Research Statement

Thomas Luckner
Dept. Mathematics, University of South Carolina, Columbia, SC 29208, USA
luckner@email.sc.edu

Introduction

My mathematical research is in the general area of number theory. I would be more specific but my projects do not fit well into a specific aspect of number theory.

My dissertation focuses on the construction, existence, and concentration of certain classes of primes in many different bases. However, I have also done work on the irreducibility of generalized Bernoulli polynomials and irreducible polynomials of the form $f(x)+Mg(x)$ where f and g are relatively prime polynomials with integer coefficients and M is a positive integer. The methodology in which I construct my research follows these broad three steps. First, identify a possible project from a previous project, from reading other papers on a topic, and/or from discussing a topic with a colleague. Second, use brut force computation or (more frequently) use self-written code and algorithms in mathematical softwares like Maple, Magma, and SageMath in an effort to identify patterns and anomalies. Lastly, attempt to prove the patterns and anomalies discovered in the previous step.

My long term goal in my research is to classify new forms of irreducible polynomials and primes and derive new ways to find such objects. While my work tends to be more theoretical, much of the results can be made applicable in cryptographic and information security fields like RSA encryption and generalizations. These new methods and objects can be applied to cryptographic systems and information security systems to improve current encryption and decryption systems.

In the last five years at the University of South Carolina, I have put my focus on identifying techniques where number theorists (and some algebraists) have used these tools to discover new classes of primes and irreducible polynomials and characterize these classes. This work has led me to the application of covering systems, prime density theorems, and Newton polygons. Below I will describe this work with more background details and I will discuss ideas for further work.

Classes of Primes and Covering Systems

The discovery and characterization of classes of primes is an abundant and old topic of research in number theory. Some well-known problems exist on the topic like the twin prime conjecture, Fermat prime conjecture, and $2^n + 1$ prime conjecture. In all these cases, the discussion is whether or not there exist infinitely many of these primes. However, the first part of these conjectures is to confirm existence. For these open problems, this step is trivial. Observe that 3 and 5 are twin primes as well as 5 and 7. For Fermat primes, $F_0 = 3$, $F_1 = 5$, and $F_2 = 17$ are all prime. For $n^2 + 1$, $2^2 + 1 = 5$, $4^2 + 1 = 17$, and $6^2 + 1 = 37$ are all prime. In my research, the existence of a specific type of prime is not obvious. I will ellaborate on this later on.

These famous primes are interesting to number theorists since the existence is apparent, but, when the numbers become large, the existence is not obvious at all. Consider the Fermat prime problem. After $F_4 = 65537$, L. Euler showed F_5 was not prime in 1732. In fact, it is believed that there are no other Fermat primes as suggested by the heuristic argument. In the case of twin primes, large primes were found, but whether there are infinitely many remains open. A. de Polignac posed a generalized version of the twin prime conjecture in 1849 and, until 2013, no progress had been made. Y. Zhang proved that there are infinitely many prime pairs with a gap of no more than 70 million. This opened the door for T. Tao and Polymath to reduce the bound to 4680 the same year. At the end of the year, J. Maynard reduced the bound down to 600 using a variation of the sieve used by Zhang. Then a variation of Polymath reduced the bound to 246 in 2014. The conjecture on primes of the form $2^n + 1$ has been labeled as one of Landau's 4 problems back in 1912 and has not been solved today.

These conjectures demonstrate how difficult it can be to prove the results about specific prime classes. This is what makes my research exciting. Some of the primes I focused on during my time at the University of South Carolina were widely digitally delicate primes, Sierpiński primes, Riesel primes, and any combination of these. W. Sierpiński proved there are infinitely many odd integers which are Sierpiski. Similarly, Riesel proved there are infinitely many odd integers which are Riesel numbers. In 1998, Brier found there are infinitely many odd integers which are both Sierpiński and Riesel and gave an explicit example. In 2013, C. Clavier found that for every nonnegative integer m, every number in the arithmetic progression

$$3316923598096294713661 + 377021473959660125796259470411 0\, m,$$

is a Brier number. Clavier found such a progression through the use of covering systems which I will talk about later. What is important to note here is that the existence of a Brier number is not obvious.

