第11卷 第4期
1991年11月

数学研究与评论
JOURNAL OF MATHEMATICAL
RESEARCH AND EXPOSITION

Vol.11 No.4
Nov., 1991

Golomb 猜想(C)的证实*

常彦勋

(河北师范学院数学研究所，石家庄)

Golomb[1]曾提出猜想(C)：存在正整数q_0，当$q>q_0$时，有限域$GF(q)$的任一非零元均可表为两本原元之和．令集合

$$C=\{q;\ GF(q)\text{的任一非零元均可表为两本原元之和}\},$$

本文利用Jacobi和等方法证明了Golomb猜想(C)，即

定理 当素数幂$q>2^{60}$时，$q\in C$．

设$F=GF(q)$是q元有限域，F的乘法群记为$F^*=F\setminus\{0\}$．对于$a\in F^*$，定义$s(a)=\frac{q-1}{d(d)}$，其中$d(a)$为a在F^*中的阶．全文中，e^*表示正整数e的全部相异素因子之积，$\omega(e)$表示e的不同素因子个数，规定$w(e)=2^{w(e)}$，μ表示Möbius函数，φ表示Euler函数．并定义$\theta(e)=\frac{\varphi(e)}{e}$及$\delta_a(e)=1$(若$(s(a),e)=1$)或0(否则)．

令e_1,e_2是$q-1$的正因子，考虑集合

$$N_a(e_1,e_2)=\{\xi\in F^*\setminus\{a\};\ (s(\xi),e_1)=(s(a-\xi),e_2)=1\}.$$

记$n_a(e_1,e_2)=|N_a(e_1,e_2)|$．为简便，这里的下标$a$有时省略．由$n_a(q-1,q-1)$的定义不难看出：若对任意$a\in F^*$，均有$n_a(q-1,q-1)>0$，则必有$q\in C$．

命题1 设e_1,e_2是$q-1$的正因子及任$a\in F^*$，则有

$$n_a(q-1,q-1)\geq n_a(e_1,q-1)+n_a(q-1,e_2)-n_a(e_1,e_2).$$

证明 根据定义由$N_a(e_1,q-1)\cup N_a(q-1,e_2)\subseteq N_a(e_1,e_2)$及$N_a(e_1,q-1)\cap N_a(q-1,e_2)\subseteq N_a(q-1,q-1)$，立得

$$n_a(e_1,e_2)\geq n_a(e_1,q-1)+n_a(q-1,e_2)-n_a(q-1,q-1).$$ ■

设x_1,x_2是F的乘性特征标(即F^*到单位复数乘法群的同态)，对于任$\beta\in F^*$，我们定义x_1x_2如下：$x_1x_2(\beta)=x_1(\beta)x_2(\beta)$，则$x_1x_2$是$F$的乘性特征标，容易验证，所有乘性特征标关于如上定义的二元运算构成群，并且是$q-1$阶的循环群G，记此循环群的单位元为x_0．而G中元x的阶为$\mathrm{ord}(x)$．扩充定义$x(0)=1$($x=x_0$时)或0($x\neq x_0$时)，对于Jacobi和

$$J(x_1,x_2)=\sum_{a+b=1,\,a,b\in F}x_1(a)x_2(b)$$

我们有下列结果[4]：

* 1987年6月17日收到．

$$\begin{cases} J(x_0, x_0) = q; \\ J(x, x_0) = J(x_0, x) = 0 \qquad (x \neq x_0); \\ J(x_1, x_2) = \sqrt{q} \quad (x_1, x_2, x_1 x_2 \neq x_0). \end{cases} \tag{*}$$

命题 2[3] $\delta_a(e) = \theta(e) \sum_{d \mid e} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(x) = d} x(a)$，对任意 $a \in F^*$.

