Sárközy 的一个加法剩余类问题

杨仕椿[1,2],汤建钢[1]

(1. 伊犁师范学院数学与统计学院,新疆 伊宁 835000)
(2. 阿坝师范高等专科学校数学系,四川 汶川 623000)

[**摘要**] 关于 $A+B$ 以及 $A\hat{+}B$ 的性质问题,一直是数论与组合数学中的困难课题和重要问题. 本文首先指出,在一般情况下,关于 Sárközy 的一个加法剩余类猜想的答案是否定的. 其次,对于模偶数 m 的既约剩余系,利用 Cauchy-Davenport 定理,给出当 $m=2p,2^kp(k\geqslant 2)$ 时该问题的两个初步的结果,这里 p 为素数. 最后,提出一些待研究的问题和猜想.

[**关键词**] 加法,剩余类,偶数模,Sárközy 问题
[**中图分类号**]O156.1 [**文献标志码**]A [**文章编号**]1001-4616(2013)02-0010-05

A Problem on the Addition of Residue Classes by Sárközy

Yang Shichun[1,2], Tang Jiangang[1]

(1. College of Mathematics and Statistics, Yili Normal University, Yining 835000, China)
(2. Department of Mathematics, ABa Teachers College, Wenchuan 623000, China)

Abstract: The characteristic of the $A+B$ and $A\hat{+}B$, is a difficult topic in number theory and combinatorics, and plays an important and profound role. In this paper, we first noted that under normal circumstances, the answer of a problem on the addition of residue classes by Sárközy is negative. Secondly, for the mode even number m of irreducible residue system, using Cauchy-Davenport theorem, we give the problem in two preliminary results when $m=2p, 2^kp(k\geqslant 2)$, where p is a prime number. Finally, we presented some problems and conjectures to be studied.

Key words: addition, residue classes, even number modulo, Sárközy problem

设 $\mathbf{Z},\mathbf{N},\mathbf{P}$ 分别表示全体整数、正整数和素数的集合. 对于整数集合 A,定义

$$A+B=\{a+b,a\in A,b\in B\},\quad A\hat{+}B=\{a+b,a\in A,b\in B,a\neq b\}.$$

关于 $A+B$ 以及 $A\hat{+}B$ 的性质,一直是数论与组合数学中的有趣的困难课题,有许多问题和猜想至今尚未解决[1-5].

设 p 为素数,Cauchy[6] 和 Davenport[7] 首先证明了以下引理:

引理 1(Cauchy-Davenport 定理) 若 A,B 是 $\mathbf{Z}/p\mathbf{Z}$ 的任意非空子集,则 $|A+B|\geqslant\min\{p,|A|+|B|-1\}$.

后来 Pollard[8] 将 $A+B$ 两个集合的和推广为多个集合之和的情况,得出了许多深刻的结论,参见文献[9-11].

当限定 $a\neq b$ 的情况时,问题则要困难一些. 1964 年,Erdös 和 Heilbronn[12] 猜想,对任意 $A\subset\mathbf{Z}/p\mathbf{Z}$,有 $|A\hat{+}A|\geqslant\min\{p,2|A|-3\}$. 1993 年,Rodseth[13] 证明了 $|A\hat{+}B|\geqslant\min\{p,2|A|-\sqrt{4|A|+1}\}$. 1994 年,Dias da Silva 和 Hamidoune[14] 完全解决了这个猜想,他们证明了

引理 2 若 A,B 是 $\mathbf{Z}/p\mathbf{Z}$ 的任意非空子集,则 $|A\hat{+}A|\geqslant\min\{p,2|A|-3\}$.

文献[15-19]对于 Cauchy-Davenport 定理的反问题进行了研究,即当 $A+B$ 满足什么条件时,A 或者 B 必定包含算术级数. 而文献[20,21]对 Abel 群进行了类似的研究,获得了许多相应的结果,参见文献[15-23].

