Freiman's $3k - 4$ Theorem

Arthur F. Ramos David Barros Hulak Ruy J. G. B. de Queiroz

July 14, 2026

Abstract

This entry formalizes Freiman's $3k - 4$ theorem for finite sets of integers: small doubling, in the range $|A + A| \leq 3|A| - 4$, forces containment in a short arithmetic progression. AI assistance was used for proof engineering. The final definitions, statements, and proofs are checked by Isabelle.

1 Overview

Freiman's $3k - 4$ theorem is a classical inverse theorem in additive combinatorics. It gives a sharp structural conclusion for finite integer sets whose two-fold sumset is only slightly larger than the Cauchy-Davenport lower bound: if A has cardinality $k \geq 3$ and $|A + A| \leq 3k - 4$, then A is contained in an arithmetic progression of length at most $|A + A| - k + 1$.

2 Formalization

The development starts with integer arithmetic progressions, affine normalization of finite integer sets, and cardinality invariance of sumsets under injective affine maps. The final proof combines these reductions with the additive-combinatorial core argument.

3 Sources

The formalization follows the standard presentation of Freiman's theorem in additive-combinatorics texts, especially Nathanson [1] and Tao and Vu [2].

Contents

theory *Freiman-Sumset-Basics*
imports *Main*
begin

definition *sumset* :: $('a::comm\text{-}monoid\text{-}add)\ set \Rightarrow 'a\ set \Rightarrow 'a\ set$ **where**
$sumset\ A\ B = \{x.\ \exists\, a{\in}A.\ \exists\, b{\in}B.\ x = a + b\}$

lemma *sumset-iff*:
$x \in sumset\ A\ B \longleftrightarrow (\exists\, a{\in}A.\ \exists\, b{\in}B.\ x = a + b)$
⟨*proof*⟩

lemma *sumsetI* [*intro*]:
assumes $a \in A\ \ b \in B$
shows $a + b \in sumset\ A\ B$
⟨*proof*⟩

lemma *sumsetE* [*elim*]:
assumes $x \in sumset\ A\ B$
obtains $a\ b$ **where** $a \in A\ \ b \in B\ \ x = a + b$
⟨*proof*⟩

lemma *sumset-as-image*:
$sumset\ A\ B = case\text{-}prod\ (+)\ `\ (A \times B)$
⟨*proof*⟩

lemma *sumset-commute*:
$sumset\ A\ B = sumset\ B\ A$
⟨*proof*⟩

lemma *empty-sumset-left* [*simp*]:
$sumset\ \{\}\ B = \{\}$
⟨*proof*⟩

lemma *empty-sumset-right* [*simp*]:
$sumset\ A\ \{\} = \{\}$
⟨*proof*⟩

lemma *sumset-assoc*:
fixes $A\ B\ C :: ('a::comm\text{-}monoid\text{-}add)\ set$
shows $sumset\ (sumset\ A\ B)\ C = sumset\ A\ (sumset\ B\ C)$
⟨*proof*⟩

lemma *finite-sumset* [*intro*]:
assumes *finite A finite B*
shows *finite* (*sumset A B*)
⟨*proof*⟩

end
theory *Freiman-3k-4*
imports
Freiman-Sumset-Basics
HOL−Computational-Algebra.Group-Closure
Kneser-Cauchy-Davenport.Kneser-Cauchy-Davenport-main-proofs
begin

4 Freiman's *3k − 4* theorem for integer sumsets

This theory develops the integer-side infrastructure for Freiman's *3k − 4* theorem. The final theorem is most naturally stated after normalizing a finite integer set by translation and dilation; the lemmas below record the affine invariance and interval containment facts used by that reduction.

4.1 Integer arithmetic progressions

definition *int-ap-segment* :: *int* ⇒ *int* ⇒ *nat* ⇒ *int set* **where**
  int-ap-segment a d n = (λ*i*. *a* + *int i* ∗ *d*) ‘ {..<*n*}

definition *int-arithmetic-progression* :: *int set* ⇒ *bool* **where**
  int-arithmetic-progression A ⟷ (∃ *a d n*. *A* = *int-ap-segment a d n*)

lemma *int-arithmetic-progressionI*:
  A = *int-ap-segment a d n* ⟹ *int-arithmetic-progression A*
  ⟨*proof*⟩

lemma *int-arithmetic-progressionE*:
  assumes *int-arithmetic-progression A*
  obtains *a d n* **where** *A* = *int-ap-segment a d n*
  ⟨*proof*⟩

lemma *finite-int-ap-segment* [*simp*]:
  finite (*int-ap-segment a d n*)
  ⟨*proof*⟩

lemma *int-ap-segment-empty* [*simp*]:
  int-ap-segment a d 0 = {}
  ⟨*proof*⟩

lemma *inj-on-int-ap-segment-index*:
  assumes *d* ≠ *0*
  shows *inj-on* (λ*i*. *a* + *int i* ∗ *d*) {..<*n*}
⟨*proof*⟩

lemma *card-int-ap-segment*:
  assumes *d* ≠ *0*
  shows *card* (*int-ap-segment a d n*) = *n*
  ⟨*proof*⟩

lemma *int-ap-segment-one-eq-atLeastAtMost*:
  assumes *a* ≤ *b*
  shows *int-ap-segment a 1* (*nat* (*b* − *a* + *1*)) = {*a*..*b*}
⟨*proof*⟩

lemma *finite-int-set-subset-min-max-ap*:
  assumes *fin*: *finite A* **and** *nonempty*: *A* ≠ {}
  shows *A* ⊆ *int-ap-segment* (*Min A*) *1* (*nat* (*Max A* − *Min A* + *1*))
⟨*proof*⟩

4.2 Affine images and sumsets

definition *affine-image-int* :: *int* ⇒ *int* ⇒ *int set* ⇒ *int set* **where**
  affine-image-int c d A = (λ*x*. *c* + *d* ∗ *x*) ‘ *A*

lemma *affine-image-int-iff*:
  x ∈ *affine-image-int c d A* ⟷ (∃ *a*∈*A*. *x* = *c* + *d* ∗ *a*)

