Distribution of the Residues and Cycle Counting.

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

Abstract

In this paper we take a closer look to the distribution of the residues of squarefree natural numbers and explain an algorithm to compute those distributions.
We also give some conjectures about the minimal number of cycles in the squarefree arithmetic progression and explain an algorithm to compute this minimal numbers.

1 Introduction

Distribution of the Residues: Let b be an arbitrary natural squarefree number. Now we ask, what is the distribution of the residues of b over all squarefree numbers. In opposite to the natural numbers, it turns out that the residues of squarefree numbers are not uniformly distributed. For example, the probability that an arbitrary squarefree number is even is $1/3$. We give a formula of the ratio of the occurrence of two residues of b if we count over all squarefree numbers. We explain an algorithm to compute these ratios.
Cycle Counting: We [PRE] introduced the notion of an S-Structure (short for squarefree structure) and took the squarefree natural numbers as primary example. We considered "arithmetic" sequences and their periodic cycles. Let $b, a \in \mathbb{S}$. An arithmetic sequence start with $a_0 = a$ and continue with $a_{i+1} = a_i \oplus b$ (i.e. the squarefree part of $a_i + b$). For every pair a, b we end up in a cycle (for details see [PRE]).
Here we give a short summary about an S-Structure. Every element of a factorial ring can be split into a squarefree and a squarefull part. Since this splitting is, in general, not unique, we took only a subset of this ring. We defined a new multiplication and a new addition, where we took the usual multiplication and addition and then skip the squarefull part of the result. In some sense, the addition and the multiplication switch their role. Unfortunately the new addition is no longer associative and therefore the distributive law is not valid.
In particular we considered the natural numbers in more detail and investigated the squarefree arithmetic sequences.
Now, we ask about the number of cycles of squarefree arithmetic sequences. We give an easy

and quite fast algorithm to compute the number of cycles. We state a bunch of conjectures but unfortunately for now we have no proofs.

2 Some notes about squarefree numbers

Before we consider the residues, we state two numeric properties of the natural squarefree numbers.

Well known is

$$\lim_{n\to\infty} \frac{\sum_{i=1,\, i \text{ is squarefree}}^{n} 1}{n} = \frac{6}{\pi^2}$$

(i.e. let $a \in \mathbb{N}$ an arbitrary natural number then a is with the probability $6/\pi^2$ squarefree)

2.1 The small primes dominate the value of the limit: Lower and upper bounds

We consider the sum $\sum_i \frac{1}{p_i^2}$, where the p_i's be primes. We give rough upper and lower bounds:

$$\frac{1}{4} \leq \sum_{i}^{\infty} \frac{1}{p_i^2} \leq \frac{1}{4} + \sum_{i=1}^{\infty} \frac{1}{(2i+1)^2} = \frac{1}{4} + \frac{\pi^2 - 8}{8}$$

Let $n > 1$ we get

$$\sum_{i}^{\infty} \frac{1}{p_i^2} \leq \sum_{1}^{n} \frac{1}{p_i^2} + \left(\frac{\pi^2 - 8}{8} - \sum_{k=1}^{(p_n-1)/2} \frac{1}{(2k+1)^2} \right) =: \sum_{1}^{n} \frac{1}{p_i^2} + A_n =: \alpha_{1,n} + A_n$$

and

$$\alpha_{1,n} \leq \alpha_1 := \sum_{i}^{\infty} \frac{1}{p_i^2} \leq \alpha_{1,n} + A_n$$

Now we compute the probability α that $c \in \mathbb{N}$ is not squarefree. A number $c \in \mathbb{N}$ is not squarefree if it exist a prime p with $p^2|c$. The compute the probability α we start with

$$\alpha \simeq \sum_{i=1}^{\infty} \frac{1}{p_i^2} =: \alpha_1$$

But we counted some numbers twice (i.e. numbers c where a pair of primes p_i, p_j exist, with $p_i^2 p_j^2 | c$). So we adjust the sum

$$\alpha \simeq \alpha_1 - \sum_{i=1, j>i}^{\infty} \frac{1}{p_i^2 p_j^2} =: \alpha_1 - \alpha_2$$

