Journal of Integer Sequences, Vol. 18 (2015),
Article 15.6.1

Powers of Two Modulo Powers of Three

Michael Coons and Heath Winning
School of Mathematical and Physical Sciences
The University of Newcastle
Callaghan, NSW
Australia
Michael.Coons@newcastle.edu.au
Heath.Winning@uon.edu.au

Abstract

Since 2 is a primitive root of 3^m for each positive integer m, the set of points $\{(n, 2^n \bmod 3^m) : n \geqslant 0\}$, viewed as a subset of $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is bi-periodic, with minimal periods $\varphi(3^m)$ (horizontally) and 3^m (vertically). We show that if one considers the classes of n modulo 6, one obtains a finer structural classification. This result is presented within the context of the question of strong normality of Stoneham numbers.

1 Introduction

If m is a positive integer, it is quite clear that the set

$$\mathcal{T}_m := \{(n, 2^n \bmod 3^m) : n \geqslant 0\},$$

viewed as a subset of $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is bi-periodic. Indeed, since 2 is coprime to 3^m for any positive integer m, for any integers $x, y \geqslant 0$, we have

$$\mathcal{T}_m \subseteq \mathcal{T}_m - (\varphi(3^m)x, 3^m y), \tag{1}$$

where $\varphi(\cdot)$ denotes the standard Euler totient function.

The periodic structure given in (1) generalizes for all powers modulo any other power. What is so surprising about this result is that this simple observation is one of the few existing structural results concerning the modular distribution of the powers of a primitive root.

In this short note, we present a small improvement on this observation. We prove that *for m a positive integer, the set $\mathcal{T}_m$ is the union of six "smaller" bi-periodic subsets of $\mathbb{Z}_{\geqslant 0}\times\mathbb{Z}_{\geqslant 0}$*. In particular, we prove the following result.

Proposition 1. *For each positive integer m and each $k\in\{0,1,2,3,4,5\}$, the set*

$$\mathcal{L}=\mathcal{L}_{m,k}:=\left\{(6n+k,2^{6n+k}\bmod 3^m):n\geqslant 0\right\}$$

is non-trivially bi-periodic. That is, for each m and each k there exist distinct pairs of non-trivial vectors $\mathbf{u}:=\mathbf{u}_{m,k}$ and $\mathbf{v}:=\mathbf{v}_{m,k}$ with $\det(\mathbf{u},\mathbf{v})\neq 0$ such that for any point $P\in\mathcal{L}$ the points $P+\mathbf{u}$ and are $P+\mathbf{v}$ are also in $\mathcal{L}$.

Note that the condition $\det(\mathbf{u},\mathbf{v})$ (the determinant of the matrix with rows $\mathbf{u}$ and $\mathbf{v}$) is nonzero ensures that the vectors $\mathbf{u}$ and $\mathbf{v}$ are not multiples of each other.

Before going on to the proof of Proposition 1, we give an example, in the form of figures, which illustrate our proposition as well as some context for our result.

To this end, note that set $\mathcal{T}_m$ has a fundamental region; the finite set

$$\{(n,2^n\bmod 3^m)\}_{0\leqslant n<\varphi(3^m)},$$

where we identify only the residue $2^n \bmod 3^m$ in the interval $[1,3^m]$, is the 'repeating part' of $\mathcal{T}_m$. For $m=7$, this fundamental region is the large plot in Figure 1. Proposition 1 gives that this fundamental region of $\mathcal{T}_m$ can be separated into six pieces each having a 'smaller' fundamental region, but which union to give $\mathcal{T}_m$. This is illustrated in Figure 1, where we have placed the large fundamental region next to the six smaller ones.

We now provide some context for Proposition 1. In fact, we stumbled upon this structure while studying the statistical properties of the binary expansion of a certain real number, which is considered quite 'random'. Classifying randomness in base expansions goes back at least to Borel [7] who defined the concept of normality.

