Some Problems in Elementary Number Theory and Modular Forms

Giuseppe Melfi

February 26, 1998

Table of Contents

Introduction **5**
Notation 7

1 Practical numbers **11**
1.1 Introduction 11
1.2 An arithmetical result 13
1.3 The structure theorem of Stewart 15
1.4 The Goldbach problem for practical numbers 18
1.5 Gaps between practical numbers 22
1.6 Binary recurrence sequences 26
1.7 Experimental results and tables 31

2 Triplets and k-tuples of twin practical numbers **33**
2.1 Triplets of twin practical numbers 34
2.2 4-tuples and 5-tuples: a conjecture 36
2.3 Attacking the conjecture 37
2.4 Reducing the conjecture to a reasonable statement 43

3 A problem on sum-free sequences **51**
3.1 A sum-free sequence with polynomial growth . 53
3.2 An elementary solution 56
3.3 A further solution 58
3.4 Some related questions 60

4 Modular forms and functions **63**
4.1 Modular forms and functions 63
4.2 Behaviour at the cusps 66
4.3 Congruence subgroups 68

5 Arithmetical applications **73**

5.1 Introduction . . . 73

5.2 Notation and definitions . . . 74

5.3 Main results . . . 75

5.4 Concluding remarks . . . 85

Bibliography **89**

Index **93**

Introduction

The general structure of this work reflects the main problems that I studied as a PhD student at the University of Pisa (1993–1997). There are five chapters, which deal with three different topics: Practical numbers (Chapters 1 and 2); Sum-free sequences (Chapter 3); Arithmetical identities related to the theory of modular forms (Chapters 4 and 5).

In Chapter 1 we extensively survey the theory of practical numbers, i.e., those positive integers m such that every positive integer $n < m$ can be represented as a sum of distinct positive divisors of m. This theory has recently received attention for some unexpected similarities with the properties of primes. We deal with both arithmetical and analytical aspects of the theory. Among other things, we prove the analogue of Goldbach's conjecture for practical numbers, showing that every even positive integer can be expressed as a sum of two practical numbers. This result gives a positive answer to a conjecture raised in 1984 [30]. Further we give an improvement of the upper bound for the gap between consecutive practical numbers: denoting by $\{s_n\}_{n\in\mathbb{N}}$ the sequence of practical numbers we prove that

$$s_{n+1} - s_n \ll \frac{s_n^{1/2}}{(\log\log s_n)^{1/2}}.$$

The problem of the asymptotic behaviour of practical numbers has been recently the object of deep studies by Tenenbaum [50], [51], and Saias [41]: denoting by $P(x)$ the counting function of practical numbers, for suitable positive constants c_1 and c_2 one has:

$$c_1 \frac{x}{\log x} < P(x) < c_2 \frac{x}{\log x}.$$

We solve another problem raised in [30], by proving that there exist infinitely many triplets of practical numbers of the form $(m-2, m, m+2)$. We conjecture that there exist infinitely many 5-tuples of practical numbers of the form $(m-6, m-2, m, m+2, m+6)$. In Chapter 2 we discuss this conjecture, and reduce it to a very reasonable, although unproved, Diophantine property of a certain pair of integer sequences.

In Chapter 3 we survey some questions about sum-free sequences, i.e., those increasing sequences of positive integers such that no term of the sequence is a sum of smaller terms. Erdős asked [14] how dense a sum-free sequence can be. He also asked for sum-free sequences $\{n_k\}_{k\in\mathbb{N}}$ "without gaps", i.e., such that $n_{k+1}/n_k \to 1$. We explicitly provide such a sequence. Further we prove that there exists a sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ which simultaneously is without gaps, and gives an improvement on the best previously known estimate of density, i.e. we get $n_k \ll k^{3+\varepsilon}$.

Chapter 4 is devoted to the theory of modular forms. It contains basic tools of the theory as well as some non-standard constructions of modular forms and functions. Further we give some examples of congruence subgroups and their generators. This chapter contains several details that, although largely implicit in the literature, we have been unable to quote by precise references.

In order to prove certain arithmetical identities involving sum-of-divisors functions, in Chapter 5 we use the basic tools developed in Chapter 4. It is interesting to remark that in a special case our method yields a well-known formula of Ramanujan. However our other identities, except for the above mentioned Ramanujan's formula, are new: for example, for every $n \equiv 2 \bmod 3$ we prove the formula

$$\sum_{\substack{k=1\\ k\equiv 1 \bmod 3}}^{n} \sigma_1(k)\sigma_1(n-k) = \frac{1}{9}\sigma_3(n),$$

where $\sigma_r(n)$ is the sum of the r-th powers of the positive divisors of n.

September 1997 GIUSEPPE MELFI

Acknowledgements

I am grateful to Carlo Viola for his constant encouragement during the last four years.

I am pleased to thank Jean-Marc Deshouillers for many helpful suggestions and answers to questions about sum-free sequences. I tackled this problem after I received two letters by Paul Erdős and conversed with him in summer 1996 at Eger (Hungary), a few weeks before his unexpected death.

I am also indebted to Don Zagier and Umberto Zannier for their helpful comments and suggestions concerning Chapters 4 and 5.

Finally, I wish to thank Maurice Margenstern for kindly suggesting several changes and improvements in the exposition of this thesis.

Notation

$\sigma(n)$	$= \sum_{d\mid n} d$
$\sigma_k(n)$	$= \sum_{d\mid n} d^k$
$P(x)$	the number of practical numbers $\leq x$
F_n	n-th Fibonacci number
L_n	n-th Lucas number
Q_i	i-th prefix of a positive integer
T_i	i-th termination of a positive integer
$\phi_d(x)$	cyclotomic polynomial for $e^{2\pi i/d}$
$\pi_2(x)$	$= \sum_{\substack{p\leq x \\ p,p+2 \text{ primes}}} 1$
$P_2(x)$	$= \sum_{\substack{m\leq x \\ m,m+2 \text{ practical}}} 1$
$u_n(P,Q)$	fundamental Lucas sequence
$v_n(P,Q)$	companion Lucas sequence
$\Phi_d(x,y)$	homogeneous cyclotomic polynomial for $e^{2\pi i/d}$
$\nu(n)$	number of distinct prime factors of n
$\varphi(n)$	Euler totient function
p_k	k-th prime number
s_k	k-th practical number
$F(a,b;c,x)$	$= {}_2F_1(a,b;c,x)$; Gauss hypergeometric series
$(a)_k$	Pochhammer symbol
Γ	$SL(2,\mathbb{Z})$; full modular group
$\mathbb{H}$	upper half-plane of $\mathbb{C}$

$E_{2k}(\tau)$	Eisenstein series of weight $2k$
$\Delta(\tau)$	monic cusp form of weight 12 for Γ
$\eta(\tau)$	Dedekind eta-function
$[x]$	integer part of x
$\{x\}$	$x - [x]$

Chapter 1

Practical numbers

1.1 Introduction

In this chapter we deal with a recent topic in elementary number theory, namely the theory of practical numbers. As extensively stated in [31], some properties of practical numbers appear to be close to those of primes, although practical numbers are defined in a completely different manner. For example, it is remarkable that at first sight the list of practical numbers shows some irregularities of distribution which resemble those of primes, and that practical numbers appear to become less frequent as the list flows.

Definition 1 *A positive integer m is said to be practical if every n with $1 < n < m$ is a sum of distinct positive divisors of m.*

This definition is due to Srinivasan, who also pointed out the first properties of practical numbers in 1948 in his short note [48]. After him, several authors dealt with various aspects of the theory of practical numbers. Erdős [13] in 1950 announced that practical numbers have zero asymptotic density. Stewart [49] proved the following structure theorem (see also Theorem 1): an integer $m \geq 2$, $m = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, with primes $q_1 < q_2 < \cdots < q_k$ and integers $\alpha_i \geq 1$, is practical if and only if $q_1 = 2$ and, for $i = 2, 3, \ldots, k$,

$$q_i \leq \sigma(q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_{i-1}^{\alpha_{i-1}}) + 1$$

where $\sigma(n)$ denotes the sum of the positive divisors of n.

Let $P(x)$ be the counting function of practical numbers:

$$P(x) = \sum_{\substack{m \le x \\ m \text{ practical}}} 1 \,.$$

Hausman and Shapiro [23] showed in 1984 that

$$P(x) \ll \frac{x}{(\log x)^\beta}$$

for any $\beta < \frac{1}{2}(1 - 1/\log 2)^2 \simeq 0.0979$. Margenstern ([30], [31]) proved that

$$P(x) \gg \frac{x}{\exp\left\{\frac{1}{2\log 2}(\operatorname{loglog} x)^2 + 3 \operatorname{loglog} x\right\}}.$$

Tenenbaum ([50], [51]) improved the above upper and lower bounds as follows:

$$\frac{x}{\log x}(\operatorname{loglog} x)^{-5/3-\varepsilon} \ll_\varepsilon P(x) \ll \frac{x}{\log x} \operatorname{loglog} x \operatorname{logloglog} x.$$

Very recently Saias [41] improved the above estimates by providing upper and lower bounds of Chebishev's type:

$$c_1 \frac{x}{\log x} < P(x) < c_2 \frac{x}{\log x}$$

for suitable positive constants c_1 and c_2. This is in accordance with the conjectured asymptotic behaviour:

Conjecture 1 (Margenstern) *There exists a constant λ such that:*

$$P(x) \sim \lambda \frac{x}{\log x}.$$

Margenstern's computations suggest $\lambda \simeq 1.341$.

The author [33] recently proved two Goldbach-type conjectures for practical numbers first stated in [30]:

1. Every even positive integer is a sum of two practical numbers;

2. There exist infinitely many practical numbers m such that $m-2$ and $m+2$ are also practical.

The purpose of this chapter is to survey some of the above results and to give some new contributions to the theory of practical numbers. Many parts of this chapter appeared in two papers of the author [33] and [34].

Sierpiński [45] and Stewart [49] independently remarked that a positive integer m is practical if and only if every integer n with $1 \leq n \leq \sigma(m)$ is a sum of distinct positive divisors of m. Here we give an alternative proof of this equivalence.

We also give an improved version of [33, Lemma 2], which yields a slightly simpler proof of the Goldbach-type result (1.) mentioned above.

As a development of the result (2.) mentioned above, we shall discuss a new problem about the 5-tuples of practical numbers of the type $m-6$, $m-2$, m, $m+2$, $m+6$: we shall justify our conjecture which states that there exist infinitely many such 5-tuples.

We study the gap between consecutive practical numbers, improving upon a result of Hausman and Shapiro [23].

Finally we prove that some binary recurrence sequences, including the classical sequences of Fibonacci, Lucas and Pell, contain infinitely many practical numbers. We incidentally note that it is unknown whether the Fibonacci sequence $\{1, 1, 2, 3, 5, \dots\}$ and the Lucas sequence $\{1, 3, 4, 7, 11, \dots\}$ contain infinitely many prime numbers. Dubner and Keller [12] announced the primality of some "titanic" (i.e., having more than 1000 digits) Fibonacci and Lucas numbers, such as F_{9311}, F_{5387}, L_{14449}, L_{7741}, L_{5851}, L_{4793}, L_{4787}.

1.2 An arithmetical result

In this section we give an equivalent definition of practical number. We begin with the following lemma:

Lemma 1 *Let m be a positive integer, and let $d_1 = 1 < d_2 < \cdots < d_r = m$ be the positive divisors of m. Let d_h be the least divisor such that $d_h \geq \sqrt{m}$. Then $d_1 + d_2 + \cdots + d_{h-1} + 1 \leq m$.*

Proof. The lemma is true for $m = 1, 2, 3, 4$. Let $m > 4$; since $d_{h-1} < \sqrt{m}$ we have

$$\begin{aligned} d_1 + d_2 + \cdots + d_{h-1} + 1 &\leq 1 + 2 + 3 + \cdots + [\sqrt{m}\,] + 1 \\ &= \frac{[\sqrt{m}\,]([\sqrt{m}\,] + 1)}{2} + 1 \\ &\leq \frac{\sqrt{m}\,(\sqrt{m} + 1)}{2} + 1 \\ &< m\ . \end{aligned}$$

□

Lemma 2 (Margenstern) *Let m be a positive integer, and let $d_1, \ldots, d_h, \ldots, d_r$ be as in Lemma 1. Then m is such that every n with $1 \leq n \leq \sigma(m)$ is a sum of distinct positive divisors of m, if and only if $d_{j+1} \leq d_1 + \cdots + d_j + 1$ for every $j = 1, \ldots, h - 1$.*

Proof. For the proof see Margenstern's paper [31]. □

Proposition 1 *A positive integer m is practical if and only if every n with $1 \leq n \leq \sigma(m)$ is a sum of distinct positive divisors of m.*

Proof. Since $\sigma(m) \geq m$, if m is such that every n with $1 \leq n \leq \sigma(m)$ is a sum of distinct positive divisors of m, *a fortiori* m is a practical number.

Let m be practical, i.e., every n with $1 \leq n \leq m$ is a sum of distinct positive divisors of m. Let $d_1, \ldots, d_h, \ldots, d_r$ be as in the preceding lemmas. For any j satisfying $1 \leq j \leq h-1$ we have $d_1 + \cdots + d_j + 1 \leq m$ by Lemma 1. Hence $d_1 + \cdots + d_j + 1$ is a sum of distinct divisors of m, of which at least one must be $\geq d_{j+1}$. It follows that $d_{j+1} \leq d_1 + \cdots + d_j + 1$, whence, by Lemma 2, every n with $1 \leq n \leq \sigma(m)$ is a sum of distinct positive divisors of m. □

1.3 The structure theorem of Stewart

In this section we shall prove a structure theorem for practical numbers. As we shall see, it will be very useful for proving our further results on practical numbers. Notations and definitions in this section are due to Margenstern ([30], [31]), who extensively studied algebraic and arithmetical properties of practical numbers.

Definition 2 *Let a, b two positive integers. We say that a represents b if b can be expressed as a sum of distinct positive divisors of a.*

Hence m is practical if and only if m represents every positive integer $n \leq m$, or equivalently, by Proposition 1, if and only if m represents every positive integer $n \leq \sigma(m)$.

Definition 3 *Let a, b two positive integers. We say that b is within the range of a if $b = 1$ or if the least prime factor p of b is such that $p \leq \sigma(a) + 1$; if $p > \sigma(a) + 1$, then b is said to be outside the range of a.*

Definition 4 *Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$ be a positive integer, with primes $1 < q_1 < q_2 < \cdots < q_k$, and positive integers α_i. We define $Q_0, Q_1, Q_2, \dots, Q_k$ as follows:*

$$\begin{cases} Q_0 = 1 \\ Q_i = Q_{i-1} q_i^{\alpha_i} \quad \text{for } i = 1, 2, \dots, k. \end{cases}$$

Every Q_i is called a prefix of n. One has $1 = Q_0 < Q_1 < \cdots < Q_k = n$. Every integer $T_j = n/Q_j$ is called a termination of n.

For example if $n = 1008 = 2^4 3^2 7$ the prefixes of n are $1, 16, 144, 1008$ and the terminations $1008, 63, 7, 1$. In order to prove the structure theorem we begin with the following lemma.

Lemma 3 *If m is a practical number and p is a prime within the range of m with $(m, p) = 1$, then for every integer n, we have that mp^n is a practical number.*

Proof. We proceed by induction on n. For $n = 0$ the statement is trivial. We assume the lemma true for every integer $\leq n$ and prove that mp^{n+1} is practical.

Let a be a positive integer with $a \leq \sigma(mp^{n+1})$. We now prove that a is a sum of distinct positive divisors of mp^{n+1}. Suppose that $a \leq \sigma(m)p^{n+1}$. We have $a = a_1 p^{n+1} + r$ where $a_1 \leq \sigma(m)$ and $0 \leq r < p^{n+1}$. Since m is practical and $a_1 \leq \sigma(m)$, a_1 is a sum of distinct positive divisors of m, hence $a_1 p^{n+1}$ is a sum of distinct positive divisors of mp^{n+1}, all multiples of p^{n+1}. Since $r < p^{n+1}$, we have $r = \sum_{k=0}^{n} r_k p^k$ with $0 \leq r_k < p$. Since p is within the range of m, r_k is a sum of distinct positive divisors of m. Hence $r_k p^k$ is a sum of distinct positive divisors of mp^{n+1} which are multiples of p^k, but of no higher power of p. For any integer k, the divisors of $r_k p^k$ are distinct and different from the divisors of $a_1 p^{n+1}$, hence if $a \leq \sigma(m)p^{n+1}$, a can be expressed as a sum of distinct positive divisors of m.

Now suppose that $\sigma(m)p^{n+1} < a \leq \sigma(mp^{n+1})$. We have $a = \sigma(m)p^{n+1} + b$, and since $(m, p) = 1$ we also have $\sigma(mp^{n+1}) = \sigma(m)\sigma(p^{n+1})$. Since $\sigma(p^{n+1}) = p^{n+1} + \sigma(p^n)$, we have $1 \leq b \leq \sigma(mp^n)$. By induction, b is a sum of distinct positive divisors of mp^n which are at most multiples of p^n, and therefore different from the divisors of mp^{n+1} which are multiples of p^{n+1}. Hence m is practical. □

Theorem 1 (B. M. Stewart) *A positive integer m is practical if and only if each termination is in the range of the corresponding prefix. In other words, if $m = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ is a practical number and $m > 1$, then $q_1 = 2$ and*

$$q_i \leq \sigma(q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_{i-1}^{\alpha_{i-1}}) + 1$$

for $i = 2, 3, \ldots, k$.

Proof. Note that 1 is practical and that 2 is the only prime within the range of 1. Hence we assume that $m \geq 2$.

The condition is necessary: let $m = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$; let $1 = Q_0 < Q_1 < \cdots < Q_k$ be the prefixes of m. Suppose that a termination of m is outside the range of the corresponding prefix. There exists an index $r \leq k - 1$, $q_{r+1} > \sigma(Q_r) + 1$. Hence m does not represent $\sigma(Q_r) + 1$. Every sum containing a divisor divisible by q_h with $h \geq r+1$ is greater than $\sigma(Q_r)+1$; but the sum of the divisors with the prime factors $q_1, q_2, \ldots, q_r$ is less than $\sigma(Q_r)$.

The condition is sufficient: we proceed by finite induction. In fact 1 is practical. Since q_1 is within the range of 1, one has that Q_1 is practical by the preceding lemma. By induction, Q_r is practical ($r \leq k-1$) and since q_{r+1} is within the range of Q_r, by the preceding lemma Q_{r+1} is practical. Therefore Q_r with $r = 1, 2, \ldots, k$ is practical. In particular $m = Q_k$ is practical. □

As a simple application of the preceding theorem, we now find a remarkable property of practical numbers as values a of suitable polynomial of degree 2 (see Proposition 2 below).

It is unknown whether the polynomial $p(x) = x^2 + 1$ has infinitely many prime values [6]. The following proposition shows that $p(x)$ has only two practical values.

Proposition 2 *The polynomial $p(x) = x^2 + 1$ has practical values only for integers $x = -1, 0$ and 1.*

Proof. Since every practical number greater than 1 is even, if $p(x) > 1$ is practical for a suitable integer x, then x is odd. On the other hand $x^2 + 1 \equiv 2 \bmod 4$ for every odd integer x and $x^2+1 \not\equiv 0 \bmod 3$. Hence a factorization of $p(x)$ with $|x| > 1$ must be of the form

$$x^2 + 1 = 2 \cdot q_1^{\alpha_1} \cdots q_l^{\alpha_l}$$

with primes $q_1 < \cdots < q_l$, $q_1 \geq 5$, and positive integers α_i. Therefore by the preceding theorem $x^2 + 1$ is not practical. □

Remark. Notice that x^2+1 is irreducible in $\mathbb{Z}[x]$. As we shall see in the next chapter, there are many polynomials highly reducible in $\mathbb{Z}[x]$ (e.g. certain products of cyclotomic polynomials) that contain infinitely many practical numbers.

With the same argument of the above proposition one can prove that the polynomial $q(x) = x^2 - 2$ has practical values only for integers $x = -2$ and 2.

1.4 The Goldbach problem for practical numbers

In this section we prove that every even positive integer is a sum of two practical numbers.

Lemma 4 *If m is a practical number and n is an integer such that $1 \leq n \leq \sigma(m)+1$, then mn is a practical number. In particular, for $1 \leq n \leq 2m$, mn is practical.*

Proof. The first assertion easily follows from Stewart's structure theorem; see also [30, p. 6]. Since $m-1$ is a sum of distinct positive divisors of m, we have $m+(m-1) \leq \sigma(m)$, i.e., $2m \leq \sigma(m)+1$, and this proves the second assertion. □

Lemma 5 *If m and $m+2$ are two practical numbers, then every even integer $2n$ with $\frac{1}{2}m^2 \leq 2n \leq \frac{7}{2}m^2$ is a sum of two practical numbers.*

Proof. We split up the interval $\left[\frac{1}{2}m^2,\, \frac{7}{2}m^2\right]$ into the union of five subintervals:

(i) $\left[\frac{1}{2}m^2,\, m^2\right[$;
(ii) $[m^2, m^2+2m]$;
(iii) $]m^2+2m, 2m^2]$;
(iv) $]2m^2, 3m^2]$;
(v) $\left]3m^2,\, \frac{7}{2}m^2\right]$.

(i) If $m=2$, the only even number contained in the interval $\left[\frac{1}{2}m^2,\, m^2\right[$ is 2, which is a sum of two practical numbers $(2=1+1)$. Suppose $m>2$ and let $2n \in \left[\frac{1}{2}m^2,\, m^2\right[$. If $2n=\frac{1}{2}m^2$ or $2n=\frac{1}{2}m^2+m$, we use the decompositions

$$\frac{1}{2}m^2 = m\left(\frac{1}{2}m-1\right)+m,$$

$$\frac{1}{2}m^2+m = m\left(\frac{1}{2}m-1\right)+2m.$$

Otherwise we can represent $2n$ as $\frac{1}{2}m^2 + km + 2j$ with $0 \leq k < \frac{1}{2}m$, $1 \leq j \leq \frac{1}{2}m$, $(k, j) \neq \left(0, \frac{1}{2}m\right)$. Then

$$2n = \frac{1}{2}m^2 + km + 2j = m\left(\frac{1}{2}m + k - j\right) + (m+2)\,j.$$

By Lemma 4, $2n$ is a sum of two practical numbers.