But in α_2 we counted again some numbers twice (i.e. numbers c where a triple of primes p_i, p_j, p_k exist, with $p_i^2 p_j^2 p_k^2 | c$). So we adjust the sum

$$\alpha \simeq \alpha_1 - \alpha_2 + \sum_{i=1, j>i, k>j}^{\infty} \frac{1}{p_i^2 p_j^2 p_k^2} =: \alpha_1 - \alpha_2 + \alpha_3$$

And so on ...
We end up with

$$\alpha = \sum_{i=1}^{\infty} (-1)^{i+1} \alpha_i$$

Now we consider α_2.

$$\alpha_2 = \sum_{i=1, j>i}^{\infty} \frac{1}{p_i^2 p_j^2} = \sum_{i=1}^{\infty} \frac{1}{p_i^2} \left(\sum_{j=i+1}^{\infty} \frac{1}{p_j^2} \right)$$

Let $\alpha_{2,n} = \sum_{i=1, j>i}^{n} \frac{1}{p_i^2 p_j^2}$ and use the upper bound of α_1.

$$\begin{aligned} \alpha_{2,n} \leq \alpha_2 &\leq (\alpha_{1,n} + A_n) \left(\sum_{j=i+1}^{n} \frac{1}{p_j^2} + A_n \right) \\ &= \alpha_{1,n} \sum_{j=i+1}^{n} \frac{1}{p_j^2} + \alpha_{1,n} A_n + A_n \sum_{j=i+1}^{n} \frac{1}{p_j^2} + A_n^2 \end{aligned}$$

Since $\sum_{i=n+1}^{\infty} \frac{1}{p_i^2} \leq A_n$ (i.e. sum up only primes p_j, with $j > n$), the term $A_n \sum_{j=i+1}^{n} \frac{1}{p_j^2}$ vanish, we get

$$\alpha_{2,n} \leq \alpha_2 \leq \alpha_{2,n} + \alpha_{1,n} A_n + A_n^2$$

This lead us to the

Proposition 1. *Let α_k and $\alpha_{k,n}$ be defined as above, with $n \geq k$. Then*

$$\alpha_{k,n} \leq \alpha_k \leq \alpha_{k,n} + \alpha_{k-1,n} A_n + \alpha_{k-2,n} A_n^2 + \cdots + \alpha_{1,n} A_n^{k-1} + A_n^k$$

Proof. We have

$$\alpha_k = \sum_{i_1=1}^{\infty} \frac{1}{p_{i_1}^2} \left(\sum_{i_2=i_1+1}^{\infty} \frac{1}{p_{i_2}^2} \cdots \left(\sum_{i_k=i_{k-1}}^{\infty} \frac{1}{p_{i_k}^2} \right) \cdots \right)$$

and

$$\alpha \leq \left(\sum_{i_1=1}^{n} \frac{1}{p_{i_1}^2} + A_n \right) \left(\left(\sum_{i_2=i_1+1}^{n} \frac{1}{p_{i_2}^2} + A_n \right) \left(\cdots \left(\sum_{i_k=i_{k-1}+1}^{n} \frac{1}{p_{i_k}^2} + A_n \right) \right) \cdots \right)$$

Note

$$\left(\sum_{i=1}^{n} \frac{1}{p_i^2}\right) A_n \neq A_n \left(\sum_{i=1}^{n} \frac{1}{p_i^2}\right)$$

Since $\sum_{i=n+1}^{\infty} \frac{1}{p_i^2} \leq A_n$ (i.e. sum up only primes p_j, with $j > n$), terms of the form $A_n \left(\sum_{i=1}^{n} \frac{1}{p_i^2}\right)$ vanish, we get the expected result. □

We have two parameters to control the limes: The number of primes and the number of terms of the approximation. We stick ourselves to the first three terms and count over the first $10, 20$ and 30 primes. We compute the lower and upper bound of the sum $\sum_{i=1}^{3} \alpha_i$:

$$\begin{aligned}
&\text{LowerBound} = \alpha_{1,n} - (\alpha_{2,n} + \alpha_{1,n} A_n + A_n^2) + \alpha_{3,n} \\
&\text{UpperBound} = (\alpha_{1,n} + A_n) - \alpha_{2,n} + (\alpha_{3,n} + \alpha_{2,n} A_n + \alpha_{1,n} A_n^2 + A_n^3)
\end{aligned}$$

