Periodica Mathematica Hungarica Vol. 38 (1–2), (1999), pp. 111–130

SUMMATORY FUNCTIONS OF DIGITAL SUMS OCCURRING IN CRYPTOGRAPHY

JÖRG M. THUSWALDNER (Leoben)

[Communicated by: Attila Pethő]

Abstract

Morain and Olivos gave two algorithms that allow fast exponentiation in elliptic curve cryptosystems. These algorithms are based on representations of integers in certain redundant binary number systems. In this paper we consider the weight and the sum of digits function of these representations. In particular, we give formulas for their summatory functions. In the proofs we use the Mellin–Perron formula. In order to apply this formula, we have to compute the analytic continuation of a class of Dirichlet series.

1. Introduction

Raising a given element of a group to large powers is an important operation in many public-key cryptosystems. Since powering is time consuming one is interested in algorithms that allow fast exponentiation. Of course, these algorithms depend on the cryptosystem in use as well as on the group on that the cryptosystem operates. A survey over the variety of known algorithms is given in Gordon [11].

In some cryptosystems, such as Diffie-Hellmann key exchange [10], a fixed number is raised to different powers. Here one could save time at the cost of storage by precomputing certain powers of this number. Other systems, for instance RSA [8], need different numbers to be raised to a fixed power. In this case it would save time to have a short *addition chain* for the exponent under consideration. An addition chain (cf. Knuth [3]) for an exponent k is an $(r+1)$-tuple $(k_0, \dots, k_r)$ of positive integers such that $k_0 = 1$, $k_r = k$ and

$$k_i = k_j + k_l \quad (1 \le j \le l < i \le r).$$

Thus, if there exists an addition chain of length r, we can compute the k-th power of a number x with r multiplications: Just compute $x^{k_0}, x^{k_1}, \dots, x^{k_r} = x^k$. Concerning the length of the shortest addition chain for k, call it $l(k)$, Erdős [15] proved that

$$l(k) = \log k + (1 + o(1))\frac{\log k}{\log \log k}.$$

Mathematics subject classification numbers, 11A63, 11M41, 68P25.
Key words and phrases. Digital sum, Dirichlet series, cryptosystem.

0031-5303/99/$5.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

One could reduce the length of an addition chain further by allowing other operations. For instance, if one allows subtraction, one obtains so called *addition-subtraction chains* (cf. Morain-Olivos [5]). An addition-subtraction chain for an exponent k is an $(r+1)$-tuple $(k_0, \dots, k_r)$ of integers such that $k_0 = 1$, $k_r = k$ and

$$k_i = \pm k_j \pm k_l \quad (1 \le j \le l < i \le r).$$

Unfortunately, subtraction in the exponent causes division, and division is in general more time consuming than multiplication. Morain and Olivos observed that this is not the case for elliptic curves, for which the inverse of a point (x, y) can be computed almost freely. For the curves $E(p) : y^2 = x^3 + ax + b$ over $GF(p)$ with $p > 3$ the inverse of a point (x, y) is $(x, -y)$. Hence, for cryptosystems on elliptic curves, which need the computation of kP for a fixed integer k and certain points $P \in E(p)$ of the elliptic curve, addition-subtraction chains are helpful to save time.

Morain and Olivos construct two algorithms that use addition-subtraction chains to compute large powers of a given number. The cost of these algorithms depends on the number of nonzero digits of the exponent k in certain representations with respect to base two. The easiest way is to work with the binary representation of k. Starting from this representation they construct representations of k in redundant number systems having base 2 and set of digits $\{-1, 0, 1\}$. The number of nonzero digits in these representations is on average smaller than in the binary representation. This causes a save of time.

The expectation μ of the nonzero digits in such a representation provides a measure for the average number of multiplications needed to compute the k-th power. Morain and Olivos gave only the main term of μ. The aim of this paper is to give an exact formula for μ for the first algorithm. For the second one we provide an asymptotic formula containing a periodic fluctuation in its second term. Furthermore, we compute formulas for the expected value of the sum of digits in these representations. Since -1 is also an element of the digit set, the sum of digits is not equal to the number of nonzero digits. If for some cryptosystem multiplication and subtraction have different cost, it is valuable to know wether there are more multiplications or more divisions to perform. This information comes from the expectation of the sum of digits function.

For the ordinary q-adic sum of digits function $\nu_q(n)$ Delange [7] computed the exact formula

$$\sum_{n<N} \nu_q(n) = \frac{q-1}{2} N \log_q N + N\Phi(\log_q N).$$

for its summatory function. Here Φ denotes a periodic fluctuation of period 1. In our first algorithm the main term of the summatory function of the sum of digits function is $\frac{1}{3} N \log_2 N$, which means, that the number of 1's is significantly larger than the number of -1's in the corresponding representation. In the second case the main term of the summatory function of the sum of digits function is of order N (i. e. $N \log_2 N$ has coefficient 0), which means that the number of 1's and -1's is roughly the same.

In the proof of the main results of the present paper, Dirichlet series play a prominent rôle. In particular, we need the meromorphic continuation of Dirichlet

series of the form

$$Z_q(s) = \sum_{j\geq 0} j^q (cd^j)^{-s} \zeta\left(s, \frac{a}{c} + \frac{b}{cd^j}\right),$$

where $\zeta(s,\alpha) = \sum_{n\geq 0}(n+\alpha)^{-s}$ denotes the Hurwitz zeta function. Since this result is of interest in its own right, we formulate it as an additional theorem.

In Section 2 we present the main results of the paper, Section 3 contains preliminary work and in Section 4 we prove the first main result. In Section 5 the meromorphic continuation of a class of Dirichlet series is esteblished, which is applied in Section 6, where the second main result is proved.

2. Statement of results

The first algorithm of Morain and Olivos [5] works with a representation that emerges from the ordinary binary one by the following transformation ($\bar{1}$ denotes the digit -1):

$$1^a \mapsto 10^{a-1}\bar{1}.$$

This means that a block of at least two ones is replaced by a block of zeros and a division. This transformation can be visualized by the automaton in Figure 1. It reads the binary representation of an integer from right to left and writes out the representation for the first algorithm. The labelling $\delta_1|\delta_2$ means that if the automaton reads the digit δ_1 it writes out the string δ_2. $\delta_1|-$ means that the automaton does not write out anything passing the corresponding edge.

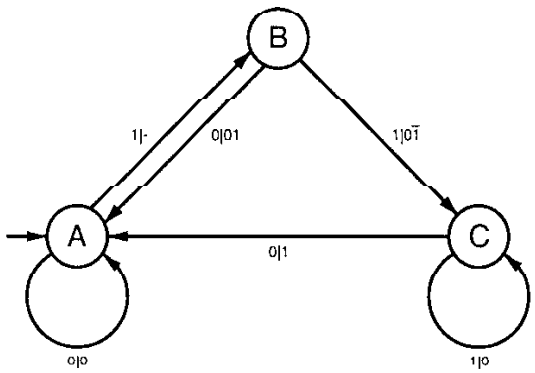

Fig. 1. The automaton corresponding to the first algorithm

Let $w_1(n)$ be the weight of n in this representation, i.e. the number of nonzero digits of n. Furthermore, let $\nu_1(n)$ be the sum of digits function of n in this representation. With these notations we get the following result.

