Sign-changes of the Thue-Morse Fractal Function and Dirichlet L-Series

Michael Drmota* **and Mariusz Skałba**** [1]

* Department of Algebra and Discrete Mathematics, Technical University of Vienna, Wiedner Hauptstrasse 8-10, A-1040 Vienna, Austria

** Institute of Mathematics, Warsaw University, Banacha 2, 02-097 Warsaw, Poland

1 Introduction

The Thue-Morse sequence [14, 9] is defined by

$$t_n = (-1)^{s(n)}, \tag{1}$$

where $s(n)$ denotes the number of ones in the binary representation of n. For any odd prime p and $i \in \mathbf{Z}$ we denote

$$S_{p,i}(n) = \sum_{0 \le j < n, j \equiv i (\mathrm{mod}\ p)} t_j \tag{2}$$

In 1969 Newman [15] has proved a remarkable conjecture of L. Moser saying that for any $n \ge 1$

$$S_{3,0}(n) > 0$$

[1]This work was supported by the Austrian Science Foundation, grant Nr. M 0038–PHY.

More precisely he has proved

$$\frac{3^\alpha}{20} < \frac{S_{3,0}(n)}{n^\alpha} < 5 \cdot 3^\alpha \qquad \text{with } \alpha = \frac{\log 3}{\log 4}$$

In 1983 Coquet [4] provided an explicit precise formula

$$S_{3,0}(n) = n^{\frac{\log 3}{\log 4}} \cdot \psi_3\left(\frac{\log n}{\log 4}\right) + \frac{\eta_3(n)}{3}$$

where ψ_3 is a continuous function, periodic with period 1 and nowhere differentiable attaining all its values in the closed interval

$$\left[\frac{2}{\sqrt{3}}, \frac{55}{3}\left(\frac{3}{65}\right)^{\frac{\log 3}{\log 4}}\right] \approx [1.15\ldots, 1.60\ldots]$$

and $\eta_3(n) =\in \{-1, 0, 1\}$.

In 1993 Grabner [11] has proved an analogous statement for $p = 5$

$$S_{5,0}(n) > 0, \qquad n \geq 1 \tag{3}$$

and gave a precise formula of the Coquet-type, computed the extremal values of the fractal function ψ_5 and its mean value. (The mean value of ψ_3 was computed in [8].) A little bit weaker statement than (3) has already been proved by Dumont [5].

A more general formula has been established in [9] (see also [10]) for those primes, for which 2 is a primitive root mod p:

$$S_{p,0}(n) = n^\alpha \cdot \psi_p\left(\frac{\log n}{(p-1)\log 2}\right) - \frac{\eta_p(n)}{p} \tag{4}$$

where ψ_p has the same general properties as ψ_3 above, $\alpha = \frac{\log p}{(p-1)\log 2}$, and

$$\eta_p(n) = \begin{cases} 0 & \text{if } 2|n \\ t_n & \text{if } 2\not| n. \end{cases}$$

Our first result is the following theorem:

Theorem 1 *Let p be a prime, $p \neq 3, 5$, such that 2 is a primitive root* mod p. *Then the function ψ_p attains both positive and negative values. Consequently $S_{p,0}(n)$ attains each integral value for infinitely many n.*

It is very interesting that $p = 17$ has the same property as 3 and 5. It has been proved recently by Grabner [12] that

$$S_{17,0}(n) > \frac{3.8}{\sqrt{17 + 4\sqrt{17}}}\, n^\alpha - 33$$

with $\alpha = \log(17+\sqrt{17})/\log(256)$. In this case 2 is not a primitive root but it generates all squares mod 17. In general, if 2 generates all squares mod p then the following formulae are known ([9]):
For $p \equiv 3 \bmod 4$ we have

$$S_{p,0}(n) = n^\alpha \cdot \psi_p\left(\frac{\log n}{(p-1)\log 4}\right) - \frac{\eta_p(n)}{p} \tag{5}$$

with α and η_p as above,
and for $p \equiv 1 \bmod 4$

$$S_{p,0}(n) = n^\alpha \cdot \psi_p\left(\frac{2\log n}{(p-1)\log 2}\right) + E_p(n), \tag{6}$$

where $E_p(n)$ is a bounded sequence and

$$\alpha = \frac{\log p + 2h\log\varepsilon}{(p-1)\log 2}$$

with h and ε being respectively the class number and fundamental unit of $\mathbf{Q}(\sqrt{p})$.

In this case we can prove a similar theorem. (Note that the case $p \equiv 3 \bmod 4$ has been already observed by Dumont [5].)

Theorem 2 *Let p be a prime, $p \neq 17, 41$, such that 2 generates all squares* mod *p. Then the function ψ_p attains both positive and negative values. Consequently $S_{p,0}(n)$ attains each integral value for infinitely many n.*

This means that the case $p = 41$ is the sole exception where we have no general answer at the moment. But there is big numerical evidence that ψ_{41} attains positive and negative values.

By inspecting the following proofs is will turn out that the zeroes of the functions ψ_p resulting from the found sign-changes converge to 1 as p tends to infinity (section 2). It is interesting that it is possible to find further zeroes of ψ_p which converge to $\frac{1}{2}$. We will discuss this phenomenon in section 3. It should be mentioned that the proof for the existence of these zeroes requires much deeper number theoretic properties. Especially in the (most difficult) case $p \equiv 1 \bmod 4$ we need an (at the moment unproved) assumption on the value $L(2,\chi)$, which resembles in some sense the famous Siegel's theorem on $L(1,\chi)$.

In [9] is also shown that $S_{p,i}(n)$, $i \neq 0$, has a similar asymptotic structure as $S_{p,0}(n)$ mainly described by a continuous fractal function $\psi_{p,i}$. In a concluding section we will briefly discuss sign-changes of these functions and generalize a result by Dumont [6] essentially saying that $\psi_{p,i}$ has a zero for $i \neq 0, 1$, if 2 is a primitive root mod p. Finally we will show that there is no correlation between the Thue-Morse sequence t_n and the Legendre symbol $(\frac{n+1}{p})$ for large n although numerical experiments for small n suggest one.

2 Sign-changes for $\mathrm{coord}_p(2) \le 2$

If the multiplicative order of $2 \bmod p$ equals s then we call the number

$$\mathrm{coord}_p(2) = \frac{p-1}{s}$$

the coorder of $2 \bmod p$. In this terminology the cases of coorder 1 and 2 are treated respectively in Theorems 1 and 2.

At the beginning we develope some general machinery. Let

$$P_M^{(l)}(x) = \prod_{j=l}^{M-1} (1 - x^{2^j}), \qquad M > l \ge 0$$

and $R_M^{(l)}(x)$ be the residue of $P_M^{(l)}(x) \bmod (x^p - 1)$:

$$R_M^{(l)}(x) = \sum_{k=0}^{p-1} r_{M,k}^{(l)} x^k, \qquad r_{M,k}^{(l)} \in \mathbf{Z} \tag{7}$$

In the sequel we shall apply several times the following, very simple rule, originally due to Stern [17, 18].

Lemma 1 *Let $f(x), g(x) \in \mathbf{Z}[x]$. Then*

$$f(x) \equiv g(x) \pmod{x^p - 1}$$

if and only if

$$f(1) = g(1) \qquad \textit{and} \qquad f(\varepsilon) = g(\varepsilon)$$

with $\varepsilon = \exp\left(\frac{2\pi i}{p}\right)$.

