POWERS IN PRIME BASES AND A PROBLEM ON CENTRAL BINOMIAL COEFFICIENTS

Sebastian Tim Holdum
Niels Bohr Institute, University of Copenhagen, Denmark
sebastian.holdum@nbi.dk

Frederik Ravn Klausen
Department of Mathematics, University of Copenhagen, Denmark
tlk870@alumni.ku.dk

Peter Michael Reichstein Rasmussen
Department of Mathematics, University of Copenhagen, Denmark
nmq584@alumni.ku.dk

Received: 7/18/14, Revised: 8/30/15, Accepted: 10/4/15, Published: 10/13/15

Abstract

It is an open problem whether $\binom{2n}{n}$ is divisible by 4 or 9 for all $n > 256$. In connection with this, we prove that for a fixed uneven m the asymptotic density of k's such that $m \nmid \binom{2^{k+1}}{2^k}$ is 0. To do so we examine numbers of the form α^k in base p, where p is a prime and $(\alpha, p) = 1$. For every n and a we find an upper bound on the number of k's less than a such that $(\alpha^k)_p$ contains less than n digits greater than $\frac{p}{2}$. This is done by showing that every sequence of the form $\langle \sigma_t, \ldots, \sigma_1, \sigma_0 \rangle$, where $0 \leq \sigma_i < p$ for $i \geq 1$ and σ_0 is in the residue class generated by α modulo p, occurs at specific places in the representation $(\alpha^k)_p$ as k varies.

1. Introduction

A well known conjecture by Erdős states that the central binomial coefficient $\binom{2n}{n}$ is never squarefree for $n > 4$. The problem was finally solved in 1996 by Granville and Ramaré [5], but is still inspiring further investigation of the central binomial coefficients. One question left unanswered can be found in *Concrete Mathematics* [4] and is the following conjecture, which is the starting point of this paper.

Conjecture 1.1. The central binomial coefficient $\binom{2n}{n}$ is divisible by 4 or 9 for every $n > 4$ except $n = 64$ and $n = 256$.

Since 4 divides $\binom{2n}{n}$ when n is not a power of 2, we consider only binomial coefficients of the form $\binom{2^{k+1}}{2^k}$ in our study of the conjecture. By Kummer's theorem, the greatest exponent of a prime p dividing the central binomial coefficient $\binom{2n}{n}$ is equal to the number of carries as n is added to itself in base p. Thus, to prove the conjecture it is sufficient to show that there are at least 2 carries when 2^k is added to itself in base 3 and $k > 8$.

In relation to this, Erdős conjectured in 1979 [2] that the base 3 representation of 2^k only omits the digit 2 for $k = 0, 2, 8$, noting that no methods for attacking it seemed to exist.

Methods for analysing the digits of powers of a number α in prime bases are scarce, and further developing such methods is what most of this paper will be concerned with.

Considering the periodicity of the base p representation of α^k, for a prime p and $(p, \alpha) = 1$, we find new patterns that allow us to bound the function

$$\mathcal{S}_p^n(a) = \#\left\{0 \leq s < a \mid (\alpha^s)_p \text{ contains less than } n \text{ digits greater than } \frac{p}{2}\right\}.$$

Specifically, we show that every sequence of the form $\langle \sigma_t, \ldots, \sigma_1, \sigma_0 \rangle$, where $0 \leq \sigma_i < p$ for $i \geq 1$ and σ_0 is in the residue class generated by α modulo p, occurs at given places in the representation $(\alpha^k)_p$ as k varies.

Interestingly, if p is not a Wieferich prime base α, it turns out that this system occurs on every digit of $(\alpha^k)_p$.

We use the above observations to show that

$$\mathcal{S}_p^n(a) \leq 8 \left(\log_p(a)\right)^{n-1} a^{\log_p\left(\frac{p+1}{2}\right)}, \tag{1}$$

and in special cases we improve results due to Narkiewicz [8], and Kennedy and Cooper [1]. The bound (1) is used to prove that for any odd $m \in \mathbb{N}$, the set of numbers k such that $m \nmid \binom{2^{k+1}}{2^k}$ has asymptotic density 0, which in the case $m = 9$ specifically addresses conjecture 1.1.