THEOREM 2.1. *The summatory functions of the weight $w_1(n)$ and the sum of digits $\nu_1(n)$ are given by*

$$\sum_{n<N} w_1(n) = \frac{3}{8} N \log_2 N + N F_1(\log_2 N) + G_1(N)$$

and

$$\sum_{n<N} \nu_1(n) = \frac{1}{8} N \log_2 N + N F_2(\log_2 N) + G_2(N).$$

$F_1(x)$, $F_2(x)$ are periodic fluctuations of period 1. If $E_{a,b}(N)$ is defined as in Lemma 4.1 and $\psi_{k;a,b}$ ($k \in \mathbb{Z}$) and $H_{a,b}(N)$ are defined as in Lemma 4.2, then the Fourier coefficients of $F_1(x)$ and $F_2(x)$ are given by

$$\begin{aligned}
f_0^{(1)} &:= -\psi_{0;28,32} + \frac{1}{4}, \\
f_k^{(1)} &:= -\psi_{k;28,32} \quad (k \neq 0), \\
f_0^{(2)} &:= \psi_{0;4,16} - \psi_{0;12,32} + \frac{1}{4}, \\
f_k^{(2)} &:= \psi_{k;4,16} - \psi_{k;12,32} \quad (k \neq 0),
\end{aligned}$$

respectively. The functions $G_1(x)$, $G_2(x)$ are defined by

$$\begin{aligned}
G_1(N) &:= E_{1,4}(N) + E_{3,8}(N) - E_{14,16}(N) - E_{0,4}(N) - H_{28,32}(N), \\
G_2(N) &:= E_{1,4}(N) - E_{3,8}(N) - E_{14,16}(N) - 2E_{6,16}(N) + H_{4,16}(N) - H_{12,32}(N).
\end{aligned}$$

The second algorithm is a slight improvement of the first one. In particular, it allows to remove an additional nonzero digit if isolated zeros occur in the representation of n. Using the first algorithm we get

$$1^a 0 1^b \mapsto 10^{a-1}\bar{1}10^{b-1}1.$$

Since $-2+1=-1$ we can now replace the string 11 by the string $0\bar{1}$. This yields

$$1^a 0 1^b \mapsto 10^a\bar{1}0^{b-1}1.$$

Again we can show this transformation with help of an automaton (cf. Figure 2).

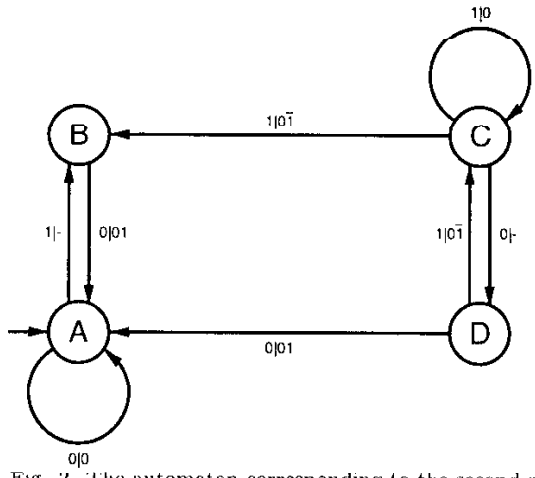

Fig. 2. The automaton corresponding to the second algorithm

As above, define $w_2(n)$ to be the weight of n and $\nu_2(n)$ to be the sum of digits of n in this representation. Then we get the following result.

THEOREM 2.2. *The summatory functions of the weight $w_2(n)$ and the sum of digits $\nu_2(n)$ are given by*

$$\sum_{n<N} w_2(n) = \frac{1}{3} N \log_2 N + N F_3(\log_4 N) + \mathcal{O}\left(N^{1-\varepsilon}\right)$$

and

$$\sum_{n<N} \nu_2(n) = N F_4(\log_4 N) + \mathcal{O}\left(N^{1-\varepsilon}\right)$$

for $\varepsilon > 0$ small enough. $F_3(x)$ and $F_4(x)$ are periodic fluctuations of period 1. If $\varphi_{k;a,b,c}$ is defined as in Lemma 6.1 and $\varphi^{(0)}_{k;a,b,c}$ is defined as in Lemma 6.2, then the Fourier coefficients of the fluctuations $F_3(x)$ and $F_4(x)$ are given by

$$\begin{aligned}
f_0^{(3)} &:= \varphi_{0;\frac{8}{3},-\frac{2}{3},16} - \varphi_{0;\frac{40}{3},-\frac{1}{3},16} - \frac{1}{4},\\
f_k^{(3)} &:= \varphi_{k;\frac{8}{3},-\frac{2}{3},16} - \varphi_{k;\frac{40}{3},-\frac{1}{3},16} \quad (k \neq 0),\\
f_0^{(4)} &:= -2\left(\varphi^{(0)}_{0;\frac{8}{3},-\frac{2}{3},16} + \varphi^{(0)}_{0;\frac{80}{3},-\frac{2}{3},32} + \varphi^{(0)}_{0;\frac{4}{3},-\frac{1}{3},8} + \varphi^{(0)}_{0;\frac{40}{3},-\frac{1}{3},16}\right)\\
&\quad - \varphi_{0;\frac{8}{3},-\frac{2}{3},16} - 2\varphi_{0;\frac{80}{3},-\frac{2}{3},32} - \varphi_{0;\frac{40}{3},-\frac{1}{3},16} + \frac{3}{4},\\
f_k^{(4)} &:= -2\left(\varphi^{(0)}_{k;\frac{8}{3},-\frac{2}{3},16} + \varphi^{(0)}_{k;\frac{80}{3},-\frac{2}{3},32} + \varphi^{(0)}_{k;\frac{4}{3},-\frac{1}{3},8} + \varphi^{(0)}_{k;\frac{40}{3},-\frac{1}{3},16}\right)\\
&\quad - \varphi_{k;\frac{8}{3},-\frac{2}{3},16} - 2\varphi_{k;\frac{80}{3},-\frac{2}{3},32} - \varphi_{k;\frac{40}{3},-\frac{1}{3},16} \quad (k \neq 0),
\end{aligned}$$

respectively.

We prove our results with help of the Mellin–Perron formula. This formula

says that for a number $c > 0$ lying in the half-plane of absolute convergence of the Dirichlet series $\sum_{n\geq 1} \lambda_n n^{-s}$ for any $m \in \mathbb{N}$ one has

$$\frac{1}{m!}\sum_{1\leq n\leq N} \lambda_n \left(1-\frac{n}{N}\right)^m = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \left(\sum_{n\geq 1}\frac{\lambda_n}{n^s}\right) N^s \frac{ds}{s(s+1)\cdots(s+m)}.$$

We will need the case $m = 1$. The Dirichlet series in our case are the Dirichlet generating functions of the first differences of $w_j(n)$ and $\nu_j(n)$ $(j = 1, 2)$. Shifting the line of integration and taking residues into account will give asymptotic expansions for the desired summatory functions.