收稿日期:2012-10-20.
基金项目:新疆维吾尔自治区普通高等学校重点学科经费资助项目(2012ZDXK21)、四川省科技厅应用基础研究重点项目(2011JYZ032)、四川省教育厅自然科学研究项目(12ZB002)、阿坝师专重点科研基金项目.
通讯联系人:汤建钢,教授,研究方向:不确定性的数学处理,经典与非经典计算理论,范畴论及其应用. E-mail:jg-tang@163.com

若将以上问题中的素数 p 换为一般的正整数,则该问题的研究很少见于文献中[2]. 1935 年,Chowla[24] 对引理 1 将素数 p 推广为任意正整数 k,但附加了很强的条件,他证明了:

引理 3(Chowla 定理) 令 k 为正整数,若 A,B 是 $\mathbf{Z}/p\mathbf{Z}$ 的任意非空子集,$0\in B$,且对任意 $b\in B$,均有 $\gcd(b,k)=1$,则 $|A+B|\geqslant\min\{k,|A|+|B|-1\}$.

对于偶数 m,2001 年,Sárközy 提出了如下猜想(见文献[25]中的猜想 66 问题(1)):

猜想 对任意 $\varepsilon>0$,m 为正偶数,$m\to\infty$,A 为模 m 的既约剩余系的一个子集,且

$$|A|>\left(\frac{1}{2}+\varepsilon\right)\varphi(m), \tag{1}$$

则 $A+A$ 包含了模 m 的几乎所有的偶剩余类.

本文对模偶数 m 的情形进行了一定的研究. 首先我们指出,在一般情况下,以上猜想的答案是否定的,例如:

反例 设 $m=30k$,且 $\gcd(k,2\cdot3\cdot5\cdot7\cdot13\cdot17\cdot19\cdot29)=1$. 令

$$A=\{a:a\equiv1,7,13,17,19,29\pmod{30},\gcd(a,k)=1\}.$$

则

$$\frac{|A|}{\varphi(m)}=\frac{6\varphi(k)}{\varphi(30k)}=\frac{6\varphi(k)}{8\varphi(k)}=\frac{3}{4},$$

但 $A+A$ 不能包含整数 $a\equiv22\pmod{30}$,因此猜想中的系数 $\frac{1}{2}+\varepsilon$ 是不正确的.

其次,设 m 为正偶数,A 为模 m 的既约剩余系的一个子集,令 $\rho_A=\frac{|A|}{\varphi(m)}$,一个自然的问题是,当集合 A 的 ρ_A 取多大时,必然有 $A+A$ 或 $A\dot{+}A$ 包含模 m 的几乎所有的偶剩余类?

在本文中,我们研究了以上问题. 本文利用 Cauchy-Davenport 定理,给出当 $m=2p,2^kp(k\geqslant2)$ 时的两个初步的结果,这里 p 为素数. 最后,我们提出一些待研究的问题和猜想.

1 主要结果及证明

定理 1 设 p 为奇素数,$m=2p$,且 $\rho_A>\frac{1}{2}$,则 $A+A$ 包含了模 m 的所有偶剩余类.

证明 由于 $\varphi(m)=\varphi(2p)=p-1$,则 $|A|\geqslant\frac{1}{2}(p+1)$. 不妨设 $A=\{a_1,a_2,\cdots,a_{(p+1)/2}\}$,其中 $\gcd(a_i,m)=1$ 对任意 $1\leqslant i\leqslant\frac{1}{2}(p+1)$ 成立. 下面我们来证明 $A+A$ 包含了模 m 的所有偶剩余类.

取集合 $B=\{b_1,b_2,\cdots,b_{\frac{p+1}{2}}\}$,其中

$$b_i=\begin{cases}a_i, & a_i<p,\\ a_i-p, & a_i>p,\end{cases} \tag{2}$$

显然对任意 b_i,均有 $0<b_i<p$,$\gcd(b_i,m)=1$,且对 $i\neq j$,有 $b_i\neq b_j$,则 $|B|=\frac{1}{2}(p+1)$. 因此由 Cauchy-Davenport 定理可得,$|B+B|=p$,即 $B+B$ 包含了模 p 的所有剩余类,于是同余方程

$$b_i+b_j\equiv n\pmod p,0\leqslant n\leqslant p-1 \tag{3}$$

必定有解(b_i,b_j).