⟨*proof*⟩

lemma *finite-affine-image-int* [*intro*]:
assumes *finite A*
shows *finite* (*affine-image-int c d A*)
⟨*proof*⟩

lemma *inj-on-affine-image-int*:
fixes *c d* :: *int*
assumes $d \neq 0$
shows *inj-on* ($\lambda x.\ c + d * x$) *A*
⟨*proof*⟩

lemma *card-affine-image-int*:
assumes *fin*: *finite A* **and** *d-nonzero*: $d \neq 0$
shows *card* (*affine-image-int c d A*) = *card A*
⟨*proof*⟩

lemma *affine-image-int-sumset*:
sumset (*affine-image-int c d A*) (*affine-image-int e d B*) =
affine-image-int ($c + e$) *d* (*sumset A B*)
⟨*proof*⟩

lemma *affine-image-int-sumset-self*:
sumset (*affine-image-int c d A*) (*affine-image-int c d A*) =
affine-image-int ($2 * c$) *d* (*sumset A A*)
⟨*proof*⟩

lemma *card-sumset-affine-image-int*:
assumes *finA*: *finite A* **and** *finB*: *finite B* **and** *d-nonzero*: $d \neq 0$
shows *card* (*sumset* (*affine-image-int c d A*) (*affine-image-int e d B*)) =
card (*sumset A B*)
⟨*proof*⟩

lemma *card-sumset-affine-image-int-self*:
assumes *fin*: *finite A* **and** *d-nonzero*: $d \neq 0$
shows *card* (*sumset* (*affine-image-int c d A*) (*affine-image-int c d A*)) =
card (*sumset A A*)
⟨*proof*⟩

lemma *affine-image-int-zero-one* [*simp*]:
affine-image-int 0 1 A = *A*
⟨*proof*⟩

4.3 Endpoint lower bound for two-fold sumsets

lemma *endpoint-affine-images-inter*:
fixes *A* :: *int set*
assumes *fin*: *finite A* **and** *nonempty*: $A \neq \{\}$
shows *affine-image-int* (*Min A*) *1 A* ∩ *affine-image-int* (*Max A*) *1 A* =
{*Min A* + *Max A*}
⟨*proof*⟩

lemma *endpoint-affine-union-card*:
fixes *A* :: *int set*
assumes *fin*: *finite A* **and** *nonempty*: $A \neq \{\}$
shows *card* (*affine-image-int* (*Min A*) *1 A* ∪ *affine-image-int* (*Max A*) *1 A*) =
$2 * card\ A - 1$
⟨*proof*⟩

lemma *endpoint-affine-images-inter-two-sets*:
fixes $A\ B :: int\ set$
assumes *finA*: *finite* A **and** *nonemptyA*: $A \neq \{\}$
assumes *finB*: *finite* B **and** *nonemptyB*: $B \neq \{\}$
shows $affine\text{-}image\text{-}int\ (Min\ A)\ 1\ B \cap affine\text{-}image\text{-}int\ (Max\ B)\ 1\ A = \{Min\ A + Max\ B\}$
⟨*proof*⟩

lemma *card-sumset-ge-card-add-card-minus-one*:
fixes $A\ B :: int\ set$
assumes *finA*: *finite* A **and** *finB*: *finite* B
assumes *nonemptyA*: $A \neq \{\}$ **and** *nonemptyB*: $B \neq \{\}$
shows $card\ A + card\ B - 1 \leq card\ (sumset\ A\ B)$
⟨*proof*⟩

lemma *card-sumset-self-ge-two-card-minus-one*:
fixes $A :: int\ set$
assumes *fin*: *finite* A **and** *nonempty*: $A \neq \{\}$
shows $2 * card\ A - 1 \leq card\ (sumset\ A\ A)$
⟨*proof*⟩

4.4 Holes in the normalized interval

definition $interval\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$interval\text{-}holes\ A = \{x.\ 0 \leq x \wedge x \leq Max\ A \wedge x \notin A\}$

definition $lower\text{-}sum\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$lower\text{-}sum\text{-}holes\ A = \{x \in interval\text{-}holes\ A.\ x \in sumset\ A\ A\}$

definition $upper\text{-}sum\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$upper\text{-}sum\text{-}holes\ A = \{x \in interval\text{-}holes\ A.\ Max\ A + x \in sumset\ A\ A\}$

definition $stable\text{-}sum\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$stable\text{-}sum\text{-}holes\ A =$
$interval\text{-}holes\ A - (lower\text{-}sum\text{-}holes\ A \cup upper\text{-}sum\text{-}holes\ A)$

definition $left\text{-}stable\text{-}sum\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$left\text{-}stable\text{-}sum\text{-}holes\ A = interval\text{-}holes\ A - lower\text{-}sum\text{-}holes\ A$

definition $right\text{-}stable\text{-}sum\text{-}holes :: int\ set \Rightarrow int\ set$ **where**
$right\text{-}stable\text{-}sum\text{-}holes\ A = interval\text{-}holes\ A - upper\text{-}sum\text{-}holes\ A$

lemma *finite-interval-holes* [*simp*]:
finite (*interval-holes* A)
⟨*proof*⟩

lemma *finite-lower-sum-holes* [*simp*]:
finite (*lower-sum-holes* A)
⟨*proof*⟩

lemma *finite-upper-sum-holes* [*simp*]:
finite (*upper-sum-holes* A)
⟨*proof*⟩

lemma *finite-stable-sum-holes* [*simp*]:
finite (*stable-sum-holes* A)
⟨*proof*⟩

lemma *finite-left-stable-sum-holes* [*simp*]:
  finite (*left-stable-sum-holes A*)
  ⟨*proof*⟩

lemma *finite-right-stable-sum-holes* [*simp*]:
  finite (*right-stable-sum-holes A*)
  ⟨*proof*⟩

lemma *stable-sum-holes-eq-left-right-inter*:
  stable-sum-holes A =
    left-stable-sum-holes A ∩ *right-stable-sum-holes A*
  ⟨*proof*⟩

lemma *left-stable-sum-hole-notin-sumset*:
  assumes *x-left*: $x \in$ *left-stable-sum-holes A*
  shows $x \in$ *interval-holes A x* $\notin$ *sumset A A*
⟨*proof*⟩

lemma *right-stable-sum-hole-notin-sumset*:
  assumes *x-right*: $x \in$ *right-stable-sum-holes A*
  shows $x \in$ *interval-holes A Max A* + $x \notin$ *sumset A A*
⟨*proof*⟩

lemma *left-stable-hole-prefix-card-le-holes*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *x-left*: $x \in$ *left-stable-sum-holes A*
  shows *card* ($A \cap \{0..x\}$) ≤ *card* ($\{0..x\} - A$)
⟨*proof*⟩

lemma *left-stable-hole-prefix-twice-card-le*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *x-left*: $x \in$ *left-stable-sum-holes A*
  shows *2* ∗ *card* ($A \cap \{0..x\}$) ≤ *nat* (x + *1*)
⟨*proof*⟩

lemma *right-stable-hole-suffix-card-le-holes*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *x-right*: $x \in$ *right-stable-sum-holes A*
  shows *card* ($A \cap \{x..Max\ A\}$) ≤ *card* ($\{x..Max\ A\} - A$)
⟨*proof*⟩

lemma *right-stable-hole-suffix-twice-card-le*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *x-right*: $x \in$ *right-stable-sum-holes A*
  shows *2* ∗ *card* ($A \cap \{x..Max\ A\}$) ≤ *nat* (*Max A* − x + *1*)
⟨*proof*⟩

lemma *hole-cover-of-no-stable-sum-holes*:
  assumes *stable-empty*: *stable-sum-holes A* = {}
  shows *card* (*interval-holes A*) ≤ *card* (*lower-sum-holes A*) + *card* (*upper-sum-holes A*)
⟨*proof*⟩

lemma *interval-holes-eq-interval-diff*:
  assumes *subset*: $A \subseteq \{0..Max\ A\}$
  shows *interval-holes A* = $\{0..Max\ A\} - A$

