Research Statement
Daniel Baczkowski

1 Interests

Mostly my interests comprise number theory and approximation theory. Specifics include problems involving coverings of the integers, counting lattice points close to smooth curves and applications to problems involving gaps in number theory, exponential sum estimates, \(Z\)-numbers, Diophantine equations involving factorials, discrepancy and distributions of sequences in \(\mathbb{R}\) and \(\mathbb{R}^2\), almost-perfect and quasi-perfect numbers, and amicable numbers.

2 Problems involving coverings of the integers

In 1960, W. Sierpiński [27] showed that there are infinitely many odd positive integers \(k\) with the property that \(k \cdot 2^n + 1\) is composite for all natural numbers \(n\). Such an integer \(k\) is called a Sierpiński number in honor of Sierpiński’s work. Two years later, J. Selfridge (unpublished) showed that 78557 is a Sierpiński number. To this day, this is the smallest known Sierpiński number. Currently, there are six candidates smaller than 78557 to consider: 10223, 21181, 22699, 24737, 55459, 67607. See http://www.seventeenorbust.com for the most up-to-date information.

Riesel numbers are defined in a similar way. An odd positive integer \(k\) is a Riesel number if \(k \cdot 2^n - 1\) is composite for all natural numbers \(n\). These were first investigated by H. Riesel in 1956 [26]. The smallest known Riesel number is 509203. The curious reader should see http://www.prothsearch.net/rieselprob.html for the remaining candidates smaller than 509203 to consider.

The usual approach for constructing Sierpiński or Riesel numbers is to use a covering – a finite set of congruences with the property that every integer satisfies at least one of the congruences. For example, consider the following implications:

\[
\begin{align*}
&n \equiv 0 \pmod{2} \quad \& \quad k \equiv 1 \pmod{3} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{3} \\
&n \equiv 0 \pmod{3} \quad \& \quad k \equiv 1 \pmod{7} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{7} \\
&n \equiv 1 \pmod{5} \quad \& \quad k \equiv 3 \pmod{5} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{5} \\
&n \equiv 11 \pmod{12} \quad \& \quad k \equiv 2 \pmod{13} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{13} \\
&n \equiv 7 \pmod{36} \quad \& \quad k \equiv 4 \pmod{73} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{73} \\
&n \equiv 19 \pmod{36} \quad \& \quad k \equiv 18 \pmod{37} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{37} \\
&n \equiv 31 \pmod{36} \quad \& \quad k \equiv 13 \pmod{19} \quad \implies \quad k \cdot 2^n - 1 \equiv 0 \pmod{19}
\end{align*}
\]

The congruences for \(n\) in the table above cover all possibilities for \(n\); that is, this set of congruences forms a covering. As the moduli of the congruences for \(k\) are relatively prime, the Chinese Remainder Theorem allows us to combine all of the congruences for \(k\) into one statement: \(k \equiv 33737173 \pmod{3 \cdot 7 \cdot 5 \cdot 13 \cdot 73 \cdot 37 \cdot 19}\), giving rise to infinitely many Riesel numbers.

Luca and Mejía-Huguet take this one step further, finding Riesel and Sierpiński numbers embedded in the Fibonacci sequence [15]. They replace \(k\) with \(F_k\), where \(F_0 = 0, F_1 = 1\)
and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$ (i.e., the Fibonacci sequence). For any positive integer $m$, one utilizes the well-known fact that the Fibonacci sequence (or more generally, any recurrence relation of integers) is periodic modulo $m$. We denote the period by $h(m)$. In order to ensure $F_k$ is a Riesel number (using this covering), one begins by solving $F_k \equiv a \pmod{m}$ where $a \pmod{m}$ represents each congruence involving $k$ in the table above. We denote these solutions as $\mathcal{A}(a,m) = \{k : F_k \equiv a \pmod{m}\}$ (mod $h(m)$) and compute them below:

- $\mathcal{A}(1,3) = \{1, 2, 7\}$ (mod 8)
- $\mathcal{A}(1,7) = \{1, 2, 6, 15\}$ (mod 16)
- $\mathcal{A}(3,5) = \{4, 6, 7, 13\}$ (mod 20)
- $\mathcal{A}(2,13) = \{3, 25\}$ (mod 28)
- $\mathcal{A}(4,73) = \{53, 95\}$ (mod 148)
- $\mathcal{A}(18,37) = \{10, 15, 28, 61\}$ (mod 76)
- $\mathcal{A}(13,19) = \{7, 11\}$ (mod 18)