Lastly, we have used computer experiments to improve a result due to Goetgheluck [3] which confirmed Conjecture 1.1 for all $n \leq 2^{4.2 \cdot 10^7}$.

Theorem 1.2. *The central binomial coefficient $\binom{2n}{n}$ is divisible by 4 or 9 for every n such that $4 < n \leq 2^{10^{13}}$ except for $n = 64$ and $n = 256$.*

See the Appendix for source code.

2. Large Digits in Prime Bases

In this section we explore the base p representation of powers of an integer α, where p is a prime not dividing α. We say that a digit n is "small" if $n < \frac{p}{2}$ and "large" otherwise. Further, p will always denote an odd prime, and $\alpha > 1$ an integer with $(\alpha, p) = 1$.

The main goal of the section is to bound the following function in various ways.

Definition 2.1. Let p be an odd prime and $a, n \in \mathbb{N}$. Fix α such that $p \nmid \alpha$. Then set

$$\mathcal{S}_p^n(a) = \#\left\{0 \leq s < a \mid (\alpha^s)_p \text{ contains} < n \text{ large digits}\right\}.$$

Bounding the S_p^n is done by considering periodic properties of α^k in base p as k varies.

2.1. Notation and Definitions

Definition 2.2. Let p be a prime and $n, k \in \mathbb{N}$. We write $p^k \mid\mid n$ if $p^k \mid n$ and $p^{k+1} \nmid n$, i.e., if k is the greatest exponent of p dividing n.

Definition 2.3. We define the following:

- $\delta = \{\alpha^k \mod p \mid k \in \mathbb{Z}\}$, i.e. δ is the set of residues generated by α modulo p.
- $\theta = \#\{a \in \delta \mid 0 \leq a < \frac{p}{2}\}$, i.e. θ is the number of small residues in δ.
- $\gamma = \text{ord}_p(\alpha) = |\delta|$.

Definition 2.4. Let $n \in \mathbb{N}_0$. We let Λ_n denote the set of sequences of the form

$$\langle \sigma_n, \sigma_{n-1}, \ldots, \sigma_1, \sigma_0 \rangle,$$

where $\sigma_0 \in \delta$ and $0 \leq \sigma_i < p$ for $1 \leq i \leq n$.

Definition 2.5. Let $m \in \mathbb{N}$ be represented in base p as $m = \sum_{i \geq 0} a_i p^i$, where $0 \leq a_j < p$. To pinpoint specific digits we make the following definitions: $a_k = (m)_p[k]$ and $\langle a_k, \cdots, a_l \rangle = (m)_p[k:l], k \geq l$.

2.2. Sequences

We will now consider the representations $(\alpha^s)_p$ when s varies to show how members of Λ_k occur as subsequences of these representations.

First, we need a couple of lemmas.

Lemma 2.6. *Let p be an odd prime and $\alpha > 1$ be given such that $(p, \alpha) = 1$. Let further $p^t \mid\mid \alpha^{\gamma p^k} - 1$ for some $t > 0$ and $k \geq 0$. Then $p^{t+1} \mid\mid \alpha^{\gamma p^{k+1}} - 1$.*

Proof. Let $\alpha^{\gamma p^k} = up^t + 1$ with $(u, p) = 1$. Then

$$\alpha^{\gamma p^{k+1}} = \left(up^t + 1\right)^p = 1 + up^{t+1} + u^2 p^{2t} \binom{p}{2} + R,$$

where R is divisible by p^{3t} and thus divisible by p^{t+2} since $t > 0$. Further, $p \mid \binom{p}{2}$, so $p^{t+2} \mid u^2 p^{2t} \binom{p}{2}$ and we get

$$\alpha^{\gamma p^{k+1}} \equiv 1 + up^{t+1} \pmod{p^{t+2}},$$

showing that $p^{t+1} \mid\mid \alpha^{\gamma p^{k+1}} - 1$. $\square$

Lemma 2.7. *Let p be an odd prime and $\alpha > 1$ be given such that $(p, \alpha) = 1$. Assume that $p^\tau \mid\mid \alpha^\gamma - 1$. Then*

$$p^{\tau+k} \mid\mid \alpha^{\gamma p^k} - 1 \text{ and } \mathrm{ord}_{p^{\tau+k}}(\alpha) = \gamma p^k$$

for every $k \geq 0$.

