ON DECIMAL EXPANSIONS OF RATIONAL NUMBERS

NEELAM VENKATA PRASAD AKULA

ABSTRACT. Given a rational number r, it is somewhat immediate that r has a decimal expansion. However, the properties of said decimal expansion are less immediate. In this paper we seek to formalize the relationship between a rational number and it's decimal expansion, determine the period of repeating decimals, and prove several theorems that relate to repeating decimals.

1. INTRODUCTION

When asked "How would you define a real number?" a very natural response is to use a decimal expansion to represent said number. A *decimal expansion* is a real number of the form $a.d_1d_2\cdots$ where a is an integer and the d_i are digits of the decimal expansion such that $0 \leq d_i \leq 9$. Clearly, a decimal expansion can also be expressed as

$$a + \frac{d_1}{10} + \frac{d_2}{100} + \cdots .$$

However, this definition is circular, what does this definition indicate about infinite sums? It would be much easier to define the reals $\mathbb{R}$ before working with these infinite sums. As such, let's formalize the reals first and then use a decimal expansion strictly as a name for any given real number. Constructing $\mathbb{R}$ is something that has been done many times, through many methods, the one of most relevance to us is through Dedekind Cuts.

Definition 1.1 (Dedekind Cut)**.** A *Dedekind Cut* is a partition of the rationals $\mathbb{Q}$ into two sets, A and A^C, such that:

i. $A \neq \emptyset$ ($A^C \neq \mathbb{Q}$).
ii. $A \neq \mathbb{Q}$ ($A^C \neq \emptyset$).
iii. If $x, y \in \mathbb{Q}$ such that $x < y$ and $y \in A$, then $x \in A$.
iv. If $x \in A$, then there exists a $y \in A$ such that $x < y$.

We then define any $r \in \mathbb{R}$ to be any subset of $\mathbb{Q}$ that satisfy the properties of the above definition, in other words—we let r be a Dedekind Cut. To rigorously demonstrate that $\mathbb{R}$ can be constructed using Dedekind Cuts we must show they satisfy arithmetic properties of $\mathbb{R}$. Specifically, we must define a total ordering, addition, multiplication, negation, and a supremum. As there is plenty of literature on this topic I will omit the proofs of which, instead opting to just list such properties.

i. $a \leq y \iff x \subseteq y$
ii. $A + B = \{a + b \mid a \in A, b \in B\}$
iii. $A \times B = \{a \times b \mid a \in A, b \in B\}$

2020 *Mathematics Subject Classification.* Primary 11T71; Secondary 11A07.
Key words and phrases. Algebraic Number Theory, Decimal Expansions, Repeating Decimals.

iv. $-A = \{-a \mid a \in A^C\}$
v. If $S \subset \mathbb{R}$ has an upper bound in $\mathbb{R}$, then it has a least upper bound in $\mathbb{R}$.

As an example we will look at what is arguably the most infamous irrational number, $\sqrt{2}$. Let $A = \{x \in \mathbb{Q} \mid x < 0 \vee x \times x = 2\}$, then A is in fact a real number and moreover $A \times A = 2$, however neither result is immediate. To show A is a real number we must show that A satisfies the four properties of a Dedekind Cut, the only non-trivial property in this case is A containing no greatest element. Observe that for any positive rational number x such that $x \times x < 2$ there exists a positive rational number y where $y = (2x+2)/(x+2)$, clearly then $y \times y < 2$. As our choice of x was arbitrary we have that A contains no greatest element. Then to show that $A \times A = 2$ first observe that clearly $A \times A \leq 2$, this requires showing that for any rational x such that $x \times x < 2$ then there is a positive $y \in A$ satisfying $x < y \times y$.

1.1. **Algebraic Concepts.** While the results of this paper can certainly be stated in a traditional number theory manner, the abstraction presented by algebraic structures can make proving these results much more elegant. In this section I provide a brief refresher on some of the concepts introduced in abstract algebra.

Definition 1.2. A group $\langle G, \star \rangle$ is a nonempty set G together with a binary operation $\star$ on G satisfying the following properties:

i. Associativity: For all $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$.
ii. Identity: There is an element $e \in G$ such that $e \star x = x = x \star e$ for all $x \in G$.
iii. Inverse: For all $x \in G$ there exists a $y \in G$ such that $x \star y = e = y \star x$.