The next table show the numerical results. We see, that the convergence is quite fast and the greater primes have low impact to the limes. We do not go deeper in this area, because we only want to give a first impression.

first n primes	LowerBound	Limes	UpperBound
10	0.3767967740	0.3920728981	0.4022854273
20	0.3839122477	0.3920728981	0.3944840555
30	0.3857284824	0.3920728981	0.3923967288

2.2 The convergence of $\lim_{n\to\infty} \frac{\sum_{i=1,\, i \textbf{ is squarefree}}^{n} 1}{n}$ is fast: Numerical tests.

To show this, we easily test the first n natural numbers and compute:

$$c = \frac{\sum_{i \text{ is squarefree}}^{n} 1}{n}$$

The next table show same numerical results of c in order to the first n natural numbers. Note the strange result for $n = 10000$. Again, we only want to give a first impression.

n	c	Limes
10	0.7000000000	0.6079271019
100	0.6100000000	0.6079271019
1000	0.6080000000	0.6079271019
10000	0.6083000000	0.6079271019
100000	0.6079400000	0.6079271019
1000000	0.6079260000	0.6079271019
10000000	0.6079291000	0.6079271019
100000000	0.6079269400	0.6079271019

3 Distribution of the Residues

Now we consider the following problem:
Let $b \in \mathbb{S}$ and $m \in \mathbb{N}$ with $0 \leq m < b$. We ask about the probability that an arbitrary $a \in \mathbb{S}$ is $a \equiv m \mod b$.
In other words. Let $b \in \mathbb{S}$ and $m \in \mathbb{N}$, $0 \leq m < b$, $a_0 = m$ and $a_{i+1} = a_i + b$ (the a_i's are natural numbers). Now we compute the

$$\lim_{n\to\infty} \frac{\sum_{i=0,\, a_i \text{ is squarefree}}^{n} 1}{n}$$

To do this, we need some

Notation 2. *Let $b \in \mathbb{S}$ and $i, j = 0, \dots, b-1$ the residues of b.*

1. *The ratio $R_{i,j} := [\#i : \#j] = r_i : r_j$ of residues, where, $\forall a \in \mathbb{S}$, $\#i = \sum_{a=1, a\equiv i \mod b}^{\infty} 1$.*
2. *Let S_m the set of numbers who are a product of exactly m different primes.*
3. *Let $\gamma_m \in S_m$ (note that γ_m is squarefree).*

Theorem 3. ***Ratios of the Residues*** *Fix $b \in \mathbb{S}$. Let $g_i = \gcd(b, i) = \prod_{k=1}^{m_i} p_k$, $0 \leq i < b$.*

$$r_i = b / \left(\sum_{k=0}^{m} (-1)^k \sum_{\gamma_k | g_i} \gamma_k \right)$$

Sketch of the proof:

1. The notes about squarefree numbers 2 lead us to the following assumption. The squarefree numbers are uniformly distributed in $\mathbb{N}$, therefore skip the factor $6/\pi$.
2. Split the natural numbers in consecutive intervals, such that each interval consist of b^2 consecutive numbers.
3. Fix i (i.e. fix a residue of b), $0 \leq i < b$. Let $a_0 = i$ and $a_{j+1} = a_j + b$ and consider

$$\lim_{n\to\infty} \frac{\sum_{j=0,\, a_j \text{ is squarefree}}^{n} 1}{n}$$

4. The non squarefree divisors of b^2 are periodic in b^2 with the period b^2. Therefore it is enough to consider only one interval.
5. In each interval there are b numbers with $a_j \equiv i \mod b$. Eliminate all a_j's, where a_j is a multiple of a non squarefree divisor of b^2.

