A few years later, he was dead, and Bondi had left the NERC to become Master of Churchill College.

10.1017/mag.2018.10

ROBIN T. CLARKE
Avenida Venâncio Aires 1001/704, Porto Alegre - RS, Brazil
e-mail: *clarke@iph.ufrgs.br*

102.02 Minimal sets for congruence classes

Introduction

A natural number x is said to be a *subsequence* of another natural number y if $x = y$ or if x can be formed by deleting one or more digits from the decimal representation of y. When this occurs, we write $x \lhd y$.

Let S be a subset of $\mathbb{N}$. A minimal element of S is one which has no subsequence other than itself in S. The minimal set $\mathcal{M}(S)$ is defined to be the set of minimal elements of S. For example,

$$\mathcal{M}(\mathbb{N}) = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\},$$
$$\mathcal{M}(2\mathbb{N}) = \{2,\ 4,\ 6,\ 8,\ 10,\ 30,\ 50,\ 70,\ 90\}.$$

Minimal sets were discussed in [1], which included important references to [2] and [3]. A theme of [1] and of the related article [4] was the difficulty of proving anything 'structural' about minimal sets and the reader was challenged to obtain such a result.

On this point, the following can be claimed as an elementary but clearly structural result which holds for all sets of natural numbers

$$\mathcal{M}(A \cup B) = \mathcal{M}\big(\mathcal{M}(A) \cup \mathcal{M}(B)\big).$$

This result can help a little in finding some minimal sets. However, the purpose of this Note is to examine minimal sets for congruence classes. For these minimal sets we shall discover some much more interesting structural relationships and use these to prove a result conjectured by Martin Kreh [4]. It may be of additional interest that this is an effective proof of Higman's Lemma [2], for these sets.

Congruence classes

Henceforth in this paper, let $m \in \mathbb{N}$ and $a \in \mathbb{Z}, 0 \leqslant a < m$.

Define $[a]_m$ to be the set of natural numbers congruent to a modulo m and let $\mathcal{M}$ be the minimal set for $[a]_m$.

Minimal sets for various congruence classes are found in [1] and [2]. For example,

$$a = 1, m = 4 \qquad \mathcal{M} = \{1,\ 5,\ 9,\ 33,\ 37,\ 73,\ 77\},$$
$$a = 2, m = 5 \qquad \mathcal{M} = \{2,\ 7\}.$$

In these examples the elements of $\mathcal{M}$ are relatively small. However, as a simple example of how to produce large elements, choose m to be a prime with 10 as a primitive root and let $a = 10^{m-2}$. The elements 10^i,

https://doi.org/10.1017/mag.2018.11 Published online by Cambridge University Press

$0 \leqslant i \leqslant m - 2$, are all distinct modulo m, and so a is the only one of these elements in $[a]_m$. Therefore $\mathcal{M}$ contains the $m - 1$ digit number a.

The maximal number of digits in $\mathcal{M}$ for some m are as shown in the following table, which uses results from [4].

	Maximum number of digits	
m	$a \neq 0$	$a = 0$
2	1	2
3	2	3
4	2	3
5	1	2
6	3	4
7	6	7
8	3	4
9	8	9
10	1	2
11	10	6
12	4	5
13	9	10
14	7	8
15	3	4
16	4	5
17	16	17
18	9	10
19	18	19
20	2	3
21	11	11

The results in this table indicate that there is some underlying structure which should be capable of investigation and explanation. Perhaps the two most obvious observations are that:

- the maximal number of digits is always less than or equal to m;
- for $a \neq 0$, the maximal number of digits is always less than m and tends to be 1 less than the maximal number for $a = 0$.

These are the observations which we shall concentrate on in this paper but there are plenty of other avenues for the interested reader to explore.

https://doi.org/10.1017/mag.2018.11 Published online by Cambridge University Press

Patterns in congruence classes

Before proving a general result on minimal sets for congruence classes, we shall introduce a simple way of grouping together different elements of a congruence class which will prove extremely useful in exploring what makes an element of a congruence class minimal or otherwise.

Consider, for example, $a = 0$ and $m = 7$. We can consider a member of the congruence class such as 993 006 to have been formed by a gradual building-up process as shown.

$$\begin{aligned} 8 \times 7 &= 56 \\ 58 \times 7 &= 406 \\ 858 \times 7 &= 6006 \\ 1858 \times 7 &= 13006 \\ 41858 \times 7 &= 293006 \\ 141858 \times 7 &= 993006 \end{aligned}$$

Ignore, for the moment, all the other multiples of 7 and just consider the structure of these numbers. Some of the features which should be noted are as follows.

- The numbers which are highlighted form a chain with each a subsequence of the next.
- The numbers which are not highlighted, that is, 5, 4, 6, 1, 2 and (0), are all residues modulo 7.
- The six multiples of 7 would have included one as a subsequence of another if two of the residues had been equal.
- If the pattern of these six multiples were continued, the seventh number would have to contain 993006 as a subsequence.