在方程(3)中,当 n 为偶数时,若 b_i,b_j 均为奇数,必然有 $b_i+b_j<p$,则取 $N=b_i+b_j=a_i+a_j$. 若 b_i,b_j 为一奇一偶,必然有 $b_i+b_j>p$,不妨设 b_i 为奇,b_j 为偶,于是取 $N=b_i+(b_j+p)=a_i+a_j$. 若 b_i,b_j 均为偶数,必然有 $b_i,b_j<p$,于是取 $N=(b_i+p)+(b_j+p)=a_i+a_j$. 因此,当偶数 n 满足 $0\leqslant n\leqslant p-1$ 时,方程

$$a_i+a_j\equiv n\pmod{2p} \tag{4}$$

必定有解(a_i,a_j)满足 $N\equiv n\pmod{2p}$. 在方程(3)中,当 n 为奇数时,若 b_i,b_j 均为奇数,$b_i+b_j>p$,则取 $N=n+p=b_i+b_j=a_i+a_j$. 若 b_i,b_j 为一奇一偶,必然 $b_i+b_j<p$,不妨设 b_j 为偶,于是取 $N=n+p=b_i+(b_j+p)=a_i+a_j$. 若 b_i、b_j 均为偶数,必然有 $b_i+b_j>p$,于是取 $N=n+p=(b_i+p)+(b_j+p)=a_i+a_j$. 因此,当偶数 n 满足 $p+1\leqslant n\leqslant2p-2$

时,方程(4)也必定有解(a_i,a_j)满足$N\equiv n(\mathrm{mod}\ 2p)$.

由于以上的$n,n+p$取遍了区间$[0,2p-2]$上所有的偶数,因此有$|A+A|=p$. 于是定理 1 得证.

定理 2　设p为奇素数,$m=2^rp$,其中$r\geqslant 2$,且$|A|\geqslant\frac{1}{2}(2^r-1)(p-1)+1$,则$A+A$包含了模$m$的所有偶剩余类.

证明　当$k=2$时,$m=4p$,令$A=A_1\cup A_2$,其中

$$A_1=\{a:1\leqslant n\leqslant 2p-1\},\quad A_2=\{a:2p+1\leqslant n\leqslant 4p-1\}.$$

由于$|A|\geqslant\frac{3}{2}(p-1)+1=\frac{1}{2}(3p-1)$,则存在$k$对数$(a_{1i},a_{2i})$,$1\leqslant i\leqslant k$,其中$a_{1i}\in A_1$,$a_{2i}\in A_2$,使得

$$a_{1i}\equiv a_{1i}(\mathrm{mod}\ 2p),\tag{5}$$

且$k\geqslant\frac{1}{2}(p+1)$. 否则,设$C_1=\{a_{11},\cdots,a_{1k}\}\subseteq A_1$,$C_2=\{a_{21},\cdots,a_{2k}\}\subseteq A_2$,且$a_{1j}\equiv a_{2j}(\mathrm{mod}\ 2p)$,$1\leqslant j\leqslant k$. 由于集合$\{1,3,\cdots,2p-1\}\setminus C_1$和集合$\{2p+1,2p+3,\cdots,4p-1\}\setminus C_2$中不含有满足同余式(5)的解,则

$$|\{1,3,\cdots,2p-1\}\setminus C_1|+|\{2p+1,2p+3,\cdots,4p-1\}\setminus C_2|+k\leqslant p-1,$$

则不满足(5)的a_{1i},a_{2i}最多共有$p-1-k$个. 于是当$k\leqslant\frac{1}{2}(p-1)$时,

$$|A|=|A_1|+|A_2|\leqslant 2k+(p-1-k)=p-1+k\leqslant p-1+\frac{1}{2}(p-1)=\frac{3}{2}(p-1),$$

矛盾,因此$k\geqslant\frac{1}{2}(p+1)$. 由于$|C_1|=k\geqslant\frac{1}{2}(p+1)$,则由定理 1 可得,对于模$2p$,$|C_1+C_1|=p$,则对于模$4p$,有$|C_1+C_1|\geqslant p$.