Proof. The first part follows easily by induction on k using Lemma 2.6. For the second part, note that

$$\gamma = \mathrm{ord}_p(\alpha) \mid \mathrm{ord}_{p^{\tau+k}}(\alpha) \text{ and } \mathrm{ord}_{p^{\tau+k}}(\alpha) \mid \gamma p^k.$$

Thus, $\mathrm{ord}_{p^{\tau+k}}(\alpha) = \gamma p^r$ for some $r \leq k$. By the first part, we have $p^{\tau+k-1} \mid\mid \alpha^{\gamma p^{k-1}} - 1$, so $p^{\tau+k} \nmid \alpha^{\gamma p^{k-1}} - 1$ and we must have $\mathrm{ord}_{p^{\tau+k}}(\alpha) = \gamma p^k$. □

With these lemmas at hand we are ready to analyse the base p representation $(\alpha^s)_p$. To do so, we use the following definition.

Definition 2.8. Let $a = \ldots a_2 a_1 a_0$ be any integer represented by an infinite sequence $(a_i)_{i \in \mathbb{N}_0}$ in some base. Then we define

$$c_{\tau,k}(a) = \langle a_{\tau+k-1}, \ldots, a_{\tau+1}, a_\tau, a_0 \rangle.$$

We make this definition since our interest lies in the digits underlined here:

$$\ldots \underline{a_{\tau+k-1} \ldots a_\tau} \ldots a_1 \underline{a_0},$$

because all the elements of Λ_n will appear periodically as subsequences of $(\alpha^s)_p$ on these positions, when s changes. This is captured in the main theorem of the section.

Theorem 2.9. *Let p be an odd prime and $\alpha > 1$ be given such that $(p, \alpha) = 1$. Further, let $\tau > 0$ be the integer satisfying $p^\tau \mid\mid \alpha^\gamma - 1$. Then for any $k \geq 0$*

$$\left\{ c_{\tau,k}((\alpha^b)_p) \mid 0 \leq b < \gamma p^k \right\} = \Lambda_k.$$

Proof. Let $T := \left\{ c_{\tau,k}((\alpha^b)_p) \mid 0 \leq b < \gamma p^k \right\}$. Clearly, $T \subseteq \Lambda_k$ since every member of T is of the form $\langle \sigma_k, \sigma_{k-1}, \ldots, \sigma_1, \sigma_0 \rangle$, where $0 \leq \sigma_i < p$ for $1 \leq i \leq k$ and $\sigma_0 \in \delta$, because $(\alpha^b)_p[0] \in \delta$ for any $b \geq 0$.

We now prove $T = \Lambda_k$, by showing $|T| = \gamma p^k = |\Lambda_k|$, where the last equality already follows from the definition of Λ_k.

Since $p^\tau \mid\mid \alpha^\gamma - 1$ both $(\alpha^b)_p[\tau - 1 : 0]$ and $(\alpha^b)_p[0]$ are periodic with respect to b with least period γ and no repetitions in the period. This means that for $b, c \geq 0$ we have $(\alpha^b)_p[\tau - 1 : 0] = (\alpha^c)_p[\tau - 1 : 0]$ if and only if $(\alpha^b)_p[0] = (\alpha^c)_p[0]$.

Now, assume for contradiction that $c_{\tau,k}((\alpha^b)_p) = c_{\tau,k}((\alpha^c)_p)$ for some $0 \leq b < c < \gamma p^k$. Since $(\alpha^b)_p[0] = (\alpha^c)_p[0]$ we have $(\alpha^b)_p[\tau - 1 : 0] = (\alpha^c)_p[\tau - 1 : 0]$, so

$(\alpha^b)_p[\tau+k-1:0] = (\alpha^c)_p[\tau+k-1:0]$, i.e. $\alpha^b \equiv \alpha^c \pmod{p^{\tau+k}}$. Therefore, $p^{\tau+k} \mid \alpha^b(\alpha^{c-b}-1)$, but this means that $p^{\tau+k} \mid \alpha^{c-b}-1$ contradicting Lemma 2.7 since $0 < c-b < \gamma p^k$.