3. The first differences of the weights and the sum of digits function

Applying the Mellin–Perron summation formula with $m = 0$ would cause that the integrand would not allow shifting the line of integration sufficiently far to the left. Thus we are forced to apply it with $m = 1$. Since for $b_n = a_n - a_{n-1}$ we have

$$\sum_{n<N} a_n = N\sum_{n<N} b_n\left(1-\frac{n}{N}\right) \tag{1}$$

if $a_0 = 0$, we have to work with the first differences of $w_1(n), w_2(n), \nu_1(n)$ and $\nu_2(n)$. Denote the difference operator by Δ. We start with the first algorithm. Observing the change of digits between consecutive numbers with help of the automaton in Figure 1 we get the values of $\Delta w_1(n)$ and $\Delta\nu_1(n)$ indicated in Table 1.

n	$\Delta w_1(n)$	$\Delta\nu_1(n)$
$n \equiv 1 \pmod 4$	1	1
$n \equiv 7 \pmod 8$	0	0
$n \equiv 3 \pmod 8$	1	-1
$n \equiv 2 \pmod 8$	0	0
$n \equiv 14 \pmod{16}$	-1	-1
$n \equiv 6 \pmod{16}$	0	-2
$n \equiv 4\cdot 2^j \pmod{16\cdot 2^j}$, $(j \geq 0)$	-1	1
$n \equiv 12\cdot 2^j \pmod{32\cdot 2^j}$, $(j \geq 0)$	-1	-1
$n \equiv 28\cdot 2^j \pmod{32\cdot 2^j}$, $(j \geq 0)$	-2	0

Table 1

Observe that the last three families of congruences cover all $n \equiv 0 \pmod 4$. Since $w_1(n) - w_1(n-1) = -1$ for two of these three congruences, we collect all three of them to the congruence $n \equiv 0 \pmod 4$. What remains is -1 for the last

congruence. Hence, we get by (1) the following formula:

$$\begin{aligned}\sum_{n<N} w_1(n) &= \sum_{n<N} (N-n)\Delta w_1(n)\\ &= \sum_{\substack{n\equiv 1 \pmod 4\\ n<N}} (N-n) + \sum_{\substack{n\equiv 3 \pmod 8\\ n<N}} (N-n) - \sum_{\substack{n\equiv 14 \pmod{16}\\ n<N}} (N-n)\\ &\quad - \sum_{\substack{n\equiv 0 \pmod 4\\ n<N}} (N-n) - \sum_{j\geq 0} \sum_{\substack{n\equiv 28\cdot 2^j \pmod{32\cdot 2^j}\\ n<N}} (N-n).\end{aligned} \tag{2}$$

In the case of the sum of digits function $\nu_1(n)$ we get in a similar way

$$\begin{aligned}\sum_{n<N} \nu_1(n) &= \sum_{n<N} (N-n)\Lambda\nu_1(n)\\ &= \sum_{\substack{n\equiv 1 \pmod 4\\ n<N}} (N-n) - \sum_{\substack{n\equiv 3 \pmod 8\\ n<N}} (N-n) - 2\sum_{\substack{n\equiv 0 \pmod{16}\\ n<N}} (N-n)\\ &\quad - \sum_{\substack{n\equiv 14 \pmod{16}\\ n<N}} (N-n) + \sum_{j\geq 0} \sum_{\substack{n\equiv 9\cdot 2^j+2 \pmod{2^{j+4}}\\ n<N}} (N-n)\\ &\quad - \sum_{j\geq 0} \sum_{\substack{n\equiv 7\cdot 2^{j+2} \pmod{2^{j+5}}\\ n<N}} (N-n).\end{aligned} \tag{3}$$

For the second algorithm the dependencies of $\Delta w_2(n)$ and $\Delta\nu_2(n)$ on the binary expansion of n are a little bit more complicated, according to the more complex structure of the automaton in Figure 2. The values are indicated in Table 2.

n	$\Delta w_2(n)$	$\Delta\nu_2(n)$
$n \equiv 1 \pmod 4$	1	1
$n \equiv 7 \pmod 8$	0	0
$n \equiv 0 \pmod 4$	-1	1
$n \equiv \frac{8}{3}4^j - \frac{2}{3} \pmod{16\cdot 4^j}$, $(j \geq 0)$	1	$-(2j+1)$
$n \equiv \frac{80}{3}4^j - \frac{2}{3} \pmod{32\cdot 4^j}$, $(j \geq 0)$	0	$-(2j+2)$
$n \equiv \frac{4}{3}4^j - \frac{1}{3} \pmod{8\cdot 4^j}$, $(j \geq 0)$	0	$-2j$
$n \equiv \frac{40}{3}4^j - \frac{1}{3} \pmod{16\cdot 4^j}$, $(j \geq 0)$	-1	$-(2j+1)$

Table 2

With help of Table 2 we can establish similar formulas as in (2) and (3) for $w_2(n)$ and $\nu_2(n)$.

In all these formulas the sums corresponding to simple congruences can be evaluated in an elementary way. For the sums caused by the families of congruences with parameter j we need the Mellin–Perron formula in order to get the value of these sums from the poles of the related Dirichlet series.

4. Proof of Theorem 2.1

We prove the theorems with help of two lemmas. The first of them is simple and treats the simple congruences. The proof of the second one makes use of the Mellin–Perron summation formula and gives the expressions of the more complicated sums depending on j.

We use the following notations. For $x \in \mathbb{R}$ we denote by $[x]$ the greatest integer being less or equal to x and by $\{x\}$ the fractional part of x. Furthermore $\mathbb{N}$ denotes the set of positive integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{R}$ denotes the set of real numbers and $\mathbb{R}^+$ denotes the set positive real numbers.

LEMMA 4.1. *For $a \in \mathbb{N}_0$ and $b \in \mathbb{N}$ with $a < b$ we have*

$$S_{a,b}(N) := \sum_{\substack{n \equiv a \pmod b \\ n < N}} (N - n) = \frac{N^2}{2b} + \left(\frac{1}{2} - \frac{a}{b}\right) N + E_{a,b}(N),$$

where $E_{a,b}(N)$ is a periodic function of period b defined by

$$E_{a,b}(N) = \frac{a}{2}\left(\frac{a}{b} - \frac{1}{2}\right) + \frac{b}{2}\left(\left\{\frac{N-a}{b}\right\} - \left\{\frac{N-a}{b}\right\}^2\right).$$

PROOF. An application of the Gaussian summation formula yields

$$\sum_{\substack{n \equiv a \pmod b \\ n < N}} (N - n) - (N - a)\left[\frac{N-a}{b} + 1\right] - \frac{b}{2}\left[\frac{N-a}{b}\right]\left[\frac{N-a}{b} + 1\right].$$

Using $[x] = x - \{x\}$ yields the result.

In the next lemma we need the Hurwitz zeta function

$$\zeta(s, \alpha) = \sum_{n \geq 0} \frac{1}{(n + \alpha)^s} \quad (\alpha \in (0, 1]).$$

This function can be analytically continued to the whole complex plane with a simple pole at 1. (cf. [14, Chapter XIII]). It has also been used by Mauclaire and Murata [16], [17] to get exact formulas for certain q-additive functions.

LEMMA 4.2. *Let $a, c \in \mathbb{N}$, $b = 2^c$, with $a < b$. Then we have the exact formula*

$$\begin{aligned} T_{a,b}(N) &:= \sum_{j \geq 0} \sum_{\substack{n \equiv a2^j \pmod{b2^j} \\ n < N}} (N - n) \\ &= \frac{N^2}{b} + \left(\frac{1}{2} - \frac{a}{b}\right) N \log_2 N + \Psi_{a,b}(\log_2 N) N + H_{a,b}(N), \end{aligned}$$

where $\Psi_{a,b}$ is a periodic fluctuation of period 1 and with Fourier coefficients ($\chi_k =$

$\frac{2\pi i}{\log 2}$)

$$\psi_{0;a,b} = \left(\frac{1}{2} - \frac{a}{b}\right)\left(\log_2 b + \frac{1}{2} - \frac{1}{\log 2}\right) - \frac{1}{2}\log_2(2\pi) + \log_2 \Gamma\left(\frac{a}{b}\right), \tag{4}$$

$$\psi_{k;a,b} = \frac{b^{-\chi_k}\zeta\left(\chi_k, \frac{a}{b}\right)}{\chi_k(\chi_k+1)\log 2} \tag{5}$$

and

$$H_{a,b}(N) := \sum_{\ell=0}^{c-1}\left(\frac{a}{2}\left(\frac{1}{2} - \frac{a}{b}\right) + \frac{b}{2}\left(\left\{\frac{2^\ell N - a}{b}\right\}^2 - \left\{\frac{2^\ell N - a}{b}\right\}\right)\right)$$

is a periodic function with period b.

