The Kummer & Courant conjectures and the two-semicircle method

Klaus Braun
Juli 30, 2022
riemann-hypothesis.de

The Kummer conjecture

The Kummer conjecture is about the distribution of the cubic exponential sums

$$S_p = \sum_{n=1}^{p} e(\frac{n^3}{p}),\ e(x) \coloneqq e^{2\pi i x}$$

with $p = 1 mod 3$ prime, (DuA). The well known bound $|S_p| \leq 2\sqrt{p}$ can be written in the form

$$\frac{S_p}{2\sqrt{p}} = \cos(2\pi\theta_p),\ \theta_p \in [0,1].$$

It is the real part of an explicit root of unity with range $(-1,1)$. Kummer's observed that $\cos(2\pi\theta_p)$ tended to lay more frequently in the interval $I_1 \coloneqq (\frac{1}{2}, 1)$ than in $I_2 \coloneqq (-\frac{1}{2}, \frac{1}{2})$ or $I_3 \coloneqq \left(-1, -\frac{1}{2}\right)$, distributed with the ratio was $3:2:1$.

From Kummer's paper (KuE6) we „quote" (translation by the author):

> *„If p is a prime in the form $p = 3n + 1$ and g a primitive root of it, then the series $1, g^1, g^2, g^3, \dots g^{n-2}$ can be ordered into the three different series $1, g^3, g^6, \dots g^{p-4}$, $g^4, g^7, \dots g^{p-3}$, $g^2, g^5, g^8 \dots g^{p-2}$. The remainders of the first series for the module p are the cubics remainders, from which we note an arbitrary one with α; the remainders of the second and third series, which we denote with β and γ, are the cubic non-remainders. The related Gaussian series*
>
> $$z_1 = \sum_0^{p-1} cos\,(\frac{2\alpha k^3\pi}{p})\ ,\ z_2 = \sum_0^{p-1} cos\,(\frac{2\beta k^3\pi}{p}),\ z_3 = \sum_0^{p-1} cos\,(\frac{2\gamma k^3\pi}{p}).$$
>
> *are the three roots of the following cubic equation:*
>
> $$z^3 = 2pz + pt$$
>
> *where t is uniquely determined by the whole integer solution of the equation $4p = t^2 + 27u^2$ and t being positive resp. negative if it is in the form $3h + 1$ resp. $3h - 1$. … The three series are not uniquely determined by the cubic equation as it is not decided, which of the three roots correspond to the which of the three series. …. I have solved this vagueness in a certain sense, but this solution is insufficient, as it requires the knowledge of the sum of all cubic remainders (and also the sums of both cubic non-remainders) smaller than $\frac{1}{2}p$. …. From those calculated sums I have determined the values of z_1, z_2, z_3 for all primes of the form $3n + 1$ less than 400 and I am publishing those, that another person can find a common law by induction, which was hidden from me. First I notice, that because t lies in the interval $-2\sqrt{p}$ and $2\sqrt{p}$, the three roots of the cubic equation have to lie in the following three intervals $I_1 \coloneqq (-2\sqrt{p}, -\sqrt{p})$, $I_2 \coloneqq (-\sqrt{p}, \sqrt{p})$, $I_3 \coloneqq (\sqrt{p}, 2\sqrt{p})$. I further note, that if one of the three series is known the other two can be rationally expressed out by it; therefore I determine only the series $z_1 = \sum_0^{p-1} cos\,(\frac{2\alpha k^3\pi}{p})$ where one can choose $\alpha := 1$. This series lies in the intervals*
>
> *I_1 : for the primes* $97, 139, 151, 199, 211, 331$
>
> *I_2 : for the primes* $13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397$
>
> *I_3 : for the primes* $7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349.$
>
> *It would now be a matter of searching which peculiarity each of those three have, where no primes is part of the other two series. The linear form of the primes seem to have no meaning, but the quadratic form $4p = t^2 + 27u^2$; perhaps also the form $p = r^2 + 3s^2$. Because I can't discover any law from this, I tried numbers, which are congruent to $\beta^{\frac{p-1}{3}}$ and $\gamma^{\frac{p-1}{3}}$; but also with little success; also, the case if the numbers 2 and 3 are either cubic remainders or not, gave me no hint. In any case the law seems to be built on deeper reasons being worth researching.*