□

Proof. (of Theorem 3) Since the elements of $\mathbb{S}$ are uniformly distributed, we can skip the factor $6/\pi$ and it is enough to consider the interval of natural numbers $[1, \ldots, b^2]$ (every interval with b^2 consecutive natural numbers is fine). We choose an interval with length b^2, since all divisors of b are periodic in b and therefore the quadratic divisors of b^2 are periodic in b^2. Let $a_{s,i} = s \cdot b + i$, $s = 0, \ldots, b$ and $1 \leq i < b$.
For every i we have the numbers $i, b+i, \ldots, (b-1)b+i$ and we eliminate all numbers that are, in respect to $b = \Pi_k^m p_k$, not squarefree (i.e. we eliminate numbers with at least one p_k, with $p_k^2 | a_{s,i}$).
Fix i, $1 \leq i < b$ let $g_i = \gcd(b, i) = \prod_{k=0}^{m_i} p_k$, with $p_0 = 1$, and then eliminate and count:
$k = 0$: In the interval are b numbers $a_{s,i}$. We have: $b = b / \sum_{\gamma_0 | g_i}$ (note, $\gamma_0 = 1$).
$k = 1$: Eliminate the $a_{s,i}$'s where a prime p exist with $p | a_{s,i}$ and $p | g_i$. We have

$$\sum_{p_k | g_i} \left(b^2 / \left(b \prod_{j \neq k} p_j \right) \right) = \sum_{\gamma_1 | g_i} \gamma_1$$

$a_{s,i}$ to eliminate.
$k = 2$: In the last step we eliminate some $a_{s,i}$ twice ($a_{s,i}$ where a $\gamma_2 | g_i$ exist). Therefore we sum up all those γ_2 and adjust the sum.
$k = 3$: In the last step we count some $a_{s,i}$ twice ($a_{s,i}$ where a $\gamma_3 | g_i$ exist). Therefore we sum up all those γ_3 and adjust the sum.
...
$k = n$: Sum up all those γ_n and adjust the sum.
... □

Corollary 4. *Let $b = p$ be prime. The corresponding r_i's are: $r_0 = p-1, r_1 = p, \ldots, r_{p-1} = p$.*

Proof. Since $\gcd(p, i) = 1$, $1 \leq i, p-1$, the corresponding r_i's are p. Except $\gcd(p, 0) = p$ (i.e. p^2 is not squarefree) and we have $r_0 = p - 1$. □

Corollary 5. *Assume the same setting as in theorem 3:*

1. *If $\gcd(b, j) = \gcd(b, i)$ then $r_j = r_i$.*
2. *If $i \in \mathbb{S}$ and the squarefree part of j is equal to i then $r_j = r_i$.*

Proposition 6. *Let $b = p$ be prime. The ratio $(\sum_{i=1}^{p-1} r_i) : r_0 = p : 1$.*

Proof. We have (Theorem 3) one residue 0 with $k_0 = p - 1$ and $p - 1$ residues with $k_i = p$. Therefore we get

$$\frac{p-1}{(p-1)p} = \frac{1}{p}$$

□

Proposition 6 implies, it is easy to compute that for $b = 2$ $r_0 : r_1 = 1 : 2$.
Theorem 3 implies, in the squarefree numbers the distribution of the residues, in opposition to $\mathbb{N}$, is no longer uniform.

Theorem 7. *Let $b \in \mathbb{S}$ with $b = \prod_{i=1}^{m} p_i$.*

$$\sum_{i=1}^{b-1} r_i : r_0 = \sum_{k=0}^{m-1} \sum_{\gamma_{m-k}|b} \gamma_{m-k} : 1$$

Sketch of the proof:

1. Induction over the number of primes of b.
2. Let $A_m = \sum_{k=0}^{m-1} \sum_{\gamma_{m-k}|b} \gamma_{m-k}$ and proof $A_{m+1} = p_{m+1}\left(A_m + 1\right) + A_m$
3. Let $r_0 = R_m$ and proof $R_{m+1} = R_m\left(p_{m+1} - 1\right)$
4. Let $S_m = R_m A_m$ and proof $S_{m+1} = A_{m+1} R_{m+1} = S_m(p_{m+1}^2 - 1) + p_{m+1} R_m (p_{m+1} - 1)$
5. Proof $S_m = \sum_{j=1}^{b-1} r_j$ for all $m \in \mathbb{N}$.

$\square$

Proof. (of Theorem 7) We proof the theorem by induction over the number of primes of b and split the proof into few steps.