PROOF. In the first step of our proof we apply the Mellin–Perron formula to the sum

$$T_{a,b}(N) := \sum_{j\geq 0} \sum_{\substack{n\equiv a2^j \pmod{b2^j} \\ n<N}} (N-n).$$

To this matter we need the Dirichlet series

$$\sum_{j\geq 0} \sum_{n\equiv a2^j \pmod{b2^j}} \frac{1}{n^s} = \frac{b^{-s}\zeta(s, \frac{a}{b})}{1-2^{-s}}.$$

Now we get

$$T_{a,b}(N) = \frac{N}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{b^{-s}\zeta\left(s, \frac{a}{b}\right)}{1-2^{-s}} N^s \frac{ds}{s(s+1)}.$$

Since $\zeta(\alpha, \sigma+it) = \mathcal{O}(|t|^{\frac{3}{4}})$ for $\sigma \geq -\frac{1}{4}$ we may shift the line of integration to $-\frac{1}{4}$. Taking residues into account yields

$$\begin{aligned} T_{a,b}(N) = {} & \frac{N^2}{b} + \left(\frac{1}{2} - \frac{a}{b}\right) N\log_2 N + \Psi_{a,b}(\log_2 N)N \\ & - \frac{N}{2\pi i}\int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty} \frac{b^{-s}\zeta\left(s, \frac{a}{b}\right)}{1-2^{-s}} N^s \frac{ds}{s(s+1)}, \end{aligned} \tag{6}$$

where $\Psi_{a,b}$ is a fluctuation of period 1 with Fourier coefficients as indicated in the statement of the lemma. Note that we used the expansion

$$\zeta(s,\alpha) = \left(\frac{1}{2} - \alpha\right) + \left(\log\Gamma(\alpha) - \frac{1}{2}\log(2\pi)\right)s + \mathcal{O}\left(s^2\right)$$

of the Hurwitz zeta function (cf. [2]) to determine the residue of the double pole at 0. What remains is to treat the integral in (6). Following [9] we use the expansion

$$\frac{1}{2^s - 1} = -\sum_{\ell\geq 0} 2^{\ell s}$$

which is valid for $\Re s < 0$ to get

$$\frac{N}{2\pi i}\int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty}\frac{b^{-s}\zeta\left(s,\frac{a}{b}\right)}{1-2^{s}}N^{s}\frac{ds}{s(s+1)}$$
$$=-\sum_{\ell\geq 0}\frac{N}{2\pi i}\int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty}b^{-s}\zeta\left(s,\frac{a}{b}\right)(2^{\ell}N)^{s}\frac{ds}{s(s+1)}.$$

To evaluate the integrals under the sum we first observe that shifting back the line of integration to 2 yields

$$\begin{aligned}&\frac{N}{2\pi i}\int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty}b^{-s}\zeta\left(s,\frac{a}{b}\right)(2^{\ell}N)^{s}\frac{ds}{s(s+1)}\\&=\frac{N}{2\pi i}\int_{2-i\infty}^{2+i\infty}b^{-s}\zeta\left(s,\frac{a}{b}\right)(2^{\ell}N)^{s}\frac{ds}{s(s+1)}\\&\quad-\left(\frac{1}{2}-\frac{a}{b}\right)N-\frac{2^{\ell-1}N^{2}}{b}.\end{aligned}\tag{7}$$

But for the latter integral we have by the Mellin–Perron formula

$$I_{\ell}:=\frac{N}{2\pi i}\int_{2-i\infty}^{2+i\infty}b^{-s}\zeta\left(s,\frac{a}{b}\right)(2^{\ell}N)^{s}\frac{ds}{s(s+1)}=2^{-\ell}\sum_{\substack{n\equiv a\,(\mathrm{mod}\,b)\\ n<2^{\ell}N}}(N-n).$$

An application of Lemma 4.1 yields, keeping in mind that $b=2^{c}$,

$$I_{\ell}=\begin{cases}\frac{2^{\ell-1}N^{2}}{b}+\left(\frac{1}{2}-\frac{a}{b}\right)N+\left(\frac{a}{2}\left(\frac{a}{b}-\frac{1}{2}\right)+\frac{b}{2}\left(\left\{\frac{2^{\ell}N}{b}-\frac{a}{b}\right\}-\left\{\frac{2^{\ell}N}{b}-\frac{a}{b}\right\}^{2}\right)\right)\\ \qquad\qquad\text{for } \ell<c\\ \frac{2^{\ell-1}N^{2}}{b}+\left(\frac{1}{2}-\frac{a}{b}\right)N\\ \qquad\qquad\text{for } \ell\geq c\end{cases}$$

Inserting this in (7) and summing up over ℓ, all the terms corresponding to $\ell\geq c$ cancel out and we get

$$\frac{N}{2\pi i}\int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty}\frac{2^{-cs}\zeta\left(b2^{2-c},s\right)}{1-2^{-s}}N^{s}\frac{ds}{s(s+1)}=H_{a,b}(N).$$

This completes the proof of the lemma.

The theorem now follows immediately by applying Lemmas 4.1 and 4.2 to the sums in (2) and (3).

5. Meromorphic continuation of a class of Dirichlet series

The meromorphic continuation of the Dirichlet series occurring in the proof of Lemma 4.2 are well known. In the proof of Theorem 2.2 we need Dirichlet series

of the shape

$$Z_q(s) := \sum_{j\geq 0} \sum_{n\equiv a4^j+b \pmod{c4^j}} \frac{j^q}{n^s}$$

for $q \in \{0,1\}$ and $a \in \mathbb{R}^+, b \in \mathbb{R}, c \in \mathbb{N}$, such that $0 < a+b < c$ and $a4^j + b \in \mathbb{N}_0$ for all $j \in \mathbb{N}_0$.

Despite the meromorphic continuation of large classes of Dirichlet series is known (cf. Müller [6], [4] and Grabner–Thuswaldner [13]), the continuation of Z_q seems to be unknown in literature. Thus we want to establish its continuation in this section. We start with the case $q = 0$.

