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

Pieter Moree

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI/95-130

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

Pieter Moree*

Abstract

Let a and b be non-zero integers. Let G be the set of natural numbers n such that n divides $a^k + b^k$ for some $k \geq 1$. We give a (weak) algebraic characterization of G and use it to derive an approximate expression for the number of the elements not exceeding x that are in G.

1 Introduction

Let a and b be two non-zero coprime integers that are fixed. 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, 15] 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 is the main focus of this paper.

I like to thank Patrick Solé for asking a question that motivated this research and 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 $\mathbf{Z}_4$-linear codes [9]. Furthermore, I thank T. Kleinjung for some inspiring discussions.

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. 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

*Max-Planck Institut für Mathematik, Gottfried-Claren Straße 26, D-53225 Bonn, Germany. Email: moree@antigone.mpim-bonn.mpg.de

induction and the binomial theorem we have $\psi^{ep^j} \equiv -1 (\text{mod } p^{1+j})$, 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 that for p odd the only solutions of $x^2 \equiv 1 (\text{mod } p^\nu)$ are $x \equiv \pm 1 (\text{mod } p^\nu)$ (this can be proved using Hensel's lifting theorem). Let p^r be good. Not surprisingly, the smallest natural number e such that $\psi^e \equiv -1 (\text{mod } p^r)$ is related to $ord_{p^r}(\psi)$.

Proposition 2 *If p^r is good, then $ord_{p^r}(\psi) = 2e$ where e is the smallest natural number such that $\psi^e \equiv -1 (\text{mod } p^r)$.*

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

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

Proposition 3 *The prime power p^r is good iff $ord_{p^r}(\psi)$ is even.*

Thus studying primes that are good is equivalent to studying primes for which $\text{ord}_p(\psi)$ is even. Several authors studied the latter question. Sierpinski [10] seems to have been the first. Hasse [4] improved on Brauer [2], who improved on Sierpinski. 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 the order of g in the multiplicative group of invertible residue classes modulo b, that is the g-adic period is equal to $\text{ord}_b(g)$. Krishnamurthy [5] conjectured that asymptotically one-third of the primes $p > 5$ have odd decimal period. Since a set of primes that has a Dirichlet density, not always has a natural density, Hasse's result is not strong enough to imply Krishnamurty's conjecture. Odoni [7] established this conjecture in a much more general form. It turns out that the set of primes under consideration is an union of an infinite number of Frobenian sets, that is sets that differ finitely from some complete set of unramified primes having prescribed Frobenius conjugacy class in some fixed Galois extension of 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 [11] and subsequently in [13], who derived a uniform version of the Prime Ideal Theorem and used that result 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 $ord_{p^r}(\psi) = ord_p(\psi)p^j$ for some $j \geq 0$.*

Proof: We have $\psi^{ord_p(\psi)} \equiv 1 (\text{mod } p)$ and $\psi^{ord_p(\psi)p^{r-1}} \equiv 1 (\text{mod } p^r)$ (cf. proof of Proposition 1). Thus $\text{ord}_{p^r}(\psi) | ord_p(\psi)p^{r-1}$ and so $\text{ord}_{p^r}(\psi) = cp^j$ for some $c | ord_p(\psi)$ and $j \geq 0$. Since $1 \equiv \psi^{cp^j} \equiv \psi^c (\text{mod } p)$, $c = ord_p(\psi)$. □

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

3 Characterization of odd good numbers

In this section a characterization result for odd good numbers will be proved. In the proof we make use of the following lemma:

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

$$x \equiv a_1 (\text{mod } 2a_1)$$

$$\cdots\cdots\cdots\cdots$$

$$x \equiv a_i (\text{mod } 2a_i)$$

$$x \equiv a_k (\text{mod } 2a_k)$$

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

Proof: The system of congruences S has a solution iff there exists odd integers $c_1, \cdots, c_k$ such that

$$a_1 c_1 = a_2 c_2 = \cdots = a_k c_k.$$

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

$$a_1' c_1 = a_2' c_2 = \cdots = a_k' c_k,$$

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

Theorem 1 *An number n coprime to $2ab$, is good iff there exists $e \geq 1$ such that $2^e || ord_p(\psi)$ for every prime dividing n.*

Proof: '⇒'. Let n be good and coprime to $2ab$. Let $p_1, \cdots, p_k$ be its prime divisors. Define e_i by $p_i^{e_i} || n$. There exists c such that, for $1 \leq i \leq k$, $\psi^c \equiv -1 (\text{mod } p_i^{e_i})$. Now using Proposition 2, it follows that $ord_{p_i^{e_i}}(\psi)$ is even and

$$c \equiv ord_{p_i^{e_i}}(\psi)/2 \ (\text{mod } ord_{p_i^{e_i}}(\psi)), \ 1 \leq i \leq k.$$

Lemma 1 with $a_i = ord_{p_i^{e_i}}(\psi)/2$, $1 \leq i \leq k$, then yields the existence of an $e \geq 1$ such that $2^e || ord_{p_i^{e_i}}(\psi)$ for $1 \leq i \leq k$. Using Proposition 4 the implication '⇒' then follows.