Recursion: A_m
Claim 1: Let $A_1 = p$, $A_2 = p_1 p_2 + (p_1 + p_2)$ and $A_m = \sum_{k=0}^{m-1} \sum_{\gamma_{m-k}| \prod_{i=1}^{m} p_i} \gamma_{m-k}$, where the p_i's are distinct primes. Then

$$A_{m+1} = p_{m+1}\left(A_m + 1\right) + A_m \ , \ p_{m+1} \nmid \prod_{i=1}^{m} p_i$$

proof of Claim 1: We consider the elements of A_{m+1}. First, all elements of $A_m p_{m+1} \subset A_{m+1}$. Second, p_{m+1} is an element of A_{m+1}. Third, $A_m \subset A_{m+1}$. Since A_{m+1} has no more elements, this proofs claim 1.

Recursion: r_0
Claim 2: Let $R_1 = p - 1$, $R_2 = p_1 p_2 - (p_1 + p_2) + 1$ and $R_m = \sum_{k=0}^{m} (-1)^k \sum_{\gamma_{m-k}| \prod_{i=1}^{m}} \gamma_{m-k}$, where the p_i's are distinct primes. Then

$$R_{m+1} = R_m\left(p_{m+1} - 1\right) \ , \ p_{m+1} \nmid \prod_{i=1}^{m} p_i$$

proof of Claim 2: We consider the elements of R_{m+1}. First, all elements of $R_m p_{m+1} \subset R_{m+1}$. Second, p_{m+1} is already mentioned, since $(-1)^m \gamma_0 = (-1)^m$ is an element of R_m. Third, $-R_m \subset R_{m+1}$. Since R_{m+1} has no more elements, this proofs claim 2.

Recursion: $S_m = A_m R_m$
Claim 3: Let $S_1 = p(p-1) = A_1 R_1$, $S_2 = p_1 p_2 (p_1 p_2 - 1) = A_2 R_2$ and $S_m = \sum_{k=0}^{m-1} (-1)^k \sum_{\gamma_{m-k} | \prod_{i=1}^m p_i} \gamma_{m-k}(\gamma_{m-k} - 1)$. Assume $S_m = A_m R_m$ then

$$S_{m+1} = A_{m+1} R_{m+1} = S_m (p_{m+1}^2 - 1) + p_{m+1} R_m (p_{m+1} - 1)\ ,\ p_{m+1} \nmid \prod_{i=1}^{m} p_i$$

proof of Claim 3: First, we consider one term of S_m and R_m, $\gamma_k(\gamma_k - 1)$ and γ_k. We get

$$p_{m+1}^2 \gamma_k(\gamma_k - 1) + p_{m+1}\gamma_k(p_{m+1} - 1) =$$

$$p_{m+1}^2 \gamma_k^2 - p_{m+1}^2 \gamma_k + p_{m+1}^2 \gamma_k - p_{m+1}\gamma_k = p_{m+1}\gamma_k(p_{m+1}\gamma_k - 1)$$

Second, $-S_m \subset S_{m+1}$. Third, since $(-1)^m \in R_m$ we also get $(-1)^m p_{m+1}^2$ and $(-1)^{m+1} p_{m+1}$ as elements of S_{m+1}. Since S_{m+1} has no more elements, this proofs claim 3.

Show: $S_m = \sum_{j=1}^{b-1} r_j$
Claim 4: Let $b \in \mathbb{S}$ and let S_m compute form the primes $p_1, \ldots, p_m$, with $\prod_{i=1}^m p_i = b$. Then

$$S_m = \sum_{j=1}^{b-1} r_j$$

proof of claim 4: Let $b = \prod_{k=1}^m p_k$ and $1 \le i < b$. For every i, with $\gamma_k | i$, we get a term $(-1)^k b/\gamma_k$ as an element of r_i. There are $b/\gamma_k - 1$ terms with $\gamma_k | i$, $i = 1, \ldots, b-1$, and we get $b/\gamma_k(b/\gamma_k - 1)$, a term of S_m. This proofs claim 4.
The proof of the theorem is complete. □

Corollary 8. *Let $b \in \mathbb{S}$ and $b = \prod_{k=1}^m p_k$. Then*

$$\sum_{i=0}^{b-1} r_i = \sum_{k=0}^{m} (-1)^k \sum_{\gamma_{m-k} | b} \gamma_{m-k}^2$$

