Numerology or Number Theory?

Nathan Ryan

September 27th, 2012
If you want the number you can find it everywhere. 216 steps from your street corner to your front door, 216 seconds you spend in the elevator, whatever. When your mind becomes obsessed you filter everything else out and find that thing everywhere. You’ve chosen 216 and you’ll find it everywhere in nature. But, Max, as soon as you discard scientific rigour, you are no longer a mathematician, you’re a numerologist.
Numerology has unquestionably stimulated investigations in number theory and bequeathed to us some most difficult problems.

- Perfect numbers
- Amicable numbers
- Sociable numbers
Six is a perfect number in itself, and not because God created all things in six days; rather the converse is true: God created all things in six days because the number is perfect.

St. Augustine, ca. 1600 years ago in City of God.

Our ancestor Jacob prepared his present in a wise way. This number 220 is a hidden secret, being one of a pair of numbers such that the parts of it are equal to the other one 284, and conversely. And Jacob had this in mind; this has been tried by the ancients in securing the love of kings and dignitaries.

Abraham Azulai, ca. 500 years ago.
If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect.

Euclid, ca. 2300 years ago:

That is, if $1 + 2 + \cdots + 2^k = 2^{k+1} - 1$ is prime, then $2^k(2^{k+1} - 1)$ is perfect.
First series of experiments:

- Are there odd perfect numbers?
- Are there amicable pairs coprime to 6? 30? 210?
- Are there sociable numbers of period 3? 4?
By experimental mathematics one typically means

1. gaining insight and intuition;
2. visualizing math principles;
3. discovering new relationships;
4. testing and especially falsifying conjectures;
5. exploring a possible result to see if it merits formal proof;
6. suggesting approaches for formal proof;
7. computing replacing lengthy hand derivations;
8. confirming analytically derived results.

And by experimental number theory I mean these ideas applied in number theoretic settings.
What is numerology?

► Historically numerology is any study of the purported divine, mystical or other special relationship between a count or measurement and observed or perceived events.

► To an experimental mathematician its noticing a few instances of a (potential) larger pattern and making an inference from that. Then the inference is tested.
The (in)famous Riemann zeta function:

▶ The function

\[
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}
\]

converges when \( \text{Re} s > 1 \) and is never 0 in this region.

▶ If we set

\[
\xi(s) = \frac{1}{2} \pi^{-s/2} s(s - 1) \Gamma(s/2) \zeta(s),
\]

then this function satisfies a functional equation

\( \xi(s) = \xi(1 - s) \). To cancel out the poles of \( \Gamma(s) \) at the negative integers, we see \( \zeta(s) \) has zeros at the negative even integers \(-2, -4, \ldots\). These are the \textit{trivial} zeros.

▶ The Riemann hypothesis says

\textit{All the nontrivial zeros of} \( \zeta(s) \) \textit{lie on the line} \( \text{Re} s = \frac{1}{2} \)
Why $\zeta$?

- Special values: the probability that as $x$ goes to infinity $N$ positive integers less than $x$ chosen uniformly at random will be relatively prime approaches $\zeta(N)$;
- $\zeta(2) = \pi^2/6$, $\zeta(3)$ is known to be irrational but is it transcendental?

Why RH?