Thus, all the elements in the definition of T are different, and $|T| = \gamma p^k$. □

2.2.1. Wieferich Primes

The main result of the section has a curious corollary related to the Wieferich primes.

Definition 2.10. Let p be a prime and $\alpha > 1$ be given such that $(\alpha, p) = 1$. Then p is a Wieferich prime base α if $p^2 \mid \alpha^\gamma - 1$.

Since numerics [6] indicate that for any $\alpha > 1$ the Wieferich primes base α are somewhat scarce, it is interesting that the following elegant property holds for any (p, α) such that p is not a Wieferich prime base α.

Corollary 2.11. Let p be a prime which is not a Wieferich prime base α. Then

$$\left\{(\alpha^b)_p[k:0] \mid 0 \le b < \gamma p^k\right\} = \Lambda_k.$$

Proof. Since p is not a Wieferich prime base α, we have $p^1 \mid\mid \alpha^\gamma$. Noticing that $c_{1,k}(a) = a[k:0]$ the corollary follows directly from Theorem 2.9. □

Thus, p not being a Wieferich prime base α implies that the first $k+1$ digits of $(\alpha^s)_p$ will form all sequences of Λ_k periodically as s varies.

2.3. Bounds on $\mathcal{S}_p^n$

The findings of the previous section allow us to obtain various bounds on the function $\mathcal{S}_p^n$. First we introduce a lemma, which is a step on the way to bounding $\mathcal{S}_p^n$ for $n = 1$.

Lemma 2.12. *Let $s, t \ge 0$, p be a prime, and $\gamma = \operatorname{ord}_p(\alpha)$. Then we have*

$$\mathcal{S}_p^1(s\gamma p^t) \le s\theta\left(\frac{p+1}{2}\right)^t.$$

Proof. The number of sequences of Λ_t containing only small digits is $\theta\left(\frac{p+1}{2}\right)^t$. Thus, by Theorem 2.9 there are at most $\theta\left(\frac{p+1}{2}\right)^t$ integers $0 \le h < \gamma p^t$, such that $(\alpha^h)_p$ does not contain any large digits. Now, letting $p^\tau \mid\mid \alpha^\gamma - 1$ we have, by Lemma 2.7, that the last $\tau + t - 1$ digits of $(\alpha^h)_p$ are periodic with respect to h with least period γp^t and no repetition in the period. Thus,

$$\Lambda_t = \left\{c_{\tau,t}((\alpha^b)_p) \mid 0 \le b < \gamma p^t\right\} = \left\{c_{\tau,t}((\alpha^b)_p) \mid r\gamma p^t \le b < (r+1)\gamma p^t\right\}$$

for every $r \in \mathbb{N}_0$, and we can see that there are at most $\theta\left(\frac{p+1}{2}\right)^t$ integers $r\gamma p^t \leq h < (r+1)\gamma p^t$ such that $(\alpha^h)_p$ does not contain any large digits.

This yields

$$\mathcal{S}_p^1(s\gamma p^t) \leq s\theta\left(\frac{p+1}{2}\right)^t.$$

□

Now, the following theorem improves a result by Narkiewicz [8] by a constant factor.

Theorem 2.13. *Let* $\alpha \equiv 2 \pmod 3$ *in the definition of* $\mathcal{S}$*. For every* $a \in \mathbb{N}$ *we have* $\mathcal{S}_3^1(a) \leq 1.3a^{\log_3(2)}$.