It is not hard to see that

$$Z_0(s) = \sum_{j\geq 0} (c4^j)^{-s} \zeta\left(s, \frac{a}{c} + \frac{b}{c4^j}\right).$$

Using the integral representation (cf. [14, p. 266])

$$\zeta(s,\alpha) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{e^{-\alpha x}}{1-e^{-x}} x^{s-1} dx, \tag{8}$$

some simple computations yield

$$Z_0(s) = \frac{1}{c^s \Gamma(s)} \int_0^\infty y^{s-1} \exp\left(-\frac{b}{c} y\right) \sum_{j\geq 0} f(4^k y) dy \tag{9}$$

with

$$f(x) = \frac{\exp(-\frac{a}{c}x)}{1-\exp(-x)}.$$

Now we want to establish the meromorphic continuation of $Z_0(s)$ via Mellin transform techniques (cf. [1] for the discussion of some important properties of the Mellin transform). To this matter we want to get an asymptotic expansion of the function in the Mellin-integral (9). First we derive the asymptotics of $\sum_{j>0} f(4^j y)$. Applying the formula (cf. [1])

$$\int_0^\infty x^{s-1} \left(\sum_{j=0}^\infty f(\lambda_j x)\mu_j\right) - \left(\sum_{j\geq 0} \mu_j \lambda_j^{-s}\right) \int_0^\infty x^{s-1} f(x) dx$$

with $\lambda_j = 4^j$ and $\mu_j = 1$ we derive, using the inverse Mellin transform,

$$\sum_{j\geq 0} f(4^j y) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\Gamma(s)\zeta\left(s, \frac{a}{c}\right)}{1-4^{-s}} y^{-s} ds \quad (c > 1).$$

Shifting the line of integration to the left and taking residues into account we get the expansion ($\chi_k = \frac{2\pi i k}{\log 4}$, $k \in \mathbb{Z}$)

$$\sum_{j\geq 0} f(4^j y) = \frac{4}{3} y^{-1} + \left(\frac{a}{c} - \frac{1}{2}\right) \frac{\log y}{\log 4} + \sum_{k\in\mathbb{Z}} \eta_k y^{-\chi_k} + \mathcal{O}(y)$$

with

$$\eta_0 = \frac{\zeta'\left(0,\frac{a}{c}\right)}{\log 4} + \frac{\gamma\left(\frac{a}{c}-\frac{1}{2}\right)}{\log 4} + \frac{1}{2}\left(\frac{1}{2}-\frac{a}{c}\right),$$

$$\eta_k = \frac{\Gamma(\chi_k)\zeta\left(\chi_k,\frac{a}{c}\right)}{\log 4} \quad (k \neq 0)$$

valid for $y \to 0+$. γ denotes the Euler–Mascherioni constant. Multiplying this with the Taylor expansion of $\exp\left(-\frac{b}{c}y\right)$ we arrive at

$$\exp\left(-\frac{b}{c}y\right)\sum_{j\geq 0} f(4^j y) = \frac{4}{3}y^{-1} - \left(\frac{1}{2}-\frac{a}{c}\right)\frac{\log y}{\log 4} + \sum_{k\in\mathbb{Z}} \eta_k y^{-\chi_k} - \frac{4b}{3c} + \mathcal{O}(y) \tag{10}$$

for $y \to 0+$. Now, write

$$\begin{aligned} c^s\Gamma(s)Z_0(s) &= \int_0^\infty f(y)y^{s-1}dy \\ &= \int_0^1 f(y)y^{s-1}dy + \int_1^\infty f(y)yx^{s-1}dy \\ &= I_1(s) + I_2(s). \end{aligned}$$

It is not hard to see that the integral $I_2(s)$ converges uniformly for all $s \in \mathbb{C}$ and thus it represents an analytic function in $\mathbb{C}$. So we are left with the integral $I_1(s)$. As in [4] we use the identities ($\Re s > 0$)

$$\int_0^1 t^{s-1}\log t dt = -\frac{1}{s^2} \quad \text{and} \quad \int_0^1 t^{s-1}dt = \frac{1}{s} \tag{11}$$

to derive the expansion

$$I_1(s) = \frac{\frac{4}{3}}{s-1} + \frac{\left(\frac{1}{2}-\frac{a}{c}\right)\frac{1}{\log 4}}{s^2} + \sum_{j\in\mathbb{Z}}\frac{\eta_j}{s+\chi_j} - \frac{\frac{4b}{9c}}{s} + \tilde{J}_{-1}(s)$$

from (10). $\tilde{J}_{-1}(s)$ denotes a function that is analytic in the half-plane $\Re s > -1$. Since $I_2(s)$ is analytic in the whole complex plane we conclude that

$$c^s\Gamma(s)Z_0(s) = \frac{\frac{4}{3}}{s-1} + \frac{\left(\frac{1}{2}-\frac{a}{c}\right)\frac{1}{\log 4}}{s^2} + \sum_{j\in\mathbb{Z}}\frac{\eta_j}{s+\chi_j} - \frac{\frac{4b}{9c}}{s} + J_{-1}(s).$$

Again, $J_{-1}(s)$ is analytic in $\Re s > -1$. Finally, we have to multiply with $\frac{1}{c^s\Gamma(s)}$. Let

$$\Psi(x) := \frac{\Gamma'(x)}{\Gamma(x)}$$

be the logarithmic derivative of the Gamma function. With help of the Laurent expansions

$$\begin{aligned} \frac{1}{c^s\Gamma(s)} &= s + (\gamma - \log c)s^2 + \left(-\frac{1}{2}(\log c)^2 - \frac{\pi^2}{12} + \frac{\gamma^2}{2} + (\log c - \gamma)\log c\right)s^3 + \mathcal{O}\left(s^4\right) \\ &= \frac{1}{c} + \mathcal{O}(s-1) = \frac{1}{\Gamma(\chi_k)c^{\chi_k}} - \frac{\Psi(\chi_k)+\log c}{\Gamma(\chi_k)c^{\chi_k}}(s-\chi_k) + \mathcal{O}\left((s-\chi_k)^2\right) \end{aligned} \tag{12}$$

we arrive at the analytic behaviour of $Z_0(s)$ in $\Re s > -1$. We formulate this result as a lemma:

LEMMA 5.1. *Let $a \in \mathbb{R}^+$, $b \in \mathbb{R}$, $c \in \mathbb{N}$, such that $0 < a+b < c$ and $a4^j+b \in \mathbb{N}_0$ for all $j \in \mathbb{N}_0$. Then the Dirichlet series*

$$Z_0(s) = \sum_{j\geq 0} \sum_{n\equiv a4^j+b \pmod{c4^j}} \frac{1}{n^s}$$

has a meromorphic continuation to the half-plane $\Re s > -1$, with simple poles at $s = 1$ and $s = \chi_k$ with $\chi_k = \frac{2\pi ik}{\log 4}$ $(k \in \mathbb{Z})$. Furthermore, we have the expansions

$$\begin{aligned} Z_0(s) &= \frac{\frac{4}{3c}}{s-1} + \mathcal{O}(1), \\ Z_0(s) &= \frac{\left(\frac{1}{2} - \frac{a}{c}\right)\frac{1}{\log 4}}{s} + \theta_0 + \mathcal{O}(s), \\ Z_0(s) &= \frac{\theta_k}{s+\chi_k} + \mathcal{O}(1), \end{aligned}$$

where

$$\begin{aligned} \theta_0 &:= \eta_0 - \frac{4b}{3c} + \left(\frac{1}{2} - \frac{a}{c}\right)\frac{1}{\log 4}, \\ \theta_k &:= \frac{\eta_k}{\Gamma(\chi_k)c^{\chi_k}} \quad (k \neq 0). \end{aligned}$$