- No zeros along the $\text{Re}s = 1$ line is equivalent to the Prime Number Theorem. (Wiener, 1951)
- The Riemann hypothesis is equivalent to the “best possible” bound for the error of the prime number theorem. (van Koch, 1901)
<table>
<thead>
<tr>
<th>Year</th>
<th>number of zeros</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1859ish</td>
<td>3</td>
<td>Riemann</td>
</tr>
<tr>
<td>1903</td>
<td>15</td>
<td>Gram</td>
</tr>
<tr>
<td>1914</td>
<td>79</td>
<td>Backlund</td>
</tr>
<tr>
<td>1925</td>
<td>138</td>
<td>Hutchinson</td>
</tr>
<tr>
<td>1935</td>
<td>1041</td>
<td>Titchmarsh</td>
</tr>
<tr>
<td>1953</td>
<td>1104</td>
<td>Turing</td>
</tr>
<tr>
<td>1956</td>
<td>15000</td>
<td>Lehmer</td>
</tr>
<tr>
<td>1956</td>
<td>25000</td>
<td>Lehmer</td>
</tr>
<tr>
<td>1958</td>
<td>35337</td>
<td>Meller</td>
</tr>
<tr>
<td>1966</td>
<td>250000</td>
<td>Lehman</td>
</tr>
<tr>
<td>1968</td>
<td>3500000</td>
<td>Rosser-Yohe-Schoenfeld</td>
</tr>
<tr>
<td>1977</td>
<td>400000000</td>
<td>Brent</td>
</tr>
<tr>
<td>1979</td>
<td>81000001</td>
<td>Brent</td>
</tr>
<tr>
<td>1982</td>
<td>200000001</td>
<td>Brent-van de Lune-te Riele-Winter</td>
</tr>
<tr>
<td>1983</td>
<td>300000001</td>
<td>van de Lune-te Riele</td>
</tr>
<tr>
<td>1986</td>
<td>1500000001</td>
<td>van de Lune-te Riele-Winter</td>
</tr>
<tr>
<td>2004</td>
<td>9000000000000</td>
<td>Wedeniwski</td>
</tr>
<tr>
<td>2004</td>
<td>100000000000000</td>
<td>Gourdon-Demichel</td>
</tr>
</tbody>
</table>
Why bother?

- Mallory: “Because it’s there”
- Pólya: “Intuition comes to us much earlier and with much less outside influence than formal arguments.”
- Galileo: “All truths are easy to understand once they are discovered; the point is to discover them.”
What are elliptic curves?

- An elliptic curve is a smooth, projective algebraic curve of genus one, on which there is a specified point $O$.

Theorem (Mordell)

*The group of rational points $E(\mathbb{Q})$ on an elliptic curve is a finitely generated abelian group.*
Conjecture (Birch and Swinnerton-Dyer)

Let $r$ be the rank of $E(\mathbb{Q})$ and let $N_p = E(\mathbb{F}_p)$. Then

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \log(x)^r \text{ as } x \to \infty.$$ 

They only went up to $p \leq 1000$!!!
Elliptic curve L-functions:

- Define $a_p = p + 1 - N_p$ and set for almost all $p$, $L_p(T) = 1 - a_p T + p T^2$ (for exposition we omit those $p$ for which the curve $E$ has not-good reduction).

- Then we define the series

$$L(E, s) = \prod_{p} \frac{1}{L_p(p^{-s})}.$$ 

- The coefficients of this L-series are multiplicative and has an analytic continuation to all of $\mathbb{C}$. If we define

$$\Lambda(E, s) = \left(\frac{N_E}{Q}\right)^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s)$$

then

$$\Lambda(E, s) = \omega \Lambda(E, 2 - s).$$
Conjecture (BSD (t-shirt version))

Let $r$ be the rank of the group $E(\mathbb{Q})$ and let

$$r_{an} := \text{ord}_{s=1} L(E, s).$$

Then $r = r_{an}$.

Evidence:

- (Cremona 2011) There are 614308 isogeny class of elliptic curves with conductor $N_{E/\mathbb{Q}} \leq 140000$. All have $r_{an} \leq 3$ and in every case $r_{an} = r$. 
Conjecture (BSD (awesome version))

Let everything you see be an important invariant of an elliptic curve \( E \):

\[
\frac{L^{(r)}(E, 1)}{r!} = \frac{\#Sha(E) \Omega_E R_E \prod_{p|n} c_p}{(\# E_{tor})^2}.
\]

Cremona has also checked this for all his curves (modulo the huge fact that almost nothing is known about Sha).
Numerology has lead to a lot of interesting number theory but this is still not experimental number theory.

Why not?

