ACTA ARITHMETICA
LXXX.3 (1997)

On the divisors of $a^k + b^k$

by

Pieter Moree (Bonn)

1. Introduction. Let a and b be two fixed non-zero coprime integers. Consider the sequence $\{u_k\}_{k=1}^{\infty}$, where $u_k = a^k + b^k$. We say $n \geq 1$ is *good* if it divides u_k for some $k \geq 1$ and *bad* otherwise. In this paper we will characterize the odd good integers (Theorem 1) and use this to derive an asymptotic formula for $G(x)$, the number of good integers not exceeding x (Theorem 5). This result implies that *almost* all integers are bad. Several authors have studied good *primes* (see e.g. [1, 19, 21] and the references cited there). Some authors studied this problem in a different guise (see Section 2). In contrast little seems to be known about good *integers*, which are the main focus of this paper.

I would like to thank Patrick Solé for asking a question that motivated this research and for his interest in my attempts to solve it. His question, to characterize numbers occurring as divisors of $2^n + 1$, arose in joint work with Vera Pless and Z. Qian on $\mathbb{Z}_4$-linear codes [14]. Furthermore, I thank T. Kleinjung for some inspiring discussions and B. Z. Moroz and G. Niklasch for helpful comments.

2. Elementary observations. To avoid trivialities assume $\psi := a/b \neq \pm 1$. If n is good, it must be coprime with a and b. Furthermore, we have $\psi^c \equiv -1 \pmod{n}$ for some natural number c. (In symmetric design parlance, see e.g. [9, p. 147], ψ is said to be semiprimitive (mod n).) Unless stated otherwise we assume in the sequel that n is coprime with $2ab$ and that p does not divide $2ab$. (The letter p always denotes a prime.) The restriction to odd good numbers is made to avoid unwieldy technical complications. Only in the proof of Theorem 5 we will consider even good numbers (which only exist in case ab is odd). If n is good, then all its divisors must be good. In particular, if p^e, $e \geq 2$, is good, then p is good. This holds also in the other direction, since if $\psi^e \equiv -1 \pmod{p}$, then by induction and the binomial

1991 *Mathematics Subject Classification*: Primary 11B83; Secondary 11N25.

theorem we have $\psi^{ep^j} \equiv -1 \pmod{p^{1+j}}$, for every $j \geq 0$. Thus we have proved:

PROPOSITION 1. *The number $p^e, e \geq 2$, is good iff p is good.*

It follows that n is good iff the squarefree kernel of n is good. We will use several times the fact that for p odd the only solutions of $x^2 \equiv 1 \pmod{p^\nu}$ are $x \equiv \pm 1 \pmod{p^\nu}$ (this is so since $(\mathbb{Z}/p^\nu\mathbb{Z})^*$ is cyclic for odd p and $\nu \geq 1$ and hence cannot contain more than one subgroup of order 2). Let p^r be good. Not surprisingly, the smallest natural number e such that $\psi^e \equiv -1 \pmod{p^r}$ is related to $\mathrm{ord}_{p^r}(\psi)$.

PROPOSITION 2. *If p^r is good, then $\mathrm{ord}_{p^r}(\psi) = 2e$ where e is the smallest natural number such that $\psi^e \equiv -1 \pmod{p^r}$.*

Proof. Clearly $\mathrm{ord}_{p^r}(\psi) \mid 2e$. Now if $\mathrm{ord}_{p^r}(\psi)$ were a divisor of e, then it would follow that $\psi^e \equiv 1 \pmod{p^r}$. Thus $\mathrm{ord}_{p^r}(\psi) = 2c$ for some c dividing e. Since ψ^c is a solution of $x^2 \equiv 1 \pmod{p^r}$ and $\psi^c \not\equiv 1 \pmod{p^r}$, we must have $\psi^c \equiv -1 \pmod{p^r}$. It follows that $c = e$, by the minimality of e. ∎

So if p^r is good, then $\mathrm{ord}_{p^r}(\psi)$ is even. On the other hand, if $\mathrm{ord}_{p^r}(\psi)$ is even, then $\psi^{\mathrm{ord}_{p^r}(\psi)/2}$ is a solution $\not\equiv 1 \pmod{p^r}$ of $x^2 \equiv 1 \pmod{p^r}$ and thus p^r is good. Thus we have deduced:

PROPOSITION 3. *The prime power p^r is good iff $\mathrm{ord}_{p^r}(\psi)$ is even.*

Thus studying primes that are good is equivalent to studying primes for which $\mathrm{ord}_p(\psi)$ is even. Several authors have investigated the latter question. Sierpiński [17] seems to have been the first. Hasse [7] improved on Brauer [2], who improved on Sierpiński. Hasse, using the arithmetic of Kummer extensions, proved a weaker version of Theorem 2 below; he showed that the set C_0 has a Dirichlet density and computed it.

It is an observation going at least back to Gauss that the g-adic period of $1/b$ is equal to $\mathrm{ord}_b(g)$, the order of g in the multiplicative group of invertible residue classes modulo b. Krishnamurthy [8] conjectured that asymptotically one-third of the primes $p > 5$ have odd decimal period. Since a set of primes which has a Dirichlet density does not always have a natural density, Hasse's result is not strong enough to imply Krishnamurty's conjecture. Odoni [12] established this conjecture in a much more general form. It turns out that the set of primes under consideration is a union of an infinite number of Frobenian sets, i.e., sets which differ finitely from some complete set of unramified primes having prescribed Frobenius conjugacy class in some fixed Galois extension of the rationals. To find a good remainder term, one thus needs to find a uniform version of Chebotarev's theorem. To this end Odoni used results obtained by Lagarias and Odlyzko. The error term obtained by Odoni was improved by Wiertelak in [18] and subsequently in [20], who used a uniform version of the Prime Ideal Theorem instead of Chebotarev's theorem.

