强伪素数、覆盖同余式组以及广义 bent 函数

姜宇鹏

中国科学院数学与系统科学研究院, 北京 100190

E-mail: jiangyupeng@amss.ac.cn

指导教师: 邓映蒲 中国科学院数学与系统科学研究院

收稿日期: 2014-09-25; 接受日期: 2015-01-22

国家自然科学基金 (批准号: 11071285 和 61121062) 和国家重点基础研究发展计划 (批准号: 2011CB302401) 资助项目

摘要 本文考虑三个问题: 强伪素数的计算、覆盖同余式组和广义 bent 函数. 本文的创新点包括:

- (1) 编程证明 3 825 123 056 546 413 051 是通过前 9 个素数为基的 Miller-Rabin 测试的最小合数;
- (2) 证明 Kim 的猜想, 即任意代数数域上的恰好覆盖同余式组必有模理想重复出现;
- (3) 证明两类广义 bent 函数不存在.

关键词 强伪素数 中国剩余定理 覆盖同余式组 广义 bent 函数 域下降方法

MSC (2010) 主题分类 11Y11, 11A51, 11R04

1 引言

数论是数学中最古老的分支之一. 它的很多结论简洁漂亮, 但是证明却往往需要高深的数学知识. 近几十年来, 数论在计算机科学、组合数学和编码密码学等领域得到广泛的应用, 这赋予了数论新的意义. 本文所讨论的三个问题, 其中强伪素数的计算跟素数判定密切相关, 属于计算数论的范畴; 覆盖同余式组是一个很有意思的问题, 并且有很多应用, 本文考虑其在代数数域的推广; 广义 bent 函数是 Bool 型 bent 函数的推广, 跟代数数论中绝对值问题密切相关.

本文是作者博士毕业论文 [1] 的一个简要介绍, 将省略绝大部分证明, 感兴趣的读者可以参见原博士论文及其他相关的文献.

2 强伪素数的计算

2.1 背景

本文从初等数论中一个著名定理开始.

定理 2.1 (Fermat 小定理) 若 p 是素数, 则对所有满足 $p \nmid a$ 的整数 a , 有

$$a^{p-1} \equiv 1 \pmod{p}.$$

由此, 本文可以定义伪素数.

定义 2.1 设 n 为奇合数, 如果整数 a 满足 $a^{n-1} \equiv 1 \pmod{n}$, 我们就称 n 是以 a 为基的伪素数 (pseudoprime).

例 2.1 $341 = 11 \cdot 31$ 是合数, 容易验证 $2^{340} \equiv 1 \pmod{341}$, 那么, 341 是以 2 为基的伪素数.

对于奇素数 p , 记 $p-1 = 2^s d$, 其中 d 为奇数. 当 $p \nmid a$ 时, 我们有

$$p \mid (a^{p-1} - 1) = (a^d - 1) \prod_{k=0}^{s-1} (a^{2^k d} + 1).$$

不难得到, $p \mid (a^d - 1)$ 或者 $p \mid (a^{2^k d} + 1)$ 对某个 $0 \leq k \leq s-1$ 成立.

我们有如下强伪素数的定义:

定义 2.2 设 n 为奇合数, 并且 $n-1 = 2^s d$, d 是奇数. 如果 n 满足 $a^d \equiv 1 \pmod{n}$ 或者 $a^{2^k d} \equiv -1 \pmod{n}$ 对某个 $0 \leq k \leq s-1$ 成立, 我们就称 n 是以 a 为基的强伪素数 (strong pseudoprime).

例 2.2 $2047 = 23 \cdot 89$ 是合数, 并且 $2046 = 2 \cdot 1023$, $2^{1023} \equiv 1 \pmod{2047}$, 所以, 2047 是以 2 为基的强伪素数.

上面的性质可以用来作素数判定, 就是著名的 Miller-Rabin 测试^[2]. 给定一个大奇数 n , 记 $n-1 = 2^s d$, d 是奇数. 随机选取小于 n 的整数 a , 若 $(a, n) \neq 1$, 则 (a, n) 就是 n 的一个非平凡的因子, 此时 n 是合数. 一般情形下, $(a, n) = 1$, 这时, 我们计算 a^d 以及 $a^{2^k d}$ 模 n 的剩余, 如果这个剩余不是等于相应的 ± 1 , 那么 n 就是合数; 如果是, 那么就说, n 是 (可能) 素数, 因为此时 n 可能是素数, 也可能是以 a 为基的强伪素数. Miller-Rabin 测试有两个明显的优点, 一是数学理论很简单; 二是它只用到模乘, 运行速度很快. 它是一个概率算法, 但是出错的概率是可控的. 我们有如下的结论: 所有 $\phi(n)$ 个与 n 互素的整数中, 使 n 为强伪素数的基 a 最多有 $\phi(n)/4$ 个^[3]. 如果我们每次都是随机选取 30 个 a , 那么一个合数被我们判定为 (可能) 素数的概率不超过 $2^{-60} < 10^{-18}$.