Proof. You just have to use the irreducibility of the p-th cyclotomic polynomial $\Phi_p(x) = 1 + x + \cdots x^{p-1}$. $\square$

In particular we always have

$$\sum_{k=0}^{p-1} r_{M,k}^{(l)} = 0$$

The importance of the numbers $r_{M,k}^{(l)}$ results from the following combinatorial observation.

Lemma 2 *The partial sums $S_{p,i}(n)$ defined in (2) and the coefficients $r_{M,k}$ given in (7) are related by*

$$S_{p,i}(2^{M-l}) = r_{M-l,i}^{(0)} = r_{M,2^l i}^{(l)}, \tag{8}$$

where $0 \le l < M$ and i is arbitrary.

Proof. Since

$$P_M^{(0)}(x) = \prod_{j=0}^{M-1}(1-x^{2^j}) = \sum_{n=0}^{2^M-1} t_n x^n$$

it immediately follows that (8) holds for $l=0$. Next observe that

$$P_M^{(l)}(x) = P_{M-l}^{(0)}(x^{2^l}).$$

Hence (8) holds for all $l<M$. □

The following lemma provides a relation between $r_{M,i}^{(l)}$ and $r_{M,i}^{(0)}$ (for $l=1,2$). Hence it is possible to calculate $S_{p,i}(2^{M-l})$ from $S_{p,i}(2^M)$.

Lemma 3 *The numbers $r_{M,j}^{(l)}$, $l=0,1,2$, are related by the following formulae:*

$$r_{M,j}^{(1)} = \frac{1}{p}\sum_{k=0}^{p-1} k r_{M,k}^{(0)} - \sum_{k=j+1}^{p-1} r_{M,k}^{(0)}, \tag{9}$$

in particular

$$r_{M,0}^{(1)} = \frac{1}{p}\sum_{k=0}^{p-1} k r_{M,k}^{(0)} + r_{M,0}^{(0)} \tag{10}$$

and

$$r_{M,j}^{(2)} = Q_j - \frac{1}{4p}\sum_{k=0}^{p-1} k^2 r_{M,k}^{(0)} + \frac{p-1}{4p}\sum_{k=0}^{p-1} k r_{M,k}^{(0)} + \frac{1}{4}\sum_{k=1}^{\frac{p-1}{2}} r_{M,2k-1}^{(0)} \tag{11}$$

where

$$Q_{2r} = -\sum_{j=r+1}^{\frac{p-1}{2}} r_{M,2j}^{(1)} - \sum_{j=1}^{\frac{p-1}{2}} r_{M,2j-1}^{(1)} \quad r=0,1,\ldots,\frac{p-1}{2} \tag{12}$$

and

$$Q_{2r-1} = -\sum_{j=r+1}^{\frac{p-1}{2}} r_{M,2j-1}^{(1)} \quad r=1,2,\ldots,\frac{p-1}{2}, \tag{13}$$

in particular

$$r_{M,0}^{(2)} = r_{M,0}^{(0)} - \frac{1}{4p}\sum_{k=0}^{p-1} k^2 r_{M,k}^{(0)} + \frac{p+3}{4p}\sum_{k=0}^{p-1} k r_{M,k}^{(0)} + \frac{1}{4}\sum_{k=1}^{\frac{p-1}{2}} r_{M,2k-1}^{(0)}. \tag{14}$$

Proof. We have

$$\sum_{j=0}^{p-1} r_{M,j}^{(1)}\varepsilon^j \quad = \quad P_M^{(1)}(\varepsilon) = (1-\varepsilon)^{-1}P_M^{(0)}(\varepsilon)$$

$$
\begin{aligned}
&= (1-\varepsilon)^{-1}\sum_{k=0}^{p-1} r_{M,k}^{(0)}(\varepsilon^k - 1) \\
&= -\sum_{k=0}^{p-1} r_{M,k}^{(0)} \cdot \sum_{j=0}^{k-1} \varepsilon^j = -\sum_{j=0}^{p-1} S_j \varepsilon^j
\end{aligned}
$$

with

$$S_j = \sum_{k=j+1}^{p-1} r_{M,k}^{(0)}$$

By the irreducibility of the p-th cyclotomic polynomial there exists $m \in \mathbf{Z}$ such that

$$r_{M,j}^{(1)} + S_j = m \quad \text{for} \quad j = 0, 1, \ldots, p-1$$

Summing up we obtain

$$m = \frac{1}{p}\sum_{j=0}^{p-1} S_j = \frac{1}{p}\left(\sum_{k=0}^{p-1} k r_{M,k}^{(0)}\right)$$

and hence (9) and (10).

In the same manner we get

$$
\begin{aligned}
\sum_{j=0}^{p-1} r_{M,j}^{(2)}\varepsilon^j &= (1-\varepsilon^2)^{-1}\sum_{k=0}^{p-1} r_{M,k}^{(1)}(\varepsilon^k - 1) \\
&= -\sum_{j=0}^{(p-1)/2} r_{M,2j}^{(1)} \sum_{k=0}^{j-1} \varepsilon^{2k} - \sum_{j=1}^{(p-1)/2} r_{M,2j-1}^{(1)} \sum_{k=0}^{(p-1)/2+j-1} \varepsilon^{2k} \\
&= \sum_{r=0}^{(p-1)/2} \varepsilon^{2r}\left(-\sum_{j=r+1}^{(p-1)/2} r_{M,2j}^{(1)} - \sum_{j=1}^{(p-1)/2} r_{M,2j-1}^{(1)}\right) \\
&\quad + \sum_{r=1}^{(p-1)/2} \varepsilon^{2r}\left(-\sum_{j=r+1}^{(p-1)/2} r_{M,2j-1}^{(1)}\right).
\end{aligned}
$$

Let Q_k be defined by (12) and (13). Then

$$\sum_{j=0}^{p-1} r_{M,j}^{(2)}\varepsilon^j = \sum_{k=0}^{p-1} Q_k \varepsilon^k.$$

Hence we obtain as above

$$r_{M,j}^{(2)} = Q_j - \frac{1}{p}\sum_{k=0}^{p-1} Q_k.$$

Since

$$\begin{aligned}\sum_{k=0}^{p-1} Q_k &= -\sum_{j=0}^{(p-1)/2} j r^{(1)}_{M,2j} - \sum_{j=1}^{(p-1)/2} \left(\frac{p-1}{2} + j\right) r^{(1)}_{M,2j-1} \\ &= -\frac{1}{2}\sum_{k=0}^{p-1} k r^{(1)}_{M,k} - \frac{p}{2}\sum_{j=1}^{(p-1)/2} r^{(1)}_{M,2j-1},\end{aligned}$$

$$\sum_{k=0}^{p-1}(-1)^k r^{(1)}_{M,k} = -\sum_{j=1}^{(p-1)/2} r^{(0)}_{M,2j-1} + \frac{1}{p}\sum_{k=0}^{p-1} k r^{(0)}_{M,k},$$

and

$$\sum_{k=0}^{p-1} r^{(1)}_{M,k} = 0$$

we obtain

$$\sum_{j=1}^{(p-1)/2} r^{(1)}_{M,2j-1} = \frac{1}{2}\sum_{j=1}^{(p-1)/2} r^{(0)}_{M,2j-1} - \frac{1}{2p}\sum_{k=0}^{p-1} k r^{(0)}_{M,k}.$$

Taking into account

$$\sum_{k=0}^{p-1} k r^{(1)}_{M,k} = -\frac{1}{2}\sum_{j=0}^{p-1} j^2 r^{(0)}_{M,j} + \frac{p}{2}\sum_{j=0}^{p-1} j r^{(0)}_{M,j}$$

we finally get

$$\sum_{k=0}^{p-1} Q_k = \frac{1}{4}\sum_{j=0}^{p-1} j^2 r^{(0)}_{M,j} - \frac{p-1}{4}\sum_{j=0}^{p-1} j r^{(0)}_{M,j} - \frac{p}{4}\sum_{j=1}^{(p-1)/2} r^{(0)}_{M,2j-1}$$

which completes the proof of Lemma 3. □

The next two propositions are refined versions of Theorems 1 and 2. They show that there are zeroes of $\psi_p(x)$ near $x = 1$.