Now, the goal is to have there exist a representative from each set of congruences such that the intersection of all congruences is nonempty. Upon computing such an intersection of these sets, one deduces if $k \equiv 1807873 \pmod{3543120}$, then $F_k$ is a Riesel number. Thus, there are infinitely many Riesel numbers in the Fibonacci sequence. In a similar fashion, one shows there are infinitely many Sierpiński numbers in the Fibonacci sequence.

Replace $F_k$, the Fibonacci sequence, with say $L_k$, the Lucas numbers ($L_0 = 2$, $L_1 = 1$, and $L_i = L_{i-1} + L_{i-2}$ for $i \geq 2$). One can show that a similar result holds. That is, there exists infinitely many Riesel–Lucas numbers and infinitely many Sierpiński–Lucas numbers. Working with Olaolu Fasoranti (an undergraduate student) and Carrie Finch, we have deduced other related theorems and are still pursuing the multitude of problems we have encountered in this work. This area is ripe with a smorgasbord of problems for students of any stature to pursue.

3 Diophantine equations involving factorials

Brocard and Ramanujan independently inquired about the solution set to the Diophantine equation (that is the positive integer solutions)

$$n! + 1 = m^2. \quad (1)$$

It is an easy task to find the three known solutions, namely when $n = 4, 5,$ and $7$. Brocard in 1876 and Ramanujan in 1913 posed the question to find all the solutions to $(3)$. The best contributions to the problem were from Overholt who showed the equation has finitely many solutions if we assume a weak version of the ABC Conjecture [22]. Also, Berndt and Galway showed that $(3)$ has no other solutions for $n \leq 10^9$ [6]. To this day, the problem remains unsolved. In [12] the above result of Overholt was generalized, Florian Luca showed that if $P(x)$ is any polynomial of degree $> 1$ with rational coefficients and one assumes the ABC Conjecture is true, then $P(x) = n!$ has only finitely many solutions.

At one of the Western Number Theory Conferences, it is claimed that Erdős believed that the related equation

$$x(x + 1) = n!$$

2
undoubtedly has only finitely many solutions, but that the problem is “quite hopeless in our lifetime or perhaps the lifetime of this miserable universe” [5]. I am interested in these types of questions.

Throughout we let \( \sigma_0, \phi, \) and \( \sigma \) denote the number of divisors function, Euler’s phi function, and the sum of divisors function, respectively. It was shown by Florian Luca (see [13]) that if one fixes a rational number \( r \), then there are a finite number of positive integers \( n \) and \( m \) for which

\[
f(n!) = r \cdot m!
\]

where \( f \) is one of \( \sigma_0, \phi, \) or \( \sigma \).

In my master’s thesis, I produced some generalizations of the above theorem. Afterwards building on my work, we (coauthored with F. Luca, M. Filaseta, and O. Trifonov) were able to generalize the above (see [3]). For a positive integer \( N \), let \( \omega(N) \) denote its number of distinct prime divisors. A consequence of our work is the following theorem.

**Theorem 1.** Let \( f \) denote one of the arithmetic functions \( \sigma_0, \phi \) or \( \sigma \), and let \( k \) be a fixed positive integer. Then there are finitely many positive integers \( n, m, a \) and \( b \) such that

\[
b \cdot f(n!) = a \cdot m!, \quad \gcd(a, b) = 1 \quad \text{and} \quad \omega(ab) \leq k.
\]

Another way to view Theorem 1 is that the total number of distinct primes dividing the numerator and denominator of the fraction obtained by reducing the quotient \( f(n!)/m! \) tends to infinity as the product \( nm \) tends to infinity.

The full strength of our statements are that the constant \( k \) above can be replaced by a function involving \( m \) or \( n \) which tends to infinity. The next three theorems are the precise statements for each function \( \sigma_0, \phi, \) and \( \sigma \), which are in fact much more general than Theorem 1.