The patterns noted above are what motivated the following proof, where the c_l correspond to the highlighted numbers and the b_l to the residues.

Theorem: (conjectured by Kreh)

Each element of $\mathcal{M}$ can have at most m digits.

Proof: Consider an element of $\mathcal{M}$ expressed as

$$a + m \sum_{i=1}^{L} x_i 10^{i-1},$$

where the x_i are digits and $x_L \neq 0$.

For $1 \leqslant l \leqslant L$, define integers a_l, b_l and c_l, with $0 \leqslant b_l < m$ and $c_l < 10^l$, by

$$a_l = a + m \sum_{i=1}^{L} x_i 10^{i-1} = b_l 10^l + c_l.$$

Then $a_L \in \mathcal{M}$ and we must prove that a_L has at most m digits.

https://doi.org/10.1017/mag.2018.11 Published online by Cambridge University Press

For $k < l$, $c_l \equiv c_k \pmod{10^k}$ so c_k is a subsequence of c_l. Therefore

$$c_1 \lhd c_2 \lhd \ldots \lhd c_L.$$

Now suppose that $b_k = b_l$. Then, for some integer t,

$$\begin{aligned} a_L &= a_l + mt10^l \\ &= (b_l + mt)10^l + c_l \\ &= (b_k + mt)10^l + c_l. \end{aligned}$$

Then $a_k + mt10^k = (b_k + mt)10^k + c_k$ would be a subsequence of a_L, a contradiction.

Therefore $\{b_l \mid 1 \leqslant l \leqslant L\}$ contains L distinct integers between 0 and $m - 1$. Furthermore, for $l < L$, if b_l was a subsequence of b_L then we would have the contradiction that $a_l = b_l10^l + c_l$ would be a subsequence of $a_L = b_L10^L + c_L$. In particular, we know that $b_l \neq 0$.

If $b_L = 0$, then a_L has at most $L \leqslant m$ digits. We can therefore suppose the decimal representation of b_L to be the string $u_1u_2\ldots u_d$, for some integer $d > 0$ and then a_L has $L + d$ digits. None of the L integers in $\{b_l\}$ can be 0 or one of the $d - 1$ integers with associated strings $u_1, u_1u_2, \ldots, u_1u_2\ldots u_{d-1}$. Therefore $L \leqslant m - d$ and a_L has at most m digits, as required.

This theorem can be strengthened under various conditions on a and m. Here we shall just consider $a \neq 0$.

Corollary: If $a \neq 0$, each element of $\mathcal{M}$ can have at most $m - 1$ digits.

Proof: If $a \neq 0$, then we can set $b_0 = a$. The proof of the Theorem then goes through as before but now with the extra restriction that no other b_l is able to equal a.

Final remarks

The main reason for an apparent lack of structure in minimal sets stems from the fact that, for x to be a subsequence of y, digits can be deleted from various different places inside the decimal representation of y. Our proof that each element of $\mathcal{M}$ can have at most m digits depended upon concentrating on the much more restrictive idea of deleting a single block of digits.

This proof explains some of the important regularities in the table of maximum numbers of digits whilst the possibility of further, less regulated, deletions must be invoked to explain other features shown in the table.

There is much more to be investigated concerning the patterns in congruence classes. In particular, it is possible to classify all the cases where $\mathcal{M}$ has an element with m digits and a proof is available by email from the author.

https://doi.org/10.1017/mag.2018.11 Published online by Cambridge University Press

Acknowledgement

The author thanks the referee for the careful reading of the manuscript and for the positive and helpful suggestions.

References

1. I. N. Baoulina, M. Kreh, J. Steuding, Deleting digits, *Math. Gaz.* **101** (March 2017) pp. 60-68.
2. G. Higman, Ordering by divisibility in abstract algebras, *Proc. London Math. Soc.* **2** (1952) pp. 326-336.
3. J. O. Shallit, Minimal primes, *J. Recreational Math.* **30** (2000) pp. 113-117.
4. M. Kreh, Minimal sets, *Journal of Integer Sequences*, **18** (2015) Article 15.5.3.

10.1017/mag.2018.11

STAN DOLAN
126A Harpenden Road, St Albans, AL3 6BZ
e-mail: *stan@standolan.co.uk*

102.03 When quadratic residues are squares

Introduction

When a square is divided by 12, the possible remainders of 0, 1, 4 and 9 are themselves squares.

A table of squares modulo n, for small values of n, shows that the bases 1, 2, 3, 4, 5 and 8 have the same property as 12.

n	Squares modulo n
1	0
2	0, 1
3	0, 1
4	0, 1
5	0, 1, 4
6	0, 1, 3, 4
7	0, 1, 2, 4
8	0, 1, 4
9	0, 1, 4, 7
10	0, 1, 4, 5, 6, 9
11	0, 1, 3, 4, 5, 9
12	0, 1, 4, 9

https://doi.org/10.1017/mag.2018.11 Published online by Cambridge University Press