A real number ξ is called *normal to the base b* (or *b–normal*) if, for any positive integer n, each of the b^n blocks of length n on the alphabet $\{0,1,\ldots,b-1\}$ occurs in the base-b expansion of ξ with equal frequency $1/b^n$. The canonical example of a normal number was given by Champernowne [8], who showed that the number

$$C_{10}:=\ 0.12345678910111213\cdots,$$

obtained by concatenating the natural numbers, is normal to the base 10. Of course, Champernowne's number is by no means random and should fail any true test of randomness. Thus normality, while a necessary property of a random number, is not sufficient. A stronger version of normality was recently introduced by Belshaw and P. Borwein [6].

Write $(\xi)_b:=0.a_0a_1a_2a_3\cdots$, and set $m_k(n):=\#\{i:a_i=k,i\leqslant n\}$. If the digits of ξ are chosen at random in the base b, the *asymptotic frequency* $m_k(n)/n$ of each 1-string approaches $1/b$ with probability 1. However, the *discrepancy* $m_k(n)-n/b$ does not approach any limit, but fluctuates. Using the law of the iterated logarithm, Belshaw and P. Borwein [6]

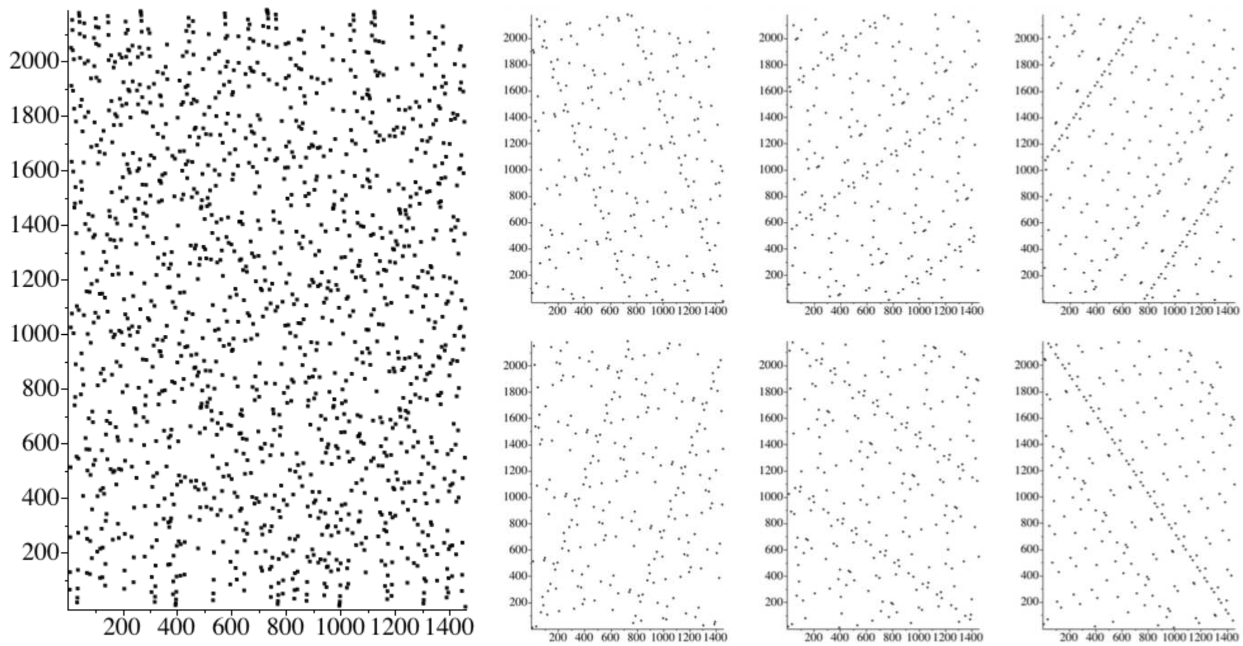

Figure 1: The large plot is the fundamental region of $\mathcal{T}_7$ and the smaller plots from left to right, in the top and bottom row, are the points $(n, 2^n \bmod 3^7)$ for $n \equiv 0, 1, 2 \pmod 6$ and $n \equiv 3, 4, 5 \pmod 6$, respectively.

