Extended Essay

Mathematics

How can we systematically characterize the divisibility rules in base-10 that would then allow us to generalize and find the divisibility rules in any base-n number system?

Topic : Number Theory & Modular Arithmetic

Word Count : 3939

Table of Contents

1. Introduction………………………………………………………………...……. 1

1.1. Introduction………..………………………………………………….…...… 1

1.2. Modular Arithmetic…………………………………...……….……...…. 3

1.3. Number Systems…………..……………………………….…………..... 7

1.4. More Definitions……………………………………………………………8

2. Divisibility rules in Decimal…………………………………………………….... 9

2.1. For 2, 5 and 10……………………………………………………….... 9

2.2. For 2^m, 5^m and 10^m……………………………………………………... 11

2.3. For 3 and 9………………………………………………………..……….... 13

2.4. For 11……………………………………………………………..……… 15

2.5. For 7 and 13……………………………………………………………..... 17

3. Divisibility rules in Non-Decimal……………………………………………... 18

3.1. For n^m & factors of n^m…………………………………………….…..... 18

3.2. For when $n^m \equiv 1 \pmod{p}$…………………………………………….……... 22

3.3. For when $n^m \equiv \pm1 \pmod{p}$……………………………………………...…... 24

4. Generalized Divisibility Rule…………………………………………..……..... 25

4.1. Formulating the Generalized Divisibility Rule……………………...……...25

4.2. Example of Generalized Divisibility Rule……………………………………..30

5. Conclusion……………………………………………………………………..... 32

6. Bibliography…………………………………………………..……………….....33

7. Appendix……………………………………………..………………….………... 34

7.1. Code used in Extended Essay…………………………………………….…… 34

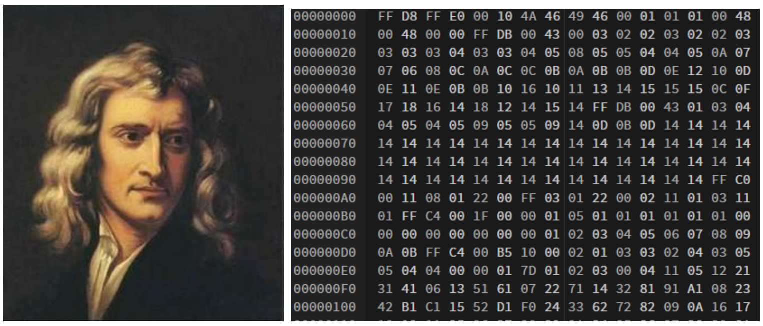
7.2. Data Generated using Code………………………………………………...… 36

1. Introduction

1.1. Introduction

Many students were taught a simple trick to determine if a number is divisible by 3, that is, if and only if the sum of the digits is divisible by 3. Back then, I also looked into whether these 'tricks' existed for other numbers, and of course they did. These tricks were called divisibility rules, and I memorised the rules for divisibility from 2 to 11, although I never bothered to understand their proofs, assuming that they worked just because they did.

A few years later when I picked up on the hobby of programming, I learned about how the numbers we use in everyday life are in the decimal number system, meaning that the numbers have 10 digits, 0 to 9, and that there are also infinitely many other number systems for all positive integers, although the only other number systems that have some sort of usage are computer bytes represented in Binary and Hexadecimal bases, or base-2 and base-16, respectively.



```
00000000   FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48
00000010   00 48 00 00 FF DB 00 43 00 03 02 02 03 02 02 03
00000020   03 03 03 04 03 03 04 05 08 05 05 04 04 05 0A 07
00000030   07 06 08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D
00000040   0E 11 0E 0B 0B 10 16 10 11 13 14 15 15 15 0C 0F
00000050   17 18 16 14 18 12 14 15 14 FF DB 00 43 01 03 04
00000060   04 05 04 05 09 05 05 09 14 0D 0B 0D 14 14 14 14
00000070   14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14
00000080   14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14
00000090   14 14 14 14 14 14 14 14 14 14 14 14 14 14 FF C0
000000A0   00 11 08 01 22 00 FF 03 01 22 00 02 11 01 03 11
000000B0   01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00
000000C0   00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09
000000D0   0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05
000000E0   05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21
000000F0   31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23
00000100   42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17
```

Figure 1. An image and its "Hexdump", showing data stored as Hexadecimal values (*Duttke J, 2021*)

Naturally, I would encounter these numbers and will have to determine what they actually mean. For example, a computer byte of '01001000' in Binary has a value of 72 when converted to Decimal. This Binary number ends with a '0', and with experience I learned that this meant that the number, when converted to Decimal, is even and can be divided by two.

In a sense, I was applying a divisibility rule on a number in Binary (Non-Decimal) to determine that it was even, and this made me wonder if the divisibility rule for 3 was transferable to Binary as well. Adding up the digits of the byte gives a total of 2, and 2 is not divisible by 3, therefore meaning that the byte is not divisible by 3. However, we do know that 72 is divisible by 3, since 7 + 2 = 9 and 9 is divisible by 3, resulting in a contradiction. When using an online calculator, the following results were obtained:

In Binary: $1001000 \div 11 = 11000$
In Decimal: $72 \div 3 = 24$

The number 72 will always be divisible by 3, regardless of what number system it is represented in. Thus, the contradiction exists since the divisibility rule for 3 in Decimal cannot be easily transferred to Binary. This piqued my interest to explore the mathematics behind the divisibility rule for 3, why it could not be applied to numbers in Binary, and subsequently what the divisibility rule by 3 would be like in Binary. Furthermore, the fact that the divisibility rule for 2 was applicable to numbers in both Decimal and Binary meant that there must be certain underlying characteristics of these bases and the number '2' that made this possible. As such, I wondered if there was a way to create a divisibility rule by any number for any number in any number system.

Thus, in this research paper, I will be walking through certain discoveries in number theory to answer my research question "**How can we systematically characterize the divisibility rules in base-10 that would then allow us to generalize and find the divisibility rules in any base-n number system?**" In particular, the concept of modular arithmetic and number systems will be used to do so. While most results are known, Lemmas, Theorems and Proofs used in this paper are my own formulation of these results.

1.2. Modular Arithmetic

Modular Arithmetic is another way of counting numbers where the numbers “wrap around” after reaching the ‘Modulo’. Indeed, modular arithmetic is used quite prevalently in our daily lives, most notably when telling times or dates - months and hours use Modulo 12 while minutes and seconds use Modulo 60. For example, in Modulo 12, numbers start ‘wrapping around’ from 1 after 12, which means that 13 is equivalent to 1, 14 to 2, etc.

AM	0	1	2	3	4	5	6	7	8	9	10	11
PM	12	13	14	15	16	17	18	19	20	21	22	23
Time	0	1	2	3	4	5	6	7	8	9	10	11

Table 1. To decipher a 24 Hour Clock

We identify 17:00 as 5 o’ clock since $17 - 12 = 5$. We also know that almost 2 days have passed if 46 hours have passed, since this number is close to 48 hours. For the above examples, modular arithmetic can be used to express them more appropriately:

$$17 \equiv 5(\bmod 12)$$
$$46 \equiv -2(\bmod 24)$$

Definition 1 (*Insall M & Weisstein E, 2021*)**:**

For any integers *k*, *p* and *x*, we write

$$k \equiv x \,(\bmod p)$$
$$\text{If \& Only If } p|k - x$$

The congruent sign (≡) is used instead of the equals sign (=) as *k* and *x* are not equal to each other, but rather congruent to each other in mod *p*.