虽然 Miller-Rabin 测试的出错概率很小, 但毕竟不是确定性的. 下面这个概念的引入就可以得到一个确定性的版本.

定义 2.3 记 p_i 为第 i 个素数, 我们把最小的以 $2, 3, \dots, p_m$ 为基的强伪素数记作 ψ_m .

这个定义是有意义的, 因为我们有如下的结论: 任意给定有限个正整数, 存在无穷多个整数 n , 使得 n 是以这些正整数为基的强伪素数^[4]. 如果我们知道了 ψ_m 的具体值, 那么对于一个小于 ψ_m 的数, 只要最多 m 次 Miller-Rabin 测试就可以确定其素性, 这是非常快速的. 当 $1 \leq m \leq 8$ 时, ψ_m 的值分别由 Pomerance 等人^[5] 和 Jaeschke^[6] 计算得到

$$\begin{aligned} \psi_1 &= 2047, & \psi_2 &= 1\,373\,653, & \psi_3 &= 25\,326\,001, & \psi_4 &= 3\,215\,031\,751, \\ \psi_5 &= 2\,152\,302\,898\,747, & \psi_6 &= 3\,474\,749\,660\,383, & \psi_7 &= \psi_8 = 341\,550\,071\,728\,321. \end{aligned}$$

在一些数学软件中, 如 Magma, 素数判定的命令就用到了 Jaeschke 的结果, 当要判定的数小于 $34 \cdot 10^{13}$ 时, 就用前 7 个素数为基运行 Miller-Rabin 测试.

2.2 算法

Zhang 和 Tang^[7] 找到了一个 19 位的合数

$$Q_{11} = 3\,825\,123\,056\,546\,413\,051,$$

这是一个以前 11 个素数为基的强伪素数, 也是当时已知的最小的以前 9 个素数为基的强伪素数. 要证明 $\psi_9 = Q_{11}$, 就要证明小于 Q_{11} 的数都不是以前 9 个素数为基的强伪素数. 我们的思路是, 找出所

有不超过 Q_{11} 的以前 8 个素数为基的强伪素数, 并说明除了 Q_{11} 之外, 其他的都不是以 $p_9 = 23$ 为基的强伪素数. 当然就得到如下的结论:

定理 2.2 $\psi_9 = \psi_{10} = \psi_{11} = 3\,825\,123\,056\,546\,413\,051$.

下面简述我们的算法, 具体细节可参见文献 [1, 8]. 我们要确定 $n \leq Q_{11}$ 是不是以前 8 个素数为基的强伪素数. 首先, 我们排除了 n 有平方因子的情形, 然后, 记 $n = p_1 \cdots p_t$, 其中 $p_1 < \cdots < p_t$. 我们主要用到如下的结论^[6]:

命题 2.3 设 $n = p_1 \cdots p_t$, 其中 $p_1, \dots, p_t$ 是两两不同的素数, a 与 n 互素, 则 n 是以 a 为基的强伪素数当且仅当 n 是以 a 为基的伪素数并且

$$v(\text{ord}_{p_1}(a)) = v(\text{ord}_{p_2}(a)) = \cdots = v(\text{ord}_{p_t}(a)),$$

其中 $\text{ord}_{p_i}(a)$ 表示 a 模 p_i 的阶, $v(k)$ 表示 k 的素因子分解中 2 的幂次.

例 2.3 例如 $\psi_2 = 1373653 = 829 \cdot 1657$, 其中

$$\text{ord}_{829}(2) = 828, \quad \text{ord}_{1657}(2) = 92, \quad v(828) = v(92) = 2, \quad \text{ord}_{829}(3) = \text{ord}_{1657}(3) = 207,$$

满足上面的命题.