**Theorem 2.** There are finitely many positive integers \( a, b, n \) and \( m \) such that

\[
b \cdot \sigma_0(n!) = a \cdot m!, \quad \gcd(a, b) = 1, \quad \omega(b) \leq m^{1/4} \quad \text{and} \quad P_0(a) \leq \frac{\log n}{22},
\]

where \( P_0(a) \) denotes the least prime not dividing \( a \).

**Theorem 3.** There are finitely many positive integers \( a, b, n \) and \( m \) such that for \( n > 1 \)

\[
b \cdot \phi(n!) = a \cdot m!, \quad \gcd(a, b) = 1 \quad \text{and} \quad \max\{\omega(a), \omega(b)\} \leq \frac{n}{1.1 \log n}.
\]

**Theorem 4.** Fix \( \varepsilon > 0 \). Then there are finitely many positive integers \( a, b, n \) and \( m \) such that

\[
b \cdot \sigma(n!) = a \cdot m!, \quad \gcd(a, b) = 1, \quad \text{and} \quad \omega(ab) \leq n^{0.2 - \varepsilon}.
\]

Let \( \nu_q(N) \) denote the exponent of \( q \) in the prime factorization of a positive integer \( N \). Each of the three theorems above was solved differently, but the techniques used were mainly ideas related to the distribution of primes and estimating \( \nu_q(f(n!)) \). The last theorem which involves \( \sigma \) was considerably more difficult than the others due to the fact that our argument
required estimating the number of times a prime \( q \) could divide integers of the form \( p^N - 1 \), in other words estimating \( \nu_q(p^N - 1) \). The techniques involved were borrowed mostly from analytic number theory: formulas for sums of functions over primes, formulas for \( \nu_p(n!) \), a version of the Brun-Titchmarsh Theorem due to Montgomery and Vaughan \[18\], and for a prime \( q \) the careful analysis of \( \nu_q(\sigma(p^{\nu_p(n!)})) \) depending on the size of the prime \( p \) dividing \( n! \).

The last idea in itself was quite involved, required several lemmas, and borrowed ideas ranging from the precise number of solutions in \( x \) to the congruence \( x \equiv 1 \pmod{q^j} \) for given positive integers \( j \) and \( N \) to estimating \( \nu_q(\Phi_d(x)) \) where \( \Phi_d(x) \) denotes the \( d \)th cyclotomic polynomial and \( d \) and \( x \) vary over the positive integers and the primes in specifically chosen intervals.

In my dissertation \[1\], it is shown that Theorem 4 holds in a more general setting, namely when replacing \( \sigma \) with \( \sigma_k \) (the sum of the \( k \)th powers of divisors) where \( k \) is any positive integer.

### 3.1 Continuing this research

In \[17\], Luca and Shparlinski showed that \(|\tau(n!)| = m!\) has finitely many solutions in \( n \) and \( m \). The next step in the above work is to prove such a statement for \( f = \tau \), the Ramanujan tau function, which is defined via

\[
\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n)q^n.
\]

It is known that \( \tau \) is also a multiplicative function and takes positive and negative values. Lehmer conjectured that \( \tau(n) \neq 0 \) for all \( n \), yet even to this day this conjecture remains unsolved. Part of Deligne’s fields medal work showed that \(|\tau(n)| \leq \sigma_0(n) \cdot n^{11/2} \). This result was actually shown for a wider class of functions and not just \( \tau \); a similar result was shown for cusp forms which are eigenforms for the Hecke operators. One can show that Luca and Shparlinski’s proof for finitely many solutions to \(|\tau(n!)| = m!\) extends; that is, if we replace \( \tau \) with any eigenform for the Hecke operators, then the resulting equation also has finitely many solutions.

Also in the case of \( \tau \), there exists a constant \( C > 0 \) such that for any prime \( p \) and \( M \geq 2 \)

\[
|\tau(p^M)| \geq p^{(11/2)(M-C\log M)}
\]

whenever \( \tau(p) \neq 0 \) (see \[21\]). This result establishes that if \( \gcd(a,b) = 1 \) and a solution to the equation \( a \cdot m! = b \cdot |\tau(n!)| \) exists for a sufficiently large \( n \), then \(|\tau(n!)| = (n!)^{11/2 + o(1)} \). Such a statement immediately gives an asymptotic relation between \( m \) and \( n \) provided that \( a \) and \( b \) are appropriately regulated.

