Squarefree arithmetic Sequences

Helmut Preininger
1200 Vienna
Austria
March 20, 2017
mailto: helmut.preininger@chello.at
hosted at: www.vixra.org

Abstract

This paper introduces the notion of an S-Structure (short for Squarefree Structure.) After establishing a few simple properties of such S-Structures, we investigate the squarefree natural numbers as a primary example. In this subset of natural numbers we consider "arithmetic" sequences with varying initial elements. It turns out that these sequences are always periodic. We will give an upper bound for the minimal and maximal points of these periods.

1 Motivation

We start with the natural numbers and define the "core" operation.

Definition 1. *Let $\mathcal{P}$ the set of all primes of $\mathbb{N}$ and $a \in \mathbb{N}$ with $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$. The **core** of a is defined as*

$$\operatorname{core}(a) := \prod_{v_p(a)\ odd} p$$

Let $\mathbb{S}$ the positive squarefree elements of $\mathbb{N}$. Now we define two operations an this set and call the structure $(\mathbb{S}, \otimes, \oplus)$ the S-Structure of $\mathbb{Z}$.

Definition 2. *The multiplication $\otimes$ is defined as*

$$\begin{array}{rrcl} \otimes: & \mathbb{S}\times\mathbb{S} & \to & \mathbb{S} \\ & a\otimes b & \mapsto & \frac{ab}{\gcd^2(a,b)} \end{array}$$

Definition 3. *The addition $\oplus$ is defined as*

$$\begin{array}{rrcl} \oplus: & \mathbb{S}\times\mathbb{S} & \to & \mathbb{S} \\ & a\oplus b & \mapsto & \operatorname{core}(a+b) \end{array}$$

Theorem 4. *The structure $(\mathbb{S}, \otimes)$ is a group.*

Proof. Let $a, b \in \mathbb{S}$.

- The neutral element is 1.
- The operation $\otimes$ is closed since $\frac{ab}{\gcd(ab)}$ is also positive and squarefree.
- The operation $\otimes$ is associative since the ring multiplication is associative.
- The existence of an inverse element: $a \otimes a = 1$.
- The operation $\otimes$ is commutative since the ring multiplication is commutative.

$\square$

Theorem 5. *Let $a, b \in \mathbb{S}$. The structure $(\mathbb{S}, \oplus)$ is closed and commutative.*

Proof. The operation $\oplus$ is closed over $\mathbb{S}$ since $\mathrm{core}(a+b)$ is positive and squarefree. The operation $\oplus$ is commutative since the ring addition is commutative. $\square$

Unfortunately, the distribution law does not hold and $\oplus$ is not associative.

2 General definition of an S-Structure

In this paper $(R, +, \cdot)$ will always be a factorial ring with $char(R) = 0$.

We now define the "core" operation. Later we use it as additional step in the usual ring addition. If possible, we choose a subset $\mathbb{S} \subseteq R$ which admits an S-Structure $(\mathbb{S}, \otimes, \oplus)$. In other words, we choose a system $\mathcal{P}$ of representatives of primes and appropriate units $\mathcal{U}$ so that we can define a set $\mathbb{S}$ of squarefree elements and an S-Structure $(\mathbb{S}, \otimes, \oplus)$.

Definition 6. *[**core**] Let $a \in R$ with $a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$, where u_a is a unit in R. The **core** of a in R is defined as*

$$\mathrm{core}(a) := u_a \prod_{v_p(a)\ odd} p$$

Definition 7. *[**The set** $\mathbb{S}$] Let $\mathcal{P}$ a set of primes of R and $\mathcal{U}$ a set of units of R. We define $\mathbb{S} := \{a \in R | u_a \prod_{p \in \mathcal{P} p} \wedge u_a \in \mathcal{U}\}$.*

Now we define the S-Structure..