We also find that | *k* - *x* | is divisible by *p*, as seen in the examples above where

$$|17 - 5| = 12,\ 12|12$$
$$|46 - (-2)| = 48,\ 24|48$$

Proposition 2:

The following properties of Modular Arithmetic are essential later on

i.

$$\begin{array}{ll} p \mid k \text{ if \& only if} & Eg: 16 \equiv 0 (\bmod 4) \\ k \equiv 0 \ (\bmod p) & \therefore 4 \mid 16 \end{array}$$

ii.

$$\begin{array}{ll} ab \equiv cd (\bmod p) \text{ if \& only if} & Eg: 15 \equiv 3 (\bmod 4) \ \& \ 17 \equiv 1 (\bmod 4) \\ a \equiv c \ (\bmod p) \ \& \ b \equiv d (\bmod p) & \therefore \quad 15 \times 17 \equiv 221 \equiv 3 \times 1 \equiv 3 (\bmod 4) \end{array}$$

iii.

$$\begin{array}{ll} a^m \equiv b^m (\bmod p) \ \forall m \in \mathbb{Z} & Eg: 5 \equiv 2 (\bmod 3) \\ \text{if \& only if } a \equiv b (\bmod p) & \therefore 5^2 \equiv 25 \equiv 2^2 \equiv 4 \equiv 1 (\bmod 3) \end{array}$$

iiii.

$$\begin{array}{ll} c \equiv 0 \ (\bmod a \times b) \text{ if \& only if} & Eg: 18 \equiv 0 (\bmod 2) \ \& \ 18 \equiv 0 (\bmod 3) \\ c \equiv 0 \ (\bmod a) \ \& \ c \equiv 0 \ (\bmod b) \ , \ a \neq b & \therefore 18 \equiv 0 (\bmod 2 \times 3) \equiv 0 (\bmod 6) \end{array}$$

$$\begin{array}{l} Eg: 18 = 2 \times 3 \times 3 \\ \therefore 2, \ 3, \ 2 \times 3, 3 \times 3, 2 \times 3 \times 3 \text{ are factors of } 18 \end{array}$$

Proof for *i.*

$$\begin{array}{l} |k - 0| \ \textit{is divisible by p} \\ \therefore |k| \ \textit{is divisible by p} \\ \therefore p \mid k \end{array}$$

□

Proof for *ii.*

$$
\begin{aligned}
&If\ \ a \equiv c(\,mod\ p)\ \ \&\ \ b \equiv d(\,mod\ p)\ ,\ then\\
&\exists\ \ e\&f \in \mathbb{Z} \text{ such that}\\
&a = ep + c\ \ \&\ \ b = f\,p + d\\
&\therefore ab = (\,ep + c)\,(\,f\,p + d)\\
&ab = ef\,p^2 + dep + cf\,p + cd\\
&\quad = (\,ef\,p + de + cf\,)\,p + cd\\
&\text{Let } ef\,p + de + cf\ = g\\
&ab\ =\ gp\ + cd,\\
&\therefore ab \equiv cd(\ \mathrm{mod}\ p)
\end{aligned}
$$

□

Proof for *iii.*

This is simply an extension of *ii*, where multiplying the equation by itself will result in powers of *a* and *b:*

$$
\begin{aligned}
&\text{If } a \equiv b(\ \mathrm{mod}\ p)\ .\ \text{then}\\
&aa \equiv bb(\ \mathrm{mod}\ p)\\
&a^2 \equiv b^2(\ \mathrm{mod}\ p)\ , a^3 \equiv b^3(\ \mathrm{mod}\ p)\ , \ldots
\end{aligned}
$$

□

Proof for *iiii.*

$$
\begin{aligned}
&c \equiv 0(\ \mathrm{mod}\ a)\ , c \equiv 0(\ \mathrm{mod}\ b)\\
&\therefore a \text{ and } b \text{ are factors of } c\\
&Factors\ of\ \ c\ = \{C_1 \times C_2 \ldots a \ldots b \ldots C_{m-1} \times C_m\}\\
&a \times b = ab\\
&\therefore ab \text{ is a factor of } c
\end{aligned}
$$

□

Thus, when determining the divisibility of *k* by any composite number (6), it is much easier to determine if *k* is divisible by the prime factors of that composite number (2 and 3).

Proposition 3 (Fermat's Little Theorem) (*Singh N, 2019*)**:**

If p is prime and is a not divisor of k, then

$$k^{p-1} \equiv 1(\bmod p)$$

This is known as Fermat's Little Theorem (FLT).

Example:

$$\text{Let } k = 5,\ p = 3$$
$$\text{By } FLT,$$
$$5^{3-1} \equiv 1(\bmod 3) \because 5^{3-1} - 1 = 24, \text{ and } 3 \mid 24$$

1.3. Number Systems

We use Decimal for the simple reason that we have 10 fingers on both hands, making it easy to count. However, number systems do exist for every single natural number. For example, the Binary (0 to 1) and Quinary (0 to 4) bases. The number 39 in Decimal when converted equals 100111 in Binary and 124 in Quinary. Despite these numbers looking extremely different, their value is still the same and are merely expressed differently.

Definition 4(*Thangarajah P, 2020*)**:**

For a number *k* in base-*n*,

$$\begin{aligned} k &= \left[k_{m-1}k_{m-2}k_{m-3}\ldots k_2k_1k_0\right]_n \\ &= k_{m-1}\times n^{m-1} + k_{m-2}\times n^{m-2} + k_{m-3}\times n^{m-3}\ldots + k_2\times n^2 + k_1\times n + k_0 \end{aligned}$$

Example:

Let $k = 39 = [100111]_2$

$$k_0 = k_1 = k_2 = k_5 = 1$$

$$k_3 = k_4 = 0$$

For number base-*n* where $n > 10$, other characters are used to represent digits. For example, 10 to 15 in Decimal are represented A, B, C, D, E and F in Hexadecimal.

Example:

$$[255]_{10} = [11111111]_2 = [\mathrm{FF}]_{16}$$

1.4. More Definitions

An arbitrary number k is represented as $[k_{m-1}k_{m-2}k_{m-3}...k_2k_1k_0]_n$, where k is m digits long. Each k_m within the square brackets represents a digit where m is its index, while n represents the base that k is in. In base-10, the ones digit has an index of 0 and is represented as k_0, while the hundreds digit has an index of 2 and is represented by k_2. This is for simplicity, since as mentioned earlier in Definition 4, the value of the hundreds digit is $k_2 \times 10^2$, and in general, the value of k_m in k is $k_m \times n^m$.

$$k \equiv x \pmod{p}$$

In Definition 1, p is used as the Modulo and for all purposes in this paper, as the number we are trying to test divisibility by. x is used to represent the remainder, and as stated in Proposition 2*i*, if $x = 0$, then p divides k.

$$n^m \equiv x_m \pmod{p}$$

In this equation, x_m refers to the remainder when dividing the number n^m by p. For the rest of the paper, m will not refer to the number of digits in k but rather

1. The index of a term if it is written in subscript.
2. A general number if it is written as m or as a power.

2. Divisibility rules in Decimal

It was observed that the divisibility rules for certain numbers are similar to one another and have the same underlying principle behind why they work. Thus, the divisibility rules for these numbers are grouped together.