Proof. With Claim 3 in the proof of last theorem we have

$$\sum_{i=0}^{b-1} r_i = r_0 + \sum_{i=1}^{b-1} r_i = \sum_{k=0}^{m} (-1)^k \sum_{\gamma_{m-k} | b} \gamma_{m-k} + \sum_{k=1}^{m} (-1)^k \sum_{\gamma_{m-k} | b} \gamma_{m-k}(\gamma_{m-k} - 1)$$

$$= \sum_{k=0}^{m} (-1)^k \sum_{\gamma_{m-k} | b} \gamma_{m-k}^2$$

□

3.1 Compute the r_i's

A consequence of the proof of Theorem 3 is that it is easy to design an algorithm to compute all r_i's of a fixed $b \in \mathbb{S}$. We split the algorithm in two procedures, the recursive procedure: SumGamma() and the main procedure: ResidVector().

3.1.1 Procedure: SumGamma

Now we briefly describe Algorithm 3.1.1. Let $GcdPrimes()$ the list of primes of $\gcd(b, i)$ and every prime of $ListIndex(p)$ return the index of p in the list $GcdPrimes()$. We want to sum up all γ_n where one prime, p, of γ_n exist with $ListIndex(p) = StartIdx$ and all other primes, p_j, of γ_n have a $Listindex(p_j) > StartIdx$. The procedure $SumGamma()$ find recursively all possible γ_n's and sum them up.

Algorithm 1 Sum up γ_n

Require: $kSum = 0$ # a global variable: here we sum up the γ_n
Require: b # a global Variable: we consider the residues of b
Require: $GcdPrimes()$ # a global List of the primes of $\gcd(b, residue)$
  INPUT: $StartIdx$ point to the element of the list $GcdPrimes()$ with listindex $StartIdx$
  INPUT: n we want combinations of n primes all with listindex $\geq$ StartIdx
  INPUT: $Term$ if we have n primes then Term hold the value of γ_n
  OUTPUT: accumulate all γ_n in the global variable $kSum$
procedure SumGamma($StartIdx, n, Term$)
  if $n \geq 0$ **then** # the combination has less then n elements
    for $k \leftarrow StartIdx$ **to** $length(GcdPrimes())$ **do**
      SumGamma($k+1, n-1, Term \cdot GcdPrimes(k)$)
    end for
  else
    $kSum = b/Term$
  end if
end procedure

3.1.2 Procedure: ResidVector

Now we describe briefly the Algorithm 3.1.2. We compute a vector $\overrightarrow{r}$, with $\dim(\overrightarrow{r}) = b$ and $r(i) = r_i$ (see algorithm 3.1.2). For every residue i we sum up all γ's and compute the correspond r_i. Note: With Corollary 5, we can skip some computation.

4 Cycle counting

Let $b \in \mathbb{S}$, consider the arithmetic sequence of b and count the cycles.
The Kronecker symbol (the Legendre symbol is a special case) give us some hints.

Algorithm 2 Compute the vector r

Require: $kSum = 0$ # a global variable: here we sum up the γ_n
Require: b # a global Variable: we consider the residues of b
Require: $GcdPrimes()$ # a global List of the primes of $\gcd(b, residue)$
INPUT: tb we consider the residues of tb
OUTPUT: r The vector of all r_i's, $1 \leq i \leq b$

```
procedure ResidVector(tb)
    b ← tb  # set the global variable
    for kp ← 1 to b do  # loop over all residues
        r(kp) ← b  # The length(GcdPrimes) = 0 recursion
        kGcd ← Gcd(b, kp)
        if kGcd > 1 then
            if kGcd < kp then  # corollary 5
                r(kp) ← r(kGcd)
            else
                GcdPrimes() ← CollectPrimes(kGcd)  # Only primes of kGcd
                for ki ← 1, length(GcdPrimes()) do
                    kSum ← 0  # initialize kSum for every r_ki
                    SumGamma(1, ki, 1)
                    r(kp) ← r(kp) + (−1)^ki kSum
                end for
            end if
        end if
    end for
end procedure
```

Definition 9. *We define the Kronecker (or Kronecker-Jacobi) symbol* $\left(\frac{a}{b}\right)$ *for any* a *and* b *in* $\mathbb{Z}$ *in the following way.*