(ii) We have

$$m^2 = \frac{m}{2}m + \frac{m}{2}m,$$

$$m^2 + 2m = m + (m+1)m,$$

and for $1 \leq k \leq m-1$

$$m^2 + 2m - 2k = km + (m-k)(m+2),$$

whence, by Lemma 4, every $2n$ satisfying $m^2 \leq 2n \leq m^2 + 2m$ is a sum of two practical numbers.

(iii) Every $2n$ satisfying $m^2 + 2m < 2n \leq 2m^2$ can be obviously represented as $2m^2 - 2mh - 2j$ for $0 \leq h \leq \frac{m}{2} - 2$ and $0 \leq j \leq m - 1$. Therefore

$$2n = 2m^2 - 2mh - 2j = (m - 2(h+1) + j)m + (m-j)(m+2),$$

whence, again by Lemma 4, $2n$ is a sum of two practical numbers.

(iv) Let now $2m^2 < 2n \leq 3m^2$. We can represent $2n$ as $2m^2 + 2mh + 2j$ for $0 \leq h \leq \frac{m}{2} - 1$ and $1 \leq j \leq m$. We have

$$2n = 2m^2 + 2mh + 2j = (m + 2(h-1) - j)m + (m+j)(m+2),$$

whence, by Lemma 4, $2n$ is a sum of two practical numbers, except for four exceptional cases which we deal with as follows:

$$2m^2 + 2m - 4 = (m+2)m + (m-2)(m+2)$$

$$2m^2 + 2m - 2 = (m+1)m + (m-1)(m+2)$$

$$2m^2 + 2m = m \cdot m + m(m+2)$$

$$2m^2 + 4m = m(m+2) + m(m+2).$$

(v) If $m = 2$, the only even number contained in the interval $\left]3m^2, \frac{7}{2}m^2\right]$ is 14, which is a sum of two practical numbers ($14 = 6 + 8$). Suppose $m > 2$ and let $2n \in \left]3m^2, \frac{7}{2}m^2\right]$. We can represent $2n$ as $\frac{7}{2}m^2 - km + 2j$ with $1 \le k \le \frac{1}{2}m$, $1 \le j \le \frac{1}{2}m$. Then

$$2n = \frac{7}{2}m^2 - km + 2j = m(2m - k - j - 3) + (m+2)\left(\frac{3}{2}m + j\right),$$

which is a sum of two practical numbers by Lemma 4. □

Theorem 2 *Every even positive integer is a sum of two practical numbers.*

Proof. Since $(2,4)$, $(4,6)$, $(6,8)$ are pairs of twin practical numbers, by Lemma 5 every $2n \le 126$ is a sum of two practical numbers. Suppose we have a sequence $\{m_n\}_{n\in\mathbb{N}}$ such that

(i) $m_1 = 16$

and for every n

(ii) m_n is practical

(iii) $m_n + 2$ is practical

(iv) $1 < m_{n+1}/m_n < \sqrt{7}$.

Since, by (iv), the intervals $\left[\frac{1}{2}m_n^2, \frac{7}{2}m_n^2\right]$ and $\left[\frac{1}{2}m_{n+1}^2, \frac{7}{2}m_{n+1}^2\right]$ overlap, every even positive integer $2n \ge 128$ is a sum of two practical numbers by Lemma 5. We shall construct a sequence $\{m_n\}_{n\in\mathbb{N}}$ satisfying (i), (ii), (iii) and a condition slightly stronger than (iv), i.e., $1 < m_{n+1}/m_n < 2$.

Let $S_0 = \{16, 30, 54, 88, 160\}$. For every $r \in S_0$, r and $r+2$ are practical numbers. Denote $S_0 = \{r_{0,1}, r_{0,2}, \ldots, r_{0,5}\}$ with $r_{0,1} < r_{0,2} < \cdots < r_{0,5}$. Note that $r_{0,i} < 2r_{0,i-1}$ $(i = 2,3,4,5)$ and $r_{0,5} = \frac{1}{2}r_{0,1}^2 + 2r_{0,1}$. Let $h_0 = 5$ and, for $k = 1, 2, \ldots$, define

$$\begin{aligned} S_k &= \left\{\tfrac{1}{2}r_{k-1,i}^2 + 2r_{k-1,i}\ ,\ r_{k-1,i}^2 + 3r_{k-1,i} \;\middle|\; i = 1, 2, \ldots, h_{k-1}\right\} \\ &= \{r_{k,1}, r_{k,2}, \ldots, r_{k,h_k}\} \end{aligned}$$

with $r_{k,1} < r_{k,2} < \cdots < r_{k,h_k}$. Further let $S = \bigcup_{k=0}^{\infty} S_k$. If we write $S = \{m_n\}_{n\in\mathbb{N}}$, with $m_n < m_{n+1}$ for every n, one can see that this sequence satisfies (i), (ii), (iii) and $m_{n+1} < 2m_n$. The proof of this is similar to the argument given in [33, Theorem 1].

We have already checked this for the set S_0. Since $r^2 + 3r = r(r+3)$, $r^2+3r+2 = (r+2)(r+1)$, $\frac{1}{2}r^2+2r = r(\frac{1}{2}r+2)$, $\frac{1}{2}r^2+2r+2 = (r+2)(\frac{1}{2}r+1)$, (ii) and (iii) hold for every set S_k by induction.

We now show, by induction on k, that $r_{k,i} < 2r_{k,i-1}$ for all $k \geq 0$ and $i = 2, 3, \ldots, h_k$. This is true for $k = 0$. Assuming that $r_{k,l} < 2r_{k,l-1}$ for some k and $l = 2, 3, \ldots, h_k$, we have, for any fixed $i \geq 2$, either $r_{k+1,i} = \frac{1}{2}r_{k,j}^2 + 2r_{k,j}$ or $r_{k+1,i} = r_{k,l}^2 + 3r_{k,l}$ for some $j \geq 2$ or $l \geq 1$ respectively. If $r_{k+1,i} = r_{k,j}^2 + 3r_{k,j}$, then

$$\frac{r_{k+1,i}}{r_{k+1,i-1}} \leq \frac{r_{k,l}^2 + 3r_{k,l}}{\frac{1}{2}r_{k,l}^2 + 2r_{k,l}} = 2 \cdot \frac{1 + \frac{3}{r_{k,l}}}{1 + \frac{4}{r_{k,l}}} < 2.$$

If $r_{k+1,i} = \frac{1}{2}r_{k,j}^2 + 2r_{k,j}$, then either

$$2 \cdot \left(\frac{1}{2}r_{k,j-1}^2 + 2r_{k,j-1}\right) > \frac{1}{2}r_{k,j}^2 + 2r_{k,j},$$

whence

$$\frac{r_{k+1,i}}{r_{k+1,i-1}} \leq \frac{\frac{1}{2}r_{k,j}^2 + 2r_{k,j}}{\frac{1}{2}r_{k,j-1}^2 + 2r_{k,j-1}} < 2,$$

or

$$2 \cdot \left(\frac{1}{2}r_{k,j-1}^2 + 2r_{k,j-1}\right) \leq \frac{1}{2}r_{k,j}^2 + 2r_{k,j},$$

whence

$$r_{k,j-1}^2 + 3r_{k,j-1} < 2 \cdot \left(\frac{1}{2}r_{k,j-1}^2 + 2r_{k,j-1}\right) \leq \frac{1}{2}r_{k,j}^2 + 2r_{k,j},$$

which implies that

$$\frac{r_{k+1,i}}{r_{k+1,i-1}} \leq \frac{\frac{1}{2}r_{k,j}^2 + 2r_{k,j}}{r_{k,j-1}^2 + 3r_{k,j-1}} < \frac{2r_{k,j-1}^2 + 4r_{k,j-1}}{r_{k,j-1}^2 + 3r_{k,j-1}} = 2 \cdot \frac{1 + \frac{2}{r_{k,j-1}}}{1 + \frac{3}{r_{k,j-1}}} < 2$$

by the inductive assumption. This proves that $m_{n+1} < 2m_n$, provided that $m_{n+1} = r_{k,i}$ for some $k \geq 0$ and $i \geq 2$. To complete the proof of the theorem, we must prove that $m_{n+1} < 2m_n$ when $m_{n+1} = r_{k,1} = \frac{1}{2}r_{k-1,1}^2 + 2r_{k-1,1}$ for some $k \geq 1$. In this case we show, by induction on k, that

$$r_{k,1} = \frac{1}{2}r_{k-1,1}^2 + 2r_{k-1,1} \in S_{k-1}.$$

This is true for $k = 1$ since $r_{1,1} = r_{0,1}^2 + 2r_{0,1} = r_{0,h_0} \in S_0$. Assuming that $r_{k,1} \in S_{k-1}$ for some k, we have, by definition of S_k,

$$r_{k+1,1} = \frac{1}{2}r_{k,1}^2 + 2r_{k,1} \in S_k.$$

This shows that $r_{k,1} = r_{k-1,j}$ for some $j \geq 2$. Hence, by the previous argument, $m_{n+1} = r_{k,1} = r_{k-1,j} < 2m_n$. □

1.5 Gaps between practical numbers

Here we give an estimate of the gap between consecutive practical numbers. The same problem for primes has been extensively studied. If $\{p_n\}_{n\in\mathbb{N}}$ is the sequence of primes, Baker and Harman [3] recently proved that

$$p_{n+1} - p_n \ll p_n^{0.535},$$

the exponent 0.535 being of course replaced by $\frac{1}{2} + \varepsilon$ under the Riemann Hypothesis. If $\{s_n\}_{n\in\mathbb{N}}$ is the sequence of practical numbers, Hausman and Shapiro [23] proved that

$$s_{n+1} - s_n \leq 2s_n^{1/2}.$$

We can improve this inequality as follows:

Theorem 3 *Let $\{s_n\}_{n\in\mathbb{N}}$ be the sequence of practical numbers and let $A > 4e^{-\gamma/2}$, where γ is the Euler-Mascheroni constant. For any sufficiently large n we have*

$$s_{n+1} - s_n < A\,\frac{s_n^{1/2}}{(\log\log s_n)^{1/2}}.$$

Proof. Let $\delta > 0$ and $c < e^\gamma$ be such that $4c^{-1/2}(1+\delta)(1-\delta)^{-1/2} < A$. Let $N_k = \prod_{p \le e^k} p^k$, where p denotes a prime. By [22, §22.9] we have

$$\lim_{k\to\infty} \frac{\sigma(N_k)}{N_k \operatorname{loglog} N_k} = e^\gamma. \tag{1.1}$$

For every k, let $m^{(k)}$ be any integer such that $N_{k-1}|m^{(k)}$, $m^{(k)}|N_k$. It is easy to see, by induction on k, that N_k is practical for all $k \ge 1$, and if $k \ge 3$ then $m^{(k)}$ is also practical. To prove this, note that $N_1 = 2$ and $N_2 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2$ are practical, and $m^{(k)}/N_{k-1}$ is a product of primes not exceeding e^k. Since $e^k \le 2N_{k-1}$ for $k \ge 3$, $m^{(k)}$ and hence N_k are practical by repeated application of Lemma 4.

Since $n|m$ easily implies $\sigma(n)/n \le \sigma(m)/m$, we get

$$\frac{\sigma(N_{k-1})}{N_{k-1} \operatorname{loglog} N_k} \le \frac{\sigma\left(m^{(k)}\right)}{m^{(k)} \operatorname{loglog} m^{(k)}} \le \frac{\sigma(N_k)}{N_k \operatorname{loglog} N_{k-1}}.$$

Clearly

$$\operatorname{loglog} N_{k-1} \sim \operatorname{loglog} N_k,$$

whence, by (1.1),

$$\lim_{k\to\infty} \frac{\sigma\left(m^{(k)}\right)}{m^{(k)} \operatorname{loglog} m^{(k)}} = e^\gamma.$$

Thus there exists an integer k_0 such that for any $k \ge k_0$

$$\min_{\substack{m \\ N_{k-1}|m \\ m|N_k}} \frac{\sigma(m)}{m \operatorname{loglog} m} > c. \tag{1.2}$$

Let s_n be a practical number such that $s_n > c\,N_{k_0}^2 \operatorname{loglog} N_{k_0}$ and let κ be the least positive integer such that

$$N_\kappa \ge \frac{s_n}{c\,N_\kappa \operatorname{loglog} N_\kappa}.$$

Further, let

$$m_1^{(\kappa)} = N_{\kappa-1} < m_2^{(\kappa)} < \cdots < m_\lambda^{(\kappa)} = N_\kappa$$

be all the integers satisfying $N_{\kappa-1}|m_i^{(\kappa)}$, $m_i^{(\kappa)}|N_\kappa$, and let ν be such that

$$m_\nu^{(\kappa)} < \frac{s_n}{c\,m_\nu^{(\kappa)} \operatorname{loglog} m_\nu^{(\kappa)}} \tag{1.3}$$

and

$$m_{\nu+1}{}^{(\kappa)} \geq \frac{s_n}{c\, m_{\nu+1}^{(\kappa)} \operatorname{loglog} m_{\nu+1}^{(\kappa)}}. \tag{1.4}$$

Let ϑ and τ be defined by $m_\nu^{(\kappa)} = \vartheta N_{\kappa-1}$, $N_\kappa = \tau m_\nu^{(\kappa)}$. Clearly $\tau > 1$. Let p'' be the least prime factor of τ, and let p' be the greatest prime $< p''$ (if $p'' = 2$, we let $p' = 1$). By Bertrand's postulate we have $p'' \leq 2p'$. Since $N_\kappa = \vartheta\tau N_{\kappa-1}$, we have

$$\vartheta\tau = \left(\prod_{p \leq e^{\kappa-1}} p\right)\left(\prod_{e^{\kappa-1} < p \leq e^\kappa} p^\kappa\right),$$

whence $p'|\vartheta\tau$, $p'|\vartheta$, and $p'|m_\nu^{(\kappa)}$. Therefore

$$p'' \cdot \frac{m_\nu^{(\kappa)}}{p'} = p'' \cdot \frac{\vartheta}{p'} \cdot N_{\kappa-1}$$

is a multiple of $N_{\kappa-1}$. Moreover

$$N_\kappa = \tau m_\nu^{(\kappa)} = p' \cdot \frac{\tau}{p''} \cdot p'' \cdot \frac{m_\nu^{(\kappa)}}{p'}$$

is a multiple of $p'' m_\nu^{(\kappa)}/p'$. Hence

$$p'' \cdot \frac{m_\nu^{(\kappa)}}{p'} = m_i^{(\kappa)}$$

for some $i > \nu$, since $p'' > p'$. It follows that

$$m_{\nu+1}^{(\kappa)} \leq p'' \cdot \frac{m_\nu^{(\kappa)}}{p'} \leq 2m_\nu^{(\kappa)}. \tag{1.5}$$

Let $q = \left[s_n/m_{\nu+1}^{(\kappa)}\right] + 1$. By (1.2) and (1.4) we have

$$\begin{aligned} q &\leq \frac{s_n}{m_{\nu+1}^{(\kappa)}} + 1 \\ &\leq c\, m_{\nu+1}^{(\kappa)} \operatorname{loglog} m_{\nu+1}^{(\kappa)} + 1 \\ &< \sigma\left(m_{\nu+1}^{(\kappa)}\right) + 1, \end{aligned}$$

whence, by Lemma 4, $r = q\, m_{\nu+1}^{(\kappa)}$ is a practical number. Further

$$r - s_n = m_{\nu+1}^{(\kappa)} \left(\left[\frac{s_n}{m_{\nu+1}^{(\kappa)}} \right] + 1 \right) - s_n > 0,$$

whence, by (1.3) and (1.5),

$$\begin{aligned} s_{n+1} - s_n &\le r - s_n \\ &= m_{\nu+1}^{(\kappa)} \left(1 - \left\{ \frac{s_n}{m_{\nu+1}^{(\kappa)}} \right\} \right) \\ &< 2 \frac{s_n}{c\, m_\nu^{(\kappa)} \operatorname{loglog} m_\nu^{(\kappa)}}. \end{aligned}$$

For any $\varepsilon > 0$ and any sufficiently large n we have, by (1.3), (1.4) and (1.5),

$$m_{\nu+1}^{(\kappa)\,2} \ge \frac{s_n}{c \operatorname{loglog} m_{\nu+1}^{(\kappa)}} \ge s_n^{1-\varepsilon} \tag{1.6}$$

and

$$\begin{aligned} s_{n+1} - s_n &< 2 \frac{m_{\nu+1}^{(\kappa)}}{m_\nu^{(\kappa)}} \cdot \frac{s_n}{c\, m_{\nu+1}^{(\kappa)} \operatorname{loglog} m_\nu^{(\kappa)}} \\ &\le 4 \frac{c^{1/2} \left(\operatorname{loglog} m_{\nu+1}^{(\kappa)} \right)^{1/2}}{s_n^{1/2}} \cdot \frac{s_n}{c \operatorname{loglog} m_\nu^{(\kappa)}} \\ &\le 4c^{-1/2}(1+\delta) \frac{s_n^{1/2}}{\left(\operatorname{loglog} m_\nu^{(\kappa)} \right)^{1/2}}. \end{aligned} \tag{1.7}$$

Since, by (1.5) and (1.6),

$$m_\nu^{(\kappa)} = \frac{m_\nu^{(\kappa)}}{m_{\nu+1}^{(\kappa)}} m_{\nu+1}^{(\kappa)} \ge \frac{1}{2} s_n^{(1-\varepsilon)/2},$$

we get

$$\operatorname{loglog} m_\nu^{(\kappa)} \ge \log \left(\frac{1-\varepsilon}{2} \log s_n - \log 2 \right) \ge (1-\delta) \operatorname{loglog} s_n,$$

whence, by (1.7),

$$s_{n+1} - s_n < A \frac{s_n^{1/2}}{(\operatorname{loglog} s_n)^{1/2}}.$$

□

Remark. By Gronwall's theorem [22, Theorem 323] we have

$$\limsup_{n\to\infty} \frac{\sigma(n)}{n \operatorname{loglog} n} = e^{\gamma},$$

which justifies the choice of the sequence N_k in our proof of the theorem.

1.6 Binary recurrence sequences

Let P and Q be non-zero integers; a pair of Lucas sequences $\{u_n(P,Q)\}$, $\{v_n(P,Q)\}$ is a pair of binary recurrence sequences defined as

$$\begin{cases} u_0(P,Q) &= 0 \\ u_1(P,Q) &= 1 \\ u_n(P,Q) &= P\,u_{n-1}(P,Q) - Q\,u_{n-2}(P,Q) \quad \text{for } n \geq 2 \end{cases}$$

and

$$\begin{cases} v_0(P,Q) &= 2 \\ v_1(P,Q) &= P \\ v_n(P,Q) &= P\,v_{n-1}(P,Q) - Q\,v_{n-2}(P,Q) \quad \text{for } n \geq 2. \end{cases}$$

The sequence $\{u_n(P,Q)\}$ is also called a *fundamental Lucas sequence* and $\{v_n(P,Q)\}$ its *companion sequence*.

Suppose $P^2 - 4Q \neq 0$ and let α, β be the distinct roots of the polynomial

$$x^2 - Px + Q.$$

We have

$$u_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

and

$$v_n(P,Q) = \alpha^n + \beta^n.$$

Using a shorter notation, we shall write u_n and v_n instead of $u_n(P,Q)$ and $v_n(P,Q)$. For $(P,Q) = (1,-1)$, u_n and v_n are the sequence of Fibonacci numbers and the sequence of Lucas numbers, respectively; for $(P,Q) = (2,-1)$, u_n is the sequence of Pell numbers [39, p. 56].