define the real number ξ to be *simply strongly normal* to the base b if for each $0 \leqslant k \leqslant b-1$, one has

$$\liminf_{n\to\infty} \frac{m_k(n) - n/b}{\sqrt{2n \log\log n}} = -\frac{\sqrt{b-1}}{b} \quad \text{and} \quad \limsup_{n\to\infty} \frac{m_k(n) - n/b}{\sqrt{2n \log\log n}} = \frac{\sqrt{b-1}}{b}.$$

We say that the real number ξ is *strongly normal* to the base b, if it is simply strongly normal to the base b^j for each integer $j \geqslant 1$. Using this definition, Belshaw and P. Borwein [6] showed that Champernowne's number is not simply strongly normal. Belshaw and P. Borwein also showed that almost all numbers are simply strongly normal, in terms of Lesbegue measure, though no (reasonable) number has been proven to satisfy the definition. Considering potential examples, Aragón Artacho et al. [1] conjectured that the Stoneham number $\alpha_{2,3} := \sum_{n\geqslant 1} \frac{1}{3^n 2^{3^n}}$ is strongly normal to the base 2. Proposition 1 is an outcome of our attack on this conjecture.

Stoneham numbers have a rich history. Stoneham [10] proved that if b is a primitive root of c^2 for c an odd prime, then the number

$$\alpha_{b,c} = \sum_{n\geqslant 1} \frac{1}{c^n b^{c^n}}$$

is normal to the base b; the 2-normality of $\alpha_{2,3}$ follows from Stoneham's result since 2 is a primitive root of 9. A much simpler proof of the 2-normality of $\alpha_{2,3}$ was given by Bailey and Misiurewicz [5]. Bailey and Crandall [4] generalized Stoneham's result by showing that $\alpha_{b,c}$ is b-normal for coprime integers $b, c \geqslant 2$.

Instead of $\alpha_{2,3}$, we considered the closely related concatenated binary number

$$w := 0.w_1 w_2 w_3 \cdots w_m \cdots$$

with each word, w_m, defined as the minimal periodic part of $(1/3^m)_2$ (the binary expansion of $1/3^m$) for integers $m \geqslant 1$. Coons [9] explains the similarity between w and $\alpha_{2,3}$. Coons [9] also provides a division algorithm to compute w_m in the desired form, and it is in the application of this algorithm that we find the orbit of the powers of 2 modulo 3^m. If one had enough information about this orbit, one could answer the question of strong normality surrounding both w and $\alpha_{2,3}$. Proposition 1 is a step toward this goal.

Remark 2. It is worth noting that strong normality is different from absolute normality. A real number is *absolutely normal* provided it is b-normal for all integers $b \geqslant 2$. The Stoneham number $\alpha_{2,3}$, while conjectured strongly normal to the base 2, is not absolutely normal. Bailey and J. Borwein [3] proved that $\alpha_{2,3}$ is not normal to the base 6. In fact, their result is much more general than this; they showed that for coprime integers $b, c \geqslant 2$, the number $\alpha_{b,c}$ is not bc-normal. Bailey and J. Borwein [2] later generalized this by showing that $\alpha_{b,c}$ is not B-normal for infinitely many distinct integers B.

Remark 3. Our computations suggest that w (and so also $\alpha_{2,3}$) is unlikely to be strongly normal to the base 2. In fact, it seems to be 'too good' in some sense, but the evidence is not strong enough to be conclusive. We had hoped the results given here would provide the tools to settle this, however, Proposition 1 does not provide enough structure to make any real progress on this difficult question.

2 Proof of Proposition 1

Proof of Proposition 1. We will show that the fundamental regions of $\mathcal{L} = \mathcal{L}_{m,k}$ are invariant when shifted in two different directions; that is there are small vectors (or points if you like) $\mathbf{u}$ and $\mathbf{v}$ (dependent on m and k), such that for any point $P \in \mathcal{L}$, we have also $P+\mathbf{u}, P+\mathbf{v} \in \mathcal{L}$. In other words, the fundamental region of each $\mathcal{L}$ exists and is smaller than that of $\mathcal{T}_m$. In the course of our proof, we provide an explicit description of the vectors $\mathbf{u}$ and $\mathbf{v}$.