'⇐'. By assumption and Proposition 4 it follows there exists $e \geq 1$ such that $2^e || ord_{p_i^{e_i}}(\psi)$ for $1 \leq i \leq k$. By Lemma 1 there exists an integer c satisfying $c \equiv ord_{p_i^{e_i}}(\psi)/2 \ (\text{mod } ord_{p_i^{e_i}}(\psi))$ for $1 \leq i \leq k$. Thus $\psi^c \equiv -1 (\text{mod } p_i^{e_i})$ for $1 \leq i \leq k$. Then, by the chinese remainder theorem, $\psi^c \equiv -1 (\text{mod } n)$. □

4 Counting good primes

In order to go beyond Theorem 1 one needs to study, for $r \geq 0$, the sets $C_r := \{p : 2^r || ord_p(\psi)\}$. Wiertelak [11] proved that C_r has a natural density and gave a remainder term, that he subsequently improved in [13]. Let $\mathrm{Li}(x)$ denote the logarithmic integral. Then it is well-known that $\pi(x)$, the number of primes not exceeding x, satisfies $\pi(x) = \mathrm{Li}(x) + O(\frac{x}{\log^3 x})$. Using this, [11, Theorem 1] and [13, Theorem 2], one deduces the following result.

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

$$C_r = \{p \in P_{a,b} : 2^r || ord_p(\psi)\}.$$

We have the estimate

$$C_r(x) = \delta_r \mathrm{Li}(x) + O(\frac{x \log\log^4 x}{\log^3 x}), \tag{1}$$

where the implied constant may depend on a and b.
If $u \neq 2u_1^2$ and $\epsilon = +1$, then

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

If $u \neq 2u_1^2$ and $\epsilon = -1$, then

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

If $u = 2u_1^2$, $\epsilon = +1$, and $\lambda = 0$, then

$$\{\delta_r\}_{r=0}^{\infty} = \{\frac{7}{24}, \frac{7}{24}, \frac{8}{24}, \frac{1}{24}, \cdots\}.$$

If $u = 2u_1^2$, $\epsilon = +1$, and $\lambda = 1$, then

$$\{\delta_r\}_{r=0}^{\infty} = \{\frac{14}{24}, \frac{8}{24}, \frac{1}{24}, \cdots\}.$$

If $u = 2u_1^2$, $\epsilon = +1$ and $\lambda \geq 2$, then

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

If $u = 2u_1^2$, $\epsilon = -1$, and $\lambda = 0$, then

$$\{\delta_r\}_{r=0}^{\infty} = \{\frac{7}{24}, \frac{7}{24}, \frac{8}{24}, \frac{1}{24}, \cdots\}.$$

If $u = 2u_1^2$, $\epsilon = -1$, *and* $\lambda = 1$, *then*

$$\{\delta_r\}_{r=0}^{\infty} = \{\frac{8}{24}, \frac{14}{24}, \frac{1}{24}, \cdots\}.$$

If $u = 2u_1^2$, $\epsilon = -1$, *and* $\lambda \geq 2$, *then*

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

The densities indicated by the dots are computed as follows; if δ_j *is the last density given and one wants to compute* δ_k $(k > j)$, *then* $\delta_k = \delta_j \cdot 2^{j-k}$.

Corollary 1 *If* ψ *is unequal to* $\pm u_1^2, \pm 2u_1^2$, *where* u_1 *is rational, then* (1) *holds with* $\delta_0 = \frac{1}{3}$ *and, for* $r \geq 1$, $\delta_r = \frac{2}{3} \cdot \frac{1}{2^r}$.

