GOLDBACH FOR GAUSSIAN, HURWITZ, OCTAVIAN AND EISENSTEIN PRIMES

OLIVER KNILL

Abstract. We formulate Goldbach type questions for Gaussian, Hurwitz, Octavian and Eisenstein primes.

1. Introduction

The **Goldbach conjecture** [18] stating that every even integer > 2 can be written as a sum of two rational primes has a calculus reformulation in that the function $g(x) = f(x)^2$, with $f(x) = \sum_p x^p/p!$ summing over all primes has positive derivatives $g^{(2k)}$ for every $k > 1$. Analogue questions can be asked in the other division algebras $\mathbb{C}, \mathbb{H}, \mathbb{O}$ as well as in number fields within $\mathbb{C}$. There is a Goldbach version by Takayoshi Mitsui for rings of integers [35] and a Goldbach conjecture by C.A. Holben and James Jordan for Gaussian primes [22]. Guided by the calculus reformulations, we look at Gaussian, Eisenstein, Quaternion and Octonion versions and make them plausible by relating them to conjectures by Edmund Landau, Viktor Bunyakovsky and Godfrey Hardy and John Littlewood. Even before the 1742 letter from Christian Goldbach to Leonard Euler, [30, 28]. René Descartes voiced a similar conjecture earlier [9, 40, 45, 38]: every even number is the sum of 1,2 or 3 primes. Edward Waring conjectured in 1770 that every odd number is either a prime or the sum of three primes. Many have done experiments. Even the Georg Cantor (1845-1918) checked in 1894 Goldbach personally up to 1000 [9] p. 422. The ternary conjecture is now proven [21]. It required to search up to $n \leq 8.87510^{30}$. The binary has been verified to $4 \cdot 10^{18}$ [12]. Landmarks in theory were Hardy-Littlewood [20] with the circle method, with genesis paper with Srinivasa Ramanujan in 1918 [19, 46], the Lev Schnirelemans theorem [23] using density and Ivan Vinogradov's theorem [48] using trigonometric sums.

Date: Jun 19, 2016.

1991 *Mathematics Subject Classification.* 11P32, 11R52, 11A41.

Key words and phrases. Gaussian primes, Hurwitz primes, Octavian primes, Eisenstein primes. Goldbach problems .

2. Gaussian primes

A Gaussian integer $z = a + ib$ is a **Gaussian prime** if it has no integer factor w with integer norm $N(z) = a^2 + b^2 = |z|^2$ satisfying $1 < |w|^2 < |z|^2$. A Gaussian integer is prime if and only if $p = N(z) = a^2 + b^2$ is a rational prime or if $ab = 0$ and $\sqrt{p}$ is a rational prime of the form $4k - 1$. This structure, which relies on Fermat's two square theorem (see [54] for a topological proof), has been known since Carl Friedrich Gauss [15]: there are three type of primes: the case $\pm 1 \pm i$ for $p = 2$, then primes of the form $\pm p$ or $\pm ip$ for rational primes $p = 4k + 3$ or then groups $\pm a \pm ib, \pm b + i \pm a$ of eight primes for rational primes of the form $p = 4k + 1$.

Lets call $Q = \{a + ib \mid a > 0, b > 0\}$ the **open quadrant** in the complex integer plane. A Gaussian integer z is called **even** if $N(z)$ is even. Evenness is equivalent to $a + b$ being even or then of being divisible by the prime $1 + i$.

