The Newman phenomenon and Lucas sequence.

Alexandre Aksenov

Abstract

This article gives an alternative proof of the fact that \( N_{\mathbb{Q}(\zeta)}(1 - \zeta) = p \) where \( p \) is an odd prime number and \( \zeta \) is a primitive \( p \)-th root of unity, and uses it to prove that \( N_{\mathbb{Q}(\zeta)}(1 + \zeta - \zeta^2) = L(p) \) the \( p \)-th Lucas number. It shows a relation between this result and a generalisation of the Newman phenomenon.

Keywords: Newman phenomenon, Möbius function, partitions of a set, Lucas numbers, cyclotomic fields.

1. Introduction.

In 1969 D.J.Newman proved the following statement:

**Theorem 1.1** (Moser’s conjecture). Let \((t_n)\) be the Thue-Morse sequence i.e.

\[ t_n = (-1)^{\text{the number of '1' digits in the binary expansion of } n \in \{1, -1\}}. \]

Then all the sums \( t_0, t_0 + t_3, t_0 + t_3 + t_6 \) (the sums of \( N \) initial terms of the sequence \((t_{3n})\)) are strictly positive.

He also gave an estimation for the rate of growth of these sums, more precisely he proved that

\[ K_1 N^{\log_3 3} < \sum_{\substack{n < N \\text{3|}n}} t_n < K_2 N^{\log_3 4} \]

for two explicit constants \( K_1 \) and \( K_2 \).

The article [2] of J.Coquet provides a more complete description of the structure of these sums via the formula

\[ \sum_{\substack{n < N \\text{3|}n}} t_n = F(\{\log_4 N\})N^{\log_3 4} + \epsilon(N) \]

where \( \{x\} \) denotes the fractional part of \( x \in \mathbb{R}, |\epsilon(N)| \leq 1 \) therefore \( \epsilon(N) \) is an error term, and \( F \) is a continuous and nowhere differentiable function. This article gives also the values of the the maximum and the minimum of \( F \), that are the best possible bounds \( K_2 \) and \( K_1 \) for \( N \) large enough.

Coquet’s result has been generalised to arbitrary odd primes \( p \) in [7]:

\[ \text{(original text continues...)} \]
Theorem 1.2 (Theorem 5.1 from \[7\]). Let $p$ be an odd prime number. Denote

$$S_q(N) = (S_{q,i}(N) = \sum_{0 \leq n < N \atop n \equiv i \mod p} t(n))_{i=0,1,\ldots,p-1} \in \mathbb{C}^p,$$

denote $T$ the $p \times p$ matrix

$$T = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & & & 0 \\ 1 & 0 & & & 0 \\ & & \ddots & \ddots & \vdots \\ 0 & & \ldots & 1 & 0 \end{pmatrix}$$

and

$$M = \prod_{m=0}^{s-1} (I - T^{2^m})$$

where $s$ is the order of the element 2 in the group $\mathbb{F}_p^\times$. Then the asymptotic behaviour of the sequence of vectors $S_q(N)$ is described by

$$S_p(N) = N^{\alpha_p} \tilde{G} \left( \frac{\log N}{rs \log 2} \right) + \tilde{E}(N)$$

(1)

where:

- $\tilde{G}(x) = \left( \tilde{G}_i(x) \right)_{i=0,1,\ldots,p-1}$ is a column vector whose components are continuous nowhere derivable periodic functions with period 1;
- $\alpha_p = \frac{\log \lambda_1}{rs \log 2}$ where $\lambda_1$ is the spectral radius of $M$ and $r \in \{1, 2, 4\}$ is the smallest integer such that the $r$-th power of the biggest (in modulus) eigenvalue of $M$ is real positive;
- $\tilde{E}(N) = O(N^{\beta_p})$ where $\beta_p$ depends on the second biggest modulus $\lambda_2$ of an eigenvalue of $M$ by

$$\beta_p = \beta_p(\lambda_2) = \begin{cases} \frac{\log \lambda_2}{s \log 2} & \text{if } \lambda_2 > 1, \\ 0 & \text{otherwise,} \end{cases}$$

They did not calculate the best possible values for bounds $K_1$ and $K_2$ since the complexity of this calculation increases very fast with $p$ (see also \[8\] for a complete study of the case $p = 5$). Remark that in fact, $r = 2$ never happens as will be proved in Section 5.

In this article we are going to further generalize the method of Coquet to a large class of $b$-multiplicative sequences with arbitrary $b > 1$ and challenge another problem explored in \[7\]: give an algebraic description for the exponent $\alpha_p$ of $N$ in the formulae analogous to (1).

Recall that a sequence $f(n)$ of real or complex numbers is called $b$-multiplicative if it satisfies $f(0) = 1$ and

$$f(ab^k + c) = f(ab^k)f(c)$$

for all $a, k \in \mathbb{N}$ and $c < b^k$.

We will also denote by $\overline{c_l c_{l-1} \ldots c_0(b)}$, or simply $\overline{c_l c_{l-1} \ldots c_0}$ when the base of the numeration system is clear, the nonnegative integer represented by the sequence $c_l c_{l-1} \ldots c_0$ in base $b$, that is:

$$\overline{c_l c_{l-1} \ldots c_0(b)} = \sum_{i=0}^{l} c_i b^i.$$
2. \(p\)-rarefaction in multiplicative sequences.

Let \(b > 1\) be an integer and \(\tau_n\) be a unit-circle-valued \(b\)-multiplicative sequence such that \(\tau_{ck^l} = \tau_c\) for any \(c, k \in \mathbb{N}\). As consequence \(\tau\) can be defined as follows: if \(\tau_{c_0c_1\ldots c_{l-1}} = c_0\) is the \(b\)-ary expansion of an integer \(n\) then

\[
\tau_n = \prod_{i=0}^{l} \tau_{c_i}
\]

and \(\tau_0 = 1\); each of the complex numbers \(\tau_1, \tau_2, \ldots, \tau_{b-1}\) is of modulus one. We will also suppose that \(\tau_n\) is not identically 1.

Under these hypotheses the Theorem 2 of \[4\] can be applied, and it states that

\[
\sum_{n=0}^{N-1} \tau_n = o(N).
\]

This bound can be made more precise.

Let us put an additional notation : for each \(c \in \{0, \ldots, b\}\) we will denote \(d(c) = \sum_{i=0}^{c-1} \tau_i\). Then for each positive integer \(N\) represented in base \(b\) by \(\overline{c_0c_1\ldots c_{l-1}}\) we get:

\[
\sum_{n=0}^{N-1} \tau_n = \sum_{n=c_0c_1\ldots c_{l-1}=0}^{c_0c_1\ldots c_{l-1}-1} \tau_n + \sum_{n=c_0c_1\ldots c_{l-1}=0}^{c_0c_1\ldots c_{l-1}-1} \tau_n + \ldots + \sum_{n=c_0c_1\ldots c_{l-1}=0}^{c_0c_1\ldots c_{l-1}-1} \tau_n
\]

\[
= \left(\sum_{c=0}^{b-1} \tau_c\right) \left(\sum_{c=0}^{b-1} \tau_c\right)^l + \tau_{c_0} \left(\sum_{c=0}^{b-1} \tau_c\right) \left(\sum_{c=0}^{b-1} \tau_c\right)^{l-1} + \ldots + \prod_{k=1}^{l} \tau_{c_k} \cdot \left(\sum_{c=0}^{b-1} \tau_c\right) \cdot d(c_0) \cdot d(b)^l.
\]

Now we can make a distinction based on the absolute value of \(d(b) = \sum_{c=0}^{b-1} \tau_c\).