Definition 8. *[**S-Structure**] Let $\mathbb{S} \subseteq R$. An S-Structure of R is a triple $(\mathbb{S}, \otimes, \oplus)$ with the following properties*

- $(\mathbb{S}, \otimes)$ *is a commutative group with 1 as neutral element and*

$$\begin{array}{rccc} \otimes: & \mathbb{S} \times \mathbb{S} & \rightarrow & \mathbb{S} \\ & a \otimes b & \mapsto & \frac{ab}{\gcd^2(a,b)} \end{array}$$

- $(\mathbb{S}, \oplus)$ *is a closed, commutative binary operation in* $\mathbb{S}$ *and*

$$\begin{array}{rccl} \oplus: & \mathbb{S} \times \mathbb{S} & \to & \mathbb{S} \\ & a \oplus b & \mapsto & \operatorname{core}(a+b) \end{array}$$

Perhaps not every ring R admits an S-Structure, but the situation is not bad.

Theorem 9. *If R is also an ordered ring, then R admits an S-Structure.*

Proof. Choose a representative system $\mathcal{P}$ of positive primes and a appropriate set of units and create $\mathbb{S}$. Since the ring operations respect the order (i.e., $\forall a, b \in R$ hold $(a, b > 0) \Rightarrow (ab > 0)$ and $(a, b > 0) \Rightarrow (a + b > 0)$), we end up with an S-Structure. $\square$

Another sort of an ring that admits an S-Structure is the following

Example 10. *Let $R = K[X]$ where K is an ordered field. Choose a system $\mathcal{P}$ of irreducible polynomials with a constant term one and the set of units $\mathcal{U} = \{u \in K | u > 0\}$. The S-Structure given by $\mathbb{S} = \{P = a_n X^n + a_{n-1} X^n + \cdots + a_1 X + a_0 \in K[X] : a_0 > 0 \wedge \operatorname{core}(P) = P\}$*

2.1 Some basic properties

If we choose a ring R and try to establish an S-Structure in it, there is the following crucial condition

Lemma 11. *If $a \in \mathbb{S}$ then $-a \notin \mathbb{S}$.*

Proof. We have $a \oplus (-a) = 0$. But $0 \notin \mathbb{S}$ because 0 has in $(\mathbb{S}, \otimes)$ no inverse. $\square$

In the following let $\mathbb{S}$ be an S-Structure of R.

Lemma 12. *Let $a, b \in \mathbb{S}$ and $m, n \in \mathbb{N}$. Then*

$$\operatorname{core}(a^n \cdot b^m) = \operatorname{core}(a^n) \otimes \operatorname{core}(b^m)$$

Proof. Let $a = b = p$ with $p \in \mathbb{S}$ and p is prime in R, then

$$\operatorname{core}(p^n \cdot p^m) = \operatorname{core}(p^{n+m}) = p^{(n+m) \mod 2}$$

and

$$\operatorname{core}(p^n) \otimes \operatorname{core}(p^m) = p^{n \mod 2} \otimes p^{m \mod 2} = p^{((n \mod 2)+(m \mod 2)) \mod 2)} = p^{(n+m) \mod 2}$$

$\square$

The next lemma gives a relation between the $\otimes$ and $\oplus$ operations. Obviously, this relation is much weaker as the relation between the operations of the ring R.

Lemma 13. *Let $a, b \in \mathbb{S}$*

$$(a \oplus b) = \gcd(a,b) \otimes \operatorname{core}\left(\frac{a+b}{\gcd(a,b)}\right)$$

Proof. Let $a, b \in \mathbb{S}$

$$a \oplus b = \operatorname{core}(a+b) = \operatorname{core}\left(\gcd(a,b) \cdot \frac{a+b}{\gcd(a,b)}\right)$$

With the above lemma we get

$$\operatorname{core}\left(\gcd(a,b) \cdot \frac{a+b}{\gcd(a,b)}\right) = \operatorname{core}(\gcd(a,b)) \otimes \operatorname{core}\left(\frac{a+b}{\gcd(a,b)}\right)$$

and with $\operatorname{core}(\gcd(a,b)) = \gcd(a,b)$

$$\operatorname{core}(\gcd(a,b)) \otimes \operatorname{core}\left(\frac{a+b}{\gcd(a,b)}\right) = \gcd(a,b) \otimes \operatorname{core}\left(\frac{a+b}{\gcd(a,b)}\right)$$

□

In an S-Structure holds a week " distribution law ".