对于 $a = 0$，补充规定

$$\delta_0(e) = \theta(e) \sum_{d \mid e} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(x) = d} x(0) = \theta(e).$$

由 $n_a(e_1, e_2)$ 和 $\delta_a(e)$ 的定义，立即有

$$n_a(e_1, e_2) = \sum_{\xi \in F^* \setminus \{a\}} \delta_\xi(e_1) \delta_{a-\xi}(e_2) = \sum_{\xi \in F} \delta_\xi(e_1) \delta_{a-\xi}(e_2) - \delta_a(e_1)\theta(e_2) - \delta_a(e_2)\theta(e_1).$$

其中第一大项又可由命题 2 及 (*) 式化为

$$\theta(e_1)\theta(e_2) \sum_{\substack{d_1 \mid e_1 \\ d_2 \mid e_2}} \frac{\mu(d_1)\mu(d_2)}{\varphi(d_1)\varphi(d_2)} \sum_{\substack{\mathrm{ord}(x_1) = d_1 \\ \mathrm{ord}(x_2) = d_2}} x_1 x_2(a) J(x_1, x_2)$$

$$= \theta(e_1)\theta(e_2)q + \theta(e_1)\theta(e_2) \left(\sum_{\substack{d_1 \mid e_1, d_1 > 1 \\ d_2 \mid e_2, d_2 > 1}} \frac{\mu(d_1)\mu(d_2)}{\varphi(d_1)\varphi(d_2)} \sum_{\substack{\mathrm{ord}(x_1) = d_1 \\ \mathrm{ord}(x_2) = d_2}} x_1 x_2(a) J(x_1, x_2) \right)$$

记最后中括号内的式子为 $M_a(e_1, e_2)$，我们有

命题 3 $|M_a(e_1, e_2)| \leq \sqrt{q}(w(e_1) - 1)(w(e_2) - 1)$.

证明

$$|M_a(e_1, e_2)| \leq \sum_{\substack{d_1 \mid e_1, d_1 > 1 \\ d_2 \mid e_2, d_2 > 1}} \left| \frac{\mu(d_1)\mu(d_2)}{\varphi(d_1)\varphi(d_2)} \right| \sum_{\substack{\mathrm{ord}(x_1) = d_1 \\ \mathrm{ord}(x_2) = d_2}} \left| x_1 x_2(a) J(x_1, x_2) \right|$$

$$= \sum_{\substack{d_1 \mid e_1^*, d_1 > 1 \\ d_2 \mid e_2^*, d_2 > 1}} \frac{1}{\varphi(d_1)\varphi(d_2)} \sum_{\substack{\mathrm{ord}(x_1) = d_1 \\ \mathrm{ord}(x_2) = d_2}} \sqrt{q} = \sqrt{q}(w(e_1) - 1)(w(e_2) - 1). \qquad \blacksquare$$

由命题 3 已知

$$M_a(e_1 e_2) \geq -\sqrt{q}(w(e_1) - 1)(w(e_2) - 1) \tag{1}$$

由 (1) 式，并注意到 $\delta_a(e_i) \leq 1$ $(i = 1, 2)$，于是有

$$n_a(e_1, e_2) \geq q\theta(e_1)\theta(e_2) - \theta(e_1)\theta(e_2)\sqrt{q}(w(e_1) - 1)(w(e_2) - 1) - \theta(e_1) - \theta(e_2)$$

$$= \theta(e_1)\theta(e_2)\sqrt{q}(\sqrt{q} - w(e_1)w(e_2)) + \theta(e_1)\theta(e_2)\sqrt{q}(w(e_1) + w(e_2) - 1) - \theta(e_1) - \theta(e_2) \tag{2}$$

把所有素数按大小顺序排列，令 p_i 表示第 i 个素数.

命题 4 设 $e_1, e_2 \mid (q-1)$，对任正整数 $q > 1$，都有 $3\sqrt{q-1} \geq \frac{1}{\theta(e_1)} + \frac{1}{\theta(e_2)}$.

证明 令 $s = w(q-1)$，$q_1, \cdots, q_s$ 为 $q-1$ 的全部相异素因子，$q_1 < q_2 < \cdots < q_s$. 由 $e_1, e_2 \mid (q-1)$ 及 $q_i \geq p_i \geq 2i - 1$，则有

$$\theta(e_1) \geq \theta(q-1) = \prod_{i=1}^{s}(1 - \frac{1}{q_i}) \geq \prod_{i=1}^{s}(1 - \frac{1}{p_i}) \geq \frac{1}{2}\prod_{i=2}^{s}(1 - \frac{1}{2i-1}) = \frac{1}{2}\prod_{i=1}^{s-1}\frac{2i}{2i+1}$$

类似地 $\theta(e_2) \geq \frac{1}{2}\prod_{i=1}^{s-1}\frac{2i}{2i+1}$，于是 $\frac{1}{\theta(e_1)} + \frac{1}{\theta(e_2)} \leq 4\prod_{i=1}^{s-1}\frac{2i+1}{2i}$.