Proof. The theorem obviously holds for $a = 1$. Now consider an $a \geq 2$, and let s, t be given such that $s \in \{1, 2\}$ and $s \cdot 2 \cdot 3^t \leq a \leq (s+1) \cdot 2 \cdot 3^t$. We now have

$$t \leq \log_3(a) - \log_3(2s),$$

and since S_3^1 clearly is weakly increasing and by Lemma 2.12, we get

$$\mathcal{S}_3^1(a) \leq \mathcal{S}_3^1\left((s+1) \cdot 2 \cdot 3^t\right) \leq (s+1) \cdot 2^t \leq (s+1) \cdot 2^{-\log_3(2s)} \cdot 2^{\log_3(a)}.$$

For $s \in \{1, 2\}$ the constant $(s+1) \cdot 2^{-\log_3(2s)}$ is maximised by $s = 1$, and so

$$\mathcal{S}_3^1(a) \leq 2 \cdot 2^{-\log_3(2)} \cdot 2^{\log_3(a)} \leq 1.3a^{\log_3(2)}.$$

□

The function $\mathcal{S}_m^1$ for $m > 2$ is studied by R. E. Kennedy and C. Cooper [1], and if we consider only the cases when m is a prime, we get the following improvement of their results, which replaces a factor increasing with m with a constant.

Theorem 2.14. *Let* p *be a prime and* α *arbitrary in the definition of* $\mathcal{S}$*. Then for all* $a \in \mathbb{N}$*, we have* $\mathcal{S}_p^1(a) \leq 4a^{\log_p\left(\frac{p+1}{2}\right)}$.

Proof. The theorem holds for $a < \gamma$ since $a < 4a^{\log_p\left(\frac{p+1}{2}\right)}$ for $a < p$.
Now let $a \geq \gamma$ and s, t be integers with $0 < s < p$ such that $s\gamma p^t \leq a < (s+1)\gamma p^t$. Now, $t \leq \log_p(a) - \log_p(s\gamma)$, and letting $\mu = \log_p\left(\frac{p+1}{2}\right)$ we get, by Lemma 2.12,

$$\begin{aligned}\mathcal{S}_p^1(a) \leq \mathcal{S}_p^1((s+1)\gamma p^t) \leq (s+1)\theta\left(\frac{p+1}{2}\right)^t &\leq (s+1)\theta\left(\frac{p+1}{2}\right)^{\log_p(a)-\log_p(s\gamma)} \\ &= (s+1)\theta\,(s\gamma)^{-\mu}\,a^{\mu}.\end{aligned}$$

Since $\theta \leq \gamma < p$ we get

$$\mathcal{S}_p^1(a) \leq \frac{s+1}{s^\mu}\gamma^{1-\mu}a^\mu \leq \frac{s+1}{s^\mu}p^{1-\mu}a^\mu = \frac{s+1}{s^\mu}\frac{2p}{p+1}a^\mu.$$

Considering $\frac{s+1}{s^\mu}$ we see that $\frac{d}{ds}\left(\frac{s+1}{s^\mu}\right) = s^{-\mu-1}(s(1-\mu)-\mu)$, and thus $\frac{s+1}{s^\mu}$ is strictly decreasing for $s \in \left[1, \frac{\mu}{1-\mu}\right)$ and strictly increasing for $s \in \left(\frac{\mu}{1-\mu}, p\right]$ and consequently attains its maximum on $[1,p]$ either at 1 or p. Since $s=1, s=p$ both yield $\frac{1+1}{1^\mu} = \frac{p+1}{p^\mu} = 2$, we get $\mathcal{S}_p^1(a) \le 4a^\mu$. □

Finally, we generalize our observations regarding $\mathcal{S}_p^n$.

Lemma 2.15. *Let $s \ge 0$, $t \ge 1$, p be a prime, and $\gamma = \operatorname{ord}_p(\alpha)$. Then we have*

$$\mathcal{S}_p^n(s\gamma p^t) \le 2s\gamma t^{n-1}\left(\frac{p+1}{2}\right)^t.$$

Proof. For $t=1$ the result is clear. Now, assume $t>1$.

First, we count the number of sequences $\eta \in \Lambda_t$ such that η contains less than n large elements. This is done by counting for each $i<n$ how many sequences $\eta \in \Lambda_t$ that contain exactly i large elements.

