

**CORRIGENDUM TO
THE h -CRITICAL NUMBER
OF FINITE ABELIAN GROUPS**
UNIFORM DISTRIBUTION THEORY 10 (2015), NO. 2, 93–115

BÉLA BAJNOK

ABSTRACT. We here correct two errors of our paper cited in the title: one in the statement of Theorem 5 and another in the proof of Theorem 11.

Communicated by Vsevolod Lev

The purpose of this note is to correct two errors in our paper “The h -critical number of finite abelian groups” [Unif. Distrib. Theory 10 (2015), no. 2, 93–115], one in the statement of Theorem 5 and the other in the proof of Theorem 11. We should mention that no other result of [2] is effected by these errors.

One of our results in [2] is the fact that the h -critical number

$$\chi(G, h) = \min\{m : A \subseteq G, |A| \geq m \Rightarrow hA = G\}$$

of any finite abelian group G of order n equals

$$\max\left\{\left(\left\lfloor\frac{d-2}{h}\right\rfloor+1\right)\cdot\frac{n}{d} : d \in D(n)\right\}+1,$$

where $D(n)$ denotes the set of positive divisors of n . In passing, we mentioned that the more general function

$$v_g(n, h) = \max\left\{\left(\left\lfloor\frac{d-1-\gcd(d, g)}{h}\right\rfloor+1\right)\cdot\frac{n}{d} : d \in D(n)\right\},$$

defined for any integer $1 \leq g \leq h$, plays a role elsewhere in additive combinatorics as well. For example, in [1] we proved that $v_{k-l}(n, k+l)$ provides a tight lower bound for the maximum size of a (k, l) -sum-free set in the cyclic group of order n .

2010 Mathematics Subject Classification: Primary 11B75; Secondary 05D99, 11B25, 11P70, 20K01.

Keywords: critical number, abelian groups, sumsets, restricted sumsets.

As an aside, in Theorem 5 of [2] we presented an alternate expression for $v_g(n, h)$; unfortunately, this expression was stated incorrectly due to an error in the proof (the last equality in line 19 on page 103 is incorrect). Here we provide the correct expression and use our original Claims 1, 2, and 3 (whose proofs are correct and thus are not repeated here) to establish the result.

THEOREM 5. *Suppose that n , h , and g are positive integers and that $1 \leq g \leq h$. For $i = 2, 3, \dots, h - 1$, let*

$$D_i(n) = \{d \in D(n) : d \equiv i \pmod{h} \text{ and } \gcd(d, g) < i\}.$$

We let I denote those values of $i = 2, 3, \dots, h - 1$ for which $D_i(n) \neq \emptyset$, and for each $i \in I$, we let d_i be the smallest element of $D_i(n)$.

Then, the value of $v_g(n, h)$ is

$$v_g(n, h) = \begin{cases} \frac{n}{h} \cdot \max \left\{ 1 + \frac{h-i}{d_i} : i \in I \right\} & \text{if } I \neq \emptyset; \\ \lfloor \frac{n}{h} \rfloor & \text{if } I = \emptyset \text{ and } g \neq h; \\ \lfloor \frac{n-1}{h} \rfloor & \text{if } I = \emptyset \text{ and } g = h. \end{cases}$$

Proof. For a positive divisor d of n , we define the function

$$f(d) = \left(\left\lfloor \frac{d-1-\gcd(d, g)}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d}.$$

In [2] we stated and proved the following three claims:

Claim 1: Let i be the remainder of d when divided by h . We then have

$$f(d) = \begin{cases} \frac{n}{h} \cdot \left(1 + \frac{h-i}{d} \right) & \text{if } \gcd(d, g) < i; \\ \frac{n}{h} \cdot \left(1 - \frac{h}{d} \right) & \text{if } h|d \text{ and } g = h; \\ \frac{n}{h} \cdot \left(1 - \frac{i}{d} \right) & \text{otherwise.} \end{cases}$$

Claim 2: Using the notations as above, assume that $\gcd(d, g) \geq i$. Then

$$f(d) \leq \begin{cases} n/h & \text{if } g \neq h; \\ (n-1)/h & \text{if } g = h. \end{cases}$$

Claim 3: For all g , h , and n we have

$$v_g(n, h) \geq \begin{cases} \lfloor \frac{n}{h} \rfloor & \text{if } g \neq h; \\ \lfloor \frac{n-1}{h} \rfloor & \text{if } g = h. \end{cases}$$

We can now conclude that Theorem 5 holds, as it follows.