We find it convenient to consider both periods as the horizontal component increases (i.e., moving to the right) and also to split the repeated lengths into two cases that will be assessed separately, small and large—inspiring the $\mathbf{u}$-$\mathbf{v}$ distinction.

Case 1: the small vectors u.

First take $m \geqslant 4$ and $r = r(k) \in \{1, 2, 3\}$. Then the small period requires the addition of the vector $\mathbf{u} = (2^r 3^{m-3}, \varepsilon 3^{m-2})$, where ε takes the value $+1$ for $k \in \{0, 1, 2\}$ and the value

-1 for $k \in \{3,4,5\}$. We write

$$P + \mathbf{u} = \left(6n + k + 2^r 3^{m-3}, 2^{6n+k} + \varepsilon 3^{m-2} \bmod 3^m\right)$$

and look at the horizontal component

$$6n + k + 2^r 3^{m-3} = 6\left(n + 2^{r-1}3^{m-4}\right) + k = 6\ell + k.$$

We show that this ℓ gives the required form in the vertical component.

Of course, this reduces to the task of confirming that there is some $T \in \mathbb{Z}$ such that the following rearrangement

$$2^{6n+k} + \varepsilon 3^{m-2} \bmod 3^m = 2^{6\ell+k} \bmod 3^m = 2^{6\left(n+2^{r-1}3^{m-4}\right)+k} - 3^m T$$

can always be done. Some rearrangement gives

$$\frac{2^{6n}2^k\left(2^{2^r 3^{m-3}} - 1\right)}{3^{m-2}} - \varepsilon = 3^2 T.$$

We note that this is equivalent to a statement modulo 3^2, and since $2^6 \equiv 1 \pmod{3^2}$, the factor 2^{6n} will not effect the solubility; we may thus ignore it completely. We now have an equation whose solubility can proved using induction on $m \geqslant 4$, namely

$$\frac{2^k\left(2^{2^r 3^{m-3}} - 1\right)}{3^{m-2}} = 3^2 T + \varepsilon. \tag{2}$$

It is straightforward to check that the base case $m = 4$ follows under the following parameters depending on k:

k	0	1	2	3	4	5
r	3	2	1	3	2	1
ε	$+1$	$+1$	$+1$	-1	-1	-1
T	207126	101	3	1657009	809	25.

Now assume that (2) has a solution for a given m and note that

$$2^{2^r 3^{(m+1)-3}} = \left(2^{2^r 3^{m-3}}\right)^3 = \left(\frac{3^{m-2}\left(3^2 T + \varepsilon\right)}{2^k} + 1\right)^3.$$

Then, expanding out the cube, we have

$$\begin{aligned}\frac{2^k\left(2^{2^r 3^{m-2}} - 1\right)}{3^{m-1}} &= \frac{2^k}{3^{m-1}}\left(\frac{\left(3^2T+\varepsilon\right)^3 3^{3m-6}}{2^{3k}} + \frac{\left(3^2T+\varepsilon\right)^2 3^{2m-3}}{2^{2k}} + \frac{\left(3^2T+\varepsilon\right)3^{m-1}}{2^k}\right)\\ &= \frac{\left(3^2T+\varepsilon\right)^3 3^{2m-5}}{2^{2k}} + \frac{\left(3^2T+\varepsilon\right)^2 3^{m-2}}{2^k} + 3^2T + \varepsilon.\end{aligned}$$

From the induction hypothesis, we have $(3^2T+\varepsilon)3^{m-2} = 2^k(2^{2^r 3^{m-3}-1})$, and so for some $d \in \mathbb{Z}$, we have $3^2T + \varepsilon = d \cdot 2^k$. Thus $(3^2T+\varepsilon)^3 = d^3 2^{3k} = A \cdot 2^{2k}$ and $(3^2T+\varepsilon)^2 = d^2 2^{2k} = B \cdot 2^k$, for some $A, B \in \mathbb{Z}$, so that

$$\frac{2^k\left(2^{2^r 3^{m-2}} - 1\right)}{3^{m-1}} = A \cdot 3^{2m-5} + B \cdot 3^{m-2} + 3^2T + \varepsilon = 3^2\left(A \cdot 3^{2m-7} + B \cdot 3^{m-4} + T\right) + \varepsilon$$

is an integer of the desired form. Thus $P + \mathbf{u} \in \mathcal{L}$, which establishes the small vector case.