⟨*proof*⟩

lemma *normalized-subset-interval*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $A \subseteq \{0..Max\ A\}$
⟨*proof*⟩

lemma *card-interval-holes*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $card\ (interval\text{-}holes\ A) = nat\ (Max\ A + 1) - card\ A$
⟨*proof*⟩

lemma *Min-eq-zero-of-zero-mem-nonneg*:
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $Min\ A = 0$
⟨*proof*⟩

lemma *normalized-endpoint-union-card*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $card\ (A \cup affine\text{-}image\text{-}int\ (Max\ A)\ 1\ A) = 2 * card\ A - 1$
⟨*proof*⟩

lemma *lower-sum-holes-disjoint-endpoint-union*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $(A \cup affine\text{-}image\text{-}int\ (Max\ A)\ 1\ A) \cap lower\text{-}sum\text{-}holes\ A = \{\}$
⟨*proof*⟩

lemma *upper-sum-holes-image-disjoint-endpoint-union*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $(A \cup affine\text{-}image\text{-}int\ (Max\ A)\ 1\ A) \cap$
    $affine\text{-}image\text{-}int\ (Max\ A)\ 1\ (upper\text{-}sum\text{-}holes\ A) = \{\}$
⟨*proof*⟩

lemma *lower-sum-holes-disjoint-upper-sum-holes-image*:
  fixes A :: *int set*
  assumes *fin*: *finite* A
  assumes *zero*: $0 \in A$
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  shows $lower\text{-}sum\text{-}holes\ A \cap affine\text{-}image\text{-}int\ (Max\ A)\ 1\ (upper\text{-}sum\text{-}holes\ A) = \{\}$
⟨*proof*⟩

lemma *normalized-sumset-lower-bound-with-holes*:

fixes A :: *int set*
assumes *fin*: *finite* A
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
shows $2 * card\ A - 1 + card\ (lower\text{-}sum\text{-}holes\ A) + card\ (upper\text{-}sum\text{-}holes\ A)$
$\leq card\ (sumset\ A\ A)$
⟨*proof*⟩

lemma *normalized-sumset-eq-endpoint-union-with-holes*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
shows $sumset\ A\ A =$
$A \cup affine\text{-}image\text{-}int\ (Max\ A)\ 1\ A \cup$
$lower\text{-}sum\text{-}holes\ A \cup$
$affine\text{-}image\text{-}int\ (Max\ A)\ 1\ (upper\text{-}sum\text{-}holes\ A)$
⟨*proof*⟩

lemma *normalized-sumset-card-eq-with-holes*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
shows $card\ (sumset\ A\ A) =$
$2 * card\ A - 1 + card\ (lower\text{-}sum\text{-}holes\ A) + card\ (upper\text{-}sum\text{-}holes\ A)$
⟨*proof*⟩

lemma *normalized-small-doubling-hole-contribution-upper*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *card-ge*: $3 \leq card\ A$
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
assumes *small-doubling*: $card\ (sumset\ A\ A) \leq 3 * card\ A - 4$
shows $card\ (lower\text{-}sum\text{-}holes\ A) + card\ (upper\text{-}sum\text{-}holes\ A) \leq card\ A - 3$
⟨*proof*⟩

lemma *normalized-max-bound-from-hole-contribution*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
assumes *hole-cover*:
$card\ (interval\text{-}holes\ A) \leq card\ (lower\text{-}sum\text{-}holes\ A) + card\ (upper\text{-}sum\text{-}holes\ A)$
shows $nat\ (Max\ A + 1) \leq card\ (sumset\ A\ A) - card\ A + 1$
⟨*proof*⟩

4.5 Modular shadows of integer sumsets

definition *mod-image-int* :: $int \Rightarrow int\ set \Rightarrow int\ set$ **where**
$mod\text{-}image\text{-}int\ n\ A = (\lambda x.\ x\ mod\ n)$ ‘ A

definition *mod-sumset-int* :: $int \Rightarrow int\ set \Rightarrow int\ set \Rightarrow int\ set$ **where**
$mod\text{-}sumset\text{-}int\ n\ A\ B = mod\text{-}image\text{-}int\ n\ (sumset\ A\ B)$

definition *mod-translate-int* :: $int \Rightarrow int \Rightarrow int\ set \Rightarrow int\ set$ **where**
$mod\text{-}translate\text{-}int\ n\ a\ H = (\lambda h.\ (a + h)\ mod\ n)$ ‘ H

definition *mod-fiber-int* :: *int* ⇒ *int set* ⇒ *int* ⇒ *int set* **where**
mod-fiber-int n S r = {*s* ∈ *S*. *s mod n* = *r*}

lemma *mod-image-int-iff*:
r ∈ *mod-image-int n A* ⟷ (∃ *a*∈*A*. *r* = *a mod n*)
⟨*proof*⟩

lemma *finite-mod-image-int* [*intro*]:
assumes *finite A*
shows *finite* (*mod-image-int n A*)
⟨*proof*⟩

lemma *mod-sumset-int-iff*:
r ∈ *mod-sumset-int n A B* ⟷ (∃ *a*∈*A*. ∃ *b*∈*B*. *r* = (*a* + *b*) *mod n*)
⟨*proof*⟩

lemma *finite-mod-sumset-int* [*intro*]:
assumes *finite A finite B*
shows *finite* (*mod-sumset-int n A B*)
⟨*proof*⟩

lemma *mod-translate-int-iff*:
r ∈ *mod-translate-int n a H* ⟷ (∃ *h*∈*H*. *r* = (*a* + *h*) *mod n*)
⟨*proof*⟩

lemma *finite-mod-translate-int* [*intro*]:
assumes *finite H*
shows *finite* (*mod-translate-int n a H*)
⟨*proof*⟩