If \(|\sum_{c=0}^{b-1} \tau_c| < 1\), the sum \(\sum_{n=0}^{N-1} \tau_n\) is bounded.

If \(|\sum_{c=0}^{b-1} \tau_c| = 1\), we get \(\sum_{n=0}^{N-1} \tau_n = O(\log N)\).

If \(|\sum_{c=0}^{b-1} \tau_c| > 1\), we are going to prove that for any fixed value of \(\log(\sum_{c=0}^{b-1} \tau_c)\), there exists a continuous and nowhere differentiable function \(F : [0, 1] \to \mathbb{C}\) such that

\[
\sum_{n=0}^{N-1} \tau(n) = F(\log_b N) N^{\frac{\log(\sum_{c=0}^{b-1} \tau_c)}{\log b}}\]

for all \(N \in \mathbb{N}\).

Remark that the final expression given in \[2\] can make sense for any (positive) real number.

**Definition 1.** Given a real number \(x > 0\) and its base \(b\) expansion of the form \(\overline{c_0c_1\ldots c_{l-1}c_{l-1}c_{l-2}\ldots}\), define \(\psi(x) = \psi_{\tau,b}(x)\) as

\[
\psi(x) = \sum_{i=-\infty}^{l} \prod_{k=i+1}^{l} \tau_{c_k} \cdot d(c_i) \cdot d(b)^i.
\]
This definition needs to be justified.

**Proposition 2.1.** Suppose that \( x \) is a number of the form \( x = b^{-m}X \) with \( m, X \in \mathbb{N} \). Then the expression in (4) takes the same value for both expansions of \( x \) in base \( b \).

**Proof.** Suppose that the expansion of \( x \) of finite length is \( \overline{c_{\ell}c_{\ell-1} \ldots c_0.c_{-1}c_{-2} \ldots c_{-m}} \), then the one of infinite length is \( \overline{c_{\ell}c_{\ell-1} \ldots c_0.c_{-1}c_{-2} \ldots (c_{-m} - 1)(b - 1)(b - 1) \ldots} \) and the proposition is equivalent to the identity

\[
\sum_{i = -m}^{l} \prod_{k > i} \tau_{c_k} \cdot d(c_i) d(b)^i = \sum_{i = -m + 1}^{l} \prod_{k > i} \tau_{c_k} \cdot d(c_i) d(b)^i + \prod_{k > -m} \tau_{c_k} \cdot d(c_{-m} - 1) d(b)^{-m} + d(b - 1) \left( \sum_{i = -\infty}^{-m-1} \prod_{k > i} \tau_{c_k} \cdot d(b)^i \right).
\]

After cancelling the terms corresponding to \( i > -m \) from the sums, we get:

\[
\prod_{k > -m} \tau_{c_k} \cdot d(c_{-m}) d(b)^{-m} = \prod_{k > -m} \tau_{c_k} \cdot d(c_{-m} - 1) d(b)^{-m} + d(b - 1) \left( \sum_{i = -\infty}^{-m-1} \prod_{k > i} \tau_{c_k} \cdot d(b)^i \right).
\]

Subtracting the first term of the right-hand side from the left-hand side gives

\[
\prod_{k > -m} \tau_{c_k} \cdot d(c_{-m}) d(b)^{-m} = d(b - 1) \left( \sum_{i = -\infty}^{-m-1} \prod_{k > i} \tau(b - 1) \cdot d(b)^i \right).
\]

After cancellation in products we get the equivalent identity

\[
d(b)^{-m} = d(b - 1) \left( \sum_{i = -\infty}^{-m-1} \prod_{k = i+1}^{i-1} \tau(b - 1) \cdot d(b)^i \right)
\]

which can be reduced by changing indexes to

\[
1 = d(b - 1) \sum_{i = -\infty}^{-1} \tau(b - 1)^{-i-1} d(b)^i.
\]

The right-hand side of this expression is equal to

\[
d(b - 1) \sum_{i = 1}^{\infty} \tau(b - 1)^{-i-1} d(b)^{-i} = \frac{d(b - 1)}{d(b)} \sum_{i = 1}^{\infty} \left( \frac{\tau(b - 1)}{d(b)} \right)^{i-1} = \left( 1 - \frac{\tau(b - 1)}{d(b)} \right) \sum_{i = 1}^{\infty} \left( \frac{\tau(b - 1)}{d(b)} \right)^{i-1} = 1.
\]

By the same method we can get the two following propositions.

**Proposition 2.2.** \( \psi \) is continuous.

**Proof.** Consider a sequence of real numbers \( x_1, x_2, \ldots, x_n, \ldots \) converging to a real \( x > 0 \). Suppose that \( x_n > x \) for all \( n \) or that \( x_n < x \) for all \( n \). We are going to choose a base \( b \) expansion of \( x \) accordingly: if \( x_n > x \), take \( \overline{c_{\ell}c_{\ell-1} \ldots c_0.c_{-1}c_{-2} \ldots} \) to be the expansion of \( x \) not ending with \( b - 1 \)'s, and if \( x_n < x \) take \( \overline{c_{\ell}c_{\ell-1} \ldots c_0.c_{-1}c_{-2} \ldots} \) to be the one not ending with zeroes.
In both cases one can find for any \( m > 0 \) a rank \( N \) such that for any \( n > N \), \( x \) and \( x_n \) have \( m \) identical digits after the radix point. Therefore,

\[
|\psi(x) - \psi(x_n)| = \left| \sum_{i=-\infty}^{m-1} \prod_{k=i}^{m-1} \tau_{\bar{c}_k} \cdot d(c_i) d(b)^i - \sum_{i=-\infty}^{m-1} \prod_{k=i}^{m-1} \tau_{\bar{c}_k} \cdot d(\bar{c}_i) d(b)^i \right|
\leq 2 \max_{c \in \{0, \ldots, b-1\}} \sum_{i=-m}^{i} |d(b)|^i \xrightarrow{m \to \infty} 0
\]

where \( \bar{c}_i \) denote the digits of \( x_n \). Therefore, the sequence \( \psi(x_n) \) converges to \( \psi(x) \).

\[\square\]

**Proposition 2.3.** \( \psi \) is nowhere differentiable.

**Proof.** We are going to to use the following characterizaion of the derivative: if \( f \) is a real function derivable at \( x \) and \( f'(x) = c \) then for every \( \epsilon > 0 \) there exists \( \delta > 0 \) such that for every \( x_1, x_2 \in \mathbb{R} \) verifying \( x - \delta < x_1 \leq x \leq x_2 < x + \delta \) and \( x_1 < x_2 \) we get

\[
c - \epsilon < \frac{f(x_2) - f(x_1)}{x_2 - x_1} < c + \epsilon.
\]