For each i we split up into two cases:

`Case 1:` The last element of η is large (which means $i>0$). This element can then be chosen in $\gamma-\theta$ ways, and there are $\binom{t}{i-1}\left(\frac{p-1}{2}\right)^{i-1}\left(\frac{p+1}{2}\right)^{t+1-i}$ ways to choose the remaining t elements such that exactly $i-1$ of them are large.

`Case 2:` The last element of η is small. This element can then be chosen in θ ways, and there are $\binom{t}{i}\left(\frac{p-1}{2}\right)^{i}\left(\frac{p+1}{2}\right)^{t-i}$ ways to choose the remaining t elements such that exactly i of them are large.

Thus, we can express the number of elements in Λ_t containing less than n large elements by

$$\begin{aligned}\sum_{i=1}^{n-1}(\gamma-\theta)\binom{t}{i-1}\left(\frac{p-1}{2}\right)^{i-1}\left(\frac{p+1}{2}\right)^{t+1-i} &+ \sum_{i=0}^{n-1}\theta\binom{t}{i}\left(\frac{p-1}{2}\right)^{i}\left(\frac{p+1}{2}\right)^{t-i}\\ &\le \gamma\left(\frac{p+1}{2}\right)^t \sum_{i=0}^{n-1}\binom{t}{i}\\ &\le \gamma\left(\frac{p+1}{2}\right)^t \sum_{i=0}^{n-1} t^i\\ &\le 2\gamma t^{n-1}\left(\frac{p+1}{2}\right)^t,\end{aligned}$$

since $t>1$.

Now, as in the proof of Lemma 2.12, we can conclude by Theorem 2.9 and Lemma 2.7 that for every $r \in \mathbb{N}_0$ there are at most $2\gamma t^{n-1}\left(\frac{p+1}{2}\right)^t$ integers $r\gamma p^t \le k < (r+1)\gamma p^t$ such that $(\alpha^k)_p$ contains less than n large digits. Thus, we have

$$\mathcal{S}_p^n(s\gamma p^t) \le 2s\gamma t^{n-1}\left(\frac{p+1}{2}\right)^t.$$

□

Theorem 2.16. *Let p be a prime and α arbitrary in the definition of $\mathcal{S}$. Then for all $a, n \in \mathbb{N}$, where $a \geq \gamma p$, we have $\mathcal{S}_p^n(a) \leq 8 \log_p(a)^{n-1} a^{\log_p\left(\frac{p+1}{2}\right)}$.*

Proof. Let $a \geq \gamma p$ be given, and s, t be integers with $0 < s < p$ and $t \geq 1$ such that $s\gamma p^t \leq a < (s+1)\gamma p^t$. Now, $t \leq \log_p(a) - \log_p(s\gamma)$, and letting $\mu = \log_p\left(\frac{p+1}{2}\right)$ we use Lemma 2.15 and the fact that $\frac{s+1}{s^\mu}\gamma^{1-\mu} \leq 4$ from the proof of Theorem 2.14 to get

$$\begin{aligned}
\mathcal{S}_p^n(a) &\leq \mathcal{S}_p^n\left((s+1)\gamma p^t\right) \\
&\leq 2(s+1)\gamma t^{n-1}\left(\frac{p+1}{2}\right)^t \\
&\leq 2(s+1)\gamma\left(\log_p(a) - \log_p(s\gamma)\right)^{n-1}\left(\frac{p+1}{2}\right)^{\log_p(a)-\log_p(s\gamma)} \\
&\leq 2(s+1)\gamma(s\gamma)^{-\mu}\log_p(a)^{n-1}a^\mu \\
&= 2\frac{s+1}{s^\mu}\gamma^{1-\mu}\log_p(a)^{n-1}a^\mu \\
&\leq 8\log_p(a)^{n-1}a^{\log_p\left(\frac{p+1}{2}\right)}.
\end{aligned}$$

□

3. Application to Central Binomial Coefficients

This section will apply the bounds on $\mathcal{S}$ to a generalisation of Conjecture 1.1 in order to show that the set of numbers not satisfying the conjecture restricted to the case $n = 2^s$ has asymptotic density 0.

For this we need the following theorem by Kummer.