2.1. Divisibility Rules for 2, 5, 10

From Definition 4, when $n = 10$, we know that every single term other than k_0 is divisible by 10, in other words,

$$k - k_0 \equiv 0 \pmod{10}$$

Example:

When $k = 3141$,

$$\begin{aligned} k &= [3141]_{10} \\ &= 3\times 10^3 + 1\times 10^2 + 4\times 10 + 1 \\ &= 3140 + 1 \end{aligned}$$

$$\text{Since } 3140 \equiv 0 \pmod{10}\text{, then}$$

$$3141 - 1 \equiv 0 \pmod{10}$$

All terms other than k_0 are multiplied by a power of 10, meaning that the value of k - k_0 is divisible by 10. For k to be divisible by 10, k_0 needs to be divisible by 10 as well. In Decimal, the only single digit number divisible by 10 is 0. Thus,

Lemma 5:

$$10 \mid k \text{ iff } k_0 = 0$$

'iff' means 'if and only if', where the conditions can only be both true or both false (*Ramsey, n.d.*). For example, it is impossible to find a k where $10 \mid k$ but $k_0 \neq 0$, or a k where $k_0 = 0$ but $10 \nmid k$.

10 = 2 × 5, which means that any number divisible by 10 will also be divisible by 2 and 5. Thus, the reasoning behind the divisibility rules for 2 and 5 are similar in that only k_0 needs to be considered. Thus,

Theorem 1:

$$p \mid k \text{ iff } p \mid k_0$$
$$\text{for any } p \in \{2, 5, 10\}$$

Example:

$$2 \mid 2718 \because 2 \mid 8$$
$$5 \mid 1415 \because 5 \mid 5$$
$$10 \mid 7950 \because 10 \mid 0$$

2.2. Divisibility Rules for 2^m, 5^m, 10^m

In Section 2.1, only 1 digit, k_0, was considered. To find how this applies to higher powers of 2, 5 and 10, the previous example can be considered again.

$$\begin{aligned} k &= [3141]_{10} \\ &= 3 \times 10^3 + 1 \times 10^2 + 4 \times 10 + 1 \\ &= 3100 + 41 \end{aligned}$$

$$\text{Since } 3100 \equiv 0 \pmod{10^2}, \text{ then } 3141 - 41 \equiv 0 \pmod{10^2}$$

It is found that except for 41, or k_1k_0, all other terms are divisible by 10^2, meaning only these digits need to be considered, By extension, only $k_2k_1k_0$ need to be considered when checking divisibility by 10^3. Continuing this shows a pattern where checking the divisibility of 10^m requires only the last m digits to be considered, and for k to be divisible by 10^m, the last m digits have to be divisible by 10^m, meaning that they must be equal to 0. Thus,

Lemma 6:

$$10^m \mid k \text{ iff } k \text{ has } m \text{ trailing 0's}$$

Since,

$$\begin{aligned} 10^m &= (2 \times 5)^m \\ &= 2^m \times 5^m \end{aligned}$$

Any number divisible by 10^m will also be divisible by 2^m and 5^m, meaning the same reasoning going from Lemma 5 to Theorem 1 can be applied when going from Lemma 6 to Theorem 2.

Theorem 2:

$$\begin{aligned} &p \mid k \text{ iff } p \mid \text{last } m \text{ digits of } k \\ &\text{for any } p \in \{2^m, 5^m, 10^m\} \forall\, m \in \mathbb{Z} \end{aligned}$$

Example:

$$\begin{aligned} &2^2 \mid 1616 \because 2^2 \mid 16 \\ &5^3 \mid 7375 \because 5^3 \mid 375 \\ &10^4 \mid 1230000 \because 10^4 \mid 0000 \end{aligned}$$

2.3. Divisibility Rules for 3 and 9

To create divisibility tests for 3 and 9, we first establish

$$10^m \equiv 1(\bmod 3, 9)\ \forall\ m \in \mathbb{Z}$$

This means that the remainder when dividing any power of 10 by 3 or 9 will be equal to 1.

Proof:

$$\begin{aligned}
&10 \equiv 1(\bmod 3, 9)\\
&\text{By Proposition } 2iii,\\
&10^m \equiv 1^m(\bmod 3, 9)\\
&\quad\;\; \equiv 1(\bmod 3, 9)
\end{aligned}$$

Another way to visualize this is that 10^m - 1 will be a string of m 9's, and is thus divisible by 9 and subsequently 3, since 3 | 9. The above congruence implies that 10^m can be rewritten as 999...999 + 1.

□

Theorem 3:

$$\begin{aligned}
&p \,\big|\, k \text{ iff } p \,\big|\, \Sigma \text{ of digits in } k\\
&\text{for any } p \in \{3, 9\}
\end{aligned}$$

Proof:

For k where

$$\begin{aligned}
k &= \left[k_{m-1}k_{m-2}k_{m-3}\cdots k_2k_1k_0\right]_{10}\\
&= k_{m-1}\times 10^{m-1} + k_{m-2}\times 10^{m-2} + k_{m-3}\times 10^{m-3}\ldots + k_2\times 10^2 + k_1\times 10 + k_0\\
&= \left(k_{m-1}\times\left(10^{\mathrm{m}-1} - 1\right) + k_{m-2}\times\left(10^{\mathrm{m}-2} - 1\right) + k_{m-3}\times\left(10^{\mathrm{m}-3} - 1\right)\ldots + k_2\times 99 + k_1\times 9\right) +\\
&\quad \left(k_{m-1} + k_{m-2} + k_{m-3}\ldots k_2 + k_1 + k_0\right)
\end{aligned}$$

The red portion above is divisible by 3 and 9, since

$$10^m \equiv 1(\mod 3, 9)$$
$$10^m - 1 \equiv 0(\mod 3, 9)$$
$$k_m(10^m - 1) \equiv 0(\mod 3, 9)$$

$\therefore$ red portion is divisible by 3 and 9

Thus, for k to be divisible by 3 or 9, the blue portion has to be divisible by 3 or 9 respectively.

Since this is the Σ of the digits, the Σ of the digits of k can determine if 3 or 9 | k.

□

Example:

$$k = 7071$$
$$\Sigma \text{ of digits of } k = 7 + 0 + 7 + 1$$
$$= 15$$

Since the Σ of digits of 7071 is 15, and 15 is a multiple of 3 but not 9, therefore $3 \mid 7071$ while $9 \nmid 7071$.

It is worth noting that while this method works for 3 and 3^2, the divisibility rule is not the same for 3^3.

$$k = 27$$
$$\Sigma \text{ of digits of } k = 2 + 7$$
$$= 9$$

Even though it is obvious that $27 \mid 27$, $27 \nmid 9$, meaning that this divisibility rule is not applicable since it does not work for all values of k. (See Lemma 9 below)

2.4. Divisibility Rule for 11

To create the divisibility rule for 11, we can first find the remainder when dividing powers of 10 by 11, or finding x_m where

$$10^m \equiv x_m (\bmod 11)$$

Example:

$$\begin{array}{llll} 10^0 \equiv 1 (\bmod 11), & \text{as } 11 \big| \left(10^0 - 1\right) & \text{or } 11 \big| 0 \\ 10^1 \equiv -1 (\bmod 11), & \text{as } 11 \big| \left(10^1 - (-1)\right) & \text{or } 11 \big| 11 \\ 10^2 \equiv 1 (\bmod 11), & \text{as } 11 \big| \left(10^2 - 1\right) & \text{or } 11 \big| 99 \\ 10^3 \equiv -1 (\bmod 11), & \text{as } 11 \big| \left(10^3 - (-1)\right) & \text{or } 11 \big| 1001 \end{array}$$

Although x_m is non-constant, $x_m = \pm 1$. Thus,

Lemma 7:

$$10^m \equiv \begin{cases} 1(\bmod 11) & \forall \text{ even numbered } m \\ -1(\bmod 11) & \forall \text{ odd numbered } m \end{cases}$$

