The elusive Bernoulli numbers

Pieter Moree

Max Planck Institute for Mathematics, Bonn

Luxembourg, December 17, 2019

Jakob Bernoulli (1654-1705)

Seki Kowa (1642-1708)

Overview of the talk

- History and definitions
- (Ir)regular Bernoulli-primes
- (Ir)regular Gennochi-primes
- Counting G-irregular primes
- Counting G-irregular primes in AP
- Denominator of Bernoulli polynomials
- Kellner's denominator conjectures
- Kellner-Erdős-Moser conjecture (if time permits!)

Middle ages...

For natural numbers $m, k \geq 1$ consider the power sum

$$S_k(m) := 1^k + 2^k + \cdots + (m-1)^k.$$

We have $S_1(m) = m(m-1)/2$.
Likewise, $S_2(m) = (m-1)m(2m-1)/6$.
Further, $S_3(m) = m^2(m-1)^2/4 = S_1(m)^2$.

Theorem Faulhaber (1580-1635)

If $2 \nmid k$, then $S_k(m) = F_k(S_1(m))$, $\deg(F_k) = (k+1)/2$.
If $2 \mid k$, then $S_k(m) = S_2(m)G_k(S_1(m))$, $\deg(G_k) = (k-2)/2$.

Enter Bernoulli-Seki numbers

We have

$$S_k(m) = \frac{1}{k+1}\sum_{j=0}^{k}\binom{k+1}{j}B_j m^{k+1-j},$$

with

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

The B_k are called Bernoulli-Seki numbers.
$B_0 = 1,\ B_1 = -1/2$
$B_{2k+1} = 0$
$B_2 = 1/6, B_4 = -1/30, B_6 = 1/42, B_8 = -1/30,$
$B_{10} = 5/66, B_{12} = -691/2730$

Jakob Bernoulli: close-up

... Atque si porrò ad altiores gradatim potestates pergere, levique negotio sequentem adornare laterculum licet :

Summae Potestatum

$\int n = \frac{1}{2}nn + \frac{1}{2}n$
$\int nn = \frac{1}{3}n^3 + \frac{1}{2}nn + \frac{1}{6}n$
$\int n^3 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}nn$
$\int n^4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$
$\int n^5 = \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}nn$
$\int n^6 = \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 - \frac{1}{6}n^3 + \frac{1}{42}n$
$\int n^7 = \frac{1}{8}n^8 + \frac{1}{2}n^7 + \frac{7}{12}n^6 - \frac{7}{24}n^4 + \frac{1}{12}nn$
$\int n^8 = \frac{1}{9}n^9 + \frac{1}{2}n^8 + \frac{2}{3}n^7 - \frac{7}{15}n^5 + \frac{2}{9}n^3 - \frac{1}{30}n$
$\int n^9 = \frac{1}{10}n^{10} + \frac{1}{2}n^9 + \frac{3}{4}n^8 - \frac{7}{10}n^6 + \frac{1}{2}n^4 - \frac{1}{12}nn$
$\int n^{10} = \frac{1}{11}n^{11} + \frac{1}{2}n^{10} + \frac{5}{6}n^9 - 1n^7 + 1n^5 - \frac{1}{2}n^3 + \frac{5}{66}n$

Quin imò qui legem progressionis inibi attentuis ensperexit, eundem etiam continuare poterit absque his ratiociniorum ambabimus : Sumtâ enim c pro potestatis cujuslibet exponente, fit summa omnium n^c seu

$$\int n^c = \frac{1}{c+1}n^{c+1} + \frac{1}{2}n^c + \frac{c}{2}An^{c-1} + \frac{c \cdot c-1 \cdot c-2}{2 \cdot 3 \cdot 4}Bn^{c-3}$$
$$+ \frac{c \cdot c-1 \cdot c-2 \cdot c-3 \cdot c-4}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}Cn^{c-5}$$
$$+ \frac{c \cdot c-1 \cdot c-2 \cdot c-3 \cdot c-4 \cdot c-5 \cdot c-6}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8}Dn^{c-7} \ldots \text{\& ita deinceps,}$$