Theorem 4 *Let $\{u_n(P,Q)\}$ be a fundamental Lucas sequence. If $P^2 - 4Q > 0$ and $PQ + P$ is even, then the sequence $\{|u_n(P,Q)|\}$ contains infinitely many practical numbers.*

Proof. We shall prove that, for sufficiently large k, $|u_{3\cdot 2^k}|$ is a practical number. Let $\{v_n\}$ be the companion sequence of $\{u_n\}$. Since $u_{2m} = u_m v_m$ for every m, we have, for $k > 0$,

$$u_{3\cdot 2^k} = u_3 \cdot \prod_{h=0}^{k-1} v_{3\cdot 2^h}.$$

Also, $P^2 - 4Q > 0$ implies $u_3 = P^2 - Q > 0$. Note that $v_3 = P(P^2 - 3Q)$, whence $\operatorname{sgn} v_3 = \operatorname{sgn} P$. Since $P^2 - 4Q > 0$, we have $\alpha, \beta \in \mathbb{R}$, whence $v_n = \alpha^n + \beta^n$ is positive for n even. Therefore

$$|u_{3\cdot 2^k}| = u_3\,|v_3| \cdot \prod_{h=1}^{k-1} v_{3\cdot 2^h}.$$

Since $PQ + P$ is even, v_{3m} is even for all m. Denoting $v'_{3m} = v_{3m}/2$, we have

$$|u_{3\cdot 2^k}| = 2^k\,u_3\,|v'_3| \cdot \prod_{h=1}^{k-1} v'_{3\cdot 2^h}.$$

Let $2^{k+1} \geq \max\{u_3, |v'_3|\}$, and define $u^*_j = 2^k\,u_3\,|v'_3| \cdot \prod_{h=1}^{j-1} v'_{3\cdot 2^h}$. We show, by induction on j, that u^*_j is practical for $j = 1,\ldots,k$. For $j = 1$ this follows from Lemma 4 applied twice, since 2^k is practical and $u_3, |v'_3| \leq 2^{k+1}$. Let $1 \leq j \leq k-1$, and assume that u^*_j is practical. We have

$$u^*_j = 2^{k-j}\,|u_{3\cdot 2^j}|$$

and

$$u_{j+1}^* = u_j^* \, v'_{3\cdot 2^j},$$

where

$$v'_{3\cdot 2^j} = \frac{1}{2} v_{3\cdot 2^j} = \frac{1}{2}\left(\alpha^{2^j} + \beta^{2^j}\right)\left(\alpha^{2^{j+1}} - \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}}\right).$$

Note that

$$\alpha^{2^j} + \beta^{2^j} = v_{2^j}$$

and

$$\alpha^{2^{j+1}} - \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}} = v_{2^{j+1}} - Q^{2^j}$$

are positive integers (not both odd). In order to prove that u_{j+1}^* is practical, by Lemma 4 applied twice it suffices to show that

$$M = \max\left\{\alpha^{2^j} + \beta^{2^j},\ \alpha^{2^{j+1}} - \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}}\right\} < u_j^*.$$

Since $x + y \leq x^2 - xy + y^2 + 1$ for all $x, y \in \mathbb{R}$, we have

$$\begin{aligned} M &\leq \alpha^{2^{j+1}} - \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}} + 1 \\ &= v_{2^{j+1}} - Q^{2^j} + 1 \\ &< v_{2^{j+1}} + Q^{2^j} \\ &= \alpha^{2^{j+1}} + \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}}. \end{aligned}$$

From $P^2 - 4Q > 0$ and $P = \alpha + \beta \neq 0$ it follows that $\alpha \neq \pm\beta$. Therefore

$$u_{2^j} = \frac{\alpha^{2^j} - \beta^{2^j}}{\alpha - \beta} \neq 0,$$

i.e., $|u_{2^j}| \geq 1$. Hence

$$\begin{aligned} M &\leq |u_{2^j}|\left(\alpha^{2^{j+1}} + \alpha^{2^j}\beta^{2^j} + \beta^{2^{j+1}}\right) \\ &= \left|\frac{\alpha^{3\cdot 2^j} - \beta^{3\cdot 2^j}}{\alpha - \beta}\right| \\ &= |u_{3\cdot 2^j}| < 2^{k-j}\,|u_{3\cdot 2^j}| = u_j^*. \end{aligned}$$

□

Theorem 5 *Let $\{v_n(P,Q)\}$ be a companion Lucas sequence with $Q=-1$ and $P>0$. If there exists a positive integer t such that v_{35t} is practical, then $\{v_n\}$ contains infinitely many practical numbers.*

Proof. We shall prove by induction that, for every $k \ge 0$, $v_{3^k 35t}$ is practical. For $k=0$ this is true by assumption. Suppose that $v_{3^k 35t}$ is practical for some k. Since $v_n = \alpha^n + \beta^n$, where α and β are the roots of the polynomial $x^2 - Px + Q$, we have

$$v_{3^{k+1}35t} = v_{3^k 35t}\left(\alpha^{3^k 70t} - \alpha^{3^k 35t}\beta^{3^k 35t} + \beta^{3^k 70t}\right).$$

Define

$$\Phi_d(x,y) = \begin{cases} x^{\varphi(d)}\phi_d(y/x) & \text{if } x \neq 0 \\ 0 & \text{if } x=y=0 \\ y^{\varphi(d)}\phi_d(x/y) & \text{if } y \neq 0, \end{cases}$$

where ϕ_d is the d-th cyclotomic polynomial and φ is the Euler totient function. Note that $x^{\varphi(d)}\phi_d(y/x) = y^{\varphi(d)}\phi_d(x/y)$ if $x \neq 0$ and $y \neq 0$.

Since $x^{70} - x^{35}y^{35} + y^{70} = \Phi_6(x,y)\,\Phi_{30}(x,y)\,\Phi_{42}(x,y)\,\Phi_{210}(x,y)$, we have

$$v_{3^{k+1}35t} = v_{3^k 35t}\,\Phi_6\left(\alpha^{3^k t},\beta^{3^k t}\right)\Phi_{30}\left(\alpha^{3^k t},\beta^{3^k t}\right)\Phi_{42}\left(\alpha^{3^k t},\beta^{3^k t}\right)\Phi_{210}\left(\alpha^{3^k t},\beta^{3^k t}\right).$$

Note that, since $Q=-1$,

$$\begin{aligned}
\Phi_6\left(\alpha^{3^k t},\beta^{3^k t}\right) &= v_{3^k 2t} - (-1)^t \\
\Phi_{30}\left(\alpha^{3^k t},\beta^{3^k t}\right) &= v_{3^k 8t} + (-1)^t v_{3^k 6t} - (-1)^t v_{3^k 2t} - 1 \\
\Phi_{42}\left(\alpha^{3^k t},\beta^{3^k t}\right) &= v_{3^k 12t} + (-1)^t v_{3^k 10t} - (-1)^t v_{3^k 6t} - v_{3^k 4t} + 1 \\
\Phi_{210}\left(\alpha^{3^k t},\beta^{3^k t}\right) &= v_{3^k 48t} - (-1)^t v_{3^k 46t} + v_{3^k 44t} + (-1)^t v_{3^k 38t} - v_{3^k 36t} \\
&\quad +2(-1)^t v_{3^k 34t} - v_{3^k 32t} + (-1)^t v_{3^k 30t} + v_{3^k 24t} \\
&\quad -(-1)^t v_{3^k 22t} + v_{3^k 20t} - (-1)^t v_{3^k 18t} + v_{3^k 16t} \\
&\quad -(-1)^t v_{3^k 14t} - v_{3^k 8t} - v_{3^k 4t} - 1.
\end{aligned}$$

Since $P > 0$ and $Q = -1$, for every $n > 0$ we have $v_n < v_{n+1}$, whence

$$\begin{aligned}
0 < v_{3^k 2t} - 1 &\le \Phi_6\left(\alpha^{3^k t}, \beta^{3^k t}\right) \le v_{3^k 2t} + 1 < v_{3^k 35t}, \\
0 < v_{3^k 8t} - v_{3^k 6t} + v_{3^k 2t} - 1 &\le \Phi_{30}\left(\alpha^{3^k t}, \beta^{3^k t}\right) \le v_{3^k 8t} + v_{3^k 6t} < v_{3^k 35t}, \\
0 < v_{3^k 12t} - v_{3^k 10t} + v_{3^k 6t} - v_{3^k 4t} &\le \Phi_{42}\left(\alpha^{3^k t}, \beta^{3^k t}\right) \le v_{3^k 12t} + v_{3^k 10t} + 1 \\
&< v_{3^k 35t}.
\end{aligned}$$

Since $v_{3^{k+1}35t}$, $v_{3^k 35t}$, $\Phi_6\left(\alpha^{3^k t}, \beta^{3^k t}\right)$, $\Phi_{30}\left(\alpha^{3^k t}, \beta^{3^k t}\right)$, $\Phi_{42}\left(\alpha^{3^k t}, \beta^{3^k t}\right)$ are positive integers, we have $\Phi_{210}\left(\alpha^{3^k t}, \beta^{3^k t}\right) > 0$, and it is easy to show that $\Phi_{210}\left(\alpha^{3^k t}, \beta^{3^k t}\right) < 2v_{3^k 48t}$. By Lemma 4, we have that

$$m = v_{3^k 35t}\, \Phi_6\left(\alpha^{3^k t}, \beta^{3^k t}\right) \Phi_{30}\left(\alpha^{3^k t}, \beta^{3^k t}\right) \Phi_{42}\left(\alpha^{3^k t}, \beta^{3^k t}\right)$$

is a practical number. Since $v_{3^{k+1}35t} = m\, \Phi_{210}\left(\alpha^{3^k t}, \beta^{3^k t}\right)$, to complete the proof it suffices to show that $2v_{3^k 48t} \le 2m$, and this can be proved by straightforward and tedious calculations that we omit. □

The Fibonacci sequence $\{u_n(1,-1)\}$ and the Pell sequence $\{u_n(2,-1)\}$ satisfy the assumptions of Theorem 4. Since $L_{630} = v_{35\cdot 18}(1,-1)$ is a practical number, the Lucas sequence $\{v_n(1,-1)\}$ satisfies the assumptions of Theorem 5. Therefore there exist infinitely many practical Fibonacci, Pell and Lucas numbers.

It is interesting to note that the first practical Fibonacci numbers are F_3, F_6, F_{12}, F_{24}, F_{30}, F_{36}, F_{42}, F_{48}, which, except for F_3, have practical subscripts. It is well known that every prime Fibonacci number, except for F_4, has a prime subscript [22, Theorem 179, p. 148–150], but there exist some practical Fibonacci numbers with non-practical subscripts. The least such number is F_{444}. In fact, $444 = 2^2 \cdot 3 \cdot 37$ is not practical, but

$$\begin{aligned}
F_{444} = \; & 2^4 \cdot 3^2 \cdot 73 \cdot 149 \cdot 443 \cdot 2221 \cdot 4441 \cdot 11987 \cdot 1121101 \cdot 54018521 \\
& \cdot 55927129 \cdot 6870470209 \cdot 8336942267 \cdot 81143477963 \\
& \cdot 1459000305513721
\end{aligned}$$

is a practical number.

1.7 Experimental results and tables

In Fig. 1.1 one can see a graphical representation of $P(x)$ for $x \leq 6000$. The numerical data in this range support Margenstern's conjecture

$$P(x) \sim \lambda \frac{x}{\log x}$$

with $\lambda \simeq 1.341$.

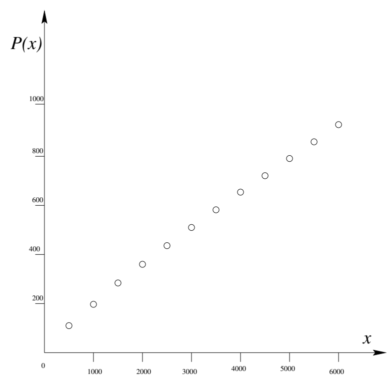

Fig. 1.1 The behavior of *P(x)*

In Fig. 1.2 there is a comparison between certain low values of $P(x)$ (circled) and the function $\lambda x/\log x$ (dotted).

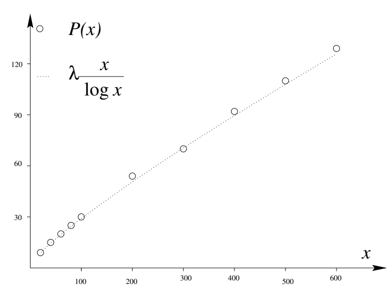

Fig. 1.2. A comparison with the conjecture

The following is a short table of practical numbers:

1	1	156	348	552	784	1020	1254	1484
2	2	160	352	558	792	1024	1260	1488
3	4	162	360	560	798	1026	1272	1496
4	6	168	364	570	800	1032	1280	1500
5	8	176	368	576	810	1036	1288	1504
6	12	180	378	580	812	1040	1290	1512
7	16	192	380	588	816	1044	1296	1518
8	18	196	384	594	820	1050	1300	1520
9	20	198	390	600	828	1056	1302	1530
10	24	200	392	608	832	1064	1312	1536
11	28	204	396	612	840	1080	1316	1540
12	30	208	400	616	858	1088	1320	1548
13	32	210	408	620	860	1092	1326	1554
14	36	216	414	624	864	1100	1332	1560
15	40	220	416	630	868	1104	1344	1566
16	42	224	420	640	870	1110	1350	1568
17	48	228	432	644	880	1116	1352	1584
18	54	234	440	648	882	1120	1360	1590
19	56	240	448	660	888	1122	1368	1596
20	60	252	450	666	896	1128	1372	1600
21	64	256	456	672	900	1134	1376	1620
22	66	260	460	680	912	1140	1380	1624
23	72	264	462	684	918	1144	1386	1632
24	78	270	464	690	920	1148	1392	1638
25	80	272	468	696	924	1152	1400	1640
26	84	276	476	700	928	1160	1404	1650
27	88	280	480	702	930	1170	1408	1656
28	90	288	486	704	936	1176	1410	1664
29	96	294	496	714	952	1184	1416	1672
30	100	300	500	720	960	1188	1428	1674
31	104	304	504	726	966	1200	1440	1680
32	108	306	510	728	968	1204	1452	1692
33	112	308	512	736	972	1216	1456	1696
34	120	312	520	740	980	1218	1458	1700
35	126	320	522	744	984	1224	1464	1710
36	128	324	528	750	990	1230	1470	1716
37	132	330	532	756	992	1232	1472	1720
38	140	336	540	760	1000	1240	1476	1722
39	144	340	544	768	1008	1242	1480	1728
40	150	342	546	780	1014	1248	1482	1736

Tab. 1.1 A short list of practical numbers.

In [31], among other things one can find further interesting remarks as well as several conjectures related to the experimental data, altogether supporting the similarity between the distribution properties of practical numbers and those of primes.

Chapter 2

Triplets and k-tuples of twin practical numbers

As we saw in the proof of Theorem 2, there exist infinitely many pairs $(m, m+2)$ of twin practical numbers (see also [31, Théorème 6] for a more general result), although it looks difficult to estimate the asymptotic behaviour of their counting function. In the proof of Theorem 2 we constructed a sequence $\{m_n\}_{n\in\mathbb{N}}$ of practical numbers such that $m_n + 2$ is also practical for every n, and such that $m_{n+1}/m_n < 2$. In [33] we get a slightly better estimate: $m_{n+1}/m_n < 3/2$. Both estimates give

$$\sum_{\substack{m\leq x \\ m,m+2 \text{ practical}}} 1 \gg \log x,$$

but this estimate is very far from the conjectured behaviour:

Conjecture 2 (Margenstern) *Let* $P_2(x) = \sum_{\substack{m\leq x \\ m,m+2 \text{ practical}}} 1$. *For a suitable constant* λ_2 *we have:*

$$P_2(x) = \sum_{\substack{m\leq x \\ m,m+2 \text{ practical}}} 1 \sim \lambda_2 \frac{x}{(\log x)^2}.$$

As is well-known, there is an analogous celebrated conjecture of Hardy and Littlewood [22, Section 22.20, p. 371–373] for $\pi_2(x)$, the counting function of the pairs of twin primes. Notice that the counting function of the pairs of twin primes has the same conjectural asymptotic behaviour.

Conjecture 3 (Hardy and Littlewood) *Let* $\pi_2(x) = \sum_{\substack{p \le x \\ p,p+2 \ primes}} 1$. *We have*

$$\pi_2(x) = \sum_{\substack{p \le x \\ p,p+2 \ primes}} 1 \sim \left(2 \prod_{p \ge 3} \left(1 - \frac{1}{(p-1)^2} \right) \right) \frac{x}{(\log x)^2}.$$

In this chapter we deal with the problem of the existence of k-tuples of twin practical numbers with $k \ge 3$.

We prove that there exist infinitely many triplets of the form $(m-2, m, m+2)$. Further we conjecture that there exist infinitely many 5-tuples of the form $(m-6, m-2, m, m+2, m+6)$. We discuss this conjecture and reduce it to very reasonable, although unproved, facts.

2.1 Triplets of twin practical numbers

The following theorem was conjectured in [30] and [31] and first proved in [33].

Theorem 6 *There exist infinitely many practical numbers* m *such that* $m-2$ *and* $m+2$ *are also practical.*

Proof. We shall prove that, for every non-negative integer k, $2 \cdot 3^{3^k \cdot 70} - 2$, $2 \cdot 3^{3^k \cdot 70}$ and $2 \cdot 3^{3^k \cdot 70} + 2$ are practical numbers.

By Stewart's structure theorem, $2 \cdot 3^{3^k \cdot 70}$ is obviously practical. We separately show, by induction on k, that $2 \cdot 3^{3^k \cdot 70} - 2$ and $2 \cdot 3^{3^k \cdot 70} + 2$ are practical. We have

$$2 \cdot 3^{70} - 2 = 2^4 \cdot 11^2 \cdot 61 \cdot 71 \cdot 547 \cdot 1093 \cdot 2664097031 \cdot 374857981681$$

and, by the structure theorem, this is a practical number. Suppose that $2 \cdot 3^{3^k \cdot 70} - 2$ is practical for some k. Then

$$2 \cdot 3^{3^{k+1} \cdot 70} - 2 = 2(3^{3^k \cdot 70} - 1)(3^{3^k \cdot 70} - 3^{3^k \cdot 35} + 1)(3^{3^k \cdot 70} + 3^{3^k \cdot 35} + 1)$$

whence, by Lemma 4 applied twice, $2 \cdot 3^{3^{k+1} \cdot 70} - 2$ is practical.

We now have

$$2 \cdot 3^{70} + 2 = 2^2 \cdot 5^2 \cdot 29 \cdot 1181 \cdot 16493 \cdot 28596961 \cdot 32839661 \cdot 94373861$$

and, by the structure theorem, this is a practical number. Suppose that $2 \cdot 3^{3^k \cdot 70} + 2$ is practical. Then

$$2 \cdot 3^{3^{k+1} \cdot 70} + 2 = 2(3^{3^k \cdot 70} + 1)\phi_{12}(3^{3^k})\phi_{60}(3^{3^k})\phi_{84}(3^{3^k})\phi_{420}(3^{3^k})$$

where $\phi_d(x)$ is the cyclotomic polynomial for $\exp(2\pi i/d)$. Here

$$\begin{aligned}
\phi_{12}(x) &= x^4 - x^2 + 1\\
\phi_{60}(x) &= x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1\\
\phi_{84}(x) &= x^{24} + x^{22} - x^{18} - x^{16} + x^{12} - x^8 - x^6 + x^2 + 1\\
\phi_{420}(x) &= x^{96} - x^{94} + x^{92} + x^{86} - x^{84} + 2x^{82} - x^{80} + x^{78} + x^{72} - x^{70}\\
&\quad + x^{68} - x^{66} + x^{64} - x^{62} - x^{56} - x^{52} - x^{48} - x^{44} - x^{40} - x^{34}\\
&\quad + x^{32} - x^{30} + x^{28} - x^{26} + x^{24} + x^{18} - x^{16} + 2x^{14} - x^{12} + x^{10}\\
&\quad + x^4 - x^2 + 1.
\end{aligned}$$

Applying four times Lemma 4, we see that $2 \cdot 3^{3^{k+1} \cdot 70} + 2$ is practical, and the theorem is proved. □

As a consequence of the preceding theorem we obtain

$$\sum_{\substack{m \le x \\ m-2,m,m+2 \text{ practical}}} 1 \gg \operatorname{loglog} x \ ,$$

very far from the following conjecture of Erdős [15]:

Conjecture 4 *There exists a positive constant c such that*

$$\sum_{\substack{m \le x \\ m-2,m,m+2 \ \textit{practical}}} 1 \gg \frac{x}{(\log x)^c} \ .$$

2.2 4-tuples and 5-tuples: a conjecture

It is shown in [31] that for any even $m > 2$, one at least of $m,\ m+2,\ m+4,\ m+6$ is not practical. In fact, among four consecutive even positive integers greater than 2, one at least is $\not\equiv 0 \bmod 3$ and $\not\equiv 0 \bmod 4$, hence is of the form $2q_1^{\alpha_1} \dots q_k^{\alpha_k}$ with odd primes $q_1 < q_2 < \dots < q_k$ and $q_1 \geq 5$.

On the other hand, explicit computations suggest the following conjecture:

Conjecture 5 *There exist infinitely many 5-tuples of practical numbers of the form* $(m-6,\ m-2,\ m,\ m+2,\ m+6)$.

Here is a short table of the first m's such that $m-6,\ m-2,\ m,\ m+2,\ m+6$ are practical numbers:

1	18	19	131070
2	30	20	219102
3	198	21	226182
4	306	22	237190
5	462	23	277506
6	1482	24	312702
7	2550	25	359658
8	4422	26	432822
9	17298	27	526878
10	23322	28	533370
11	23550	29	584166
12	40350	30	659934
13	52578	31	1032858
14	67938	32	1051650
15	88506	33	1140414
16	92202	34	1142658
17	96222	35	1243170
18	123006	36	1255422

Tab. 2.1 The first m's such that $m-6, m-2, m, m+2, m+6$ are practical numbers.

In the remaining part of this chapter we develop some theoretical arguments in support of the above conjecture.

A reasonable attempt to prove the conjecture might be to ask whether there exist infinitely many n such that $2 \cdot 3 \cdot (3^{n-1}-1),\ 2 \cdot (3^n - 1),\ 2 \cdot 3^n,\ 2 \cdot (3^n + 1),\ 2 \cdot 3 \cdot (3^{n-1} + 1)$ are practical numbers: in fact these 5-tuples are of the form of our conjecture. This approach is similar to the problem of the triplets that we solved in the preceding theorem.

As a related result, we prove the following proposition:

Proposition 3 *If* $s_2 = 2 \cdot (3^n - 1)$, $s_3 = 2 \cdot 3^n$, $s_4 = 2 \cdot (3^n + 1)$ *are practical numbers, and* $n > 1$, *then* n *is even and* $16 | s_2$, $18 | s_3$, $20 | s_4$. *Further, denoting* $s_1 = 2 \cdot 3 \cdot (3^{n-1} - 1)$, $s_5 = 2 \cdot 3 \cdot (3^{n-1} + 1)$, *we have that* $12 | s_1$, $24 | s_5$.