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,

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

where G_r is the set of natural numbers including 1, that are composed of primes in C_r only. The sets G_r are completely multiplicative; $ab \in G_r$ if and only if $a, b \in G_r$, where a and b are natural numbers. Thus the problem of estimating $G_{odd}(x)$, and, as will be seen, that of estimating $G(x)$, reduces to that of estimating $G_r(x)$ for $r \geq 1$. (If S is any set of natural numbers, then $S(x)$ denotes the number of elements n in S with $1 < n \leq x$.) 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*

$$\sum_{p \in S,\ p \leq x} 1 = \tau \mathrm{Li}(x) + O(\frac{x}{\log^N x}),$$

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 [6, Chapter 4], is tantalizing close to what we need in order to prove Theorem 5, namely:

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

$$\sum_{p \in S,\ p \leq x} 1 = \tau \mathrm{Li}(x) + O(\frac{x \log \log^g x}{\log^3 x}), \tag{2}$$

where $\tau > 0$ *and* $g \geq 0$ *are fixed. Then*

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

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

Proof: The proof given in [6] of Theorem 3 can be easily transformed into a proof of this assertion. Since the proof of Theorem 3 is rather long and technical, we just indicate the changes that have to be made. For convenience put $l_2(x) = \log\log(x+16)$. If in Lemma 3 we assume that the error is $R_G(x) = O(l_2(x)^g x \log^{-3} x)$, then one easily checks that the error in the conclusion of Theorem 3 now becomes $O(l_2(x)^g/\log x)$. We can choose constants c_0 and c_1 such that the quantity between absolute signs in the second displayed formula on p. 93 is bounded by $h_G(x) := \min(c_0, c_1 l_2(x)^g/\log x)$ for $x > 1$ and is a positive non-increasing function. It is no longer true that the integral $\int_1^\infty h_G(v)dv/v$ converges (p. 97). The equation (6) now becomes $\int_0^\vartheta h_G(x^z)dz = O(l_2(x)^{g+1}/\log x)$. The statement at the top of p. 98 about the first term of the right hand side, now becomes that it is of order $l_2(x)^{g+1}\log^{\tau-1} x$. All the remaining error terms on pp. 98-99 that include either $\log^{\tau-1} x$ or $\log^{\tau-2} x$, have to be multiplied by $l_2(x)^{g+1}$. $\square$

Next it will be shown how Theorems 1, 2 and 4, can be used to deduce the following estimate for $G(x)$:

Theorem 5 *Let a and b be two non-zero coprime integers such that $a \neq \pm b$. Let G denote the set of integers $m > 1$ such that $m|a^k + b^k$ for some $k \geq 1$. Let $G(x)$ be the number of elements in G not exceeding x. Then there exist positive constants $c_0, \cdots, c_t$ such that*

$$G(x) = \frac{x}{\log x}(c_0 \log^{\delta_0} x + c_1 \log^{\delta_1} x + \cdots + c_t \log^{\delta_t} x + O(\log^\epsilon x)), \qquad (3)$$

where t is the smallest number such that $\delta_s \leq \epsilon$ for every $s > t$, and $\delta_0, \cdots, \delta_t$ are given in Theorem 2. The implied constant and $c_0, \cdots, c_t$ may depend on a and b.

Corollary 2 *Let λ and u_1 be as in Theorem 2. We have $G(x) \sim c\frac{x}{\log^\alpha x}$, for some constant $c > 0$, where in case $u \neq 2u_1^2, \alpha = \frac{2}{3}\cdot\frac{1}{2^\lambda}$, in case $u = 2u_1^2$, $\alpha = \frac{2}{3}$ if $\lambda = 0$, $\alpha = \frac{5}{12}$ if $\lambda = 1$ and $\alpha = \frac{1}{3}\cdot\frac{1}{2^\lambda}$ if $\lambda \geq 2$.*

Proof: There are no even good integers in case ab is even. Then, by Theorem 1,

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

Next assume that ab is odd. Let $m = 2^\nu\mu$, μ odd, be a good divisor. In case $\mu > 1$, $\mu \in G_r$, $r \geq 2$, it follows that $\mu|a^k + b^k$, where k is even. Since $a^k + b^k \equiv 2 (\mathrm{mod}\ 4)$, $\nu = 0$ or $\nu = 1$. In case $\mu \in G_1$, $\mu|a^k + b^k$, where k is odd. Since for arbitrary $v \geq 0$, the only solution of $x^k \equiv -1 (\mathrm{mod}\ 2^v)$, is $x \equiv -1 (\mathrm{mod}\ 2^v)$, it follows that $0 \leq \nu \leq w$, where $2^w || a + b$. From this and Theorem 1 it is deduced that