The next proposition relates ord_{p^r} to ord_p.

Proposition 4. *Let p^r be an odd prime power. Then $\mathrm{ord}_{p^r}(\psi) = \mathrm{ord}_p(\psi)p^j$ for some $j \geq 0$.*

Proof. We have $\psi^{\mathrm{ord}_p(\psi)} \equiv 1 \pmod{p}$ and $\psi^{\mathrm{ord}_p(\psi)p^{r-1}} \equiv 1 \pmod{p^r}$ (cf. proof of Proposition 1). Thus $\mathrm{ord}_{p^r}(\psi) \mid \mathrm{ord}_p(\psi)p^{r-1}$ and so $\mathrm{ord}_{p^r}(\psi) = cp^j$ for some $c \mid \mathrm{ord}_p(\psi)$ and $j \geq 0$. Since $1 \equiv \psi^{cp^j} \equiv \psi^c \pmod{p}$, $c = \mathrm{ord}_p(\psi)$. ■

(It is not difficult to give an expression for j, however this will not be needed for our purposes.)

3. Characterization of odd good numbers. In this section we will derive a characterization for odd good numbers. In the proof we will make use of the following

Lemma 1. *Let $a_1, \ldots, a_k$ be natural numbers. The system S of congruences*

$$x \equiv a_1 \pmod{2a_1}, \ldots, x \equiv a_i \pmod{2a_i}, \ldots, x \equiv a_k \pmod{2a_k}$$

has a solution x iff there exists $e \geq 0$ such that $2^e \parallel a_i$ for $1 \leq i \leq k$.

Proof. The system of congruences S has a solution iff there exist odd integers $c_1, \ldots, c_k$ such that

$$a_1c_1 = \ldots = a_kc_k.$$

It is clearly necessary that the exact power of 2, say 2^e, dividing a_1 must equal the exact power of 2 dividing a_i for $2 \leq i \leq k$. Put $a_i' = a_i/2^e$. Then the a_i' are odd and it remains to show that

$$a_1'c_1 = \ldots = a_k'c_k,$$

for certain odd integers $c_1, \ldots, c_k$. The choice $c_i = \mathrm{lcm}(a_1', \ldots, a_k')/a_i'$, with $1 \leq i \leq k$, will do. ■

Theorem 1. *A number n coprime to $2ab$ is good iff there exists $e \geq 1$ such that $2^e \parallel \mathrm{ord}_p(\psi)$ for every prime p dividing n.*

Proof. ($\Rightarrow$) Let n be good and coprime to $2ab$. Let $p_1, \ldots, p_k$ be its prime divisors. Define e_i by $p_i^{e_i} \parallel n$. There exists c such that, for $1 \leq i \leq k$, $\psi^c \equiv -1 \pmod{p_i^{e_i}}$. Now, using Proposition 2, we see that $\mathrm{ord}_{p_i^{e_i}}(\psi)$ is even and

$$c \equiv \mathrm{ord}_{p_i^{e_i}}(\psi)/2 \pmod{\mathrm{ord}_{p_i^{e_i}}(\psi)}, \quad 1 \leq i \leq k. \tag{1}$$

Lemma 1 with $a_i = \mathrm{ord}_{p_i^{e_i}}(\psi)/2$, $1 \le i \le k$, then yields the existence of an $e \ge 1$ such that $2^e \parallel \mathrm{ord}_{p_i^{e_i}}(\psi)$ for $1 \le i \le k$. Using Proposition 4, the implication ⇒ then follows.

(⇐) By assumption and Proposition 4, there exists $e \ge 1$ such that $2^e \parallel \mathrm{ord}_{p_i^{e_i}}(\psi)$ for $1 \le i \le k$. By Lemma 1 there exists an integer c satisfying $c \equiv \mathrm{ord}_{p_i^{e_i}}(\psi)/2 \pmod{\mathrm{ord}_{p_i^{e_i}}(\psi)}$ for $1 \le i \le k$. Thus $\psi^c \equiv -1 \pmod{p_i^{e_i}}$ for $1 \le i \le k$ and hence $\psi^c \equiv -1 \pmod{n}$. ■

4. Counting good primes. In order to go beyond Theorem 1, one needs to study, for $r \ge 0$, the sets $C_r := \{p : 2^r \parallel \mathrm{ord}_p(\psi)\}$. Wiertelak [18] proved that C_r has a natural density and gave a remainder term which he subsequently improved in [20]. Let $\mathrm{Li}(x)$ denote the logarithmic integral. It is well known that $\pi(x)$, the number of primes not exceeding x, satisfies

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{\log^3 x}\right).$$

Combining this with [18, Theorem 1] and [20, Theorem 2], one deduces the following result.

Theorem 2. *Let a and b be two non-zero integers. Put $\psi = a/b$. Assume that $\psi \ne \pm 1$. Let λ be the largest number such that $|\psi| = u^{2^\lambda}$, where u is a rational number. Let $\varepsilon = \mathrm{sign}(\psi)$. Let $P_{a,b}$ be the set of primes not dividing $2ab$. Put, for $r \ge 0$,*

$$C_r = \{p \in P_{a,b} : 2^r \parallel \mathrm{ord}_p(\psi)\}.$$

We have the estimate

$$C_r(x) = \delta_r \,\mathrm{Li}(x) + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right), \tag{2}$$

where the implied constant may depend on a and b. For $\varepsilon = +1$, the constants $\{\delta_r\}_{r=0}^{\infty}$ are given by

$$\left\{1 - \frac{2}{3}\cdot\frac{1}{2^\lambda}, \frac{1}{3}\cdot\frac{1}{2^\lambda}, \ldots\right\}$$

if $u \ne 2u_1^2$, with rational u_1;

$$\left\{\frac{7}{24}, \frac{7}{24}, \frac{8}{24}, \frac{1}{24}, \ldots\right\}$$

if $u = 2u_1^2$ and $\lambda = 0$;

$$\left\{\frac{14}{24}, \frac{8}{24}, \frac{1}{24}, \ldots\right\}$$

if $u = 2u_1^2$ *and* $\lambda = 1$, *and*, *if* $u = 2u_1^2$ *and* $\lambda \ge 2$, *by*

$$\left\{1 - \frac{1}{3} \cdot \frac{1}{2^\lambda}, \frac{1}{3} \cdot \frac{1}{2^{\lambda+1}}, \ldots\right\}.$$