(HaH) §20.6: „… *Die Bearbeitung der Kummerschen Vermutung für kubische Charaktere nach dem Primzahlmodus $p = 1\ mod\ 3$ wäre für die Zahlentheorie vielleicht fruchtbarer als die Bemühungen so vieler Fachleute und Laien um die große Fermatsche Vermutung*".

Remarks: By appealing to a heuristic form of the circle method Patterson's heuristic fell short of a proof of his conjecture explaining the bias observed by Kummer (DuA). This was due to insufficent bounds for the minor arcs. There is also a refinement from the Patterson conjecture that features an error term capturing square root cancellation. In (DuA) the Patterson conjecture is confirmed conditionally on the assumption of the Generalized Riemann Hypothesis, i.e. all non-trivial zeros of all Dirichlet L –functions have real part equal to $1/2$.

Gaussian numbers

The prime elements of $Z[i]$ are also known as Gaussian primes. An associate of a Gaussian prime is also a Gaussian prime. The conjugate of a Gaussian prime is also a Gaussian prime; this implies that Gaussian primes are symmetric about the real and imaginary axes.

The Gaussian integers form a principal ideal domain, i.e., they form also a unique factorization domain. This implies that a Gaussian integer is irreducible (that is, it is not the product of two non-units) if and only if it is prime (that is, it generates a prime ideal).

The norm of a Gaussian integer is a sum of two squares. A whole number with norm equal one is called an unit. The norm of a prime ideal is a prime number, (HuA).

The norm of a Gaussian integer is the basis of the Euler factorization method. The sum of two squares can be factorized into Gaussian integers. The Gaussian integers can be factorizied further, (ToH).

The four-square theorem of Lagrange states that every positive integer is the sum of four squares. Its proof is based on the theorem that any prime is the sum of four squares, (HaG) 20.5. For further theorems about integral and prime quaternions we refer to (HaG1) 20.6 ff.

A positive integer is a Gaussian prime if and only if it is a prime number p that is congruent to $3\ mod\ 4$ (that is, it may be written $4n + 3$, with n a nonnegative integer). The other prime numbers are not Gaussian primes, but each is the product of two conjugate Gaussian primes.

A Gaussian integer $a + ib$ is a Gaussian prime if and only if either its norm is a prime number, or it is the product of a unit $\{\pm 1, \pm i\}$ and a prime number of the form $4n + 3$.

It follows that there are three cases for the factorization of a prime number p in the Gaussian integers:

1. If the prime number p is congruent to $3\ mod\ 4$, then it is a Gaussian prime
2. If p is congruent to $1\ mod\ 4$, then p is a decomposed prime in the Gaussian integers (i.e., it is the product of a Gaussian prime by its conjugate, both of which are non-associated Gaussian primes (neither is the product of the other by a unit)
3. If $p = 2$, we have $2 = (1 + i)(1 - i) = i(1 - i)^2$; that is, 2 is the product of the square of a Gaussian prime by a unit; it is the unique ramified prime in the Gaussian integers.

In summary:

Every odd prime in the form $p = 4k + 1$ and $p = 2$ can be represented as the sum of two squares of two whole (positive or negative integer) numbers a and b. This is never the case for primes in the form $q = 4k + 3$, or more generally, the sum of two squares of two whole numbers a and b is only divisible by a prime number q, if a and b are divisible by q.