Proof. For $n = 2$ the proposition is true and for $n = 3$ we have that s_2 is not practical. Hence we assume $n > 3$. Since $3 \not| s_2$, then $s_2 = 2^{\alpha_0} q_1^{\alpha_1} \dots q_k^{\alpha_k}$ with primes $q_1 < q_2 < \dots < q_k$, with $q_1 \geq 5$ and positive integers $\alpha_0, \dots, \alpha_k$. Further

$$3^n - 1 \equiv 0 \bmod 5 \iff n \equiv 0 \bmod 4,$$

$$3^n - 1 \equiv 0 \bmod 7 \iff n \equiv 0 \bmod 6,$$

$$3^n - 1 \equiv 2 \bmod 4 \iff n \equiv 1 \bmod 2.$$

Hence if n were odd, we would have $\alpha_0 = 2$ and $q_1 \geq 11$ and by the structure theorem s_2 would not be practical. Therefore n is even. In particular $3^n - 1 \equiv 0 \bmod 8$, i.e., $16 | s_2$.

Trivially that $18 | s_3$.

Since n is even, $3^n + 1 \equiv 2 \bmod 4$, hence $s_4 = 2^{\beta_0} r_1^{\beta_1} \dots r_h^{\beta_h}$ with $\beta_0 = 2$ and with primes $r_1 < r_2 < \dots < r_k$, with $r_1 \geq 5$ and positive integers $\beta_1, \dots, \beta_k$. On the other hand $3^{2j} + 1 \not\equiv 0 \bmod 7$ for any j, and since s_4 is practical, we must have $r_1 \leq 8$ and $r_1 \neq 7$, hence $r_1 = 5$ and $n \equiv 2 \bmod 4$, so $20 | s_4$.

Since $s_1 = s_3 - 6$ and $s_1 = s_2 - 4$, we respectively get $3 | s_1$ and $4 | s_1$, i.e., $12 | s_1$.

Since $s_5 = s_3 + 6$ and $s_5 = s_2 + 8$, we respectively get $3 | s_1$ and $8 | s_1$, i.e., $24 | s_5$. □

In particular for every 5-tuple of practical number of the form $(m - 6, m - 2, m, m + 2, m + 6)$ we must have $m \equiv 2 \bmod 4$.

2.3 Attacking the conjecture

Here we study some arithmetical questions related to our approach for Conjecture 5.

Proposition 4 *Let* $\{p_k\}_{k \in \mathbb{N}}$ *be the sequence of primes, and let* $n_k = \prod_{i=1}^{k} p_i$. *For every integer* $k \geq 1$, *the number* $2 \cdot (3^{n_k} - 1)$ *is a practical number.*

Proof. A direct computation shows that for $k = 1, 2, \ldots, 10$ the statement is true. We now assume the proposition true for $k \geq 10$, and prove that $2 \cdot (3^{n_{k+1}} - 1)$ is a practical number. Note that $n_{k+1} = n_k p_{k+1}$, whence

$$2 \cdot (3^{n_{k+1}} - 1) = 2 \cdot (3^{n_k} - 1) \prod_{d \mid n_k} \phi_{dp_{k+1}}(3).$$

By the inductive assumption $2 \cdot (3^{n_k} - 1)$ is a practical number. Note that for every positive integer n, $\phi_n(3)$ is a positive integer (see also (2.1) below). Further if $dp_{k+1} < n_k$ then $\phi_{dp_{k+1}}(3) < 3^{n_k} - 1$. In fact

$$3^{n_k} - 1 > 3^{dp_{k+1}} - 1 = \phi_{dp_{k+1}}(3) \prod_{\substack{r \mid dp_{k+1} \\ r < dp_{k+1}}} \phi_r(3) > \phi_{dp_{k+1}}(3).$$

Hence we have

$$2 \cdot (3^{n_{k+1}} - 1) = 2 \cdot (3^{n_k} - 1) \prod_{\substack{d \mid n_k \\ d < n_k/p_{k+1}}} \phi_{dp_{k+1}}(3) \cdot \prod_{\substack{d \mid n_k \\ d > n_k/p_{k+1}}} \phi_{dp_{k+1}}(3)$$

and by the inductive assumption and by Stewart's structure theorem, we have that $2 \cdot (3^{n_k} - 1) \prod_{\substack{d \mid n_k \\ d < n_k/p_{k+1}}} \phi_{dp_{k+1}}(3)$ is practical. To prove the proposition, by iterated applications of Stewart's structure theorem, we shall prove that every factor of the form $\phi_{dp_{k+1}}(3)$ with $d \mid n_k$ and $d > n_k/p_{k+1}$ is bounded by a product of suitable $\phi_{d'}(3)$'s with $d' \mid n_{k+1}$ and $d' < dp_{k+1}$.

By [40], for every integer $n > 1$ one has

$$\left(\frac{16}{27}\right)^{2^{\nu(n)-2}} 3^{\varphi(n)} < \phi_n(3) < \left(\frac{3}{2}\right)^{2^{\nu(n)-1}} 3^{\varphi(n)}, \tag{2.1}$$

where $\nu(n)$ is the number of distinct prime factors of n and φ is the Euler totient function. Note that for $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_\ell^{\alpha_\ell}$ with primes $q_1 < \cdots < q_\ell$ and positive integers $\alpha_1, \ldots \alpha_\ell$ one has

$$2^{\nu(n)-1} = \overbrace{2 \cdot 2 \cdots 2}^{\ell-1 \text{ times}} \leq \varphi(q_2^{\alpha_2}) \varphi(q_3^{\alpha_3}) \cdots \varphi(q_\ell^{\alpha_\ell}) \leq \varphi(n),$$

hence from (2.1) one easily gets

$$\varphi(n) \log \frac{4}{\sqrt{3}} < \log \phi_n(3) < \varphi(n) \log \frac{9}{2}.$$

Let $d|n_k$, $d > n_k/p_{k+1}$ and suppose $d \neq n_k$. Let $l < k$ such that

$$\max\{p, p \not| d\} = p_l.$$

For $1 \leq i \leq k-l$ define $d_i = dp_l/p_{l+i}$. Obviously $d > d_1 > d_2 > \cdots > d_{k-l}$. Also

$$\varphi(d_i p_{k+1}) = \frac{p_l - 1}{p_{l+i} - 1}\varphi(dp_{k+1}).$$

If $4 \leq l \leq k-4$ one has:

$$\begin{aligned}
\log \prod_{i=1}^{4} \phi_{d_i p_{k+1}}(3) &> \left(\sum_{i=1}^{4} \varphi(d_i p_{k+1})\right) \log \frac{4}{\sqrt{3}} \\
&= (p_l - 1)\left(\sum_{i=1}^{4} \frac{1}{p_{l+i} - 1}\right) \varphi(dp_{k+1}) \log \frac{4}{\sqrt{3}} \\
&> \varphi(dp_{k+1}) \log \frac{9}{2} > \log \phi_{dp_{k+1}}(3),
\end{aligned}$$

hence

$$\prod_{i=1}^{4} \phi_{d_i p_{k+1}}(3) > \phi_{dp_{k+1}}(3).$$

If $l > k-4 \geq 4$, we must have $d = n_k/p_l$. In fact if $d < n_k/p_l$, we would have $d < n_k/2p_l$, and for $k \geq 10$ we have $2p_l > p_{k+1}$, whence $d < n_k/p_{k+1}$, a contradiction.

Let $d'_1 = n_k/p_k$, $d'_2 = n_k/2p_k$, $d'_3 = n_k/3p_k$, $d'_4 = n_k/6p_k$, $d'_5 = n_k/5p_k$, $d'_6 = n_k/10p_k$. Again $d > d'_1 > d'_2 > \cdots > d'_6$. We have:

$$\varphi(d'_1 p_{k+1}) = \varphi(d'_2 p_{k+1}) = \frac{p_l - 1}{p_k - 1}\varphi(dp_{k+1}),$$

$$\varphi(d'_3 p_{k+1}) = \varphi(d'_4 p_{k+1}) = \frac{p_l - 1}{2(p_k - 1)}\varphi(dp_{k+1}),$$

$$\varphi(d'_5 p_{k+1}) = \varphi(d'_5 p_{k+1}) = \frac{p_l - 1}{4(p_k - 1)}\varphi(dp_{k+1}),$$

hence

$$\begin{aligned}\log \prod_{i=1}^{6} \phi_{d'_i p_{k+1}}(3) &> \frac{7}{2}\frac{p_l - 1}{p_k - 1}\varphi(dp_{k+1}) \log \frac{4}{\sqrt{3}} \\ &> \varphi(dp_{k+1}) \log \frac{9}{2} > \log \phi_{dp_{k+1}}(3).\end{aligned}$$

In particular

$$\prod_{i=1}^{6} \phi_{d'_i p_{k+1}}(3) > \phi_{dp_{k+1}}(3).$$

If $l = 3$ it is easy to prove that

$$\prod_{i=1}^{5} \phi_{d_i p_{k+1}}(3) > \phi_{dp_{k+1}}(3).$$

If $l = 1, 2$ or if $d = n_k$ then $d = \delta p_3 p_4 \dots p_k$ with $\delta = 1, 2, 3, 6$. In any of these cases it is not difficult to find a suitable number of cyclotomic polynomials of index $d' | dp_{k+1}$ and $d' < dp_{k+1}$ such that their product valuated at 3 is greater than $\phi_{dp_{k+1}}(3)$. $\square$

The preceding proposition suggests the following definition:

Definition 5 *Let $\mathcal{D} = \{d_1, d_2, \dots, d_n\}$ be an ordered finite sequence of positive integers. For $1 < i \leq n$ we say that d_i is admissible for $\mathcal{D}$ if*

$$\sum_{j<i} \varphi(d_j) \log \frac{4}{\sqrt{3}} > \varphi(d_i) \log \frac{9}{2}.$$

Remark that this definition depends on the arrangement of the elements of $\mathcal{D}$.

Lemma 6 *Let $\mathcal{D} = \{d_1, d_2, \dots, d_n\}$ be a finite sequence of positive integers ordered in increasing order. Suppose that $d \in \mathcal{D}$ is admissible for $\mathcal{D}$. Let $q \in \mathbb{N}$ and let $\mathcal{D}(q)$ be the set of its divisors. Let $\mathcal{D}' = \mathcal{D}(q) \cdot \mathcal{D}$ ordered in increasing order. Then qd is admissible for $\mathcal{D}'$.*

Proof. We can assume that q is a prime. Since d is admissible for $\mathcal{D}$ there exist $d_{i_1}, \ldots, d_{i_\ell}$ with $\max_{1\le j\le \ell}\{d_{i_j}\} < d$ such that

$$\sum_{j=1}^{\ell} \varphi(d_{i_j}) \log \frac{4}{\sqrt{3}} > \varphi(d) \log \frac{9}{2}.$$

We can assume that $(d_{i_j}, q) = 1$ for $j \le h$ and that $q | d_{i_j}$ for $j > h$. We now take $\ell + h$ terms of $\mathcal{D}'$ less than dq as follows: for $1 \le j \le h$ we take d_{i_j} and qd_{i_j}. Notice that

$$\varphi(d_{i_j}) + \varphi(qd_{i_j}) = q\varphi(d_{i_j}).$$

For $j > h$ we take qd_{i_j}. In this case

$$\varphi(qd_{i_j}) = q\varphi(d_{i_j}).$$

Since q is a prime, $d_{i_1}, d_{i_2}, \ldots, d_{i_\ell}, qd_{i_1}, qd_{i_2}, \ldots, qd_{i_h}$ are distinct and less than qd. Further

$$\begin{aligned}\left(\log \frac{4}{\sqrt{3}}\right)\left(\sum_{j=1}^{\ell} \varphi(qd_{i_j}) + \sum_{j=1}^{h} \varphi(d_{i_j})\right) &= q\left(\log \frac{4}{\sqrt{3}}\right)\sum_{j=1}^{\ell}\varphi(d_{i_j}) \\ &> q\left(\log \frac{9}{2}\right)\varphi(d) \\ &\ge \left(\log \frac{9}{2}\right)\varphi(dq)\end{aligned}$$

and this proves the admissibility of dq for $\mathcal{D}'$. □

Lemma 7 *Let $\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$ be an ordered finite sequence of positive integers. Suppose that $M \cdot \prod_{j=1}^{i} \phi_{d_j}(3)$ is practical and that for $j > i$ d_j is admissible for $\mathcal{D}$. Then*

$$M \cdot \prod_{j=1}^{n} \phi_{d_j}(3)$$

is practical.

Proof. In order to prove this lemma by finite induction, suppose that for an index $h \geq i$ the number $M \cdot \prod_{j=1}^{h} \phi_{d_j}(3)$ is practical. We shall prove that $M \cdot \prod_{j=1}^{h+1} \phi_{d_j}(3)$ is practical. We have

$$M \cdot \prod_{j=1}^{h+1} \phi_{d_j}(3) = M \cdot \prod_{j=1}^{h} \phi_{d_j}(3) \cdot \phi_{d_{h+1}}(3).$$

By the structure theorem it suffices to prove that

$$\phi_{d_{h+1}}(3) \leq 2M \prod_{j=1}^{h} \phi_{d_j}(3).$$

By (2.1) one has

$$\log \phi_{d_{h+1}}(3) < \varphi(d_{h+1}) \log \frac{9}{2}$$

and since $h+1 > i$, d_{h+1} is admissible for $\mathcal{D}$. Hence

$$\begin{aligned}
\log \phi_{d_{h+1}}(3) &< \varphi(d_{h+1}) \log \frac{9}{2} \\
&< \left(\log \frac{4}{\sqrt{3}}\right) \sum_{j=1}^{h} \varphi(d_j) \\
&< \sum_{j=1}^{h} \log \phi_{d_j}(3) \\
&= \log \prod_{j=1}^{h} \phi_{d_j}(3) \\
&< \log \left(2M \prod_{j=1}^{h} \phi_{d_j}(3)\right)
\end{aligned}$$

and this proves the statement. □

2.4 Reducing the conjecture to a reasonable statement

We now define two auxiliary sequences of increasing positive integers, $m_n^{(e)}$ and $m_n^{(o)}$. Let $\{p_n\}_{n\in\mathbb{N}}$ be the increasing sequence of primes ($p_1 = 2$) and let

$$\begin{cases} m_1^{(e)} & = 2 \\ m_2^{(e)} & = 2\cdot 5 \\ m_3^{(e)} & = 2\cdot 5\cdot 11 \\ m_n^{(e)} & = \begin{cases} m_{n-1}^{(e)}\cdot p_{2n} & \text{if } m_{n-1}^{(e)} < m_{n-1}^{(o)} \text{ and } n > 3 \\ m_{n-1}^{(e)}\cdot p_{2n-1} & \text{if } m_{n-1}^{(e)} > m_{n-1}^{(o)} \text{ and } n > 3 \end{cases} \end{cases} \tag{2.2}$$

and

$$\begin{cases} m_1^{(o)} & = 3 \\ m_2^{(o)} & = 3\cdot 7 \\ m_3^{(o)} & = 3\cdot 7\cdot 13 \\ m_n^{(o)} & = \begin{cases} m_{n-1}^{(o)}\cdot p_{2n} & \text{if } m_{n-1}^{(o)} < m_{n-1}^{(e)} \text{ and } n > 3 \\ m_{n-1}^{(o)}\cdot p_{2n-1} & \text{if } m_{n-1}^{(o)} > m_{n-1}^{(e)} \text{ and } n > 3. \end{cases} \end{cases} \tag{2.3}$$

Remark that

$$\lim_{n\to\infty} \frac{m_n^{(e)}}{m_n^{(o)}} = 1$$

and that $(m_n^{(e)}, m_n^{(o)}) = 1$ for every n. We can now prove the following

Proposition 5 *For every sufficiently large n the numbers*

(i) $\quad 2\cdot 3\cdot (3^{m_n^{(o)}} - 1)$

(ii) $\quad 2\cdot (3^{m_n^{(e)}} - 1)$

(iii) $\quad 2\cdot (3^{m_n^{(e)}} + 1)$

(iv) $\quad 2\cdot 3\cdot (3^{m_n^{(o)}} + 1)$

are all practical numbers.

Proof. The proof is similar for each of the above four cases. We shall prove that, for each number *(i), (ii), (iii), (iv)* and for sufficiently large n, there exists an arrangement $\mathcal{D}_n$ of divisors (respectively divisors of $m_n^{(o)}$, divisors of $m_n^{(e)}$, divisors of $2m_n^{(e)}$ which are not divisors of $m_n^{(e)}$, and divisors of $2m_n^{(o)}$ which are not divisors of $m_n^{(o)}$) and a finite set $\mathcal{A} \subseteq \mathcal{D}_n$, independent of n and formed by a suitable number of terms at the beginning of the arrangement of $\mathcal{D}_n$, with the properties that every term of $\mathcal{D}_n - \mathcal{A}$ is admissible for $\mathcal{D}_n$. Since each number *(i), (ii), (iii), (iv)* is of the form $M \cdot \prod_{d\in\mathcal{D}_n} \phi_d(3)$ and $M \cdot \prod_{d\in\mathcal{A}} \phi_d(3)$ is practical, by Lemma 7 we achieve the proof.

(i). We have

$$2 \cdot 3 \cdot (3^{m_n^{(o)}} - 1) = 2 \cdot 3 \cdot \prod_{d|m_n^{(o)}} \phi_d(3).$$

Let

$$\begin{aligned} A_1(n) &= \prod_{\substack{d|m_n^{(o)} \\ d\leq 23}} \phi_d(3) \\ B_1(n) &= \prod_{\substack{d|m_n^{(o)} \\ 23<d<m_n^{(o)}/3}} \phi_d(3) \\ C_1(n) &= \phi_{m_n^{(o)}/3}(3) \cdot \phi_{m_n^{(o)}}(3). \end{aligned}$$

We have $2 \cdot 3 \cdot (3^{m_n^{(o)}} - 1) = 2 \cdot 3A_1(n)B_1(n)C_1(n)$. For sufficiently large n, $A_1(n)$ does not depend on n since

$$A_1(n) = \phi_1(3)\phi_3(3)\phi_7(3)\phi_{13}(3)\phi_{17}(3)\phi_{21}(3)\phi_{23}(3).$$

Hence for sufficiently large n

$$\begin{aligned} 2 \cdot 3A_1(n) = \ & 2^2 \cdot 3 \cdot 13 \cdot 47 \cdot 1093 \cdot 1871 \cdot 34511 \cdot \\ & \cdot 368089 \cdot 797161 \cdot 1001523179 \end{aligned}$$

which is a practical number by the structure theorem. The next step is to prove that $2 \cdot 3A_1(n)B_1(n)$ is practical.

For $n = 5, 6, 7, 8$ one can directly check that every divisor d of $m_n^{(o)}$ with $17 < d < m_n^{(o)}/3$ is admissible for the increasing arrangement of the divisors of $m_n^{(o)}$, hence by the preceding lemma $2 \cdot 3A_1(n)B_1(n)$ is practical. Let $n \geq 8$ and assume that there exists an arrangement $\mathcal{D}_n$ of the divisors of $m_n^{(o)}$ such that every divisor d with $17 < d < m_n^{(o)}/3$ is admissible for $\mathcal{D}_n$. Let $m_{n+1}^{(o)} = m_n^{(o)} p$ and define the following arrangement $\mathcal{D}_{n+1}$ of the divisors of $m_{n+1}^{(o)}$ with $\mathcal{D}_{n+1} \supset \mathcal{D}_n$. First we put the ordered finite sequence $\mathcal{D}_n$ excluding $m_n^{(o)}/3$ and $m_n^{(o)}$; then we put $p\mathcal{D}_n$ again excluding $m_{n+1}^{(o)}/3$ and $m_{n+1}^{(o)}$; then we put the ordered set of the four numbers $m_n^{(o)}/3$, $m_n^{(o)}$, $m_{n+1}^{(o)}/3$ and $m_{n+1}^{(o)}$.

For the first set of divisors d of $m_{n+1}^{(o)}$ it is obvious that every $d > 17$ is admissible for $\mathcal{D}_{n+1}$ since d is admissible for $\mathcal{D}_n$ and $\mathcal{D}_{n+1} \supset \mathcal{D}_n$. This easily implies that for the second set of divisors (see the proof of Lemma 6) every divisor of $m_{n+1}^{(o)}$ of the form dp with $d | m_n^{(o)}$ and $d > 17$ (in this set $d < m_n^{(o)}/3 < m_{n+1}^{(o)}/3$) is admissible. If a divisor of this set is of the form dp with $d | m_n^{(o)}$ and $d = 1, 3, 7, 13$ or 17 and $n \geq 8$ we have:

$$\begin{aligned} \left(\log \frac{9}{2}\right) \varphi(dp) &\leq \left(\log \frac{9}{2}\right) \cdot 16 \cdot (p-1) \\ &< \left(\log \frac{\sqrt{3}}{4}\right) \left(m_n^{(o)} - \varphi(m_n^{(o)}) - \varphi\left(\frac{m_n^{(o)}}{3}\right)\right) \\ &= \left(\log \frac{\sqrt{3}}{4}\right) \sum_{\substack{d' | m_n^{(o)} \\ d' < m_n^{(o)}/3}} \varphi(d') \end{aligned}$$

and in our arrangement every $d' | m_n^{(o)}$, $d' < m_n^{(o)}/3$ precedes dp, hence dp is admissible.

In order to prove the admissibility of all divisors d of $m_{n+1}^{(o)}$ with $17 < d < m_{n+1}^{(o)}/3$ it remains to prove that $m_n^{(o)}/3$ and $m_n^{(o)}$ are admissible for $\mathcal{D}_{n+1}$. Since $n \geq 8$ we have $p \geq 61$, hence $p - 1 > 6 \log \frac{9}{2} / \log \frac{\sqrt{3}}{4}$. This implies that

$$\varphi\left(\frac{m_n^{(o)}}{3}\right) \log \frac{9}{2} < \varphi(m_n^{(o)}) \log \frac{9}{2} < \varphi\left(\frac{m_n^{(o)}}{7} p\right) \log \frac{\sqrt{3}}{4},$$

i.e., both $m_n^{(o)}/3$ and $m_n^{(o)}$ are admissible for $\mathcal{D}_{n+1}$.