Proposition 14. *Let $a, b \in \mathbb{S}$*

$$a \otimes (b \oplus b) = (a \otimes b) \oplus (a \otimes b)$$

Proof. Since $(\mathbb{S}, \otimes)$ is a group, $(\mathbb{S}, \otimes)$ is also associative.
With the above lemma and $c \in \mathbb{S}$ we get

$$c \oplus c = \gcd(c,c) \otimes \operatorname{core}\left(\frac{c+c}{\gcd(c,c)}\right) = c \otimes \operatorname{core}(2)$$

Therefore the left hand side is

$$a \otimes (b \oplus b) = a \otimes (b \otimes \operatorname{core}(2)) = a \otimes b \otimes \operatorname{core}(2)$$

and the right hand side is

$$(a \otimes b) \oplus (a \otimes b) = (a \otimes b) \otimes \operatorname{core}(2) = a \otimes b \otimes \operatorname{core}(2).$$

□

3 Arithmetic sequences in $(\mathbb{S}, \oplus)$.

In this section we investigate the S-Structure, $(\mathbb{S}, \otimes, \oplus)$, on $\mathbb{N}$ in more detail.

Notation

- $\overrightarrow{\mathbf{b}}$:= a vector with n dimensions and $b_k \in \mathbb{S}$, $i = k, \ldots, n$.
- $\mathbf{F}\left(\overrightarrow{\mathbf{b}}\right)$:= Set of the sequences a_i with arbitrary starting value $a_0 \in \mathbb{S}$ and $a_{i+1} := a_i \oplus b_k$, where
$$k = \begin{cases} 1 & i \equiv 0 \mod n \\ (i \mod n) + 1 & elsewhere \end{cases}$$
Set
- $\mathbf{M}(\overrightarrow{\mathbf{b}})$:= Set of the minimal Elements of the cycles of $F(\overrightarrow{b})$ (with arbitrary starting value).
- $\mathbf{N}(\overrightarrow{\mathbf{b}})$:= Set of the maximal elements of the cycles of $F(\overrightarrow{b})$ (with arbitrary starting value).
- $\kappa_{\mathbf{p}}$:= Let p a prime and fix $\overrightarrow{b}$. Assume p^2 is the first possible reduction (i.e., $p^2 \cdot \text{core}(a_i) = a_i$) in a subsequence of $F(\overrightarrow{b})$ with arbitrary starting value $a_0 \in \mathbb{S}$. Then κ_p is the maximal index with $p^2 | \kappa_p$.

4 Upper bounds for $\max(M(b))$ and $\max(N(b))$ with $\dim(b) = n$.

In this section we fix $n \in \mathbb{N}$ and let $\overrightarrow{b} = (b_k)_{k \in \{1,\ldots,n\}}$ a vector of elements of $\mathbb{S}$.

Lemma 15. *Let p a prime. In every subsequence of $F(\overrightarrow{b})$ with $\dim(\overrightarrow{b}) = n$ hold*

$$\kappa_p \leq \left(p^2 - 1\right) \cdot n$$

or

$$\kappa = \infty$$

Proof. We only consider the elements $a_{i+k\cdot n}$, $k = 0, \ldots, p^2 - 1$. That gives p^2 possible remainders (i.e. $a_{i+k\cdot n} \mod p^2$). If there occur a reduction it must be on an index $i = 1, \ldots, (p^2 - 1)n$, or never. We have to consider the elements $a_{i+k\cdot n}$ because it must hold for arbitrary b_i. $\square$

Theorem 16. *Consider a sequence $F(\overrightarrow{b})$ with $\dim(\overrightarrow{b}) = n$ and let $c = \sum_{i=1}^{n} b_i$.*

1. *Let p_c the minimal prime with $p_c \nmid c$ then $\kappa_{p_c} \leq (p_c^2 - 1)\, n$.*