设

$$C_1+C_1=\{a_{1i}+a_{1j},a_{1k}+a_{1l},\cdots,a_{1u}+a_{1v}\},$$

其中$a_{1i}+a_{1j},a_{1k}+a_{1l},\cdots,a_{1u}+a_{1v}$模$2p$互不同余,则$a_{1i}+a_{1j}+2p,a_{1k}+a_{1l}+2p,\cdots,a_{1u}+a_{1v}+2p$模$4p$也互不同余. 由于对$1\leqslant j\leqslant k$,有$a_{1j}+2p=a_{2j}$,即$a_{1i}+a_{2j},a_{1k}+a_{2l},\cdots,a_{1u}+a_{2v}$模$4p$互不同余,因此对于模$4p$,有

$$|C_1+C_2|=|\{a:a=a_{1i}+a_{2j},a_{1i}\in C_1,a_{2j}\in C_2\}|\geqslant|C_1+C_1|\geqslant p.$$

另一方面,在模$2p$互不同余的和式$a_{1i}+a_{1j},a_{1k}+a_{1l},\cdots,a_{1u}+a_{1v}$,以及模$4p$互不同余的和式$a_{1i}+a_{2j},a_{1k}+a_{2l},\cdots,a_{1u}+a_{2v}$中,如果存在$a_{1i}+a_{1j}$与$a_{1k}+a_{2u}$,使得$a_{1i}+a_{1j}\equiv a_{1k}+a_{2u}(\mathrm{mod}\ 4p)$,则$a_{1i}+a_{1j}\equiv a_{1k}+a_{1u}+2p(\mathrm{mod}\ 4p)$,即$a_{1i}+a_{1j}\equiv a_{1k}+a_{1u}(\mathrm{mod}\ 2p)$,矛盾,因此对于模$4p$,

$$\{a_{1i}+a_{1j},a_{1k}+a_{1l},\cdots,a_{1u}+a_{1v}\}\cap\{a_{1i}+a_{2j},a_{1k}+a_{2l},\cdots,a_{1u}+a_{2v}\}=\Phi.$$

于是

$$|A+A|\geqslant|(C_1+C_1)\cup(C_1+C_2)|\geqslant|\{a_{1i}+a_{1j},a_{1k}+a_{1l},\cdots,a_{1u}+a_{1v}\}\cup\{a_{1i}+a_{2j},a_{1k}+a_{2l},\cdots,a_{1u}+a_{2v}\}|=p+p=2p.\tag{6}$$

所以,此时定理成立.

假设定理当$r=s$时成立,即若$|A|\geqslant\frac{1}{2}(2^s-1)(p-1)+1$,则有$|A+A|=2^{s-1}p$,那么当$r=s+1$时,令

$$A=A_3\cup A_4=\{a:1\leqslant n\leqslant 2^sp-1\}\cup\{a:2^sp+1\leqslant n\leqslant 2^{s+1}p-1\}.$$

同理可得,存在k对整数a_{3i},a_{4i},$1\leqslant i\leqslant k$,其中$a_{3i}\in A_3$,$a_{4i}\in A_4$,使得$a_{3i}\equiv a_{4i}(\mathrm{mod}\ 2^sp)$,且$k\geqslant\frac{1}{2}(2^s-1)(p-1)+1$.