Now consider widely digitally delicate primes. For a prime to be digitally delicate, it must be composite when any digit is changed to another digit. For example,

294001 is a prime where

$$d94001, \quad 2d4001, \quad 29d001, \quad 294d01, \quad 2940d1, \quad \text{and} \quad 29400d$$

are composite or equal to 294001 for every $d \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Now this is a computatable process with a finite number of steps to determine if it is true. Widely digitally delicate primes are digitally delicate primes, but they also must be composite if any of the infinitely many leading zeros is changed to another digit. For example, 294001 is not a widely digitally delicate prime since 10294001 is a prime. The fact that there are infinitely many leading zeros that, when changed, could result in a composite number makes this problem less computable. In fact, the only know example of a widely digitally delicate prime was found by J. Grantham and is 4030 digits. Also, J. Rodgers determined the first $2.5 \cdot 10^{11}$ integers are not widely digitally delicate. Thus, the existence is difficult to show, and the concentration of such primes seems small. However, this is not the case.

D. Shiu showed that in any arithmetic progression containing infinitely many primes, there are arbitrarily long sequences of consecutive primes. Even further, J. Maynard showed that for every positive integer k, in any arithmetic progression $Am + B$, where $A > 0$, $B \geq 0$ and $m \geq 0$ are integers with A and B fixed and $\gcd(A, B) = 1$, a positive proportion of positive integers ℓ are such that $p_\ell, p_{\ell+1}, \ldots, p_{\ell+k-1}$ are all in the arithmetic progression $Am + B$, where p_j denotes the j^{th} prime. If we consider Clavier's arithmetic progression of Brier numbers, we notice that

$$3316923598096294713661 \quad \text{and} \quad 377021473959660125796259470411 0$$

are relatively prime. In any arithmetic progression $Am + B$ with $\gcd(A, B) = 1$, there are infinitely many primes. Thus, Shiu's theorem gives that there arbitrarily long sequences of consecutive primes in the progression which are Brier numbers. M. Filaseta and J. Juillerat used this idea to construct an arithmetic progression of widely digitally delicate primes $Am + B$ for which $\gcd(A, B) = 1$ to reach the same conclusion about widely digitally delicate primes. This confirms there is a positive proportion of primes which are widely digitally delicate contrary to what it seems. It is worth mentioning that Filaseta and J. Southwick also showed this result by a similar argument, but with a constructed sieve.

The construction of both the arithmetic progressions was based on the use of covering systems. Thus, in my research I constructed covering systems for primes that are both widely digitally delicate and Brier numbers. For widely digitally delicate primes, Filaseta and Juillerat made 18 covering systems, one for each possible digit increase or decrease. For the case of Brier primes, I made covering systems for both Sierpiński primes and Riesel primes without repeating the primes used in the other 18 covering systems. Filaseta and I were able to conclude that there are arbitrarily long sequences of consecutive primes that are widely digitally delicate

and Brier numbers. The most interesting aspect of this result is that despite there being a positive proportion of primes that are both widely digitally delicate and Brier numbers, there is no known example. Additionally, this result allowed us to conclude the same as Filaseta and Juillerat for widely digitally delicate primes but in base 2.

These results open up the opportunity to consider other bases for any combination of the above prime classes. T. Tao and S. Konyagin have independently work on widely digitally delicate primes in alternate bases. Any prime classification with similar structure can warrant the same results. In the future, I plan to explore these other classes and attempt conclude similar results. This highlights the importance of constructing arithmetic progressions of specific classes of primes. I intend to explore other constructions of arithmetic progressions of specific prime classes and make conclusions about their densities and occurrences amongst all primes.

Irreducible Polynomials and Newton Polygons

Almost all of my work on irreducible polynomials has focused around the use of Newton polygons. The work is focused on the use of the following theorem by Dumas (1906).

