INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8(2) (2008), #A4

# ADDITIVE BASES REPRESENTATIONS IN GROUPS

**L. Haddad**
*120 rue de Charonne, 75011 Paris, France*
labib.haddad@wanadoo.fr

**C. Helou**[1]
*Penn State University, 25 Yearsley Mill Rd, Media, PA 19063, USA*
cxh22@psu.edu

*Received:1/2/07, Accepted: 4/27/07, Published: 8/1/08*

**Abstract**

We show that the additive group of any finite field $K$ of characteristic $\neq 2$ has a basis for which the number of representations of the elements of the field is bounded by a constant independent of $K$. We also establish a similar result for the additive group of any vector space $V$ over a field of characteristic $\neq 2$. Moreover, if $V$ is infinite, then the number of such representations never exceeds 2. We further prove that every modular group $\mathbb{Z}/n\mathbb{Z}$ has a basis for which the number of representations is bounded independently from $n$. Thus, in all these additive groups, the analogue of the Erdős-Turán conjecture for $\mathbb{N}$ fails to hold.

*– To Mel Nathanson on his 60th birthday*

## 1. Introduction

The analogue of the Erdős-Turán conjecture [1, 2, 4], about the unboundedness of the number of representations by an additive basis of the natural numbers $\mathbb{N} = \{0, 1, \dots\}$, does not, in general, hold in abelian groups. This was first established by Puš [9], then remarkably extended by Nathanson [8]. To measure the extent to which it fails in a given semigroup $S$, we introduce the invariant $\tau(S)$, lying in $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$. First, for a subset $A$ of $S$ and for $x \in S$, the number of representations of $x$ by $A$ is $r(A, x) = |\{(a, b) \in A \times A : a + b = x\}|$, and $A$ is called a basis of $S$ if $r(A, x) > 0$ for all $x \in S$. Let $s(A) = \sup\{r(A, x) : x \in S\}$. Then define $\tau(S) = \inf\{s(A) : A \in \mathbb{B}(S)\}$, where $\mathbb{B}(S)$ is the set of all bases of $S$. Clearly, $\tau(S) \geq 2$

[1]Corresponding author

for a nontrivial $S$, and the minimum is attained in many cases. Thus, while the Erdős-Turán conjecture asserts that for the additive semigroup $\mathbb{N}$, we should have $\tau(\mathbb{N}) = \infty$, it follows from [7] that $\tau(\mathbb{Z}) = 2$, for the group of rational integers $\mathbb{Z}$.

Here, we give explicit bases for the additive group of the product of two fields, for which the number of representations is effectively bounded under proper conditions. In particular, $\tau(K \times K) = 2$ if $K$ is an algebraically closed field of characteristic $\neq 2$ and $\tau(K \times K) \leq 18$ if $K$ is a finite field of odd characteristic. We deduce that $\tau(V) = 2$ for the additive group of any infinite vector space $V$ over a field of characteristic $\neq 2$. We also point to a simple relation between $\tau(\mathbb{N})$ and the sequence of $\tau(\mathbb{Z}/m\mathbb{Z})$, for the positive integers $m$ and the corresponding modular groups $\mathbb{Z}/m\mathbb{Z}$, and using a method of Ruzsa [10], we prove that $\tau(\mathbb{Z}/m\mathbb{Z})$ is bounded by a constant independent of $m$ (that is to say, absolutely bounded) . We conclude that $\tau(\mathbb{F}_q)$ is also absolutely bounded, for all finite fields $\mathbb{F}_q$ of odd characteristic. More generally, we deduce that $\tau(V)$ is absolutely bounded for the additive group of any vector space $V$ over any field $K$ of characteristic $\neq 2$.