In case $\varepsilon = -1$ *the sequence* $\{\delta_r\}_{r=0}^\infty$ *is formed out of the corresponding case with* $\varepsilon = +1$ *by interchanging the first two terms. Thus*, *for example*, *if* $u \ne 2u_1^2$ *and* $\varepsilon = -1$, *then*

$$\{\delta_r\}_{r=0}^\infty = \left\{\frac{1}{3} \cdot \frac{1}{2^\lambda}, 1 - \frac{2}{3} \cdot \frac{1}{2^\lambda}, \frac{1}{3} \cdot \frac{1}{2^{\lambda+1}}, \ldots\right\}.$$

The densities indicated by the dots are computed as follows: *If* δ_j *is the last density given*, *then* $\delta_k = \delta_j \cdot 2^{j-k}$ *for* $k > j$.

Corollary 1. *If* ψ *is neither of the form* $\pm u_1^2$ *nor* $\pm 2u_1^2$, *with rational* u_1, *then* (2) *holds with* $\delta_0 = \frac{1}{3}$ *and*, *for* $r \ge 1$, $\delta_r = \frac{2}{3} \cdot \frac{1}{2^r}$.

5. Counting good integers. Let G_{odd} denote the set of odd good integers and G the set of good integers. Then, by Theorem 1,

$$G_{\text{odd}} = \bigcup_{r=1}^{\infty} G_r,$$

where G_r is the set of natural numbers including 1 which are composed of primes in C_r only. The sets G_r are completely multiplicative; $cd \in G_r$ if and only if $c, d \in G_r$, where c and d are natural numbers. Thus the problem of estimating $G_{\text{odd}}(x)$, and, as we will see, that of estimating $G(x)$, reduces to that of estimating $G_r(x)$ for $r \ge 1$. (If S is any set of natural numbers, then $S(x)$ denotes the number of elements n in S with $1 < n \le x$.) In order to estimate $G_r(x)$, we use an estimate of the following form:

Theorem 3. *Let* S *be a completely multiplicative set such that*

$$\sum_{p \in S,\, p \le x} 1 = \tau \operatorname{Li}(x) + O\left(\frac{x}{\log^N x}\right),$$

where $\tau > 0$ *and* $N > 3$ *are fixed. Then*

$$S(x) = cx \log^{\tau-1} x + O(x \log^{\tau-2} x),$$

where $c > 0$ *is a constant.*

This result, which is a particular case of Theorem 2 of [10, Chapter 4], is tantalizingly close to what we will need in order to prove Theorem 5, namely:

Theorem 4. *Let* S *be a completely multiplicative set such that*

$$\sum_{p \le x} f(p) = \tau \operatorname{Li}(x) + O\left(\frac{x(\log\log x)^g}{\log^3 x}\right), \tag{3}$$

where $\tau > 0$ and $g \geq 0$ are fixed and f denotes the characteristic function of S. Then

$$S(x) = \sum_{n \leq x} f(n) = cx \log^{\tau - 1} x + O(x(\log\log x)^{g+1} \log^{\tau-2} x),$$

where

$$c = \frac{1}{\Gamma(\tau)} \lim_{s \downarrow 1} (s-1)^{\tau} L_f(s) > 0,$$

Γ denotes the Gamma function and

$$L_f(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \qquad (\mathrm{Re}\, s > 0).$$

Remark. For convenience of proof the characteristic function of S is introduced. Notice that if S is a completely multiplicative set, then its characteristic function f is completely multiplicative, that is, $f(cd) = f(c)f(d)$ for all natural numbers c and d.

Proof of Theorem 4. Assume f satisfies the conditions of Theorem 4. Then, by Abel summation,

$$\sum_{p \leq x} f(p) \log p = \tau x + O\biggl(\frac{x l_2(x)^g}{\log^2 x}\biggr), \tag{4}$$

where $l_2(x) = \log\log(x+16)$. Put $\Lambda_f(n) = f(p^r) \log p$ if $n = p^r$ is a prime power and $\Lambda_f(n) = 0$ otherwise. Using (4) one deduces

$$\sum_{n \leq x} \Lambda_f(n) = \sum_{p \leq x} f(p) \log p + \sum_{m \geq 2} \sum_{p^m \leq x} f(p^m) \log p = \tau x + O\biggl(\frac{x l_2(x)^g}{\log^2 x}\biggr).$$

From this it follows by Abel summation that

$$\sum_{n \leq x} \frac{\Lambda_f(n)}{n} = \tau \log x + B_f + O\biggl(\frac{l_2(x)^g}{\log x}\biggr), \tag{5}$$

where B_f is a constant. Another estimate that is needed is the following:

$$\sum_{n \leq x} \frac{f(n)}{n} = O(\log^{\tau} x). \tag{6}$$

Noticing that

$$\sum_{n \leq x} \frac{f(n)}{n} \leq \prod_{p \leq x} \biggl(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \ldots\biggr) \ll \prod_{p \leq x} \biggl(1 + \frac{f(p)}{p} + O\biggl(\frac{1}{p^2}\biggr)\biggr)$$
$$\ll \exp\biggl\{\sum_{p \leq x} \frac{f(p)}{p} + O(1)\biggr\} \ll \exp\{\tau \log\log x + O(1)\} \ll \log^{\tau} x,$$

where we use the fact that $\sum_{p\le x} f(p)/p = \tau \log\log x + O(1)$, which follows from (3) on using Abel summation, (6) follows.