Let \( x \) be a positive real number represented in base \( b \) by the sequence of digits \( c_0c_{-1} \ldots c_{-e-1}c_{-2} \ldots \) that does not end by \( b - 1 \)'s. Let \( J_n \) be the strictly increasing sequence of indexes such that \( c_{-J_n} < b - 1 \). For each \( n \) denote

\[
x_n = c_0c_{-1} \ldots c_{-e-1}c_{-2} \ldots c_{J_n}
\]

and

\[
y_n = c_0c_{-1} \ldots c_{-e-1}c_{-2} \ldots (c_{J_n} + 1).
\]

Then \( y_n > x \geq x_n \) and \( \lim_{n \to \infty} (y_n - x_n) = 0 \) and

\[
\psi(y_n) - \psi(x_n) = \prod_{k \geq J_n} \tau_{\bar{c}_k} d(b)^{-J_n}.
\]

Therefore

\[
\frac{\psi(y_n) - \psi(x_n)}{y_n - x_n} = \left( \frac{d(b)}{b} \right)^{-J_n} \xrightarrow{n \to \infty} +\infty.
\]

This proves that the sequence \( \frac{\psi(y_n) - \psi(x_n)}{y_n - x_n} \) cannot converge to any finite complex number, and, as consequence, the function \( \psi \) cannot be differentiable at \( x \). \( \square \)

By its definition, \( \psi(bx) = d(b) \psi(x) \). Now we can define the function \( F \) satisfying the formula (4). For any \( x > 0 \) denote

\[
F(\log_b x) = \psi(x) x^{\frac{\log d(b)}{\log b}}.
\]

(5)

This is a continuous function of a real argument. In the formula (4), \( \log d(b) \) can be taken to be any fixed value, and the other logarithms are those of positive real arguments, so they are supposed to be real. \( F \) is also periodic of period 1 which finishes the proof of (4). Indeed, if \( y = \log_b x \), then

\[
F(y + 1) = F(\log_b(bx)) = d(b) \psi(x) \cdot b^{\frac{\log d(b)}{\log b}} x^{\frac{\log d(b)}{\log b}} = \psi(x) x^{\frac{\log d(b)}{\log b}} = F(y).
\]

The problem of Newman phenomenon can be challenged using this result. Suppose that \( t_n \) is a \( b \)-multiplicative sequence satisfying the above hypotheses, \( p \) is a prime number coprime to \( b \) and \( \zeta \) is a \( p \)-th root of unity. Then the \( p \)-rarefied sum of \( t_n \) can be written as:

\[
\sum_{n < N} 1_{p|n} t_n = \sum_{n < N} \frac{1}{p} \left( 1 + \zeta^n + \zeta^{2n} + \ldots + \zeta^{(p-1)n} \right) t_n = \frac{1}{p} \left( \sum_{n < N} t_n + \sum_{n < N} \sum_{j \in \mathbb{Z}_p} \zeta^{jn} t_n \right).
\]
If we define \( s \) to be the order of \( b \) in the group \( \mathbb{F}_p^\times \), we obtain that \( \zeta^j t_n \) are \( b^s \)-multiplicative sequences. Applied to the particular case of the Thue-Morse sequence as \( t_n \), our method is the direct generalization of the method used in [2] and [8].

The following chapters will be concentrated on one example of study of the constant \( d(b^s) \) associated to sequences of the form \( \tau_n = \zeta^j t_n \) where \( t_n \) is a precise sequence of \(+1\)s and \(-1\)s. We hope that the tools developed for this example will be useful for similar questions. But before going to particular cases, let’s add a general remark about the rarefied \(+1/−1\) sequences.

Consider, as before, a \( b \)-multiplicative sequence \( t_n \) satisfying the conditions stated at the beginning of this chapter and composed only of numbers \(+1\)s and \(-1\)s. Let \( p \) be a prime number coprime to \( b \), and let \( s, \zeta \) and the sequence \( \tau \) be as above, let \( \langle b \rangle \) be the subgroup of \( \mathbb{F}_p^\times \) generated by \( b \). Then the constant \( d(b^s) \) associated to \( \tau \) is

\[
d(b^s) = \frac{b^s - 1}{\sum_{n=0}^{b^s-1} t_n \zeta^n}
\]

and it can also be written, by the \( b \)-multiplicativity of \( t_n \) as

\[
d(b^s) = \prod_{k=0}^{s-1} \left( \sum_{c=0}^{b-1} t_c b^k c \right) = \prod_{j \in \langle b \rangle} \left( \sum_{c=0}^{b-1} t_c \zeta^{jc} \right).
\]

It follows from this formula that \( d(b^s) \) is an element of a number field of degree at most \( \frac{p-1}{s} \). Indeed, in the group \( \mathbb{F}_p^\times \) there are \( \frac{p-1}{s} \) classes modulo \( \langle b \rangle \) and to each class \([j]\) we can associate the number

\[
\xi[j] = \sum_{n=0}^{b^s-1} t_n \zeta^{jn}.
\]

All the symmetric polynomials in the numbers \( \xi[j] \) are integers which proves our claim.

Given this result, it is natural to study the numbers

\[
\xi[i] = \prod_{j \in \langle b \rangle} \left( \sum_{c=0}^{b-1} t_c \zeta^{jc} \right)
\]

(regardless on whether \( s = \frac{p-1}{b} \)) instead of numbers \( d(b^s) \); this will be the perspective of the following sections.

Let us suggest a notation for the \( b \)-multiplicative sequences composed of \( 1\)s and \(-1\)s by the sequence of \( '+\)' and \( '-1\) signs corresponding to the \( b \) initial terms of the sequence. For instance, with this notation, the Thue-Morse sequence is the sequence \( " + − " \).

3. Poker combinatorics.

This section can be seen as a box of useful tools. Its main result is the following:

**Lemma 3.1.** Let \( p \) be a prime number and \( 0 \leq n < p \) an integer. Denote \( A_0(n, p) \) the number of subsets of \( \mathbb{F}_p^\times \) of \( n \) elements that sum up to \( 0 \) (modulo \( p \)) and \( A_1(n, p) \) the number of those subsets that sum up to \( 1 \). Then

\[
A_0(n, p) - A_1(n, p) = (-1)^n.
\]
Let’s begin the proof with an obvious observation: if we define in analogous way the numbers $A_2(n,p)$, $A_3(n,p)$, $\ldots$, $A_{p-1}(n,p)$, they are all equal to $A_1(n,p)$ since multiplying a set that sums to 1 by a constant residue $c \in \mathbb{F}_p^\times$ gives a set that sum up to $c$, and this correspondence is a bijection.