## 2. Preliminary Results

Let $S$ be an additive abelian semigroup, and $A, B$ two subsets of $S$. For any $x \in S$, let $R(A, B; x) = \{(a, b) \in A \times B : a + b = x\}$ and $r(A, B; x) = |R(A, B; x)|$, where $|E|$ denotes the cardinality of the set $E$ in $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$. Let $s(A, B) = \sup\{r(A, B; x) : x \in S\}$. In particular, if $A = B$, we write $R(A, x), r(A, x)$ and $s(A)$ for $R(A, A; x)$, $r(A, A; x)$ and $s(A, A)$, respectively. The *sumset* of $A$ and $B$ is defined as $A + B = \{a + b : (a, b) \in A \times B\}$. We say that $B$ is a *basis* of $A$ if $B \subset A \subset B + B$. The set of all bases of $A$ is denoted by $\mathbb{B}(A)$. Now we define $\tau(A) = \inf\{s(B) : B \in \mathbb{B}(A)\}$, in $\overline{\mathbb{N}}$.

All intervals considered hereafter are in the set $\mathbb{Z}$ of rational integers. The function $n \mapsto \tau([0, n])$, from $\mathbb{N}$ into itself, is an increasing function which satisfies the property $\sup\{\tau([0, n]) : n \in \mathbb{N}\} = \tau(\mathbb{N})$ (see [2]).

The following simple results will be needed in the sequel.

**Lemma 2.1.** *Let $S$ and $T$ be additive abelian semigroups.*

(1) *If $A = \bigcup_i A_i$ and $B = \bigcup_j B_j$ are unions of two families $(A_i)$ and $(B_j)$ of subsets of $S$, then $s(A, B) \leq \sum_{i,j} s(A_i, B_j)$.*
(2) *If $S$ is a group, $A, B$ are subsets of $S$, and $u, v \in S$, then $s(u + A, v + B) = s(A, B)$.*
(3) *If $S \times T$ is the product semigroup of $S$ and $T$, then $\tau(S \times T) \leq \tau(S)\tau(T)$.*

*Proof.* (1) From the definitions, $R(A, B; x) = \bigcup_{i,j} R(A_i, B_j; x)$, so $r(A, B; x) \leq \sum_{i,j} r(A_i, B_j; x)$,

for all $x \in S$. The first inequality follows.

(2) For any $x \in S$, we have $R(u+A, v+B; x) = R(A, B; x-u-v)$, and thus $r(u+A, v+B; x) = r(A, B; x-u-v)$. Since $x \mapsto x-u-v$ is a permutation of the group $S$, the equality follows upon taking the supremum for $x \in S$, i.e. for $y = x-u-v$ ranging in $S$.

(3) For any $A \in \mathbb{B}(S)$ and $B \in \mathbb{B}(T)$, we have $A \times B \in \mathbb{B}(S \times T)$, and therefore $\tau(S \times T) \le s(A \times B)$. Moreover, $r(A \times B, (s,t)) = r(A,s)r(B,t)$ for all $(s,t) \in S \times T$, and thus $s(A \times B) = s(A)s(B)$. The last inequality follows. □

## 3. Products of Fields

Let $K$ be a field. We denote by $K^* = K \setminus \{0\}$ the multiplicative group of $K$, by $\mathbb{S}(K^*) = \{x^2 : x \in K^*\}$ the subgroup of the square elements of $K^*$, and by $\iota(K) = (K^* : \mathbb{S}(K^*))$ the index of the subgroup $\mathbb{S}(K^*)$ in the group $K^*$. We also write $\mathbb{S}(K) = \mathbb{S}(K^*) \cup \{0\}$ for the set of all the squares in $K$. We consider the product group $K \times K$, of the additive group of $K$ by itself, and the subsets $A(u) = \{(x, ux^2) : x \in K\}$ of $K \times K$, where $u \in K$.

**Proposition 3.1.** *Let $K$ be a field of characteristic $\neq 2$. Let $t \in K \setminus \{0, -1\}$, and set $u = 1+t$, $v = 1+1/t$ and $w = u+v$. We then have*

(1) $w \cdot \mathbb{S}(K) = t \cdot \mathbb{S}(K)$.
(2) $A(u) + A(v) = \{(a,b) \in K \times K : (b-a^2) \in t \cdot \mathbb{S}(K)\}$.
(3) $s(A(u)) = s(A(u), A(v)) = s(A(v)) = 2$.