Case 2: the large vectors v.

For this case, we require two subcases, each following in the same spirit as the first case.

Case 2a: when $k \in \{1, 2, 4, 5\}$. We begin with $m \geqslant 2$ and take $\mathbf{v} = (2^r 3^{m-2}, \varepsilon 3^{m-1})$ where the ε takes the value $+1$ or -1 depending on the value of k (to be described later). As in Case 1, we look at the horizontal component of

$$P + \mathbf{v} = \left(6n + k + 2^r 3^{m-2}, 2^{6n+k} + \varepsilon 3^{m-1} \bmod 3^m\right),$$

which, as before, defines the quantity ℓ as

$$6\left(n + 3^{m-3}\right) + k = 6\ell + k.$$

Again as before, we show that this ℓ gives the required form of the vertical component.

As previously, this reduces to the task of confirming that there is some $T \in \mathbb{Z}$ such that the rearrangement

$$2^{6n+k} + \varepsilon 3^{m-1} \equiv 2^{6\left(n+3^{m-3}\right)+k} \pmod{3^m} = 2^{6\left(n+3^{m-3}\right)+k} + 3^m T,$$

can always be made. Rearranging, we have

$$\frac{2^{6n}2^k\left(2^{2^r 3^{m-2}} - 1\right)}{3^{m-1}} = 3T + \varepsilon,$$

so that, omitting the 2^{6n} as before, this becomes

$$\frac{2^k\left(2^{2^r 3^{m-2}} - 1\right)}{3^{m-1}} = 3T + \varepsilon. \tag{3}$$

We prove induction to show solubility. Again, it is straightforward to check that the base case $m = 2$ follows using the following parameters depending on k in (3);

k	1	2	4	5
r	1	2	1	2
ε	-1	-1	$+1$	$+1$
T	1	7	5	53

Now assuming (3) has a solution for a given m, and noting that

$$2^{2^r 3^{m-1}} = \left(2^{2^r 3^{m-2}}\right)^3 = \left(\frac{(3T+\varepsilon)\,3^{m-1}}{2^k} + 1\right)^3,$$

we have

$$\begin{aligned}\frac{2^k\left(2^{2^r 3^{m-1}} - 1\right)}{3^m} &= \frac{2^k}{3^m}\left(\frac{(3T+\varepsilon)^3\,3^{3m-3}}{2^{3k}} + 3\frac{(3T+\varepsilon)^2\,3^{2m-2}}{2^{2k}} + 3\frac{(3T+\varepsilon)\,3^{m-1}}{2^k}\right)\\ &= \frac{(3T+\varepsilon)^3\,3^{2m-3}}{2^{2k}} + \frac{(3T+\varepsilon)^2\,3^{m-1}}{2^k} + 3T + \varepsilon.\end{aligned}$$

The induction hypothesis gives that $2^k \mid (3T+\varepsilon)$, which allows us to write $(3T+\varepsilon)^3\,3^{2m-3} = C \cdot 2^{2k} 3^{2m-3}$ and $(3T+\varepsilon)^2\,3^{m-1} = D \cdot 2^k 3^{m-1}$ for some $C, D \in \mathbb{Z}$. Thus

$$\frac{2^k\left(2^{2^r 3^{m-1}} - 1\right)}{3^m} = 3\left(C \cdot 3^{2m-4} + D \cdot 3^{m-2} + T\right) + \varepsilon$$

is an integer of the desired form and so $P + \mathbf{v} \in \mathcal{L}$.