If the operation $\star$ is an operation such that $x \star y = y \star x$ for all $x, y \in G$ (commutativity) we say G is an *abelian* group. For any subset H of a group G, we have that H is a *subgroup* of G if H itself is a group with respect to the operation of G. If G is a finite group, that is it contains a finite number of elements, then the *order* of G, notated as $|G|$ or $\mathrm{ord}(G)$, is the number of elements in G. An example of an abelian group would be $\langle \mathbb{Z}, + \rangle$, the integers under addition, with 0 as the identity element and the inverse of a being $-a$.

Definition 1.3 (Rings)**.** A ring $\langle R, +, \times \rangle$ is a nonempty set R together with two binary operations $+$ and $\times$ on R satisfying the following properties:

i. $\langle R, + \rangle$ is an additive group.
ii. Associativity: for all $s, t, u \in R$, $(s \times t) \times u = s \times (t \times u)$.
iii. Left distribution: for all $s, t, u \in R$, $s \times (t + u) = (s \times t) + (s \times u)$.
iv. Right distribution: for all $s, t, u \in R$, $(s + t) \times u = (s \times u) + (t \times u)$.

Similarly to a group we can list some properties of special rings. If $st = ts$ for $s, t \in R$ then we say R is a *commutative* ring. A subset S of a ring R is a *subring* of R is S is itself a ring under the operations of R. If there is some nonzero element $e \in R$ such that $es = s = se$ for all $s \in R$ then e is called an *identity* for R and R is said to be a ring with identity. A *field* is a commutative ring R with identity in which every nonzero element has an inverse.

1.2. **The Theorems of Lagrange and Euler.** With our algebraic structures in hand we can prove Lagrange's Theorem, and in turn use it to prove Euler's Theorem. In the following section we will use Euler's Theorem extensively.

Theorem 1.1 (Lagrange's Theorem)**.** *Suppose G is a finite group and $H \leq G$, then $|H|$ divides $|G|$, in particular, $|G| = [G : H] \cdot |H|$.*

Proof. The right cosets of H in G are the equivalence classes of a certain equivalence relation on G. Specifically, call x and y in G equivalent if there exists $h \in H$ such that $x = yh$. Therefore, the right cosets form a partition of G. Each right coset aH has the same cardinality as H since $x \mapsto ax$ defines a bijection $H \to aH$ (with inverse $y \mapsto a^{-1}y$). The number of right cosets is the index, given as, $[G : H]$. Therefore, $|G| = [G : H] \cdot |H|$. □

Theorem 1.2 (Euler's Theorem)**.** *Let $\phi(n)$ be Euler's totient function (the number of integers relatively prime to n). If n and a are coprime positive integers then,*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. The residue classes modulo n that are coprime to n form a group under multiplication, then $|\mathbb{Z}/n\mathbb{Z}| = \phi(n)$. If a is any number coprime to n then a is in one of the residue classes, and its powers $a, a^2, \ldots, a^k \pmod{n}$ form a subgroup of the group of residue classes (all of order k), with $a^k \equiv 1 \pmod{n}$. Lagrange's Theorem says that $k \mid \phi(n)$, it follows then that $\phi(n) = km$ for some $m \in \mathbb{Z}$.

$$a^{\phi(n)} = a^{km} = \left(a^k\right)^m \equiv 1^m = 1 \equiv 1 \pmod{n}$$ □

2. Decimal Expansions of Rationals

With Euler's Theorem in hand, we can now begin to address the problem at hand. In this section we seek to formalize the relationship between a rational number and it's decimal expansion.

First and foremost, we must define the classes of a decimal expansion. We say a decimal expansion is *terminating* if at some point in the sequence of integers in the expansion is followed only by 0. If an expansion has a subsequence of digits that repeats we say such an expansion is *repeating.* Lastly, if an expansion is not terminating and not repeating we call it *non-repeating.*

As mentioned earlier, the idea that a rational number has a decimal expansion is somewhat immediate, but what class of expansion is still unclear. As it turns out, we have that a number is rational if and only if it's decimal expansion is either repeating or terminating. To show this result, we will first prove two lemmas.