One seemingly hopeful approach to obtain results similar to Theorem 4 for \( \tau \) (or any eigenform for the Hecke operators), would be to utilize a result of Corvaja and Zannier about greatest common divisors of rational functions evaluated at \( S \)-units \[7\]. Kumar and Ram Murty have discovered many distributions properties of \( \tau(p) \) (or any eigenform for the Hecke operators) as \( p \) varies over the primes assuming GRH (the generalized Riemann Hypothesis for Artin \( L \)-series) \[20\]. Thus via GRH to obtain even stronger results, it may be possible to prove a result for \( \tau \) (or, again, any eigenform for the Hecke operators) similar to
Theorem 4. The difference between the cases $\sigma$ and $\tau$, simply stated, is due to the fact that $\sigma(p^{N-1}) = (p^N - 1)/(p - 1)$ which can be viewed as a product of cyclotomic polynomials in one variable $p$ (a rational prime), and $\tau(p^{N-1}) = (\alpha^N - \beta^N)/(\alpha - \beta)$ where $\alpha$ and $\beta$ are the roots of the characteristic polynomial $\lambda^2 - \tau(p)\lambda + p^{11}$. The latter expression for $\tau(p^{N-1})$ can be viewed as a product of cyclotomic polynomials in two variables $\alpha$ and $\beta$ (which are complex numbers).

4 Counting lattice points and applications

Until the 1980’s, exponential sums were the best approach to estimate the number of lattice points close to a smooth curve. Alas a new elementary method was developed by Filaseta, Huxley, Sargos, and Trifonov. Their ideas were a mixture of approximation theory, combinatorics, and geometry. Far from exhaustion, the applications of these results appear more and more fruitful. For example in [10], Filaseta and Trifonov proved that there exists a $c > 0$ such that the interval $(x, x + cx^{1/5}\log x)$ contains a squarefree number for all $x \geq 2$ (and were awarded the Distinguished Award of the Hardy-Ramanujan Society for this work). Afterwards in their pulchritudinous paper [9], they extended their result to the existence of $k$-free numbers in short intervals, found estimates for the distribution of squarefull integers (integers $n$ such that if $p | n$ then $p^2 | n$) in short intervals, and provided a number of other results. To date, the best known result for distributions of squarefull numbers was given by Trifonov in [28]. He showed that if $Q(x)$ denotes the number of squarefull integers less than or equal to $x$, then

$$Q(x + x^{1/2+\theta}) - Q(x) \sim \frac{\zeta(3/2)}{2\zeta(3)}x^{\theta}$$

for $\theta$ satisfying $19/154 < \theta < 1/2$. The goal for this research is to see what is the smallest $\theta \in (0, 1/2)$ so that the above asymptotic relation holds. The result does not hold for $\theta = 0$, since P. Shui showed that there are infinitely many $n$ such that there is no squarefull number between $n^2$ and $(n + 1)^2$ [19]. This should be compared to a result of De Koninck and Luca who showed in [8] that there are infinitely many $n$ such that $[n, n + n^{1/2}]$ contains $\gg (\log n/\log \log n)^{1/3}$ squarefull numbers.

Konyagin used the methods of counting lattice points close to smooth curves to obtain estimates for the least prime factor of binomial coefficients $\binom{n}{k}$ (see [11]). Moreover, the general methods have been utilized to obtain results about $k$-free values of irreducible polynomials and binary forms in algebraic number fields.

For a real number $x$, let $||x||$ denote the closest integer to $x$. In all of these estimates, given a real-valued function $f(x)$ defined on $I$ and given $\delta > 0$, one wishes to estimate the cardinality of the set

$$S = S(f, \delta) = \{x \in I \cap \mathbb{Z} : ||f(x)|| \leq \delta\}.$$

If $|S|$ denotes the cardinality of $S$, then often one obtains estimates which depend on the derivatives of $f$. That is, assuming the derivatives of $f$ are well behaved and considering $f$ on a dyadic interval say $[M, 2M]$, one derives upper bounds for $|S|$ that involve $M$, $\delta$, and the derivatives of $f$. It has been common practice to define $T$ so that the derivatives of the
function \( f : [M, 2M] \rightarrow \mathbb{R} \) satisfy
\[
\frac{c_r T}{M^r} \leq |f^{(r)}(x)| \leq \frac{C_r T}{M^r}
\]  
(3)
for certain values of \( r \geq 1 \) depending on the scenario at hand. Hence, \( |S| \) will depend on \( M, T, \delta, r, \) and the constants \( c_r \) and \( C_r \).