exponentem potestatis ipsius n continué minuendo binario, quosque perveniatur ad n vel nn. Literae capitales A, B, C, D & c. ordine denotant coëfficientes ultimorum terminorum pro $\int nn$, $\int n^4$, $\int n^6$, $\int n^8$, & c. nempe

$$A = \frac{1}{6}, B = -\frac{1}{30}, C = \frac{1}{42}, D = -\frac{1}{30}.$$

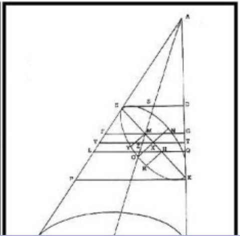
Jakob Bernoulli: charming words...

With the help of this table it took me less than half of a quarter of an hour to find that the tenth powers of the first 1000 numbers being added together will yield the sum

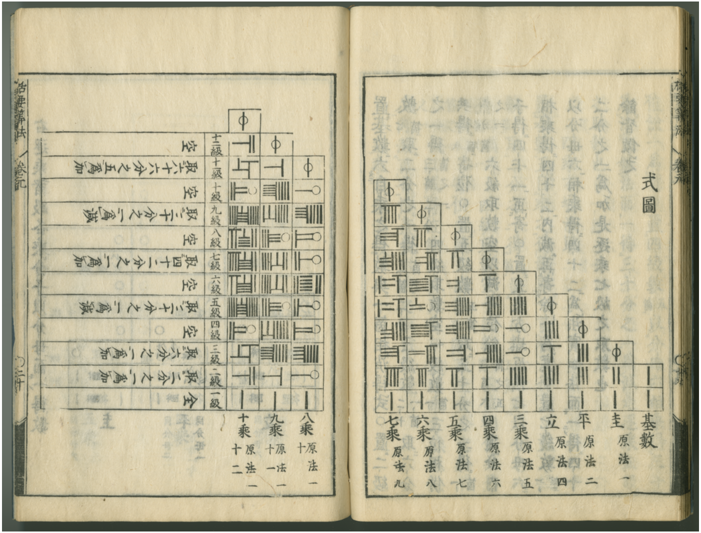
$$91,409,924,241,424,243,424,241,924,242,500$$

From this it will become clear how useless was the work of Ismael Boulliau spent on the compilation of his voluminous Arithmetica Infinitorum in which he did nothing more than compute with immense labour the sums of the first six powers, which is only a part of what we have accomplished in the space of a single page."


ISMAELIS BULLIALDI
OPVS NOVVM
AD
ARITHMETICAM
INFINITORUM
Libris sex comprehensum,
In quo plura à nullis hactenus edita demonstrantur.



Seki Kowa: close-up



(Ir)regular Bernoulli primes, I

Let $p > 2$ be a prime. Write

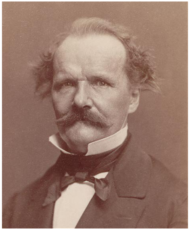
$$h_p = \text{class number of } \mathbb{Q}(\zeta_p)$$
$$h_p^+ = \text{class number of } \mathbb{Q}(\zeta_p + \zeta_p^{-1})$$

Kummer showed that

$$h_p^- = h_p/h_p^+ \in \mathbb{N}$$

An odd prime p is regular if and only if $p \nmid h_p^-$.
Irregular: 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, . . .

Ernst Eduard Kummer (1810-1893)



(Ir)regular Bernoulli primes, II

Kummer's goal was to prove Fermat's Last Theorem.

Kummer

If p is regular, then $x^p + y^p = z^p$ has only trivial solutions.

Write $B_k = U_k/V_k$ with $(U_k, V_k) = 1$.

Kummer (1850)

The prime p is irregular if $p \mid U_k$ for some $k \in \{2, 4, \ldots, p-3\}$. The pair (k, p) is said to be an irregular pair.

Kummer (1851)

If $\ell \equiv k \not\equiv 0 \pmod{p-1}$, then $\frac{B_\ell}{\ell} \equiv \frac{B_k}{k} \pmod{p}$.

What is known

It is not known whether there are infinitely many regular primes!

Jensen, 1915

There are infinitely many primes $p \equiv 5 \pmod 6$ that are irregular.