If $I = \emptyset$, then by Claims 2 and 3, we have

$$v_g(n, h) = \begin{cases} \lfloor \frac{n}{h} \rfloor & \text{if } g \neq h, \\ \lfloor \frac{n-1}{h} \rfloor & \text{if } g = h; \end{cases}$$

while if $I \neq \emptyset$, then, since only the first possibility in Claim 1 yields a value $f(d) > n/h$, we have

$$v_g(n, h) = \max \{f(d) : d \in D(n)\} = \frac{n}{h} \cdot \max \left\{ 1 + \frac{h-i}{d_i} : i \in I \right\}.$$

The proof of Theorem 5 is thus complete. \square

Our second correction here is regarding the *restricted h -critical number* of a finite abelian group G , defined as

$$\chi^{\wedge}(G, h) = \min\{m : A \subseteq G, |A| \geq m \Rightarrow h^{\wedge}A = G\}.$$

In [2] we determined $\chi^{\wedge}(G, h)$ for cyclic groups G of even order and all positive integers h . The cases of

$$h \leq 2 \quad \text{or} \quad h \geq n/2$$

have been addressed elsewhere (and more generally) in [2], leaving only

$$3 \leq h \leq n/2 - 1,$$

for which we presented Theorem 11. Unfortunately, the proof of Theorem 11 contains an inaccuracy: in the third line, the inequality

$$3 \leq h \leq n/2$$

should instead be

$$3 \leq h \leq (n+2)/4.$$

Since this error appeared repeatedly, it is best if we present the proof in its entirety below. We also use the opportunity to shorten the last part of our argument.

THEOREM 11. Suppose that n is even and $n \geq 12$. Then

$$\chi^{\wedge}(\mathbb{Z}_n, h) = \begin{cases} n/2 + 1 & \text{if } 3 \leq h \leq n/2 - 2; \\ n/2 + 2 & \text{if } h = n/2 - 1. \end{cases}$$

Proof. Our methods are similar to the one by Gallardo, Grekos, et al. in [3], where they established the result for $h = 3$. We first show that it suffices to treat the cases of

$$3 \leq h \leq (n+2)/4.$$

To conclude that we then have

$$\chi^{\wedge}(\mathbb{Z}_n, h) = n/2 + 1 \quad \text{for } n/4 + 1 \leq h \leq n/2 - 2$$

as well, note that, obviously,

$$\chi^{\wedge}(\mathbb{Z}_n, h) \geq n/2 + 1,$$

and that if A is a subset of \mathbb{Z}_n of size $n/2 + 1$, then, since

$$3 \leq n/2 + 1 - h \leq (n + 2)/4,$$

we have

$$|h^{\wedge}A| = |(n/2 + 1 - h)^{\wedge}A| = n.$$

Similarly, with

$$\chi^{\wedge}(\mathbb{Z}_n, 2) = n/2 + 2 \quad \text{and} \quad \chi^{\wedge}(\mathbb{Z}_n, 3) = n/2 + 1$$

we can settle the case of $h = n/2 - 1$. Choosing a subset A of \mathbb{Z}_n of size $n/2 + 1$ for which $|2^{\wedge}A| < n$ implies that we also have

$$|(n/2 - 1)^{\wedge}A| < n$$

and thus $\chi^{\wedge}(\mathbb{Z}_n, n/2 - 1)$ is at least $n/2 + 2$ while for any $B \subset \mathbb{Z}_n$ of size $n/2 + 2$ we get

$$|(n/2 - 1)^{\wedge}B| = |3^{\wedge}B| = n.$$

Therefore, for the rest of the proof, we assume that $3 \leq h \leq (n + 2)/4$.

Since we clearly have $\chi^{\wedge}(\mathbb{Z}_n, h) \geq n/2 + 1$, it suffices to prove the reverse inequality. For that, let A be a subset of \mathbb{Z}_n of size $n/2 + 1$; we need to prove that $h^{\wedge}A = \mathbb{Z}_n$.

Let O and E denote the set of odd and even elements of \mathbb{Z}_n , respectively, and let A_O and A_E be the set of odd and even elements of A , respectively. Note that both A_O and A_E have size at most $n/2$ and thus neither can be empty. We will consider four cases:

- Assume first that $|A_O| \leq 2$. Then $|A_E| \geq n/2 - 1$. Observe that $3 \leq h \leq (n + 2)/4$ and $n \geq 12$ imply that

$$2 \leq h - 1 < h \leq n/2 - 3,$$

and $n/2 - 1$ is not a divisor of n . Therefore, by Theorem 14, both $(h - 1)^{\wedge}A_E$ and $h^{\wedge}A_E$ have size at least $n/2$. But, of course, both $(h - 1)^{\wedge}A_E$ and $h^{\wedge}A_E$ are subsets of E , so

$$(h - 1)^{\wedge}A_E = h^{\wedge}A_E = E.$$

Now let a be any element of A_O , we then see that

$$a + (h-1)\hat{A}_E = a + E = O.$$

Therefore,

$$(a + (h-1)\hat{A}_E) \cup h\hat{A}_E = O \cup E = \mathbb{Z}_n;$$

since both $a + (h-1)\hat{A}_E$ and $h\hat{A}_E$ are subsets of $h\hat{A}$, we get $h\hat{A} = \mathbb{Z}_n$.