lemma *mod-translate-int-subset-residues*:
assumes *n-pos*: *0* < *n*
shows *mod-translate-int n a H* ⊆ {*0*..*n* − *1*}
⟨*proof*⟩

lemma *mod-add-translate-inj-on-residues*:
fixes *a n* :: *int*
assumes *n-pos*: *0* < *n*
shows *inj-on* (λ*h*. (*a* + *h*) *mod n*) {*0*..*n* − *1*}
⟨*proof*⟩

lemma *card-mod-translate-int-eq*:
fixes *H* :: *int set*
assumes *n-pos*: *0* < *n*
assumes *H-sub*: *H* ⊆ {*0*..*n* − *1*}
shows *card* (*mod-translate-int n a H*) = *card H*
⟨*proof*⟩

lemma *sum-coset-lower-upper-inter-card*:
fixes *A H* :: *int set*
assumes *n-pos*: *0* < *n*
assumes *finA*: *finite A*
assumes *max-eq*: *Max A* = *n*
assumes *H-sub*: *H* ⊆ {*0*..*n* − *1*}
assumes *zero-H*: *0* ∈ *H*
assumes *add-closed*: ⋀*x y*. *x* ∈ *H* ⟹ *y* ∈ *H* ⟹ (*x* + *y*) *mod n* ∈ *H*
assumes *b-in*: *b* ∈ *A* **and** *b-bounds*: *0* ≤ *b b* < *n*
assumes *c-in*: *c* ∈ *A* **and** *c-bounds*: *0* ≤ *c c* < *n*
defines *R* ≡ *mod-translate-int n b H*

defines $S \equiv$ *mod-translate-int n c H*
defines $K \equiv$ *mod-translate-int n* $((b + c)$ *mod n*$)$ *H*
assumes *K-disj*: $K \cap A = \{\}$
shows *card* $H \leq$
1 + *card* ((*lower-sum-holes* $A \cap$ *upper-sum-holes* $A) \cap K$) +
card $(R - A)$ + *card* $(S - A)$
⟨*proof*⟩

lemma *mod-fiber-int-subset*:
mod-fiber-int n S r $\subseteq S$
⟨*proof*⟩

lemma *finite-mod-fiber-int* [*intro*]:
assumes *finite S*
shows *finite* (*mod-fiber-int n S r*)
⟨*proof*⟩

interpretation *Zmod*: *additive-abelian-group* $\{$*0..int* $((p ::$ *nat*$) - 1)\}$
$(\lambda x\ y.\ (x + y)$ *mod int p*$)$ *0::int*
⟨*proof*⟩

lemma *zmod-sumset-eq-mod-sumset-int*:
fixes *A B* :: *int set*
assumes *p-pos*: $0 < p$
assumes *A-sub*: $A \subseteq \{$*0..int* $p - 1\}$
assumes *B-sub*: $B \subseteq \{$*0..int* $p - 1\}$
shows *Zmod.sumset p A B* = *mod-sumset-int* (*int p*) *A B*
⟨*proof*⟩

lemma *zmod-kneser-self*:
fixes *B* :: *int set*
assumes *p-pos*: $0 < p$
assumes *B-sub*: $B \subseteq \{$*0..int* $p - 1\}$
assumes *fin*: *finite B*
assumes *nonempty*: $B \neq \{\}$
defines $C \equiv$ *Zmod.sumset p B B*
defines $H \equiv$ *Zmod.stabilizer p C*
shows *card* $C \geq 2 *$ *card* (*Zmod.sumset p B H*) $-$ *card H*
⟨*proof*⟩

lemma *zmod-sumset-iff*:
$x \in$ *Zmod.sumset p A B* $\longleftrightarrow$
$(\exists\, a \in A \cap \{$*0..int* $(p - 1)\}$.
$\exists\, b \in B \cap \{$*0..int* $(p - 1)\}$. $x = (a + b)$ *mod int p*$)$
⟨*proof*⟩

lemma *zmod-singleton-sumset-eq-mod-translate-int*:
assumes *p-pos*: $0 < p$
assumes *a-carrier*: $a \in \{$*0..int* $p - 1\}$
assumes *H-sub*: $H \subseteq \{$*0..int* $p - 1\}$
shows *Zmod.sumset p* $\{a\}$ *H* = *mod-translate-int* (*int p*) *a H*
⟨*proof*⟩

lemma *zmod-self-sumset-contains-set*:
assumes *p-pos*: $0 < p$
assumes *B-sub*: $B \subseteq \{$*0..int* $p - 1\}$
assumes *zero-B*: $0 \in B$
shows $B \subseteq$ *Zmod.sumset p B B*
⟨*proof*⟩

lemma *zmod-sumset-stabilizer-subset*:
  assumes *p-pos*: $0 < p$
  assumes *A-sub-C*: $A \subseteq C$
  assumes *C-sub*: $C \subseteq \{0..int\ p - 1\}$
  shows $Zmod.sumset\ p\ A\ (Zmod.stabilizer\ p\ C) \subseteq C$
$\langle proof \rangle$

lemma *zmod-obtain-sum-coset-disjoint-D*:
  fixes $B :: int\ set$
  assumes *p-pos*: $0 < p$
  assumes *B-sub*: $B \subseteq \{0..int\ p - 1\}$
  assumes *finB*: *finite B*
  assumes *zero-B*: $0 \in B$
  defines $C \equiv Zmod.sumset\ p\ B\ B$
  defines $H \equiv Zmod.stabilizer\ p\ C$
  defines $D \equiv Zmod.sumset\ p\ B\ H$
  assumes *not-subset*: $\neg B \subseteq H$
  obtains $b\ c$ **where** $b \in B\ c \in B\ Zmod.sumset\ p\ \{((b + c)\ mod\ int\ p)\}\ H \cap D = \{\}$
$\langle proof \rangle$

lemma *mod-image-int-subset-residues*:
  assumes *n-pos*: $0 < n$
  shows $mod\text{-}image\text{-}int\ n\ A \subseteq \{0..n - 1\}$
  $\langle proof \rangle$

lemma *mod-sumset-int-mod-image-self*:
  assumes *n-pos*: $0 < n$
  shows $mod\text{-}sumset\text{-}int\ n\ (mod\text{-}image\text{-}int\ n\ A)\ (mod\text{-}image\text{-}int\ n\ A) =$
    $mod\text{-}sumset\text{-}int\ n\ A\ A$
$\langle proof \rangle$