我们用这个命题来搜索可行的素因子, 若 n 的素因子个数为 t , 则 $p_1 < \sqrt[t]{Q_{11}}$, 那么, p_2 就要满足

$$p_1 < p_2 < \sqrt[t-1]{\frac{Q_{11}}{p_1}},$$

并且 $v(\text{ord}_{p_2}(a)) = v(\text{ord}_{p_1}(a))$ 对 $a = 2, 3, \dots, 19$ 都成立, 类似可以得到 p_3 的取值范围. 最后, 我们的算法按素因子个数分成 4 种情形: $t \geq 5$, $t = 4$, $t = 3$ 和 $t = 2$. 特别是 $t = 2$ 这种情形, 此时, $n = p_1 p_2$, 我们要按照 p_1 的大小分 3 类, 并且对 $10^6 < p_1 < 10^8$ 这种情形, 还要根据中国剩余定理分成

$$p_1 \equiv 3 \pmod{4}, \quad p_1 \equiv 5 \pmod{8}, \quad p_1 \equiv 1 \pmod{8}.$$

用中国剩余定理分类很有必要, 我们一开始没有分类, 程序运行了十几天都没有终止. 分类之后, 整个程序在个人电脑上运行的时间不到 5 天. 我们的算法不仅高效, 而且是天然并行的, 各种情形互不相关, 可以分别运行. 我们算法的结果见表 1.

容易验证, 表 1 中 8 个强伪素数中只有 Q_{11} (第 1 行) 是以 $p_9 = 23$ 为基的强伪素数, 其他的都不是. 这样就证明了定理 2.2.

表 1 不超过 Q_{11} 的强伪素数

	强伪素数	分解
$t = 3$	3 825 123 056 546 413 051	149 491·747 451·34 233 211
	230 245 660 726 188 031	214 831·787 711·1 360 591
$t = 2$	84 983 557 412 237 221	206 135 341·412 270 681
	1 134 931 906 634 489 281	753 303 361·1 506 606 721
	1 144 336 081 150 073 701	756 417 901·1 512 835 801
	1 167 748 053 436 849 501	764 116 501·1 528 233 001
	1 646 697 619 851 137 101	907 385 701·1 814 771 401
	341 550 071 728 321	10 670 053·32 010 157

2.3 展望

Zhang^[9] 给出了 $12 \leq m \leq 19$ 时 ψ_m 的上界及相关的猜想. 特别地, 他猜想

$$\begin{aligned}\psi_{12} &= N_{12} = 318\,665\,857\,834\,031\,151\,167\,461 \text{ (24 位)} \\ &= 399\,165\,290\,221 \cdot 798\,330\,580\,441,\end{aligned}$$

这是已知的最小的以前 12 个素数为基的强伪素数, 感兴趣的读者可以试着解决这个问题.

3 覆盖同余式组

覆盖同余式组是 Erdős 提出的一个概念, 它最初是定义在整数上的, 后来 Kim 研究代数数域上的覆盖同余式组.

3.1 定义与背景

定义 3.1 设 a_i 和 n_i 为整数, $\{a_i \bmod n_i\}_{i=1}^k$ 为有限个同余式, 如果每个整数至少满足其中某个同余式, 我们把 $\{a_i \bmod n_i\}_{i=1}^k$ 称为一个覆盖同余式组 (a covering system of congruences).

例 3.1 $\{0 \bmod 2, 1 \bmod 2\}$ 是一个覆盖同余式组, 就是我们熟悉的偶数和奇数. 可以验证 $\{0 \bmod 2, 0 \bmod 3, 1 \bmod 4, 1 \bmod 6, 11 \bmod 12\}$ 也是一个覆盖同余式组, 它的每一个模数都是不相同的.

1950 年, Erdős^[10] 通过覆盖同余式组给出了一个无穷奇数列, 其中每个数都不能表示成 $2^n + p$ (p 是素数) 这种形式, 这是覆盖同余式组这个概念的起源. 自那以后, 覆盖同余式组得到了广泛的研究, 除了自身有趣的性质之外, 它还与许多其他数论问题相关. 另外, Neumann^[11] 发起了一般群上陪集覆盖的研究. 著名学者孙智伟在这个方向做了大量工作, 感兴趣的读者可以参考其个人主页的综述文献 [12] 以及其他相关文献 [13, 14] 等. 最近, 覆盖同余式组中的著名问题 — 最小模数问题被 Hough^[15] 攻破. 本文考虑一类特殊的覆盖同余式组.

定义 3.2 在定义 3.1 中, 如果我们要求每一个整数恰好只满足其中一个同余式, 那么我们就称 $\{a_i \bmod n_i\}_{i=1}^k$ 为一个不相交的覆盖同余式组 (a disjoint (or an exact) covering system of congruences).

上面例子中把整数分成偶数和奇数就是最简单的不相交的覆盖同余式组. 不相交的覆盖同余式组有如下的性质:

定理 3.1 如果 $\{a_i \bmod n_i\}_{i=1}^k$ 是一个不相交的覆盖同余式组, 且记 $1 < n_1 \leq n_2 \leq \cdots \leq n_k$, 则

$$n_{k-1} = n_k.$$

证明 我们可以认为对所有 $1 \leq i \leq k$ 都有 $0 \leq a_i < n_i$, 则

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n = \sum_{i=1}^k \sum_{j=0}^{\infty} z^{a_i+jn_i} = \sum_{i=1}^k \frac{z^{a_i}}{1-z^{n_i}}.$$

若 $n_{k-1} < n_k$, 让 $|z| < 1$ 并且逼近 $e^{\frac{2\pi\sqrt{-1}}{n_k}}$, 左边趋于一个有限值, 而右边趋于无穷的, 这是一个矛盾.