Proposition 1 *Suppose that* p *is a prime,* $p \neq 3, 5, 11$*, such that* 2 *is a primitive root* mod p*. Then*

$$\psi_p\left(1 - \frac{1}{p-1}\right) > 0 \quad \textit{and} \quad \psi_p\left(1 - \frac{2}{p-1}\right) < 0.$$

Proof. By (4) it suffices to show that $S_{p,0}$ attains both positive and negative values. Since

$$P^{(0)}_{p-1}(\varepsilon) = \prod_{j=0}^{p-2}\left(1 - \varepsilon^{2^j}\right) = \prod_{k=1}^{p-1}\left(1 - \varepsilon^k\right) = p$$

we have

$$r_{p-1,i} = \begin{cases} p-1 & \text{for } i = 0, \\ -1 & \text{for } i \ne 0 \end{cases} \tag{15}$$

and therefore

$$S_{p,0}(2^{p-1}) = p - 1 > 0.$$

By (8) and Lemma 3 we again have

$$S_{p,0}(2^{p-2}) = r^{(1)}_{p-1,0} = -\frac{p-1}{2} + p - 1 = \frac{p-1}{2} > 0$$

but

$$S_{p,0}(2^{p-3}) = r^{(2)}_{p-1,0} = \frac{p-1}{2} - \frac{p^2-1}{24} < 0$$

for $p > 11$. □

This proves Theorem 1 for $p > 11$. Finally in the case $p = 11$ it can be directly checked that $S_{11,0}(23) = -1$ and $S_{11,0}(199) = 1$. Hence by (4) the function ψ_{11} attains positive and negative values.

Proposition 2 *Suppose that p is a prime, $p \ne 17, 41$, such that 2 generates all squares* $\bmod p$. *If $p \equiv 3 \bmod 4$ then*

$$\psi_p\left(1 - \frac{1}{2(p-1)}\right) > 0 \quad \textit{and} \quad \psi_p\left(1 - \frac{1}{p-1}\right) < 0$$

whereas if $p \equiv 1 \bmod 4$ then

$$\psi_p\left(1 - \frac{2}{p-1}\right) > 0 \quad \textit{and} \quad \psi_p\left(1 - \frac{4}{p-1}\right) < 0.$$

Proof. First, let $p \equiv 3 \bmod 4$. Since 2 is a quadratic residue this is equivalent with $p \equiv 7 \bmod 8$. By [9], p. 7, class 2A, we have

$$P^{(0)}_{2(p-1)}(\varepsilon) = p^2$$

and hence

$$r_{2(p-1),i} = \begin{cases} p(p-1) & \text{for } i = 0, \\ -p & \text{for } i \ne 0 \end{cases}$$

So we can proceed as in the proof of Proposition 1. The only difference is that all formulae are multiplied by p and that we have to use (5) instead of (4).

Second, let $p \equiv 1 \bmod 4$ or equivalently $p \equiv 1 \bmod 8$. It results from [9], Appendix, by an easy induction on t that for any odd t we have

$$P^{(0)}_{t\frac{p-1}{2}}(\varepsilon) = p^{\frac{1}{2}(t-1)}(a_t\sqrt{p} + pb_t),$$

where

$$2a_t, 2b_t \in \mathbf{Z},$$
$$a_t < 0, b_t > 0, \text{ and}$$
$$a_t^2 - pb_t^2 = -1.$$

Hence by using

$$\sum_{i=0}^{p-1} (\frac{i}{p})\varepsilon^i = \sqrt{p}$$

we obtain

$$r^{(0)}_{t\frac{p-1}{2},i} = \begin{cases} p^{\frac{1}{2}(t-1)} b_t(p-1) & \text{for } i = 0, \\ p^{\frac{1}{2}(t-1)}(-b_t + (\frac{i}{p})a_t) & \text{for } i \neq 0. \end{cases}$$

This gives

$$S_{p,0}(2^{t\frac{p-1}{2}-1}) = r^{(1)}_{t\frac{p-1}{2},i} = p^{\frac{1}{2}(t-1)} b_t \frac{p-1}{2} > 0.$$

In order to calculate $r^{(2)}_{t\frac{p-1}{2},0}$ we need the sum

$$\sum_{k=0}^{p-1} Q_k = \left(\frac{p^3-p}{24} b_t + \frac{a_t}{4} \sum_{j=0}^{p-1} j^2 (\frac{j}{p}) \right) p^{\frac{1}{2}(t-1)}$$

and a formula by Siegel [16]

$$\sum_{j=0}^{p-1} j^2 (\frac{j}{p}) = \frac{6}{\pi^4} \zeta_{\mathbf{Q}(\sqrt{p})}(2) p^{\frac{5}{2}}$$

to obtain

$$\begin{aligned} r^{(2)}_{t\frac{p-1}{2},0} &= r^{(1)}_{t\frac{p-1}{2},0} - \frac{1}{p}\sum_{k=0}^{p-1} Q_k \\ &= \left(b_t \left(\frac{p-1}{2} - \frac{p^2-1}{24} \right) - \frac{3a_t}{2\pi^4} \zeta_{\mathbf{Q}(\sqrt{p})}(2) p^{\frac{3}{2}} \right) p^{\frac{1}{2}(t-1)}. \end{aligned}$$

From the product representations of ζ-functions it follows

$$\zeta_{\mathbf{Q}(\sqrt{p})}(2) = \zeta(2)^2 (1 - \frac{1}{p^2}) \prod_{Q \in \mathcal{N}} (1 - \frac{2}{Q^2+1}),$$

where $\mathcal{N}$ denotes the set of all primes which are quadratic non-residues mod p. Because

$$-a_t < b_t \sqrt{p}$$

the number $r^{(2)}_{t\frac{p-1}{2},0}$ will be negative if

$$\prod_{Q\in\mathcal{N}}(1-\frac{2}{Q^2+1})<1-\frac{12}{p+1} \tag{16}$$

For $p<10^4, p\neq 17,41$, (16) can be proved using a computer program or simply an appropriate table of primitive roots mod p. For $p>10^4$ we proceed as follows. If there is a quadratic non-residue mod p less than $\sqrt{\frac{p-5}{6}}$ then (16) is fulfilled. Otherwise let n denote the number of elements of $\mathcal{N}$ in the interval $(0,\sqrt{p})$. The number of all quadratic non-residues mod p in $(0,\sqrt{p})$ is therefore not greater than $2n$. Using Thue's theorem concerning linear congruences ([19]) we obtain

$$2n\cdot 4\sqrt{p}\geq \frac{p-1}{2}$$

hence

$$n>6 \qquad \text{for} \quad p>10^4$$

But for $n\geq 7$ we have

$$\prod_{Q\in\mathcal{N}}(1-\frac{2}{Q^2+1})^{-1}>\prod_{Q\in\mathcal{N},Q<\sqrt{p}}(1+\frac{2}{Q^2+1})>1+\frac{14}{p}>(1-\frac{12}{p+1})^{-1}$$

hence (16). So we have proved that for $p\neq 17,41$ there exists a positive constant $c(p)$ (independent on t) such that

$$S_{p,0}(2^{t\frac{p-1}{2}-2})=r^{(2)}_{t\frac{p-1}{2},0}<-c(p)b_t p^{\frac{1}{2}(t-1)}.$$