Gaussian numbers and the $\zeta(s)$ function

Let $r(n)$ denote the "number of representations" function as a sum of two squares

$$r(n) \coloneqq \#\{(a,b) \in R^2 | a^2 + b^2 = n\}.$$

The Hurwitz Zeta function is the Dirichlet series defined by, (IvA) 1.8,

$$L(s,\chi) \coloneqq \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1} \text{ for } Re(s) > 1$$

Then for the character function defined by, (ZaD) §2, (HaG) 17.9,

$$\chi(s) \coloneqq \begin{cases} 1 \, for \, n = \ 1 \, mod \, 4 \\ -1 \, for \, n = -1 \, mod \, 4 \\ 0 \, for \, n = \ \ 0 \, mod \, 2 \end{cases}$$

the corresponding Dirichlet series results into

$$\frac{1}{4} \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = \zeta(s) L(s).$$

For $L(s)$ the following representations are valid, (ZaD) S. 31,

$$L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{t^{s-1}}{e^t + e^{-t}} dt$$

with the following relationship to the Euler number

$$L(-n) = \frac{1}{2} E_n, \; L(2n+1) = \frac{(-1)^n E_{2n}}{2^{2n+2}(2n)!} \pi^{2n+1}, \; n = 0,1,2, \ldots .$$

Hurwitz quaternions

The set of Hurwitz quaternion integers provides an Euclidian ring domain (as the Gaussian integers), (HuA). The number of representations of an whole positive number n as a sum of of four quadrats is, depending if this number is odd or even, the 8-times resp. the 24-times of the sum of the odd divisors of the number n, (HuA). The unit elements of Q_{24} form the lattice of the regular, self-dual 24-cell, which does not have a regular analogue in any other dimension. We note that the 3-dimensional unit sphere S^3 contains the not abelian Q_{24} unit group of the Hurwitz quaternions.

From (HaG) 20.7, we recall:

> „If α is an integral quaternion, then one at least of its associates has integral coordinates; and if α is odd, then one at least of its associates has non-integral coordinates."

In (CoB) a "unique factorization of Hurwitz quaternions" is proposed, where any non-unit Hurwitz quaternion can be factored uniquely, up to a series of unit-migrations, meta-commutations, and re-combinations.

The quaternion rotation operator

The perhaps primary application of quaternions is the quaternion rotation operator. This is a special quaternion triple-product (unit quaternions and rotating imaginary vector) competing with the conventional (Euler) matrix rotation operator. The quaternion rotation operator can be interpreted as a frame or a point-set rotation, (KuJ). Its outstanding advantages compared to the Euler geometry are

- the axes of rotation and angles of rotation are independent from the underlying coordinate system and directly readable
- there is no need to to take care about the sequencing of the rotary axes.

In the context of the proposed UFT, (BrK), but also in the context to prove the Courant conjecture the quaternion rotation operator is proposed alternatively to the Euclidian rotation, (appendix).

The two-semicircle method to prove the Kummer conjecture

The Kummer conjecture deals with cubic characters in the form $p = 3k + 1$. This set can be decomposed into

- all odd squares of $3k + 1$
- all even squares of $3k + 1$
- all remaining odd numbers
- all remaining even numbers.

The link to the related $\{4n - 3{,}4n - 1{,}2n\}$ decomposition of the set of integers is given by the fact, that the „distance" between the consecutive odd squares of $n = 3k + 1$ is $\{4l - 1\}$, and that the „distance" between the consecutive even squares of of $n = 3k + 1$ is $\{2l\}$. This property provides the conceptual data for an appropriate framework set-up of the proposed two-semicircle method with the following key differentation tot he Hardy-Littlewood circle method, (BrK):