定理 3.1 最早由文献 [16] 证明, 后来 Berger 等人^[17, 18] 用组合的方法推广了这个结果. 他们的结果中不止是对最大的模数, 而是对每一个模数的重复次数有一个下界的估计. 我们的结果主要是把他们的结果推广到代数数域上的覆盖同余式组. 我们先介绍代数数域上覆盖同余式组的概念.

定义 3.3 给定一个代数数域 K , 记其代数整数环为 $\mathcal{O}_K$, 对每一个 $\alpha \in \mathcal{O}_K$ 以及 $\mathcal{O}_K$ 理想 $I \neq \mathcal{O}_K$, $\alpha + I$ 表示由所有满足 $\beta \equiv \alpha \pmod{I}$ 的代数整数 β 构成的集合. 如果 $\mathcal{O}_K$ 中每一个元素必满足某一个同余式, 我们称 $\{\alpha_i + I_i\}_{i=1}^k$ 为 K 上的一个覆盖同余式组. 如果每一个代数整数恰好满足其中一个同余式, 那么我们称 $\{\alpha_i + I_i\}_{i=1}^k$ 为一个不相交的覆盖同余式组.

Kim 最早研究代数数域上的覆盖同余式组, 他猜想代数数域上的不相交覆盖同余式组也有理想重复出现, 并且他在文献 [19] 中证明了在某些二次域的不相交覆盖同余式组中, 范数最大的模理想必定重复出现. Kim 的方法类似于定理 3.1 证明中的解析方法. 该方法推广到代数数域上有两个难点: 一是代数数域中的理想不一定是主理想, 还有就是代数数域扩张次数越大该方法越复杂. 我们用 Berger 等人的方法结合中国剩余定理很好地解决了这个问题.

3.2 重复的模理想

我们首先要固定一些记号. K 是一个代数数域, $\mathcal{O}_K$ 为其代数整数环. $\{\alpha_i + I_i\}_{i=1}^k$ 是 K 上的一个不相交的覆盖同余式组. 设

$$I = \bigcap_{i=1}^k I_i,$$

并有素理想分解

$$I = \prod_{j=1}^l \mathfrak{p}_j^{r_j},$$

这里 $\mathfrak{p}_j$ 是 $\mathcal{O}_K$ 上两两不同的素理想, $r_j > 0$. 对每一个 $\mathfrak{p}_j$, 记其范数 $N(\mathfrak{p}_j) = n_j$. 根据 I 的定义, 不难有 $I_i \mid I$ 对所有 I_i 成立.

我们先给出如下定义:

定义 3.4 记 $\mathcal{I} = \{I_i \mid 1 \leq i \leq k\}$ 是一些 $\mathcal{O}_K$ 理想组成的多重集, 对一个理想 $I \in \mathcal{I}$, 如果 $\mathcal{I}$ 中所有满足 $I \mid J$ 的理想 J 都有 $I = J$, 我们称 I 为整除极大的 (division maximal).

我们的一个结果是这样的:

定理 3.2 设 $\{\alpha_i + I_i\}_{i=1}^k$ 是 K 上的一个不相交的覆盖同余式组, 如果 I_i 是整除极大的, 那么 I_i 至少重复出现 $\min\{n_j \mid \mathfrak{p}_j \mid I_i\}$ 次.

下面简述我们的证明思路. 我们知道在代数整数环 $\mathcal{O}_K$ 中有

$$N(I) = \prod_{j=1}^l n_j^{r_j}$$

个模 I 不同的剩余类. 我们考查平行多面体

$$P(n; \mathbf{b}) = \{\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathbb{Z}^n \mid 0 \leq c_i < b_i, \text{ 任意 } 1 \leq i \leq n\},$$

其中 $n, \mathbf{b}$ 与 I 密切相关, 定义如下:

$$n = \sum_{j=1}^l r_j, \quad \mathbf{b} = (\underbrace{n_1, \dots, n_1}_{r_1}, \underbrace{n_2, \dots, n_2}_{r_2}, \dots, \underbrace{n_l, \dots, n_l}_{r_l}).$$

该平行多面体包含的点数和模 I 的剩余类一样多. 我们的证明思路是, 通过中国剩余定理构造两者之间的一个双射. 由于 $I_i \mid I$, 每一个 $\alpha_i + I_i$ 可以看成是一些模 I 剩余类的并, 我们把 $\alpha_i + I_i$ 在双射下

的像称为一个胞. 一个不相交的覆盖同余式组就对应 $P(n; \mathbf{b})$ 的一个胞拆分. 最后通过考察胞拆分的性质得到定理 3.2 的结果.