Next we use the iterative process as explained in §4.11 of the book of Postnikov [15] to establish that

$$\sum_{n\le x} \frac{f(n)}{n} = a_1 \log^\tau x + a_2 \log^{\tau-1} x + O(l_2(x)^{g+1} \log^{\tau-2} x), \tag{7}$$

with a_1, a_2 constants. The approach is to start the iteration with the initial estimate (6) and iterate three times to obtain (7). Choose $c_0 > 0$ such that

$$h(x) := \min\left(1, c_0 \frac{l_2(x)^g}{\log(x+1)}\right)$$

is positive non-increasing for $x > 1$. Thus, by (5),

$$\left|\sum_{n\le x} \frac{\Lambda_f(n)}{n} - \tau \log x - B_f\right| \le c_1 h(x)$$

for $x > 1$, where c_1 is a constant. Putting

$$\mu_f(x) = \sum_{n\le x} \frac{f(n)}{n} \quad \text{and} \quad g(x) = \sum_{n\le x} \frac{f(n)}{n} h\left(\frac{x}{n}\right),$$

we have, noticing that $f(n)\log n = \sum_{d\mid n} f(d)\Lambda_f(n/d)$,

$$\begin{aligned}\sum_{n\le x} \frac{f(n)\log n}{n} &= \sum_{n\le x}\sum_{d\mid n} \frac{f(d)\Lambda_f(n/d)}{d(n/d)} = \sum_{d\le x} \frac{f(d)}{d} \sum_{k\le x/d} \frac{\Lambda_f(k)}{k} \\ &= \tau \sum_{n\le x} \frac{f(n)}{n} \log\left(\frac{x}{n}\right) + B_f \mu_f(x) + O(g(x)).\end{aligned}$$

We write this equality in the form

$$-\sum_{n\le x} \frac{f(n)}{n} \log\left(\frac{x}{n}\right) + \mu_f(x)\log x = \tau \sum_{n\le x} \frac{f(n)}{n} \log\left(\frac{x}{n}\right) + B_f\mu_f(x) + O(g(x)).$$

This inequality in turn can be written as

$$\mu_f(x)\log x - (\tau+1)\int_1^x \frac{\mu_f(v)}{v}\, dv = B_f \mu_f(x) + O(g(x)). \tag{8}$$

Since $h(x) = O(1)$, the right hand side of (8) is $O(\mu_f(x)) = O(\log^\tau x)$ by (6) and thus

$$\mu_f(x)\log x - (\tau+1)\int_1^x \frac{\mu_f(v)}{v}\, dv = O(\log^\tau x). \tag{9}$$

So

$$\frac{\mu_f(x)}{x\log^{\tau+1}x}-\frac{\tau+1}{x\log^{\tau+2}x}\int_1^x\frac{\mu_f(v)}{v}\,dv=O\biggl(\frac{1}{x\log^2 x}\biggr).$$

Replacing x by u in this relation and integrating from 2 to x, we obtain

$$\int_2^x\frac{\mu_f(u)}{u\log^{\tau+1}u}\,du-(\tau+1)\int_2^x\frac{1}{u\log^{\tau+2}u}\int_1^u\frac{\mu_f(v)}{v}\,dv\,du=c_2+O\biggl(\frac{1}{\log x}\biggr),$$

for some constant c_2. Interchanging the order of integration in the second integral we obtain

$$\int_2^x\frac{\mu_f(u)}{u\log^{\tau+1}u}\,du-(\tau+1)\int_2^x\frac{\mu_f(v)}{v}\biggl(\int_v^x\frac{du}{u\log^{\tau+2}u}\biggr)dv$$
$$-(\tau+1)\int_1^2\frac{\mu_f(v)}{v}\biggl(\int_2^x\frac{du}{u\log^{\tau+2}u}\biggr)dv=c_2+O\biggl(\frac{1}{\log x}\biggr),$$

whence

$$\int_2^x\frac{\mu_f(u)}{u\log^{\tau+1}u}\,du+\int_2^x\frac{\mu_f(v)}{v}\biggl(\frac{1}{\log^{\tau+1}x}-\frac{1}{\log^{\tau+1}v}\biggr)dv$$
$$+\int_1^2\frac{\mu_f(v)}{v}\biggl(\frac{1}{\log^{\tau+1}x}-\frac{1}{\log^{\tau+1}2}\biggr)dv=c_2+O\biggl(\frac{1}{\log x}\biggr).$$

After cancellation we have

$$\frac{1}{\log^{\tau+1}x}\int_1^x\frac{\mu_f(v)}{v}\,dv=c_3+O\biggl(\frac{1}{\log x}\biggr),$$

i.e.

$$\int_1^x\frac{\mu_f(v)}{v}\,dv=c_3\log^{\tau+1}x+O(\log^{\tau}x),$$

for some constant c_3. So along with (9) we obtain

$$\mu_f(x)=a_1\log^{\tau}x+O(\log^{\tau-1}x), \tag{10}$$

for some constant a_1. We start the next iteration by estimating the right hand side of (8) more precisely than $O(\log^{\tau}x)$. To this end the term $g(x)$ appearing in (8) will be investigated more closely.

