{cases} 2q(q-1)^2 \text{ if } q \equiv 1 \pmod{6}, \\ 2q(q-1)^2 + 3(q-1) \text{ if } q \equiv 4 \pmod{6}. \end{cases}$$

证明 由 $\alpha^3 = 1, \alpha \in F_q$ 知, $q \equiv 1 \pmod{3}$, 则 $3 \mid q^2 + q + 1$, 从而 $\text{ord}(\alpha) \mid q^2 + q + 1$. $u, w \in F_{q^3}^*$ 时, $-1 = (-u^{q-1})^{q^2+q+1} = (1 + \alpha v^{q-1})^{q^2+q+1} = (1 + \alpha V)^{q^2+q+1}$, 其中 $V = v^{q-1}$. $v, w \in F_{q^3}^*$ 时, $-1 = (-\alpha v^{q-1})^{q^2+q+1} = (1 + u^{q-1})^{q^2+q+1} = (1 + U)^{q^2+q+1}$, 其中 $U = u^{q-1}$.

若 $v=0$, 则 q 为偶数, $1 + u^{q-1} = 0$, 有 $u^{q-1} = 1$, 则 $w \in F_{q^3}^*$. 若 $u=0$, 则 q 为偶数, $\alpha + w^{q-1} = 0$, $w^{q-1} = \alpha$, $\text{ord}(\alpha) \mid q^2 + q + 1$, $w \in F_{q^3}^*$. 由此可得有理点形式.

注 2 当 $\alpha \in F_{q^3}^*$, $\text{ord}(\alpha) \mid q^2 + q + 1$ 时, $\exists \beta \in F_{q^3}^*$, s.t. $\alpha = \beta^{q-1}$, 方程变为 $u^{q-1} + (\beta v)^{q-1} + w^{q-1} = 0$, 定理 6 结论仍然成立.

推论 4 $P^2(F_q)$ 上费马曲线 $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0$ ($\alpha \in F_q^*$) 有理点形式如下:

- (1) 当 $\alpha = -2$ 时, $[u, v, w]$, 其中 $u, v, w \in F_q^*$;
- (2) 当 $\alpha = -1$ 时, $[0, v, w]$, $[u, v, 0]$, $u, v, w \in F_q^*$;
- (3) 当 $p = 2$ 时, $[u, 0, w]$, 其中 $u, w \in F_q^*$.

推论 5 $P^3(F_q)$ 上费马曲线 $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$ 的有理点形式如下:

- (1) $p = 2$ 时, $[u, v, w, 1]$ 或 $[u, v, w, x]$, 其中第 2 个形式 $\{u, v, w, x\} = \{0, x_1, x_2\}$, $u, v, w, x_i \in F_q^*$, $i = 1, 2$;
- (2) $p = 3$ 时, $[u, v, w, x]$, 其中 $\{u, v, w, x\} = \{0, 1, x_1, x_2\}$, $x_i \in F_q^*$, $i = 1, 2$.

有理点的个数 N 满足:

$$N = \begin{cases} (q-1)^3 + C_4^2(q-1) & \text{if } p = 2, \\ C_4^1(q-1)^2 & \text{if } p = 3. \end{cases}$$

参考文献:

- [1] Wolfmann J. The number of solutions of certain diagonal

equations over finite fields[J]. Journal of Number Theory, 1992, 42(2):247-257.

- [2] Moisio M. On the number of rational points on some families of Fermat curves over finite fields[J]. Finite Fields and Their Applications, 2007, 13(3):546-562.
- [3] Hou X D, Sze C. On certain diagonal equations over finite fields[J]. Finite Fields and Their Applications, 2009, 15(6):633-643.
- [4] Voloch J F, Zieve M E. Rational points on some Fermat curves and surfaces over finite fields[J]. International Journal of Number Theory, 2014, 10(2):603-621.
- [5] 张禾瑞. 近世代数基础[M]. 北京: 高等教育出版社, 1978:151-174.
- [6] Lidl R, Niederreiter H. Finite fields[M]. Cambridge: Cambridge Univ Press, 1997:187-239.
- [7] Ireland K, Rosen M. A classical introduction to modern number theory[M]. New York: Springer-verlag, 1990: 138-161.

Rational Points on Fermat Curves over Finite Fields

XU Lang, CAO Wei*

(Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: We give an explicit description of F_{q^i} -rational points and the number of points in $P^2(F_{q^i})$ on the Fermat curve $u^{q-1} + \alpha v^{q-1} + w^{q-1} = 0$ ($\alpha \in F_q^*$) for $i \in \{1, 2, 3\}$. We find a simple formula of the number of rational points in $P^2(F_{q^2})$ on the Fermat curve for $\alpha \in F_{q^2}^*$. A sufficient condition is obtained for the product uvw to be a cube in F_{q^i} where $[u, v, w]$ is the points on these curves.

Key words: Fermat curves; finite fields; projective space; affine space; rational points

(责任编辑 史小丽)