Best result in this spirit to this date:

Metsänkylä, 1976

Given an integer $m > 2$, let H be a proper subgroup of $\mathbb{Z}_m^*$. Then there exist infinitely many irregular primes not lying in the residue classes in H.

Put $\pi_B(x) = \#\{p \leq x \ : \ p \text{ is irregular}\}$.

Luca, Pizarro-Madariaga and Pomerance (2015)

$$\pi_B(x) \geq (1 + o(1)) \frac{\log \log x}{\log \log \log x}.$$

Siegel's heuristics

Heuristic of Siegel, 1954

We should have

$$\pi_B(x) \sim \left(1 - \frac{1}{\sqrt{e}}\right)\pi(x) \sim 0.39\ldots \frac{x}{\log x}.$$

The reasoning behind this conjecture is as follows. We assume that U_{2k}, the numerator of B_{2k}, is not divisible by p with probability $1 - 1/p$. Therefore, on assuming independence of divisibility by distinct primes, we expect that p is regular with probability

$$\left(1 - \frac{1}{p}\right)^{\frac{p-3}{2}},$$

which, with increasing p, tends to $e^{-1/2}$.

The refined class number – general definition

- K number field
- S=finite set of places, including all the infinite ones
- $\mathcal{O}_S$ = ring of S-integers
- $\zeta_S(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_S} (N\mathfrak{a})^{-s}$
- T finite set of places disjoint from S
- $\zeta_{S,T}(s) = \prod_{v \in T} (1 - Nv^{1-s}) \zeta_S(s)$
- $\zeta_{S,T}(s) = -\frac{h_{S,T} R_{S,T}}{w_{S,T}} s^n \pmod{s^{n+1}}$, $n = \#S - 1$

The refined class number – in particular

- $K_p = \mathbb{Q}(\zeta_p)$, $K_p^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$
- S_p, S_p^+ = set of all infinite places of K_p, respectively K_p^+
- T_p, T_p^+ = finite set of places above 2
- $h_{p,2}$ = the (S_p, T_p)-refined class number
- $h_{p,2}^+$ = the (S_p^+, T_p^+)-refined class number
- $h_{p,2}^- = h_{p,2}/h_{p,2}^+ \in \mathbb{N}$

Theorem

If p is Gennochi-irregular (G-irregular), then $p \mid h_{p,2}^-$.
If $2^{p-1} \not\equiv 1 \pmod{p^2}$, then the converse is also true.

Genocchi numbers

Angelo Gennochi
(1817-1889)

The Genocchi numbers have the generating series

$$\frac{2t}{e^t + 1} = \sum_{k=1}^{\infty} G_k \frac{t^k}{k!}, \;\; G_k = 2(1 - 2^k)B_k.$$

A prime p is G-regular if $p \nmid G_2 G_4 \cdots G_{p-3}$.
The first few G-irregular ones are:

$$17, 31, 37, 41, 43, 59, 67, 73, 89, 97, 101, 103, 109, \ldots$$

Su Hu, Min-Soo Kim, M. and Min Sha
Irregular primes with respect to Gennochi numbers and Artin's primitive root conjecture
Journal of Number Theory **205** (2019), 59–80.

Counting G-irregular primes

Observation

An odd prime p is G-regular iff it is B-regular and satisfies $\mathrm{ord}_p(4) = (p-1)/2$.

$$\mathrm{ord}_p(a) = \min\{k \geq 1 : a^k \equiv 1 \pmod{p}\}.$$

Note that $\mathrm{ord}_p(4) \mid (p-1)/2$.

$5, 7, 11, 13, 19, 37, 47, 53, 59, 61, 67, 71, 79, 83, 101, 103, \ldots$

Question

Are there infinitely many primes p such that $\mathrm{ord}_p(4) = (p-1)/2$?

This is an Artin primitive root type conjecture

Counting near-primitive roots

Put $\mathcal{P}(g,t) = \{p : p \equiv 1 \pmod{t},\ \text{ord}_p(g) = (p-1)/t\}$.