We take $0<\theta<1-\varepsilon_0$, where ε_0 $(0<\varepsilon_0<1)$ is fixed and make the following estimates:

$$\begin{aligned}
g(x) &= \sum_{x^{1-\theta}<n\le x} \frac{f(n)}{n} h\Big(\frac{x}{n}\Big) + g(x^{1-\theta})\\
&= \sum_{x^{1-\theta}<n\le x} \frac{f(n)}{n} h\Big(\frac{x}{n}\Big) + O\Big(h(x^{\theta}) \sum_{n\le x} \frac{f(n)}{n}\Big)\\
&= \sum_{x^{1-\theta}<n\le x} \frac{f(n)}{n} h\Big(\frac{x}{n}\Big) + O(\theta^{-1} l_2(x)^g \log^{\tau-1} x)\\
&= \int\limits_{1-\theta}^{1} h(x^{1-u})\, d\mu_f(x^u) + O(\theta^{-1} l_2(x)^g \log^{\tau-1} x).
\end{aligned}$$

Put $D_f(x) = \mu_f(x) - a_1 \log^\tau x$. We then obtain

$$\begin{aligned}
g(x) = \tau a_1 \log^\tau x \int\limits_{1-\theta}^{1} h(x^{1-u}) u^{\tau-1}\, du + \int\limits_{1-\theta}^{1} h(x^{1-u})\, dD_f(x^u)&\\
+ O(\theta^{-1} l_2(x)^g \log^{\tau-1} x).&
\end{aligned}$$

Recalling that $\mathrm{var}_{a\le z\le b} h(z) = \int_a^b |dh(z)|$, we obtain

$$\begin{aligned}
&\Big| \int\limits_{1-\theta}^{1} h(x^{1-u})\, dD_f(x^u) \Big|\\
&\qquad = \Big| h(1) D_f(x) - h(x^\theta) D_f(x^{1-\theta}) - \int\limits_{1-\theta}^{1} D_f(x^u)\, dh(x^{1-u}) \Big|\\
&\qquad \le O(\log^{\tau-1} x) + \max_{x^{1-\theta}\le z\le x} D_f(z)\, \mathrm{var}_{1\le z\le x^\theta} h(z) = O(\log^{\tau-1} x),
\end{aligned}$$

since $h(x^\theta) = O(1)$, $D_f(x) = O(\log^{\tau-1} x)$ by (10) and $\mathrm{var}_{1\le z\le x^\theta} h(z) = O(1)$. Since

$$\int\limits_{1-\theta}^{1} h(x^{1-u}) u^{\tau-1}\, du = \int\limits_{0}^{\theta} h(x^z)(1-z)^{\tau-1}\, dz = O(\theta),$$

we obtain on putting $\theta = l_2(x)^{g/2}/\sqrt{\log x}$ and gathering the various error terms

$$\begin{aligned}
g(x) &= \tau a_1 \log^\tau x \int\limits_{1-\theta}^{1} h(x^{1-u}) u^{\tau-1}\, du + O(\log^{\tau-1} x) + O(\theta^{-1} l_2(x)^g \log^{\tau-1} x)\\
&= O(\theta \log^\tau x) + O(\log^{\tau-1} x) + O(\theta^{-1} l_2(x)^g \log^{\tau-1} x)\\
&= O(l_2(x)^{g/2} \log^{\tau-1/2} x).
\end{aligned}$$

Inserting this into (8) and using (10) we obtain (9) with the sharpened right hand side

$$B_f a_1 \log^\tau x + O(l_2(x)^{g/2} \log^{\tau-1/2} x).$$

Then making one more iteration, we find (on keeping track of the new, sharpened, right hand sides)

$$\mu_f(x) = a_1 \log^\tau x + a_2 \log^{\tau-1} x + O(l_2(x)^{g/2} \log^{\tau-3/2} x),$$

for some constant a_2. Next put $\Delta_f(x) = \mu_f(x) - a_1 \log^\tau x - a_2 \log^{\tau-1} x$. We have already seen that $\Delta_f(x) = O(l_2(x)^{g/2} \log^{\tau-3/2} x)$. We now obtain, for $0 < \vartheta < 1 - \varepsilon_0$,

$$\begin{aligned}(11)\qquad g(x) = \tau a_1 \log^\tau x \int\limits_{1-\vartheta}^{1} h(x^{1-u}) u^{\tau-1}\, du \\ + (\tau-1) a_2 \log^{\tau-1} x \int\limits_{1-\vartheta}^{1} h(x^{1-u}) u^{\tau-2}\, du \\ + \int\limits_{1-\vartheta}^{1} h(x^{1-u})\, d\Delta_f(x^u) + O(\vartheta^{-1} l_2(x)^g \log^{\tau-1} x).\end{aligned}$$

We have

$$\begin{aligned}(12)\qquad \int\limits_{1-\vartheta}^{1} h(x^{1-u}) u^{\tau-1}\, du &= \int\limits_{0}^{\vartheta} h(x^z)(1-z)^{\tau-1}\, dz = O\Big(\int\limits_{0}^{\vartheta} h(x^z)\, dz\Big) \\ &= O\Big(\frac{1}{\log x} \int\limits_{1}^{x^\vartheta} \frac{h(v)}{v}\, dv\Big) = O\Big(\frac{l_2(x)^{g+1}}{\log x}\Big).\end{aligned}$$

Using (12) we see that the first term in the right hand side of (11) is of order $l_2(x)^{g+1} \log^{\tau-1} x$. The second term in (11) is of order $\log^{\tau-1} x$. Proceeding as in the derivation of the estimate for

$$\Big|\int\limits_{1-\vartheta}^{1} h(x^{1-u})\, dD_f(x^u)\Big|,$$

we obtain

$$\Big|\int\limits_{1-\vartheta}^{1} h(x^{1-u})\, d\Delta_f(x^u)\Big| = O(l_2(x)^{g/2} \log^{\tau-3/2} x)$$

and so

$$\begin{aligned}g(x) = O(l_2(x)^{g+1} \log^{\tau-1} x) + O(\log^{\tau-1} x) \\ + O(l_2(x)^{g/2} \log^{\tau-3/2} x) + O(\vartheta^{-1} l_2(x)^g \log^{\tau-1} x).\end{aligned}$$

On taking $\vartheta = 1/2$ we obtain $g(x) = O(l_2(x)^{g+1}\log^{\tau-1} x)$. Inserting this into (8) and making a final iteration, we then find (on keeping track of the new, sharpened, right hand sides) the estimate (7).