*Proof.* (1) Clearly, $uv = u+v = w = (1+t)^2/t \neq 0$, so that $wt = (1+t)^2 \in \mathbb{S}(K^*)$. Therefore $w$ and $t$ are in the same coset of $\mathbb{S}(K^*)$ in $K^*$, and thus $w \cdot \mathbb{S}(K) = t \cdot \mathbb{S}(K)$.

(2-3) For any $u, v \in K$ such that $u+v \neq 0$, the set $A(u)+A(v)$ consists of the elements $(a,b) \in K \times K$ for which there exist $x, y \in K$ satisfying $x+y = a$ and $ux^2 + vy^2 = b$, i.e. such that the quadratic equation $ux^2 + v(a-x)^2 - b = 0$ has a solution $x$ in $K$. This is equivalent to its discriminant $b(u+v) - a^2uv$ (to within a factor of 4) being a square in $K$. Moreover, the equation has at most two solutions in $K$, and it has exactly two in some cases such as for $a = 0$ and $b = u+v$, so that $s(A(u), A(v)) = 2$. In particular, for the choice of $u$ and $v$ made here, $(a,b)$ lies in $A(u)+A(v)$ if and only if $w(b-a^2)$ is a square in $K$, i.e. $(b-a^2)$ lies in $w \cdot \mathbb{S}(K) = t \cdot \mathbb{S}(K)$. Moreover, since $2u$, $2v$ and $u+v$ are nonzero, $s(A(u)) = s(A(v)) = s(A(u), A(v)) = 2$. □

**Theorem 3.2.** *Let $K$ be a field of characteristic $\neq 2$ in which the index $\iota(K)$ is finite, equal to $n$. Let $\{t_i : 1 \le i \le n\}$ be a set of coset representatives of $\mathbb{S}(K^*)$ in $K^*$, with $t_1 = 1$, and assume that they satisfy the following conditions:*

*(H)* $(t_i+1)(t_i+t_j+2)\left(t_i+\frac{1}{t_j}+2\right)\left(\frac{1}{t_i}+\frac{1}{t_j}+2\right)\neq 0$, *for all* $1\leq i,j\leq n$.

*Set* $u_i=1+t_i$ *and* $v_i=1+\frac{1}{t_i}$, *for* $1\leq i\leq n$. *Then* $B=\bigcup_{i=1}^n (A(u_i)\cup A(v_i))$ *is a basis of the additive group* $K\times K$ *and* $s(B)\leq 2(2n-1)^2$.

*Proof.* By assumption, $K^*=\bigcup_{i=1}^n t_i\cdot\mathbb{S}(K^*)$ and therefore $K=\bigcup_{i=1}^n t_i\cdot\mathbb{S}(K)$. Hence, for any $(a,b)\in K\times K$, there exists $i\in\{1,\dots,n\}$ such that $(b-a^2)\in t_i\cdot\mathbb{S}(K)$, and therefore, in view of 3.1, $(a,b)\in A(u_i)+A(v_i)$. Thus $K\times K\subset\bigcup_{i=1}^n (A(u_i)+A(v_i))\subset B+B$, i.e. $B$ is a basis of $K\times K$. Moreover, the conditions (H) translate into: $u_i\neq 0,\ v_i\neq 0,\ u_i+u_j\neq 0,\ u_i+v_j\neq 0$ and $v_i+v_j\neq 0$, for all $1\leq i,j\leq n$. So, by 3.1, $s(A(u_i),A(u_j))=s(A(u_i),A(v_j))=s(A(v_i),A(v_j))=2$, for all $i,j$. Note also that, since $t_1=1$, we have $u_1=v_1=2$. Thus $B$ is a union of at most $2n-1$ distinct sets of the type $A(w_k)$, with $\{w_1,w_2,\dots,w_{2n-1}\}=\{u_1,u_2,v_2,\dots,u_n,v_n\}$ and $s(A(w_k),A(w_l))=2$, for all $1\leq k,l\leq 2n-1$. Hence, by 2.1, $s(B)\leq\sum_{1\leq k,l\leq 2n-1} s(A(w_k),A(w_l))=2(2n-1)^2$. □