Lemma 2.1. *Let x be a decimal expansion that is either terminating or repeating. Then x is a rational number.*

Proof. Suppose that x is a terminating decimal expansion, and without loss of generality suppose that $0 < x < 1$. It follows that $x = 0.a_1 \cdots a_n 000\ldots$, where $a_1 \cdots a_n$ is a finite sequence of digits such that $0 \leq a_i \leq 9$. It follows rather trivially that:

$$x = 0.a_1 \cdots a_n 000\ldots \implies x = \frac{a_1 \cdots a_n}{10^n}.$$

Now suppose that x is a repeating decimal expansion with the same constraint of $0 < x < 1$, then $x = 0.\overline{a_1 \cdots a_n}$. Let $\hat{a_n} = a_1 \cdots a_n$, now observe:

$$\left(10^n x = \hat{a_n}.\overline{\hat{a_n}}\right) - \left(x = 0.\overline{\hat{a_n}}\right) \implies x(10^n - 1) = \hat{a_n} \implies x = \frac{a_1 \cdots a_n}{10^n - 1}$$

Clearly, with both respective cases we have that x is a rational number. □

Lemma 2.2. *Let x be a rational number given as p/q where* $\gcd(p, q) = 1$ *and $p < q$. Then x has either a repeating or terminating decimal expansion.*

Proof. Suppose that $x \in \mathbb{Q}$ such that $x = p/q$ where $\gcd(p, q) = 1$ and $p < q$. Moreover, assume that $\gcd(q, 10) = 1$. By Euler's Theorem,

$$10^{\phi(q)} \equiv 1 \pmod{q} \implies 10^{\phi(q)} - 1 = qa$$

for some integer a. Then,

$$x = \frac{p}{q} = \frac{pa}{10^{\phi(q)} - 1} = \frac{pa}{10^{\phi(q)}} \times \frac{1}{1 - \frac{1}{10^{\phi(q)}}} = pa \sum_{i=1}^{\infty} \left(\frac{1}{10^{\phi(q)}} \right)^i$$

Now observe that pa is an integer, which when represented as a sequence of digits is length $\phi(q)$, by the infinite series we have that

$$x = \frac{pa}{10^{\phi(q)}} + \frac{pa}{10^{2\phi(q)}} + \cdots \implies x = 0.\overline{pa}$$

As such, we see that x has a repeating decimal expansion when $\gcd(q, 10) = 1$.

If $\gcd(q, 10) \neq 1$ then the prime factorization of q includes either 2, 5, or both. Suppose that $q = 2^\alpha 5^\beta$ and $\gamma = \operatorname{lcm}(\alpha, \beta)$, then

$$x = \frac{p}{q} = \frac{p}{2^\alpha 5^\beta} \times \frac{10^\gamma}{10^\gamma} = \frac{pa}{10^\gamma}$$

for some integer a. It follows from the previous lemma that $pa/10^\gamma$ is in fact a terminating decimal expansion.

If q contains other factors besides 2, 5 then we multiply by the same 10^γ, where γ is the same as defined above, until we reach a rational where $\gcd(q, 10) = 1$. It follows that we then get a repeating decimal expansion, and when combined with the terminating decimal expansion given from the 10^γ, gives us a "padded" repeating decimal expansion. □

With these two lemmas the following theorem and corollary are immediate.

Theorem 2.3. *A number is rational if and only if it has either a repeating or terminating decimal expansion.*

Corollary. *A number is irrational if and only if it has a non-repeating decimal expansion.*

3. Period of a Repeating Decimal Expansion

Having shown that all rationals have either a repeating or terminating decimal expansion, we can now shift our attention to those rationals that result in a repeating expansion. The *period* of a repeating decimal expansion is the length of the repetend, or the number of digits in the sequence of the repeating figure. As we have seen, a repeating decimal only occurs when the denominator of a rational is coprime to 10. To investigate this matter we will first look at rationals of the form $1/p$ for some prime $p \neq 2, 5$.