lemma *zmod-sumset-trivial-stabilizer-card-ge*:
  fixes $B :: int\ set$
  assumes *p-pos*: $0 < p$
  assumes *B-sub*: $B \subseteq \{0..int\ p - 1\}$
  assumes *fin*: *finite B*
  assumes *nonempty*: $B \neq \{\}$
  defines $C \equiv Zmod.sumset\ p\ B\ B$
  assumes *trivial*: $Zmod.stabilizer\ p\ C = \{0\}$
  shows $2 * card\ B - 1 \leq card\ C$
$\langle proof \rangle$

lemma *zmod-nontrivial-stabilizer-obtain-positive-period*:
  fixes $C :: int\ set$
  assumes *p-pos*: $0 < p$
  assumes *nontrivial*: $Zmod.stabilizer\ p\ C \neq \{0\}$
  obtains h **where** $h \in Zmod.stabilizer\ p\ C\ 0 < h\ h < int\ p$
$\langle proof \rangle$

lemma *residue-add-closed-mult*:
  fixes $H :: int\ set$
  assumes *n-pos*: $0 < n$
  assumes *zero*: $0 \in H$
  assumes *add-closed*: $\bigwedge x\ y.\ x \in H \Longrightarrow y \in H \Longrightarrow (x + y)\ mod\ n \in H$
  assumes *h-in*: $h \in H$
  shows $(int\ m * h)\ mod\ n \in H$
$\langle proof \rangle$

lemma *residue-add-closed-diff*:
  fixes H :: *int set*
  assumes *n-pos*: $0 < n$
  assumes *zero*: $0 \in H$
  assumes *add-closed*: $\bigwedge x\ y.\ x \in H \Longrightarrow y \in H \Longrightarrow (x + y)\ mod\ n \in H$
  assumes *x-in*: $x \in H$
  assumes *y-in*: $y \in H$
  shows $(x - y)\ mod\ n \in H$
⟨*proof*⟩

lemma *residue-add-closed-obtain-proper-divisor*:
  fixes H :: *int set*
  assumes *n-pos*: $0 < n$
  assumes *H-sub*: $H \subseteq \{0..n - 1\}$
  assumes *zero*: $0 \in H$
  assumes *add-closed*: $\bigwedge x\ y.\ x \in H \Longrightarrow y \in H \Longrightarrow (x + y)\ mod\ n \in H$
  assumes *nontrivial*: $H \neq \{0\}$
  assumes *proper*: $H \neq \{0..n - 1\}$
  obtains d **where** $1 < d$ $d\ dvd\ n$ $\bigwedge h.\ h \in H \Longrightarrow d\ dvd\ h$
⟨*proof*⟩

lemma *residue-add-closed-min-step-eq*:
  fixes H :: *int set*
  assumes *n-pos*: $0 < n$
  assumes *H-sub*: $H \subseteq \{0..n - 1\}$
  assumes *zero*: $0 \in H$
  assumes *add-closed*: $\bigwedge x\ y.\ x \in H \Longrightarrow y \in H \Longrightarrow (x + y)\ mod\ n \in H$
  assumes *nontrivial*: $H \neq \{0\}$
  defines $d \equiv Min\ (H - \{0\})$
  shows $0 < d$
    and $d\ dvd\ n$
    and $H = \{x \in \{0..n - 1\}.\ d\ dvd\ x\}$
⟨*proof*⟩

lemma *zmod-stabilizer-add-closed*:
  assumes *x-in*: $x \in Zmod.stabilizer\ p\ C$
  assumes *y-in*: $y \in Zmod.stabilizer\ p\ C$
  shows $(x + y)\ mod\ int\ p \in Zmod.stabilizer\ p\ C$
⟨*proof*⟩

lemma *zmod-stabilizer-obtain-proper-divisor*:
  fixes C :: *int set*
  assumes *p-pos*: $0 < p$
  assumes *nontrivial*: $Zmod.stabilizer\ p\ C \neq \{0\}$
  assumes *proper*: $Zmod.stabilizer\ p\ C \neq \{0..int\ p - 1\}$
  obtains d **where** $1 < d$ $d\ dvd\ int\ p$
    $\bigwedge h.\ h \in Zmod.stabilizer\ p\ C \Longrightarrow d\ dvd\ h$
⟨*proof*⟩

lemma *zmod-full-stabilizer-zero-imp-carrier-subset*:
  fixes C :: *int set*
  assumes *p-pos*: $0 < p$
  assumes *C-sub*: $C \subseteq \{0..int\ p - 1\}$
  assumes *zero-C*: $0 \in C$
  assumes *full*: $Zmod.stabilizer\ p\ C = \{0..int\ p - 1\}$
  shows $\{0..int\ p - 1\} \subseteq C$
⟨*proof*⟩

lemma *mod-image-int-normalized-interval*:

fixes A :: *int set*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
shows *mod-image-int* n $A = A - \{n\}$
⟨*proof*⟩

lemma *card-mod-image-int-normalized-interval*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
shows *card* (*mod-image-int* n A) = *card* $A - 1$
⟨*proof*⟩

lemma *normalized-mod-sumset-trivial-stabilizer-card-ge*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
defines $B \equiv$ *mod-image-int* n A
defines $p \equiv$ *nat* n
defines $C \equiv$ *Zmod.sumset* p B B
assumes *trivial*: *Zmod.stabilizer* p $C = \{0\}$
shows $2 *$ *card* $A - 3 \leq$ *card* (*mod-sumset-int* n A A)
⟨*proof*⟩

lemma *mod-image-int-subset-mod-sumset-self*:
assumes *zero*: $0 \in A$
shows *mod-image-int* n $A \subseteq$ *mod-sumset-int* n A A
⟨*proof*⟩

lemma *card-eq-sum-mod-fibers*:
fixes S :: *int set*
assumes *fin*: *finite* S
shows *card* S = ($\sum r \in$*mod-image-int* n S. *card* (*mod-fiber-int* n S r))
⟨*proof*⟩

lemma *card-mod-fiber-pos*:
fixes S :: *int set*
assumes *fin*: *finite* S
assumes *r-in*: $r \in$ *mod-image-int* n S
shows $0 <$ *card* (*mod-fiber-int* n S r)
⟨*proof*⟩

lemma *normalized-endpoint-zero-fiber-card-ge3*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *n-pos*: $0 < n$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
shows $3 \leq$ *card* (*mod-fiber-int* n (*sumset* A A) 0)
⟨*proof*⟩

lemma *normalized-endpoint-nonzero-fiber-card-ge2*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *r-in*: $r \in$ *mod-image-int* n A
assumes *r-ne*: $r \neq 0$
shows $2 \leq$ *card* (*mod-fiber-int* n (*sumset* A A) r)
⟨*proof*⟩

lemma *card-sumset-ge-mod-sumset-plus-card*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
shows *card* (*sumset* A A) $\geq$ *card* (*mod-sumset-int* n A A) + *card* A
⟨*proof*⟩