2. *For every $F(\overrightarrow{b})$ hold*

   (a) $\max(M(\overrightarrow{b})) \leq c$

   (b) $\max(N(\overrightarrow{b})) \leq (p_c^2 - 1)\, c$

Proof. ad 1: Lemma 15 implies $\kappa_p \leq (p^2 - 1) \cdot n$ or $\kappa = \infty$. With $\gcd(p_c, c) = 1$ follows $\kappa_p \leq (p^2 - 1) \cdot n$.
ad 2a, 2b: We use again lemma 15. We take only the elements $a_{i+k\cdot n}$, $k = 1, \ldots, (p^2-1)$. We consider the worst case of the reduction and estimate the value of a_i where $(a_i + (p^2-1)c)p^2 \geq a_i$. If a_i is greater the sequence shrinks after a reduction. // We have:

$$\begin{aligned} \frac{a_i + (p^2-1)\, c}{p^2} &\geq a_i \\ \left(p^2 - 1\right) c &\geq \left(p^2 - 1\right) a_i \\ c &\geq a_i \end{aligned}$$

it follows $\max(M(\overrightarrow{b})) \leq c$ and $\max(N(\overrightarrow{b})) \leq (p_c^2 - 1)\, c$. □

Corollary 17. *If $c \notin M(\overrightarrow{b})$ then $(p_c^2 - 1)\, c \notin N(\overrightarrow{b})$.*

Theorem 18. *Let $F(\overrightarrow{b})$ and $F(\overrightarrow{b^*})$ two sets of sequences, where $\overrightarrow{b^*}$ is a cyclic permutation of $\overrightarrow{b}$.*
The finite sequence g_i is a cycle in $F(\overrightarrow{b})$ if and only if g_i is a cycle in $F(\overrightarrow{b^*})$.

Proof. We consider the sequence of one cycle. A cyclic permutation of the b_i in the vector $\overrightarrow{b}$ does not change the order of the additions. Let b_k, $k > 1$, the new b_1^* element of $\overrightarrow{b^*}$ and choose as the starting value b_{k-1}. □

5 Arithmetic sequences of the Form $F(b)$ with $\dim(b) = 1$.

Notation Later on we often consider sequences $a_i, \mathrm{core}(a_i + b) = a_{i+1}, \mathrm{core}(a_{i+1} + b) = a_{i+2}, \ldots$ and we use the following notation:
$a_i \rightarrow a_{i+1}, \rightarrow a_{i+2} \downarrow \mathrm{core}(a_{i+2}), \ldots$
We write $\cdots \rightarrow \ldots$ if $\mathrm{core}(a_i + b) = a_i + b$ and $\cdots \rightarrow .. \downarrow \ldots$ if a reduction occurs (i.e. $\mathrm{core}(a_i + b) < a_i + b$.

Lemma 19. *Let $g, p \in \mathbb{N}$, p is prime, $0 < g < p$ and $g \nmid p$. For all elements a_i in the sequence: $g \rightarrow (g+p) \rightarrow (g+2p) \rightarrow \ldots$ hold $p^2 \nmid a_i$ and there are only p distinct remainders possible.*

Proof. Since $g \nmid p$, $(g+kp) \equiv 0 \mod p^2$ is not possible and the remainders $0, p, 2p, \ldots, (p-1)p$ are shifted by g. $\square$

Theorem 20. *Let $q, b, m \in \mathbb{N}$ and g, p as in lemma 19 and $\gcd(p, q) = 1$. Let $G(q)$ the set of the first p elements of $gq + m \to (g + p)q + m \to (g + 2p)q + m \to \ldots$. Let $R(q)$ the set of the remainders of $(g + kp)q \equiv q \mod p^2$ with $0 \leq k < p$.*
There exists $f \in R(q)$, with $p^2|f$ if and only if there exists $t \in R(q)$ with $((m \mod p)+f) \equiv 0 \mod p^2$.

Proof. With lemma 19 there exists only p remainders and the are shifted. $\square$

5.1 Necessary property: $\gcd(b, 6) = 1$

Theorem 21. *Let $b \in \mathbb{S}$ and $\gcd(b, 6) = 1$. It follows*

- $\max(M(b)) = b$
- $\max(N(b)) = 3b$

Proof. Consider the sequence: $b \to 2b \to 3b \to 4b \downarrow b$. $\square$

5.2 Necessary property: $\gcd(b, 6) = 3$

Theorem 22. *Let $b \in \mathbb{S}$ and $\gcd(b, 6) = 3$. It follows*

1. $\max(M(b)) < b$
2. $\max(N(b)) < 3b$

Proof. Assume $b = 3q \in M(b)$.
1) Let $\max(M(b)) = b = 3q$. Consider the sequence $3q \to 6q \to 9q \downarrow q$. Contradiction
2) Corollary 17 implies $\max(N(b)) < 3b$. $\square$