Theorem [Wagstaff (1982), method of Hooley (1967)]

Under GRH, we have

$$\mathcal{P}(g,t)(x) = (\delta_g(t) + o(1))\frac{x}{\log x}.$$

Unconditionally we have, for all x large enough,

$$\mathcal{P}(g,t)(x) \le (\delta_g(t) + \epsilon)\frac{x}{\log x}.$$

Making the density explicit

Continued

We have

$$\delta_g(t) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{nt}, g^{1/nt}) : \mathbb{Q}]}$$

with

$$\delta_g(t)/A \in \mathbb{Q}$$

explicit, and

$$A = \prod_q \left(1 - \frac{1}{q(q-1)}\right) \approx .3739558136192022880547\ldots$$

the Artin constant.

Our case: computing $\delta_4(2)$

We have

$$\delta_4(2) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_{2n}, 2^{1/n}) : \mathbb{Q}]}$$

Note that $\sqrt{2} \in \mathbb{Q}(\zeta_m)$ iff $8 \mid m$.
Assume $4 \nmid n$. We have

$$[\mathbb{Q}(\zeta_{2n}, \sqrt{2} : \mathbb{Q}] = 2\varphi(2n).$$

$$[\mathbb{Q}(\zeta_{2n}, 2^{1/n}) : \mathbb{Q}] = n\varphi(2n).$$

We find that

$$\delta_4(2) = \sum_{n=1}^{\infty} \frac{\mu(n)}{\varphi(2n)n} = \frac{3}{4} \sum_{2\nmid n}^{\infty} \frac{\mu(n)}{\varphi(n)n} = \frac{3}{2}A.$$

Counting G-irregular primes

Theorem

Asymptotically we have

$$\pi_G(x) > \Big(1 - \frac{3}{2}A - \epsilon\Big)\pi(x) > 0.439 \cdot \pi(x).$$

Conjecture

Asymptotically we have

$$\pi_G(x) \sim \Big(1 - \frac{3A}{2\sqrt{e}}\Big)\pi(x) \approx 0.66 \cdot \pi(x).$$

G-irregular primes in AP

An odd prime p is G-regular iff it is B-regular and satisfies $\mathrm{ord}_p(4) = (p-1)/2$.

Observation

Primes p satisfying $p \equiv 1 \pmod 8$ are G-irregular.

$$1 = \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv 4^{\frac{p-1}{4}} \pmod p.$$

$$\overline{17}, 31, 37, \overline{41}, 43, 59, 67, \overline{73}, \overline{89}, \overline{97}, 101, 103, 109, \ldots$$

Question

Does each primitive residue class contain infinitely many G-irregular primes?

Primes in AP with prescribed primitive root

This density, under GRH, was first explicitly determined by the speaker (around 1998). For Genocchi we need a simple variation:

$$\mathcal{Q}(d,a)(x) = \{p > 2 : p \equiv a \pmod{d},\ \ \mathrm{ord}_p(4) = (p-1)/2\}$$

Unconditionally

$$\mathcal{Q}(d,a)(x) < \frac{(\delta(d,a)+\epsilon)}{\varphi(d)}\frac{x}{\log x},$$

with $\delta(d,a)/A \in \mathbb{Q}$ and explicit.
Under GRH, we have

$$\mathcal{Q}(d,a)(x) = \frac{(\delta(d,a)+o(1))}{\varphi(d)}\frac{x}{\log x}.$$

Practice versus theory

Table: The ratio $\mathcal{Q}(d,a)(x)/\pi(x;d,a)$ for $x = 5 \cdot 10^6$

$p \equiv a \pmod{d}$	experimental	$\delta(d,a)$
$p \equiv 1 \pmod{3}$	0.449049	0.448746
$p \equiv 2 \pmod{5}$	0.589614	0.590456
$p \equiv 1 \pmod{4}$	0.374664	0.373955
$p \equiv 9 \pmod{20}$	0.395498	0.393637
$p \equiv 11 \pmod{12}$	0.898284	0.897493
$p \equiv 19 \pmod{20}$	0.789316	0.787275
$p \equiv 7 \pmod{8}$	0.747300	0.747911
$p \equiv 13 \pmod{24}$	0.598815	0.598329