另一方面，对任正整数 $q>1$，用数学归纳法容易验证 $q-1\geq\frac{16}{9}(2s-1)=\frac{16}{9}(2\omega(q-1)-1)$

于是，$3\sqrt{q-1}\geq 4\sqrt{2s-1}=4\sqrt{\prod_{i=1}^{s-1}(\frac{2i+1}{2i}\cdot\frac{2i}{2i-1})}>4\prod_{i=1}^{s-1}\frac{2i+1}{2i}\geq\frac{1}{\theta(e_1)}+\frac{1}{\theta(e_2)}$.

命题 5 当 $q\geq 4$ 时，则有

$$\sqrt{q}\theta(e_1)\theta(e_2)(w(e_1)+w(e_2)-1)\geq\theta(e_1)+\theta(e_2).$$

证明 当 $w(e_1)+w(e_2)-1\geq 3$ 时，由命题 4，

$$\sqrt{q}\,\theta(e_1)\theta(e_2)(w(e_1)+w(e_2)-1)>3\sqrt{q-1}\,\theta(e_1)\theta(e_2)\geq\theta(e_1)+\theta(e_2).$$

当 $w(e_1)+w(e_2)\leq 3$ 时，直接验证即可.

命题 6 当素数幂 $q>w^4(q-1)\geq 4$ 时，则有 $q\in C$.

证明 在(2)式中取 $e_1=e_2=q-1$，并由命题 5 得 $n_a(q-1,q-1)\geq\theta^2(q-1)\sqrt{q}(\sqrt{q}-w^2(q-1))>0$，即有 $q\in C$.

下面我们来完成定理的证明：若 $\omega(q-1)\geq 16$，可设 $\omega(q-1)=16+t$，t 为非负正整数，于是 $q>q-1\geq\prod_{i=1}^{16+t}p_i=\prod_{i=1}^{16}p_i\cdot 16^t$，而 $2^{4\omega(q-1)}=2^{64}\cdot 16^t$，因 $\prod_{i=1}^{16}p_i>3.25\times 10^{19}$，故有

$$\frac{q}{w^4(q-1)}\geq\frac{\prod_{i=1}^{16}p_i}{2^{64}}>1.76>1,$$

即 $q>w^4(q-1)$，由命题 6 可知 $q\in C$.

若 $w(q-1)\leq 15$，因 $q>2^{60}=(2^{15})^4\geq w^4(q-1)$，由命题 6 知 $q\in C$，故当 $q>2^{60}$ 时，$q\in C$.

感谢导师康庆德教授的悉心指导和关心帮助.

参 考 文 献

[1] S. W. Golomb, Algebraic construction for Costas arrays, J. Combin. Theory (Ser A), 37(1984), 13—21.

[2] S. D. Cohen, Consecutive primitive roots in a finite field, P. Amer. Math. Soc., 2:93(1985), 189—197.

[3] S. D. Cohen, Primitive roots in the quadratic extension of a finite field, J. London Math. Soc., 2: 27(1983), 221—228.

[4] K. Ireland and M. Rosen, A classcial introduction to modern number theory, Spring-Verlag, New York, Heidelberg and Berlin, 1982.

[5] D. A. Burgess, Character sums and primitive roots in finite field, Proc. London Math.Soc., 3:17(1967), 11—25.

[6] E. Vegh, Pairs of consecutive primitive roots modulo a prime, Proc. Amer. Math. Soc., 19(1968), 1169—1170.

[7] 沈中琦，关于Golomb猜想的若干结果，四川大学学报，4(1985)，22—24.

[8] 李复中，关于Golomb猜想，东北师范大学学报(自然科学版)，4(1984)，35—38.

The Verification of Golomb's Conjecture (C)

Chang Yanxun

(Research Inst. of Math., Hebei Normal College)

Abstract

S. W. Golomb proposed the conjecture (C): There exists a postiive integer q_0, such that every non-zero element in GF(q) can be written as a sum of two primitive roots if $q>q_0$, In this paper, we give a proof of Golomb's conjecture (C).