Theorem 3.1 (Kummer [7]). *Let $n, m \geq 0$ and p be a prime. Then the greatest exponent of p dividing $\binom{n+m}{m}$ is equal to the number of carries, when n is added to m in base p.*

Further we define the following function:

Definition 3.2. Let $m \in \mathbb{N}$ be odd. Then we define

$$\mathcal{T}_m(a) = \#\left\{0 \leq s < a \,\middle|\, m \nmid \binom{2^{s+1}}{2^s}\right\}.$$

It is clear that to show Conjecture 1.1 we would have to bound $\mathcal{T}_9$ by $\mathcal{T}_9(a) \leq 5$ for all a. Instead we can get a partial result by connecting $\mathcal{T}$ and $\mathcal{S}$ in the following way:

Lemma 3.3. *Let $a, n \in \mathbb{N}$, $\alpha = 2$ in the definition of $\mathcal{S}$, and p be an odd prime. Then $\mathcal{T}_{p^n}(a) \le \mathcal{S}_p^n(a)$.*

Proof. Adding 2^s to itself in base p will yield at least one carry for every large digit in $(2^s)_p$. Thus, by Kummer's theorem, we must have $\mathcal{T}_{p^n}(a) \le \mathcal{S}_p^n(a)$. □

With this at hand, it is possible to give an asymptotic upper bound on $\mathcal{T}_m$ for every odd m.

Theorem 3.4. *Let $m > 1$ be odd and let p be the greatest prime dividing m. Then*

$$\mathcal{T}_m(a) = o\left(a^{\log_p\left(\frac{p+1}{2}\right)+\epsilon}\right)$$

for any $\epsilon > 0$.

Proof. Assume m has prime factorisation $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ with $p_1 < p_2 < \cdots < p_k$. Then $\mathcal{S}_{p_i}^{\beta_i}(a) = O\left(\log_{p_k}(a)^{\beta_k - 1} a^{\log_{p_k}\left(\frac{p_k+1}{2}\right)}\right)$ for all $1 \le i \le k$, since $p_i \le p_k$, and thus,

$$\mathcal{T}_m(a) \le \sum_{i=1}^{k} \mathcal{S}_{p_i}^{\beta_i}(a) = O\left(\log_{p_k}(a)^{\beta_k-1} a^{\log_{p_k}\left(\frac{p_k+1}{2}\right)}\right) = o\left(a^{\log_{p_k}\left(\frac{p_k+1}{2}\right)+\epsilon}\right)$$

for any $\epsilon > 0$. □

Although we still cannot give a definite answer to Conjecture 1.1, we do get the following corollary.

Corollary 3.5. For every odd m the set of integers s such that $m \nmid \binom{2^{s+1}}{2^s}$ has asymptotic density 0.

Proof. By Theorem 3.4 we have $\mathcal{T}_m(a) = o(a)$. □

Since the case $m = 9$ is not special in this corollary, it seems natural to pose the following conjecture, which strengthens Conjecture 1.1.

Conjecture 3.6. For every odd m there is an $N \in \mathbb{N}$ such that $m \mid \binom{2^{k+1}}{2^k}$ for every $k \ge N$.

It seems by Theorem 2.9 and by computer heuristics that the digits of $(2^s)_p$ are uniformly distributed for large s in the sense that for any $0 \le a < p$ most digits in the representation have probability roughly $1/p$ of being a.

Assuming such a random distribution of the digits in the representation and considering computer experiments on a selection of primes $p < 200$ has lead to the following conjecture.

Conjecture 3.7. For an odd prime, p, let $\epsilon_p(a)$ be the function satisfying $p^{\epsilon_p(a)} \mid\mid a$ for every a. Then

$$\epsilon_p\left(\binom{2^{k+1}}{2^k}\right) = \frac{\log(2)}{2\log(p)} \cdot k + O(\sqrt{k}).$$

Acknowledgement The authors wish to thank prof. Søren Eilers for his helpful guidance and suggestions in the writing process; prof. Carl Pomerance for his encouragement and support; and the anonymous referee for his/her suggestions that significantly improved some of the proofs of this paper.