Lemma 3.1. *Let p be a prime such that $p \neq 2, 5$. Then the period of the rational $1/p$, denoted as l_p, is the smallest integer k satisfying $10^k \equiv 1 \pmod{p}$.*

Proof. Let n be the smallest integer satisfying $10^n \equiv 1 \pmod{p}$, we call this the *multiplicative order of 10 modulo p*, then $p \mid (10^n - 1)$. This implies that for some integer r, $pr = 10^n - 1$. It follows that r is the repetend as an integer. Then,

$$0.\overline{r} = r\frac{1}{10^n} + r\frac{1}{10^{2n}} + \cdots = r\left(\frac{1}{10^n} + \frac{1}{10^{2n}} + \cdots\right) = r\sum_{i=1}^{\infty} \frac{1}{10^{in}}$$

So we have a geometric series,

$$r\sum_{i=1}^{\infty}\frac{1}{10^{in}} = r\frac{1}{10^n}\frac{1}{1-\frac{1}{10^n}} = \frac{10^n-1}{p}\frac{1}{10^n}\frac{10^n}{10^n-1} = \frac{1}{p}$$

Which is our desired result of $1/p$. $\square$

So we have that the period of rationals of the form $1/p$ is given as $\mathrm{ord}_p(10)$, a natural extension then is to rationals of the form $1/n$ (n still coprime to 10). So far we have been utilizing the basics of number theory arithmetic to prove the desired results, however we still have many tools of abstract algebra on hand. It turns out that such tools will in fact make our lives much simpler when it comes to proving the theorem regarding the period of $1/n$. To do so, first recall the Chinese Remainder Theorem.

Theorem 3.2 (Chinese Remainder Theorem)**.** *Let $n_1, \dots, n_k$ be integers greater than 1, and let N be the product of such n_i. If the n_i are pairwise coprime, then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution.

Naturally, the connection between the Chinese Remainder Theorem and the problem at hand is not very apparent. To see how this theorem is useful we will restate it in a more abstract manner.

Theorem 3.2 (Chinese Remainder Theorem)**.** *Let $n_1, \dots, n_k$ be integers greater than 1, and let N be the product of such n_i. If the n_i are pairwise coprime, then the map*

$$x \pmod{N} \mapsto \{x \pmod{n_1}, \dots, x \pmod{n_k}\}$$

defines a ring isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

We can now extend Lemma 3.1 with the following theorem.

Theorem 3.3. *Let n be an integer such that $\gcd(n, 10) = 1$, and the prime factorization of $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then the period of $1/n$, denoted as l_n, is given as lcm$(l_{p_1^{\alpha_1}}, \dots, l_{p_k^{\alpha_k}})$, where $l_{p_i^{\alpha_i}}$ is the period of the ith rational $1/p_i^{\alpha_i}$.*

Proof. By Lemma 3.1 we have that the period of $1/p$ is given as $\mathrm{ord}_p(10)$. It follows that for n such that $\gcd(n, 10) = 1$, $\mathrm{ord}_n(10)$ is the same as the order of the congruence class $[10]$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. By the Chinese Remainder Theorem we have that $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ gives us the following ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z},$$

which when shifted to the group of units, gives the following isomorphism of groups,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

This isomorphism is what is needed to show $l_n = \mathrm{lcm}(l_1, \dots, l_k)$. $\square$

It is quite immediate that given any rational we can easily compute its period using Theorem 3.3. For example, given the number $x = 15/70$ observe:

$$x = \frac{15}{70} = \frac{3}{14} = \frac{3}{2 \cdot 7} \implies l_{14} = \text{lcm}(l_2, l_7) = 6 \quad \text{and} \quad \frac{15}{70} = 0.2\overline{142857}$$

So not only may we generalize this result to any rational number, we can go one step further and generalize these results to base-a. A change in base would only require a change in which multiplicative order we find, base-a would indicate we must find $\text{ord}_p(a)$ for all respective primes.

4. Primitive Roots and Nine's Complements

Given the results in Section 3, we can now shift our attention to the study of strictly repeating decimals. Specifically, we are interested in properties of repeating decimals and how they correspond to primitive roots. Then we can focus our study on the repetends themselves, culminating in a theorem from 19th century French mathematician E. Midy.

4.1. **Primitive Roots.**

A natural extension of any work done with multiplicative orders is that of a primitive root.

Definition 4.1 (Primitive Root)**.** Let $a, p \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Then we say a is a *primitive root* modulo n if $\text{ord}_n(a) = \phi(n)$.