定理 3.2 虽然解决了 Kim 的猜想, 并且对整除极大理想的重复次数也有一个下界, 但它的界不是最好的. 我们来看下面这个例子, 为了使表述简单, 我们用整数上的覆盖同余式组来说明.

例 3.2 $\{0 \bmod 2, 1 \bmod 8, 3 \bmod 8, 5 \bmod 8, 7 \bmod 8\}$ 是一组不相交的覆盖同余式组, 根据定理 3.2, 模数 8 最少出现 2 次, 但实际上 8 这个模数出现了 4 次.

我们的论文中有如下进一步的结果:

定理 3.3 设 $\{\alpha_i + I_i\}_{i=1}^k$ 是 $\mathcal{O}_K$ 上的一个不相交的覆盖同余式组, 不是所有的模理想 I_i 都相等, 那么每一个 I_i 至少要重复的次数为

$$\min \left\{ G \left(\frac{I_i}{I_i + I_j} \right) \mid I_j \neq I_i \right\}.$$

这里, 对一个理想 I , $G(I) = \max\{N(\mathfrak{p}^r) \mid \mathfrak{p}^r \mid I, \mathfrak{p} \text{ 是素理想}, r \geq 0\}$, 其中 $\frac{I_i}{I_i + I_j}$ 表示分式理想的除法.

对于例 3.2, 由于理想相加有 $(8) + (2) = (2)$, $G(8/2) = 4$, 由定理 3.3, 模数 8 的至少重复次数是 4 次. 关于定理 3.2 和 3.3 的详细证明, 请读者参见文献 [1, 20].

4 广义 bent 函数

4.1 定义及背景

定义 4.1 设 q 和 n 为正整数, $q \geq 2$, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, $\zeta_q = e^{2\pi\sqrt{-1}/q}$, 函数 $f: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$ 称为广义 bent 函数, 是指对每一个 $\lambda \in \mathbb{Z}_q^n$, 有

$$\left| \sum_{x \in \mathbb{Z}_q^n} \zeta_q^{f(x) - x \cdot \lambda} \right| = q^{\frac{n}{2}},$$

并称 $[n, q]$ 为广义 bent 函数 f 的类型.

bent 函数 ($q = 2$ 的情形) 最初由 Rothaus^[21] 于 1976 年提出, 并于 1985 年由 Kumar 等人^[22] 推广 ($q \geq 2$ 的情形). 作为一类有最大非线性度的函数, bent 函数在密码、编码以及组合中有重要的应用. 在密码中, bent 函数用于非线性组合器可以很好地抗击相关攻击和最佳线性逼近攻击; 在编码中, 我们需要一簇周期序列, 使得它们之间的相关值以及每一个序列的自相关值都较小, bent 函数产生的序列就有这种性质; 在组合中, Dillon^[23] 证明了 bent 函数是初等 Hadamard 差集的特征函数.

由于 bent 函数有着如此重要的作用, bent 函数得到了广泛的研究. 构造 bent 函数以及证明某些类型的 bent 函数不存在都是非常重要的课题. Rothaus^[21] 证明了当且仅当 n 是偶数时, 类型为 $[n, 2]$ 的 bent 函数存在. Kumar 等人^[22] 构造出了 n 是偶数或者 $q \not\equiv 2 \pmod{4}$ 的广义 bent 函数, 但是当 n 为奇数并且 $q \equiv 2 \pmod{4}$ 时, 还没有一例这样的广义 bent 函数被构造出来. 对某些类型, 证明了该类型的广义 bent 函数不存在.

我们考虑 n 是奇数并且 $q \equiv 2 \pmod{4}$ 这种情形, 记 $q = 2N$, N 是一个奇数. Kumar 等人^[23] 证明了, 如果存在整数 s 使得 $2^s \equiv -1 \pmod{N}$, 则对任意奇数 n , 不存在类型为 $[n, 2N]$ 的广义 bent 函数. Pei^[24] 证明了类型为 $[1, 14]$ 的广义 bent 函数不存在. Akyildiz 等人^[25] 以及 Ikeda^[26] 有一些结果, 请参见相关文献. 特别要提到, 冯克勤及其合作者在这方面有大量工作, 参见文献 [27–30].