Proof:

$$10^2 \equiv 1 (\bmod 11)$$

$$10^{2m} \equiv 1^m \equiv 1 (\bmod 11)$$

$$10^1 \equiv -1 (\bmod 11)$$

$$10^{2m+1} = 10^{2m} \times 10^1 \equiv 1 \times -1 \equiv -1 (\bmod 11)$$

□

Each term in the number k can just be replaced by an equivalent number in mod 11.

$$
\begin{aligned}
k &= \left[k_{m-1}k_{m-2}k_{m-3}\ldots k_2k_1k_0\right]_{10}\\
&= k_{m-1}\times 10^{m-1} + k_{m-2}\times 10^{m-2} + k_{m-3}\times 10^{m-3}\ldots + k_2\times 10^2 + k_1\times 10 + k_0\\
&\equiv \pm k_{m-1} \mp k_{m-2} \pm k_{m-3}\ldots + k_2 - k_1 + k_0 (\bmod 11)
\end{aligned}
$$

The final congruence is simply the alternating Σ of k, or the Σ of the digits of its even terms minus the Σ of the digits of its odd terms, and this means that

$$k - \text{ Alternating } \Sigma \text{ of digits of } k \equiv 0 \ (\bmod 11)$$

and that only the alternating Σ needs to be considered when checking for divisibility by 11.

Theorem 4:

$$11 \mid k \text{ iff } 11 \mid \text{Alternating} \sum \text{of digits of } k$$

Example:

Let $k = 34551$

$$
\begin{aligned}
k &= \left[34551\right]_{10}\\
\text{Alternating } \Sigma \text{ of digits } &= 3 - 4 + 5 - 5 + 1\\
&= 0
\end{aligned}
$$

Since 11 | 0, it follows that 11 | 34551.

2.5. Divisibility Rules for 7 and 13

The last single digit prime number not covered is 7. To check the divisibility of *k* by 7, we can again find x_m where

$$10^m(\bmod 7) \equiv x_m$$

$$\begin{array}{ll} 10^0 \equiv 1(\bmod 7) & 10^4 \equiv -1\times 3 \equiv -3(\bmod 7) \\ 10^1 \equiv 3(\bmod 7) & 10^5 \equiv -3\times 3 \equiv -2(\bmod 7) \\ 10^2 \equiv 3\times 3 \equiv 2(\bmod 7) & 10^6 \equiv -2\times 3 \equiv 1 \equiv 10^0(\bmod 7) \\ 10^3 \equiv 2\times 3 \equiv -1(\bmod 7) & 10^7 \equiv 1\times 3 \equiv 3 \equiv 10^1(\bmod 7) \end{array}$$

Since $10^6 \equiv 10^0$ as shown above, the sequence of x_m for $0 \le m \le 5$ will be the same when $6 \le m \le 11$, or that this sequence of

$$x_m = \{1, 3, 2, -1, -3, -2\}$$

repeats. When $p = 13$, it is also found that:

$$10^0 \equiv 10^6 \equiv 1(\bmod 13)$$

Which means again that x_m repeats every 6 terms where

$$x_m = \{1, -3, -4, -1, 3, 4\}$$

Thus, to find if 7 or 13 divides *k,* the corresponding values of x_m are substituted into each 10^m and iff 7 or 13 divides this new number, then 7 or 13 | *k*

Theorem 5:

$p \mid k$ iff $p \mid \Sigma$ of the digits of *k* multiplied by corresponding values of x_m for $p \in \{7, 13\}$

Example:

Let $k = 111\ 111$,

$$111111 \equiv 1\times 1 + 1\times 3 + 1\times 2 + 1\times -1 + 1\times -3 + 1\times -2 \equiv 0\ (\bmod 7)$$

$$111111 \equiv 1\times 1 + 1\times -3 + 1\times -4 + 1\times -1 + 1\times 3 + 1\times 4 \equiv 0(\mathit{mod}\ 13)$$

Since $7 \mid 0\ \&\ 13 \mid 0$,

$7 \mid 111111\ \&\ 13 \mid 111111$

3. Divisibility rules for numbers in Non-Decimal

In this section, general properties of divisibility rules from base-10 that exist for any base-*n* will be covered.

3.1. Divisibility by n^m & factors of n^m

Decimal (base-10)	Binary (base-2)	Trinary (base-3)	Quanary (base-4)	Quinary (base-5)	Senary (base-6)
0	0	0	0	0	0
1	1	1	1	1	1
2	10	2	2	2	2
3	11	10	3	3	3
4	100	11	10	4	4
5	101	12	11	10	5
6	110	20	12	11	10
7	111	21	13	12	11
8	1000	22	20	13	12
9	1001	100	21	14	13
10	1010	101	22	20	14
11	1011	102	23	21	15
12	1100	110	30	22	20

Table 2: 0 to 12 expressed in Binary, Trinary, Quanary, Quinary and Senary

In base-10, it is found that k is divisible by 10^m iff there are m trailing 0's. The above table shows the number 0 to 12 in base-n, $n \in \{10, 2, 3, 4, 5, 6\}$. In these bases, the value $[10]_n = n$ (Highlighted red in Table 2). In fact, this applies for all bases (Other than Unary, base-1), since after reaching the highest digit (which will always be n-1), adding 1 to k means k_0 will reset to 0 while k_1 will increase from 0 to 1, resulting in $[k_1k_0]_n = [10]_n$, which we know n divides since:

$$n - 1 + 1 = n$$
$$n \mid n \ \forall\, n \geq 2$$

For $k = [100]_n$, it is found that

$$\begin{aligned} k &= [100]_n \\ &= 1 \times n^2 + 0 \times n + 0 \\ &= n^2 \end{aligned}$$

This can be seen in the table above $2^2 = [100]_2$, $[3^2]_{10} = [100]_3$. Furthermore, expanding this to n^3, it is found that $2^3 = [1000]_2$. Thus,

Lemma 8:

$$n^m \mid [k]_n \text{ iff } [k]_n \text{ has } m \text{ trailing 0's}$$

Proof:

$$\begin{aligned} k &= \left[k_{m-1}k_{m-2}k_{m-3}\ldots k_2k_1k_0\right]_n \\ &= k_{m-1} \times n^{m-1} + k_{m-2} \times n^{m-2} + k_{m-3} \times n^{m-3} \ldots + k_2 \times n^2 + k_1 \times n + k_0 \end{aligned}$$

Since all terms other than k_0 are multiples of n,

$$k - k_0 \equiv 0(\bmod n)$$

By the same logic,

$$k - k_1k_0 \equiv 0\left(\bmod n^2\right)$$
$$k - k_2k_1k_0 \equiv 0\left(\bmod n^3\right)$$

□

Thus, for k to be divisible by n^m, only the last m digits need to be considered, and again, the only possible values for these digits is 0, meaning that these digits must be trailing 0's iff $n^m \mid k$.

Example:

In the table above, since $[1100]_2$ has 2 trailing 0's, it must be divisible by 2^2. Indeed, $[1100]_2$ = 12, which is divisible by 4. In Trinary, Quandary and Senary,

$$12 = [110]_3 = [30]_4 = [20]_6$$

Since these values each have 1 trailing 0, these values are divisible by 3^1, 4^1 and 6^1 respectively. We know this is true since these numbers are all factors of 12. Furthermore, since the quinary form of 12, $[22]_5$,does not end with a 0, we also know that $5 \nmid 12$.

The same pattern is also noticed when considering the divisibility by factors of n, $m \geq 2$. The comparison for this in base-10 is how only the last m digits needs to be considered when finding divisibility by 2^m and 5^m.