设$C_3=\{a_{13},\cdots,a_{3k}\}\subseteq A_3$,$C_4=\{a_{41},\cdots,a_{4k}\}\subseteq A_4$,且$a_{3j}\equiv a_{4j}(\mathrm{mod}\ 2^sp)$,$1\leqslant j\leqslant k$. 于是由归纳假设可得,$|C_3+C_3|=2^{s-1}p$. 与$k=2$时的证明情形一样,类似可得,集合$C_3+C_3$中的模$2^sp$互不同余的和式,与集合$C_3+C_4$中的模$2^{s+1}p$互不同余的和式,均模$2^{s+1}p$互不同余,且它们各自有$2^{s-1}p$个,因此

$$|A+A|\geqslant|(C_3+C_3)\cup(C_3+C_4)|\geqslant 2^{s-1}p+2^{s-1}p=2^sp,\tag{7}$$

则此时定理也成立. 于是定理 2 得证.

利用定理 2 的证明,同理可得出以下一般的结论:

定理 3　设m为偶数,A是模m的既约剩余系的一个子集,且当$|A|\geqslant k$时,有$|A+A|=\frac{1}{2}m$,则当B是

模 $2m$ 的既约剩余系的一个子集,满足 $|B|\geqslant k+\varphi(m)$ 时,必定有 $|B+B|=m$.

同样,根据引理 2,以及定理 1、2 的证明,我们同理可得出关于 $A\hat{+}A$ 的类似结论.

定理 4 设 p 为奇素数,$m=2^r p$,其中 $r\geqslant 1$,且 $|A|\geqslant\frac{1}{2}(2^r-1)(p-1)+3$,则 $A\hat{+}A$ 包含了模 m 的所有偶剩余类.

2 一些问题和猜想

问题 1 设集合 A 为模 m 的既约剩余系的任意一个子集,$A+A$(或 $A\hat{+}A$)包含了模 m 的几乎所有的偶剩余类,则 ρ_A 的最小值为多少?

例 1 设 $m=60\,k$,且 $\gcd(k,2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot31\cdot37\cdot43\cdot47\cdot49\cdot53)=1$. 令

$$A=\{a:a\equiv1,7,11,13,17,19,23,31,37,43,47,49,53\pmod{60},\gcd(a,k)=1\},$$

则 $\frac{|A|}{\varphi(m)}=\frac{13}{16}$,但 $A+A$ 不能包含整数 $a\equiv52\pmod{60}$.

例 1 表明,$\rho_A>\frac{13}{16}$. 对此,我们猜想:

猜想 1 若 A 为模 m 的既约剩余系的任意一个子集,且 $\rho_A>\frac{7}{8}$,则 $A+A$ 包含了模 m 的所有偶剩余类.

另一方面,对于正整数 m,是否存在一个元素个数最少的模 m 的既约剩余系的一个子集 A,使得 $A+A$ 包含模 m 的所有剩余类? 例如,当 $m=17$ 时,令 $A=\{a:a\equiv1,2,3,6,8,9,12\pmod{17}\}$,此时 $\rho_A=\frac{7}{16}<\frac{1}{2}$,而 $A+A$ 包含了模 17 的所有剩余类. 一个使 ρ_A 更小的例子是:

例 2 令 $m=37$,取

$$A=\{a:a\equiv1,2,3,4,5,6,11,17,23,18,29,36\pmod{37}\},$$

则 $\rho_A=\frac{12}{36}=\frac{1}{3}$. 对此我们有

问题 2 设集合 A 为模 m 的既约剩余系的某一个子集,且 $A+A$(或 $A\hat{+}A$)包含了模 m 的所有剩余类,则 ρ_A 最小能取多大?

问题 3 当奇素数 p 较大时,对任意 p,是否存在模 p 的既约剩余系的一个子集 A,且 $\rho_A<\frac{1}{3}$,使得 $A+A$(或 $A\hat{+}A$)包含模 p 的所有剩余类?

根据偶数 Goidbach 猜想,当偶数 m 足够大时,取 $A=\{a:a\in P,a<m\}$,则 $A+A$ 可能包含了模 m 的几乎所有偶剩余类,由素数定理 $\pi(x)<\frac{x}{\log x}$ 可得,此时 $\rho_A=\frac{m}{\varphi(m)\log m}$,因此 ρ_A 可能小于任意给定的正数 ε. 例如,设 p 为素数,$m=2p$,则当 p 足够大时,

$$\rho_A=\frac{2p}{\varphi(2p)\log 2p}=\frac{2p}{(p-1)\log 2p}\to0.$$

于是我们猜想:

猜想 2 当偶数 m 足够大时,存在模 m 的既约剩余系的一个子集 A,且 $\rho_A<\varepsilon$,ε 为任意给定的正数,使得 $A+A$ 包含了模 m 的几乎所有偶剩余类.