- Next, we assume that $|A_E| \leq 2$. In this case, an argument similar to the one in the previous case yields that

$$(h-1)\hat{A}_O = \begin{cases} O & \text{if } h \text{ is even,} \\ E & \text{if } h \text{ is odd;} \end{cases}$$

and

$$h\hat{A}_O = \begin{cases} E & \text{if } h \text{ is even,} \\ O & \text{if } h \text{ is odd.} \end{cases}$$

Let a be any element of A_E ; we get

$$(a + (h-1)\hat{A}_O) \cup h\hat{A}_O = \mathbb{Z}_n$$

regardless of whether h is even or odd; therefore, $h\hat{A} = \mathbb{Z}_n$.

Before turning to the last two cases, we observe that, since $h \leq (n+2)/4$, we have

$$|A| = n/2 + 1 \geq 2h,$$

and thus at least one of A_O or A_E must have size at least h .

- Consider the case when $|A_O| \geq 3$ and $|A_E| \geq h$. Referring to Theorem 14 again, we deduce that $(h-2)\hat{A}_E$ and $(h-1)\hat{A}_E$ both have size at least $|A_E|$, and that $2\hat{A}_O$ is of size at least $|A_O|$.

Now let g_O be any element of O ; we have

$$|g_O - A_O| + |(h-1)\hat{A}_E| \geq |A_O| + |A_E| = n/2 + 1.$$

But $g_O - A_O$ and $(h-1)\hat{A}_E$ are both subsets of E , so they cannot be disjoint; this then means that g_O can be written as the sum of an element of A_O and $h-1$ distinct elements of A_E , so $g_O \in h\hat{A}$.

Similarly, for any element g_E of E , we have

$$|g_E - (h-2)\hat{A}_E| + |2\hat{A}_O| \geq |A_E| + |A_O| = n/2 + 1,$$

and thus g_E can be written as the sum of $h-2$ distinct elements of A_E and two distinct elements of A_O , so $g_E \in h\hat{A}$.

Combining the last two paragraphs yields $O \cup E \subseteq h\hat{A}$ and thus $h\hat{A} = \mathbb{Z}_n$.

- For our fourth case, assume that $|A_E| \geq 3$ and $|A_O| \geq h$. As above, we can conclude that $|(h-2)\hat{A}_O| \geq |A_O|$, $|(h-1)\hat{A}_O| \geq |A_O|$, and $|2\hat{A}_E| \geq |A_E|$. Let g be any element of \mathbb{Z}_n . If g and h are of the same parity (both even or both odd), then we find that $g - (h-2)\hat{A}_O$ and $2\hat{A}_E$ are each subsets of E . As above, we see that they cannot be disjoint, and thus

$$g \in (h-2)\hat{A}_O + 2\hat{A}_E \subseteq h\hat{A}.$$

The case when g and h have opposite parity is similar: this time we see that $g - (h-1)\hat{A}_O$ and A_E are each subsets of E and that they cannot be disjoint, so

$$g \in (h-1)\hat{A}_O + A_E \subseteq h\hat{A}.$$

This completes our proof. □

Acknowledgements. The author wishes to thank Ryan Matzke for alerting him to the error in Theorem 5 and Krishna Kripa for calling his attention to the inaccuracy in the proof of Theorem 11.

REFERENCES

- [1] BAJNOK, B.: *On the maximum size of a (k, l) -sum-free subset of an abelian group*, Int. J. Number Theory **5** (2009), no. 6, 953–971.
- [2] ———: *The h -critical number of finite abelian groups*, Unif. Distrib. Theory **10** (2015), no. 2, 93–115.
- [3] GALLARDO, L.—GREKOS, G. ET AL.: *Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős-Ginzburg-Ziv problem*, J. London Math. Soc. (2), **65** (2002), no. 3, 513–523.

Received December 7, 2016

Accepted March 2, 2017

Béla Bajnok

*Gettysburg College,
300 North Washington Street,
Gettysburg, PA,
USA 17325*

E-mail: bbajnok@gettysburg.edu