References

[1] Cooper, C., Kennedy, R. E., A Generalization of a Result by Narkiewicz Concerning Large Digits of Powers, *Publ. Elektroteh. Fak., Univ. Beogr., Ser. Mat.* **11** (2000), 36–40.

[2] Erdős, P., Some Unconventional Problems in Number Theory, *Math. Mag.* **52** (1979), 67–70.

[3] Goetgheluck, P., On prime divisors of binomial coefficients, *Math. Comp.* **51** (1988), 325–329.

[4] Graham, R. L., Knuth, D., Patashnik, O., Concrete Mathematics, Second Edition, Addison-Wesley 2nd ed. 1998.

[5] Granville, A., Ramaré, O., Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients, *Mathematika* **43** (1996), 73–107.

[6] Keller, W., Richstein, J., Solutions of the Congruence $a^{p-1} \equiv 1 \pmod{p^r}$, *Math. Comp.* **74** (2004), 927–936.

[7] Kummer, E. E., Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146.

[8] Narkiewicz, W., A note on a paper of H. Gupta concerning powers of two and three, *Univ. Beograd. Publ. Elektrotechn. Fak. Ser. Mat.* **678–715** (1980), 173–174.

Appendix

The following code checks that the central binomial coefficient $\binom{2n}{n}$ is divisible by 4 or 9 for every n such that $4 < n \leq 2^{10^{13}}$ except for $n = 64$ and $n = 256$. The Java-code checks the first 35 digits of the base 3 representation of 2^k for every k such that $0 < k < 10^{13}$. Every k such that the first 35 digits of 2^k do not contain two 2's is written to a file containing special cases. These cases are then checked individually by the Python-code.

JAVA source

```java
import java.io.FileWriter;
import java.io.IOException;
import java.io.File;

class NewSearcher {
   private static int[] number = new int[35];
   private static int size = 0;
   private static final int MAX_SIZE = 35;

   private static final String ERROR_FILE = "Check_needed.txt";

   public static void main(String[] args) {
      deleteFile(ERROR_FILE);

      addNum(1);

      for (int a=0; a<10000000; a++) {
         for (int b=0; b<1000000; b++) {
            if (doubleIt()) {
               String output = String.format("%d%06d", a, b);
               System.out.println(output);
               writeNumberToFile(ERROR_FILE, output);
            }
         }
      }
   }

   private static void addNum(int num) {
      if (size < MAX_SIZE) {
         number[size] = num;
         size ++;
      }
   }

   public static boolean doubleIt() {
      int totalCarry = 0;
      int carry = 0;
      int i=0;

      while (totalCarry < 2 && i<size) {
         int res = (number[i]*2 + carry);
         carry = (res>=3) ? 1 : 0;
         number[i] = (res % 3);
         if (carry==1) totalCarry ++;
         i++;
      }
```

```
        while (i<size) {
            int res = (number[i]*2 + carry);
            carry = (res>=3) ? 1 : 0;
            number[i] = (res % 3);
            i++;
        }

        if (carry == 1) {
            addNum(1);
        }
        return (totalCarry<2);
    }

    public static void writeNumberToFile(String filename, String number)
         {
        try
        {
            FileWriter fw = new FileWriter(filename, true);
            fw.write(number + "\r\n");
            fw.close();
        }
        catch(IOException e)
        {
            System.out.println("IOException: " + e.getMessage());
        }
    }

    public static void deleteFile(String filename) {
        try {
            File toDelete = new File(filename);
            toDelete.delete();
        } catch (Exception e) {

        }
    }
}
```

Python source

```
def mod(n, md):
    if n < 10:
        return 2**n%md

    return 2**(n%2)*mod(n/2, md)**2%md

def checkCarry(n):
    tmp = n
    count = 0
    while tmp and count<2:
        if tmp%3 == 2:
            count += 1
        tmp /= 3

    return count<2

fil = file("Check_needed.txt", "r")

nls = []

while True:
    try:
        next = int(fil.readline())
        if checkCarry(mod(next, 3**50)):
            nls.append(next)
    except ValueError:
        break

for i in nls:
    if checkCarry(mod(i, 3**80)):
        print i
```