To complete the proof of *(i)* we now prove that for sufficiently large n $m_{n+1}^{(o)}/3$ and $m_{n+1}^{(o)}$ are admissible for $\mathcal{D}_{n+1}$ so by the preceding proposition

$2\cdot 3\cdot(3^{m^{(o)}_{n+1}}-1)$ is practical. In fact, since $\varphi(m_n^{(o)}p)=o(m_n^{(o)}p)$, for sufficiently large n we have:

$$\begin{aligned}\left(\log\frac{\sqrt{3}}{4}\right)\sum_{\substack{d\mid m^{(o)}_{n+1}\\ d<m^{(o)}_{n+1}/3}}\varphi(d) &= \left(\log\frac{\sqrt{3}}{4}\right)\left(m_n^{(o)}p-\varphi(m_n^{(o)}p)-\varphi\left(\frac{m_n^{(o)}p}{3}\right)\right)\\ &> \left(\log\frac{9}{2}\right)\varphi(m_n^{(o)}p)\\ &= \max\left\{\varphi\left(\frac{m_n^{(o)}p}{3}\right),\varphi\left(m_n^{(o)}p\right)\right\}\log\frac{9}{2}\end{aligned}$$

as required.

(ii). We have

$$2\cdot(3^{m_n^{(e)}}-1)=2\cdot\prod_{d\mid m_n^{(e)}}\phi_d(3).$$

Let

$$\begin{aligned}A_2(n) &= \prod_{\substack{d\mid m_n^{(e)}\\ d\le 29}}\phi_d(3)\\ B_2(n) &= \prod_{\substack{d\mid m_n^{(e)}\\ 29<d<m_n^{(e)}/3}}\phi_d(3)\\ C_2(n) &= \phi_{m_n^{(e)}/3}(3)\cdot\phi_{m_n^{(e)}}(3)\end{aligned}$$

hence $2(3^{m_n^{(e)}}-1)=2A_2(n)B_2(n)C_2(n)$. For sufficiently large n, $A_2(n)$ does not depend on n since

$$A_2(n)=\phi_1(3)\phi_2(3)\phi_5(3)\phi_{10}(3)\phi_{11}(3)\phi_{19}(3)\phi_{22}(3)\phi_{29}(3).$$

Hence for sufficiently large n

$$\begin{aligned}2A_2(n)= {}& 2^4\cdot 11^2\cdot 23\cdot 59\cdot 61\cdot 67\cdot 661\cdot 1597\cdot 3851\cdot 28537\\ &\cdot 363889\cdot 20381027\end{aligned}$$

which is a practical number by the structure theorem. The remaining part of Case *(ii)* is similar to Case *(i)*.

(iii). We have

$$2 \cdot (3^{m_n^{(e)}} + 1) = 2 \cdot \prod_{\substack{d \mid 2m_n^{(e)} \\ d \nmid m_n^{(e)}}} \phi_d(3).$$

Let

$$\begin{aligned} A_3(n) &= \prod_{\substack{d \mid 2m_n^{(e)} \\ d \nmid m_n^{(e)} \\ d \le 148}} \phi_d(3) \\ B_3(n) &= \prod_{\substack{d \mid 2m_n^{(e)} \\ d \nmid m_n^{(e)} \\ 148 < d < 2m_n^{(e)}/3}} \phi_d(3) \\ C_3(n) &= \phi_{2m_n^{(e)}/3}(3) \cdot \phi_{2m_n^{(e)}}(3) \end{aligned}$$

hence $2(3^{m_n^{(e)}} + 1) = 2A_3(n)B_3(n)C_3(n)$. For sufficiently large n, $A_3(n)$ does not depend on n since

$$A_3(n) = \phi_4(3)\phi_{20}(3)\phi_{44}(3)\phi_{76}(3)\phi_{116}(3)\phi_{148}(3).$$

Hence for sufficiently large n

$$\begin{aligned} 2A_3(n) = \; & 2^2 \cdot 5^2 \cdot 149 \cdot 1181 \cdot 5501 \cdot 12413 \cdot 570461 \cdot 953861 \cdot 5301533 \cdot \\ & \cdot 25480398173 \cdot 3794512766529000523013 \cdot \\ & \cdot 1426597598014049207713915 93 \end{aligned}$$

which is a practical number by the structure theorem. The remaining part of Case *(iii)* is similar to the preceding cases.

(iv). We have

$$2 \cdot 3 \cdot (3^{m_n^{(o)}} + 1) = 2 \cdot 3 \cdot \prod_{\substack{d \mid 2m_n^{(o)} \\ d \nmid m_n^{(o)}}} \phi_d(3).$$

Let

$$A_4(n) = \prod_{\substack{d \mid 2m_n^{(o)} \\ d \nmid m_n^{(o)} \\ d \le 34}} \phi_d(3)$$

$$B_4(n) = \prod_{\substack{d \mid 2m_n^{(o)} \\ d \nmid m_n^{(o)} \\ 34 < d < 2m_n^{(e)}/3}} \phi_d(3)$$

$$C_4(n) = \phi_{2m_n^{(o)}/3}(3) \cdot \phi_{2m_n^{(o)}}(3)$$

hence $2 \cdot 3(3^{m_n^{(o)}} + 1) = 2 \cdot 3A_4(n)B_4(n)C_4(n)$. For sufficiently large n, $A_4(n)$ does not depend on n since

$$A_4(n) = \phi_2(3)\phi_6(3)\phi_{14}(3)\phi_{26}(3)\phi_{34}(3).$$

Hence for sufficiently large n

$$2 \cdot 3A_4(n) = 2^3 \cdot 3 \cdot 7 \cdot 103 \cdot 307 \cdot 547 \cdot 1021 \cdot 398581$$

which is a practical number by the structure theorem. The remaining part of Case *(iv)* is similar to the preceding cases. □

Note that the preceding proposition incidentally provides a second proof of Theorem 6.

Remark. The arguments of the proof of the preceding proposition are suitable to exhibit an effectively computable constant c with $0 < c < 1$ such that for every odd positive integer $r < c \min\{m_n^{(e)}, m_n^{(o)}\}$ the numbers

$$\text{(i')} \quad 2 \cdot 3 \cdot (3^{rm_n^{(o)}} - 1)$$

$$\text{(ii')} \quad 2 \cdot (3^{rm_n^{(e)}} - 1)$$

$$\text{(iii')} \quad 2 \cdot (3^{rm_n^{(e)}} + 1)$$

$$\text{(iv')} \quad 2 \cdot 3 \cdot (3^{rm_n^{(o)}} + 1)$$

are all practical numbers.

We are ready to prove the following

Theorem 7 *At least one of the two following statements holds:*

(a) There exist only finitely many pairs $(m_n^{(e)}, m_n^{(o)})$ *such that the Diophantine equation*

$$xm_n^{(e)} - ym_n^{(o)} = 1$$

has a solution in odd integers x, y *and* $0 < x, y < c\min\{m_n^{(e)}, m_n^{(o)}\}$*, where* c *is defined as above.*

(b) There exist infinitely many 5-tuples of practical numbers of the form $(m-6,\ m-2,\ m,\ m+2,\ m+6)$.

Proof. Suppose that for infinitely many n there exist $m_n^{(e)}$, $m_n^{(o)}$ and odd integers x_n, y_n such that $0 < x_n, y_n < c\min\{m_n^{(e)}, m_n^{(o)}\}$ and $x_n m_n^{(e)} - y_n m_n^{(o)} = 1$. Then for sufficiently large n the numbers $2 \cdot 3(3^{y_n m_n^{(o)}} - 1)$, $2(3^{x_n m_n^{(e)}} - 1)$, $2(3^{x_n m_n^{(e)}} + 1)$, $2 \cdot 3(3^{y_n m_n^{(o)}} + 1)$ are practical numbers by preceding remark. Hence for $m = 2 \cdot 3^{x_n m_n^{(e)}}$, the numbers $m - 6 = 2 \cdot 3(3^{y_n m_n^{(o)}} - 1)$, $m - 2 = 2(3^{x_n m_n^{(e)}} - 1)$, m, $m + 2 = 2(3^{x_n m_n^{(e)}} + 1)$ and $m + 6 = 2 \cdot 3(3^{y_n m_n^{(o)}} + 1)$ are practical numbers. □

We remark that statistical arguments suggest that *(a)* should be false, although a proof of this seems to be difficult at first sight.

Here we give a table, for $n \leq 28$, of $\max\{x_n, y_n\}/\min\{m_n^{(e)}, m_n^{(o)}\}$, where (x_n, y_n) denotes the minimal solution of $x_n m_n^{(e)} - y_n m_n^{(o)} = 1$ with $x_n, y_n > 0$:

n	$\max\{x_n, y_n\}/\min\{m_n^{(e)}, m_n^{(o)}\}$
4	1.1464
5	0.5664
6	0.4725
7	1.0632
8	0.6149
9	0.5835
10	0.6452
11	0.2628
12	0.3792
13	0.5130
14	0.9658
15	0.0587
16	0.9239
17	0.9082
18	0.5328
19	0.6265
20	0.5096
21	0.2425
22	0.4523
23	0.1205
24	0.8573
25	0.9386
26	0.7556
27	0.0535
28	0.1132

Tab 2.2. Results related to the Diophantine equation $x_n m_n^{(e)} - y_n m_n^{(o)} = 1$.

The table suggests that for sufficiently large n the distribution of the above values may be uniform in $[0, 1]$, as expected.

Chapter 3

A problem on sum-free sequences

This chapter arises from a letter of Erdős [16] in which he states some of his favourite problems on additive number theory. Here we deal with one of these problems. This problem was first raised by Erdős and Deshouillers in a conversation. Successively I had several useful discussions with both Erdős and Deshouillers. Most of the material of this chapter is contained in the paper [9], which originated from these collaborations.

We begin with a definition concerning certain positive integer sequences.

Definition 6 *An increasing sequence of positive integers $\{n_k\}_{k\in\mathbb{N}}$ is called a sum-free sequence if every term is never a sum of distinct smaller terms. In other words if*

$$\sum_{j=1}^{k} n_{i_j} = n_m$$

with $i_1 < i_2 < \cdots < i_k$ implies $k = 1$ and $n_{i_1} = n_m$.

This definition first appeared in an old paper [14] of Erdős, where he also proved certain related results and raised several interesting problems. In [21, Section E28] these sequences are also called A-sequences. Erdős proved that for any sum-free sequence $\{n_k\}$ one has

$$\sum_{j=1}^{\infty} \frac{1}{n_j} < 103,$$

and since the sequence of powers of 2 is a sum-free sequence for which the sum of reciprocals is 2, it is natural to define

$$R = \sup_{\{n_k\}\ \text{sum-free}} \left\{ \sum_{j=1}^{\infty} \frac{1}{n_j} \right\}.$$

Hence $2 \leq R \leq 103$. Levine and O'Sullivan [28] improved on this estimate in 1977 establishing $2.035 < R < 4$. In 1987, Abbott [1] further improved on the lower bound getting $2.064 < R$.

In another paper Levine [27], settling a conjecture of Erdős, proved that if $\{n_k\}$ is a sum-free sequence with $n_1 > x$ then

$$\sum_{j=1}^{\infty} \frac{1}{n_j} < \log 2 + \varepsilon(x),$$

where $\lim_{x\to\infty} \varepsilon(x) = 0$.

Some other papers have been recently devoted to a special kind of finite sum-free sequences, namely those finite sequences $\{n_k\}$ of positive integers having the property that whenever a given positive integer can be written as a sum of distinct elements of the sequence, the number of summands is fixed. In other words, for these sequences, also called admissible sequences, no positive integer m can be expressed as two sums of distinct elements of $\{n_k\}$ with a different number of summands. For some interesting results on finite admissible sequences one can see [10], [11].

Here we are interested in infinite sum-free sequences. In the above-mentioned [16] letter Erdős wrote:

"I am not able to find a sequence of integers $n_1 < n_2 < \dots,\ \ n_{k+1}/n_k \to 1$ and n_h is never a sum of smaller n_i's [...] *Deshouillers and I raised this question."*

We refer to the above problem as the Erdős-Deshouillers problem. For a sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ we shall denote by $A(x)$ its counting function:

$$A(x) = \sum_{n_k < x} 1.$$

Define

$$\varrho = \sup_{\{n_k\}\ \text{sum-free sequence}} \{\lambda \mid A(x) \gg x^{\lambda}\}.$$

Erdős proved that $2/7 \le \varrho \le (\sqrt{5}-1)/2$. Here we improve the lower bound of ϱ, namely we prove $1/3 \le \varrho$.

In Section 1 we give a clever example, due to Erdős [14], of a sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ with polynomial growth. However, the example does not solve the Erdős-Deshouillers problem, i.e., for this sequence we have

$$\limsup_{k\to\infty} \frac{n_{k+1}}{n_k} > 1.$$

In Section 2 we give an elementary solution of the problem, providing a sequence with the required properties, but with sub-exponential growth.

Finally in Section 3 we give a further solution, kindly communicated by Deshouillers, by providing a sequence with polynomial growth. We prove that for any $\varepsilon > 0$, there exists a sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ which solves the above Erdős-Deshouillers problem, and such that

$$A(x) \gg x^{\frac{1}{3}-\varepsilon}.$$

In Section 4 we study other related questions. Among other things we prove that any sum-free sequence cannot grow too slowly: in fact we prove that every sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ has zero asymptotic density and for $\alpha > (\sqrt{5}-1)/2 \simeq 0.618$ we have

$$\liminf_{x\to\infty} \frac{A(x)}{x^\alpha} = 0.$$

3.1 A sum-free sequence with polynomial growth

In this section we shall describe an interesting method, due to Erdős [14], to construct sum-free sequences. This allows us to construct an increasing sequence of positive integers $n_1 < n_2 < \dots$ such that the equation

$$n_k = n_{i_1} + n_{i_2} + \cdots + n_{i_r} \tag{3.1}$$

has no solution with $i_1 < i_2 < \cdots < i_r$ and $r > 1$. For this sequence one gets

$$A(x) \gg x^{2/7}.$$

Notice that this estimate is not the best possible. Also, the sequence does not satisfy the condition

$$\lim_{k\to\infty} \frac{n_{k+1}}{n_k} = 1, \tag{3.2}$$

but, in our opinion, the method is interesting, and susceptible of further improvements.

Proposition 6 (Erdős) *There exists a sum-free sequence* $\{n_k\}_{k\in\mathbb{N}}$ *such that* $A(x) \gg x^{2/7}$.

Proof. Let $n_1 = 1$ and define recursively the other terms as follows. Suppose that $n_1, \dots, n_{k_i}$ are defined and that $n_1, \dots, n_{k_i}$ is a finite sum-free sequence. Let $B_{i+1} = 2\sum_{r=1}^{k_i} n_r$. We can assume that $B_{i+1} > 40$ (for example if we take $n_k = 2^{k-1}$, for $k = 1, \dots, 6$). Let

$$n_{k_i+l} = 1 + lB_{i+1}, \quad 1 \le l \le \left[\frac{B_{i+1}^2}{10}\right], \tag{3.3}$$

where $[m]$ denotes the integer part of m. Note that $n_{k_i+l} \le \frac{B_{i+1}^3}{10} + 1$. One can easily see that (3.1) has no solution. Suppose that

$$n_{k_i+l} = \sum_{s=1}^{t_1} n_{k_i+r_s} + \sum_{s=1}^{t_2} n_{j_s} = \Sigma_1 + \Sigma_2 \tag{3.4}$$

where $j_1 < j_2 < \cdots < j_{t_2} \le k_i$. We first prove that $t_1 \le \left[\frac{B_{i+1}}{2}\right]$. In fact, assuming $t_1 > \left[\frac{B_{i+1}}{2}\right]$, by (3.3) we have

$$\Sigma_1 \ge \sum_{l=1}^{t_1} 1 + lB_{i+1} > \frac{t_1^2}{2}B_{i+1} \ge \frac{B_{i+1}^3}{8} > n_{k_i} + l$$

contradicting (3.4). Hence $t_1 \le \left[\frac{B_{i+1}}{2}\right]$ and by (3.3) one has

$$\Sigma_1 \equiv t_1 \bmod B_{i+1}.$$

By (3.3) we have $n_{k_i+l} \equiv 1 \bmod B_{i+1}$, hence by (3.4)

$$\Sigma_2 > \left[\frac{B_{i+1}}{2}\right]. \tag{3.5}$$

But $\Sigma_2 \leq \sum_{j=1}^{k_i} n_j = \dfrac{B_{i+1}}{2}$, contradicting (3.5). This proves that (3.1) has no solution. Let now

$$B_{i+2} = 2\sum_{r=1}^{k_{i+1}} n_r, \quad n_{k_{i+1}+l} = 1 + lB_{i+2}, \quad 1 \leq l \leq \left[\frac{B_{i+2}^2}{10}\right] \tag{3.6}$$

where $k_{i+1}k_i + \left[\dfrac{B_{i+1}^2}{10}\right]$. By (3.3) and (3.6) one has

$$\begin{aligned} B_{i+2} &= 2\sum_{r=1}^{k_{i+1}} n_r + 2\sum_{l=1}^{\left[\frac{B_{i+1}^2}{10}\right]} n_{k_i+l} \\ &< B_{i+1} + 2\left[\frac{B_{i+1}^2}{10}\right]\left(\frac{B_{i+1}^3}{10}+1\right) \\ &< B_{i+1}^5. \end{aligned}$$

Hence by (3.6)

$$A(B_{i+2}) > k_{i+1} > \frac{B_{i+1}^2}{10} > \frac{1}{10}B_{i+2}^{\frac{2}{5}}.$$

Further we have

$$A(TB_{i+2}) \geq \left[\frac{B_{i+1}^2}{10}\right] + T - 1 > \frac{1}{10}B_{i+2}^{\frac{2}{5}} + T. \tag{3.7}$$

For $1 \leq T \leq \dfrac{B_{i+2}^{\frac{2}{5}}}{10}$, we have $A(TB_{i+2}) \geq \dfrac{B_{i+2}^{\frac{2}{5}}}{10}$ and in the worst case

$$A\left(\frac{B_{i+2}^{\frac{7}{5}}}{10}\right) > \frac{B_{i+2}^{\frac{2}{5}}}{10} = \left(\frac{1}{10}\right)^{\frac{5}{7}} \cdot \left(\frac{1}{10}B_{i+2}^{\frac{7}{5}}\right)^{\frac{2}{7}},$$

hence for $B_{i+2} \le x \le B_{i+2}^{\frac{7}{5}}$ we have $A(x) > cx^{\frac{2}{7}}$. If $T > \frac{B_{i+2}^{\frac{2}{5}}}{10}$, then the main term in (3.7) is T and the worst case also gives $T = \frac{B_{i+2}^{\frac{2}{5}}}{10}$.

Therefore for every x

$$A(x) > cx^{\frac{2}{7}}.$$

□

3.2 An elementary solution

In this section we construct a suitable sequence with the properties required by the Erdős-Deshouillers problem.

Proposition 7 *There is an explicitly computable sum-free sequence $\{n_k\}_{k\in\mathbb{N}}$ such that*

$$\lim_{k\to\infty} \frac{n_{k+1}}{n_k} = 1.$$

Proof. For every positive integer h, define $A_1^{(h)} = 10^{h-1}$, $A_{10^{h+2}-1}^{(h)} = 10^{2h+3}$, and choose $A_1^{(h)} < A_2^{(h)} < \cdots < A_{10^{h+2}-1}^{(h)}$, such that for sufficiently large h,

$$\frac{A_{i+1}^{(h)}}{A_i^{(h)}} \le 10^{2(h+4)/(10^{h+2}-2)} \quad \text{for every } i \text{ with } 1 \le i \le 10^{h+2}-2.$$

This can be made, for example, by recursively defining

$$\begin{cases} A_1^{(h)} &= 10^{h-1} \\ A_i^{(h)} &= \max\left\{A_{i-1}^{(h)}+1, [10^{h-1}\cdot 10^{i(h+4)/(10^{h+2}-1)}]\right\} \quad \text{for } i > 1. \end{cases}$$

Let

$$\begin{aligned} S_h = \ & \left\{A_i^{(h)}\cdot 10^{h(h+5)/2} + 10^{(h-1)(h+4)/2}, i = 1, 2, \ldots, 10^{h+2}-1\right\} \\ = \ & \left\{s_{1,h}, s_{2,h}, \ldots, s_{10^{h+2}-1,h}\right\} \end{aligned}$$

with $s_{1,h} < s_{2,h} < \cdots < s_{10^{h+2}-1,h}$. Let

$$S = \bigcup_{h=1}^{\infty} S_h = \{n_1, n_2, \dots\}$$

with $n_1 < n_2 < \dots$. Note that $\max S_h < \min S_{h+1}$. In fact

$$\max S_h = s_{10^{h+2}-1,h} = 10^{(h^2+9h+6)/2} + 10^{(h-1)(h+4)/2}$$

and

$$\min S_{h+1} = s_{1,h+1} = 10^{(h^2+9h+6)/2} + 10^{h(h+5)/2}.$$

Hence for every k we have that n_{k+1}/n_k is of the form $s_{i+1,h}/s_{i,h}$ for suitable i and h or of the form $s_{1,h+1}/s_{10^{h+2}-1,h}$. In the first case one easily gets for sufficiently large h

$$\frac{s_{i+1,h}}{s_{i,h}} < \frac{A_{i+1}^{(h)}}{A_i^{(h)}} < 10^{2(h+4)(10^{h+2}-2)}.$$

In the latter case one has

$$\frac{s_{1,h+1}}{s_{10^{h+2}-1,h}} = \frac{10^{(h^2+9h+6)/2} + 10^{h(h+5)/2}}{10^{(h^2+9h+6)/2} + 10^{(h-1)(h+4)/2}}.$$

This proves that

$$\lim_{k\to\infty} \frac{n_{k+1}}{n_k} = 1.$$

Let us show that S is sum-free. Suppose that $n \in S$. For a suitable h, we have that $n \in S_h$. Suppose that $n = \sum_{i\in I} n_i$ with $n_i \in S$, and let $l = \min\{j, \exists i \in I, n_i \in S_j\}$. We have

$$n \equiv \#\{n_i, n_i \in S_l\} \cdot 10^{(l-1)(l+4)/2} \bmod 10^{l(l+5)/2}.$$

Since

$$\#\{n_i, n_i \in S_l\} \le 10^{l+2} - 1,$$

one has that

$$n \not\equiv 0 \bmod 10^{l(l+5)/2}.$$

But $n \in S_h$, hence for every $j < h$

$$n \equiv 0 \bmod 10^{j(j+5)/2}$$

and

$$n \equiv 10^{(h-1)(h+4)/2} \bmod 10^{h(h+5)/2}.$$

Therefore $l = h$ and $\#\{n_i, n_i \in S_l\} = 1$, i.e., n is not a sum of distinct smaller terms $n_i \in S$.