- a matter of scale
- a matter of rigor
- a matter of the tools being used
- a matter of its “generalizability”
Three examples from my work:

- Böcherer’s Conjecture
- Harder’s Conjecture
- Rankin-Convolution of two Siegel modular forms
Let $\mathbb{H}$ be the complex upper halfplane and $k \in \mathbb{Z}$. Let \[ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) = \Gamma \] act on $z \in \mathbb{H}$ via fractional linear transformations: $\gamma(z) = \frac{az+b}{cz+d}$. Then a modular form of weight $k$ is a function $f : \mathbb{H} \to \mathbb{C}$ that is holomorphic on $\mathbb{H}$, and holomorphic at $\infty$ so that

$$f(\gamma(z)) = (cz+d)^k f(z), \text{ for all } \gamma \in \Gamma.$$ 

Note that $f(z) = f(z+1)$ and thus $f$ has a Fourier expansion (here $q = \exp(2\pi iz)$)

$$f(z) = \sum_{n \geq 0} a_f(n) q^n.$$ 

Note that MFs have: (1) a group, (2) a halfplane, (3) holomorphy conditions, and (4) a functional equation in terms of the action of the group on the halfplane.
Siegel Modular Forms

Let $\mathbb{H}_g = \{Z = X + iY \in M(g, \mathbb{C}) : Z^t = Z, Y > 0\}$ and $k \in \mathbb{Z}$. Let $\gamma = (\begin{array}{cc} A & B \\ C & D \end{array}) \in \text{Sp}(2g, \mathbb{Z}) = \Gamma$ act on $Z \in \mathbb{H}_g$ via fractional linear transformations:

$$\gamma(Z) = (AZ + B)(CZ + D)^{-1}.$$ Then a Siegel modular form of weight $k$ and genus $g$ is a function $F : \mathbb{H}_g \to \mathbb{C}$ that is holomorphic on $\mathbb{H}_g$, and holomorphic at $\infty$ so that

$$F(\gamma(Z)) = \det(CZ + D)^k F(Z), \text{ for all } \gamma \in \Gamma.$$

Note that $F(Z) = F(Z + I_g)$ and thus $F$ has a Fourier expansion (here $q$ is suitably defined)

$$F(Z) = \sum_{T \geq 0} a_F(T)q^T.$$

where the $T$ are positive semidefinite quadratic forms.
Examples of Siegel modular forms:
- classical modular forms are Siegel of genus 1;
- given integers $g$ and $\ell$ and a positive definite integer-valued quadratic form $Q$ in $\ell$ variables,

$$\theta_Q^{(g)}(Z) = \sum_{s \in M(g \times \ell, \mathbb{Z})} e^{2\pi i \text{Tr}(Qs^tZs)};$$

is a Siegel modular form of genus $g$ and weight $\ell/2$;
- given a classical modular form of weight $2k - 2$ one can (Saito-Kurokawa) “lift” it to an arithmetically indistinguishable Siegel modular form of weight $k$. 
Why do modular forms belong to arithmetic?

▶ theta series like the above
▶ spaces of modular forms of a fixed weight are finite dimensional and there is a commuting family of normal operators $T(1), T(2), T(3), \ldots$ acting on these spaces. By easy linear algebra there is a basis of eigenforms that are eigenforms for all of the operators $T(n)$. We write

$$f|T(n) = \lambda_f(n)f$$

when $f$ is an eigenform.

▶ These are the Hecke eigenforms and their coefficients are of arithmetic interest.
Let $F$ be a Hecke eigenform of genus 2 and weight $k$. Then we can define

$$L(s, F) = \prod_p \frac{1}{L_p(p^{-s})} = \sum_{n=1}^{\infty} b_n n^{-s}$$

where

$$L_p(T) = 1 - \lambda_F(p) T + (\lambda_F(p)^2 - \lambda_F(p^2) - p^{2k-4}) T^2 - \lambda_F(p) p^{2k-3} T^3 + p^{4k-6} T^4.$$ 

and $b_n$ is the result of carrying out the multiplication.

- This is an L-function in that it has an analytic continuation, a functional equation (though I typically normalize so that the functional equation is $s \mapsto 1 - s$), has multiplicative coefficients $b_n$, etc.