Let us deal with a simpler version of the lemma that includes order of elements and repetitions, that is, counts the following objects:

**Definition 2.** Denote $E_{x}^{k_1,k_2,\ldots,k_n}(n,p)$ (where $x \in \mathbb{F}_p$ and $k_1,k_2,\ldots,k_n \in \mathbb{F}_p^\times$) the number of sequences $(x_1,x_2,\ldots,x_n)$ of elements of $\mathbb{F}_p$ such that

$$\sum_{i=1}^{n} k_i x_i = x.$$ 

We will also denote $E_{x}^{1,1,\ldots,1}(n,p)$ by $E_x(n,p)$.

Then we get the following

**Proposition 3.2.** If $n$ is even,

$$E_{0}^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n + p - 1}{p} \quad \text{and} \quad E_{1}^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n - 1}{p};$$

if $n$ is odd,

$$E_{0}^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n - p + 1}{p} \quad \text{and} \quad E_{1}^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n + 1}{p}.$$ 

In both cases,

$$E_{0}^{k_1,k_2,\ldots,k_n}(n,p) - E_{1}^{k_1,k_2,\ldots,k_n}(n,p) = (-1)^n.$$

**Proof.** By induction on $n$. For $n = 0$ or $n = 1$ the result is trivial. For bigger $n$ we always get:

$$E_{0}^{k_1,k_2,\ldots,k_n}(n,p) = (n-1)E_{0}^{k_1,k_2,\ldots,k_{n-1}}(n-1,p)$$

and

$$E_{1}^{k_1,k_2,\ldots,k_n}(n,p) = E_{0}^{k_1,k_2,\ldots,k_{n-1}}(n-1,p) + (p-2)E_{1}^{k_1,k_2,\ldots,k_{n-1}}(n-1,p)$$

since the sequences of length $n$ summing up (with coefficients) to $x$ are exactly expansions of sequences of length $n-1$ summing up (again, with coefficients) to another residue than $x$ and the correspondence is a bijection. Injecting formulas for $n-1$ concludes the induction. $\square$

Now we are going to prove Lemma 3.1 for small $n$. If $n = 0$ or $n = 1$, the lemma is clear. For $n = 2$, there is one more sequence $(x,y) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ that sums up to 0, but that counts the sequences of the form $(x,x)$ which should be thrown out. Since $p$ is prime, these sequences contribute once for every non-zero residue modulo $p$, and throwing them out increases the zero’s advantage to 2. Now, we have to identify each couple $(x,y)$ and $(y,x)$ to be the same, so we get the difference 1 back, establishing the lemma 1 for $n = 2$.

For $n = 3$, counting all the sequences $(x,y,z) \in \mathbb{F}_p^\times$ gives a difference $E_0 - E_1 = -1$. The sequences $(x,x,z)$ contribute one time more often to the sum equal to 0, so throwing them out adds −1 to the total difference. The same thing applies to sequences of the form $(x,y,y)$ and $(x,x,y)$. Done that, we get an intermediate difference of −4, but the triples of the form $(x,x,y)$ have been thrown out 3 times, which is equivalent to saying they count −2 times. So they should be "reinjected" with the coefficient 2. As $p$ is prime and bigger than 3, the redundant triples contribute once for each non-zero residue; therefore we accumulate the
difference of \(-4 - 2 = -6\). We have then to identify permutations, that is to divide score by 6 which gives the final result \(-1\).

Now, here is the explicit calculation for the case \(n = 4\):

\[
\begin{align*}
1 & \quad \text{(corresponds to } E_0(4,p) - E_1(4,p)\text{)} \\
+6 & \quad \text{(for throwing out } (x,x,y,z), (x,y,x,z), (x,y,z,x), (x,y,y,z), (x,y,z,x)\text{)} \\
+2 \times 4 & \quad \text{(for reinjecting } (x,x,x,y), (x,x,y,x), (x,y,x,x)\text{ and } (x,y,y,y)\text{)} \\
+1 \times 3 & \quad \text{(for reinjecting } (x,x,y,y), (x,y,x,y), (x,y,y,x)\text{)} \\
+6 \times 1 & \quad \text{(for throwing out } (x,x,x,x)\text{)}
\end{align*}
\]

\[= 24\]

which is \(4!\), therefore the lemma 1 is proved for \(n = 4\).

For a general \(n\) we can calculate the difference between the number of sequences that give 0 and the number of those giving 1 by assigning to all sequences in \(\mathbb{F}_p^n\) an intermediate coefficient equal to one, then by reducing it by one for each couple of equal terms, then increasing by 2 for each triple of equal terms, and so on, proceeding by successive adjustments of coefficients, each step corrsponding to a "poker combination" of \(n\) cards. If after adding the contributions of all the steps and the initial \((-1)^n\), we get \((-1)^n n!\). Lemma 3.1

is valid for \(n\) independently from \(p\) provided that \(p > n\) is prime.

In what follows we are going to formalize the concept of poker combination using the notions exposed in \([9]\). Call a partition of the set \(\{1, 2, \ldots, n\}\) a choice of pairwise disjoint nonempty subsets \(B_1, B_2, \ldots, B_c\) of \(\{1, 2, \ldots, n\}\) of nonincreasing sizes \(|B_i|\), and such that \(B_1 \cup B_2 \cup \cdots \cup B_c = \{1, 2, \ldots, n\}\). The set \(\Pi_n\) of all partitions of \(\{1, 2, \ldots, n\}\) is partially ordered by reverse refinement: for each two partitions \(\pi\) and \(\tau\), we say that \(\pi \geq \tau\) if each block of \(\pi\) is included in a block of \(\tau\). We define the Möbius function \(\mu(\pi, x)\) on \(\Pi_n\) (the definition and notation are due to \([9]\)) recursively by:

if \(x = \{\{1\}, \{2\}, \ldots, \{n\}\} = \emptyset\), then \(\mu(\emptyset, x) = 1\); if \(x\) is bigger than \(\emptyset\), then

\[
\mu(\emptyset, x) = - \sum_{\substack{y \in \Pi_n \\text{ with } y < x}} \mu(\emptyset, y).
\]

Figure 1 illustrates the structure of \(\Pi_n\) in the case \(n = 7\). It brings together all the partitions of \(\{1, 2, \ldots, 7\}\) of the same type that is with the same sequence \((B_1, B_2, \ldots, B_c)\) of sizes of blocks and indicates in the square brackets the values of the Möbius function associated to each type:

This figure uses the following notations (borrowed from poker) for types of partitions:

- Pair: the type \((2, 1, 1, \ldots, 1)\).
- 2p, 3p: two and three pairs respectively i.e. the types \((2, 2, 1, 1, 1)\) and \((2, 2, 2, 1)\).
- \(n\) of a kind: the type \((n, 1, 1, \ldots, 1)\).
- Full House: \((3, 2, 1, 1)\).
- \(n_1 \oplus n_2 \oplus \ldots \oplus n_k\): the type \((n_1, n_2, \ldots, n_k, 1, 1, \ldots, 1)\).

By the Corollary to the Proposition 3 section 7 of \([11]\) and the first Theorem from the section 5.2.1 of \([9]\), if \(x\) is a subdivision of type \((\lambda_1, \lambda_2, \cdots, \lambda_n)\), then

\[
\mu(\emptyset, x) = \prod_{i=1}^{n} (-1)^{\lambda_{i} - 1}(\lambda_{i} - 1)!
\]
but we won’t need this formula directly.