We express $\sum_{n\le x} f(n) = S(x)$ in terms of $\mu_f(x)$:

$$S(x) = \sum_{n\le x}\frac{f(n)}{n}n = x\mu_f(x) - \int_2^x \mu_f(t)\,dt + O(1).$$

By substituting the estimate (7) in this expression we obtain

$$\begin{aligned}S(x) &= x(a_1\log^\tau x + a_2\log^{\tau-1}x + O(\log^{\tau-2}x))\\ &\quad - \int_2^x (a_1\log^\tau t + a_2\log^{\tau-1}t + O(\log^{\tau-2}t))\,dt + O(1)\\ &= \tau a_1 x\log^{\tau-1}x + O(xl_2(x)^{g+1}\log^{\tau-2}x).\end{aligned}$$

It remains to show that

$$\tau a_1 = \frac{1}{\Gamma(\tau)}\lim_{s\downarrow 1}(s-1)^\tau L_f(s) > 0.$$

Notice that the condition of [15, Lemma 6, p. 96] is satisfied. So by the last identity on p. 98 of [15] we have

$$\mu_f(x) = \frac{C}{\Gamma(\tau+1)}\log^\tau x\biggl(1 + O\biggl(\frac{1}{\log\log x}\biggr)\biggr),$$

where $C = \lim_{s\downarrow 1}(s-1)^\tau L_f(s)$ and therefore

$$\tau a_1 = \frac{\tau C}{\Gamma(\tau+1)} = \frac{1}{\Gamma(\tau)}\lim_{s\downarrow 1}(s-1)^\tau L_f(s).$$

(Here we used the fact that S is a semigroup and that its zetafunction equals $L_f(s)$.) That τa_1 is positive follows from the fact that C is positive, which follows from the proof of [15, Lemma 6, p. 96], but is omitted in the statement. This completes the proof of Theorem 4. ■

Next we deduce from Theorems 1, 2 and 4 an estimate for $G(x)$ which, since $\lim_{r\to\infty}\delta_r = 0$, has error $O(x\log^{\delta-1}x)$ for arbitrary given $\delta > 0$. Notice that the first term in (13) is not necessarily the dominant one.

Theorem 5. *Let a and b be two non-zero coprime integers such that $a \ne \pm b$. Let G denote the set of integers $m > 1$ such that m divides $a^k + b^k$ for some $k \ge 1$. Let $G(x)$ be the number of elements in G not exceeding x. Then, for $t \ge 1$, there exist positive constants $c_1, \ldots, c_t$ such that*

$$G(x) = \frac{x}{\log x}(c_1\log^{\delta_1}x + c_2\log^{\delta_2}x + \ldots + c_t\log^{\delta_t}x + O(\log^{\delta_{t+1}}x)), \tag{13}$$

where $\delta_1, \ldots, \delta_t$ are given in Theorem 2. The implied constant and $c_1, \ldots, c_t$ may depend on a and b.

COROLLARY 2. *Let λ and u_1 be as in Theorem 2. We have $G(x) \sim cx\log^{-\alpha} x$, for some constant $c > 0$, where in case $u \neq 2u_1^2$, $\alpha = 1 - \frac{1}{3} \cdot \frac{1}{2^\lambda}$ if $\varepsilon = +1$ and $\alpha = \frac{2}{3} \cdot \frac{1}{2^\lambda}$ if $\varepsilon = -1$. If $u = 2u_1^2$ and $\varepsilon = +1$, then $\alpha = \frac{2}{3}$ if $\lambda \le 1$ and $\alpha = 1 - \frac{1}{3} \cdot \frac{1}{2^{\lambda+1}}$ if $\lambda \ge 2$. If $u = 2u_1^2$ and $\varepsilon = -1$, then $\alpha = \frac{2}{3}, \frac{5}{12}, \frac{1}{3} \cdot \frac{1}{2^\lambda}$ according as $\lambda = 0$, $\lambda = 1$ or $\lambda \ge 2$.*

Proof. There are no even good integers when ab is even. In this case, by Theorem 1,

$$G(x) = \sum_{r=1}^{\infty} G_r(x).$$

Next assume that ab is odd. Let $m = 2^\nu \mu$ with μ odd be a good divisor, whence $m \mid a^k + b^k$ for some $k \ge 1$. First assume $\mu > 1$. By Theorem 1, $\mu \in G_r$ for some (unique) $r \ge 1$. If $r \ge 2$ it follows by (1) that k is even. Then $a^k + b^k \equiv 2 \pmod 4$ and hence $\nu = 0$ or $\nu = 1$. If $r = 1$ it follows by (1) that k is odd. Since for arbitrary $\xi \ge 0$, the only solution of $x^k \equiv -1 \pmod{2^\xi}$ is $x \equiv -1 \pmod{2^\xi}$, it follows that $0 \le \nu \le w$, where $2^w \parallel a + b$. Finally, in case $\mu = 1$ we have $2^\nu = a^k + b^k$. This Diophantine equation has at most w solutions, as one easily checks. From these restrictions on ν and Theorem 1, we deduce

$$G(x) = \sum_{z=0}^{w} G_1\left(\frac{x}{2^z}\right) + \sum_{r=2}^{\infty} \left\{ G_r\left(\frac{x}{2}\right) + G_r(x) \right\} + O(1).$$