An application of (6) (and the boundedness of $E_p(n)$) completes the proof of Proposition 2. □

3 Further Zeroes of ψ_p

In section 2 it is shown that for almost all primes p with $\mathrm{coord}_p(2)\leq 2$ the function $\psi_p(x)$ has a zero near $x=1$. It seems to be an interesting question to describe the set Z_p of all zeroes of ψ_p. For a moment, let us concentrate on primes p, where 2 is a primitive root. Using (4) it turns out that any (even) n with $S_{p,0}(n)=0$ induces infinitely many zeroes of $\psi_p(x)$ located very close to

$$x_0=\frac{\log n}{(p-1)\log 2} \bmod 1.$$

In fact we can prove more than that.

Proposition 3 *Let p be a prime, $p \neq 3, 5$ such that 2 is a primitive root* mod p. *Then the Hausdorff dimension $d_H(Z_p)$ of the set of zeroes Z_p of $\psi_p(x)$ is bounded below by*

$$d_H(Z_p) \geq \frac{\log((p-1)/2)}{(p-1)\log 2}.$$

Proof. By Proposition 1 $S_{p,0}(2^{p-2}) > 0$ and $S_{p,0}(2^{p-3}) < 0$ for $p \neq 3, 5, 11$. Furthermore we already mentioned that $S_{11,0}(23) < 0$ and $S_{11,0}(199) > 0$. In any case there is an even positive integer n_0 such that $S_{p,0}(n_0) = 0$. By (4) this directly provides a zero $x_0 = \frac{\log n_0}{(p-1)\log 2}$ of $\psi_p(x)$. Suppose that $n_0 \equiv k \bmod p$, $0 \leq k < p$. Then $S_{p,0}(n_0 + 2j) = 0$, $-k < 2j \leq p - k$, which leads to $\frac{p-1}{2}$ or $\frac{p-3}{2}$ additional zeroes. Furthermore, for any j we have $S_{p,0}(2^{p-1}(n_0 + 2j)) = 0$, where we can use the same idea as above and obtain $S_{p,0}(2^{p-1}(n_0+2j)+2l) = 0$, $-k - 2j < 2l \leq p - k - 2j$. Again this leads to $\frac{p-1}{2}$ or $\frac{p-3}{2}$ additional zeroes of $\psi_p(x)$ for any j. Let $Z_p(x_0)$ denote the closure of all of these zeroes which can be obtained inductively by this process. Since $\psi_p(x)$ is continuous all elements of $Z_p(x_0)$ are zeroes of $\psi_p(x)$ and the Hausdorff dimension $d_H(Z_p(x_0))$ is given by

$$\frac{\log((p+1)/2)}{(p-1)\log 2} \quad \text{or by} \quad \frac{\log((p-1)/2)}{(p-1)\log 2}$$

(compare with [7]). $\square$

The only disadvantage of Propostion 3 is that it does not say anything about the distribution of the zeroes in the interval $[0, 1)$. The proof only uses zeroes very close to 1. However, by looking at

$$S_{p,0}(2k) = n^{\alpha}\psi_p\left(\frac{\log(2k)}{(p-1)\log 2}\right), \quad 0 < k \leq 2^{p-2}$$

for small values of p with $\mathrm{coord}_p(2) = 1$ one finds lots of different zeroes of $\psi_p(x)$ very well dispersed. (For $p = 11$ you will find 42 zeroes, for $p = 13$ 280 zeroes and for $p = 19$ more than 3000 zeroes.) Therefore one can conjecture that (for fixed $\mathrm{coord}_p(2)$) and for any $\varepsilon > 0$ almost all primes p have the property that in any interval of length ε there are zeroes of $\psi_p(x)$. But a proof of such a property seems to be hopeless at the moment. The determination of the Hausdorff dimension $d_H(Z_p)$ is surely much easier.

In the sequel we will show that the function $\psi_p(x)$ has not only zeroes near $x = 1$ but also near $x = \frac{1}{2}$. Our method essentially uses properties of Dirichlet L-series. For $\mathrm{coord}_p(2) = 1$ we need Dirichlet's class number formula and use the fact that the class number $h > 0$ which is in fact a property of $L(1, \chi)$ (where χ denotes the quadratic character). Furthermore for $\mathrm{coord}_p(2) = 2$ we need a special property of $L(2, \chi)$ (where χ denotes the biquadratic character) in order to show that there is a sign change of $\psi_p(x)$ near $x = \frac{1}{2}$. Recall that the proof of the sign change of $\psi_p(x)$ near $x = 1$ ($p \equiv 1 \bmod 4$, Proposition 2) also requires estimates for $\zeta_{\mathbf{Q}(\sqrt{p})}(2) = L(2, \chi)L(2, \chi^2)(1 - p^{-2})^{-1}$. These results suggest that there might be a hidden connection between the distribution of Z_p and properties of Dirichlet L-series. Maybe this is a hint how to find an explanation of he above observation on the distribution of Z_p.

We start with the following lemma, that, as we hope, is of own interest, and presents a slightly generalized version of a beautiful and forgotten result by M. Stern [1, 17, 9].

Lemma 4 *Let p be an odd prime and $S \subset \mathrm{N}$ a fixed halfsystem* $\bmod p$*, that means:*

1) $s, t \in S, s \neq t \Longrightarrow s \not\equiv \pm t (\bmod p)$

2) $\# S = \frac{p-1}{2}$

Then

$$\prod_{t \in S}(1-x^t) \equiv (-1)^R \sum_{n=0}^{p-1} \left(\frac{-2s+4n}{p}\right) x^n \mod (x^p - 1)$$

where

$$R = \#\left\{t \in S \mid \{\frac{t}{p}\} > \frac{1}{2}\right\}, \quad s = \sum_{t \in S} t$$