So how does this relate to our study on repeating decimals? Recall that for $1/p$, l_p is given as $\text{ord}_p(10)$. Then, for primes such that $\text{ord}_p(10) = p - 1$ we also have that $\phi(p) = p - 1$. This implies that for rationals of the form $1/p$ whose period length is $p - 1$ we have that 10 as a primitive root mod p. As an example observe the rational $1/7 = 0.\overline{142857}$. It follows that $l_7 = \text{ord}_p(10) = 6 = \phi(7)$. As such 10 is a primitive root modulo 7. This leads to a Conjecture first thought of by Gauss,

Conjecture 4.1 (Gauss)**.** There are infinitely many primes p such that 10 is a primitive root mod p.

A related conjecture is Artin's conjecture on primitive roots. This is quite beyond the scope of this paper, so instead I will reference Hooley's "On Artin's Conjecture"[2]. However, one related result that is within bounds of this material is the primitive root theorem.

Theorem 4.1 (Primitive Root Theorem)**.** *There exists a primitive root modulo m if and only if $m = 2, 4, p^\alpha, 2p^\alpha$ where p is an odd prime and α a positive integer.*

One rather interesting property of this decimal expansion is the repetend itself. Up until now, we have not cared for the repetend instead only focusing on the period of such a repetend. A natural intuition would indicate that the repetend of rationals with primes that have 10 as a primitive root would be somewhat special. Before continuing further, as an example we will list the repetends for all rationals of the form $a/7$ such that $a/7$ has a repeating decimal expansion.

Given this table a somewhat interesting observation are the digits used in the actual repetends themselves. Upon further inspection one will see that all repetends contain the same digits, differing only by cyclic permutation. Moreover, we can call this repetend a *cyclic number*. It follows then, that primes who have 10 as a primitive root generate cyclic numbers. A more formal definition of a cyclic number is as follows.

Rational	Repetend
1/7	142857
2/7	285714
3/7	428571
4/7	571428
5/7	714285
6/7	857142

Definition 4.2. A cyclic number is an integer in which cyclic permutations of the digits are successive integer multiples of the number.

4.2. **Nine's Complements.** Further investigation into the properties of a cyclic number reveal an interesting property related to the notion of base-10 nine's complements. Observe, in the case of 1/7, that 1 corresponds to 8, 4 corresponds to 5, and 2 corresponds to 7. With their correlation of course being the sum is 9. This specific property was formalized by 19th Century French mathematician E. Midy.

Theorem 4.2 (Midy's Theorem)**.** *Let a/p, where p is a prime, be a rational with a repeating decimal expansion. If the expansion has period $2n$*

$$\frac{a}{p} = 0.\overline{\underbrace{r_1 \cdots r_n}_{n}\underbrace{r_{n+1} \cdots r_{2n}}_{n}}$$

then the digits in the second half of the repetend are the nine's complement of the first half. For $i < n$ we have, $r_i + r_{i+n} = 9$. Moreover, $r_1 \cdots r_n + r_{n+1} \cdots r_{2n} = 10^n - 1$.

As with the proof for Theorem 3.3, the proof of this can be pleasantly stated using the results of abstract algebra (think cyclic groups). However, the intuition behind the proof is not as clear as a traditional direct proof, for that reason we present the following proof.

Proof. Suppose $p \neq 2, 5$ is a prime, and a an integer coprime to p. Then we know that,

$$\frac{a}{p} = 0.\overline{a_1 \cdots a_n} = \frac{r}{m(10^k - 1)}$$

where r is the integer representation of the repetend, and $m(10^k - 1) = 10^l - 1$ for period length l. Since $10^l - 1$ is a multiple of p, $10^k - 1$ is not a multiple of p (since $k < l$), and p is prime, therefore m is a multiple of p. Specifically, we see that $am/p = r/(10^k - 1)$ is an integer, $r \equiv 0 \pmod{10^k - 1}$. Let us split r into two equal parts, r_0 and r_1. Note that r_0 and r_1 are both represented by strings of k digits so they both satisfy $0 \leq r_i \leq 10^k - 1$. Clearly, r_0 and r_1 cannot both equal 0 (since that would imply $a/p = 0$), similarly they both cannot equal $10^k - 1$ (since that would imply $a/p = 1$). Therefore, $0 < r_0 + r_1 < 2(10^k - 1)$, and since $r_0 + r_1$ is a multiple of $10^k - 1$, it follows that $r_0 + r_1 = 10^k - 1$. □

There is much more to say about this matter, than just Midy's Theorem. However, the extensions and rigorous proofs of which are beyond the scope of this paper so instead I urge the reader to read Leavitt's "A Theorem on Repeating Decimals" [3].