Example:

When $n = 6$,

$$k = [k_{m-1}k_{m-2}k_{m-3}...k_2k_1k_0]_6$$
$$= k_{m-1} \times 6^{m-1} + k_{m-2} \times 6^{m-2} + k_{m-3} \times 6^{m-3} ... + k_2 \times 6^2 + k_1 \times 6 + k_0$$

Factors of 6 excluding 1 & itself : 2 & 3

$$k = [k_{m-1}k_{m-2}k_{m-3}...k_2k_1k_0]_6$$
$$= k_{m-1} \times 2^{m-1} \times 3^{m-1} + k_{m-2} \times 2^{m-2} \times 3^{m-2} + k_{m-3} \times 2^{m-3} \times 3^{m-3} ...$$
$$+ k_2 \times 2^2 \times 3^2 + k_1 \times 2 \times 3 + k_0$$

Thus to find if the factors of $6^m \mid [k]_6$, only the last m digits need to be considered.

Example:

In Senary, only numbers ending with 0 or 3 are divisible by 3, and only numbers ending with 0, 2 or 4 are divisible by 2. Subsequently,

Theorem 6:

$$\text{Factors of } n^m \,|[k]_{\mathrm{n}} \text{ iff } n^m \mid \text{last } m \text{ digits of } [k]_n$$

From here, it is noticed that it is only in even number systems where divisibility by 2 can be checked just using k_0, since 2 is a factor of only even numbers.

3.2. Divisibility when $n^m \equiv 1 \pmod{p}$

In base-10, it was found that the divisibility rules for 3 and 9 are similar because $10^m \equiv 1$ (mod 3,9) for all values of m and because of this, it is possible to substitute every 10^m with 1 and thus find the divisibility of a number by 3 or 9 by adding the Σ of its digits. In this case,

$$10^m \equiv c(\text{ mod } 3, 9) \;\; \forall\, m \in \mathbb{Z}$$

Where $c = 1$. However, this is something that may not apply in other number systems.

Example:

$$\begin{aligned} &2 \equiv 2(\text{ mod } 3) \\ &2^2 \equiv 1(\text{ mod } 3) \\ &2^3 \equiv \; 2(\text{ mod } 3) \end{aligned}$$

Thus,

$$2^m \not\equiv c(\text{ mod } 3, 9) \;\; \forall\, m \in \mathbb{Z}$$

Since the value of $x_m \neq 1$ for all values of m in Binary (unlike in Decimal) in Modulo 3, the divisibility rule for 3 in Decimal will not apply to Binary. Furthermore, since the only non-zero number that remains constant when raised to any power is 1, the only possible value for c is 1.

$$\begin{aligned} &\text{Find } p \text{ for } n \; s.t. \\ &n^m \equiv 1(\text{ mod } p) \; \forall\, m \in \mathbb{Z} \\ &n^1 \equiv 1(\, mod\; p) \;\text{ implies that } n^m \equiv 1^m \equiv 1(\text{ mod } p) \; \forall\, m \in \mathbb{Z} \\ &n \equiv 1(\text{ mod } p) \\ &n - 1 \; \equiv \; 0(\text{ mod } p) \end{aligned}$$

Since $p \mid n$-1 , possible values of p is n-1 and all of its factors.

Examples:

In base-10, n-1 = 9, and factors of 9 excluding 1 are 3 and 9. Thus,

$$10^m \equiv 1(\bmod p) \ \forall\ m \in \mathbb{Z},\ p \in \{3, 9\}$$

In base-5, n-1 = 4, and factors of 4 excluding 1 are 2 and 4. Thus,

$$5^m \equiv 1(\bmod p) \ \forall\ m \in \mathbb{Z},\ p \in \{2, 4\}$$

In base-13, n-1 = 12, and thus,

$$13^m \equiv 1(\bmod p) \ \forall\ m \in \mathbb{Z},\ p \in \{2, 3, 4, 6, 12\}$$

In actuality, p can also be equal to 1, However, this is meaningless, since $[k]_n \equiv 0$ (mod 1) for all integer values of k, n.

Since it is established that for these values of n and p,

$$n^m \equiv 1(\bmod p) \ \forall\ m \in \mathbb{Z}$$

Thus, the divisibility rule for 3 and 9 in Decimal can also be applied here, meaning

Theorem 7:

$p \mid [k]_n$ iff $p \mid \Sigma$ of digits in $[k]_n$ only for p,n such that $n \equiv 1(\bmod p)$

Example:

Let $k = [2D]_{16}$ and $p = 5$.

Since $16 \equiv 1(\bmod 5)$,
Σ of digits of k: $[2 + D]_{16} = 15$
Since $5 \mid 15,\ 5 \mid \mathrm{k}$

3.3. Divisibility when $n^m \equiv \pm 1 \pmod{p}$

The last general case to consider would be when

$$n^m \equiv \pm c \pmod{p} \quad \forall\, m \in \mathbb{Z}$$

Again, the only non-zero value of c is 1, since this is the only number that has the same absolute value when raised to any power. In Modulo 11, base-10, odd powers of 10 are replaced with -1. Thus,

> Find p for n such that
> $n^m \equiv -1 \pmod{p}$ $\forall$ odd numbered m
> $n^1 \equiv -1 \pmod{p}$ implies that $n^m \equiv (-1)^m \equiv -1 \pmod{p}$ $\forall$ odd numbered m
> $\therefore n + 1 \equiv 0 \pmod{p}$

Since $p \mid n+1$, possible values of p are $n+1$ and all of its factors.

Example:

In base-5, $n+1 = 6$, and factors of 6 excluding 1 are 2, 3 and 6. Thus,

$$5^m \equiv -1 \pmod{p} \quad \forall \text{ odd numbered } m,\ p \in \{2, 3, 6\}$$

In base-13, $n+1 = 14$, and thus,

$$13^m \equiv -1 \pmod{p} \quad \forall \text{ odd numbered } m,\ p \in \{2, 7, 14\}$$

This means that to find if $p \mid [k]_n$ where $p \mid n^m+1$, the alternating Σ of the digits of k can be used. Thus,

Theorem 8:

$p \mid [k]_n$ iff $p \mid$ Alternating Σ of digits in $[k]_n$ only for p,n such that $n \equiv -1 \pmod{p}$

Example:

Let $k = [139]_{13}$ and $p = 7$. Since 7 is a factor of $n+1=14$

> Alternating Σ of digits of k: $[1 - 3 + 9]_{13} = 7$
> Since $7 \mid 7,\ 7 \mid \mathrm{k}$
> $[139]_{13} = 217,\ 217 = 31 \times 7$

4. Generalized Divisibility Rule

4.1. Formulating the Generalized Divisibility Rule

From all the examples above, it can be seen that even in different bases, divisibility rules are transferable provided they have the same conditions. Lastly, the divisibility rules for 7 and 13 in base-10 can be adapted to become the Generalized Divisibility Rule in any base-*n.* To find the divisibility for the number *k* in base-*n* by the number *p*, or to find if the statement below is true,

$$k_n \equiv 0(\bmod p)$$

the number *k* is first expressed as the Σ of its digits multiplied by a power of *n*. Then, for each power of *n, n^m*, the value of x_m is found such that it satisfies the equation below.

$$n^m(\bmod p) \equiv x_m, x \in \mathbb{Z}$$

Where *p* is expressed as a list of its prime factors, *P*. Then, x_m is found for all values of *m* for each value of *P*. It is guaranteed that the values of x_m will repeat at most every *p*-1 terms if *P* is prime and is not a divisor of *n.*

Proof:

By FLT,

$$n^{p-1} \equiv 1(\bmod p)$$
$$\text{Since } n^0 \equiv 1(\bmod p)$$

Therefore, the series of x_m will have another x_m = 1 when *m* = *p*-1, meaning that it repeats itself in at most *p*-1 terms. However, it is possible that it might repeat earlier, as seen when *n* = 10 and *p* = 13, where the repeat cycle is 6, which is lower than 12.