Proof. By Lemma 1 it suffices to show that both sides assume the same values for $x = 1$ and $x = \varepsilon = \exp \frac{2\pi i}{p}$. We proceed in proving only the non-trivial part. Set

$$L = \prod_{t \in S}(1-\varepsilon^t) = \prod_{q \in T}(1-\varepsilon^{2q})$$

where

$$T = 2^{p-2}S = \{2^{p-2}t \mid t \in S\}.$$

Then we have

$$\begin{aligned} L &= \varepsilon^{\sum_{q \in T} q} \prod_{q \in T}(\varepsilon^{-q} - \varepsilon^q) = \varepsilon^{2^{p-2}s}(-1)^{\frac{p-1}{2}} \prod_{q \in T}(\varepsilon^q - \varepsilon^{-q}) \\ &= \varepsilon^{2^{p-2}s}(-1)^{\frac{p-1}{2}} \cdot \mathrm{sign}(T) \cdot \prod_{x=1}^{\frac{p-1}{2}}(\varepsilon^x - \varepsilon^{-x}) \end{aligned}$$

where

$$\mathrm{sign}(T) = (-1)^{\#\{q \in T \mid \{\frac{q}{p}\} > \frac{1}{2}\}}$$

After performing standard calculations ([3], p. 381, ex. 13–14)

$$\prod_{x=1}^{\frac{p-1}{2}}(\varepsilon^x - \varepsilon^{-x}) = (\frac{-2}{p}) i^{(\frac{p-1}{2})^2} \sqrt{p}$$

and using Gauss lemma on least residues

$$\mathrm{sign}(T) = (\frac{2^{p-2}}{p})\mathrm{sign}(S) = (\frac{2}{p})(-1)^R$$

we obtain

$$L = (-1)^R \varepsilon^{2^{p-2}s} i^{(\frac{p-1}{2})^2} \sqrt{p}.$$

Using again the representation of Gauss sums we finally get

$$\begin{aligned} L &= (-1)^R \sum_{j=0}^{p-1} (\frac{j}{p}) \varepsilon^{j+2^{p-2}s} = (-1)^R \sum_{n=0}^{p-1} (\frac{n-2^{p-2}s}{p}) \varepsilon^n \\ &= (-1)^R \sum_{n=0}^{p-1} (\frac{4n-2s}{p}) \varepsilon^n. \qquad \square \end{aligned}$$

Now assume that 2 is a primitive root $\bmod p$. Then

$$S = \{1, 2, 4, \ldots, 2^{\frac{p-3}{2}}\}$$

is a half-system mod p and therefore by the above lemma

$$R^{(0)}_{\frac{p-1}{2}}(x) = (-1)^R \sum_{n=0}^{p-1} \left(\frac{n+1}{p}\right) x^n, \tag{17}$$

especially $S_{p,0}(2^{\frac{p-1}{2}}) = (-1)^R$. This representation will be used in the proof of the following proposition.

Proposition 4 *Suppose that p is a prime such that 2 is a primitive root* $\bmod p$. *If $p \equiv 3 \bmod 4$ and $p > 163$ then*

$$\psi_p\left(\frac{1}{2}\right) \psi_p\left(\frac{1}{2} - \frac{1}{p-1}\right) < 0 \tag{18}$$

whereas if $p \equiv 1 \bmod 4$ and $p > 13$ then

$$\psi_p\left(\frac{1}{2} - \frac{1}{p-1}\right) \psi_p\left(\frac{1}{2} - \frac{2}{p-1}\right) < 0. \tag{19}$$

Proof. First suppose that $p \equiv 3 \bmod 4$. By using (17), Lemma 3, and Dirichlet's class number formula we direcly obtain

$$S_{p,0}(2^{\frac{p-1}{2}-1}) = r^{(1)}_{\frac{p-1}{2},0} = (-1)^R \left[1 + \frac{1}{p} \sum_{k=0}^{p-1} k \left(\frac{k+1}{p}\right)\right] = (-1)^R (1-h)$$

where h is the class number of $\mathbf{Q}(\sqrt{-p})$. Therefore for $p > 163$ we have

$$S_{p,0}(2^{\frac{p-1}{2}}) S_{p,0}(2^{\frac{p-1}{2}-1}) < 0$$

which proves (18).

If $p \equiv 1 \bmod 4$ then

$$r^{(0)}_{\frac{p-1}{2},0} = r^{(1)}_{\frac{p-1}{2},0} = (-1)^R$$

and

$$r^{(2)}_{\frac{p-1}{2},0} = (-1)^R \left[1 - \frac{3}{2\pi^4}\zeta_{\mathbf{Q}(\sqrt{p})}(2)p^{\frac{3}{2}}\right]$$

as in the proof of Proposition 2. Because of the trivial estimate

$$\zeta_{\mathbf{Q}(\sqrt{p})}(2) > 1$$

the expression in the above bracket is negative for $p \geq 17$ and hence (19). □

Finally let us consider the case where 2 generates all squares $\bmod\, p$. The case $p \equiv 3 \bmod 4$ will turn out to be very simple whereas the remaining case $p \equiv 1 \bmod 4$ is much more involved.

Proposition 5 *Suppose that p is a prime such that 2 generates all squares* $\bmod\, p$. *If $p \equiv 3 \bmod 4$ then*

$$\psi_p\left(\frac{1}{2}\right) < 0 \quad and \quad \psi_p\left(\frac{1}{2} - \frac{1}{p-1}\right) > 0. \tag{20}$$

If $p \equiv 1 \bmod 4$ and $p^{\frac{3}{2}}|\Im(L(2,\chi))| > 40\pi^2$, where $L(s,\chi)$ denotes the Dirichlet L-series of the biquadratic character $\bmod\, p$, *then either*

$$\psi_p\left(\frac{1}{2} - \frac{2}{p-1}\right)\psi_p\left(\frac{1}{2} - \frac{4}{p-1}\right) < 0 \tag{21}$$

or

$$\psi_p\left(\frac{1}{2}\right)\psi_p\left(\frac{1}{2} + \frac{2(\log 5/4)/(\log 2)}{p-1}\right) < 0 \tag{22}$$

Especially if $p \equiv 2 \bmod 3$ and p is sufficiently large then $p^{\frac{3}{2}}|\Im(L(2,\chi))| > 40\pi^2$.

If $p \equiv 3 \bmod 4$ then we have by [9]

$$P^{(0)}_{p-1}(\varepsilon) = -p.$$

Hence we can proceed as in the proof of Proposition 1 to obtain (20) for $p > 11$.

If $p \equiv 1 \bmod 4$ then the situation is much more complicated. In order to complete the proof of Proposition 5 we will use a series of lemmata.

Lemma 5 *Suppose that $p \equiv 1 \bmod 4$ such that 2 generates all squares* $\bmod\, p$. *Then we have*

$$P^{(0)}_{t\frac{p-1}{4}}(\varepsilon) = \prod_{i=0}^{t\frac{p-1}{4}-1}(1-\varepsilon^{2^i}) = \pm\sqrt{a_t\sqrt{p} + b_t p}\cdot\varepsilon^{-1}\cdot p^{\frac{t-1}{4}}$$

for any positive integer $t \equiv 1 \bmod 4$, where a_t, b_t are defined in the proof of Proposition 2.