5. Weiferich Primes

Given a rational $1/p$ for p prime, we know its period is given as l_p a natural extension is rationals of the form $1/p^k$ for some $k \in \mathbb{Z}$. Generally speaking, the pattern is that the period of such a repetend will be given as $p^{k-1}l_p$. We say generally as there are known counterexamples, however such numbers are exceedingly rare to come by. To investigate the matter further we define what a base-a Weiferich prime is.

Definition 5.1 (Base$-a$ Weiferich Prime)**.** A base-a Weiferich prime is a prime p that satisfies

$$a^{\phi(p)} \equiv 1 \pmod{p^2}$$

It follows then, that for base-10 the known counterexamples of $1/p^2$ being given as pl_p are in fact the base-10 Weiferich primes (these are 3, 487, and $56,598,313$). An extension of Weiferich primes are "extended Weiferich primes", given as primes that satisfy $a^{\phi(p)} \equiv 1 \pmod{p^n}$ for $n \in \mathbb{Z}$. Similar to Gauss's Conjecture, we have the following,

Conjecture 5.1. There are infinitely many base-a Weiferich primes.

While the general consensus is that there are infinitely many, it is evident that they are exceedingly rare to come by. In base-10 we know of three and have been searching for over two decades now (currently up to $\approx 10^{15}$). Shifting back to our period length, we see that while we can not guarantee *when* the period length will be $p^{k-1}l_p$, we do know that once a period length follows this pattern then so will it's subsequent powers of p. Related to this is of course the notion of a full repetend prime, rather the occurrences of full repetend primes.

Definition 5.2. A full repetend prime (or proper prime) in base-b is a prime number such that the Fermat quotient, given as,

$$q_p(b) = \frac{b^{p-1} - 1}{p}$$

produces a cyclic number. If the cyclic number generated by p possess $p-1$ digits then of course b is a primitive root modulo p.

Corollary. *Suppose a/p has a repeating decimal in base-b, if b is a power of another prime (i.e. $b = 9 = 3^3$) then there will be no full repetend primes base-b. Moreover, b is not a primitive root modulo p.*

This result may not be immediate, but follows when you think of what the period length of a full repetend prime would be in powers of prime bases. Similarly, when $b \equiv 0, 1 \pmod 4$, no such full repetend prime exists. The last property (of interest) of full repetend primes is that if a full repetend prime ends in the digit '1' in base-b, then each digit $0, 1, \ldots, b-1$ appears in the repetend the same number of times as each other digit, which once again follows from results with cyclic groups.

Acknowledgements

This paper was written as part of a semester-long independent study under Alex Suárez-Beard. His knowledge on this topic and patience with mentoring allowed for this independent study to be both highly enjoyable and informative. The bulk of the material in this paper was derived through working with him, with some

additional material from *Elementary Number Theory and its applications* by Rosen [4]. Lastly, much of the algebra learned was derived from *Abstract Algebra* by Crown, Fenrick, and Valenza [1].

References

[1] Gary D. Crown, Maureen H. Fenrick, and Robert J. Valenza, *Abstract algebra*, M. Dekker, New York, 1986.

[2] Christopher Hooley, *On artin's conjecture.* **225** (1967), 209–220.

[3] W. G. Leavitt, *A theorem on repeating decimals*, The American Mathematical Monthly **74** (1967), no. 6, 669–673, available at `https://doi.org/10.1080/00029890.1967.12000016`.

[4] Kenneth Rosen, *Elementary number theory and its applications*, 6th ed., Addison-Wesley, Boston, 2011.

Department of Mathematics, University of Maryland
Email address: `nakula@umd.edu`
URL: `www.math.umd.edu/~nakula`