1. *If* $b = 0$*, then* $\left(\frac{a}{0}\right) = 1$ *if* $a = \pm 1$*, and equal to* 0 *otherwise.*

2. *For* $b \neq 0$*, write* $b = \Pi p$*, where the* p *are not necessarily distinct primes (including* $p = 2$*), or* $p = -1$ *to take care of sign. Then we set*

$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ *is the Legendre symbol for* $p > 2$*, and we define*

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \text{ is even} \\ (-1)^{(a^2-1)/8}, & \text{if } a \text{ is odd.} \end{cases}$$

and also

$$\left(\frac{a}{-1}\right) = \begin{cases} 1, & \text{if } a \geq 0 \\ -1, & \text{if } a < 0. \end{cases}$$

We summarize the properties of the Kronecker symbol. More details in [COH].

Theorem 10. *The Kronecker symbol has the following properties:*

1. $\left(\frac{a}{b}\right) = 0$ *if and only if* $\gcd(a, b) \neq 1$

2. *For all* a, b *and* c *we have*

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right), \ \left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right) \text{ if } bc \neq 0$$

3. $b \geq 0$ *being fixed, the symbol* $\left(\frac{a}{b}\right)$ *is periodic in* a *of period* $4b$ *if* $b \equiv 2 \mod 4$*, otherwise it is periodic of period* b*.*

4. $a \neq 0$ *being fixed (positive or negative), the symbol* $\left(\frac{a}{b}\right)$ *is periodic in* b *of period* $|a|$ *if* $a \equiv 0, 1 \mod 4$*, otherwise it is periodic of period* $4|a|$*.*

Notation 11. .
$\mathcal{E}_c$: *The set of the elements of one cycle* c*.*
$\mathcal{A}_c$: *The set of the elements of one cycle* c *in addition with it's attraction elements.*
$E_c = |\mathcal{E}_c|$: *The number of elements of one cycle* c*.*
$M(b)$: *The set of the minimal elements of all cycles of* b*.*
$C_b = |M(b)|$: *The number of the cycles of* b*.*
$\mathrm{core}(n)$: *The squarefree part of a natural number* n*.*

Lemma 12. *Let $a \in \mathbb{N}$, $p > 2$ a prime, and $p \nmid a$. If $\left(\frac{a}{p}\right) = 1, -1$. Then*

$$\left(\frac{a}{p}\right) = \left(\frac{\operatorname{core}(a)}{p}\right)$$

Proof. It hold, $a = q \operatorname{core}(a)$ where q is quadratic, but for a quadratic q term hold $\left(\frac{q}{p}\right) = 1$. Since the Kronecker symbol is multiplicative, the proof is complete. □

Theorem 13. *Let b a prime, $b > 3$. The number of cycles of b is $C_b \geq 3$.*

Proof. Since b is prime and $b > 3$, we have the cycle

$$b \to 2b \to 3b \to 4b \downarrow b$$

Lemma 12 shows, if b is a prime and $\forall a \in \mathbb{N}$ with $\left(\frac{a}{p}\right) = \{1, -1\}$ than $\left(\frac{a}{b}\right) = \left(\frac{\operatorname{core}(a)}{p}\right)$. Therefore it exists, at least, one cycle c such that $\left(\frac{a_i}{p}\right) = 1$ for all $a_i \in c$ and one cycle where $\left(\frac{a_i}{p}\right) = -1$. □

Theorem 14. *Let $b \in \mathbb{S}$ even, $\mathcal{E}_b$ the elements of a cycle of b where one element (and therefore all elements) $e_i \in \mathcal{E}_b$ $\left(\frac{e_i}{b}\right) \neq 0$. Then $E_b \equiv 0 \mod 4$.*

Proof. Since for all even numbers b of $\mathbb{S}$ we have $b \equiv 2 \mod 4$ and Theorem 10 says, that the Kronecker symbol is periodic in e_i of period $4b$, the theorem follows. □

Observation 15. *Let $b = p_c \cdot q$ where p_c is the smallest prime that divide b, and $q \geq 1$. Then the next table shows, for some primes p_c and $b \leq 33000$, the minimal number of cycles of $b = p_c \cdot q$.*