4.2 冯克勤结果的推广

根据广义 bent 函数的定义, 如果类型为 $[n, q]$ 的广义 bent 函数存在, 则在代数整数环 $\mathbb{Z}[\zeta_q]$ 中存在绝对值等于 $q^{n/2}$ 的元素. 冯克勤等人就是通过证明这样的代数整数不存在来说明相应的广义 bent 函数不存在. 而这也正好能让我们利用域下降方法来推广他们的结果.

我们来看文献 [30] 的一个结果. 记 $q = 2N$, N 是一个奇数, 分解成两个素因子的乘积 $N = p_1 p_2$, 并且

$$(p_1, p_2) = (239, 383), (263, 463), (263, 479), (311, 359), (359, 191), (367, 383), (463, 479), (479, 271). \quad (*)$$

定理 4.1 当 $n = 1, 3, 5$ 并且 $N = p_1 p_2$, 其中 (p_1, p_2) 取 $(*)$ 中的值, 则 $\mathbb{Z}[\zeta_N]$ 中不存在绝对值等于 $(2N)^{n/2}$ 的元素, 进而不存在类型为 $[n, 2N]$ 的广义 bent 函数.

根据分圆整数的简单知识, 此时, 我们有 $\mathbb{Z}[\zeta_{2N}] = \mathbb{Z}[\zeta_N]$. 为了使表述简单, 我们在上面的定理中给出了 N 的具体值, 其实该结果对一类 N 都是成立的, 具体参见文献 [30].

我们主要用到 Schmidt 的域下降方法^[31], 该方法用来解决绝对值问题, 进而在代数组组合方面有很重要的应用. Schmidt 的结果简述如下: 如果 $X \in \mathbb{Z}[\zeta_m]$, 满足 $X\bar{X} = l$, 这里 l 和 m 都是正整数, $\bar{X}$ 表示 X 的复共轭, 那么存在 $j \in \mathbb{Z}$, 使得 $X\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,l)}]$, 其中 $F(m, l) \mid m$, 其具体定义参见文献 [31]. 由于

$$X\zeta_m^j \overline{(X\zeta_m^j)} = X\bar{X} = l,$$

这个结论说明, 如果 $\mathbb{Z}[\zeta_m]$ 里面有一个元素 X 满足 $X\bar{X} = l$, 那么在一个可能更小的代数整数环 $\mathbb{Z}[\zeta_{F(m,l)}]$ 中也存在一个元素具有相同的绝对值.

利用域下降方法, 加上代数数论的技巧, 就能推广定理 4.1 的结果. 我们的结果也是对一类 N 成立, 这里只给出一些具体的值. 详细结果可参见文献 [1, 32]. 我们的一个结果可以在素因子 p_1 上加一个任意正幂次.

定理 4.2 当 $n = 1, 3, 5$ 并且 $N = p_1^e p_2$, 其中 (p_1, p_2) 取 $(*)$ 中的值, e 为任意正整数, 则 $\mathbb{Z}[\zeta_N]$ 中不存在绝对值等于 $(2N)^{n/2}$ 的元素, 进而不存在类型为 $[n, 2N]$ 的广义 bent 函数.

我们的结果也可以在 p_2 上加一个幂次, 不过此时 n 只能等于 1.

定理 4.3 $N = p_1^e p_2^3$ 或者 $p_1^e p_2^5$, 其中 (p_1, p_2) 取 $(*)$ 中的值, e 为任意正整数, 则 $\mathbb{Z}[\zeta_N]$ 中不存在绝对值等于 $(2N)^{n/2}$ 的元素, 进而不存在类型为 $[1, 2N]$ 的广义 bent 函数.

4.3 类型 $[3, 2 \cdot 23^e]$

在本小节中, $N = 23^e$, e 为任意正整数. 由于

$$\sqrt{-23}^{3e} \cdot \frac{3 + \sqrt{-23}}{2} \in \mathbb{Z}[\zeta_N],$$

并且其绝对值等于 $(2 \cdot 23^e)^{\frac{3}{2}}$, 冯克勤的方法对这一类参数不适用. 根据广义 bent 函数的定义, 存在代数整数满足特定的绝对值只是广义 bent 函数存在的一个必要条件. 我们需要更多的性质来证明该类型的广义 bent 函数不存在. 下面只介绍 $e = 1$ 这种情形, $e > 1$ 证明过程类似.

首先, 我们利用素理想分解以及类群同态来找出所有满足绝对值条件的代数整数.