Counting G-irregular primes in AP

Theorem

For all x sufficiently large,

$$\pi_G(d,a)(x) > (1-\delta(d,a)-\epsilon)\pi(x;d,a).$$

Conjecture

Asymptotically we have

$$\pi_G(d,a)(x) \sim \left(1-\frac{\delta(d,a)}{\sqrt{e}}\right)\pi(x;d,a).$$

Bernoulli polynomials

The Bernoulli polynomials have the generating series

$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}.$$

We have

$$B_n(X) = \sum_{k=0}^{n} \binom{n}{k} B_k X^{n-k}.$$

$$S_{n-1}(N) = \sum_{j=1}^{N-1} j^{n-1} = \frac{B_n(N) - B_n}{N} = \frac{\widetilde{B}_n(N)}{N}.$$

Denominator

$s_b(n)$ = sum of the base b digits of n

$$\mathfrak{P}_n = \prod_{\substack{p \text{ prime} \\ s_p(n) \geq p}} p, \quad \mathfrak{P}_n^+ = \prod_{\substack{p > \sqrt{n} \\ s_p(n) \geq p}} p, \quad \mathfrak{P}_n = \mathfrak{P}_n^- \mathfrak{P}_n^+$$

Kellner (2017)

$$\mathfrak{P}_n \widetilde{B}_n(X) \in \mathbb{Z}[X]$$

Example

$\widetilde{B}_5(X) = B_5(X) = X^5 - \frac{5}{2}X^4 + \frac{5}{3}X^3 - \frac{1}{6}X$
$s_2(1.4 + 1) = 2, s_3(1.3 + 2) = 3, s_5(1.5) = 1, s_p(5) = 1$

$$\mathfrak{P}_5 = 6$$

Kellner's conjectures

Conjecture (Kellner, 2017)

a) For $n > 192$ we have $P(\mathfrak{P}_n^+) > \sqrt{n}$.

b) There is some absolute constant $\kappa > 0$ such that

$$\omega(\mathfrak{P}_n^+) \sim \kappa \frac{\sqrt{n}}{\log n}, \quad n \to \infty$$

Theorem (BLMS, 2018)

a) For $n > n_0$ we have $P(\mathfrak{P}_n^+) \gg n^{20/37}$.

b) Asymptotically

$$\omega(\mathfrak{P}_n^+) \sim 2 \frac{\sqrt{n}}{\log n}.$$

c) $\log(\mathfrak{P}_n^+) \sim \sqrt{n}$

Consecutive denominators

O. Bordellès, F. Luca, P. Moree and I.E. Shparlinski,
Denominators of Bernoulli polynomials,
Mathematika **64** (2018), 519–541.

Behaviour of consecutive denominators

For any $x \geq 3$ we have:

- the divisibility $\mathfrak{P}_{n+1} \mid \mathfrak{P}_n$ holds for all except maybe at most $o(x)$ positive integers $n \leq x$
- the divisibility $\mathfrak{P}_{n+1} \mid \mathfrak{P}_n$ and the inequality $\mathfrak{P}_n > \mathfrak{P}_{n+1}$ hold simultaneously for at least $(\log 2 + o(1))x$ positive integers $n \leq x$ as $x \to \infty$;
- the equality $\mathfrak{P}_q = \mathfrak{P}_{q+1}$ holds for all except maybe at most $o(\pi(x))$ primes $q \leq x$

Small primes dividing $\mathfrak{P}_n$

Theorem

All primes $p \leq (1/2 - \epsilon) \log\log n / \log\log\log n$, with at most one exception, divide $\mathfrak{P}_n$ for all n large enough.

As $2 \nmid \mathfrak{P}_{2^n}$, the exceptional prime sometimes exists.

Theorem (Stewart, 1980)

For $n > 25$ we have

$$s_a(n) + s_b(n) > \frac{\log\log n}{\log\log\log n + C(a,b)} - 1,$$

for some constant $C(a, b)$.

We made $C(a, b)$ explicit.

Kellner-Erdős-Moser Conjecture

Conjecture (Bernd Kellner, 2011)

If m and k are positive integers with $m \geq 3$ then the ratio $S_k(m+1)/S_k(m)$ is an integer iff $(m,k) \in \{(3,1),(3,3)\}$.