**Remark 3.3.** For a field $K$, if the index $\iota(K)$ is finite, then it is a power of 2, since the quotient group $K^*/\mathbb{S}(K^*)$ is a 2-group (see [6]). In particular, if $K$ is algebraically closed, this index is 1. If $K$ is a finite field of characteristic $\neq 2$, this index is 2, since the map $x\mapsto x^2$ induces a group isomorphism from $K^*/\{\pm 1\}$ onto $\mathbb{S}(K^*)$. Note further that, given any power of 2, there exist fields $K$ for which the index $\iota(K)$ is equal to that power of 2. The index can also be infinite as in the case of the field $\mathbb{Q}$ of rational numbers.

**Corollary 3.4.** *Let* $K$ *be a field of characteristic* $\neq 2$ *in which the index* $\iota(K)$ *is finite, equal to* $n$. *Then the additive group of* $K\times K$ *satisfies* $\tau(K\times K)\leq 2(2n-1)^2$.

*In particular, if* $K$ *is finite, then* $\tau(K\times K)\leq 18$.

*Proof.* If $K$ is infinite, every coset $t\cdot\mathbb{S}(K^*)$ of $\mathbb{S}(K^*)$ in $K^*$ is infinite, so that we may choose the coset representatives $t_i$ in 3.2 to satisfy the conditions (H). Hence the existence of a basis $B$ of $K\times K$ such that $s(B)\leq 2(2n-1)^2$.

If $K$ is finite, then $n=2$, as noted in 3.3. So the conditions (H) boil down to the following ones: each of $t_2+1,\ t_2+3,\ 3t_2+1$ is not zero, where $t_2$ lies in $K^*\setminus\mathbb{S}(K^*)$. These can be easily satisfied whenever $|K|\geq 7$. Indeed, if $K=\mathbb{F}_7=\mathbb{Z}/7\mathbb{Z}$, then $K^*\setminus\mathbb{S}(K^*)=\{3,5,6\}$, and we may take $t_2=3$ or 5. Otherwise, $|K|\geq 9$ and $K^*\setminus\mathbb{S}(K^*)$ contains 4 or more elements, among which one at least satisfies the three conditions imposed on $t_2$. So, by 3.2, the additive group $K\times K$ has a basis $B$ such that $s(B)\leq 18$. There remain the cases of $K=\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$, with $p=3$ or 5, where direct constructions yield bases $B$ of $K\times K$ with $s(B)$ smaller than 18 (e.g. $B=A\times A$, where $A=\{0,1,2\}$). □

**Corollary 3.5.** *If $K$ is an algebraically closed field of characteristic $\neq 2$, then $\tau(K \times K) = 2$.*

This is just a special case of 3.4, in which the index $\iota(K) = 1$.

**Remark 3.6.** If the characteristic of $K$ is 2, then the above results are not in general valid, since in that case, for any subset $B$ of $K \times K$, we have $s(B) = r(B, (0,0)) = |B|$.

The cases where $K$ is either algebraically closed or is a finite field are contained in [3].

## 4. Modular Groups and Finite Fields

For a positive integer $m$, we consider the quotient ring $\mathbb{Z}/m\mathbb{Z}$ and the canonical homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, defined by $\pi(x) = \bar{x} = x + m\mathbb{Z}$ (in $\mathbb{Z}/m\mathbb{Z}$) for any $x \in \mathbb{Z}$.