命题 4.4 若 $\alpha \in \mathbb{Z}[\zeta_{23}]$, 那么 $\alpha\bar{\alpha} \neq 46$; 进一步, 如果 $\alpha\bar{\alpha} = 46^3$, 那么 α 一定有如下的形式:

$$\alpha = \sqrt{-23}^3 \cdot \frac{3 \pm \sqrt{-23}}{2} \cdot (\pm \zeta_{23}^i).$$

由上面命题的第一部分, 我们知道不存在类型为 $[1, 23]$ 的广义 bent 函数, 这也是文献 [27] 的一个结果. 如果 f 是一个类型为 $[3, 46]$ 的广义 bent 函数, 那么对任意的 $\lambda \in \mathbb{Z}_{46}^3$, 记

$$F(\lambda) = \sum_{x \in \mathbb{Z}_{46}^3} \zeta_{46}^{f(x) - x \cdot \lambda},$$

则由上面的命题有

$$F(\lambda) = \sqrt{-23}^3 \cdot \frac{3 \pm \sqrt{-23}}{2} \cdot (\pm \zeta_{23}^i).$$

其次, 我们来找出对某些 $\lambda \in \mathbb{Z}_{46}^3$, $F(\lambda)$ 满足的一些关系. 在加法群 $\mathbb{Z}_{46}^3$ 中有 7 个元素的阶是 2, 如 $v = (23, 0, 0)$. 对任一个 2 阶元 v , 我们能证明 $F(\lambda) = \pm F(\lambda + v)$ 对任意的 $\lambda \in \mathbb{Z}_{46}^3$ 成立.

然后, 我们通过 bent 函数满足的条件来求 $\mathbb{Z}_{46}^3$ 的一些子集的势. 记

$$v_1 = (23, 0, 0), \quad v_2 = (0, 23, 0), \quad v_3 = (23, 23, 0),$$

它们满足: 如果 $\{i, j, k\}$ 是 $\{1, 2, 3\}$ 的一个置换, 那么有 $v_i + v_j = v_k$. 记

$$S = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_1)\},$$

则我们能证明

$$|S| = 4 \cdot 23^3.$$

再定义 S 的子集

$$P = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_1) = F(x + v_2)\},$$

我们证明

$$|P| = 2 \cdot 23^3.$$

进一步分拆 P , 得到子集

$$Q = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_1) = F(x + v_2) = F(x + v_3)\},$$

结合命题 4.4 的结果, 我们证明 $Q = P$, 则 $|Q| = 2 \cdot 23^3$.

最后, 我们不难发现, 如果 $x \in Q$, 那么 $x + v_1$, $x + v_2$ 和 $x + v_3$ 都属于 Q , 所以, $|Q| \equiv 0 \pmod{4}$, 这就得到矛盾了. 对 $e > 1$, 证明过程类似, 所以, 我们有下面的定理:

定理 4.5 当 $n = 1$ 和 3 时, 不存在类型为 $[n, 2 \cdot 23^e]$ 的广义 bent 函数.

4.4 小结

本节证明了两类广义 bent 函数不存在, 一类是用 Schmidt 的域下降方法结合冯克勤的结果得到; 另一类就是考虑分圆域 $K = \mathbb{Q}(\zeta_{23^e})$ 的性质, 结合 bent 函数的特性得到. 自从 Kumar 等人 [22] 于 1985 年推广了 bent 函数的定义以来, 过去了近 30 年, 数学家们还没有构造出一例类型满足 n 为奇数并且 $q \equiv 2 \pmod{4}$ 的广义 bent 函数. 人们普遍相信不存在这样的广义 bent 函数, 但是已证明的不存在的类型只占这里的一小部分, 这个问题还远远没有解决.

致谢 衷心感谢邓映蒲研究员的悉心指导以及信息安全中心的所有老师和同学.