Prime p_c:	*2*	*3*	*5*	*7*	*11*	*13*	*17*	*19*	*23*	*29*
Cycles C_b:	*3**	*6***	*7*	*7*	*7*	*7*	*7*	*7*	*7*	*7*

**) Except for $b = 2 \cdot 5$ and $b = 2 \cdot 7$ which have 2 cycles.*
***) Except for $b = 3 \cdot 5$ which has 4 cycles.*

Conjecture 16. *Let $b \in \mathbb{S}$ and C_b the number of cycles of b.*

1. *If $C_b = 1$, then $b = 1, 2$.*
2. *If $C_b = 2$, then $b = 3, 10, 14$.*
3. *If $C_b = 3$ and b not prime, then $b = 2q$, with q prime.*

Conjecture 17. *Let $C_b = 4$ and b not prime then $b = 2q$ where $q = 5 \cdot 11, 7 \cdot 17, 7 \cdot 19$ or q prime.*

Conjecture 18. *Let $C_b = 5$ and b not prime then $b = 15$ or $b = 2q$ where $q = 3 \cdot 7, 5 \cdot 7, 3 \cdot 19, 7 \cdot 11, 5 \cdot 31, 5 \cdot 53, 7 \cdot 43, 5 \cdot 71$ or q prime.*

Conjecture 19. *Let $c_b = 6$ and b not prime then $\gcd(b, 6) \geq 2$.*
Let $c_b = 6$ and $b = 3q$ then q is prime.

4.1 Function: CountCycles

Now we briefly describe Algorithm 4.1. Since every cycle has an element $\leq b$ (see Theorem 21), we test only squarefree numbers $kInit$, with $1 \leq kInit \leq b$. Since the cycles (including their attraction regions) are distinct (see Lemma 20) we store in the bitvector $oldCyc$ all tested numbers a_i, represented as $oldCyc(a_i) = 1$.

Lemma 20. *Let $b \in \mathbb{S}$ and c_1, c_2 be two cycles of b with distinct minimal elements. Then*

$$\mathcal{A}_{c_1} \cap \mathcal{A}_{c_2} = \emptyset$$

Proof. Since, the result of $a \oplus b$ is unique, every starting value of an arithmetic sequence can end up in only one cycle. □

In ([PRE], Theorem 16) we proofed the following theorem:

Theorem 21. *The maximal element of $M(b)$ is $\leq b$.*

References

[COH] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 138, Springer Verlag, 1996.

[PRE] H. Preininger, *Squarefree Arithmetic Sequences*, 2017, www.vixra.org/pdf/1703.0192v1.pdf

Algorithm 3 CountCycles(): Compute the number of cycles of b

INPUT: a squarefree number
OUTPUT: the number of cycles

1: **function** COUNTCYCLES(b)
2:     # we need two BitVectors $Cyc()$ and $oldCyc()$, both with $dim = b$
3:     # $oldCyc()$ hold all old detected cycle elements
4:     # $Cyc()$ hold all new (and old) cycle elements
5:     $kInit \leftarrow 1$
6:     **loop**
7:         $kNow \leftarrow kInit$
8:         **loop**
9:             **if** $kNow \leq b$ **then**
10:                 **if** $oldCyc(kNow) = 1$ **then** # $kNow$ is element of an older cycle
11:                     **break** # goto line 21
12:                 **end if**
13:                 **if** $Cyc(kNow) = 1$ **then**
14:                     $kCnt \leftarrow kCnt + 1$ # one more cycle
15:                     **break** # goto line 21
16:                 **end if**
17:                 $Cyc(kNow) \leftarrow 1$ # otherwise set the element
18:             **end if**
19:             $kNow \leftarrow kNow \oplus b$ # compute the new element
20:         **end loop** # refresh the $oldCyc()$ vector
21:         $oldCyc() \leftarrow Copy(Cyc())$
22:         **while** $oldCyc(kInit) = 1$ **do**
23:             $kInit \leftarrow succ(kInit)$ # the next squarefree number
24:             **if** $kInit > b$ **then**
25:                 **break** 2 # goto line 29
26:             **end if**
27:         **end while**
28:     **end loop**
29:     **return** $kcnt$
30: **end function**