**Proposition 4.1.** *Let $m$ be a positive integer and $A$ a finite non-empty subset of $\mathbb{N}$, with $a = \min(A)$ and $b = \max(A)$. Let $C = \pi(A)$.*

(1) *For any $n \in \mathbb{N}$, we have $r(C, \bar{n}) \leq \sum_{k\in\mathbb{Z}} r(A, n + km)$.*

*Moreover, $s(C) \leq ([2(b-a)/m] + 1) \cdot s(A)$, where $[x]$ is the largest integer $\leq x$, for a real number $x$.*

(2) *If the restriction of $\pi$ to $A$ is injective (e.g. if $m > b - a$), then, for all $n \in \mathbb{N}$, we have $r(A, n) \leq r(C, \bar{n}) = \sum_{k\in\mathbb{Z}} r(A, n + km)$, and thus $s(A) \leq s(C)$.*

(3) *If $m > b$, then $r(C, \bar{n}) = r(A, n) + r(A, n + m)$ for $0 \leq n < m$, and thus $s(C) \leq 2 \cdot s(A)$.*

(4) *If $m > 2b$, then $r(C, \bar{n}) = r(A, n)$ for $0 \leq n < m$, and thus $s(C) = s(A)$.*

(5) *If $A \in \mathbb{B}([0, m-1])$, then $C \in \mathbb{B}(\mathbb{Z}/m\mathbb{Z})$ and $s(A) \leq s(C) \leq 2s(A)$.*

*Proof.* (1) We have $R(C, \bar{n}) = \{(\bar{x}, \bar{y}) \in C \times C : \bar{x} + \bar{y} = \bar{n}\} = \bigcup_{k\in\mathbb{Z}} \{(\bar{x}, \bar{y}) \in C \times C : x + y = n + km\} = \pi \times \pi \left(\bigcup_{k\in\mathbb{Z}} R(A, n + km)\right)$, so that $r(C, \bar{n}) \leq \sum_{k\in\mathbb{Z}} r(A, n + km)$. Moreover, the latter summation can be restricted to the integers $k$ in the interval $[(2a-n)/m, (2b-n)/m]$, since $r(A, n+km) = 0$ for $n+km$ outside $[2a, 2b]$ which contains $A+A$. But the number of integers $k$ in the former interval is $\leq [2(b-a)/m]+1$. Hence $\sum_{k\in\mathbb{Z}} r(A, n+km) \leq ([2(b-a)/m]+1) \cdot s(A)$, and the result follows.

(2) In this case, the map $\pi$ induces a bijection from $A$ onto $C$, so that, in view of the proof of (1), $R(C, \bar{n})$ is in bijection, via $\pi \times \pi$, with the disjoint union of sets $\bigcup_{k\in\mathbb{Z}} R(A, n + km)$. This yields the result.

(3) and (4) follow from (2), since $r(A, x) = 0$ for $x > 2b$ or $x < 0$.

(5) follows from (2) and (3). $\square$

**Corollary 4.2.** *For any positive integer $m$, we have $\tau(\mathbb{Z}/m\mathbb{Z}) \leq 2\tau([0, m-1])$.*

Indeed, by 4.1, (5), for any $A \in \mathbb{B}([0, m-1])$, we have $\pi(A) \in \mathbb{B}(\mathbb{Z}/m\mathbb{Z})$ and $s(\pi(A)) \leq 2s(A)$, which yields the result.

**Corollary 4.3.** *We have* $\sup\{\tau(\mathbb{Z}/m\mathbb{Z}) : m \geq 1\} \leq 2\tau(\mathbb{N})$.

This follows from 4.2 and the property $\tau(\mathbb{N}) = \sup\{\tau([0, n]) : n \in \mathbb{N}\}$, established in ([2], 3.4).

**Remark 4.4.** In view of 4.3, if the sequence $(\tau(\mathbb{Z}/m\mathbb{Z}))_{m\geq 1}$ were unbounded, then $\tau(\mathbb{N})$ would be infinite, i.e. the Erdős-Turán conjecture in $\mathbb{N}$ would hold. However, as will be shown below, this is not the case.

**Definition 4.5.** For a subset $E$ of $\mathbb{Z}$, the *size* of $E$ is the number of its elements, the *interior size* of $E$ is the largest size of intervals contained in $E$, and the *exterior size* of $E$ is the smallest size of intervals containing $E$. The three "sizes" coincide when $E$ is an interval of $\mathbb{Z}$.