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

We now use Theorem 4 to estimate $G_r(x)$ for $r \geq 1$. By Theorem 2, (2) is satisfied with $\tau = \delta_r$ and $g = 4$. Applying Theorem 4 and using $\delta_r \leq 1$ yields

$$G_r(x) = d_r x \log^{\delta_r - 1} x + O(x l_2(x)^5 \log^{\delta_r - 2} x) = d_r x \log^{\delta_r - 1} x + O(x \log^{\epsilon - 1} x), \qquad (4)$$

for some positive d_r. The result now follows, both if ab is even and otherwise, if we show that

$$\sum_{r=t+1}^{\infty} G_r(x) = O(x \log^{\epsilon-1} x). \tag{5}$$

To that end, notice that the primes in C_t, $t \geq s \geq 1$, satisfy $p \equiv 1(\text{mod } 2^s)$. Thus

$$\sum_{r \geq s} G_r(x) \leq \sum_{\substack{n \leq x \\ p|n \Rightarrow p \equiv 1(\text{mod } 2^s)}} 1.$$

The latter sum can be estimated by Theorem 3, or of course its improvement Theorem 4, on using the estimate

$$\pi(x; 2^s, 1) := \sum_{p \leq x,\ p \equiv 1(\text{mod } 2^s)} 1 = \frac{1}{2^{s-1}} \text{Li}(x) + O(\frac{x}{\log^4 x}),$$

which follows from the Prime Number Theorem for arithmetic progressions. Thus by choosing s large enough (taking $2^{s-1} \geq 1/\epsilon$ will do), we can ensure that $\sum_{r \geq s} G_r(x) = O(x \log^{\epsilon-1} x)$. By the definition of t and (4) we have

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

Thus (5) holds and the result follows. □

Remark. If (1) would be true with a sharper error term, this would, at least by the approach followed here, not lead to an improvement in the error of (3).

6 An example

As an example let us consider the case where $a = 2$ and $b = 1$. (This is the most relevant for coding theory purposes, cf. [9].) Using special cases of quadratic, biquadratic and octic reciprocity (cf. [2]), one deduces the following information on the sets C_r :

Theorem 6 *Let p be an odd prime and $2^r || p-1$. Then*

(i) $p \in C_0$ *if* $p \equiv 7(\text{mod } 8)$ *or* $r = 3$ *and p is represented by the form* $65X^2 + 256XY + 256Y^2$;

(ii) $p \in C_1$ *if* $p \equiv 3(\text{mod } 8)$ *or* $r = 3$ *and p is represented by the form* $X^2 + 256Y^2$;

(iii) $p \in C_2$ *if* $p \equiv 5(\text{mod } 8)$;

(iv) $p \in C_{r-2}$ *if p is represented by the form* $65X^2 + 256XY + 256Y^2$ *and* $r \geq 4$;

(v) $p \in C_{r-1}$ *if p is represented by the form* $17X^2 + 64XY + 64Y^2$.

By Theorem 5 it follows that if $0 < \epsilon < \frac{1}{24}$ and t is the smallest integer such that $48 \cdot 2^t \geq 1/\epsilon$, then there exist positive constants $c_1, \cdots, c_t$ such that

$$G(x) = \frac{x}{\log x}(c_1 \log^{\frac{1}{3}} x + c_2 \log^{\frac{7}{24}} x + \sum_{k=0}^{t} c_{3+k} \log^{\frac{1}{3} \cdot \frac{1}{2^{k+3}}} x + O(\log^{\epsilon} x)). \qquad (6)$$

In order to prove this directly, a weaker version of Theorem 2 will do. On using [8, Theorem 2] an error term of $x \log^{-5/3} x$ in Theorem 2 suffices, on using [3, Theorem 2] an error term of $x \log^{-3/2} x$. Moreover, as trivially good numbers in this case are odd, consideration of even good numbers is not necessary.

Notice 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 $n < 100$ that are $\not\equiv 7 \pmod 8$ are $21, 35, 45, 49, 51, 69, 73, 75, 77, 85, 89, 91$ and 93. The bad numbers $n < 200$ that have no divisors $\equiv 7 \pmod 8$ are $51, 73, 85, 89$, $123, 153$ and 187. There are $O(x \log^{-1/2} x)$ integers $\leq x$ that have no divisors $\equiv 7 \pmod 8$. By equation (6), $O(x \log^{-1/2} x)$ of these are bad.

References

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

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

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

[4] 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.

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

[6] P. Moree, *Psixyology and Diophantine equations*, PhD. Thesis, Leiden University, The Netherlands, 1993.

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

[8] R. W. K. Odoni, A problem of Rankin on sums of powers of cusp-form coefficients, *J. London Math. Soc.* **44** (1991), 203-217.

[9] V. Pless, P. Solé and Z. Qian, Cyclic self dual Z_4-codes and type I lattices, preprint.

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

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

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

[13] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.* **43** (1984), 177-190.

[14] K. Wiertelak, On the density of some sets of integers, *Funct. Approx. Comment. Math.* **19** (1990), 71-76.

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