Proof. Since $p \equiv 1 \bmod 8$ we can write $p = 8q + 1$ for some integer q. By taking into account the congruence $2^{2q} \equiv -1 \bmod p$ we obtain

$$P_{4tq}^{(0)}(\varepsilon) = \prod_{i=0}^{4tq-1}(1-\varepsilon^{2^i}) = \prod_{i=0}^{2tq-1}(1-\varepsilon^{2^i})(1-\varepsilon^{-2^i}) = \left(\varepsilon P_{2tq}^{(0)}(\varepsilon)\right)^2$$

for odd t. Hence

$$P_{2tq}^{(0)}(\varepsilon) = \pm\sqrt{a_t\sqrt{p}+b_tp}\cdot\varepsilon^{-1}\cdot p^{\frac{t-1}{4}}$$

for $t \equiv 1 \bmod 4$. $\square$

From now let us fix a primary element $\omega \in \mathbf{Z}[i]$ with norm p:

$$\omega = \alpha + \beta i, \quad \alpha \equiv 1 \bmod 4, \quad \beta \equiv 0 \bmod 4$$

It is well known ([2]) that

$$\mathcal{G}(4) = \sum_{n=0}^{p-1}\varepsilon^{n^4} = \sqrt{p} \pm \sqrt{2p - 2\alpha\sqrt{p}}.$$

Hence, both $\sqrt{a_t\sqrt{p}+b_tp}$ and $\sqrt{2p-2\alpha\sqrt{p}}$ generate subextensions of $\mathbf{Q}(\varepsilon)$ of degree 4 over $\mathbf{Q}$. But for any $d|p-1$ the field $\mathbf{Q}(\varepsilon)$ contains a unique subextension K_d of degree d over $\mathbf{Q}$. Thus

$$K_4 = \mathbf{Q}\left(\sqrt{p}, \sqrt{a_t\sqrt{p}+b_tp}\right) = \mathbf{Q}\left(\sqrt{p}, \sqrt{2p+2\alpha\sqrt{p}}\right)$$

and consequently there exist $c_t, d_t \in \mathbf{Q}$ such that

$$(2p + 2\alpha\sqrt{p}) = (a_t\sqrt{p}+b_tp)(c_t + d_t\sqrt{p})^2.$$

(Note that $(2p-2\alpha\sqrt{p})(2p+2\alpha\sqrt{p}) = (2\beta\sqrt{p})^2$. Therefore we can work with $2p+2\alpha\sqrt{p}$ instead of $2p-2\alpha\sqrt{p}$.) From this one can express c_t, d_t uniquely up to sign:

$$\begin{aligned} c_t^2 &= b_tp - a_t\alpha - \beta \\ d_t^2 &= \frac{1}{p}(b_tp - a_t\alpha + \beta) \\ c_td_t &= b_t\alpha - a_t \end{aligned}$$

where we have specified the sign of β such that

$$\alpha a_t \equiv \beta \pmod p \quad \text{for} \quad t \equiv 1 \bmod 4$$

This specifictaion is independent of t since $a_{t+4} \equiv a_t \bmod p$. Now we define

$$z_t = d_t + (b_tc_t + a_td_t)i \quad \text{and} \tag{23}$$
$$u_{t,j} = \Re(z_t\chi(j)) \in \mathbf{Z} \tag{24}$$

with a biquadratic character χ uniquely determined by the choise of ω (see [13]).

Lemma 6 *The numbers $u_{t,j}$ defined in (24) satisfy*

$$\sum_{j=0}^{p-1} u_{t,j} = 0 \qquad \text{and} \qquad \left(\sum_{j=0}^{p-1} u_{t,j}\varepsilon^j\right)^2 = a_t\sqrt{p} + b_t p. \tag{25}$$

Consequently

$$P^{(0)}_{t\frac{p-1}{4}}(\varepsilon) = \pm p^{\frac{t-1}{4}} \sum_{j=0}^{p-1} u_{t,j+1}\varepsilon^j.$$

Proof. Obvioulsy

$$\sum_{j=0}^{p-1} u_{t,j} = 0.$$

Hence (25) is equivalent to the following system of equations

$$\sum_{j=0}^{p-1} u_{t,j}u_{t,-j} = b_t(p-1), \tag{26}$$

$$\sum_{j=0}^{p-1} u_{t,j}u_{t,i-j} = -b_t + \left(\frac{i}{p}\right) a_t \tag{27}$$

Since $|z_t|^2 = 2b_t$ we obtain

$$\begin{aligned}\sum_{j=0}^{p-1} u_{t,j}^2 &= \frac{1}{4}\sum_{j=0}^{p-1}(z_t\chi(j) + \overline{z_t}\overline{\chi(j)})^2 \\ &= \frac{1}{4}(z_t^2 + \overline{z_t}^2)\sum_{j=0}^{p-1}\left(\frac{j}{p}\right) + \frac{1}{2}|z_t|^2(p-1) = b_t(p-1)\end{aligned}$$

which proves (26). In order to prove (27) we express the left-hand side by Jacobi sums

$$\begin{aligned}&\frac{1}{4}\sum_{j=0}^{p-1}(z_t\chi(j) + \overline{z_t}\overline{\chi(j)})(z_t\chi(i-j) + \overline{z_t}\overline{\chi(i-j)}) \\ &\qquad = 2\Re\left(\frac{z_t^2}{4}(\frac{i}{p})J(\chi,\chi)\right) + |z_t|^2\Re\frac{1}{2}J(\chi,\overline{\chi})\end{aligned}$$

By using the classical formulae

$$\begin{aligned}J(\chi,\chi) &= -\omega = -\alpha - \beta i \\ J(\chi,\overline{\chi}) &= -1\end{aligned}$$

(see e.g. [13]) and the relation

$$z_t^2 = \frac{2}{p}(\beta + \alpha i)(1 + a_t i)$$

we directly get (27). □

The integers c_t, d_t are only determined uniquely up to sign. Therefore we can assume w.l.o.g. that this sign is chosen in a way that $(p = 8q + 1)$

$$P_{2tq}^{(0)}(\varepsilon) = p^{\frac{t-1}{4}} \sum_{j=0}^{p-1} u_{t,j+1}\varepsilon^j.$$

Hence

$$r_{2tq,j}^{(0)} = u_{t,j+1} p^{\frac{t-1}{4}}$$

Since

$$\sum_{k=0}^{p-1} k r_{2tq,j}^{(0)} = p^{\frac{t-1}{4}} \Re \left(z_t \sum_{k=0}^{p-1} k\chi(k+1) \right) = 0$$

we obtain by Lemma 3

$$S_{p,0}(2^{2tq-1}) = r_{2tq,0}^{(1)} = S_{p,0}(2^{2tq}) = r_{2tq,0}^{(0)} = u_{t,1} p^{\frac{t-1}{4}}.$$

Therefore we have to use Lemma 3 a second time. From

$$\frac{1}{4}\sum_{j=0}^{p-1} j^2 u_{t,j+1} - \frac{p}{4} \sum_{j=1}^{(p-1)/2} u_{t,2j} = \frac{1}{4}\Re \left(z_t \sum_{j=0}^{p-1} j^2\chi(j) \right)$$

we get

$$S_{p,0}(2^{2tq-2}) = r_{2tq,0}^{(2)} = u_{t,1} p^{\frac{t-1}{4}} - p^{\frac{t-5}{4}} \frac{1}{4} \Re \left(z_t \sum_{j=0}^{p-1} j^2\chi(j) \right).$$

Now observe that (see [20])

$$\sum_{j=0}^{p-1} j^2 \chi(j) = pB_{2,\chi} = -2pL(-1,\chi)$$

and that $L(-1,\chi)$ is related to $L(2,\chi)$ by the functional equation

$$L(-1,\chi) = \frac{-p^{\frac{3}{2}}}{2\pi^2} \frac{\sqrt{p}}{\tau(\overline{\chi})} L(2,\overline{\chi}) = -\frac{p^2}{2\pi^2}\tau(\overline{\chi})^{-1} L(2,\overline{\chi}),$$

where $\tau(\overline{\chi})$ is the normed quartic Gauss sum. Therefore, the problem of sign change of the fractal function ψ_p can be reduced to to a property of $L(2,\chi)$.