Theorem 1. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a nonnegative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to p, using exactly one translate for each edge of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.*

A Newton polygon with respect to a prime is the convex hull of a graph of points (x_i, y_i) with $x_0 = 0$, $x_1 = 1$, ..., $x_n = n$ where n is the degree of the polynomial and y_i is the highest power of the prime that divides the associated coefficient. For example, the Newton polygon for $f(x) = x^3+3x^2+12x+9$ with respect to the prime 3 is the convex hull of the points $(0, 0)$, $(1, 1)$, $(2, 1)$, and $(3, 2)$. This means the Newton polygon is made of the lines connecting $(0, 0)$ to $(2, 1)$ and $(2, 1)$ to $(3, 2)$. The theorem says that if there are factors $g(x)$ and $h(x)$ of the polynomial $f(x)$, then the slopes of any Newton polygon edge with respect to p (up to translation) will be the reciporcal of the degrees of the factors, d_g and d_h, times some constant. For example, consider the same $f(x)$ from earlier. Take $p = 3$. Then the Newton polygon of $f(x)$ with respect to 3 has 2 edges: one of slope $1/2$ and the other of slope 1. Therefore, if there are factors of $f(x)$, they will be of degree 2 or 1.

The important question now is how does the theorem demonstrate irreducibility. Consider the following polynomial: $f(x) = x^6+24x^5+12x^3-18x+36$. The Newton polygon of $f(x)$ with respect to 2 will be the lines connecting $(0,0)$ to $(5,1)$ and $(5,1)$ to $(6,2)$. Thus, the possible degrees of factors are 5 and 1. The Newton polygon of $f(x)$ with respect to 3 will be the lines connecting $(0,0)$ to $(3,1)$ and $(3,1)$ to $(6,2)$. Thus, the possible degree of factors of $f(x)$ is only 3. Since the Newton polygons give factors that do not match, $f(x)$ is irreducible. Now we show how this is useful in my research.

Let $B_m^{(l)}(x)$ be the generalized Bernoulli polynomial such that

$$f(x) = \left(\frac{t}{e^t-1}\right)^l e^{tx} = \sum_{m=0}^{\infty} B_m^{(l)}(x)\frac{t^m}{m!}.$$

A. Adelberg has shown numerous results about even m for $B_m^{(m)}(x)$, but Adelberg and Filaseta showed that 1/5 of all $B_m^{(m)}(x)$ are irreducible. In their paper, they focused on a specific class of even m and showed that these will always be irreducible by use of Eisenstein's Criterion. Note that Newton polygons are a stronger argument for irreducibility than Eisenstein's Criterion. Filaseta and I are currently working on improving this bound by using Newton polygons. I am excited about this project due to the potential that the approach of Newton polygons provides because of the following conjecture. Adelberg conjectures that if m is even, then $B_m^{(m)}$ is irreducible, and when m is odd, $B_m^{(m)}$ is the product of $x-m/2$ and an irreducible polynomial. If this is correct, there is much room for improvement on the 1/5 bound since Adelberg and Filaseta only account for some of the even cases. We are still in the thick of this project and intend to make strides this academic year.

Another ongoing project deals with $f(x)+Mg(x)$ where M is a positive integer and f and g are relatively prime integer polynomials. Filaseta and R. Wilcox have shown some results on the polynomials without coming up with an explicit bound on M. My goal is to find an explicit bound on M depending on f and g. If $d_f < d_g$, we have shown there is such a bound, depending on f and g, that gives $f(x)+Mg(x)$ is irreducible when a prime p^k divides the leading coefficient of $f(x)+Mg(x)$ but p^{k+1} does not. The structure of the proof depends on the 2 edges of Newton polygon with respect to p. The slopes of these edges give a contradiction due to the relationship of the slopes to the degrees of the factors. This result is complete and is being submitted this academic year.