Case 2b: when $k \in \{0, 3\}$. We now take $m \geqslant 4$ and $\mathbf{v} = (2 \cdot 3^{m-3}, \varepsilon \cdot 2 \cdot 3^{m-2})$, where the ε takes the value $+1$ or -1 depending on the value of k. Then we have

$$P + \mathbf{v} = \left(6\left(n + 3^{m-4}\right) + k, 2^{6n+k} + \varepsilon \cdot 2 \cdot 3^{m-2} \mod 3^m\right),$$

where we now wish to express the vertical component as

$$2^{6n+k} + \varepsilon \cdot 2 \cdot 3^{m-2} \equiv 2^{6\left(n+3^{m-4}\right)+k} \pmod{3^m}.$$

Since $\gcd(2,3) = 1$, we can divide both sides by 2 and then rearrange to give

$$\frac{2^{6n+k-1}\left(2^{2\cdot 3^{m-3}} - 1\right)}{3^{m-2}} = 3^2 T + \varepsilon.$$

Now we can remove a $2^{6(n-1)}$ by the same method as in Case 1, and so we have only to prove that

$$\frac{2^{k+5}\left(2^{2\cdot 3^{m-3}} - 1\right)}{3^{m-2}} = 3^2 T + \varepsilon$$

is true for all $m \geqslant 4$. But this is exactly what we proved in the first case (with $k = 2, 5$), and so we can have $P + \mathbf{v} \in \mathcal{L}$.

A straightforward comparison of the r values for the various $\mathbf{u}$-$\mathbf{v}$ pairs shows that $\det(\mathbf{u}, \mathbf{v}) \neq 0$, which completes our proof. $\square$

3 Acknowledgments

The authors thank the anonymous referee for comments that greatly improved the exposition of this paper. The research of M. Coons was supported by Australian Research Council grant DE140100223 and the research of H. Winning was supported by a Summer Research Scholarship from the Priority Research Centre for Computer-Assisted Research Mathematics and its Applications.

References

[1] Francisco J. Aragón Artacho, David H. Bailey, Jonathan M. Borwein, and Peter B. Borwein, Walking on real numbers, *Math. Intelligencer* **35** (1) (2013), 42–60.

[2] David H. Bailey and Jonathan M. Borwein, Nonnormality of Stoneham constants, *Ramanujan J.* **29** (2012), 409–422.

[3] David H. Bailey and Jonathan M. Borwein, Normal numbers and pseudorandom generators. In *Computational and Analytical Mathematics*, Vol. 50 of *Springer Proc. Math. Stat.*, Springer, 2013, pp. 1–18.

[4] David H. Bailey and Richard E. Crandall, Random generators and normal numbers, *Experiment. Math.* **11** (2002), 527–546 (2003).

[5] David H. Bailey and Michał Misiurewicz, A strong hot spot theorem, *Proc. Amer. Math. Soc.* **134** (2006), 2495–2501.

[6] Adrian Belshaw and Peter Borwein, Champernowne's number, strong normality, and the X chromosome. In *Computational and Analytical Mathematics*, Vol. 50 of *Springer Proc. Math. Stat.*, Springer, 2013, pp. 29–44.

[7] E. Borel, Les probabilités denombrables et leurs applications arithmétiques, *Palermo Rend.* **27** (1909), 247–271.

[8] D. G. Champernowne, The construction of decimals normal in the scale of ten, *J. London Math. Soc.* **8** (1933), 254–260.

[9] Michael Coons, An arithmetical excursion via Stoneham numbers, *J. Aust. Math. Soc.* **96** (2014), 303–315.

[10] R. G. Stoneham, A general arithmetic construction of transcendental non-Liouville normal numbers from rational fractions, *Acta Arith.* **16** (1969/1970), 239–253.

2010 *Mathematics Subject Classification*: Primary 11A07 Secondary 11A63.
Keywords: primitive root, strong normality, normality.

(Concerned with sequences A000079 and A000244.)

Received May 11 2015; revised version received May 18 2015. Published in *Journal of Integer Sequences*, May 29 2015.

Return to Journal of Integer Sequences home page.