Let $A(x)$ the counting function of $\{n_k\}$. Assuming $\max S_h < x \leq \max S_{h+1}$ we have $A(x) < 2 \cdot 10^{h+3}$ and $10^{(h^2+9h+6)/2} < x$. Since $(h+3) \leq (h^2+9h+6)^{1/2}$ one easily gets

$$A(x) \ll \exp\{c(\log x)^{1/2}\}.$$

In the next section we find other sequences solving the Erdős-Deshouillers problem with a better asymptotic behaviour.

3.3 A further solution

In this section we prove the following

Theorem 8 *There exists a sum-free sequence $\{n_k\}_{k \in \mathbb{N}}$ such that*

$$\lim_{k \to \infty} \frac{n_{k+1}}{n_k} = 1,$$

and with polynomial growth.

Proof. Let α be a quadratic irrational and let $\varepsilon > 0$. Let $\zeta(s)$ be the Riemann zeta-function and let H be a fixed positive constant greater than $\zeta(1+\varepsilon)$. Let k be a positive integer. By the Erdős-Turán inequality (cf. [25], example 3.2 p. 124), we have

$$\# \left\{ n \in [M+1, M+N] \;\middle|\; \frac{1}{H(k+1)^{1+\varepsilon}} < \{\alpha n\} < \frac{1}{Hk^{1+\varepsilon}} \right\}$$

$$\geq \frac{(1+\varepsilon)N}{Hk^{2+\varepsilon}} - C \log^2 N,$$

where $\{u\}$ denotes the fractional part of the real number u.

Thus there exists N_0 not depending on M such that if $N \geq \max\{N_0, k^{2+2\varepsilon}\}$ there exists n in $[M+1, M+N]$ such that $\dfrac{1}{H(k+1)^{1+\varepsilon}} < \{\alpha n\} < \dfrac{1}{Hk^{1+\varepsilon}}$. This allows us to construct by induction a sequence $n_1 < n_2 < \cdots$ such that $n_1 \geq N_0$ and such that for every k

$$\frac{1}{H(k+1)^{1+\varepsilon}} < \{\alpha n_k\} < \frac{1}{Hk^{1+\varepsilon}}.$$

Further for every sufficiently large k

$$n_{k-1} < n_k \leq n_{k-1} + k^{2+2\varepsilon}. \tag{3.8}$$

The property (3.8) implies that

$$n_k \ll k^{3+2\varepsilon},$$

or, equivalently, if $A(x)$ denotes the counting function of $\{n_k\}_{k\in\mathbb{N}}$ we have in this case

$$A(x) \gg x^{\frac{1}{3+2\varepsilon}} \gg x^{\frac{1}{3}-\varepsilon}.$$

We now prove that $\{n_k\}_{k\in\mathbb{N}}$ is a sum-free sequence. In fact if we assume that $\{n_k\}_{k\in\mathbb{N}}$ is not a sum-free sequence, we have for a suitable subscript k

$$n_k = n_{i_1} + \cdots + n_{i_s} \text{ with } k > i_1 > \cdots > i_s,$$

which implies $\alpha n_k = \alpha n_{i_1} + \cdots + \alpha n_{i_s}$. On the other hand $\{\alpha n_k\} < \dfrac{1}{Hk^{1+\varepsilon}}$ and for each $j = 1, \ldots, s$ we have $\{\alpha n_{i_j}\} > \dfrac{1}{Hk^{1+\varepsilon}}$ hence

$$\frac{1}{Hk^{1+\varepsilon}} < \{\alpha n_{i_1}\} + \cdots + \{\alpha n_{i_s}\} < \frac{1}{H}\sum_{\ell=1}^{\infty}\frac{1}{\ell^{1+\varepsilon}} < 1,$$

whence

$$\frac{1}{Hk^{1+\varepsilon}} < \{\alpha n_{i_1} + \cdots + \alpha n_{i_s}\} = \{\alpha n_k\} < \frac{1}{Hk^{1+\varepsilon}},$$

a contradiction which proves the result. □

3.4 Some related questions

Theorem 9 *If $\{n_k\}_{k\in\mathbb{N}}$ is a sum-free sequence then it has zero asymptotic density.*

Proof. Suppose that there exists $h > 0$ such that for sufficiently large n, $\#\{n_k \mid n_k < n\} > hn$. Let $r = [1/h] + 1$, and $b = n_1 + n_2 + \ldots + n_r$. Let $\varepsilon > 0$. There exists a sufficiently large m such that the interval $[n_{r+1}, m - b]$ contains at least $(h - \varepsilon)m$ integers belonging to $\{n_k\}_{k\in\mathbb{N}}$. For every integer l, with $0 \le l \le r$ define $s_0 = 0$ and $s_l = n_1 + n_2 + \ldots + n_l$. Further define the set R_l as follows:

$$R_l = \Big\{s_l + n_j \mid l + 1 \le j \le r + (h - \varepsilon)m\Big\}.$$

Each R_l contains at least $[(h - \varepsilon)m]$ distinct positive integers. Further $\max R_l \le m$. Notice that if $l \ne l'$ then $R_l \bigcap R_{l'} = \emptyset$. Indeed if $s_l + n_j = s_{l'} + n_{j'}$, with $l < l'$, then $n_j = (s_{l'} - s_l) + n_{j'}$, i.e., n_j is a sum of distinct smaller terms of $\{n_k\}_{k\in\mathbb{N}}$. Hence the interval $[1, m]$ contains at least $(r+1)[(h-\varepsilon)m]$ distinct positive integers. But if ε is sufficiently small

$$(r + 1)[(h - \varepsilon)m] > m.$$

Therefore $\{n_k\}_{k\in\mathbb{N}}$ has zero asymptotic density. □

This argument can be used to prove a further similar result.

Theorem 10 *Let $\alpha > (\sqrt{5} - 1)/2 \simeq 0.618$. Let $\{n_k\}_{k\in\mathbb{N}}$ be a sum-free sequence. Then*

$$\liminf_{n\to\infty} \frac{A(n)}{n^\alpha} = 0,$$

where $A(n)$ is the counting function of $\{n_k\}_{k\in\mathbb{N}}$.

Proof. It suffices to prove that for every $\alpha > (\sqrt{5}-1)/2$, there exist infinitely many n such that $A(n) \le n^\alpha$.

If $\alpha \ge 1$ this follows from the preceding theorem. Let $(\sqrt{5}-1)/2 < \alpha < 1$. Suppose that $A(n) > n^\alpha$ for sufficiently large n. Let m be such an n. Then the interval $[1, m]$ contains at least m^α integers belonging to $\{n_k\}_{k\in\mathbb{N}}$. Let $r = [m^{1-\alpha}] + 1$. If m is sufficiently large, $r = A(n_r) > n_r^\alpha$, i.e., $n_r < r^{1/\alpha}$. Let $b = n_1 + n_2 + \ldots + n_r$. Since $r = O(m^{1-\alpha})$, we have that $n_r = O(m^{\frac{1}{\alpha}-1})$ and $b = O(m^{\frac{1}{\alpha}-\alpha})$. Since $\alpha > (\sqrt{5}-1)/2$ we have $b = o(m)$. Let $\varepsilon > 0$. If m is sufficiently large, the interval $[n_{r+1}, m-b]$ contains at least $(m-b)^\alpha - r$ integers belonging to $\{n_k\}_{k\in\mathbb{N}}$. Since $(m-b)^\alpha - r - m^\alpha = o(m^\alpha)$, for sufficiently large m we have $(m-b)^\alpha - r > (1-\varepsilon)m^\alpha$, namely the interval $[n_{r+1}, m-b]$ contains at least $(1-\varepsilon)m^\alpha$ integers belonging to $\{n_k\}_{k\in\mathbb{N}}$. As in the preceding theorem, let R_l be defined as follows:

$$R_l = \{s_l + n_j \mid l + 1 \leq j \leq r + (1-\varepsilon)m^\alpha\}.$$

Each R_l contains at least $[(1-\varepsilon)m^\alpha]$ distinct positive integers. Further $\max R_l \leq m$ and for $l \neq l'$, $R_l \bigcap R_{l'} = \emptyset$.

Hence the interval $[1, m]$ contains at least $(r+1)[(1-\varepsilon)m^\alpha]$ distinct positive integers. On the other hand, if ε is sufficiently small

$$(r+1)[(1-\varepsilon)m^\alpha] > m.$$

This completes the proof. □

We end this chapter with a different open problem raised by Erdős during a conversation I had with him:

Problem *Prove or disprove that there exists an infinite admissible sequence* $\{n_k\}_{k\in\mathbb{N}}$ *such that*

$$\lim_{k\to\infty} \frac{n_{k+1}}{n_k} = 1.$$

Chapter 4

Modular forms and functions

In this chapter we survey some basic tools about modular forms and functions. Fourier expansions of modular forms of weight $2k$ are related to the functions $\sigma_{2k-1}(n)$. Hence suitable relations involving modular forms can be translated into relations among sum-of-divisors functions. Modular forms for the full modular group yield well-known arithmetical identities [43, p. 152]. In order to find further identities, we require modular forms for certain congruence subgroups.

Ample surveys of the theory of modular forms and functions can be found in literature. In particular we quote [20], [24], [43] and [44] for our purposes.

In this chapter we mainly show how to construct suitable modular forms for certain congruence subgroups. These modular forms will be used in the next chapter to prove some remarkable arithmetical identities.

4.1 Modular forms and functions

In this section we recall classical tools about modular forms and functions. We shall denote by τ an element of $\mathbb{H}$, the upper half-plane of $\mathbb{C}$. For $\tau \in \mathbb{H}$, let $q = e^{2\pi i\tau}$ and $q_m = e^{2\pi i\tau/m}$. Let $\Gamma = SL(2,\mathbb{Z})$.

Definition 7 *A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight $2k$ for Γ if*

$$(c\tau + d)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau) \qquad \text{for every } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

and if f is regular at ∞, i.e.,

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n.$$

We define $f(\infty) = a_0$. If $a_0 = 0$ then f is called a cusp form for the full modular group Γ.

For each integer $m \geq 2$, we define the congruence subgroups $\Gamma(m)$, $\Gamma_1(m)$ and $\Gamma_0(m)$ as usual:

$$\Gamma(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| a \equiv d \equiv 1 \bmod m,\ b \equiv c \equiv 0 \bmod m \right\},$$

$$\Gamma_1(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| a \equiv d \equiv 1 \bmod m,\ c \equiv 0 \bmod m \right\},$$

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| c \equiv 0 \bmod m \right\}.$$

If G is a subgroup of Γ and $G \supseteq \Gamma(m)$, we say that G is a congruence subgroup of level m. The subgroup $\Gamma(m)$ is also called the principal congruence subgroup of level m. Generalizing the preceding definition we state the following

Definition 8 *A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight $2k$ for a congruence subgroup G of level m if*

$$(c\tau + d)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau) \qquad \text{for every } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \tag{4.1}$$

and

$$(c\tau + d)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right) = \sum_{n=0}^{\infty} a_{n,A} q_m^n \qquad \text{for every } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \tag{4.2}$$

where the coefficients $a_{n,A}$ depend on the matrix A.

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $c \neq 0$, we call a/c a finite cusp and define $f(a/c) = a_{0,A}$. Further we define $f(\infty) = a_{0,I}$.

Notice that the definition of $f(a/c)$ does not depend on the choice of the coefficients b and d in A (see [24, Prop. 16, p. 126]). It is worth remarking that

$$f\left(\frac{a}{c}\right) = a_{0,A} = \lim_{\tau \to i\infty} (c\tau + d)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right).$$

Definition 9 *If $a_{0,A} = 0$ for every $A \in \Gamma$, then f is called a cusp form for G.*

In other words, a cusp form is a modular form that vanishes at every finite cusp $a/c \in \mathbb{Q}$ and at the cusp ∞.

For integers $k \geq 2$, as is well-known [43], the Eisenstein series

$$E_{2k}(\tau) = 1 + \frac{2}{\zeta(1-2k)} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

are modular forms of weight $2k$ for Γ, and

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

is a cusp form of weight 12 for Γ.

We shall also denote $E_{2k,m}(\tau) = E_{2k}(m\tau)$. As we shall see, for $k \geq 2$, the functions $E_{2k,m}$ are modular forms of weight $2k$ for $\Gamma_0(m)$.

We shall denote by $S_{2k}(G)$ the vector space of the cusp forms of weight $2k$ for G.

Definition 10 *Let F be a closed subset of $\mathbb{H}$. We say that F is a fundamental domain for G if*

(i) every $\tau \in \mathbb{H}$ is G-equivalent to a $\tau' \in F$;

(ii) no two distinct τ, τ' in the interior of $\mathbb{H}$ are G-equivalent.

A fundamental domain F for Γ is shown in Fig. 4.1.

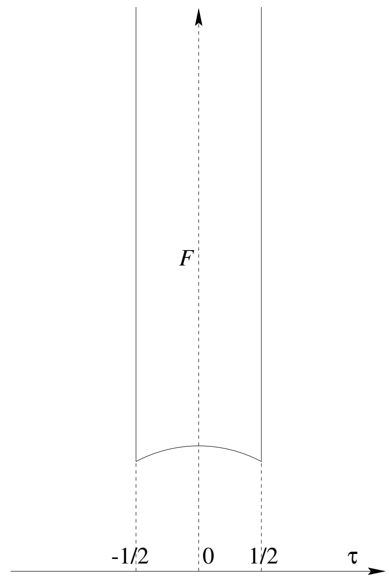

Fig. 4.1 A fundamental domain for Γ

4.2 Behaviour at the cusps

Let r be any positive integer. Using modular properties of $E_{2k}(\tau)$, both for $k = 1$ and for $k \geq 2$, we can find the expansions of $E_{2k,r}$ at the cusps. Let $(a, c) = 1$. In the usual topology of $\mathbb{H} \cup \{\text{cusps}\}$ (see [24, p. 103–105]) we have, for $k \geq 2$ and $\varepsilon \to 0$,

$$E_{2k,r}\left(\frac{a}{c} + \varepsilon\right) \sim \frac{(c, r)^{2k}}{r^{2k} c^{2k} \varepsilon^{2k}}.$$

In fact if b, d are integers such that $ad - bc = 1$, denoting

$$\xi = -\frac{d}{c} - \frac{1}{\varepsilon c^2} \in \mathbb{H},$$

we have

$$\frac{a}{c} + \varepsilon = \frac{a\xi + b}{c\xi + d},$$

$$c\xi + d = -\frac{1}{\varepsilon c}.$$

Hence

$$E_{2k}\left(\frac{a}{c}+\varepsilon\right)=E_{2k}\left(\frac{a\xi+b}{c\xi+d}\right)=(c\xi+d)^{2k}E_{2k}(\xi).$$

Since, for $\varepsilon\to 0$ in the usual topology of $\mathbb{H}\cup\{\text{cusps}\}$, $\operatorname{Im}\xi\to+\infty$, it follows that $E_{2k}(\xi)\to 1$, i.e., $E_{2k}(\frac{a}{c}+\varepsilon)\sim\frac{1}{\varepsilon^{2k}c^{2k}}$. If r is any positive integer, denoting $a'=ra/(r,c)$ and $c'=c/(r,c)$, $\varepsilon'=r\varepsilon$, we have $(a',c')=1$, whence

$$E_{2k,r}\left(\frac{a}{c}+\varepsilon\right)=E_{2k}\left(\frac{a'}{c'}+\varepsilon'\right)\sim\frac{1}{\varepsilon'^{2k}c'^{2k}}=\frac{(c,r)^{2k}}{r^{2k}c^{2k}\varepsilon^{2k}}.$$

With the same notation as above, for a modular form f of weight $2k$ we have

$$f\left(\frac{a}{c}\right)=\lim_{\tau\to i\infty}(c\tau+d)^{-2k}f\left(\frac{a\tau+b}{c\tau+d}\right)=\lim_{\varepsilon\to 0}(c\varepsilon)^{2k}f\left(\frac{a}{c}+\varepsilon\right),$$

therefore, for $k\geq 2$

$$E_{2k,r}\left(\frac{a}{c}\right)=\lim_{\varepsilon\to 0}(c\varepsilon)^{2k}E_{2k,r}\left(\frac{a}{c}+\varepsilon\right)=\frac{(c,r)^{2k}}{r^{2k}}. \tag{4.3}$$

The function $E_2(\tau)=1-24\sum_{n=1}^{\infty}\sigma_1(n)q^n$ is not a modular form, so we cannot define $E_2(a/c)$ and $E_{2,r}(a/c)$. However for any $\varepsilon\in\mathbb{H}$, we have $a/c+\varepsilon\in\mathbb{H}$, and we can try to derive the asymptotic behaviour of E_2 and $E_{2,r}$ in a neighborhood of a/c of the usual topology of $\mathbb{H}\cup\{\text{cusps}\}$. We have under the action of Γ

$$E_2\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^2E_2(\tau)+\frac{6}{\pi i}c(c\tau+d),$$

whence

$$E_2\left(\frac{a}{c}+\varepsilon\right)=E_2\left(\frac{a\xi+b}{c\xi+d}\right)=(c\xi+d)^2E_2(\xi)+\frac{6}{\pi i}c(c\xi+d).$$

Therefore

$$E_{2,r}\left(\frac{a}{c}+\varepsilon\right)=E_2\left(\frac{a'}{c'}+\varepsilon'\right)\sim\frac{1}{\varepsilon'^2c'^2}=\frac{(c,r)^2}{r^2c^2\varepsilon^2}.$$

In the next section, we shall see that suitable functions depending on E_2 and $E_{2,r}$ are modular forms for certain congruence subgroups.

4.3 Congruence subgroups

Here we are also interested in modular forms and functions for suitable congruence subgroups.

From the above-mentioned modular properties of $E_2(\tau)$, it immediately follows that $G(\tau) = E_2(\tau) - mE_2(m\tau)$ is a modular form of weight 2 for $\Gamma_0(m)$. In fact for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(m)$, we have that $c_1 = c/m$ is an integer and

$$\begin{aligned} G\left(\frac{a\tau+b}{c\tau+d}\right) &= E_2\left(\frac{a\tau+b}{c\tau+d}\right) - mE_2\left(\frac{a(m\tau)+bm}{c_1(m\tau)+d}\right) \\ &= (c\tau+d)^2E_2(\tau) + \frac{6}{\pi i}c(c\tau+d) \\ &\quad -m(c_1m\tau+d)^2E_2(m\tau) - m\frac{6}{\pi i}c_1(c_1m\tau+d) \\ &= (c\tau+d)^2E_2(\tau) - m(c\tau+d)^2E_2(m\tau) \\ &= (c\tau+d)^2G(\tau), \end{aligned}$$

i.e., G verifies the condition (4.1). With the notation of the preceding section we have

$$\begin{aligned} G\left(\frac{a}{c}\right) &= \lim_{\varepsilon\to 0}(c\varepsilon)^{2k}G\left(\frac{a}{c}+\varepsilon\right) \\ &= \lim_{\varepsilon\to 0}(c\varepsilon)^{2k}\left(E_2\left(\frac{a}{c}+\varepsilon\right) - mE_{2,m}\left(\frac{a}{c}+\varepsilon\right)\right) \\ &= 1 - \frac{(c,m)^2}{m}, \end{aligned}$$

whence G verifies (4.2).

We now prove that for $k \geq 2$, the functions $E_{2k,m}$ are modular forms of weight $2k$ for $\Gamma_0(m)$. In fact we have:

$$\begin{aligned} E_{2k,m}\left(\frac{a\tau+b}{c\tau+d}\right) &= E_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) - mE_{2k}\left(\frac{a(m\tau)+bm}{c_1(m\tau)+d}\right) \\ &= (c\tau+d)^2E_2(\tau) - m(c_1m\tau+d)^2E_2(m\tau) \\ &= (c\tau+d)^2E_2(\tau) - m(c\tau+d)^2E_2(m\tau) \\ &= (c\tau+d)^2E_{2k,m}(\tau), \end{aligned}$$

verifying (4.1). By (4.3) $E_{2k,m}$ also verifies (4.2).

In certain cases we need to check (4.1) in a different way. For example, one can check (4.1) only for the generators of G. In order to apply this method, we must find these generators. This is not easy in general, but for congruence subgroups of low level it can be done quite easily.

We now prove some results that will be useful in this context.

Proposition 8 *The principal congruence subgroup $\Gamma(m)$ of level m is isomorphic to a subgroup of $\Gamma_0(m^2)$ of index $\varphi(m)$.*

Proof. Let $\psi : \Gamma(m) \to \Gamma_0(m^2)$ be defined by

$$\psi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} 0 & -1 \\ m & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1/m \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c/m \\ -bm & a \end{pmatrix}.$$

Obviously ψ is an injective homomorphism.

Let

$$G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \bmod m, c \equiv 0 \bmod m^2\right\} \subset \Gamma_0(m^2).$$

We shall see that Im $\psi = G$ and that $[\Gamma_0(m^2) : G] = \varphi(m)$, completing the proof. In fact for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \psi\left(\begin{pmatrix} d & -c/m \\ -bm & a \end{pmatrix}\right)$$

and obviously $\begin{pmatrix} d & -c/m \\ -bm & a \end{pmatrix} \in \Gamma(m)$, whence Im $\psi = G$.