Lemma 7 *Suppose that*

$$p^{\frac{3}{2}}|\Im(L(2,\chi))| > 40\pi^2 \tag{28}$$

then either (21) or (22).

Proof. Since $\arg\tau(\overline{\chi})^2 = \pi - \arg\omega$ ([13], Prop. 9.10.1) and

$$\arg z_t^2 = \frac{\pi}{2} - \arg\omega + \arg(1+a_t i)$$

we obtain

$$\arg\left(z_t^2\left(\sum_{j=0}^{p-1} j^2\chi(j)\right)^2\right) = -\frac{\pi}{2} + \arg(1+a_t i) + 2\arg L(2,\overline{\chi})$$

and consequently

$$\arg\left(z_t\sum_{j=0}^{p-1} j^2\chi(j)\right) = -\frac{\pi}{2} + \mathcal{O}(a_t^{-1}) + \arg L(2,\overline{\chi}) + \eta\pi$$

with $\eta \in \{0,1\}$. Hence (28) implies that for sufficiently large t we have

$$\frac{1}{4p}\left|\Re\left(z_t\sum_{j=0}^{p-1} j^2\chi(j)\right)\right| > 10|z_t|. \tag{29}$$

Now we will distinguish two cases. First suppose that $\Re\left(z_t\sum_{j=0}^{p-1} j^2\chi(j)\right)$ and $u_{t,1}$ have the same sign. Then by Lemma 3

$$S_{p,0}\left(2^{2qt-1}\right)S_{p,0}\left(2^{2qt-2}\right) = r^{(1)}_{2tq,0}r^{(2)}_{2tq,0} < -c_1(p)p^{\frac{t-1}{2}}$$

with $c_1(p) > 0$ independent of t. In the second case observe that

$$\begin{aligned} S_{p,0}\left(\frac{5}{4}2^{2tq}\right) &= S_{p,0}\left(2^{2tq}\right) - S_{p,1}\left(\frac{1}{4}2^{2tq}\right) \\ &= r^{(0)}_{2tq,0} - r^{(2)}_{2tq,4} = u_{t,1} - r^{(2)}_{2q,4}. \end{aligned}$$

Since

$$r^{(2)}_{2q,4} = Q_4 - p^{\frac{t-5}{4}}\frac{1}{4}\Re\left(z_t\sum_{j=0}^{p-1} j^2\chi(j)\right)$$

and

$$\begin{aligned} |Q_4| &= |r^{(1)}_{2tq,0} + r^{(1)}_{2tq,2} + r^{(1)}_{2tq,4}| \\ &= |3u_{t,1} + 2u_{t,2} + 2u_{t,3} + u_{t,4} + u_{t,5}| \\ &\leq 9|z_t| \end{aligned}$$

we similarly obtain

$$S_{p,0}\left(2^{2qt}\right) S_{p,0}\left(\frac{5}{4}2^{2qt}\right) < -c_2(p)p^{\frac{t-1}{2}}$$

with $c_2(p) > 0$ independent of t. Since the error term $E_p(n)$ is bounded in (6) we have proved the Lemma. □

It remains to verify (28). Unfortunately we cannot prove (28) in general. However, if $p \equiv 2 \bmod 3$ (i.e. 3 is quadratic non-residue mod p if $p \equiv 1 \bmod 8$) then

$$|\arg(L(2,\chi))| > c > 0$$

since the term $\log(1 \pm 3^{-2})$ dominates the sum

$$\arg(L(2,\chi)) = -\sum_{\left(\frac{q}{p}\right)=-1} \log\left(1 - \frac{\chi(q)}{q}\right).$$

This completes the proof of Proposition 5.

We want to append a Lemma where we prove a weaker statement than (28).

Lemma 8 *Let* $p \equiv 1 \bmod 8$ *be a prime and* χ *a biquadratic character* mod p. *Then*

$$p^{\frac{7}{2}}|\Im(L(2,\chi))| > c$$

with some constant $c > 0$ *independent of* p.

Proof. By the functional equation of $L(s,\chi)$ we obtain

$$L(-1,\chi)^4\overline{\omega}^2 = p^7\left(\frac{L(2,\overline{\chi})}{2\pi^2}\right)^4.$$

If $L(2,\overline{\chi})$ were real then it would follow from the fact

$$L(-1,\chi) = -\frac{1}{2p}\sum_{j=1}^{p-1} j^2\chi(j) \in \mathbf{Z}[i]$$

that

$$L(-1,\chi)^4\overline{\omega}^2 \in \mathbf{Z}$$

and consequently

$$\exp_\omega(L(-1,\chi)^4\overline{\omega}^2) = \exp_{\overline{\omega}}(L(-1,\chi)^4\overline{\omega}^2)$$

which is obviously false. Hence

$$|\Im(L(-1,\chi)^2\overline{\omega}))| \geq 1.$$

On the other hand

$$|L(-1,\chi)^2\overline{\varpi}| = p^{\frac{7}{2}}\frac{|L(2,\overline{\chi})|^2}{4\pi^4}$$

which proves the Lemma. □

Nevertheless, we are convinced that (28) is true in general. Let us conclude this section with a conjecture.

Conjecture. *Let* $p \equiv 1 \bmod 8$ *be a prime and* χ *a biquadratic character* mod p. *Then*

$$\lim_{p\to\infty} p^{\varepsilon}|\Im(L(2,\chi))| = \infty.$$

for any $\varepsilon > 0$.

For our purpose it would be sufficient to verify this conjecture for $\varepsilon = \frac{3}{2}$. Moreover it should be noted that a general verification would imply that for any $\varepsilon > 0$ and sufficiently large p there exists a quadratic non-residue $n \bmod p$ of size $0 < n < p^{\varepsilon}$. (Let n denotes the smallest quadratic non-residue $\bmod\, p$. Then $|\arg(L(2,\chi)| \le c/n$.)

4 Related Problems

It is not only interesting to study the behaviour of $S_{p,0}(n)$. Dumont [5] observed that $S_{3,1}(n)$ is always negative and that $S_{3,2}(n)$ attains positive and negative values. Furthermore in [6] it is shown that if 2 is a primitive root $\bmod\, p$ then

$$\liminf_{n\to\infty} |S_{p,i}(n)|n^{-\alpha} = 0,$$

for $i \ne 0, 1$, where $\alpha = \frac{\log p}{(p-1)\log 2}$. Since $S_{p,i}(n)$ has a similar representation as $S_{p,0}(n)$ in (4) in terms of continuous fractal functions $\psi_{p,i}$ (see [9])

$$S_{p,i}(n) = n^{\alpha}\cdot\psi_{p,i}\left(\frac{\log n}{(p-1)\log 2}\right) - \frac{\eta_p(n)}{p} \tag{30}$$

it follows that $\psi_{p,i}$ has a zero for $i \ne 0, 1$. The following theorem provides a more precise and complete description of the behaviour of these functions.

Theorem 3 *Let* p *be a prime such that* 2 *is a primitive root* $\bmod\, p$. *Then the functions* $\psi_{p,i}$, $i = 0, 1, \ldots, p-1$, *attain both positive and negative values with the only exceptions* $\psi_3 = \psi_{3,0}$, $\psi_{3,1}$, *and* $\psi_5 = \psi_{5,0}$.