参考文献

- 1 姜宇鹏. 数论及某些相关问题. 博士学位论文. 北京: 中国科学院大学, 2013
- 2 Rabin M O. Probabilistic algorithm for testing primality. *J Number Theory*, 1980, 12: 128–138
- 3 Koblitz N. *A Course in Number Theory and Cryptography*. 2nd ed. New York: Springer, 2000, 130–134
- 4 Alford W R, Granville A, Pomerance C. There are infinitely many Carmichael numbers. *Ann Math*, 1994, 139: 703–722
- 5 Pomerance C, Selfridge J L, Wagstaff Jr S S. The pseudoprimes to $25 \cdot 10^9$. *Math Comp*, 1980, 35: 1003–1026
- 6 Jaeschke G. On strong pseudoprimes to several bases. *Math Comp*, 1993, 61: 915–926
- 7 Zhang Z, Tang M. Finding strong pseudoprimes to several bases, II. *Math Comp*, 2003, 72: 2085–2097
- 8 Jiang Y, Deng Y. Strong pseudoprimes to the first eight prime bases. *Math Comp*, 2014, 83: 2915–2924
- 9 Zhang Z. Two kinds of strong pseudoprimes up to 10^{36} . *Math Comp*, 2007, 76: 2095–2107
- 10 Erdős P. On integers of the form $2^n + p$ and some related problems. *Summa Brasil Math*, 1950, 2: 113–123
- 11 Neumann B H. Groups covered by finitely many cosets. *Publ Math Debrecen*, 1954, 3: 227–242
- 12 Sun Z-W. Problems and results on covering systems. [Http://math.nju.edu.cn/~zwsun/Cover.pdf](http://math.nju.edu.cn/~zwsun/Cover.pdf)
- 13 Sun Z-W. On the Herzog-Schönheim conjecture for uniform covers of groups. *J Algebra*, 2004, 273: 153–175
- 14 Sun Z-W. On the range of covering functions. *J Number Theory*, 2005, 111: 190–196
- 15 Hough H. Solution of the minimum modulus problem for covering systems. *Ann Math*, 2015, 181: 361–382
- 16 Novák B, Známský Š. Disjoint covering systems. *Amer Math Monthly*, 1974, 81: 42–45
- 17 Berger M A, Felzenbaum A, Fraenkel A S. A non-analytic proof of the Newman-Známský result for disjoint covering systems. *Combinatorica*, 1986, 6: 235–243
- 18 Berger M A, Felzenbaum A, Fraenkel A S. Improvements to the Newman-Známský result for disjoint covering systems. *Acta Arith*, 1988, 50: 1–13
- 19 Kim S. Exact covering systems in quadratic number fields. *Quart J Math*, 2012, 63: 165–180
- 20 Jiang Y, Deng Y. Exact covering systems in number fields. *Quart J Math*, 2014, 65: 211–223
- 21 Rothaus O S. On “bent” functions. *J Combin Theory Ser A*, 1976, 20: 300–305
- 22 Kumar P V, Scholtz R A, Welch L R. Generalized bent functions and their properties. *J Combin Theory Ser A*, 1985, 40: 90–107
- 23 Dillon J F. Elementary Hadamard difference sets. PhD Thesis. Baltimore: University of Maryland, 1974
- 24 Pei D. On nonexistence of generalized bent functions. *Lecture Notes in Pure and Appl Math*, 1993, 141: 165–172
- 25 Akyildiz E, Güloğlu I S, İkeda M. A note of generalized bent functions. *J Pure Appl Algebra*, 1996, 106: 1–9
- 26 İkeda M. A remark on the non-existence of generalized bent functions. *Lecture Notes in Pure and Appl Math*, 1999, 204: 109–119
- 27 冯克勤. 广义 bent 函数和虚二次域理想类数. *中国科学 A 辑*, 2000, 30: 489–496
- 28 Feng K, Liu F. New results on the nonexistence of generalized bent functions. *IEEE Trans Inform Theory*, 2003, 49: 3066–3071
- 29 Feng K, Liu F. Non-existence of some generalized bent functions. *Acta Math Sin Engl Ser*, 2003, 19: 39–50
- 30 马智, 刘凤梅, 冯克勤. 关于广义 bent 函数不存在性的新结果 (II). *中国科学 A 辑*, 2002, 32: 1–9
- 31 Schmidt B. Cyclotomic integers and finite geometry. *J Amer Math Soc*, 1999, 12: 929–952
- 32 Jiang Y, Deng Y. New results on nonexistence of generalized bent functions. *Des Codes Cryptogr*, doi: 10.1007/s10623-014-9923-y, 2014

Strong pseudoprimes, covering systems of congruences and generalized bent functions

JIANG YuPeng

Abstract In this paper, we consider three problems, which are the computation of strong pseudoprimes, covering systems of congruences and generalized bent functions. Our highlights include: (1) through programming, proving that 3 825 123 056 546 413 051 is the smallest composite passing Miller-Rabin test to the first nine prime bases; (2) proving Kim’s conjecture that exact covering systems of congruences in any algebraic number field must have repeated moduli; (3) proving that two classes of generalized bent functions do not exist.

Keywords strong pseudoprime, Chinese remainder theorem, covering systems of congruences, generalized bent functions, field descent method

MSC(2010) 11Y11, 11A51, 11R04

doi: 10.1360/N012014-00196

姜宇鹏, 2008 年获清华大学理学学士学位, 2013 年获中国科学院数学与系统科学研究院理学博士学位, 2013 年 7 月起在中国科学院信息工程研究所做博士后, 主要研究方向包括计算数论、密码学.

邓映蒲研究员, 1993 年获武汉大学理学学士学位, 2002 年获北京大学理学博士学位. 现为中科院数学与系统科学研究院研究员、博士生导师. 研究方向包括代数组合论、密码学、计算数论.