**Lemma 4.6.** *Let $n$ be a positive integer, $C$ a subset of $\mathbb{Z}$ and $B = \pi(C)$.*

(1) *If the interior size of $C + C$ is $\geq n$, then $B$ is a basis of $\mathbb{Z}/n\mathbb{Z}$.*
(2) *If the exterior size of $C + C$ is $\leq qn$, for some positive integer $q$, then $s(B) \leq q \cdot s(C)$.*

*Proof.* (1) In the first case, $C + C \supset I$ where $I$ is an interval of size $n$. Hence $B + B = \pi(C + C) \supset \pi(I) = \mathbb{Z}/n\mathbb{Z}$, so that $B$ is a basis of $\mathbb{Z}/n\mathbb{Z}$.

(2) In the second case, $C+C \subset J$ where $J$ is an interval of size $qn$. Hence, for any $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, we have $R(B, \bar{x}) = \pi \times \pi(\bigcup_{y\in Y} R(C, y))$, where $Y = \pi^{-1}(\bar{x}) \cap (C+C) \subset \pi^{-1}(\bar{x}) \cap J$, and $|Y| \leq |\pi^{-1}(\bar{x}) \cap J| = |\{x+kn \in J : k \in \mathbb{Z}\}| \leq q$ since $|J| = qn$. Therefore $r(B, \bar{x}) \leq |Y| \cdot s(C) \leq q \cdot s(C)$, for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, and the result follows. □

The following result is an adaptation of section 3 of Ruzsa's paper [10].

**Proposition 4.7.** *For any odd prime number $p$, there exists a subset $C$ of $\mathbb{Z}$ of exterior size $\leq 4p^2$ such that the interior size of $C + C$ is $\geq 2p^2$ and $s(C) \leq 288$.*

*Proof.* We identify the elements of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with the integers $0, 1, \ldots, p-1$, consider the additive group $G = \mathbb{F}_p \times \mathbb{F}_p$ and define the map $f : G \to \mathbb{Z}$ by $f(a, b) = a + 2pb$. Then $f$ is an injective map and $f(G) \subset [0, 2p^2 - p[$.

For any elements $(s,t),(v,w),(s',t'),(v',w')$ in $G$, if $f(s,t)+f(v,w)=f(s',t')+f(v',w')$, then $(s,t)+(v,w)=(s',t')+(v',w')$. Indeed, the first equality implies that $|2p(t+w-t'-w')| = |s'+v'-s-v| < 2p$, so that $t+w-t'-w'=s'+v'-s-v=0$, which yields the second equality. It follows that $s(f(X)) \leq s(X)$, for any subset $X$ of $G$.

By 3.4, there exists a basis $B$ of $G$ such that $s(B) \leq 18$. Let $A = f(B)$. Then $s(A) \leq s(B) \leq 18$. Given $n \in \mathbb{N}$, let $a, b \in \mathbb{N}$ be such that $n = a + 2pb$ and $0 \leq a < 2p$ (Euclidean division), and let $(\bar{a}, \bar{b})$ be the canonical image of $(a,b)$ in $G$, i.e. $\bar{a} \equiv a \pmod{p}$ and $\bar{b} \equiv b \pmod{p}$, where $0 \leq \bar{a}, \bar{b} \leq p-1$. Since $B$ is a basis of $G$, there exist two elements $(x,y)$ and $(x',y')$ in $B$ such that $(x,y)+(x',y')=(\bar{a},\bar{b})$, so that $x+x' \equiv a \pmod{p},\ y+y' \equiv b \pmod{p}$ and $0 \leq x+x',\ y+y' \leq 2(p-1)$. Therefore $x+x'-a=ip$ and $y+y'-b=jp$, with integers $i,j$ such that $-2 < i \leq 1$ and $-b/p \leq j \leq 1$. In particular, if $n$ lies in the interval $[0, 2p^2[$, then $b < p$ and $-1 < j \leq 1$. Moreover, setting $u = f(x,y)$ and $u' = f(x',y')$, we have $u, u' \in A$ and $u+u'-n = x+x'-a+2p(y+y'-b) = ip + 2jp^2$, with $-1 \leq i \leq 1$ and $0 \leq j \leq 1$, so that $n-(u+u')$ lies in $E = \{-2p^2-p, -2p^2, -2p^2+p, -p, 0, p\}$. Thus every integer $n \in [0, 2p^2[$ lies in the set $A+A+E$.