□

When calculating the repeat cycle for all numbers in all bases, there seems to be no general pattern as to when the series repeats (See Section 7.2). Thus, the best way to find x_m would be to calculate every value of x_m until $x_m = 1$, $m \neq 0$. For example, when $n = 10$ and $p = 3^4$,

$$10^0 \equiv 1(\mod 81)$$

$$\ldots$$

$$10^9 \equiv 1(\mod 81)$$

Thus, the series of x_m is found to repeat every 9 terms (See Lemma 9 below).

When p is non-prime the following may happen:

When $p = 7 \times 13 \times 17 \times 19 = 29393$, the sequence repeats every 144 terms.

$$10^0 \equiv 1(\mod 29393)$$

$$\ldots$$

$$10^{144} \equiv 1(\mod 29393)$$

This is because the factors of p repeat after every 6, 6, 16 and 18 terms respectively. Thus, their values converge at the lowest common multiple, which is 144. Since there exists a lowest common multiple of any set of numbers, the series of x_m must repeat for any value of p.

From there, the corresponding values of x_{m} in Modulo P are substituted into n^m, where P refers to each prime factor of p. Let the Σ of these new numbers be S.

Theorem 9:

$$P \mid [k]_n \text{ iff } P \mid S$$

If the value of S is too large and unrecognizable, the same divisibility rule can be applied on S recursively to obtain a smaller value that is recognizable. Once it is verified that a value of P eventually divides S, it will imply that the first $P \mid S$ and thus $P \mid [k]_n$

This process is repeated for other prime factors of *p*. If *P* takes on the form of any of the (factors of n^m, *n*-1 or *n*+1) then it would be much faster to use those divisibility rules instead.

Finally, we can prove that the Generalized Divisibility Rule exists for any value of *k,n* & *p* where

Theorem 10:

$$\boldsymbol{p \mid [k]_{\mathrm{n}} \text{ iff all values of } \mathrm{P} \mid [k]_{\mathrm{n}},}$$

Proof:

Theorem 10 is Proposition 2*iiii.* rewritten to fit the new variables *k*, *n* & *p* to become the Generalized Divisibility Rule. Thus, its proof is the same.

□

Lemma 9:

When $n = 10$, $p = 3^m$, $m \geq 3$, the series of x_m will repeat at most every $3^{m\text{-}2}$ terms.

Proof:

$$10^0 \equiv 1(\bmod p)\ \forall\, p \geq 2$$

When $m = 3$,

$$10^{3^{3-2}} - 1 = 999 = 37 \times 3^3$$

$$\therefore 3^3 \,\Big|\, 10^{3^{3-2}} - 1$$

$$\therefore 10^3 \equiv 1\left(\bmod 3^3\right)$$

Thus, the sequence repeats every 3 terms, $x_m = \{1, 10, 19\}$.

Assume $3^v \mid (10^3)^{v\text{-}2}\text{-}1$ is true (when $m = v$)

$$\exists\ A\ s.t.$$

$$10^{3^{v-2}} - 1 = 3^v \times A$$

$$10^{3^{v-1}3^{-1}} = 3^v \times A + 1$$

$$\left(10^{3^{v-1}}\right)^{\frac{1}{3}} = 3^v \times A + 1$$

$$10^{3^{v-1}} = (3^v A + 1)^3$$

$$10^{3^{v-1}} = (3^v A)^3 + 3\left(3^{2v} A^2 \times 1\right) + 3\left(3^v A \times 1^2\right) + 1^3$$

$$10^{3^{v-1}} - 1 = 3^{3v} A^3 + 3 \times 3^{2v} A^2 + 3 \times 3^v A$$

$$10^{3^{v-1}} - 1 = 3^{3v} A^3 + 3^{2v+1} A^2 + 3^{v+1} A$$

$$10^{3^{v-1}} - 1 = 3^{v+1} \times \left(3^{2v-1} A^3 + 3^v A^2 + A\right)$$

$$\text{Let} \left(3^{2v-1} A^3 + 3^v A^2 + A\right) = B$$

$$10^{3^{v-1}} - 1 = 3^{v+1} \times B$$

$$\therefore 3^{m+1} \,\Big|\, 10^{3^{m+1-2}} - 1$$

It is true that the relation below is true when $m = 3$, and assuming it is true when $m = v$ implies that it is also true when $m = v + 1$. Thus,

$$3^m \,\Big|\, 10^{3^{m-2}} - 1\ \forall\, m \geq\ 3$$

□

Therefore,

$$10^{3^{m-2}} - 1 \equiv 0(\bmod 3^{m})$$

$$10^{3^{m-2}} \equiv 1(\bmod 3^{m})$$

$$\text{Since } 10^{0} \equiv 1(\bmod 3^{m})$$

Thus, the sequence will repeat at most every 3^{m-2} terms. The use of technology verifies that the sequence repeats every 3^{m-2} terms.

Example:

For 27:

$3^{3-2}=3,\ x_{m}=\{1, 10, 19\}$

For 81:

$3^{4-2}=9,\ x_{m}=\{1, 10, 19, 28, 37, 46, 55, 64, 73\}$

There are 27 terms when $p = 3^5$ and 81 when $p = 3^6$. These sequences can be found in Section 6.3.

4.2. Example of Generalized Divisibility Rule

To find if 5040 | k, k = $[1261620]_7$,

1. Prime factorize 5040:

$$5040 = 2^4 \times 3^2 \times 5 \times 7$$

2. Test divisibility by 7:

Since $[1261620]_7$ ends with a 0 ($k_0 = 0$), it is divisible by its base, 7

3. Test divisibility by 5:

$$7^0 \equiv 1(\bmod 5)$$
$$7^1 \equiv 2(\bmod 5)$$
$$7^2 \equiv 4(\bmod 5)$$
$$7^3 \equiv 3(\bmod 5)$$
$$7^4 \equiv 1(\bmod 5)$$

Therefore, x_m repeats every 4 terms, $x_m = \{1, 2, 4, 3\}$

$$[1261620]_7 \equiv 1\times 4 + 2\times 2 + 6\times 1 + 1\times 3 + 6\times 4 + 2\times 2 + 0\times 1\ (\bmod 5)$$
$$[1261620]_7 \equiv 45 \equiv 0(\bmod 5)$$

4. Test divisibility by 9:

$$7^0 \equiv 1(\bmod 9)$$
$$7^1 \equiv 7(\bmod 9)$$
$$7^2 \equiv 4(\bmod 9)$$
$$7^3 \equiv 1(\bmod 9)$$

Therefore, x_m repeats every 3 terms, $x_m = \{1, -2, 4\}$

$$[1261620]_7 \equiv 1\times 1 + 2\times 4 + 6\times -2 + 1\times 1 + 6\times 4 + 2\times -2 + 0\times 1\ (\bmod 5)$$
$$[1261620]_7 \equiv 18 \equiv 0(\bmod 9)$$

5. Test divisibility by 2^4:

$$
\begin{aligned}
7^0 &\equiv 1(\bmod 16)\\
7^1 &\equiv 7(\bmod 16)\\
7^2 &\equiv 1(\bmod 16)
\end{aligned}
$$