I intend to continue improvements on the generalized Bernoulli polynomial irreducibility concentration by the use of Newton polynomials. To be more specific, I would like to consider the odd cases independently to see how useful the Newton polygons can be in that context. This methodology can be extended to alternate forms of polynomials which I will explore. The applications of Newton polygons are vast and bountiful, lending themselves to a dense research space. The two above examples of polynomials are quite different examples of applying Newton polygons to identifying irreducible polynomials.

References

[1] A. Adelberg, *On the degrees of irreducible factors of higher order bernoulli polynomials*, Acta Arith., Vol. 62 (1992): pp. 329-342.

[2] A. Adelberg and M. Filaseta, *On mth order Bernoulli polynomials of degree m that are Eisenstein*, Colloq. Math., 93(1): 21-26, 2002.

[3] G. Dumas, *Sur quelques cas dirreductibilité des polynômes á coefficients rationnels*, Journal de Math. Pure et Appl. 2 (1906), 191-258.

[4] P. Erdős, *Solution to problem 1029: Erdos and the computer*, Mathematics Magazine 52 (1979), 180-181.

[5] M. Filaseta and J. Juillerat, *Consecutive primes which are widely digitally delicate*, INTEGERS: Ron Graham Memorial Volume, Vol. 21A, 2021, Paper No. A12, 37 pp.; also see, Number Theory and Combinatorics: A Collection in Honor of the Mathematics of Ronald Graham, edited by Bruce M. Landman, Florian Luca, Melvyn B. Nathanson, Jaroslav Nešetřil and Aaron Robertson, Berlin, Boston: De Gruyter, 2022, pp. 209–248.

[6] M. Filaseta and J. Juillerat, Data for "Consecutive primes which are widely digitally delicate," https://people.math.sc.edu/filaseta/ConsecutiveWDDPrimes.html.

[7] M. Filaseta, J. Juillerat and T. Luckner, *Primes which are widely digitally delicate and Brier numbers*, preprint on arXiv (2022), https://arxiv.org/abs/2209.10646.

[8] M. Filaseta, J. Juillerat and J. Southwick, *Widely digitally stable numbers*, Combinatorial and Additive Number Theory IV (ed. M. Nathanson), Springer Proc. Math. Stat. 347, Springer, Cham, 2021, 161–193.

[9] M. Filaseta and J. Southwick, *Primes that become composite after changing an arbitrary digit*, Math. Comp. 90 (2021), 979–993.

[10] M. Filaseta and R. Wilcox. *An explicit dense universal Hilbert set*, Math. Proc. Cambridge Philos. Soc., 167, 531-547 (2019).

[11] J. Grantham, *Finding a widely digitally delicate prime*, preprint on arXiv (2021), https://arxiv.org/abs/2109.03923.

[12] "PrimeGrid", https://www.primegrid.com/ (Updates per prime search).

[13] O. Gerard, author, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A076335, Nov. 7, 2002.

[14] S. V. Konyagin, *Numbers that become composite after changing one or two digits*, Pioneer Jour. of Algebra, Number Theory and Appl. 6 (2013), 1–7.

[15] J. Maynard, *Dense clusters of primes in subsets*, Compositio Math. 152 (2016), 1517–1554.

[16] S. Nadis, "Mathematicians Find a New Class of Digitally Delicate Primes", Quanta Magazine, March 30, 2021, https://www.quantamagazine.org/mathematicians-find-a-new-class-of-digitally-delicate-primes-20210330/.

[17] M. Parker, Stand-Up Maths: How do you prove a prime is infinitely fragile?, July 28, 2021, `https://www.youtube.com/watch?v=p3Khnx0lUDE`.

[18] H. Riesel, *Några stora primtal*, Elementa 39 (1956), 258–260.

[19] D. K. L. Shiu, *Strings of congruent primes*, J. Lond. Math. Soc. 61 (2000), 359–373.

[20] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. 15 (1960), 73–74.

[21] N. J. A. Sloane, author, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A076336, Nov. 7, 2002.

[22] T. Tao, *A remark on primality testing and decimal expansions*, J. Aust. Math. Soc. 91 (2011), 405–413.

[23] D. W. Wilson, editor, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A101036, Jan. 17, 2005.