We are also going to use the following definition: let \( s = (x_1, x_2, \ldots, x_n) \) be a sequence of \( n \) nonzero residues modulo \( p \) regarded as a function

\[ s : \{1, 2, \ldots, n\} \rightarrow \mathbb{F}_p^\times. \]

Then its coimage is the partition of \( \{1, 2, \ldots, n\} \) whose blocks are the nonempty preimages of elements of \( \mathbb{F}_p^\times \). Now we can prove the following proposition that puts together all the previous study.

**Proposition 3.3.** The difference

\[ A_0(n, p) - A_1(n, p) \]

*does not depend on* \( p \)* provided that* \( p \)* is a prime number* bigger than* \( n \).

**Proof.** We are going to describe an algorithm that computes this difference (which is the one applied earlier for small values of the argument). For each subdivision \( x \) of the set \( \{1, 2, \ldots, n\} \), denote by \( r_0(x, p) \) the number of sequences \( (x_1, x_2, \ldots, x_n) \) of elements of \( \mathbb{F}_p^\times \) of coimage \( x \) that sum up to 0, denote by \( r_1(x, p) \) the number of those sequences of coimage \( x \) that sum up to 1 and denote \( r(x, p) = r_0(x, p) - r_1(x, p) \). Then,

\[ n!(A_0(n, p) - A_1(n, p)) = r(0, p). \]

Denote, for each subdivision \( y \) of \( \{1, 2, \ldots, n\} \),

\[ s(y, p) = \sum_{x \geq y} r(x, p). \]
Then, by Proposition 3.2
\[
s(y, p) = (-1)^{c(y)}
\]
where \(c(y)\) is the number of blocks in the subdivision \(y\). By the Möbius inversion formula (see [9]),
\[
r(\hat{0}, p) = \sum_{y \in \Pi_n} \mu(\hat{0}, y) s(y, p) = \sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y).
\]
If we compute this sum, we get the value of \(A_0(n, p) - A_1(n, p)\) independently from \(p\).

The last move can seem artificial but it is sufficient to complete the proof of Lemma 3.1. Remark that \(A_0(n, p) = A_0(n, p-1-n)\) since saying that the sum of some subset of \(\mathbb{F}_p^\times\) is 0 is equivalent to saying that the sum of its complement is 0. For the same kind of reason, \(A_1(n, p) = A_{-1}(n, p-1-n) = A_1(n, p-1-n)\).

Now we can prove Lemma 3.1 by induction on \(n\). It has already been proved for small values of \(n\). If \(n > 4\), by Bertrand’s postulate, there is a prime number \(p'\) such that \(n < p' < 2n\). Replace \(p\) by \(p'\) (by the proposition 3.3 this leads to an equivalent statement) then \(n\) by \(p' - 1 - n\) (using the above remark). As \(p' - 1 - n < n\), the step of induction is done.

The two following consequences of the lemma 3.1 have, in fact, a much simpler proof (see, for example [3]).

**Corollary 3.4.** Let \(p\) be prime. Then, in the polynomial ring \(\mathbb{Z}[T]/(T^p - 1)\),
\[
\prod_{j \in \mathbb{F}_p^\times} (1 - T^j) = (p - 1) - \sum_{i \in \mathbb{F}_p^\times} T^i.
\]

**Proof.** By expanding the product we get:
\[
\prod_{j \in \mathbb{F}_p^\times} (1 - T^j) = C_0 + C_1T + C_2T^2 + \ldots + C_{p-1}T^{p-1}
\]
where
\[
C_i = \sum_{n=0}^{p-1} (-1)^n A_i(n, p).
\]
By the properties of the numbers \(A_i(n, p)\), \(C_1 = C_2 = \ldots = C_{p-1}\) and (lemma 3.1) \(C_0 - C_1 = p\). As the sum of all the \(C_i\) is 0, we get necessarily
\[
C_0 = p - 1 \text{ and } C_1 = -1.
\]

**Corollary 3.5.** Let \(p\) be a prime number and \(\zeta\) be a primitive \(p\)-th root of unity. Then,
\[
\prod_{j \in \mathbb{F}_p^\times} (1 - \zeta^j) = p.
\]

**Proof.** This is trivial from the previous result.

---

1 A purely combinatorial and more general proof exists: see the Chapter 3 of [12], formula (31)
4. Some lemmas about Lucas numbers.

The Lucas numbers have the same formula as Fibonacci numbers but different starting terms. Their definition is as follows:

**Definition 3.** The sequence $L_n$ of Lucas numbers is defined by:

\[
L_0 = 2, \\
L_1 = 1, \\
\text{and for every } n \in \mathbb{N} \\
L_{n+2} = L_n + L_{n+1}.
\]

(6)

This is the sequence A000032 in OEIS.

To make clear the problem of offset, let us define the version of Fibonacci sequence that will be used.

**Definition 4.** The sequence of Fibonacci numbers is defined by

\[
F_0 = 0, \\
F_1 = 1, \\
\text{and for every } n \in \mathbb{N} \\
F_{n+2} = F_n + F_{n+1}.
\]

(7)

This chapter collects some properties of Lucas numbers which are analogous to properties of Fibonacci numbers but are difficult to find in literature. The first one draws the relation between both sequences.

**Proposition 4.1.**

\[
\forall n \geq 1 \quad L_n = F_{n-1} + F_{n+1}.
\]

*Proof.* For $n$ equal 1 and 2 this formula is checked directly. For bigger values of $n$, it follows from inductive definitions of Lucas and Fibonacci numbers. \qed

Let us recall the combinatorial definition of Fibonacci numbers: if $n \geq 2$, $F_n$ is the number of ways to put disjoint "dominos" (i.e., subsets of the form $\{k, k+1\}$) on the integer interval $[1, n-1]$. The Lucas numbers have a similar characterization:

**Proposition 4.2.** If $n \geq 3$, $L_n$ is the number of ways to put disjoint "dominos" (i.e., subsets of the form $\{k, k+1\}$) on the circle $\mathbb{Z}/n\mathbb{Z}$.

*Proof.* Distinguish three types of placements of dominos following what happens to a fixed element of $\mathbb{Z}/n\mathbb{Z}$, say to 0.

If in no domino is located at 0, these placements are equivalent to the placements of dominos on the interval $[1, n-1]$ and we count $F_n$ of these.

If there is a domino '0—1', then the remaining have to be placed on the interval $[2, n-1]$ and we count $F_{n-1}$ ways of doing it.
If there is a domino \((p - 1)\rightarrow 0\)', the count is the same with the interval \([1, p - 2]\).

The sum of these three numbers is \(F_n + F_{n-1} + F_{n-1} = F_{n+1} + F_{n-1} = L_n\).

The last property interesting in the perspective of this article is purely of number-theoretical kind.