Let $g : \Gamma_0(m^2) \to \mathbb{Z}_m^*$ be defined by

$$g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a \bmod m.$$

Since $ad-bc = 1$ and $bc \equiv 0 \bmod m^2$, we have $(a, m^2) = 1$, whence $(a, m) = 1$. Therefore g is well-defined. Also, g is an homomorphism. In fact

$$\begin{aligned} g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) &= g\left(\begin{pmatrix} aa'+bc' & * \\ * & * \end{pmatrix}\right) \\ &= aa' \bmod m \\ &= g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot g\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right). \end{aligned}$$

Clearly $\ker g = G$, whence

$$\frac{\Gamma_0(m^2)}{\ker g} \simeq \mathbb{Z}_m^*$$

and therefore $[\Gamma_0(m^2) : G] = \varphi(m)$. □

Remark. Since $\varphi(2) = 1$, by the above proposition, $\Gamma(2)$ is isomorphic to a subgroup of $\Gamma_0(4)$ of index 1, namely $\Gamma(2) \simeq \Gamma_0(4)$.

Example 1. By the preceding proposition we have that $\Gamma(3)$ is isomorphic to a subgroup G of $\Gamma_0(9)$ of index 2. Let $\psi : \Gamma(3) \to G$ be such identification. If $V_1, \ldots, V_k$ span $\Gamma(3)$ then $\psi(V_1), \ldots, \psi(V_k)$ are a set of generators for G. Further, if $W \in \Gamma_0(9) - G$, then $\psi(V_1), \ldots, \psi(V_k), W\psi(V_1), \ldots, W\psi(V_k)$ are a set of generators for $\Gamma_0(9)$. As we shall see in the next chapter, this example has an unexpected arithmetical application.

We can also construct a fundamental domain for $\Gamma_0(9)$. We have (see [24]) that

$$\begin{cases} T^{-j}S & \text{for } j = 0, 1, \ldots, p^a - 1 \\ ST^{-jp}S & \text{for } j = 0, 1, \ldots, p^{a-1} - 1 \end{cases}$$

is a complete set of representatives of the cosets of $\Gamma_0(p^a)$ in Γ. Hence a fundamental domain for $\Gamma_0(9)$, as represented in Fig. 4.2, is

$$F' = \left(\bigcup_{j=0}^{8} ST^j F\right) \bigcup \left(\bigcup_{j=0}^{2} ST^{jp} SF\right)$$

where F is a fundamental domain for Γ (in Fig. 4.2 we take the fundamental domain F represented in Fig 4.1).

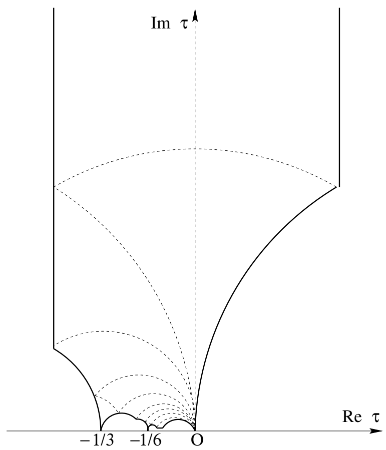

Fig. 4.2 A fundamental domain for $\Gamma_0(9)$

Chapter 5

Arithmetical applications

5.1 Introduction

Let $\sigma_m(n)$ denote the sum of the m-th powers of the positive divisors of n, and let $\sigma_m(0) = \frac{1}{2}\zeta(-m)$ where $\zeta(s)$ is the Riemann zeta-function.

In this chapter, using the theory of modular forms, we prove seven identities of the following type:

$$\sum_{k=0}^{[n/m]} \sigma_r(k)\sigma_s(n-mk) = P\sigma_{r+s+1}(n) + Qn\sigma_{r+s-1}(n) \tag{5.1}$$

which hold for every n satisfying suitable congruences, for suitable integers $m \geq 2$ and $r, s = 1$ or 3, and for rationals P and Q (Theorem 12). We also prove a further identity similar to (5.1) but of a slightly different kind, namely

$$\sum_{\substack{k=0 \\ k\equiv 1 \bmod 3}}^{n} \sigma_1(k)\sigma_1(n-k) = \frac{1}{9}\sigma_3(n) \qquad \text{for every } n \equiv 2 \bmod 3.$$

In a celebrated paper [37], Ramanujan, using elementary arguments, proved nine identities of the type (5.1) with $m = 1$. Ramanujan's nine identities can be also obtained in a natural way from the theory of modular forms for the full modular group (see [43]). Also a short elementary proof of Ramanujan's identities is due to Skoruppa [47].

We remark that one of the formulae we prove in Theorem 12, namely (5.10) below, is explicitly mentioned by Ramanujan himself in [37]. Unfortunately, he never provided either of the two proofs he announced. The first proof of the formula (5.10) below was given by Masser (see [5]) seventy years later. As far as we know, the other formulae proved in Theorem 12 appear to be new.

In Theorem 11 we also provide, via modular forms, a formula for the case $r = s = 1$ and any m, which contains an error term. When the error term vanishes this formula yields special cases of (5.1), i.e., the identities (5.8), (5.11), (5.12), (5.13) and (5.14) below.

We also give alternative proofs of the five identities (5.8)–(5.12). These proofs are based on certain formulae of Ramanujan, involving elliptic integrals of the first kind, contained in his Notebooks [38]. This alternative method is likely to correspond to one of the proofs that Ramanujan had in mind for the identity (5.10).

I am pleased to thank Don Zagier for his helpful and illuminating comments, and in particular for suggesting the proof of Theorem 11. I am also indebted to Umberto Zannier for pointing out to me the interpretation of the identities of Ramanujan's type in terms of modular forms, as well as for his constant encouragement and for several helpful suggestions.

I talked about these topics in a conference at Eger, Hungary, in 1996, and most of the material contained in this chapter can be found in my paper [35].

5.2 Notation and definitions

Let $F(a,b;c;x) = {}_2F_1(a,b;c;x)$ denote the Gauss hypergeometric series:

$$F(a,b;c;x) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{x^k}{k!},$$

where $c \neq 0, -1, -2, \dots$ and the Pochhammer symbols $(a)_k, (b)_k, (c)_k$ are defined by

$$(a)_0 = 1, \quad (a)_k = a(a+1)(a+2)\cdots(a+k-1) \quad \text{for } k = 1, 2, 3, \dots.$$

As is well-known, for $a = b = \frac{1}{2}$, $c = 1$ and $0 < x < 1$, the function $F(\frac{1}{2}, \frac{1}{2}; 1; x)$ is related to the complete elliptic integral of the first kind.

In accordance with Ramanujan's notation (see [4] and [38]), let, for $0 < x < 1$,

$$y = \pi \frac{F(\frac{1}{2}, \frac{1}{2}; 1; 1-x)}{F(\frac{1}{2}, \frac{1}{2}; 1; x)} \tag{5.2}$$

and

$$z = F(\tfrac{1}{2}, \tfrac{1}{2}; 1; x). \tag{5.3}$$

5.3 Main results

We begin this section with the following theorem:

Theorem 11 *Let m be a positive integer and define $\beta(m) = m^2 \prod_{p|m}(1 + p^{-2})$. For every positive integer n with $(m, n) = 1$ and for an arbitrary $\epsilon > 0$, we have*

$$\sum_{k=0}^{[n/m]} \sigma_1(k)\sigma_1(n-mk) = \frac{5}{12\beta(m)}\sigma_3(n) - \frac{1}{4m}n\sigma_1(n) + O\left(n^{\frac{3}{2}+\epsilon}\right).$$

Proof. As we saw in the preceding chapter, $G_m(\tau) = E_2(\tau) - mE_{2,m}(\tau)$ is a modular form of weight 2 for $\Gamma_0(m)$. Hence the function

$$F_m(\tau) := (G_m(\tau))^2 - E_4(\tau) - m^2 E_{4,m}(\tau)$$

is a modular form of weight 4 for $\Gamma_0(m)$. Combining the Fourier expansions of E_2 and E_4 with the first of Ramanujan's nine identities [37]:

$$\sum_{k=0}^{n} \sigma_1(k)\sigma_1(n-k) = \frac{5}{12}\sigma_3(n) - \frac{1}{2}n\sigma_1(n), \tag{5.4}$$

we find that the n-th Fourier coefficient of $\frac{-1}{1152m}F_m(\tau)$ is

$$c(n) = \frac{n}{4m}\sigma_1(n) + \frac{n}{4}\sigma_1^*\left(\frac{n}{m}\right) + \sum_{0\le k\le n/m} \sigma_1(k)\sigma_1(n-mk),$$

where

$$\sigma_1^*\left(\frac{n}{m}\right) := \begin{cases} \sigma_1\left(\frac{n}{m}\right) & \text{for } m|n \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $c(n)$ is defined also for $(m,n) \neq 1$.

In a similar manner one can find the asymptotic formula for $F_m(a/c + \varepsilon)$. For $(a,c) = 1$, we have $E_{4,r}(a/c) = E_{4,r}(1/c)$ and $F_m(a/c) = F_m(1/c)$. This allow us to simplify the study of the behaviour at the cusps in a sense that will be clear below. Now we shall prove that, for $r|m$ and $\alpha_m(r) := r^2 \prod_{p|(r,m/r)}(1-p^{-2})$, the function

$$F_{0,m}(\tau) := F_m(\tau) + \frac{2m}{\beta(m)} \sum_{r|m} \alpha_m(r) E_{4,r}(\tau) = \sum_{n=0}^{\infty} c_{0,m}(n) q^n \tag{5.5}$$

is a cusp form for $\Gamma_0(m)$. This can be done by looking at one prime number at a time. Assuming $m = p^\mu$ one has

$$F_{p^\mu}(\infty) = -2p^\mu, \qquad F_{p^\mu}\left(-\frac{1}{kp}\right) = -2p^{2+2v_p(k)-\mu}, \qquad F_{p^\mu}(0) = -2p^{-\mu},$$

$$E_{4,p^i}(\infty) = 1, \qquad E_{4,p^i}\left(-\frac{1}{kp}\right) = p^{4\min\{0, v_p(k)-i+1\}}, \qquad E_{4,p^i}(0) = p^{-4i},$$

where $v_p(k)$ is the exponent of the prime p in the factorization of k. As a set of representatives of the cusps for $\Gamma_0(m)$ we can take the cusps ∞, 0, and $-1/kp$ for $k = 1, 2, \ldots, p^{\mu-1} - 1$ (see [24, p. 107–108]). Therefore $F_{0,p^\mu}(\tau) = F_{p^\mu}(\tau) + \sum_{i=0}^{\mu} x_i E_{4,p^i}(\tau)$ is a cusp form if it vanishes at the cusps ∞, 0, and $-1/kp$ for $k = 1, 2, \ldots, p^{\mu-1} - 1$. Notice that there are only $\mu - 1$ distinct conditions at the cusps $-1/kp$, since for $(h', p^\mu) = (k', p^\mu)$ the condition at $-1/h'p$ is the same as the condition at $-1/k'p$. Thus one gets the following linear system of $\mu + 1$ equations in the $\mu + 1$ unknowns $x_0, x_1, \ldots, x_\mu$:

$$\begin{cases} x_0 + p^{-4}x_1 + p^{-8}x_2 + \ldots + p^{-4\mu+4}x_{\mu-1} + p^{-4\mu}x_\mu = 2p^{-\mu} \\ x_0 + x_1 + p^{-4}x_2 + \ldots + p^{-4\mu+8}x_{\mu-1} + p^{-4\mu+4}x_\mu = 2p^{-\mu+2} \\ \vdots \qquad \ldots\ldots \qquad \vdots \\ x_0 + x_1 + x_2 + \ldots + x_{\mu-1} + p^{-4}x_\mu = 2p^{\mu-2} \\ x_0 + x_1 + x_2 + \ldots + x_{\mu-1} + x_\mu = 2p^\mu, \end{cases}$$

whose solution is

$$x_0 = \frac{2}{p^\mu + p^{\mu-2}}, \quad x_\mu = \frac{2p^{\mu+2}}{p^2+1},$$

and for $i = 1, \dots, \mu - 1$

$$x_i = 2\frac{p^{2i} - p^{2i-2}}{p^\mu + p^{\mu-2}}.$$

Denoting $u_{p^i} = x_i$, we may express the above solution as

$$u_r = \frac{2p^\mu}{\beta(p^\mu)}\alpha_{p^\mu}(r) \quad \text{for each } r|p^\mu. \tag{5.6}$$

In the general case, for an arbitrary positive integer $m = q_1^{\mu_1} \cdots q_h^{\mu_h}$ with primes $q_1, \dots, q_h$ and positive integers $\mu_1, \dots, \mu_h$, one gets a similar system of $d(m)$ (the number of positive divisors of m) linear equations in the $d(m)$ unknowns u_r for $r|m$. This is done by imposing that $F_{0,m}(\tau) = F_m(\tau) + \sum_{r|m} u_r E_{4,r}(\tau)$ vanishes at $1/n$ for every $n|m$. One has the system

$$\sum_{r|m} \frac{(r,n)^4}{r^4} u_r = 2\frac{n^2}{m} \qquad \text{for each } n|m,$$

whose solution is

$$u_r = \frac{2m}{\beta(m)}\alpha_m(r),$$

as is easily seen using (5.6) for each $q_j^{\mu_j}$ $(j = 1, \dots, h)$. This proves (5.5).

Hence the n-th Fourier coefficient of $\frac{-1}{1152m}F_{0,m}$ is bounded by $O(n^{\frac{3}{2}+\epsilon})$ (see for example [42]), i.e.,

$$-\frac{1}{1152m}c_{0,m}(n) = c(n) - \frac{5}{12\beta(m)} \sum_{r|(m,n)} \alpha_m(r)\sigma_3\left(\frac{n}{r}\right) = O\left(n^{\frac{3}{2}+\epsilon}\right)$$

for all n. For $(m,n) = 1$ this is our theorem. □

In some cases the error term vanishes, and this yields special cases of identities (5.1). In the following theorem we obtain eight identities.

Theorem 12 *If* $n \equiv 2 \bmod 3$, *then*

$$\sum_{\substack{k=0 \\ k \equiv 1 \bmod 3}}^{n} \sigma_1(k)\sigma_1(n-k) = \frac{1}{9}\sigma_3(n). \tag{5.7}$$

If n is a positive odd integer, then

$$\sum_{k=0}^{[n/2]} \sigma_1(k)\sigma_1(n-2k) = \frac{1}{12}\sigma_3(n) - \frac{1}{8}n\sigma_1(n), \tag{5.8}$$

$$\sum_{k=0}^{[n/2]} \sigma_1(k)\sigma_3(n-2k) = \frac{1}{48}\sigma_5(n) - \frac{1}{16}n\sigma_3(n), \tag{5.9}$$

$$\sum_{k=0}^{[n/2]} \sigma_3(k)\sigma_1(n-2k) = \frac{1}{240}\sigma_5(n), \tag{5.10}$$

$$\sum_{k=0}^{[n/4]} \sigma_1(k)\sigma_1(n-4k) = \frac{1}{48}\sigma_3(n) - \frac{1}{16}n\sigma_1(n). \tag{5.11}$$

If $n \not\equiv 0 \bmod 3$, then

$$\sum_{k=0}^{[n/3]} \sigma_1(k)\sigma_1(n-3k) = \frac{1}{24}\sigma_3(n) - \frac{1}{12}n\sigma_1(n). \tag{5.12}$$

If $n \equiv 8 \bmod 16$ and $n \not\equiv 0 \bmod 5$, then

$$\sum_{k=0}^{[n/5]} \sigma_1(k)\sigma_1(n-5k) = \frac{5}{312}\sigma_3(n) - \frac{1}{20}n\sigma_1(n). \tag{5.13}$$

If n satisfies one of the following conditions:

(i) $n \equiv 2 \bmod 3$;
(ii) $n \equiv 1 \bmod 3$ *and there exists a prime* $p \equiv 2 \bmod 3$ *such that* $p|n$ *but* $p^2 \not| n$;

then

$$\sum_{k=0}^{[n/9]} \sigma_1(k)\sigma_1(n-9k) = \frac{1}{216}\sigma_3(n) - \frac{1}{36}n\sigma_1(n). \tag{5.14}$$

Proof. Let $f(\tau)$ be a non-vanishing modular form of weight $2k$ for $\Gamma(m)$. We consider the Riemann surface $\mathcal{S}$ associated with $\Gamma(m)$. We associate with f the differential $\omega = f(\tau)(d\tau)^k$ of weight k on $\mathbb{H}$. Then ω corresponds to a differential ω^* of weight k on $\mathcal{S}$ (see also [46]). We want to compare the order $n_p(f)$ of f at the point p with the order $\nu_{p^*}(\omega^*)$ of ω^* at the point p^* of $\mathcal{S}$ corresponding to p. This appears in [46, Prop. 3.7, p. 28]. We distinguish three cases, according to the nature of p:

(i) p is a *regular point*, i.e., it is not a fixed point of some non-identical transformation in $\Gamma(m)$. In this case $n_p(f) = \nu_{p^*}(\omega^*)$;

(ii) p is an *elliptic fixed point* of period $e_p \in \{2, 3\}$ (the points in this set are Γ-equivalent either to $i = \sqrt{-1}$ or to $\rho = e^{2\pi i/3}$). Now $n_p(f) = e_p \nu_{p^*}(\omega^*) + k(e_p - 1)$;

(iii) p is either ∞ or a finite parabolic point. We have $n_p(f) = \nu_{p^*}(\omega^*) + k$.

We let $F \subset \mathbb{H} \cup \{\text{cusps}\}$ be a system of representatives for the action of $\Gamma(m)$, so the map $p \mapsto p^*$ is 1-1. Also, let F_1, F_2 and F_3 be the subsets of F made up of the points satisfying the above properties (i), (ii) and (iii) respectively.

We now apply the Riemann-Roch theorem to ω^*; this implies that

$$\sum_{p^* \in S} \nu_{p^*}(\omega^*) = 2k(g-1),$$

where g is the genus of $\mathcal{S}$. We get

$$\sum_{p \in F_1} n_p(f) + \sum_{p \in F_2} \frac{1}{e_p} n_p(f) + \sum_{p \in F_3} n_p(f) = k \left(2g - 2 + \sum_{p \in F_2} (1 - 1/e_p) + \#F_3 \right),$$

where $\#F_3$ denotes the cardinality of F_3.

We point out that, in each concrete case, the above formula may also be obtained by complex integration on the boundary of a fundamental domain for $\Gamma(m)$, similarly to [43, Ch. VII, Th. 3, p. 139].

Let $p \in F_1 \cup F_3$. Since $n_{p'}(f) \geq 0$ for every $p' \in F$, we have

$$\begin{aligned} n_p(f) &\leq \left(\sum_{p' \in F_1} n_{p'}(f) + \sum_{p' \in F_2} \frac{1}{e_{p'}} n_{p'}(f) + \sum_{p' \in F_3} n_{p'}(f) \right) \\ &\leq k \left(2g - 2 + \sum_{p' \in F_2} (1 - 1/e_{p'}) + \#F_3 \right). \end{aligned}$$

For $m \geq 2$ we also have, as is easy to see, $\#F_2 = 0$ ([44, Prop. 1.39, p. 22]) and $\#F_3 \leq m^2$, whence

$$n_p(f) \leq k(2g - 2 + m^2).$$

As an application of this formula, we now prove (5.7).

For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ denote $A(\tau) = \dfrac{a\tau + b}{c\tau + d}$ and $J_A(\tau) = c\tau + d$. Let $m \geq 2$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(m)$. Define $T_0, T_1, \ldots, T_{m-1}$ by

$$T_j = \begin{pmatrix} a + jc & (b + jd - ja - j^2 c)/m \\ mc & d - jc \end{pmatrix}.$$

Since $a \equiv d \bmod m$ and $b \equiv c \equiv 0 \bmod m$, $(b + jd - ja - j^2 c)/m$ is an integer, and it is easy to show that $T_j \in \Gamma$. Moreover

$$\frac{A(\tau) + j}{m} = T_j \left(\frac{\tau + j}{m} \right).$$

For $2k = 2, 4$ and $j = 0, 1, \ldots, m - 1$, let

$$E^*_{2k,j}(\tau) = E_{2k} \left(\frac{\tau + j}{m} \right).$$

If $2k = 4$ we have

$$\begin{aligned} E^*_{4,j}\big(A(\tau)\big) &= E_4\left(\frac{A(\tau)+j}{m}\right) \\ &= E_4\left(T_j\left(\frac{\tau+j}{m}\right)\right) \\ &= \left(J_{T_j}\left(\frac{\tau+j}{m}\right)\right)^4 \cdot E_4\left(\frac{\tau+j}{m}\right) \\ &= J_A(\tau)^4 E^*_{4,j}(\tau), \end{aligned}$$

and it is straightforward to check that $E^*_{4,j}$ is holomorphic at every cusp. Hence $E^*_{4,j}$ is a modular form of weight 4 for $\Gamma(m)$.

If $2k = 2$, we have

$$\begin{aligned} E^*_{2,j}\big(A(\tau)\big) &= E_2\left(T_j\left(\frac{\tau+j}{m}\right)\right) \\ &= \frac{6}{\pi i} mc J_{T_j}\left(\frac{\tau+j}{m}\right) + \left(J_{T_j}\left(\frac{\tau+j}{m}\right)\right)^2 E^*_{2,j}(\tau) \\ &= \frac{6}{\pi i} mc J_A(\tau) + J_A(\tau)^2 E^*_{2,j}(\tau). \end{aligned}$$

If $a = (a_0, \ldots, a_{m-1}) \in \mathbb{C}^m$ is such that $\sum a_j = 0$, one easily gets that the function E_a defined by

$$E_a(\tau) = \sum_{j=0}^{m-1} a_j E^*_{2,j}(\tau)$$

is a modular form of weight 2 for $\Gamma(m)$.