Hardy-Littlewood circle method	**Two-semicircle method**
winding number n	A pair of semicircle numbers $\left(\mathrm{n} - \frac{1}{2}, n\right)$
a single distribution function	two distinct distribution functions (**)
zeros of the orthonormal system $\{e^{2\pi i n z}\}$ of $L_2(S^1)$	complex-valued zeros $\{z_n\}_{n\in N}$ of the Kummer function ${}_1F_1\left(\frac{1}{2}, \frac{3}{2}; z\right)$ and absolute values of their imaginary parts $\lvert Im(z_n)\rvert = 2\pi\omega_n$ with $n - \frac{1}{2} < \omega_n < n$ and related retarded/condensed sequences ω_n^*, (*), (BrK)
$\{n\}$	$\{2n - 1{,}2n\} = \{4n - 3{,}4n - 1{,}2n\}$ (**)
Gaussian numbers, (HaG)	Hurwitz numbers, (HuA)
norm: sum of two squares, (Moc)	norm: sum of four squares, (MoC)
Euclidian rotations with fixed winding axis governed by the winding number n	quaternion rotation with dynamic winding axes governed by the odd and even squares of integers resp. their corresponding indices of the retarded/condensed sequence ω_n^* enjoying the Kadec condition

Reference

(BrK) Braun K., A toolbox to solve the RH and to build a non-harmonic Fourier series based two-semicircle method, www.riemann-hypothesis.de

(*) In the context of non-harmonic Fourier series governed by Kadec's theorem and Avdonin's (generalized) theorem of ¼-in the mean we note that the "retarded" sequences of $(2k - 1)$ resp. $((4k - 3), (4k - 1))$ resp. $((8k - 7), (8k - 5), (8k - 3), (8k - 1))$ are condensed by the factor ¼. *„It is interesting to note that Euclid's procedure to prove that the sequences of primes is infinite also works starting with* $n = 0$ *, i.e., without any knowledge about primes*", (HaH) S. 4.

(**) and related distribution functions built according to (PoG1). We note that the set of even integers is an ideal in the ring of Z. In case the Goldbach conjecture is valid this means that each even integer $2n = p + q$ is the norm of a quaternion if $p, q = 1 mod 4$.

Appendix

Hurwitz quaternions and symmetry groups

For each quaternion of S^3 there is a quaternion represention as a sum of two product terms in the form $e \cdot cos\left(\frac{\omega}{2}\right) + q \cdot sin\left(\frac{\omega}{2}\right)$, where e denotes the „real“ quaternion unit, q denotes a purely imaginary quaternion with norm equal one, and ω denotes an angle between zero and 2π, (EbH) 7.3. We also note that S^1 and S^3 are the only spheres with a "continuous" group structure, (EbH) 7.2. From the fundamental theorem of algebra for quaternions it follows that there are exactly n roots of any quaternion with not vanishing imaginary part, (EbH) 7.1.8.

The 1-dimensional S^1 unit sphere is isomorphic to $U(1)$; the 3-dimensional S^3 unit sphere is isomorphic to $SU(2)$.

The groups S^1 and S^3 have parameter representations, (EbH) 3.5.4(2'), 7.3.2(3). There are epimorphisms between S^3 and $SO(3)$, resp. between $S^3 \times S^3$ and $SO(4)$. The group $SO(4)$ contains isomorphic normal subgroups to the group S^3, i.e. it is a not „simple“ Lie group. The groups $SO(n)$, $n > 4$, are all „simple“, i.e. they have not trivial coherent normal subgroups. The groups $SO(2n+1)$ have no normal subgroup unequal (e). The groups $SO(4)$ have exactly the not trivial normal subgroup $\{e, -e\}$, (EbH) 7.3.4.

With respect to the proposed united field theory (UFT) we note that the 1-dimensional unit sphere in R^2 corresponds to the Lie group $U(1)$. The related number grid is built by the Eisenstein numbers. Regarding the characteristics of S^1 and S^3 in the context of Hurwitz quaternions and the proposed united field theory (UFT) we note a possible conceptual link to the Courant conjecture, (CoR) p. 763:

Families of spherical waves for arbitrary time-like lines exist only in the case of two or four variables, and then only if the differential equation is equivalent to the wave equation.