lemma *normalized-small-doubling-mod-stabilizer-nontrivial*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *card-ge*: $3 \leq$ *card* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *small-doubling*: *card* (*sumset* A A) $\leq 3 *$ *card* $A - 4$
defines $B \equiv$ *mod-image-int* n A
defines $p \equiv$ *nat* n
defines $C \equiv$ *Zmod.sumset* p B B
shows *Zmod.stabilizer* p $C \neq \{0\}$
⟨*proof*⟩

lemma *normalized-small-doubling-obtain-positive-mod-period*:
fixes A :: *int set*
assumes *fin*: *finite* A
assumes *card-ge*: $3 \leq$ *card* A
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *small-doubling*: *card* (*sumset* A A) $\leq 3 *$ *card* $A - 4$
defines $B \equiv$ *mod-image-int* n A
defines $p \equiv$ *nat* n
defines $C \equiv$ *Zmod.sumset* p B B
obtains h **where** $h \in$ *Zmod.stabilizer* p C $0 < h$ $h < n$
⟨*proof*⟩

lemma *two-sided-unstable-hole-notin-mod-sumset*:
fixes A :: *int set*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *x-bounds*: $0 < x$ $x < n$
assumes *lower-missing*: $x \notin$ *sumset* A A
assumes *upper-missing*: $n + x \notin$ *sumset* A A

shows $x \notin$ *mod-sumset-int n A A*
⟨*proof*⟩

lemma *mod-sumset-gap-imp-stable-sum-hole*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *x-bounds*: $0 < x$ $x < n$
assumes *gap*: $x \notin$ *mod-sumset-int n A A*
shows $x \in$ *stable-sum-holes A*
⟨*proof*⟩

lemma *stable-sum-holes-eq-mod-sumset-gaps*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
shows *stable-sum-holes A* =
{x. $0 < x \wedge x < n \wedge x \notin$ *mod-sumset-int n A A*}
⟨*proof*⟩

lemma *mod-sumset-int-eq-mod-image-union-sum-holes*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *max-eq*: *Max A* $= n$
shows *mod-sumset-int n A A* =
mod-image-int n A ∪ *lower-sum-holes A* ∪ *upper-sum-holes A*
⟨*proof*⟩

lemma *card-mod-sumset-int-eq-card-mod-image-plus-unstable-holes*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *max-eq*: *Max A* $= n$
shows *card* (*mod-sumset-int n A A*) =
card (*mod-image-int n A*) + *card* (*lower-sum-holes A* ∪ *upper-sum-holes A*)
⟨*proof*⟩

lemma *card-mod-sumset-int-eq-card-A-minus-one-plus-unstable-holes*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *n-pos*: $0 < n$
assumes *subset*: $A \subseteq \{0..n\}$
assumes *zero*: $0 \in A$
assumes *top*: $n \in A$
assumes *max-eq*: *Max A* $= n$
shows *card* (*mod-sumset-int n A A*) =

    card A − *1* + *card* (*lower-sum-holes A* ∪ *upper-sum-holes A*)
⟨*proof*⟩

lemma *normalized-sumset-card-eq-mod-sumset-plus-card-inter-holes*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *n-pos*: *0* < *n*
  assumes *subset*: *A* ⊆ {*0*..*n*}
  assumes *zero*: *0* ∈ *A*
  assumes *top*: *n* ∈ *A*
  assumes *max-eq*: *Max A* = *n*
  assumes *nonneg*: ⋀*x*. *x* ∈ *A* ⟹ *0* ≤ *x*
  shows *card* (*sumset A A*) =
    card (*mod-sumset-int n A A*) + *card A* +
    card (*lower-sum-holes A* ∩ *upper-sum-holes A*)
⟨*proof*⟩

lemma *card-mod-sumset-int-eq-diameter-minus-stable-holes*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *n-pos*: *0* < *n*
  assumes *subset*: *A* ⊆ {*0*..*n*}
  assumes *zero*: *0* ∈ *A*
  assumes *top*: *n* ∈ *A*
  assumes *max-eq*: *Max A* = *n*
  shows *card* (*mod-sumset-int n A A*) = *nat n* − *card* (*stable-sum-holes A*)
⟨*proof*⟩

lemma *mod-sub-translate-inj-on-residues*:
  fixes *x n* :: *int*
  assumes *n-pos*: *0* < *n*
  shows *inj-on* (λ*y*. (*x* − *y*) *mod n*) {*0*..*n* − *1*}
⟨*proof*⟩

lemma *card-mod-sub-translate-eq*:
  fixes *A* :: *int set*
  fixes *x n* :: *int*
  assumes *n-pos*: *0* < *n*
  assumes *A-sub*: *A* ⊆ {*0*..*n* − *1*}
  shows *card* ((λ*y*. (*x* − *y*) *mod n*) ‘ *A*) = *card A*
⟨*proof*⟩

lemma *stable-mod-gap-translate-disjoint*:
  fixes *A* :: *int set*
  assumes *n-pos*: *0* < *n*
  assumes *x-mod*: *x mod n* = *x*
  assumes *gap*: *x* ∉ *mod-sumset-int n A A*
  shows (λ*y*. (*x* − *y*) *mod n*) ‘ *mod-image-int n A* ∩ *mod-image-int n A* = {}
⟨*proof*⟩

lemma *stable-mod-gap-card-le-half-diameter*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *n-pos*: *0* < *n*
  assumes *subset*: *A* ⊆ {*0*..*n*}
  assumes *zero*: *0* ∈ *A*
  assumes *top*: *n* ∈ *A*
  assumes *x-mod*: *x mod n* = *x*
  assumes *gap*: *x* ∉ *mod-sumset-int n A A*

shows *2* $*$ (*card A* $-$ *1*) $\leq$ *nat n*
⟨*proof*⟩

lemma *stable-sum-holes-empty-of-short-diameter*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: *3* $\leq$ *card A*
assumes *zero*: *0* $\in$ *A*
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
assumes *short*: *nat* (*Max A*) $\leq$ *2* $*$ *card A* $-$ *3*
shows *stable-sum-holes A* = {}
⟨*proof*⟩

lemma *stable-sum-holes-nonempty-imp-large-diameter*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: *3* $\leq$ *card A*
assumes *zero*: *0* $\in$ *A*
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
assumes *stable-nonempty*: *stable-sum-holes A* $\neq$ {}
shows *2* $*$ *card A* $-$ *2* $\leq$ *nat* (*Max A*)
⟨*proof*⟩