4.1 My contribution and how to continue this work

Let \( N(Q) \) denote the number of \( q \leq Q \) where \( q \) is a prime raised to an odd power, say \( q = p^{2k+1} \), such that \( p \mid \lfloor 2q^{1/2} \rfloor \). As noted in [16], J.-P. Serre ascertained that the largest number of \( \mathbb{F}_q \)-rational points on curves of small genus over the finite field \( \mathbb{F}_q \) depends on the aforementioned divisibility property. In [2], Trifonov and I have extended some of the estimates involving lattice points close to smooth curves and apply our results to obtain improvements on the problem of estimating \( N(Q) \) which was done in [16]. We show that \( N(Q) \ll Q^{5/42} \) where as for comparison the previous bound was \( N(Q) \ll Q^{17/140} \); indeed, notice that \( 5/42 = 0.11904\ldots \) and \( 17/140 = 0.121428\ldots \). In particular, we prove the following theorem which in itself has intrinsic value.

**Theorem 5.** Suppose that \( f(x) \) satisfies (3) for \( r = 2, 3, \ldots, n \). If \( \delta < \kappa T^{\frac{n-3}{n-2}} M^{\frac{n-1}{(n-2)^2}} \) for any absolute constant \( \kappa > 0 \), then
\[
|S| \ll M^{\frac{n-1}{n+1}} T^{\frac{2}{n(n+1)}} + M \delta^{\frac{2}{(n-2)(n-1)}} + M (\delta TM^{1-n})^{\frac{1}{n^2-3n+4}}
\]
where the constant in ‘\( \ll \)’ depends only on the constants in (3) and \( \kappa \).

The shear beauty of such a universal theorem in itself deems satisfaction, but the succinct general statement should undoubtedly produce future applications. Indeed, in the past such estimates were developed case by case depending on the problem at hand (for example, the case \( n = 3 \) was utilized for squarefree integer results). Now, instead one can choose the optimal value of \( n \) to be applied to aspiring future works.

5 More works in progress

I have pondered many other problems in number theory and made some partial progress on several. One such problem is listed below.

5.1 Amicable pairs

A pair of positive integers \((m, n)\) are amicable if \( \sigma(m) = \sigma(n) = m + n \) where \( \sigma \) denotes the sum of divisors function. For over a thousand years, only this pair, 220 and 284, was known and discovered by Iamblichus in the fourth century BC. Later Thabit ibn Qurra, Fermat, Descartes, Euler, and many others made some progress on studying these numbers. Today, close to twelve million amicable numbers are known (cf. Jan Munch Pedersen’s extensive
list of amicable pairs at [23]). Let \( A(x) \) denote the number of amicable pairs \( \leq x \). Carl Pomerance has shown that

\[
A(x) \ll x \cdot \exp\{-c \log x \log \log x^{1/3}\}
\]

for some \( c > 0 \) (see [24], [25]). It is still unknown as to whether or not infinitely many amicable pairs exist. Also, it remains an open question as to whether any amicable pairs of opposite parity exist. We have considered a related question of Florian Luca’s of determining all positive integers \( a \) such that \( a \) and \( a+1 \) are amicable [14]. I am interested in the following:

**Conjecture 1.** There exists no amicable pairs of the form \((a, a+1)\) where \( a \) is a positive integer.

It is not too difficult to show that if such a solution exists, then \( a \) is an odd square and \( a + 1 = 2^\alpha m^2 \) with \( m \) odd and \( \alpha \geq 1 \). Evidently, this problem is related to the study of quasi-perfect and almost-perfect numbers (i.e. \( n \) such that \( \sigma(n) = 2n+1 \) and \( \sigma(n) = 2n-1 \), respectively).

**References**


[3] D. Baczkowski, M. Filaseta, F. Luca and O. Trifonov, *On values of \( \frac{d(n)!}{m} \), \( \frac{\phi(n)!}{m} \) and \( \frac{\sigma(n)!}{m} \)*, accepted by Int. J. of Number Theory.