Now we proceed with establishing the meromorphic continuation of $Z_1(s)$. As above, one can see, using the integral representation (8) that

$$Z_1(s) = \frac{1}{c^s\Gamma(s)} \int_0^\infty y^{s-1} \exp\left(-\frac{b}{c}y\right) \sum_{j\geq 0} jf(4^j y),$$

with $f(x)$ as before. Again we compute an asymptotic expansion for the function in the Mellin-integral. Via the inverse Mellin-integral

$$\sum_{j\geq 0} jf(4^j y) = \int_{c-i\infty}^{c+i\infty} \frac{\Gamma(s)\zeta\left(s, \frac{a}{c}\right)}{(2^s - 2^{-s})^2} y^{-s} ds$$

we derive, shifting to the left the line of integration and taking residues into account,

$$\sum_{j\geq 0} jf(4^j y) = \frac{4}{9}y^{-1} + \frac{1}{2}\left(\frac{1}{2} - \frac{a}{c}\right)\frac{(\log y)^2}{(\log 4)^2} + \sum_{k\in Z} \eta_k^{(1)} y^{-\chi_k} \log y + \sum_{k\in Z} \eta_k^{(0)} y^{-\chi_k} + \mathcal{O}(y)$$

for $y \to 0+$. Here

$$\begin{aligned} \eta_0^{(1)} &:= -\frac{\zeta'\left(0, \frac{a}{c}\right)}{(\log 4)^2} + \frac{\gamma\left(\frac{1}{2} - \frac{a}{c}\right)}{(\log 4)^2}, \\ \eta_k^{(1)} &:= -\frac{\zeta\left(\chi_k, \frac{a}{c}\right)\Gamma(\chi_k)}{(\log 4)^2} \quad (k \neq 0) \end{aligned}$$

and

$$\eta_0^{(0)} := \frac{\zeta''\left(0,\frac{a}{c}\right)}{2(\log 4)^2} - \frac{\gamma\zeta'\left(0,\frac{a}{c}\right)}{(\log 4)^2} + \left(\frac{\frac{1}{12}\pi^2+\frac{1}{2}\gamma^2}{(\log 4)^2} - \frac{1}{12}\right)\left(\frac{1}{2}-\frac{a}{c}\right),$$
$$\eta_k^{(0)} := \frac{\zeta\left(\chi_k,\frac{a}{c}\right)\Psi(\chi_k)\Gamma(\chi_k) + \zeta'\left(\chi_k,\frac{a}{c}\right)\Gamma(\chi_k)}{(\log 4)^2} \quad (k\neq 0).$$

Multiplication with the Taylor expansion of $\exp\left(-\frac{b}{c}y\right)$ yields

$$\exp\left(-\frac{b}{c}y\right)\sum_{j\geq 0} jf(4^j y)$$
$$= \frac{4}{9}y^{\ 1} + \frac{1}{2}\left(\frac{1}{2}-\frac{a}{c}\right)\frac{(\log y)^2}{(\log 4)^2} + \sum_{k\in\mathbb{Z}}\eta_k^{(1)}y^{-\chi_k}\log y + \sum_{k\in\mathbb{Z}}\eta_k^{(0)}y^{-\chi_k} - \frac{4b}{9c} + \mathcal{O}(y).$$

Now we can split the Mellin-integral as in the case of $Z_0(s)$. Again it is easy to see that the integral from 1 to ∞ forms an entire function. Using the identities in (11) and

$$\int_0^1 t^{s-1}(\log t)^2 dt = \frac{2}{s^3},$$

we arrive at the representation

$$c^s\Gamma(s)Z_1(s) = \frac{\frac{4}{9}}{s-1} + \frac{\left(\frac{1}{2}-\frac{a}{c}\right)\frac{1}{(\log 4)^2}}{s^3} + \sum_{k\in\mathbb{Z}}\frac{\eta_k^{(1)}}{(s+\chi_k)^2} + \sum_{k\in\mathbb{Z}}\frac{\eta_k^{(0)}}{s+\chi_k} - \frac{\frac{4b}{9c}}{s} + J_{-1}(s).$$

$J_{-1}(s)$ denotes a function, which is analytic in the half-plane $\Re s > -1$. As before, we have to multiply with $\frac{1}{c^s\Gamma(s)}$. Using the Laurent expansions (12) of this function around 1 and χ_k we arrive at

LEMMA 5.2. *Let $a\in\mathbb{R}^+, b\in\mathbb{R}, c\in\mathbb{N}$, such that $0<a+b<c$ and $a4^j+b\in\mathbb{N}_0$ for all $j\in\mathbb{N}_0$. Then the Dirichlet series*

$$Z_1(s) = \sum_{j\geq 0}\sum_{n\equiv a4^j+b(\bmod c4^j)}\frac{j}{n^s}$$

has a meromorphic continuation to the half-plane $\Re s > -1$, with a simple pole at $s=1$ and double poles at $s=\chi_k$ with $\chi_k = \frac{2\pi i k}{\log 4}$ $(k\in\mathbb{Z})$. Furthermore, we have the expansions

$$Z_1(s) - \frac{4}{9c}\frac{1}{s-1} + \mathcal{O}(1),$$
$$Z_1(s) = \frac{\frac{1}{2}-\frac{a}{c}}{(\log 4)^2}\frac{1}{s^2} + \frac{\theta_0^{(1)}}{s} + \theta_0^{(0)} + \mathcal{O}(s),$$
$$Z_1(s) := \frac{\theta_k^{(1)}}{(s-\chi_k)^2} + \frac{\theta_k^{(0)}}{s-\chi_k} + \mathcal{O}(1) \quad (k\neq 0),$$

where

$$\theta_0^{(1)} := \frac{\frac{1}{2}-\frac{a}{c}}{(\log 4)^2}(\gamma - \log c) + \eta_0^{(1)},$$

$$\theta_0^{(0)} := \frac{\frac{1}{2}-\frac{a}{c}}{(\log 4)^2}\left(\frac{1}{2}(\log c)^2 - \frac{\pi^2}{12} + \frac{\gamma^2}{2} - \gamma \log c\right) + \eta_0^{(1)}(\gamma - \log c) + \left(\eta_0^{(0)} - \frac{4b}{9c}\right),$$

$$\theta_k^{(1)} := \frac{\eta_k^{(1)}}{\Gamma(\chi_k)c^{\chi_k}} \quad (k \neq 0),$$

$$\theta_k^{(0)} := \frac{\eta_k^{(0)} - (\Psi(\chi_k) + \log c)\varphi_k^{(1)}}{\Gamma(\chi_k)c^{\chi_k}} \quad (k \neq 0),$$

R emark 5.1. It is possible to establish a meromorphic continuation of $Z_0(s)$ and $Z_1(s)$ in the whole complex plane by our methods. In the lemmas we only collected those results that we will need in the proof of Theorem 2.2. Since the result on the meromorphic continuation is of interest in its own right, we formulate it as an additional theorem.

THEOREM 5.1. *Let $a \in \mathbb{R}^+, b \in \mathbb{R}, c, d \in \mathbb{N}$, such that $d \geq 2$, $0 < a + b < c$ and $a4^j + b \in \mathbb{N}_0$ for all $j \in \mathbb{N}_0$. Then the Dirichlet series*

$$Z_q(s) = \sum_{j \geq 0} j^q (cd^j)^{-s} \zeta\left(s, \frac{a}{c} + \frac{b}{cd^j}\right)$$

($q \in \mathbb{N}_0$) has a meromorphic continuation to the whole complex plane with a simple pole at 1 and poles of order $1+q$ at $\frac{2\pi i k}{\log d} - n$ ($n \in \mathbb{N}_0, k \in \mathbb{Z}$). The residues at the poles are explicitely computable.

Since we want to apply the Mellin–Perron formula, it is important, how fast the functions $Z_q(s)$ ($q \in \{0,1\}$) increase for $|t| \to \infty$ ($s = \sigma + it$). For each σ let $\mu_q(\sigma)$ be the lower bound of numbers ξ, such that

$$Z_q(\sigma + it) = \mathcal{O}\left(|t|^{\xi}\right).$$

For $\sigma > 0$, $\mu_q(\sigma)$ is determined by the order of magnitude of the Hurwitz zeta function. Since

$$\zeta(s, \alpha) = \mathcal{O}\left(|t|^{\frac{1}{2}}\right) \quad \text{for } \sigma > 0,$$

we conclude that $\mu_q(\sigma) \leq \frac{1}{2}$ for $\sigma > 0$. It follows from the general theory of Dirichlet series (cf. Titchmarsh [12, 5.65 and 9.41]), that $\mu_q(\sigma)$ is a continuous function. Hence, there is an $\varepsilon > 0$, such that

$$\mu_q(\sigma) < 1 \quad \text{for } \sigma \geq -\varepsilon. \tag{13}$$

6. Proof of Theorem 2.2

As a first step, we prove two lemmas that deal with the sums over the congruences of the more complicated type in Table 2.