Proof. Since the case $i = 0$ is settled in Theorem 1 we can restrict to the case $i > 0$. By (15) we have $S_{p,i}(2^{p-1}) = -1 < 0$ for $i > 0$, whereas

$$S_{p,i}(3\cdot 2^{p-1}) = S_{p,i}(2^{p-1}) - S_{p,i-1}(2^{p-1}) - S_{p,i-1}(2^{p-1}) = 1 > 0$$

for $i \geq 3$. Here we have used a formula of [9]

$$S_{p,i}(n2^M) = \sum_{j=0}^{n-1} t_j S_{p,i-2^M j}(2^M) \tag{31}$$

which follows by easy induction on n. Hence $\psi_{p,i}$ changes its sign for $i \geq 3$.

By Lemma 3 we obtain $r^{(1)}_{p-1,i} = \frac{p-1}{2} - i$ and therefore

$$S_{p,i}(2^{p-2}) = r^{(1)}_{p-1,2i} = \frac{p-1}{2} - (2i \bmod p).$$

Thus $S_{p,i}(2^{p-2}) > 0$ for $i = 1,2$ and $p \geq 11$ and the sign of the corresponding functions $\psi_{p,i}$ changes, too.

The case $p = 3$ is completely settled in [5]. Furthermore it is easy to verify that $S_{5,1}$ and $S_{5,2}$ attain positive and negative values. This completes the proof of Theorem 3. □

If 2 generates the squares mod p the situation is more difficult. We will give a partial answer.

Theorem 4 *Let p be a prime such that 2 generates all squares* mod p.

If $p \equiv 3 \bmod 4$ then the functions $\psi_{p,i}$, $i = 0, 1, \ldots, p-1$, attain both positive and negative values.

If $p \equiv 1 \bmod 4$ and $i \leq c\sqrt{p}$, where $c > 0$ is a sufficiently small constant, then the functions $\psi_{p,i}$ attain both positive and negative values.

The case $p \equiv 3 \bmod 4$ can be treated as in the proof of Theorem 3 whereas if $p \equiv 1 \bmod 4$ we just have to modify the proof of Proposition 2.

Finally we want to discuss a "twisted" Thue-Morse sequence $t_n(\frac{n+1}{p})$, where $(\frac{n+1}{p})$ is the Legendre symbol. Its partial sums

$$T_p(n) = \sum_{0 \leq j < n} t_j (\frac{j+1}{p})$$

can be interpreted as a linear combination

$$T_p(n) = \sum_{i=0}^{p-1} (\frac{i+1}{p}) S_{p,i}(n)$$

of $S_{p,i}(n)$. If one tries to calculate $T_p(n)$ for small n it often occurs that $T_p(n) > 0$. For example, if $p = 53$ then $(\frac{n+1}{53})$ seems to be a very good "approximation" for t_n. Hence $T_{53}(n)$ is large for small n. However, there is surely no correlation for large n since $T_p(n) = \mathcal{O}(n^\alpha)$ for some $\alpha < 1$. Moreover, the following theorem holds.

Theorem 5 *Let p be a prime, $p \neq 3, 5$, such that 2 is a primitive root* $\bmod p$. *Then $T_p(n)$ attains each integral value for infinitely many n.*

Proof. By (31) and (17) we get

$$S_{p,0}(n2^{\frac{p-1}{2}}) = \sum_{0 \le j < n} t_j S_{p,j}(2^{\frac{p-1}{2}}) = (-1)^R \sum_{0 \le j < n} t_j(\frac{j+1}{p}) = (-1)^R T_p(n).$$

Now observe that $\log n$ is dense $\bmod 1$. Hence, by (4), by the continuity of ψ_p, and by Theorem 1 if follows that $T_p(n)$ attains each integral value infinitely often. □

The proof of Theorem 5 also shows that $T_3(n) > 0$ and $T_5(n) > 0$ for all n, i.e. $S_{3,0}(n) > S_{3,1}(n)$ and

$$S_{5,0}(n) + S_{5,3}(n) > S_{5,1}(n) + S_{5,4}(n).$$

The first inequality is not so interesting since $S_{3,0}(n) > 0$ and $S_{3,1}(n) < 0$ (see [5]) but the second one is probably new. It seems to be an interesting problem to descibe all linear combinations of $S_{p,i}(n)$ which are always positive.

References

[1] P. Bachmann, Niedere Zahlentheorie, Teubner, Leipzig, 1910.

[2] B.C. Berndt, R.J. Evans, The determination of Gauss sums, Bull. Am. Math. Soc., New Ser. **5**, 107–129 (1981).

[3] S.I. Borevich, I.R. Shafarevich, Zahlentheorie, Birkhäuser Verlag Basel und Stuttgart, 1966.

[4] J. Coquet, A summation formula related to the binary digits, Invent. Math. **73**, 107 –115, (1983).

[5] J.M. Dumont, Discrépance des progressions arithméthiques dans la suite de Morse, C. R. Acad. Sci. Paris, Série I **297** (1983), 145–148.

[6] J.M. Dumont, Discrépance des progressions arithméthiques dans la suite de Morse, These, Universitè de Provence, 1984.

[7] K.J. Falconer, The Geometry of Fractal Sets, Cambridge Tracts in Mathematics 85, Cambridge University Press, Cambridge, 1985.

[8] P. Flajolet, P.J. Grabner, P. Kirschenhofer, H. Prodinger, and R.F. Tichy, Mellin Transforms and asymptotics: digital sums, Theor. Comput. Sci. , to appear.

[9] S. Goldstein, K.A. Kelly, and E.R. Speer, The fractal structure of rarefied sums of the Thue-Morse sequence, J. Number Theory **42**, 1–19 (1992).

[10] P.J. Grabner, Completely q-multiplicative functions: the Mellin transform approach, Acta Arith. **65**, 85–96, (1993).

[11] P.J. Grabner, A note on the parity of the sum-of-digits function, Séminaire Lotharingien de Combinatoire, Publication de l'I.R.M.A., Strasbourg, to appear.

[12] P.J. Grabner, private communication.

[13] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer-Verlag New-York Heidelberg Berlin, 1982.

[14] M. Morse, Reccurent geodesics on a surface of negative curvature, Trans. Am. Math. Soc. **22**, 84–100 (1921).

[15] D.J. Newman, On the number of binary digits in a multiple of three, Proc. Am. Math. Soc. **21**, 719–721 (1969).

[16] C.L. Siegel, Bernoullische Polynome und quadratische Zahlkörper, Nachr. Akad. Wiss. Gött., II. Math.-Phys. Kl. **2**, 7–38 (1969).

[17] M. Stern, Ueber eine der Theilung der Zahlen ähnliche Untersuchung und deren Anwendung auf die Theorie der quadratischen Reste, Journ. Reine Angew. Math. **61**, 66–94 (1863).

[18] M. Stern, Zur Theorie der quadratischen Reste, Journ. Reine Angew. Math. **61**, 334–349 (1863).

[19] A. Thue, Et par antydninger til en taltheorietisk method, in Selected Mathematical Papers of Axel Thue, Universitetsforlaget, Oslo, 1977, 57–75.

[20] L. C. Washington, Introduction to cyclotomic fields, Springer-Verlag, New York, 1982.