Let $D = \{-2p^2, -p, 0, p\}$ and $C = A+D$. Since $D+D \supset E$, then $C+C$ contains $A+A+E$, which contains $[0, 2p^2[$, so that the interior size of $C+C$ is $\geq 2p^2$. Since $A \subset f(G) \subset [0, 2p^2-p[$, then $C$ is contained in $[-2p^2, 2p^2[$, so that the exterior size of $C$ is $\leq 4p^2$. Moreover, $C$ being the union of 4 translates of $A$, by 2.1, we have $s(C) \leq 4^2 s(A) \leq 16 \cdot 18$. $\square$

**Theorem 4.8.** *There exists an absolute constant $c > 1$ such that $\tau(\mathbb{Z}/n\mathbb{Z}) \leq c$, for all positive integers $n$.*

*Proof.* Assume first that $n \geq 8$. Let $m = [\sqrt{n/2}]$. By Bertrand's postulate [5], there exists an odd prime number $p$ such that $m < p \leq 2m$. Then $n \leq 2p^2$ and $p^2 \leq 2n$. By 4.7, there exists a subset $C$ of $\mathbb{Z}$ of exterior size $\leq 4p^2 \leq 8n$ such that the interior size of $C+C$ is $\geq 2p^2 \geq n$ and $s(C) \leq 288$. So, by 4.6, the canonical image $B = \pi(C)$ of $C$ is a basis of $\mathbb{Z}/n\mathbb{Z}$, and $s(B) \leq 8 \cdot s(C) \leq 8 \cdot 288 = c$. Hence $\tau(\mathbb{Z}/n\mathbb{Z}) \leq c$ for $n \geq 8$, and the inequality holds trivially for $n < 8$. $\square$

**Corollary 4.9.** *The additive group of any finite field $F$ of characteristic $\neq 2$ satisfies $\tau(F) \leq 18c$. Thus $\tau(F)$ is absolutely bounded over the class of all such finite fields $F$.*

*Proof.* Let $F = \mathbb{F}_q$ be a finite field of characteristic $p \neq 2$, with $q = p^n$ elements, where $n$ is the dimension of $\mathbb{F}_q$ over $\mathbb{F}_p$.

If $n$ is even, $n = 2m$ with an integer $m > 0$, then $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ as an $\mathbb{F}_p$-vector space and as an additive group. Hence $\tau(\mathbb{F}_q) = \tau(\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}) \leq 18$, by 3.4.

If $n$ is odd, $n = 2m + 1$ with an integer $m \geq 0$, then $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_{p^{2m}} \times \mathbb{F}_p$. Hence $\tau(\mathbb{F}_q) = \tau(\mathbb{F}_{p^{2m}} \times \mathbb{F}_p) \leq \tau(\mathbb{F}_{p^{2m}})\tau(\mathbb{F}_p) \leq 18\tau(\mathbb{F}_p) \leq 18c$, in view of 2.1, the above result for $n$ even, and 4.8. $\square$

**Remark 4.10.** The value of the absolute constant $c = 8 \cdot 288 = 2304$, which appears in 4.8 and 4.9, can presumably be lowered. Some examples of values for $\mathbb{Z}/n\mathbb{Z}$ are:

$$\tau(\mathbb{Z}/n\mathbb{Z}) = \begin{cases} 2, & \text{if} \quad n = 2, 3 \\ 3, & \text{if} \quad n = 4, 5, 7 \\ 4, & \text{if} \quad n = 6 \quad \text{or} \quad 8 \leq n \leq 15 \\ 5, & \text{if} \quad 16 \leq n \leq 19 \quad \text{or} \quad n = 23 \\ 6, & \text{if} \quad n = 20, 21, 22, 24, 25 \end{cases}$$

Furthermore, in view of the inequality in 4.2 and the computations made in [2], we have
$\tau(\mathbb{Z}/n\mathbb{Z}) \leq 8$ for $n \leq 46$,
$\tau(\mathbb{Z}/n\mathbb{Z}) \leq 10$ for $n \leq 60$,
$\tau(\mathbb{Z}/n\mathbb{Z}) \leq 12$ for $n \leq 224$.