LEMMA 6.1. *Let $a \in \mathbb{R}^+, b \in \mathbb{R}, c \in \mathbb{N}$, such that $0 < a+b < c$ and $a4^j+b \in \mathbb{N}_0$ for all $j \in \mathbb{N}_0$. Then we have the asymptotic formula ($\chi_k = \frac{2\pi i k}{\log 4}$, $k \in \mathbb{Z}$)*

$$\begin{aligned} U_{a,b,c}(N) &:= \sum_{j\geq 0} \sum_{\substack{n\equiv a4^j+b \pmod{c4^j} \\ n<N}} (N-n) \\ &= \frac{2}{3c}N^2 + \left(\frac{1}{2} - \frac{a}{c}\right) N \log_4 N \\ &\quad + \sum_{k\in\mathbb{Z}} \varphi_{k;a,b,c} N^{-\chi_k} N + \mathcal{O}\left(N^{1-\varepsilon}\right) \end{aligned}$$

for ε small enough and

$$\begin{aligned} \varphi_{0;a,b,c} &:= \theta_0 - \left(\frac{1}{2} - \frac{a}{c}\right)\frac{1}{\log 4}, \\ \varphi_{k;a,b,c} &:= \frac{\theta_k}{\chi_k(\chi_k \quad 1)} \quad (k \neq 0). \end{aligned}$$

PROOF. An application of the Mellin–Perron formula yields

$$\sum_{j\geq 0} \sum_{\substack{n\equiv a4^j+b \pmod{c4^j} \\ n<N}} (N-n) - \frac{N}{2\pi i}\int_{2-i\infty}^{2+i\infty} Z_0(s) N^s \frac{ds}{s(s+1)}.$$

By (13) it is possible to shift the line of integration to the left until we arrive at $-\varepsilon \pm i\infty$. Taking residues into account we get the terms stated in the lemma using the expansion

$$\frac{N^s}{s(s+1)} = \frac{1}{s} + (\log N - 1) + \mathcal{O}(s)$$

and the meromorphic continuation of $Z_0(s)$ in Lemma 5.1. The error term comes from the fact that

$$\int_{-\varepsilon-i\infty}^{-\varepsilon+i\infty} Z_0(s) N^s \frac{ds}{s(s+1)} = \mathcal{O}\left(N^{-\varepsilon}\right).$$

LEMMA 6.2. *Let $a \in \mathbb{R}^+, b \in \mathbb{R}, c \in \mathbb{N}$, such that $0 < a+b < c$ and $a4^j+b \in \mathbb{N}_0$ for all $j \in \mathbb{N}_0$. Then we have the asymptotic formula ($\chi_k = \frac{2\pi i k}{\log 4}$, $k \in \mathbb{Z}$)*

$$\begin{aligned} V_{a,b,c}(N) := \sum_{j\geq 0} j \sum_{\substack{n\equiv a4^j+b \pmod{c4^j} \\ n<N}} (N-n) &= \frac{2}{9c}N^2 + \frac{\frac{1}{2}-\frac{a}{c}}{2} N(\log_4 N)^2 \\ &\quad + \sum_{k\in\mathbb{Z}} \varphi^{(1)}_{k;a,b,c} N^{-\chi_k} N \log_4 N \\ &\quad + \sum_{k\in\mathbb{Z}} \varphi^{(0)}_{k;a,b,c} N^{-\chi_k} N + \mathcal{O}\left(N^{1-\varepsilon}\right) \end{aligned}$$

for ε small enough and

$$\varphi^{(1)}_{0;a,b,c} := \theta^{(1)}_0 \log 4 - \frac{\frac{1}{2}-\frac{a}{c}}{\log 4},$$

$$\varphi^{(1)}_{k;a,b,c} := \frac{\theta^{(1)}_k}{\chi_k(\chi_k+1)} \quad (k \neq 0),$$
$$\varphi^{(0)}_{0;a,b,c} := \frac{\frac{1}{2}-\frac{a}{c}}{(\log 4)^2} - \theta^{(1)}_0 + \theta^{(0)}_0,$$
$$\varphi^{(0)}_{k;a,b,c} := -\frac{\theta^{(0)}_k - \theta^{(1)}_k(2\chi_k+1)}{\chi_k(\chi_k+1)} \quad (k \neq 0).$$

PROOF. The proof runs along the same lines as the poof of the previous lemma. We start with the representation

$$\sum_{j\geq 0} j \sum_{\substack{n\equiv a4^j+b \pmod{c4^j} \\ n<N}} (N-n) = \frac{N}{2\pi i}\int_{2-i\infty}^{2+i\infty} Z_1(s)N^s \frac{ds}{s(s+1)}.$$

Then we apply Lemma 5.2 and the representations

$$\frac{N^s}{s(s+1)} = \frac{1}{s} + (\log N - 1) + \left(\frac{1}{2}(\log N)^2 - \log N + 1\right)s + \mathcal{O}\left(s^2\right)$$
$$= \frac{N^{\chi_k}}{\chi_k(\chi_k+1)} + \frac{N^{\chi_k}}{\chi_k(\chi_k+1)}\left(\log N - \frac{1}{\chi_k} - \frac{1}{\chi_k+1}\right)(s-\chi_k) + \mathcal{O}\left((s-\chi_k)^2\right).$$

Shifting the line of integration is again justified by (13).

Now we are in a position to prove Theorem 2.2. The asymptotic formula for the summatory function of $w_2(n)$ follows immediately from the representation

$$\sum_{n<N} w_2(n) = S_{1,4}(N) - S_{0,4}(N) + U_{\frac{8}{3},-\frac{2}{3},16}(N) - U_{\frac{40}{3},-\frac{1}{2},16}(N),$$

which can easily be obtained from Table 2. The coefficients of N^2 cancel out, hence the main term is of order $N\log_2 N$ as stated in the theorem.

The proof of the expansion of $\nu_2(n)$ is more complicated. From Table 2 we get the representation

$$\begin{aligned}\sum_{n<N}\nu_2(n) = {} & S_{1,4}(N) + S_{0,4}(N) - 2V_{\frac{8}{3},-\frac{2}{3},16}(N) - U_{\frac{8}{3},-\frac{2}{3},16}(N) \\ & - 2V_{\frac{80}{3},-\frac{2}{3},32}(N) - 2U_{\frac{80}{3},-\frac{2}{3},32}(N) - 2V_{\frac{4}{3},-\frac{1}{2},8}(N) \\ & - 2V_{\frac{40}{3},-\frac{1}{3},16}(N) - U_{\frac{40}{3},-\frac{1}{3},16}(N).\end{aligned} \tag{14}$$

It is easy to see that the coefficients of N^2 and $N(\log_4 N)^2$ cancel out. What remains, is to prove that the same holds for the coefficients of $N^{1+\chi_k}\log_4 N$ $(k\in\mathbb{Z})$. We start with the case $k=0$. Define the functions

$$u_1(\alpha) := \frac{1}{2}-\alpha, \qquad v_1(\alpha) := -\frac{\frac{1}{2}-\alpha}{\log 4},$$
$$v_2(\alpha,\beta) := \frac{\frac{1}{2}-\alpha}{\log 4}(\gamma - \log\beta) - \frac{\zeta'(0,\alpha)}{\log 4}, \quad v_3(\alpha) := \frac{\gamma\left(\frac{1}{2}-\alpha\right)}{\log 4}.$$