**Theorem 4.3.** Let \(n \geq 3\) be an odd integer. Then all prime factors of \(L_n\) are either 2 or congruent to 1 or \(-1\) modulo 5.

Its proof follows the one that characterizes the sums of two squares. let’s begin with the following.

**Proposition 4.4.** For each \(n \geq 1\), \(L_{n+1}L_{n-1} = L_n^2 + (-1)^{n+1}5\).

**Proof.** By induction on \(n\). For \(n = 1\), the statement is clear. For bigger \(n\), it is equivalent to
\[
L_{n-1}^2 + L_nL_{n-1} = L_n^2 + (-1)^{n+1}5 \quad \text{(by applying (3) to } L_{n+1}),
\]
\[
L_{n-1}^2 = L_n(L_n - L_{n-1}) + (-1)^{n+1}5,
\]
\[
L_{n-1}^2 + (-1)^n5 = L_nL_{n-2} \quad \text{(by applying it once more to } L_n - L_{n-1}),
\]
which is the proposition 4.4 for \(n - 1\). □

**Proof of Theorem 4.3.** For Lucas numbers with odd index, the proposition 4.4 takes the form:
\[L_nL_{n-2} = L_{n-1}^2 - 5\] (where \(n\) is odd).

If \(p\) is an odd prime number congruent to 2 or 3 modulo 5, by the quadratic reciprocity law the congruence
\[L^2 - 5 \equiv 0 \mod p\]
has no integer solutions, which implies that \(p\) cannot divide \(L_n\). □

5. The particular case of the Thue-Morse sequence.

This chapter and the next one will deal with the problem of study of the numbers
\[
\xi[a] = \prod_{j \in a} \left( \sum_{c=0}^{b-1} t_c \zeta^j \right)
\]
(8)
where \(\zeta\) is a primitive \(p\)-th root of unity (\(p\) prime), \(\Gamma\) is a subgroup of \(\mathbb{F}_p^\times\) and \(t_c \in \{1, -1\}\). The case corresponding to the rarefied Thue-Morse sequence (that is, \(b = 2, t_0 = 1\) and \(t_1 = -1\)) is the one that has been studied rather extensively in the article [8]; in this chapter we are going to recall their results and prove refined versions of some of them.

The first result is: for any sequence \(t_n\) if the subgroup \(\Gamma\) is of even order, all the numbers \(\xi^{[a]}\) are real positive. Indeed, in this case \(-1 \in \Gamma\) therefore the product [8] is composed of pairs of complex-conjugate terms. If \(\Gamma\) is of odd order and the sequence \(t_n\) is the Thue-Morse sequence, then
\[
\prod_{j \in a} (1 - \zeta^j) = \prod_{j \in \frac{1}{2}a} (\zeta^{-j} - \zeta^j) = \prod_{j \in \frac{1}{2}a} \left( 2i \sin \frac{2\pi i}{p} \right)
\]
where \( \frac{1}{2} \) corresponds to the inverse of 2 in \( \mathbb{F}_p \). Therefore, in this case the numbers \( \xi^{[a]} \) are pure imaginary (this is a stronger version of the Proposition 3.3 of [7]).

Therefore, the numbers \( \xi^{[1]} \) and \( \xi^{[i]} \) are explicitly described by their product (equal to \( p \)) and their sum. Some values of the latter are given in the appendix A.

6. The case of the sequence "++−".

In this chapter we are going to answer one question about the sequence "++−" that is, the 3-multiplicative sequence defined by

\[
t_n = (-1)^{\text{the number of '2' digits in the ternary expansion of } n}.
\]

Its initial terms are:

\[
11\bar{1} 11\bar{1} 11\bar{1} 11\bar{1} \ldots \quad (\text{where } \bar{1} \text{ stands for } -1);
\]

this can be seen as the "simplest" particular case of our subject after the Thue-Morse sequence. The main result of this section is the following one:

**Theorem 6.1.** Let \( p \) be an odd prime number and \( \zeta \) a primitive \( p \)-th root of unity. Then,

\[
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 + \zeta - \zeta^2) = L_p,
\]

\( L_p \) being the \( p \)-th Lucas number.

The case \( p = 3 \) is irrelevant to the study of the rarefied "++−" sequences since the 3-rarefied sequence \( t_{3n} \) is identical to \( t_n \). The first terms of the sequence \( L_p \) where \( p \geq 5 \) is prime, are given in the Appendix B.

**Proof of the theorem [6,7]**

We are going to adapt the methods from the Section 3 to prove this result. Begin with some new notations.

**Definition 5.** If \( f \) is a linear application from \( \mathbb{F}_p^{p-1} \) to \( \mathbb{F}_p \) of the form

\[
f(x_1, x_2, \ldots, x_{p-1}) = f_1x_1 + f_2x_2 + \ldots + f_{p-1}x_{p-1}
\]

(9)

where the coefficients \( f_1, f_2, \ldots, f_{p-1} \) are 0 or 2, and \( i \) is an element of \( \mathbb{F}_p \), denote by \( B_i(f, p) \) the number of sequences \( (x_1, x_2, \ldots, x_{p-1}) \) that are permutations of \( \mathbb{F}_p^i \) and such that \( f(x_1, x_2, \ldots, x_{p-1}) = i \), and by \( A_i(f, p) \) the same thing but permutations between places corresponding to the same coefficient \( f_k \) inside the sequence \( (x_1, x_2, \ldots, x_{p-1}) \) (that is, permutations leading to the same expression in (9) are considered to be the same).

We are going to denote by \( n_0(f) \) the number of coefficients of \( f \) equal to 0, by \( n_1(f) \) the number of those equal to 1 and \( n_2(f) \) the number of those equal to 2.

For example, if the coefficients of \( f \) are only 0s and 1s , then

\[
A_i(f, p) = A_i(n_1(f), p) \quad \text{and} \quad B_i(f, p) = n_0(f)!n_1(f)!A_i(n_1(f), p).
\]

As before, the numbers \( B_i(f, p) \) are the same for each \( i \in \mathbb{F}_p^\times \). If we calculate the norm of \( (1 + \zeta - \zeta^2) \) by expanding the product, we get the following: in \( \mathbb{Z}[T]/(T^p - 1) \),

\[
\prod_{j \in \mathbb{F}_p^\times} (1 + T^j - T^{2j}) = C_0 + C_1T + C_2T^2 + \ldots + C_{p-1}T^{p-1}
\]
where
\[ C_i = \sum_{f} (-1)^{n_2(f)} A_i(f, p) \] (10)
the last sum running on all linear combinations satisfying the conditions in definition 5. And,
\[ N(1 + \zeta - \zeta^2) = C_0 - C_1. \] (11)

The differences \( A_0(f, p) - A_1(f, p) \) can be calculated in this new setting. First, in all cases, \( B_i(f, p) = n_0(f)!n_1(f)!n_2(f)!A_i(f, p) \). If the sum of all coefficients of \( f \) is smaller than \( p \), then the algorithm of successive readjustments of coefficients, described in the proposition 5, together with the lemma 1 proves that
\[ B_0(f, p) - B_1(f, p) = (-1)^{n_1(f) + n_2(f)} (n_1(f) + n_2(f))!n_0(f)! \] (12)
which implies
\[ A_0(f, p) - A_1(f, p) = (-1)^{n_1(f) + n_2(f)} \left( \frac{n_1(f) + n_2(f)}{n_1(f)} \right). \] (13)