4.6 Normalization by the diameter gcd

definition *shifted-int-set* :: *int set* $\Rightarrow$ *int set* **where**
shifted-int-set A = ($\lambda x.$ *x* $-$ *Min A*) ‘ *A*

definition *int-set-content* :: *int set* $\Rightarrow$ *int* **where**
int-set-content A = *Gcd* (*shifted-int-set A*)

definition *normalized-int-set* :: *int set* $\Rightarrow$ *int set* **where**
normalized-int-set A = ($\lambda x.$ *x div int-set-content A*) ‘ *shifted-int-set A*

lemma *finite-shifted-int-set* [*intro*]:
assumes *finite A*
shows *finite* (*shifted-int-set A*)
⟨*proof*⟩

lemma *finite-normalized-int-set* [*intro*]:
assumes *finite A*
shows *finite* (*normalized-int-set A*)
⟨*proof*⟩

lemma *zero-in-shifted-int-set*:
assumes *finite A* **and** *A* $\neq$ {}
shows *0* $\in$ *shifted-int-set A*
⟨*proof*⟩

lemma *int-set-content-dvd-shift*:
assumes *x* $\in$ *A*
shows *int-set-content A dvd x* $-$ *Min A*
⟨*proof*⟩

lemma *int-set-content-dvd-shifted*:
assumes *s* $\in$ *shifted-int-set A*
shows *int-set-content A dvd s*
⟨*proof*⟩

lemma *card-ge2-imp-Min-less-Max*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows *Min A* $<$ *Max A*
⟨*proof*⟩

lemma *int-set-content-pos*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows $0 <$ *int-set-content A*
⟨*proof*⟩

lemma *normalized-int-set-reconstruction*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows *affine-image-int* (*Min A*) (*int-set-content A*) (*normalized-int-set A*) $=$ *A*
⟨*proof*⟩

lemma *card-normalized-int-set*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows *card* (*normalized-int-set A*) $=$ *card A*
⟨*proof*⟩

lemma *card-sumset-normalized-int-set*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows *card* (*sumset* (*normalized-int-set A*) (*normalized-int-set A*)) $=$
    card (*sumset A A*)
⟨*proof*⟩

lemma *zero-in-normalized-int-set*:
  assumes *finite A* **and** $A \neq \{\}$
  shows $0 \in$ *normalized-int-set A*
⟨*proof*⟩

lemma *normalized-int-set-nonneg*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  assumes *x-in*: $x \in$ *normalized-int-set A*
  shows $0 \le x$
⟨*proof*⟩

lemma *Gcd-normalized-int-set*:
  assumes *fin*: *finite A* **and** *card-ge2*: $2 \le$ *card A*
  shows *Gcd* (*normalized-int-set A*) $= 1$
⟨*proof*⟩

lemma *group-closure-eq-UNIV-of-Gcd-one*:
  fixes *A* :: *int set*
  assumes *Gcd A* $= 1$
  shows *group-closure A* $=$ *UNIV*
  ⟨*proof*⟩

lemma *common-divisor-dvd-one-of-Gcd-one*:
  fixes *A* :: *int set*
  assumes *gcd-one*: *Gcd A* $= 1$
  assumes *dvd-all*: $\bigwedge a.\ a \in A \Longrightarrow d$ *dvd* a
  shows *d dvd* (*1* :: *int*)
⟨*proof*⟩

lemma *dvd-of-dvd-mod-and-modulus*:
  fixes *a n d* :: *int*
  assumes *d-n*: *d dvd n*
  assumes *d-mod*: *d dvd* (*a mod n*)

shows *d dvd a*
⟨*proof*⟩

lemma *Gcd-one-not-all-mod-multiples-of-proper-divisor*:
fixes *A* :: *int set*
assumes *gcd-one*: *Gcd A = 1*
assumes *d-gt-one*: *1 < d*
assumes *d-n*: *d dvd n*
assumes *residues*: $\bigwedge a.\ a \in A \Longrightarrow d\ dvd\ (a\ mod\ n)$
shows *False*
⟨*proof*⟩

lemma *normalized-mod-image-subset-stabilizer-contradicts-Gcd-one*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: $3 \le card\ A$
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
assumes *gcd-one*: *Gcd A = 1*
assumes *small-doubling*: $card\ (sumset\ A\ A) \le 3 * card\ A - 4$
assumes *stable-nonempty*: $stable\text{-}sum\text{-}holes\ A \neq \{\}$
defines $n \equiv Max\ A$
defines $B \equiv mod\text{-}image\text{-}int\ n\ A$
defines $p \equiv nat\ n$
defines $C \equiv Zmod.sumset\ p\ B\ B$
assumes *B-subset-H*: $B \subseteq Zmod.stabilizer\ p\ C$
shows *False*
⟨*proof*⟩

lemma *Min-normalized-int-set*:
assumes *fin*: *finite A* **and** *card-ge2*: $2 \le card\ A$
shows *Min* (*normalized-int-set A*) = *0*
⟨*proof*⟩

lemma *affine-image-int-subset-ap*:
assumes $A \subseteq int\text{-}ap\text{-}segment\ a\ d\ n$
shows $affine\text{-}image\text{-}int\ c\ e\ A \subseteq int\text{-}ap\text{-}segment\ (c + e * a)\ (e * d)\ n$
⟨*proof*⟩

4.7 Progression covers

definition *progression-cover-length-at-most* :: *int set* ⇒ *nat* ⇒ *bool* **where**
progression-cover-length-at-most A L ⟷
$(\exists\, a\ d\ n.\ 0 < d \wedge A \subseteq int\text{-}ap\text{-}segment\ a\ d\ n \wedge n \le L)$

lemma *progression-cover-length-at-mostI*:
assumes $0 < d$ **and** $A \subseteq int\text{-}ap\text{-}segment\ a\ d\ n$ **and** $n \le L$
shows *progression-cover-length-at-most A L*
⟨*proof*⟩

lemma *progression-cover-length-at-mostE*:
assumes *progression-cover-length-at-most A L*
obtains *a d n* **where** $0 < d$ $A \subseteq int\text{-}ap\text{-}segment\ a\ d\ n$ $n \le L$
⟨*proof*⟩

lemma *progression-cover-length-at-most-mono*:
assumes *cover*: *progression-cover-length-at-most A L*
assumes *le*: $L \le M$
shows *progression-cover-length-at-most A M*