Since $S_k(m+1) = S_k(m) + m^k$, we have

$$\frac{S_k(m+1)}{S_k(m)} \in \mathbb{Z} \text{ iff } \frac{m^k}{S_k(m)} \in \mathbb{Z}.$$

Kellner-Erdős-Moser Conjecture

For positive integers a, k, m with $m \geq 3$,

$$aS_k(m) = m^k \iff (a,k,m) \in \{(1,1,3),(3,3,3)\}$$

The case $a = 1$: The Erdős-Moser conjecture

Conjecture (P. Erdős, 1950)

The equation $1^k + 2^k + \cdots + (m-1)^k = m^k$ has only $1 + 2 = 3$ as a solution.

Theorem (L. Moser, 1953)

If (m, k) is a solution with $k \geq 2$, then $m > 10^{10^6}$.

Can be sharpened to $m > 10^{9 \cdot 10^6}$.

Theorem (Y. Gallot, M., W. Zudilin, 2011)

If (m, k) is a solution with $k \geq 2$, then $m > 10^{10^9}$.

Results on $aS_k(m) = m^k$

Theorem (I. Baoulina and M., 2015)

Suppose that (m, k) is a nontrivial solution of $aS_k(m) = m^k$ and p is a prime dividing m. Then

- *p is an irregular prime;*
- $p^2 \mid U_k$;
- $k \equiv r \pmod{p-1}$ *for some irregular pair (r, p).*

Generalizes case $a = 1$ [M., te Riele and Urbanowicz (1994)].

Corollary 1

If a has a regular prime divisor, then the equation $aS_k(m) = m^k$ has no nontrivial solutions.

(Ir)regular Bernoulli primes, III

Let $\mathcal{I}$ be the set of integers composed solely of irregular primes.

Suppose that $0 < \delta < 1$. *If*

$$\pi_B(x) < (1-\delta)\frac{x}{\log x}, \ x \to \infty,$$

then $\mathcal{I}(x) \ll x(\log x)^{-\delta}$ *and, in particular,* $\mathcal{I}$ *has natural density* 0.

(That is $\mathcal{I}(x)/x \to 0$ as $x \to \infty$.)

Under the above assumption on $\pi_B(x)$ *we have that the set of possible integer ratios of consecutive power sums is of density zero.*

THANK YOU!

...and thank you, Bernd Kellner!

References

- Su Hu, Min-Soo Kim, Pieter Moree and Min Sha
  Irregular primes with respect to Gennochi numbers and Artin's primitive root conjecture
  Journal of Number Theory **205** (2019), 59–80.
- O. Bordellès, F. Luca, P. Moree and I.E. Shparlinski,
  Denominators of Bernoulli polynomials,
  Mathematika **64** (2018), 519–541.
- I.N. Baoulina and P. Moree, Forbidden integer ratios of consecutive power sums, in "From Arithmetic to Zeta-Functions - Number Theory in Memory of Wolfgang Schwarz", Eds. J. Sander, J. Steuding and R. Steuding, Springer, 2016, 1–30.

My other EM papers

- Research
- M., H.J.J. te Riele, J. Urbanowicz, Divisibility properties of integers x, k satisfying $1^k + \cdots + (x-1)^k = x^k$, *Math. Comp.* **63** (1994), 799-815.
- On a theorem of Carlitz-von Staudt, *C. R. Math. Rep. Acad. Sci. Canada* **16** (1994), 166-170.
- Diophantine equations of Erdös-Moser type, *Bull. Austral. Math. Soc.* **53** (1996), 281-292.
- Y. Gallot, M. and W. Zudilin, The Erdős-Moser equation $1^k + 2^k + \cdots + (m-1)^k = m^k$ revisited using continued fractions, *Math. Comp.* **80** (2011), 1221-1237.
- Educational
- A top hat for Moser's four mathemagical rabbits, *Amer. Math. Monthly* **118** (2011), 364-370.
- Moser's mathemagical work on the equation $1^k + 2^k + \ldots + (m-1)^k = m^k$, *Rocky Mountain J. of Math.*, **43** (2013), 1707-1737.