We now use Theorem 4 to estimate $G_r(x)$ for $r \ge 1$. By Theorem 2, (3) is satisfied with $\tau = \delta_r$ and $g = 4$. Applying Theorem 4 and using $\delta_r \le 1$, we obtain

$$\begin{aligned} G_r(x) &= d_r x \log^{\delta_r - 1} x + O(x l_2(x)^5 \log^{\delta_r - 2} x) \\ &= d_r x \log^{\delta_r - 1} x + O(x \log^{\delta_{t+1} - 1} x), \end{aligned} \tag{14}$$

for some positive constant d_r. The result now follows, irrespective of whether ab is even or not, once we show that

$$\sum_{r=t+1}^{\infty} G_r(x) = O(x \log^{\delta_{t+1} - 1} x). \tag{15}$$

To this end, notice that the primes in C_t, $t \ge s \ge 1$, satisfy $p \equiv 1 \pmod{2^s}$. Thus

$$\sum_{r \ge s} G_r(x) \le \sum_{\substack{n \le x \\ p \mid n \Rightarrow p \equiv 1 \,(\mathrm{mod}\, 2^s)}} 1.$$

This latter sum can be estimated with the help of Theorem 3, or of course its improvement Theorem 4, and the estimate

$$\pi(x;2^s,1) := \sum_{\substack{p\le x\\ p\equiv 1 \,(\mathrm{mod}\, 2^s)}} 1 = \frac{1}{2^{s-1}}\,\mathrm{Li}(x) + O\biggl(\frac{x}{\log^4 x}\biggr),$$

which follows from the Prime Number Theorem for arithmetic progressions. Thus by choosing s large enough (taking $2^{s-1} \ge 1/\delta_{t+1}$ will do), we can ensure that $\sum_{r\ge s} G_r(x) = O(x\log^{\delta_{t+1}-1} x)$. By (14), $t \ge 1$, and the fact that $\{\delta_r\}_{r=2}^{\infty}$ is monotonic decreasing, we have

$$\sum_{t+1\le r\le s} G_r(x) = O(x\log^{\delta_{t+1}-1} x).$$

Thus (15) holds and the result follows. ■

Remark 1. If (2) were true with a sharper error term, this would not lead to an improvement in the error of (13), at least by the approach followed here.

Remark 2. In [11] the estimate (13) with $\delta_i = 2^{1-i}/3$ is established for the counting function of the divisors of the sequence $2, 1, 3, 4, 7, 11, \ldots$ of Lucas numbers.

6. An example and an application.

As an example let us consider the case of $a = 2$ and $b = 1$. (This is relevant for coding theory purposes, cf. [14].) Using special cases of quadratic, biquadratic and octic reciprocity (cf. [2]) and Hasse's technique from [7] to compute Dirichlet densities, it is not difficult to prove:

THEOREM 6. *Let p be an odd prime and $2^r \,\|\, p-1$. Then at most one of the following holds*:

(i) *If* $p \equiv 7 \pmod 8$, *then* $p \in C_0$;
(ii) *If* $r = 3$ *and* p *is represented by the form* $X^2 + 64(X+2Y)^2$, *then* $p \in C_0$;
(iii) *If* $p \equiv 3 \pmod 8$, *then* $p \in C_1$,
(iv) *If* $r = 3$ *and* p *is represented by the form* $X^2 + 256Y^2$, *then* $p \in C_1$;
(v) *If* $p \equiv 5 \pmod 8$, *then* $p \in C_2$;
(vi) *If* $r \ge 4$ *and* p *is represented by the form* $X^2 + 64(X+2Y)^2$, *then* $p \in C_{r-2}$;
(vii) *If* p *is represented by the form* $X^2 + 16(X+2Y)^2$, *then* $p \in C_{r-1}$.

The smallest odd prime that is not covered is 337. *The Dirichlet density of the primes not covered is* 1/32.

By Theorem 5 it follows that for $t \geq 0$, there exist positive constants $c_1, \ldots, c_{3+t}$ such that

$$G(x) = \frac{x}{\log x}\Big(c_1 \log^{1/3} x + c_2 \log^{7/24} x + \sum_{k=0}^{t} c_{3+k} \log^{\frac{1}{3}\cdot\frac{1}{2^{k+3}}} x + O(\log^{\frac{1}{3}\cdot\frac{1}{2^{t+4}}} x)\Big). \tag{16}$$

In order to prove this directly, a weaker version of Theorem 2 will do. On using [13, Theorem 2] an error term of $O(x \log^{-5/3} x)$ in Theorem 2 suffices, on using [6, Theorem 2] an error term of $O(x \log^{-3/2} x)$. Moreover, since good numbers in this case are obviously odd, even good numbers need not be considered.

Note that an integer n has a divisor $m \equiv 7 \pmod 8$ if and only if either there is a prime $p \equiv 7 \pmod 8$, or both a prime $p \equiv 3 \pmod 8$ and a prime $q \equiv 5 \pmod 8$ dividing n. Using Theorem 6 one then deduces:

LEMMA 2. *If n has a divisor m such that $m \equiv 7 \pmod 8$, then n is bad.*

The bad numbers $n < 100$ which are not congruent to $7 \pmod 8$ are $21, 35, 45, 49, 51, 69, 73, 75, 77, 85, 89, 91$ and 93. The bad numbers $n < 200$ which have no divisors congruent to $7 \pmod 8$ are $51, 73, 85, 89, 123, 153$ and 187. There are $O(x \log^{-1/2} x)$ integers $\leq x$ without divisors congruent to $7 \pmod 8$. By equation (16), $O(x \log^{-1/2} x)$ of these are bad. Thus Lemma 2 allows one to find all but $O(x \log^{-1/2} x)$ of the bad integers not exceeding x.