⟨*proof*⟩

lemma *progression-cover-of-diameter-bound*:
  assumes *fin*: *finite A*
  assumes *nonempty*: $A \neq \{\}$
  assumes *len-le*: *nat* (*Max A* − *Min A* + *1*) ≤ *L*
  shows *progression-cover-length-at-most A L*
⟨*proof*⟩

lemma *progression-cover-affine-image-pos*:
  assumes *cover*: *progression-cover-length-at-most A L*
  assumes *e-pos*: *0* < *e*
  shows *progression-cover-length-at-most* (*affine-image-int c e A*) *L*
⟨*proof*⟩

theorem *freiman-3k-minus-4-from-diameter-bound*:
  assumes *fin*: *finite A*
  assumes *card-ge*: *3* ≤ *card A*
  assumes *diameter-le*: *nat* (*Max A* − *Min A* + *1*) ≤ *card* (*sumset A A*) − *card A* + *1*
  shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-max-bound*:
  assumes *fin*: *finite A*
  assumes *card-ge*: *3* ≤ *card A*
  assumes *zero*: *0* ∈ *A*
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  assumes *max-bound*: *nat* (*Max A* + *1*) ≤ *card* (*sumset A A*) − *card A* + *1*
  shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-hole-contribution*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *card-ge*: *3* ≤ *card A*
  assumes *zero*: *0* ∈ *A*
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  assumes *hole-cover*:
    card (*interval-holes A*) ≤ *card* (*lower-sum-holes A*) + *card* (*upper-sum-holes A*)
  shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-no-stable-sum-holes*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *card-ge*: *3* ≤ *card A*
  assumes *zero*: *0* ∈ *A*
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  assumes *stable-empty*: *stable-sum-holes A* = {}
  shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-short-diameter*:
  fixes *A* :: *int set*
  assumes *fin*: *finite A*
  assumes *card-ge*: *3* ≤ *card A*
  assumes *zero*: *0* ∈ *A*
  assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \le x$
  assumes *short*: *nat* (*Max A*) ≤ *2* ∗ *card A* − *3*

shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-stable-hole-contribution*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: *3* ≤ *card A*
assumes *zero*: *0* ∈ *A*
assumes *nonneg*: ⋀*x*. *x* ∈ *A* ⟹ *0* ≤ *x*
assumes *small-doubling*: *card* (*sumset A A*) ≤ *3* ∗ *card A* − *4*
assumes *stable-contribution*:
stable-sum-holes A ≠ {} ⟹
card A − *2* ≤ *card* (*lower-sum-holes A*) + *card* (*upper-sum-holes A*)
shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

lemma *normalized-stabilizer-count*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: *3* ≤ *card A*
assumes *zero*: *0* ∈ *A*
assumes *nonneg*: ⋀*x*. *x* ∈ *A* ⟹ *0* ≤ *x*
defines *n* ≡ *Max A*
defines *B* ≡ *mod-image-int n A*
defines *p* ≡ *nat n*
defines *C* ≡ *Zmod.sumset p B B*
defines *H* ≡ *Zmod.stabilizer p C*
defines *D* ≡ *Zmod.sumset p B H*
assumes *not-subset*: ¬ *B* ⊆ *H*
shows *card H* ≤
1 + *card* (*lower-sum-holes A* ∩ *upper-sum-holes A*) +
2 ∗ (*card D* − *card B*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-stabilizer-count*:
fixes *A* :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: *3* ≤ *card A*
assumes *zero*: *0* ∈ *A*
assumes *nonneg*: ⋀*x*. *x* ∈ *A* ⟹ *0* ≤ *x*
assumes *gcd-one*: *Gcd A* = *1*
assumes *small-doubling*: *card* (*sumset A A*) ≤ *3* ∗ *card A* − *4*
defines *n* ≡ *Max A*
defines *B* ≡ *mod-image-int n A*
defines *p* ≡ *nat n*
defines *C* ≡ *Zmod.sumset p B B*
defines *H* ≡ *Zmod.stabilizer p C*
defines *D* ≡ *Zmod.sumset p B H*
assumes *stabilizer-count*:
stable-sum-holes A ≠ {} ⟹
¬ *B* ⊆ *H* ⟹
card H ≤
1 + *card* (*lower-sum-holes A* ∩ *upper-sum-holes A*) +
2 ∗ (*card D* − *card B*)
shows *progression-cover-length-at-most A* (*card* (*sumset A A*) − *card A* + *1*)
⟨*proof*⟩

theorem *normalized-progression-cover-from-gcd-one*:
fixes *A* :: *int set*

assumes *fin*: *finite A*
assumes *card-ge*: $3 \leq$ *card A*
assumes *zero*: $0 \in A$
assumes *nonneg*: $\bigwedge x.\ x \in A \Longrightarrow 0 \leq x$
assumes *gcd-one*: *Gcd A* $= 1$
assumes *small-doubling*: *card* (*sumset A A*) $\leq 3 *$ *card A* $- 4$
shows *progression-cover-length-at-most A* (*card* (*sumset A A*) $-$ *card A* $+ 1$)
⟨*proof*⟩

theorem *freiman-3k-minus-4-from-normalized-core*:
assumes *core*:
$\bigwedge B.$ *finite B* $\Longrightarrow$
$3 \leq$ *card B* $\Longrightarrow$
$0 \in B \Longrightarrow$
$(\bigwedge x.\ x \in B \Longrightarrow 0 \leq x) \Longrightarrow$
Gcd B $= 1 \Longrightarrow$
card (*sumset B B*) $\leq 3 *$ *card B* $- 4 \Longrightarrow$
progression-cover-length-at-most B (*card* (*sumset B B*) $-$ *card B* $+ 1$)
assumes *fin*: *finite A*
assumes *card-ge*: $3 \leq$ *card A*
assumes *small-doubling*: *card* (*sumset A A*) $\leq 3 *$ *card A* $- 4$
shows *progression-cover-length-at-most A* (*card* (*sumset A A*) $-$ *card A* $+ 1$)
⟨*proof*⟩

4.8 The target statement

The AFP-facing statement combines the normalization lemmas above with the additive-combinatorial core proof: a finite integer set A with *card* (*sumset A A*) $\leq 3 *$ *card A* $- 4$ and $3 \leq$ *card A* is contained in an arithmetic progression of length at most *card* (*sumset A A*) $-$ *card A* $+ 1$.

theorem *freiman-3k-minus-4*:
fixes A :: *int set*
assumes *fin*: *finite A*
assumes *card-ge*: $3 \leq$ *card A*
assumes *small-doubling*: *card* (*sumset A A*) $\leq 3 *$ *card A* $- 4$
shows *progression-cover-length-at-most A* (*card* (*sumset A A*) $-$ *card A* $+ 1$)
⟨*proof*⟩

end

References

[1] M. B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, 1996.

[2] T. Tao and V. H. Vu. *Additive Combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2006. DOI: https://doi.org/10.1017/CBO9780511755149.