For $1 \le t \le m-1$ let

$$E^{(m)}_{2k,t}(\tau) = \sum_{\substack{n>0 \\ n \equiv t \bmod m}} \sigma_{2k-1}(n) q_m^n \qquad (2k = 2 \text{ or } 4).$$

Denoting $c_2 = -1/24$, $c_4 = 1/240$, we seek a vector $a = (a_0, \ldots, a_{m-1}) \in \mathbb{C}^m$ such that

$$E^{(m)}_{2k,t}(\tau) = c_{2k} \sum_{j=0}^{m-1} a_j E^*_{2k,j}(\tau).$$

This immediately leads to the following linear system:

$$\begin{cases} a_0 & +a_1 & +a_2 & +\dots & +a_{m-1} & =0 \\ a_0 & +\omega a_1 & +\omega^2 a_2 & +\dots & +\omega^{m-1} a_{m-1} & =0 \\ \dots & \dots\dots\dots & \dots\dots\dots & \dots\dots & \dots\dots\dots\dots & \dots \\ a_0 & +\omega^t a_1 & +\omega^{2t} a_2 & +\dots & +\omega^{(m-1)t} a_{m-1} & =1 \\ \dots & \dots\dots\dots & \dots\dots\dots & \dots\dots & \dots\dots\dots\dots & \dots \\ a_0 & +\omega^{m-1} a_1 & +\omega^{2(m-1)} a_2 & +\dots & +\omega^{(m-1)^2} a_{m-1} & =0, \end{cases}$$

where $\omega = e^{2\pi i/m}$. The matrix Ω of the coefficients is a Vandermonde matrix, whence

$$\det \Omega = \prod_{0 \le j < i \le m-1} \left(\omega^i - \omega^j \right) \neq 0,$$

and the linear system has a unique solution $a = (a_0, \dots, a_{m-1})$. Hence $E^{(m)}_{2k,t}(\tau)$ is a modular form of weight $2k$ for $\Gamma(m)$. Let

$$f(\tau) := \left(E^{(3)}_{2,1}(\tau) \right)^2 - \frac{1}{9} E^{(3)}_{4,2}(\tau).$$

By the preceding argument f is a modular form of weight 4 for $\Gamma(3)$. The genus of the Riemann surface associated to $\Gamma(3)$ is 0 (see [20, Theorem 8, p. 15]), hence for $f \not\equiv 0$ and for every $p \in \mathbb{H} \cup \{\text{cusps}\}$, we have that $n_p(f) \le 14$. On the other hand, the formula (5.7) holds for $n = 2, 5, 8, 11, 14$, i.e., $n_\infty(f) > 14$. Therefore $f(\tau) \equiv 0$, i.e., the identity (5.7).

To prove (5.8), (5.11) and (5.12) we consider $F_{0,m}(\tau)$ respectively with $m = 2, 4$ and 3. As we saw in the preceding theorem, $F_{0,m}(\tau)$ is a cusp form of weight 4 for $\Gamma_0(m)$. Further for every positive integer k and $m \ge 2$ (see [8]),

$$\begin{aligned} \dim S_{2k}(\Gamma_0(m)) &= \frac{2k-1}{12} m \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 + \frac{1}{p} \right) + \dim M_{2-2k}(\Gamma_0(m)) \\ &\quad - \frac{1}{2} \sum_{c \mid m} \varphi\left((c, \frac{m}{c}) \right) + \frac{(-1)^k}{4} \psi(m) + \gamma(k) \vartheta(m), \end{aligned}$$

where φ is the Euler totient function and

$$\vartheta(m) = \begin{cases} 0 & \text{for } 9 \mid m \\ \displaystyle\prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{for } 9 \nmid m, \end{cases}$$

$$\psi(m) = \begin{cases} 0 & \text{for } 4 \mid m \\ \displaystyle\prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 + \left(\frac{-4}{p}\right)\right) & \text{for } 4 \nmid m, \end{cases}$$

$$\gamma(k) = \begin{cases} 0 & \text{for } k \equiv 2 \bmod 3 \\ -\frac{1}{3} & \text{for } k \equiv 1 \bmod 3 \\ \frac{1}{3} & \text{for } k \equiv 0 \bmod 3, \end{cases}$$

where $(\frac{\cdot}{p})$ for odd primes is the Legendre symbol and where $(\frac{-3}{2}) = -1$ and $(\frac{-4}{2}) = 0$.

In particular $\dim S_4(\Gamma_0(m)) = 0$ for $m = 2, 3, 4$. Hence $F_{0,m}(\tau) \equiv 0$, respectively proving (5.8), (5.12) and (5.11). Since $\dim S_6(\Gamma_0(2)) = 0$, one can prove the identities (5.9) and (5.10) in a similar manner.

Let $F_{0,5}(\tau) = \sum_{n=1}^{\infty} c_{0,5}(n) q^n$. In this case $\dim S_4(\Gamma_0(5)) = 1$. In fact it is spanned by $(\eta(\tau)\eta(5\tau))^4$, where $\eta(\tau) = e^{\pi i \tau/12} \prod_{n=1}^{\infty}(1 - q^n)$ is the Dedekind eta function [24, Prop. 19, p. 130]. So $F_{0,5}(\tau)$ is a Hecke eigenform. In particular for every m, n with $(m, n) = 1$, it is $c_{0,5}(m) c_{0,5}(n) = c_{0,5}(mn)$. Since $c_{0,5}(8) = 0$, we have $c_{0,5}(8n) = 0$, for every integer n with $(n, 8) = 1$, and this proves (5.13).

Since $\dim S_4(\Gamma_0(9)) = 1$ we have that $F_{0,9}(\tau) = \sum_{n=1}^{\infty} c_{0,9}(n) q^n$ is a Hecke eigenform for $\Gamma_0(9)$. Consider now $\eta^*(\tau) = \eta(3\tau)^8 = q \prod_{n=1}^{\infty}(1 - q^{3n})^8$. We now prove that η^* is a cusp form of weight 4 for $\Gamma_0(9)$, hence a constant multiple of $F_{0,9}$.

Recall the Dedekind's functional equation. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $c > 0$ we have [2, Ch. 3, Th. 3.4, p. 52]

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)=\varepsilon(a,b,c,d)\{-i(c\tau+d)\}^{1/2}\eta(\tau)$$

where we take the branch of $\{-i(c\tau+d)\}^{1/2}$ which has value 1 when $c\tau+d=i$ and

$$\varepsilon(a,b,c,d)=\exp\left\{\pi i\left(\frac{a+d}{12c}+s(-d,c)\right)\right\}$$

where

$$s(h,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right).$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma_0(9)$ we have

$$\eta^*\left(\frac{a\tau+b}{c\tau+d}\right)=\eta\left(3\frac{a\tau+b}{c\tau+d}\right)^8=\eta\left(\frac{a(3\tau)+b}{\frac{c}{3}(3\tau)+d}\right)^8.$$

Since $\begin{pmatrix} a & 3b \\ c/3 & d \end{pmatrix}\in\Gamma_0(3)\subset\Gamma$, we have

$$\begin{aligned}\eta^*\left(\frac{a\tau+b}{c\tau+d}\right) &= \varepsilon\left(a,3b,\frac{c}{3},d\right)^8\left(\frac{c}{3}(3\tau)+d\right)^4\eta(3\tau)^8\\ &= \varepsilon\left(a,3b,\frac{c}{3},d\right)^8(c\tau+d)^4\eta(3\tau)^8.\end{aligned}$$

In order to verify the condition (4.1), we must check that $\varepsilon(a,3b,c/3,d)^8=1$ for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma_0(9)$, and clearly it suffices to check it for a set of generators of $\Gamma_0(9)$.

In the preceding chapter, Example 1, we saw how to find a set of generators of $\Gamma_0(9)$ from a set of generators of $\Gamma(3)$. As a set of generators of $\Gamma(3)$ we take [17]

$$V_1=\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, V_2=\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}, V_3=\begin{pmatrix} -2 & 3 \\ -3 & 4 \end{pmatrix}.$$

Let ψ be as in Example 1. We have that

$$\psi(V_1) = \begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}, \quad \psi(V_2) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \psi(V_3) = \begin{pmatrix} 4 & 1 \\ -9 & -2 \end{pmatrix}$$

span a congruence subgroup $G \subseteq \Gamma_1(9)$. Notice that $W = \begin{pmatrix} 2 & 1 \\ 9 & 5 \end{pmatrix} \in \Gamma_0(9) - G$, hence $\psi(V_1), \dots, \psi(V_3), W\psi(V_1), \dots, W\psi(V_3)$, i.e.,

$$\begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 1 \\ -9 & -2 \end{pmatrix},$$

$$\begin{pmatrix} -7 & 1 \\ -36 & 5 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ -81 & -1 \end{pmatrix}$$

are a set of generators for $\Gamma_0(9)$. With a bit of computation we can finally check that η^* verifies (4.1).

Since $\eta(\tau)^{24} = \Delta(\tau)$ is a cusp form for the full modular group, we have that η^* verifies (4.2) and vanishes at every cusp. Since $\eta(3\tau)^8 \in S_4(\Gamma_0(9))$, we have $c_{0,9}(n) = 0$ for $n \equiv 2 \bmod 3$ and, by multiplicativity, this immediately implies (5.14). □

In [32] one can find further interesting discussions about cusp forms of the type

$$f(\tau) = \prod_{j=1}^{s} \eta(t_j\tau)_j^r$$

where $t_1, t_2, \dots, t_s$ are positive integers and $r_1, r_2, \dots, r_s$ are arbitrary integers.

5.4 Concluding remarks

Five of the preceding eight identities, i.e., (5.8)–(5.12), can be also proved by using certain formulae from Ramanujan's Notebooks. In this context, for $0 < x < 1$ let $w = e^{-y}$, where y is defined by (5.2), and let z be defined by (5.3). Let

$$L(w) = 1 - 24\sum_{k=1}^{\infty} \frac{kw^k}{1-w^k}, \quad M(w) = 1 + 240\sum_{k=1}^{\infty} \frac{k^3w^k}{1-w^k},$$

$$N(w) = 1 - 504 \sum_{k=1}^{\infty} \frac{k^5 w^k}{1 - w^k}.$$

Since

$$\sum_{k=1}^{\infty} \frac{k^\alpha w^k}{1 - w^k} = \sum_{k=1}^{\infty} \sum_{h=1}^{\infty} k^\alpha w^{hk} = \sum_{m=1}^{\infty} w^m \sum_{hk=m} k^\alpha = \sum_{m=1}^{\infty} \sigma_\alpha(m) w^m,$$

we have

$$L(w) = -24 \sum_{k=0}^{\infty} \sigma_1(k) w^k, \quad M(w) = 240 \sum_{k=0}^{\infty} \sigma_3(k) w^k,$$

$$N(w) = -504 \sum_{k=0}^{\infty} \sigma_5(k) w^k.$$

Recall that (see [37])

$$\sum_{k=0}^{n} \sigma_1(k) \sigma_3(n-k) = \frac{7}{80} \sigma_5(n) - \frac{1}{8} n \sigma_3(n). \tag{5.15}$$

Let n be a positive odd integer. For $0 < w < 1$, by [4, Ch. 17, Entry 13, p. 126–127] one can easily deduce

$$\left(2L(w^2) - L(w)\right)^2 = \frac{4}{5} M(w^2) + \frac{1}{5} M(w),$$

$$M(w) \left(2L(w^2) - L(w)\right) = \frac{32}{21} N(w^2) - \frac{11}{21} N(w)$$

and

$$M(w^2) \left(2L(w^2) - L(w)\right) = \frac{22}{21} N(w^2) - \frac{1}{21} N(w).$$

Equating coefficients of w^n and then using (5.4) and (5.15), we obtain (5.8), (5.9) and (5.10).

In a similar manner the identities (5.11) and (5.12) can be obtained using [4, Example (ii) and (iii), p. 139] and [4, Ch. 21, Entry 3 (i), p. 460] respectively.

One can also prove some other formulae, related to the derivatives of suitable modular functions, similar to certain formulae of Lahiri [26]. For instance, it is easy to show that if n is a positive odd integer, then

$$\sum_{k=0}^{[n/2]} k\sigma_1(k)\sigma_1(n-2k) = \frac{1}{48}n\sigma_3(n) - \frac{1}{48}n^2\sigma_1(n).$$

It is known that for $m = 1$ there are only nine possible identities (see [18], [19], [29]).

An interesting open question is to prove (or disprove) that the identities we found in Theorem 12 are the only identities with $m > 1$. Explicit computation shows that for $r = s = 1$ and $m < 100$ there is no new identity, and it is likely that Theorem 12 is exhaustive.

Bibliography

[1] H. L. ABBOTT, *On sum-free sequences*, Acta Arith. **48** (1987), 93–96.

[2] T. M. APOSTOL, Modular Functions and Dirichlet Series in Number Theory, GTM 41, Springer-Verlag 1976.

[3] R. C. BAKER, G. HARMAN, *The difference between consecutive primes*, Proc. London Math. Soc. **72** (1996), 261–280.

[4] B. C. BERNDT, Ramanujan's notebooks part III, Springer-Verlag 1991.

[5] B. C. BERNDT, R. J. EVANS, *Chapter 15 of Ramanujan's Second Notebook: Part 2, Modular forms*, Acta Arith. **47** (1986), 123–142.

[6] N. BOSTON, M. L. GREENWOOD, *Quadratics Representing Primes*, Am. Math. Monthly **102** (1995), 595–599.

[7] H. CARTAN, Théorie élémentaire des fonctions analitiques d'une ou plusieures variables complexes, 4^{th} edition, Hermann Paris 1961.

[8] H. COHEN, J. OESTERLÉ, *Dimensions des espaces de formes modulaires*, Lecture Notes in Mathematics **627** (1976), Springer-Verlag, 69–78.

[9] J-M. DESHOUILLERS, P. ERDŐS, G. MELFI, *On a question about sum-free sequences*, to appear in Discrete Mathematics.

[10] J-M. DESHOUILLERS, G. FREIMAN, *On an additive problem of Erdős and Straus. I*, Isr. J. Math. **92** (1995), 33-43.

[11] J-M. DESHOUILLERS, G. FREIMAN, *On an additive problem of Erdős and Straus. II*, to appear.

[12] H. Dubner, W. Keller , *New Fibonacci and Lucas primes*, Abstr. Papers pres. to the AMS **99** (1995), 267.

[13] P. Erdős, *On a Diophantine equation*, Mat. Lapok **1** (1950), 192–210, Hungarian. Russian and English summaries.

[14] P. Erdős, *Some remarks on number theory, III.*, Mat. Lapok **13** (1962), 28–38.

[15] P. Erdős, *personal communication,* 1996 III 19.

[16] P. Erdős, *personal communication,* 1996 V 29.

[17] H. Frasch, *Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen*, Math. Ann. **108** (1933), 229–252.

[18] C. C. Grosjean. *An infinite set of recurrence formulae for the divisor sums, Part 1*, Bull. Soc. Math. Belgique **29** (1977), 3–49.

[19] C. C. Grosjean. *An infinite set of recurrence formulae for the divisor sums, Part 2*, Bull. Soc. Math. Belgique **29** (1977), 95–138.

[20] R. C. Gunning, Lectures on modular forms, Princeton University Press 1962.

[21] R. K. Guy, Unsolved Problems in Number Theory, 2^{nd} Edition, Springer-Verlag 1994.

[22] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 5^{th} edition, Clarendon Press Oxford 1980.

[23] M. Hausman, H. N. Shapiro, *On practical numbers*, Comm. Pure Appl. Math. **37** (1984), 705–713.

[24] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, 2^{nd} edition, GTM 97, Springer-Verlag 1993.

[25] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, John Wiley, New York 1974.

[26] D. B. Lahiri, *Some arithmetical identities for Ramanujan's and divisor functions*, Bull. Austral. Math. Soc. **1** (1969), 307–314.

[27] E. Levine, *An extremal result for sum-free sequences*, J. Number Theory **12** (1980), 251–257.

[28] E. Levine, J. O'Sullivan, *An upper estimate for the reciprocal sum of a sum-free sequence*, Acta Arith. **34** (1977) 9–24.

[29] J. Levitt, *On a problem of Ramanujan*, M. Phil. Thesis, University of Nottingham, 1978.

[30] M. Margenstern, *Results and conjectures about practical numbers*, C.R. Acad. Sc. Paris **299** (1984), 895–898.

[31] M. Margenstern, *Les nombres pratiques: théorie, observations et conjectures*, J. Number Theory **37** (1991), 1–36.

[32] Y. Martin, *Multiplicative η-quotients*, Trans. of the AMS **348** (1996), 4825–4856.

[33] G. Melfi, *On two conjectures about practical numbers*, J. Number Theory **56** (1996), 205–210.

[34] G. Melfi, *A survey on practical numbers*, Rend. Sem. Mat. Uni. Pol. Torino **53** (1995), 347–359.

[35] G. Melfi, *On some modular identities*, to appear in Proceedings of the Number Theory Conference of Eger 1996.

[36] G. Melfi, G. Morelli, *Alcune notevoli identità per le somme dei divisori di certi numeri*, Archimede **47** (1995), 20–23.

[37] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. **22** (1916), 159–184.

[38] S. Ramanujan, Notebooks (2 volumes), Tata Institute of Fundamental Research, Bombay 1957.

[39] P. Ribenboim, The Book of Prime Number Records, Springer-Verlag 1988.

[40] B. Richter, *Eine Abschätzung der Werte der Kreisteilungspolynome für reelles Argument*, J. Reine. Angew. Math. **267** (1974), 74–76.

[41] E. Saias, *Entiers à diviseurs denses 1*, Journal of Number Theory **62** (1997), 163–191.

[42] P. Sarnak, Some applications of modular forms, Cambridge University Press 1990.

[43] J. P. Serre, Cours d'arithmétique, 3^{rd} edition, Presses universitaires de France 1988.

[44] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton University Press 1971.

[45] W. Sierpiński, *Sur une propriété des nombres naturels*, Ann. Mat. Pura Appl. **39** (1955), 69–74.

[46] J. H. Silverman, Advanced topics in the Arithmetic of Elliptic Curves, GTM 151, Springer-Verlag 1994.

[47] N-P. Skoruppa, *A quick combinatorial proof of Eisenstein series identities*, J. Number Theory **43** (1993), 68–73.

[48] A. K. Srinivasan, *Practical numbers*, Curr. Sci. **6** (1948), 179–180.

[49] B. M. Stewart, *Sums of distinct divisors*, Amer. J. Math. **76** (1954), 779–785.

[50] G. Tenenbaum, *Sur un problème de crible et ses applications*, Ann. Sci. Ec. Norm. Sup. (4) **19** (1986), 1–30.

[51] G. Tenenbaum, *Sur un problème de crible et ses applications, 2. Corrigendum et étude du graphe divisoriel*, Ann. Sci. Ec. Norm. Sup. (4) **28** (1995), 115–127.

Index

Abbott, 52
additive number theory, 51
admissibility, 41, 45
admissible, 40–42, 44, 45
admissible sequence, 52, 61
arrangement, 40, 44, 45
asymptotic density, 53

Baker, 22
Bertrand's postulate, 24

Chebishev, 12
companion Lucas sequence, 26
congruence subgroup, 64, 67–70, 85
  generators of, 69, 70, 84, 85
  level of, 64, 69
  principal, 64, 69
cusp, 64–67, 76, 79, 81, 82, 85
cyclotomic, 40

Dedekind, 83
  eta-function, 83
  functional equation, 83
Deshouillers, 51–53, 56, 58
Diophantine equation, 49
Dubner, 13

Eisenstein series, 65
elliptic integral, 74
Erdős, 7, 11, 51–53, 56, 58, 61
Euler
  Euler-Mascheroni constant, 22
  totient function, 29, 38, 83

Fibonacci, 13, 27, 30
Fourier, 63, 75, 77
full modular group, 64
fundamental domain, 65, 66
fundamental Lucas sequence, 26

gap, 13, 22
Gauss hypergeometric series, 74
Goldbach, 5, 12, 18
Gronwall, 26

Hardy, 33, 34
Harman, 22
Hausman, 12, 13, 22
Hecke, 83
holomorphic, 63, 64

k-tuples
  5-tuples, 13, 36
Keller, 13

Lahiri, 86
Legendre, 83
Levine, 52
Littlewood, 33, 34

Lucas, 9, 13, 26, 27, 29, 30

Margenstern, 7, 12, 14, 15, 31, 33, 34
Masser, 74
modular, 6, 63–68, 73–75, 79, 81, 82, 85, 86
  coefficient of a modular form, 64, 65
  cusp form, 64, 65, 76, 82, 83, 85
  form, 6, 63–65, 67, 68, 73, 75, 76, 79, 81–83, 85
  function, 6, 63–65, 67, 68
  weight of a modular form, 75, 79, 81–83

O'Sullivan, 52
ordered set, 45

Pell, 13, 27, 30
Pochhammer, 74
practical, 5, 9, 11–15, 17–20, 22, 23, 25, 27–38, 41–49
  table of practical numbers, 31
prime, 34

Ramanujan, 6, 73–75, 85
Riemann Hypothesis, 22
Riemann surface, 79, 82
  genus, 79, 82
Riemann zeta-function, 58, 73
Riemann-Roch theorem, 79

Saias, 5, 12
Shapiro, 12, 13, 22
Sierpiński, 13
Skoruppa, 73
Srinivasan, 11
Stewart, 11, 13, 15, 18, 34, 38
structure, 18, 34, 35, 37, 38, 42, 44, 46–48
sum-free sequence, 6, 51–54, 56, 58–60
sum-of-divisors, 6, 63

Tenenbaum, 5, 12
Turán, 58
twin practical numbers, 33
twin primes, 33

Vandermonde, 82
Viola, 7

Zagier, 7, 74
Zannier, 7, 74