If the sum of coefficients of \( f \) is greater than (or equal to) \( p \), formulae (12) and (13) no longer work because we can get \( p \) on intermediate stages when adding coefficients of \( f \). To help to this, we can replace \( f \) by the linear combination \( 2 - f \) whose \( k \)-th coefficient is \((2 - f_k)\). Both functions are related by the formula
\[ (2 - f)(x_1, x_2, \ldots, x_{p-1}) = -f(x_1, x_2, \ldots, x_{p-1}) \]
and the new linear combination’s sum of coefficients is \( 2(p - 1) - (2n_2(f) + n_1(f)) < p \) if \( 2n_2(f) + n_1(f) \geq p \). Accordingly to this, the associated difference is
\[ A_0(f, p) - A_1(f, p) = A_0(2 - f, p) - A_1(2 - f, p) = (-1)^{n_0(f) + n_1(f)} \left( \frac{n_0(f) + n_1(f)}{n_0(f)} \right). \] (14)

If we put both formulas (13) and (14) into (10) and (11), we get the following expression (the linear combinations in (10) are indexed first by \( n_0(f) \) then by \( n_2(f) \)):
\[ N(1 + \zeta - \zeta^2) = \sum_{n_0=0}^{p-1} \left( \sum_{n_2=0}^{\min(p-1-n_0, n_0)} (-1)^{p-1-n_0-n_2} \left( \frac{p-1-n_0}{n_2} \right) + \sum_{n_2=n_0+1}^{p-1-n_0} \left( \frac{p-1-n_0}{n_2} \right) \right). \] (15)

Now we are going to identify these numbers as numbers of ways to put dominos on the circle \( \mathbb{Z}/p\mathbb{Z} \) with restrictions. The terms of the first sum that correspond to \( n_0 = \frac{p-1}{2}, \ldots, p-2 \) are zero, and the term corresponding to \( n_0 = p-1 \) is one. Further, each term corresponding to \( n_0 = 0, \ldots, \frac{p-3}{2} \) is equal to the number of putting \( n_0 + 1 \) dominos on the circle \( \mathbb{Z}/p\mathbb{Z} \).

Indeed, call the first domino the first domino encountered when we walk on the circle in the direction 0, 1, 2, \ldots. If no domino is located at \( (p-1) \), suppose that the first domino is located at \( (n_2 - n_0 - 1, n_2 - n_0) \) leaving \( p - 1 - n_2 + n_0 \) free squares after it for the remaining \( n_0 \) dominos. The number of ways to put \( n_0 \) dominos on the line strip of length \( p - 1 - n_2 + n_0 \) is exactly \( \binom{p-1-n_2+n_0}{n_0} \) which is equal to a term of the last sum of (15).

The second sum of (15) can be reduced to a more compact form by the following
Proposition 6.2. For each \( m, n \in \mathbb{N} \) such that \( n \geq m \),

\[
\sum_{k=0}^{m} (-1)^{k+n} \binom{n}{k} = (-1)^{m+n} \binom{n-1}{m}.
\]

Proof. By induction on \( m \). For \( m = 0 \), the statement is trivial. To prove it for \( m + 1 \), apply the induction hypothesis and get:

\[
\sum_{k=0}^{m+1} (-1)^{k+n} \binom{n}{k} = (-1)^{m+n} \binom{n-1}{m} + (-1)^{m+n+1} \binom{n}{m+1} \\
= (-1)^{m+n+1} \left( \binom{n}{m+1} - \binom{n-1}{m} \right) = (-1)^{m+n+1} \binom{n-1}{m-1}.
\]

By this proposition, if \( n_0 < \frac{p-1}{2} \), the second sum of (15) equals

\[
\sum_{n_2=0}^{\min(p-1-n_0, n_0)} (-1)^{n_0+n_2} \binom{p-1-n_0}{n_2} = \binom{p-2-n_0}{n_0}
\]

which is the first term of the third sum which, itself, equals the number of placements of \( n_0 + 1 \) dominos such that one domino is placed at \( '0-1' \). We can identify this term to the number of placements of \( n_0 + 1 \) dominos with one domino placed at \( '(p-1)-0' \) thus completing the description of all possible placements of dominos on the circle \( \mathbb{Z}/p\mathbb{Z} \).

7. Further questions.

In the current state of things, we know much about the Thue-Morse sequence but we only answered the first question about the sequence " + + − ". It could be interesting, on one hand, to see whether the techniques developed here can be used to expand our knowledge about the rarefied Thue-Morse sequences, and therefore, about the class number of the quadratic fields, and, on the other hand, to prove for the sequence " + + − ", analogous results to those we have already for the Thue-Morse sequence. Also, the sequence " + + − " has no reason to be unique in its kind: other multiplicative sequences can have the similar properties.

Furthermore, I think that Carthage must be destroyed.\(^\text{2}\)

\(^2\)Cato the Elder, 234-149 BC
Appendices.

A. Traces of \( \zeta^{[1]} \) corresponding to the subgroup of squares in \( \mathbb{F}_p^\times \) in the Thue-Morse case.

The following table lists some values of \( \text{Tr}_{Q(\sqrt{p})/Q} N_{Q(\zeta)/Q(\sqrt{p})} (1 - \zeta) \) where \( p \) is a prime number congruent to 1 modulo 4 and \( \zeta \) is a primitive \( p \)-th root of unity. These numbers are given in the form of product of numbers that are products of 2 and 5, and of pseudoprimes.

| \( p \) | \( \text{Tr} N(1 - \zeta) \) |
|---|---|
| 5 | 5 |
| 13 | 13 |
| 17 | 2 \cdot 17 |
| 29 | 29 |
| 37 | 2 \cdot 37 |
| 41 | 10 \cdot 41 |
| 53 | 53 |
| 61 | 5 \cdot 61 |
| 73 | 250 \cdot 73 |
| 89 | 2 \cdot 53 \cdot 89 |
| 97 | 2 \cdot 97 \cdot 569 |
| 101 | 2 \cdot 101 |
| 109 | 25 \cdot 109 |
| 113 | 2 \cdot 73 \cdot 113 |
| 137 | 2 \cdot 137 \cdot 149 |
| 149 | 5 \cdot 149 |
| 157 | 17 \cdot 157 |
| 173 | 173 |
| 181 | 97 \cdot 181 |
| 193 | 10 \cdot 109 \cdot 193 \cdot 233 |
| 197 | 2 \cdot 197 |
| 229 | 2 \cdot 173 \cdot 229 |
| 233 | 2 \cdot 37 \cdot 41 \cdot 233 |
| 241 | 50 \cdot 241 \cdot 182969 |
| 257 | 50 \cdot 41 \cdot 257 |
| 269 | 10 \cdot 269 |
| 277 | 157 \cdot 277 |
| 281 | 10 \cdot 281 \cdot 12689 |
| 293 | 293 |
| 313 | 10 \cdot 17 \cdot 29 \cdot 313 \cdot 2909 |
| 317 | 2 \cdot 317 |
| 337 | 2 \cdot 337 \cdot 55335641 |
| 349 | 2 \cdot 17 \cdot 29 \cdot 349 |
| 353 | 2 \cdot 353 \cdot 3793 |
| 373 | 10 \cdot 53 \cdot 373 |
| 389 | 10 \cdot 13 \cdot 389 |
| 397 | 173 \cdot 397 |
B. Lucas numbers of prime index.