致谢 作者衷心感谢审稿专家的宝贵修改意见!

[参考文献]

[1] Guy R K. Unssolved Problems in Number Theory[M]. New York:Springer Verlag,2004.

[2] Tao T,Vu V. Additive Eombinatorics[M]. Cambridge:Cambridge University Press,2006.

[3] Erdös P,Sárközy A,Sós V T. On additive properties of general sequences[J]. Discrete Math,1994,136:75-99.

[4] Tang M,Chen Y G. On additive properties of general sequences[J]. Bull Austral Math Soc,2005,71:479-485.

[5] Chen Y G, Sárközy A, Sós V T, et al. On the monotonicity properties of additive representation functions[J]. Bull Austral Math Soc, 2005, 72: 129-138.
[6] Cauchy A L. Recherches sur les nombres[J]. J Ecole Polytech, 1813, 9: 99-116.
[7] Davenport H. On the addition of residue classes[J]. J London Math Soc, 1935, 10: 30-32.
[8] Pollard J M. A generalisation of the theorem of Cauchy and Davenport[J]. J London Math Soc, 1974, 8: 460-462.
[9] Pollard J M. Addition properties of residus classes[J]. J London Math Soc, 1975, 11: 147-152.
[10] Mann H B. Addition Theorems: The Addition Theorems of Group Theory and Number Theory[M]. New York: Interscience Publ, 1965.
[11] Nathanson M. Additive Number Theory: Inverse Problems and the Geometry of Sumsets[M]. New York: Springer-Verlag, 1996.
[12] Erdös P, Heilbronn H. On the addition of residue classes mod p[J]. Acta Arith, 1964, 9: 149-159.
[13] Rodseth Øystein J. Sums of distinct residues mod p[J]. Acta Arith, 1993, 25(2): 181-184.
[14] Dias da Silva J A, Hamidoune Y O. Cyclic spaces for Grassmann derivatives and additive theory[J]. Bull London Math Soc, 1994, 26(2): 140-146.
[15] Vosper A G. The critical pairs of subsets of a group of prime order[J]. J London Math Soc, 1956, 31: 200-205.
[16] Kneser M. Ein Satz über abelsche gruppen mit anwendungen auf die geometrie der zahlen[J]. Math Z, 1955, 64: 429-434.
[17] Károlyi G. A compactness argument in the additive theory and the polynomial method[J]. Discrete Math, 2005, 302(1/3): 124-144.
[18] Hamidoune Y O, Rodseth Øystein J. An inverse theorem mod p[J]. Acta Arith, 2000, 92(3): 251-262.
[19] Hamidoune Y O, Serra O, Zémor G. On the critical pair theory in $\mathbf{Z}/p\mathbf{Z}$[J]. Acta Arith, 2006, 121(2): 99-15.
[20] Károlyi G. An inverse theorem for the restricted set addition in abelian groups[J]. J Algebra, 2005, 290(2): 557-593.
[21] Lev V F. Restricted set addition in groups. Ⅰ. The classical setting[J]. J London Math Soc, 2000, 62(1): 27-40.
[22] Bourgain J. Roth's theorem on progressions revisited[J]. J Anal Math, 2008, 104(1): 155-192.
[23] Vu V H, Wood P M. The inverse Erdös-Heilbronn problem[J]. The Electronic Journal of Combinatorics, 2009, 16(1): R100.
[24] Chowla I. A theorem on the addition of residue classes[J]. Proc Indian Acad Sci, 1935, 2: 242-243
[25] Sárközy A. Unsolved problems in number theory[J]. Periodica Math Hungar, 2001, 42: 17-35.

[责任编辑:丁 蓉]