In the context of the Teichmueller theory with respect to the Riemann & Hyperbolic surfaces we mention that the compactification of the field of complex numbers C, the Riemann sphere, is homeomorphic to S^2. In the context of the proposed Hilbert space framework we note the relationship oft he Teichmüller space with the fractional Hilbert space $H_{1/2}$.

In (AdS), (FiD) quaternionic Hilbert spaces (in particular, Krein spaces) for various applications to quantum mechanics are provided.

In (AlD) quaternionic inner product spaces including ortho-complemented subspaces are studied. The main result is that a closed uniformly positive subspace in a quaternionic Krein space is ortho-complemented.
Employing quaternionic Newton’s law, in (ArI) it is shown that the energy conservation equation is the analog of Lorenz gauge in electromagnetism.

Regarding the crucial difference between the algebra based gauge theory and the analysis based GRT we quote from (BlC):

„*The correspondence between symmetries and conserved quantities is one of the most important principles of physics. The crucial difference between gauge theories and the GRT is that the symmetries of the GRT act on the space-time itself and not only on the degree of freedoms of the „internal“ fields.*

The vacuum Einstein equations state that the Ricci curvature Ric(g) of a lorentzian metric g is identically zero. Recast as hamiltonian evolution equations, they become a hamiltonian system on the cotangent bundle of the manifold MΣ of smooth riemannian metrics on a manifold Σ which represents the typical Cauchy hypersurface.

As in every lagrangian field theory with symmetries, the initial data must satisfy constraints. But, unlike those of gauge theories, the constraints of general relativity do not arise as momenta of any hamiltonian group action. In this paper, (BlC), we show that the bracket relations among the

constraints of general relativity are identical to the bracket relations in the Lie algebroid of a groupoid consisting of diffeomorphisms between space-like hypersurfaces in spacetimes. A direct connection is still missing between the constraints themselves, whose definition is closely related to the Einstein equations, and our groupoid, in which the Einstein equations play no role at all. We discuss some of the difficulties involved in making such a connection.

In contrast to classical mechanics and gauge field theories, the conserved quantities of the GRT do not span a symmetry algebra in the conventional sense. Instead, a so-called Hamiltonian Lie algebroid can be obtained from a naturally constructed symmetry groupoid."

Kummer's regular and irregular primes

Kummer introduced the concept of regular and irregular primes based on an underlying „ideal complex number" concept. There are infinitely many irregular primes congruent to $3\ mod\ 4$, ((JeK).

(Kummer) **Theorem 1.1.2** (CoJ):

> The prime p is irregular if and only if p divides the numerator of at least one of $\zeta(-1)$, $\zeta(-3)$, … $\zeta(4-p)$.

Let B_m denotes a Bernoulli number in the even-suffix notation. Then the Kummer theorem states that p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers B_2, B_4, … B_{p-3}, (KuE4).

As part of his proof Kummer showed the following congruences

Theorem 1.1.3 (CoJ):

> Let n and m be odd positive integers such that $n = m \neq -1 mod(p-1)$. Then the rational numbers $\zeta(-n)$ and $\zeta(-m)$ are p -integral, and $\zeta(-n) = \zeta(-m) mod\ p$.

For the rational Bernoulli numbers it holds $B_{2k+1} = 0$; for the Euler integer numbers it holds $E_{2k-1} = 0$.

Carlitz called an odd prime prime p to be irregular with respect to the Euler numbers if it divides one of the numbers E_2, E_4, … E_{p-3}, He proved that the number of such primes is infinite, (CaL).

For any irregular prime p the pair $(p, 2k)$ is called a irregular pair, if p is irregular and $2 \leq 2k \leq p-3$.

From the Hensel lemma it follows the

Lemma:

> Let p denote an odd prime number and $a \in Z_2$ where p is not a divisor of a. Then a is a square in Z_2 iff a is a quadratic rest $mod\ p$.
>
> If $a \in Z_2$ is odd, then a is a square in Z_2 iff $a = 1 mod 8$.