The following table lists Lucas numbers \( L(p) \) in the form of product of pseudoprimes for prime numbers \( p \) bigger than 3. Note that, by the Theorem 1 and the fact that \( L(n) \) is even if and only if 3 divides \( n \), all prime factors end by 1 or \(-1\). Note also that some of the last factorizations are long to calculate on software like PARI.

| \( p \) | \( L(p) \) |
|---|---|
| 5 | 11 |
| 7 | 29 |
| 11 | 199 |
| 13 | 521 |
| 17 | 3571 |
| 19 | 9349 |
| 23 | 139 \cdot 461 |
| 29 | 59 \cdot 19489 |
| 31 | 3010349 |
| 37 | 54018521 |
| 41 | 370248451 |
| 43 | 6709 \cdot 144481 |
| 47 | 6643838879 |
| 53 | 119218851371 |
| 59 | 709 \cdot 8969 \cdot 336419 |
| 61 | 5600748293801 |
| 67 | 4021 \cdot 24994118449 |
| 71 | 688846502588399 |
| 73 | 151549 \cdot 11899937029 |
| 79 | 32361122672259149 |
| 83 | 35761381 \cdot 620241259 |
| 89 | 179 \cdot 22235502640988369 |
| 97 | 3299 \cdot 56678557502141579 |
| 101 | 809 \cdot 7879 \cdot 201062946718741 |
| 103 | 619 \cdot 1031 \cdot 5257480026438961 |
| 107 | 47927441 \cdot 479836483312919 |
| 109 | 128621 \cdot 788071 \cdot 593985111211 |
| 113 | 41670427844921037470771 |
| 127 | 509 \cdot 5081 \cdot 487681 \cdot 13822681 \cdot 19954241 |
| 131 | 1049 \cdot 414988698461 \cdot 5477332620091 |
| 137 | 541721291 \cdot 789248787093058281 |
| 139 | 30859 \cdot 253279129 \cdot 14331800109223159 |
| 149 | 952111 \cdot 4434539 \cdot 3263039535803245519 |
| 151 | 1511 \cdot 109734721 \cdot 217533000184835774779 |
| 157 | 39980051 \cdot 16188856575286517881849171 |
| 163 | 1043201 \cdot 6601501 \cdot 1686454671192230445929 |
| 167 | 766531 \cdot 103849927693584542320127327909 |
| 173 | 78889 \cdot 6248069 \cdot 16923049609 \cdot 171246170261359 |
| 179 | 359 \cdot 1066737847220321 \cdot 66932254279484647441 |
| 181 | 97379 \cdot 21373261504197751 \cdot 3224235648564069 |
| 191 | 22921 \cdot 395586472506832921 \cdot 910257559954057439 |
| 193 | 303011 \cdot 76225351 \cdot 935527893146187207403151261 |
| 197 | 31498587119111339 \cdot 470190722895068350249889 |
A source code to compute the Thue-Morse sequence.

The following fragments of source codes are intended to calculate a value of the Thue-Morse sequence and they can be inserted into a C program. They use as input a variable \( n \) of type \texttt{unsigned int} and a variable \texttt{thueMorse} of type \texttt{int}, and assign to \texttt{thueMorse} the value

\[
t_n = (-1)^t \text{ the number of ‘1’ digits in binary expansion of } n.
\]
The following code is written in the AT&T syntax and designed for compilation by gcc.

```
asm("movl $1, %0;
    "cmpl $0, %1;
    "jnp _byte2;
    "negl %0;
    "_byte2:;
    "roll $8,%1;
    "cmpl $0, %1;
    "jnp _byte3;
    "negl %0;
    "_byte3:;
    "roll $8,%1;
    "cmpl $0, %1;
    "jnp _byte4;
    "negl %0;
    "_byte4:;
    "roll $8,%1;
    "cmpl $0, %1;
    "jnp _fini;
    "negl %0;
    "_fini:;"
); 
```

Users of Visual C++ will need the following version (written with INTEL syntax) instead:

```
__asm{
    push eax
    push ebx
    mov ebx, n

    mov eax, 1
    cmp ebx, 0
    jnp _byte2
    neg eax
    _byte2:
    rol ebx, 8
    cmp ebx, 0
    jnp _byte3
    neg eax
    _byte3:
    rol ebx, 8
    cmp ebx, 0
    jnp _byte4
    neg eax
    _byte4:
    rol ebx, 8
    cmp ebx, 0
    jnp _fini 
}```
These inline assembly codes outperform anything that can be written in C, which is why I suggest to use them as a fragment of code instead of function.

References

[1] Z.I. Borevitch et I.R. Shafarevitch, *Théorie des nombres*, Gautier-Villars Paris (1967).

[2] J. Coquet, A summation formula related to the binary digits, *Inv. Math.* 73 (1983), 123–137.

[3] H.G. Diamond and H. Pollard, *The theory of algebraic numbers 2nd edition*, The Mathematical Association of America (1975)

[4] M. Drmota and J. Morgenbesser, Generalized Thue-Morse sequence of Squares, accepted for publication (2010) in *Israel Journal of Number Theory*, the full text is available at: [http://dmg.tuwien.ac.at/jmorgen/ConfPub.html](http://dmg.tuwien.ac.at/jmorgen/ConfPub.html).

[5] M. Drmota and M. Skalba, Rarified sums of the Thue-Morse sequence, *Trans. Amer. Math. Soc.* 352 (1999), 609–640.

[6] M. Drmota and Th. Stoll, Newman’s phenomenon for generalized Thue-Morse sequences, *Discrete Math.* 308 (2008) no.7, 1191–1208.

[7] S. Goldstein, K. Kelly and E. Speer, The Fractal Structure of Rarefied Sums of the Thue-Morse Sequence, *J. Number Theory* 42 (1992), 1–19.

[8] P.J. Grabner, A note on the parity of the sum-of-digits function, *Actes 30ième Séminaire Lotharingien de Combinatoire* (Gerolfingen, 1993), 35–42.

[9] J.P.S. Kung, G.-C. Rota and C.-H. Yan, *Combinatorics: The Rota Way*, Cambridge University Press (2009).

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

[11] G.-C. Rota, On the Foundations of Combinatorial Theory I. Theory of Möbius Functions, *Z. Wahrscheinlichkeitstheorie* 2 (1964), 340–368.

[12] R.P. Stanley, *Enumerative combinatorics*, Cambridge University Press (1997).