For $m \geq 1$, let K_m denote the cyclotomic number field $\mathbb{Q}(e^{2\pi i/m})$. The prime divisors of $\{2^k + 1\}$ are related to the Stufe (level) of a number field. Identities similar to

$$(X_1^2 + X_2^2)(Y_1^2 + Y_2^2) = (X_1Y_1 - X_2Y_2)^2 + (X_1Y_2 + X_2Y_1)^2$$

hold for 4 and 8 variables as well. One might ask whether there exist such identities for sums of squares of n variables (where $n \neq 1, 2, 4, 8$). This is connected (see [16]) with the notion of the Stufe, $s(K)$, of a field K; i.e. the smallest positive integer for which the equation $-1 = \alpha_1^2 + \ldots + \alpha_s^2$ ($\alpha_i \in K$) is solvable. (If this equation is not solvable in K, the field K is called formally real and one puts $s(K) = \infty$.) Pfister proved that the Stufe of any field, if it exists, is a power of two. Hilbert proved that $s(K_m) \leq 4$ for $m \geq 3$. More recent contributions involving the Stufe of cyclotomic number fields can be found in [3, 4, 5]. If $4 \mid m$, then $i \in K_m$ and thus $s(K_m) = 1$. Thus assume $4 \nmid m$. In that case Fein *et al.* [5] proved a result which is equivalent with the assertion that $s(K_m) = 2$ iff m is divisible by some prime divisor of the sequence $\{2^k + 1\}_{k=1}^{\infty}$. (Thus $s(K_m) = 4$ iff m is coprime with all numbers in $\{2^k + 1\}_{k=1}^{\infty}$.) This result in combination with Theorem 6 gives Theorem 1 of both [3] and [4] and Theorem 4 of [5]. Using Theorems 2 and 4 one deduces:

THEOREM 7. *The number of $m \le x$ such that $\mathbb{Q}(e^{2\pi i/m})$ is of Stufe* 4, $\mathrm{St}_4(x)$, *equals*

$$\mathrm{St}_4(x) = c\frac{x}{\log^{17/24} x}\left(1 + O\left(\frac{(\log\log x)^5}{\log x}\right)\right),$$

where $c > 0$ is a constant.

Remark. It seems that the authors of [5] believed that their Theorem 5 was new with them. However, this result is due to Hasse [7], but the method of proof in [5] provides an interesting alternative to Hasse's method.

References

[1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. 551, 1995.

[2] A. Brauer, *A note on a number theoretical paper of Sierpiński*, Proc. Amer. Math. Soc. 11 (1960), 406–409.

[3] P. Chowla, *On the representation of* -1 *as a sum of squares in a cyclotomic field*, J. Number Theory 1 (1969), 208–210.

[4] P. Chowla and S. Chowla, *Determination of the Stufe of certain cyclotomic fields*, ibid. 2 (1970), 271–272.

[5] B. Fein, B. Gordon and J. H. Smith, *On the representation of* -1 *as a sum of two squares in an algebraic number field*, ibid. 3 (1971), 310–315.

[6] H. Halberstam, unpublished manuscript, 1995.

[7] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a* $\neq 0$ *von gerader bzw. ungerader Ordnung mod. p ist*, Math. Ann. 166 (1966), 19–23.

[8] E. V. Krishnamurthy, *An observation concerning the decimal periods of prime reciprocals*, J. Recreational Math. 24 (1969), 212–213.

[9] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, 1983.

[10] P. Moree, *Psixyology and Diophantine equations*, Ph.D. Thesis, Leiden University, 1993.

[11] —, *Counting divisors of Lucas numbers*, MPI-Bonn preprint No. 34, 1996.

[12] R. W. K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory 13 (1981), 303–319.

[13] —, *A problem of Rankin on sums of powers of cusp-form coefficients*, J. London Math. Soc. 44 (1991), 203–217.

[14] V. Pless, P. Solé and Z. Qian, *Cyclic self dual* $\mathbb{Z}_4$*-codes*, Finite Fields Appl. 3 (1997), 48–69.

[15] A. G. Postnikov, *Introduction to Analytic Number Theory*, Transl. Math. Monographs 68, Amer. Math. Soc., Providence, R.I., 1988.

[16] A. R. Rajwade, *Squares*, Cambridge University Press, 1993.

[17] W. Sierpiński, *Sur une décomposition des nombres premiers en deux classes*, Collect. Math. 10 (1958), 81–83.

[18] K. Wiertelak, *On the density of some sets of primes. I, II*, Acta Arith. 34 (1977/78), 183–196, 197–210.

[19] K. Wiertelak, *On the density of some sets of primes. III*, Funct. Approx. Comment. Math. 10 (1981), 93–103.

[20] —, *On the density of some sets of primes. IV*, Acta Arith. 43 (1984), 177–190.

[21] —, *On the density of some sets of primes* p, *for which* $\mathrm{ord}_p(n) = d$, Funct. Approx. Comment. Math. 21 (1992), 69–73.

Max-Planck-Institut für Mathematik
Gottfried-Claren Str. 26
53225 Bonn, Germany
E-mail: moree@mpim-bonn.mpg.de

Received on 2.1.1996
and in revised form on 28.10.1996 (2912)