Theorem 23. *Let $b \in \mathbb{S}$ and let $\gcd(b, 6 \cdot 5) = 3$. It follows*

1. $(2b/3) \leq \max(M(b))$
2. $2b/3 + m \notin M(b)$, *if* $m = 2, 4, 6, \ldots$
3. $2b/3 + m \notin M(b)$, *if* $((5b/3) \mod 4) \neq (m \mod 4)$ *and* $m = 1, 3, \ldots$
4. $2b/3 + m \notin M(b)$, *if* $b/3 \equiv 1, 4, 7 \mod 9$ *and* $m \equiv 1, 4, 7 \mod 9$
5. $2b/3 + m \notin M(b)$, *if* $b/3 \equiv 2, 5, 8 \mod 9$ *and* $m \equiv 2, 5, 8 \mod 9$
6. $b/3 \in M(b)$

Proof. Let $q = b/3$.
ad 1: Assume $2q \in M(b)$. Consider the sequence: $2q \to 5q \to 8q \downarrow 2q$ with $5 \nmid q$, i.e., $2q = 2b/3 \in M(b)$.
ad 2: Assume $2q + m \in M(b)$, if $m = 2, 6, 10, \ldots$. Consider the sequence $(2q + m) \downarrow \frac{2q+m}{4}$. Contradiction.
Assume $2q + m \in M(b)$, if $m = 4, 8, 12, \ldots$. Consider the sequence $2q + m \to 5q + m \to 8q + m \downarrow \frac{8q+m}{4}$. Since $2q + m > \frac{8q+m}{4}$ a contradiction.
ad 3: Assume $2q + m \in M(b)$,if $m = 1, 3, 5, \ldots$. Consider the sequence $2q + m \to 5q + m$, but, if $(q \mod 4) \neq (m \mod 4)$ then $4|(5q + m)$. Since $2q + m > \frac{5q+m}{4}$ a contradiction.
ad 4: Assume $2q + m \in M(b)$, if $q \equiv 1 \mod 9$ and $m \equiv 1 \mod 9$. Consider the remainder sequence and recall $3 \nmid q$: $2 + 1 \to 5 + 1 \to 8 + 1 \Rightarrow 9|(8q + m)$. Since $2q + m > \frac{8q+m}{9}$ a contradiction. Applies analogously to all other 8 combinations.
ad 5: Assume $2q + m \in M(b)$, $q \equiv 2 \mod 9$ and $m \equiv 2 \mod 9$. Consider the remainder sequences and recall $3 \nmid q$: $4 + 2 \to 10 + 2 \to 16 + 2 \Rightarrow 9|(8q + m)$. Since $2q + m > \frac{8q+m}{9}$ a contradiction. Applies analogously to all other 8 combinations.
ad 6: Consider the sequence $q \to 4q \downarrow q$. □

Remark 24. *In some cases $2b/3 = \max(M(b))$ is not valid. The smallest counterexamples are $b = 1023, 13107, 16383, 17391, 23529$.*

Theorem 25. *Let $b \in \mathbb{S}$ and let $\gcd(b, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 41) = 3 \cdot 5$. It follows*

1. *$11b/15 \in M(b)$.*
2. *$b \notin M(b)$.*
3. *$11b/15 + m \notin M(b)$, if $m = 2, 6, 10, \ldots$.*
4. *$11b/15 + m \notin M(b)$, if $m = 8, 16, 24, \ldots$.*
5. *$11b/15 + m \notin M(b)$, if $b/15 \equiv 1, 4, 7 \mod 9$ and $m \equiv 1, 4, 7 \mod 9$.*
6. *$11b/15 + m \notin M(b)$, if $b/15 \equiv 2, 5, 8 \mod 9$ and $m \equiv 2, 5, 8 \mod 9$.*