- Consider a quadratic Dirichlet character $\chi_D = \left( \frac{D}{.} \right)$. Then one can “twist” the original L-function to get

$$L(s, F \otimes \chi_D) = \sum_{n=1}^{\infty} b_n \chi_D(n) n^{-s}.$$
L functions and central values

- vanishings are of particular interest (BSD says a vanishing implies $E(\mathbb{Q})$ is infinite); vanishings of families of twists especially (Random matrix theorem predictions);
- want to do this with SMFs but how do we know $L(s, 1/2, F \otimes \chi_D)$ is 0? It’s a floating point number on a computer.

Nathan Ryan Numerology or Number Theory?
We need a discretization: Böcherer’s Conjecture (as investigated by myself and Gonzalo Tornaría) relates the central values $L(1/2, F \otimes \chi_D)$ to an average of Fourier coefficients of $F$ indexed by quadratic forms of discriminant $D$.

In particular,

$$B_{\ell,F}(D)^2 = \alpha_{\ell D} k_F L(1/2, F \otimes \chi_\ell) L(F, 1/2, F \otimes \chi_D) |D\ell|^{k-1}$$

for some positive constant $k_F$ independent of $\ell$ and $D$.

made use of some “magical” numerical integration techniques and convergence accelerators.
Consider the classical modular form

$$\Delta(q) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots = \sum_{n=1}^{\infty} \tau(n)q^n.$$ 

Ramanujan discovered a number of congruences involving the coefficients of $\Delta$: e.g.,

$$\tau(p) \equiv p^{11} + 1 \pmod{691}$$

for all primes $p$.

This is part of a more general phenomenon: if a “large” prime $\ell \geq k - 1$ divides the numerator of the zeta-value $\zeta(-k+1)$, then the constant term of the Eisenstein series $E_k$ is zero modulo $\ell$. This can be interpreted to say that there is a congruence mod $\ell$ between this Eisenstein series and some cuspidal eigenform of weight $k$. 

Nathan Ryan

Numerology or Number Theory?
Harder’s Conjecture:

Let $f$ be a classical Hecke eigenform of weight $r$ and let $t \in \mathbb{Z}$. If a “large” prime $\ell$ divides the algebraic part of the special value of $L(f, t)$, then there exists a Siegel modular form $F$ of a weight determined by $t$ and $r$ so that there is a congruence involved the Hecke eigenvalues of $F$ and $f$ modulo $\ell$.

In work with Alex Ghitza and David Sulon we verified this conjecture in a dozen or so cases.

In order to find the algebraic part of an a special value we made heavy use of the “magical” LLL algorithm.
Consider two Siegel Hecke eigenforms $F, G$ of genus 2 and weight $k$. One can write their Fourier expansions as

$$F(Z) = \sum_{N=1}^{\infty} F_N q^N, \text{ and } G(Z) = \sum_{N=1}^{\infty} G_N q^N.$$ 

one can form the infinite sum

$$D_{F,G}(s) := \zeta(2s - 2k + 4) \sum_{N \geq 1} \langle F_N, G_N \rangle N^{-s}$$

where $\langle \cdot, \cdot \rangle$ is the so-called Petersson inner-product.

when $F$ is a Saito-Kurokawa lift the series $D_{F,F}$ is just the L-function of $F$ we defined above.
What about \( D_{F,F}(s) \) when \( F \) is not a lift?

- Skoruppa, Strömberg and I prove numerically that in this case \( F \) is not even an L-function since the coefficients of \( D_{F,F}(s) \) aren’t multiplicative;
- We used the “magic” of interval arithmetic to be provably sure that our computations were correct.
To conclude I’d like to say that much of my research follows a

Theory developing algorithms, knowing what questions to ask

Computation implementing the algorithms, carrying out large scale computations efficiently

Theory understanding what we see in our computations, using the data to rework our conjectures and hypotheses, apply the data to some larger framework, ask more questions

Cycle rinse and repeat