## 5. Vector Spaces

**Theorem 5.1.** *If $V$ is an infinite vector space over a field $K$ of characteristic $\neq 2$, then the additive group of $V$ satisfies $\tau(V) = 2$.*

*Proof.* Let $F$ be the prime subfield of $K$.

If $V$ is uncountable, then it is infinite-dimensional over $F$. Hence $V$ is isomorphic to $V \times V$ as a vector space over $F$. Now, there is an algebraically closed field $L$ which is an extension of the field $F$ and such that $V$ is isomorphic to $L$ as a vector space over $F$. So $V$ and $L \times L$ are isomorphic as vector spaces over $F$ and, therefore, also as abelian groups. Thus $\tau(V) = \tau(L \times L) = 2$, in view of 3.5. Indeed, the field $L$ can be obtained as follows. By adjoining to $F$ enough transcendental elements over $F$, one gets a field extension $E$, purely transcendental over $F$, isomorphic to $V$ as a vector space over $F$. Now the algebraic closure $L$ of $E$ has the same cardinality as $E$ (see [6]), hence the equality between degrees $[L : F] = [E : F]$, since $E$ is uncountable and $F$ is countable. So $L$ is isomorphic to $E$, and thus to $V$, as a vector space over $F$.

If $V$ is denumerable, then the additive group of $V$ is a countably infinite abelian group such that the set $\{2v : v \in V\}$ is infinite (since the characteristic of $K$ is not 2), so that by [8], $V$ has a basis $B$ such that $s(B) = 2$, and therefore $\tau(V) = 2$. $\square$

**Corollary 5.2.** *The additive group of any vector space $V$ over a field $K$ of characteristic $\neq 2$ satisfies $\tau(V) \leq 18c$, where $c$ is the absolute constant in 4.8.*

*Thus $\tau(V)$ is absolutely bounded over the class of all such vector spaces $V$.*

*Proof.* If $V$ is infinite, then $\tau(V) = 2$ by 5.1. On the other hand, the additive group of a finite vector space V over a field K is isomorphic to the additive group of a finite field with the same characteristic, and the result follows from 4.9. □

**Corollary 5.3.** *The invariant $\tau(K)$ is absolutely bounded over the class of all fields $K$ of characteristic $\neq 2$. In particular, if $K$ is infinite, then $\tau(K) = 2$.*

## References


1. P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212-215; MR 3,270e.

2. G. Grekos, L. Haddad, C. Helou, J. Pihko, *On the Erdős-Turán conjecture*, J. Number Theory **102** (2003), 339-352.

3. L. Haddad and C. Helou, *Bases in some additive groups and the Erdős-Turán conjecture*, J. Combinatorial Theory, series A **108** (2004), 147–153.

4. H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford, 1966; MR 35 1565.

5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edition, Oxford University Press, 1979; MR 81i:10002.

6. S. Lang, *Algebra*, Revised third edition, Springer, New York, 2002; MR 2003e:00003.

7. M. B. Nathanson, *Unique representation bases for the integers*, Acta Arith. **108** (2003), 1-8.

8. M. B. Nathanson, *Representation functions of additive bases for abelian semigroups*, Int. J. Math. Math. Sci. **2004:30** (2004), 1589–1597.

9. V. Puš, *On multiplicative bases in abelian groups*, Czech. Math. J. **41** (1991), 282-287.

10. I. Z. Ruzsa, *A just basis*, Monatsh. Math. **109** (1990), 145-151; MR 91e:11016.