Proof. Let $q = b/15$ (recall $3 \nmid q$).
ad 1: Assume $11q \in M(b)$. Consider the sequence $11q \to 26q \to 41q \to 56q \downarrow 14q \to 29q \to 44q \downarrow 11q$, i.e., $11q \in M(b)$.
ad 2: Assume $15q \in M(b)$. Consider the sequence $15q \to 30q \to 45q \downarrow 5q$, a contradiction.
ad 3: Assume $11q+m \in M(b)$, $m = 2, 6, 10, \ldots$. Consider the sequence $11q+m \to 26q+m \downarrow \frac{26q+m}{4}$. Since $11q + m > \frac{26q+m}{4}$, a contradiction.
ad 4: Assume $11q + m \in M(b)$, if $m = 8, 16, 24, \ldots$. Consider the sequence $11q + m \to 26q + m \to 41q + m \to 56q + m \downarrow \frac{56q+m}{8}$. Since $11q + m > \frac{56q+m}{8}$, a contradiction.
ad 5: Assume $11q + m \in M(b)$,if $q \equiv 1 \mod 9$ and $m \equiv 1 \mod 9$. Consider the remainder sequence $11 + 1 \to 26 + 1 \Rightarrow 9|(26q + m)$. Since $11q + m > \frac{26q+m}{9}$ a contradiction. Applies analogously to all other 8 combinations.

ad 6: Assume $11q + m \in M(b)$, if $q \equiv 2 \mod 9$ and $m \equiv 2 \mod 9$. Consider the remainder sequence $22 + 2 \to 52 + 2 \Rightarrow 9|(26q + m)$. Since $11q + m > \frac{26q+m}{9}$ a contradiction. Applies analogously to all other 8 combinations. $\square$

Theorem 26. *Let $b \in \mathbb{S}$ and let $\gcd(b, 2 \cdot 3 \cdot 5 \cdot 7) = 3 \cdot 5 \cdot 7$. It follows*

1. $b/3 \in M(b)$.
2. $b/3 + m \notin M(b)$, *if* $(b/3 \mod 4) \neq (m \mod 4)$ *and* $m = 1, 3, 5, \ldots$.
3. $b/3 + m \notin M(b)$, *if* $m \equiv 0 \mod 4$.
4. $b/3 + m \notin M(b)$, *if* $(b/3 \mod 4) = (m \mod 4)$.
5. $b/3 + m \notin M(b)$, *if* $(b/3 \equiv 1, 4, 7 \mod 9)$ *and* $m \equiv 2, 5, 8 \mod 9$.
6. $b/3 + m \notin M(b)$, *if* $(b/3 \equiv 2, 5, 8 \mod 9)$ *and* $(m \equiv 1, 4, 7 \mod 9)$.

Proof. Let $q = b/3$ (recall $2 \nmid q$ and $3 \nmid q$). // ad 1: Assume $q \in M(b)$. Consider the sequence $q \to 4q \downarrow q$, i.e., $q \in M(b)$.
ad 2: Assume $q + m \in M(b)$, if $(q \mod 4) \neq (m \mod 4)$ and $m = 1, 3, 5, \ldots$. Consider the sequence $q + m \downarrow \frac{q+m}{4}$, a contradiction.
ad 3: Assume $q \in M(b)$, if $m \equiv 0 \mod 4)$. Consider the sequence $q + m \to 4q + m \downarrow \frac{4q+m}{4}$. Since $q + m > \frac{4q+m}{4}$, a contradiction.
ad 4: Assume $q + m \in M(b)$, if $(q \mod 4) = (m \mod 4)$. Consider the sequence $q + m \to 4q + m \to 7q + m \downarrow \frac{7q+m}{4}$.
ad 5: Assume $q + m \in M(b)$, if $q \equiv 1 \mod 9$ and $m \equiv 2 \mod 9$. Consider the remainder sequence $1 + 2 \to 4 + 2 \to 7 + 2 \Rightarrow 9|(7q + m)$. Since $q + m > \frac{7q+m}{9}$ a contradiction. Applies analogously to all other 8 combinations.
ad 6: Assume $q + m \in M(b)$, if $q \equiv 2 \mod 9)$ and $m \equiv 1 \mod 9)$. Consider the remainder sequence $2 + 1 \to 8 + 1 \Rightarrow \frac{8q+m}{9}$. Since $q + m > \frac{8q+m}{9}$, a contradiction. Applies analogously to all other 8 combinations. $\square$