Therefore, x_m repeats every 2 terms, $x_m = \{1, 7\}$

$$[1261620]_7 \equiv 1\times 1 + 2\times 7 + 6\times 1 + 1\times 7 + 6\times 1 + 2\times 7 + 0\times 1 \ (\bmod 16)$$

$$[1261620]_7 \equiv 48 \equiv 0(\bmod 16)$$

Since all $P \mid k$, $P \in \{2^4,3^2,5,7\}$, then by **Theorem 10**,

$$5040 \mid [1261620]_7$$

Proof:

$$
\begin{aligned}
&[1261620]_7 = 166320\\
&166320 = 33\times 5040\\
&\therefore 5040 \mid [1261620]_7
\end{aligned}
$$

□

5. Conclusion

In conclusion, by considering modular arithmetic and how numbers are represented in each of the number bases, the process for checking the divisibility of any number in any base by any number can be found. It is worth noting that while this process is extremely systematic, it is obviously not the most efficient. For example, a number in Decimal is divisible by 7 iff $7 \mid k - 2k_0$ (*Banfill J, 2012*), which is much simpler and faster than substituting values of {1, 3, 2, -1, -3, -2}into each term. Furthermore, using the Generalized Divisibility Rule also becomes impractical as p approaches infinity, since finding prime factors of p gets much harder even for computers, let alone finding it manually. Lastly, since computers and calculators are always accessible, it might seem useless to learn divisibility rules that take much longer to do as compared to checking directly. However, this process is able to deepen our understanding as to how number systems, modular arithmetic and divisibility works, which had answered the questions that I originally had before starting research on this topic.

6. Bibliography

Banfill, J. (2012). Numbers divisible by 7. Retrieved April 10, 2021, from https://www.aaamath.com/div66_x7.htm

Duttke, J. (2021). HexEd.it :Browser-based online and offline hex editing. Retrieved April 10, 2021, from https://hexed.it/

Insall, M., & Weisstein, E. (2021). "Modular Arithmetic." From MathWorld--A Wolfram Web Resource. Retrieved April 10, 2021, from https://mathworld.wolfram.com/ModularArithmetic.html

Ramsey. (n.d.). 'If and only if'. Retrieved April 10, 2021, from http://www.math.hawaii.edu/~ramsey/Logic/Iff.html

Singh, N. (2019). Fermat's little theorem. Retrieved April 10, 2021, from https://www.geeksforgeeks.org/fermats-little-theorem/#:~:text=Fermat's%20little%20theorem%20states%20that,an%20integer%20multiple%20of%20p.&text=ap%20%E2%89%A1%20a%20(mod,an%20integer%20multiple%20of%20p.

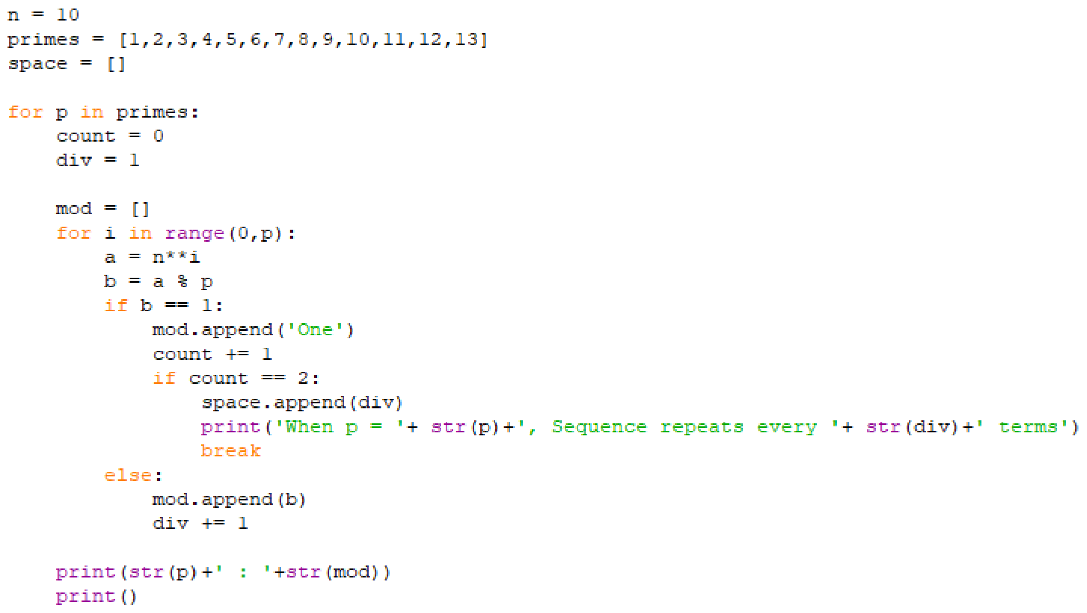
Thangarajah, P. (2020). 7.2: Number bases. Retrieved April 10, 2021, from https://math.libretexts.org/Courses/Mount_Royal_University/MATH_2150%3A_Higher_Arithmetic/7%3A_Number_systems/7.2%3A_Number_Bases

7. Appendix

7.1. Code used in Extended Essay

$$n^m(mod\ p) \equiv x_m, x \in \mathbb{Z}$$

A programme was written in Python to find x_m for all terms when given a base and a list of p.

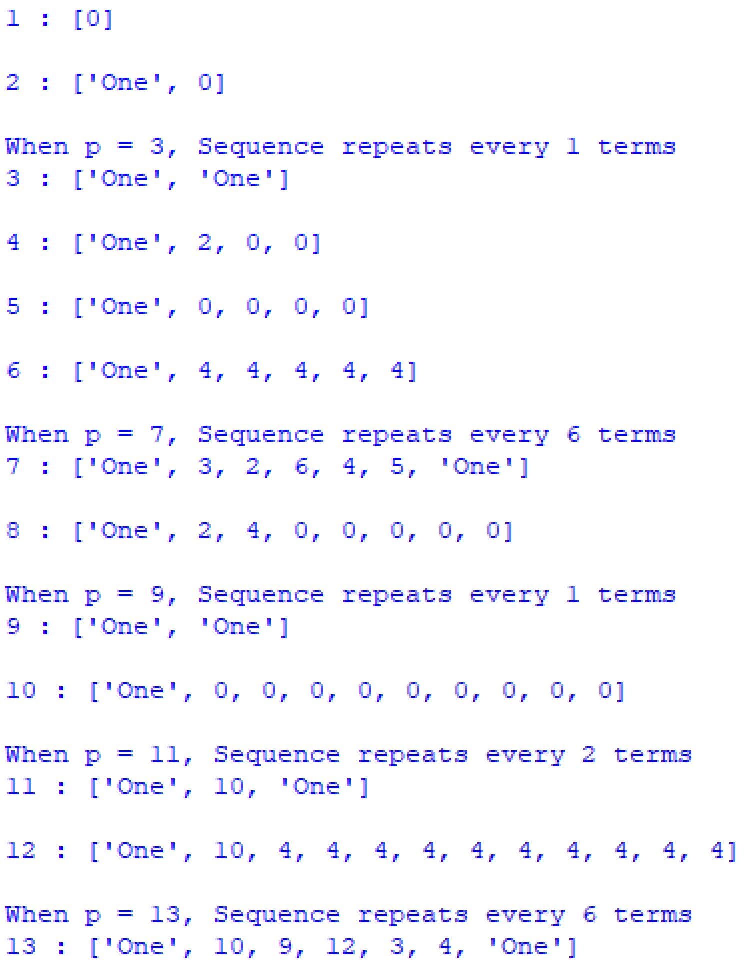


```
n = 10
primes = [1,2,3,4,5,6,7,8,9,10,11,12,13]
space = []

for p in primes:
    count = 0
    div = 1

    mod = []
    for i in range(0,p):
        a = n**i
        b = a % p
        if b == 1:
            mod.append('One')
            count += 1
            if count == 2:
                space.append(div)
                print('When p = '+ str(p)+', Sequence repeats every '+ str(div)+' terms')
                break
        else:
            mod.append(b)
            div += 1

    print(str(p)+' : '+str(mod))
    print()
```

Figure 2 : Code used to generate values of x_m given n and p

Code can be found online and copied at https://pastebin.com/eaRsXMJr

Although the list of p is called primes, it actually accepts a list of any integers, as seen in how the numbers 1, 4, 6, 8, 9, 10 and 12 are in the list. When running this code, this is its output.