Then, by Lemma 6.1 the coefficient of $N \log_4 N$ in the expansion of $U_{a,b,c}(N)$ is given by $u_1\left(\frac{a}{c}\right)$. By Lemma 6.2 the contribution of $N \log_4 N$ in $V_{a,b,c}$ is given by $v_1\left(\frac{a}{c}\right) + v_2\left(\frac{a}{c}, c\right) + v_3\left(\frac{a}{c}, c\right)$. Inserting this in (14), we conclude that the coefficient of $N \log_4 N$ in the expansion of the summatory function of $\nu_2(n)$ is given by

$$-4\left(v_1\left(\frac{1}{6}\right) + v_1\left(\frac{5}{6}\right) + v_3\left(\frac{1}{6}\right) + v_3\left(\frac{5}{6}\right)\right)$$
$$-2\left(v_2\left(\frac{1}{6}, 16\right) + v_2\left(\frac{1}{6}, 8\right) + v_2\left(\frac{5}{6}, 32\right) + v_2\left(\frac{5}{6}, 16\right)\right)$$
$$-\left(3u_1\left(\frac{5}{6}\right) + u_1\left(\frac{1}{6}\right)\right) =: -s_1 - s_2 - s_3.$$

We have to show that $s_1 + s_2 + s_3 = 0$. It is easy to see that $s_1 = 0$ and $s_3 = -\frac{2}{3}$. In order to be able to deal with s_2, we need the following lemma:

LEMMA 6.3.

$$v_2\left(\frac{1}{6}, c\right) + v_2\left(\frac{5}{6}, 2c\right) = \frac{1}{6}.$$

PROOF. Since (cf. [2])

$$\zeta'(s, \alpha) - \log \Gamma(\alpha) - \frac{1}{2}\log 2\pi,$$

we have

$$v_2\left(\frac{1}{6}, c\right) = \frac{\frac{1}{2} - \frac{1}{6}}{\log 4}(\gamma - \log c) - \frac{\log \Gamma\left(\frac{1}{6}\right) - \frac{1}{2}\log 2\pi}{\log 4}.$$

Using the well-known identity $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$, simple calculations yield

$$v_2\left(\frac{1}{6}, c\right) = -\frac{\frac{1}{2} - \frac{5}{6}}{\log 4}(\gamma - \log 2c) + \frac{\log \Gamma\left(\frac{5}{6}\right) - \frac{1}{2}\log 2\pi}{\log 4} + \frac{1}{6}.$$

Since the right hand side is equal to $v_2\left(\frac{5}{6}, 2c\right) + \frac{1}{6}$, the result follows.

Lemma 6.3 yields $s_2 = \frac{2}{3}$, and we have proved that $s_1 + s_2 + s_3 = 0$.

It remains to show that the coefficients of $N^{1+\chi_k} \log_4 N$ $(k \neq 0)$ vanish. Define

$$w(\alpha, \beta) := -\frac{\zeta(\chi_k, \alpha)}{\beta^{\chi_k}(\log 4)^2(\chi_k + 1)\chi_k}.$$

By Lemma 6.2 and (14) the coefficient of $N^{1+\chi_k} \log_4 N$ is equal to

$$w\left(\frac{1}{6}, 8\right) + w\left(\frac{1}{6}, 16\right) + w\left(\frac{5}{6}, 16\right) + w\left(\frac{5}{6}, 32\right).$$

Since $w(\alpha, \beta) = -w(\alpha, 2\beta)$, this sum is zero.

The Fourier coefficients of the fluctuation in the summatory function of $\nu_2(n)$ can be computed easily by inserting the Fourier coefficients of Lemmas 6.1 and 6.2. With that the theorem is proved.

ACKNOWLEDGEMENT. The author wants to acknowledge the hospitality of Prof. A. Pethő and T. Herendi from the University of Debrecen. Some work for this paper was done during his stay at Debrecen in April 1998.

REFERENCES

[1] P. FLAJOLET, M. REGNIER and R. SEDGEWICK, Some uses of the Mellin integral transform in the analysis of algorithms, in: *Combinatorial algorithms on words*, 241–254, A. Apostolico and Z. Galil, **12**, ASI Series. Series F: Computer and Systems Sciences, Springer, Berlin, 1985.

[2] H. MÜLLER, Über Werte polynomialer Dirichlet-Reihen im Nullpunkt, *Arch. Math.* **66** (1996), 30–34.

[3] D. E. KNUTH, *The Art of Computer Programming, Vol 2: Seminumerical Algorithms*, Addison Wesley, London, 1981.

[4] H. MÜLLER, Über die Meromorphe Fortsetzung einer Klasse verallgemeinerter Zeta-funktionen, *Arch. Math.* **58** (1992), 265–275.

[5] F. MORAIN and J. OLIVOS, Speeding up the Computations on an Elliptic Curve Using Addition-Subtraction Chains, *Inform Theory Appl.* **24** (1990), 531–543.

[6] H. MÜLLER, On Generalized Zeta-Functions at Negative Integers, *Illinois J. Math.* **32** (1988), 222–229.

[7] H. DELANGE, Sur la fonction sommatoire de la fonction "Somme des Chiffres", *Enseign. Math.* **21** (1975), 31–47.

[8] R. RIVEST, A. SHAMIR and L. M. ADLEMAN, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM* **21** (1978), 120–126.

[9] P. FLAJOLET, P. J. GRABNER, P. KIRSCHENHOFER, H. PRODINGER and R. F. TICHY, Mellin Transform and Asymptotics: Digital Sums, *Theoret. Comput. Sci.* **123** (1994), 291–314.

[10] W. DIFFIE and M. E. HELLMAN, New Directions in Cryptography, *IEEE Trans. Inform. Theory* **22** 1976, 644–654.

[11] D. M. GORDON, A Survey of Fast Exponentiation Methods, *J. Algorithms* **27** (1998), 129–146.

[12] E. C. TITCHMARSH, *The Theory of Functions*, 2nd. ed., Oxford University Press, London, 1975.

[13] P. J. GRABNER and J. M. THUSWALDNER, Analytic Continouation of a Class of Dirichlet Series, *Abh. d. Math. Sem. Univ. Hamburg* **66** (1996), 241–247.

[14] E. T. WHITTAKER and G. N. WATSON, *A Course in Modern Analysis*, Cambridge University Press, Cambridge, 1927.

[15] P. ERDŐS, Remarks on Number Theory. III: Addition Chains, *Acta Arith.* **6** (1960), 77–81.

[16] J. L. MAUCLAIRE and L. MURATA, On q-additive functions. I, *Proc. Jap. Acad., Ser. A* **59** (1983), 274–276.

[17] J. L. MAUCLAIRE and L. MURATA, On q-additive functions. II, *Proc. Jap. Acad., Ser. A* **59** (1983), 441–444.

(Received: September 7, 1998)

JÖRG M. THUSWALDNER
INSTITUT FÜR MATHEMATIK UND ANGEWANDTE GEOMETRIE
ABTEILUNG FÜR MATHEMATIK UND STATISTIK
MONTANUNIVERSITÄT LEOBEN
FRANZ-JOSEF-STRASSE 18
A-8700 LEOBEN
AUSTRIA