Remark 27. *In some cases $b/3 = \max(M(b))$ is not valid. The smallest counterexamples are $b = 1365, 1785, 1995, 15015$.*

5.3 Necessary property $\gcd(b, 6) = 2$

Theorem 28. *Let $b \in \mathbb{S}$ and let $\gcd(b, 6) = 2$. It follows*

1. $\max(M(b)) < b$
2. $\max(N(b)) < 8b$

Proof. Assume, $\max(M(b) = b = 2q$.
ad 1: Consider the sequence $2q \to 4q \downarrow q$, a contradiction.
ad 2: Corollary 17 implies $\max(N(b)) < 8b$. $\square$

Theorem 29. *Let $b \in \mathbb{S}$ and let* $\gcd(b, 6 \cdot 5 \cdot 7) = 2$. *It follows*

1. $b/2 \in M(b)$
2. $b/2 + m \notin M(b)$, *if* $m = 1, 3, 5, \ldots$

Proof. Let $q = b/2$.
ad 1: Consider the sequence $q \to 3q \to 5q \to 7q \to 9q \downarrow q$.
ad 2: Assume $q + m \in M(b)$, if $m = 1, 3, 5, \ldots$. Consider the sequence $q + m \to 3q + m$. For all 4 remainder combinations it hold: either $4|(q + m)$ or $4|3q + m$, a contradiction. $\square$

Remark 30. *In some cases* $b/2 = \max(M(b))$ *is not valid. The smallest counterexample is* $b = 1342$.

5.4 Necessary property $\gcd(b, 6) = 6$

Theorem 31. *Let $b \in \mathbb{S}$ and* $\gcd(b, 6) = 6$. *It follows*

1. $\max(M(b)) < b$
2. $\max(N(b)) < (p_c^2 - 1)b$

Proof. Let $q = b/6$.
ad 1: Consider the sequence $6q \to 12q \downarrow 3q$
ad 2: Corollary 17 implies $\max(N(b)) < (p_c^2 - 1)b$. $\square$

Theorem 32. *Let $b \in \mathbb{S}$ and* $\gcd(b, 6 \cdot 7) = 6 \cdot 7$. *It follows*

1. $b/3 \in M(b)$
2. $b/3 + m \notin M(b)$, *if* $m = 2, 4, 6, \ldots$

Proof. Let $q = b/42$.
ad 1: Consider the sequence $14q \to 56q \downarrow 14q$
ad 2: Assume $m \equiv 2 \mod 4$. Consider the sequence $14q + m \downarrow \frac{14q+m}{4}$, a contradiction.
Assume $m \equiv 0 \mod 4$. Consider the sequence $14q + m \to 56q + m \downarrow \frac{56q+m}{4}$. Since $14q + m > \frac{56q+m}{4}$, a contradiction. $\square$

Remark 33. *In some cases* $b/3 = \max(M(b))$ *is not valid. The smallest counterexample is* $b = 1302$.

The theorems 23, 25, 26, 29 and 32 are special cases of a general theorem and it is easy to find more special cases.
Now the general

Theorem 34. *Let $m, c \in \mathbb{S}$ with $b \in M(c)$. Let $\mathcal{C}_m := (m_0, m_1, \ldots, m_k)$, with $m_0 = m$ and $m_{i+1} = m_i + c$, the cycle in $F(c)$. Let $b \in \mathbb{S}$, with $b = f\,c$ and $\forall_{m_i \in \mathcal{C}} \gcd(f, m_i) = 1$.
Then $m\,f \in M(b)$ and $f\,\mathcal{C}_m := (fm_0, fm_1, \ldots, fm_k)$ is a cycle in $F(b)$.*

Proof. Since $\forall_{m_i \in \mathcal{C}} \gcd(f, m_i) = 1$, f does not influence the sequence $m \to m + c \to \cdots \to m + kc \downarrow m$. Obviously f depends on b and m. $\square$