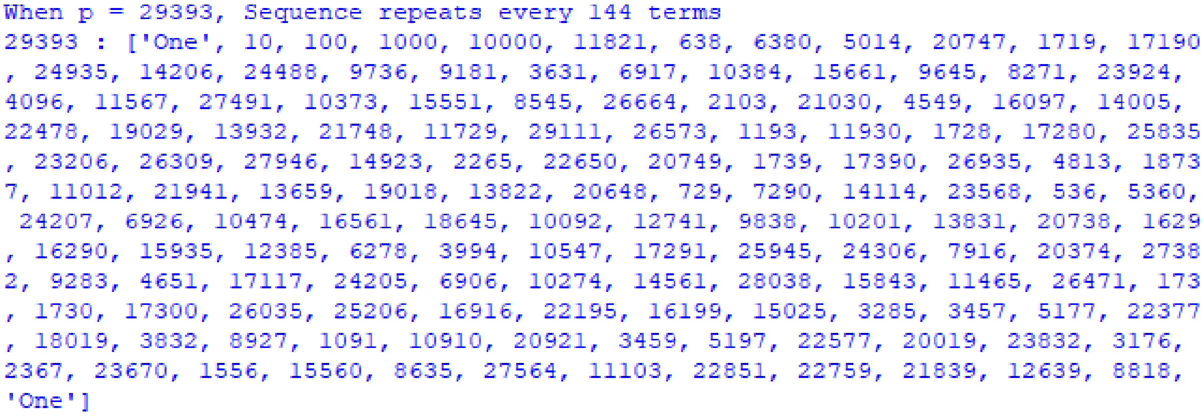
```
1 : [0]

2 : ['One', 0]

When p = 3, Sequence repeats every 1 terms
3 : ['One', 'One']

4 : ['One', 2, 0, 0]

5 : ['One', 0, 0, 0, 0]

6 : ['One', 4, 4, 4, 4, 4]

When p = 7, Sequence repeats every 6 terms
7 : ['One', 3, 2, 6, 4, 5, 'One']

8 : ['One', 2, 4, 0, 0, 0, 0, 0]

When p = 9, Sequence repeats every 1 terms
9 : ['One', 'One']

10 : ['One', 0, 0, 0, 0, 0, 0, 0, 0, 0]

When p = 11, Sequence repeats every 2 terms
11 : ['One', 10, 'One']

12 : ['One', 10, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4]

When p = 13, Sequence repeats every 6 terms
13 : ['One', 10, 9, 12, 3, 4, 'One']
```

Figure 3: Values of x_m when n = 10 and p = Prime numbers from 2 to 13

The programme generates a list of x_m based on what p and n are, and if $x_m = 1$ for some value of m ≠ 0, the programme will mention how many terms are in the sequence before it repeats. By Fermat's Little Theorem, only p-1 terms need to be found. Furthermore, if the sequence repeats earlier than expected (such as in the case of 3, 9, 11 and 13), the programme will terminate the process for that value of p and proceed to the next p in the list *primes*, until every p in that list has been done.

7.2. Data Generated using Code

Of course, the code above can be used to find any value and sequence of x_m given *n* and *p*. The data below shows the length of each cycle of x_m for all prime values of *p* up to 997 and when $n = 10$. This was how the conclusion that there was no general trend for every number was made, as well as how Lemma 9 was discovered, which would have been impossible without the help of the code I wrote. Data for Lemma 9: https://pastebin.com/jQWYjmQg



```
When p = 29393, Sequence repeats every 144 terms
29393 : ['One', 10, 100, 1000, 10000, 11821, 638, 6380, 5014, 20747, 1719, 17190
, 24935, 14206, 24488, 9736, 9181, 3631, 6917, 10384, 15661, 9645, 8271, 23924,
4096, 11567, 27491, 10373, 15551, 8545, 26664, 2103, 21030, 4549, 16097, 14005,
22478, 19029, 13932, 21748, 11729, 29111, 26573, 1193, 11930, 1728, 17280, 25835
, 23206, 26309, 27946, 14923, 2265, 22650, 20749, 1739, 17390, 26935, 4813, 1873
7, 11012, 21941, 13659, 19018, 13822, 20648, 729, 7290, 14114, 23568, 536, 5360,
 24207, 6926, 10474, 16561, 18645, 10092, 12741, 9838, 10201, 13831, 20738, 1629
, 16290, 15935, 12385, 6278, 3994, 10547, 17291, 25945, 24306, 7916, 20374, 2738
2, 9283, 4651, 17117, 24205, 6906, 10274, 14561, 28038, 15843, 11465, 26471, 173
, 1730, 17300, 26035, 25206, 16916, 22195, 16199, 15025, 3285, 3457, 5177, 22377
, 18019, 3832, 8927, 1091, 10910, 20921, 3459, 5197, 22577, 20019, 23832, 3176,
2367, 23670, 1556, 15560, 8635, 27564, 11103, 22851, 22759, 21839, 12639, 8818,
'One']
```

Fig 4: Values of x_m when $p = 29392$, $n = 10$

Table 3: Table of Prime Numbers and length of each cycle of x_m in base-10

p = Prime Number	Length of each cycle of x_m	p = Prime Number	Length of each cycle of x_m
2	1	439	219
3	1	443	221
5	1	449	32
7	6	457	152
11	2	461	460
13	6	463	154
17	16	467	233
19	18	479	239
23	22	487	486
29	28	491	490
31	15	499	498

37	3	503	502
41	5	509	508
43	21	521	52
47	46	523	261
53	13	541	540
59	58	547	91
61	60	557	278
67	33	563	281
71	35	569	284
73	8	571	570
79	13	577	576
83	41	587	293
89	44	593	592
97	96	599	299
101	4	601	300
103	34	607	202
107	53	613	51
109	108	617	88
113	112	619	618
127	42	631	315
131	130	641	32
137	8	643	107
139	46	647	646
149	148	653	326
151	75	659	658
157	78	661	220
163	81	673	224
167	166	677	338
173	43	683	341
179	178	691	230
181	180	701	700
191	95	709	708

193	192	719	359
197	98	727	726
199	99	733	61
211	30	739	246
223	222	743	742
227	113	751	125
229	228	757	27
233	232	761	380
239	7	769	192
241	30	773	193
251	50	787	393
257	256	797	199
263	262	809	202
269	268	811	810
271	5	821	820
277	69	823	822
281	28	827	413
283	141	829	276
293	146	839	419
307	153	853	213
311	155	857	856
313	312	859	26
317	79	863	862
331	110	877	438
337	336	881	440
347	173	883	441
349	116	887	886
353	32	907	151
359	179	911	455
367	366	919	459
373	186	929	464
379	378	937	936

383	382	941	940
389	388	947	473
397	99	953	952
401	200	967	322
409	204	971	970
419	418	977	976
421	140	983	982
431	215	991	495
433	432	997	166