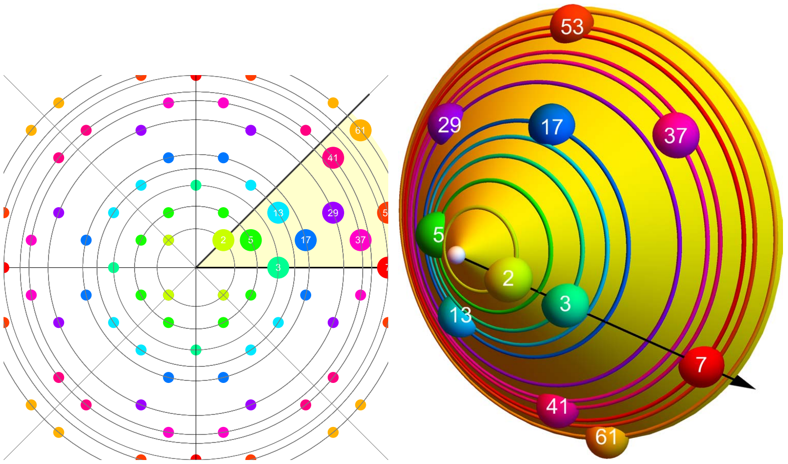


Figure 1. Gaussian primes cover the rational primes in a natural way. Only the order is scrambled although. There is a dihedral D_4 symmetry of the primes generated by conjugation and multiplication by units. On the cone $\mathbb{C}/D_4$, the angle distribution appears pretty random away from the identification line.

Conjecture: Every even Gaussian integer $a + ib$ with $a > 1, b > 1$ in Q is the sum of two Gaussian primes in Q.

This can again be reformulated using Taylor or Fourier series. In the Taylor case, the conjecture is equivalent with

$$f(x,y) = \sum_{p=a+ib \in Q} \frac{x^a}{a!} \frac{y^b}{b!}$$

having the property that $g = f^2$ has all even derivatives $g^{(k,l)}$ positive if $k+l$ is even and $k > 1, l > 1$. The Fourier case appear with $x = \exp(i\alpha), y = \exp(i\beta)$. Such algebraic reformulations make the statement natural. The conjecture looks toughest at the boundary of Q, where less possibilities for summation appear. The extremest case is $z = 2n + 2i$, where $z = (a+i) + (b+i)$ forces $2n = a+b$ with a^2+1, b^2+1 both being prime. We see:

Remark: Gaussian Goldbach implies the Landau conjecture on the infinitude of primes of the form n^2+1.

Since Landau appears currently out of reach, proving the Gaussian Goldbach will not be easy. There is still the possibility although of a counter example. It looks unlikely, given the amazing statistical regularity predicted by Hardy and Littlewood. But a surprise is always possible. Here is the ternary version which like in the real case does not require an evenness condition:

Conjecture: Every Gaussian integer $a+ib$ in Q satisfying $a > 2, b > 2$ is the sum of three Gaussian primes in Q.

Lets compare with what has been asked before:
Holben and Jordan [22] formulate as 'conjecture D" the statement that every even Gaussian integer is the sum of two Gaussian primes, and then "conjecture E": if n is a Gaussian integer with $N(n) > 2$, then it can be written as a sum $n = p+q$ of two primes for which the angles between n and p as well as n and q are both $\leq \pi/4$. Their conjecture F claims that for $N(n) > 10$, one can write n as a sum of two primes p, q for which the angles between n and p and n and q are both $\leq \pi/6$. Mitsui [35] formulates a conjecture for number fields which of course include Gaussian and Eisenstein cases. In the Gaussian case, it states that every even Gaussian integer is the sum of two Gaussian primes. This is conjecture D in [22]. Even when using the full set of primes, the evenness condition is necessary. The smallest Gaussian integer which is not the sum of two Gaussian primes is $4+13i$. The smallest real one is 29. The Holben-Jordan conjecture implies the Mitsui statement. In the Eisenstein case, we see that every Eisenstein integer is the sum of two Eisenstein primes without evenness condition. The question makes

sense also in the $\mathbb{Z}$: is every even integer the sum of two **signed primes**, where the set of **signed primes** is $\{\dots, -7, -5, -3, -2, 2, 3, 5, 7, \dots\}$. The smallest number which is not the sum of two signed primes is 23. By Goldbach, all even numbers should be the sum of two signed primes. The sequence of numbers [2]. which are not representable as the sum of two signed primes contains the number 29 as the later is also not a sum of two Gaussian primes. We will predict however that every rational integer to be the sum of two Eisenstein primes simply because every Eisenstein integer seems to be the sum of two Eisenstein primes.

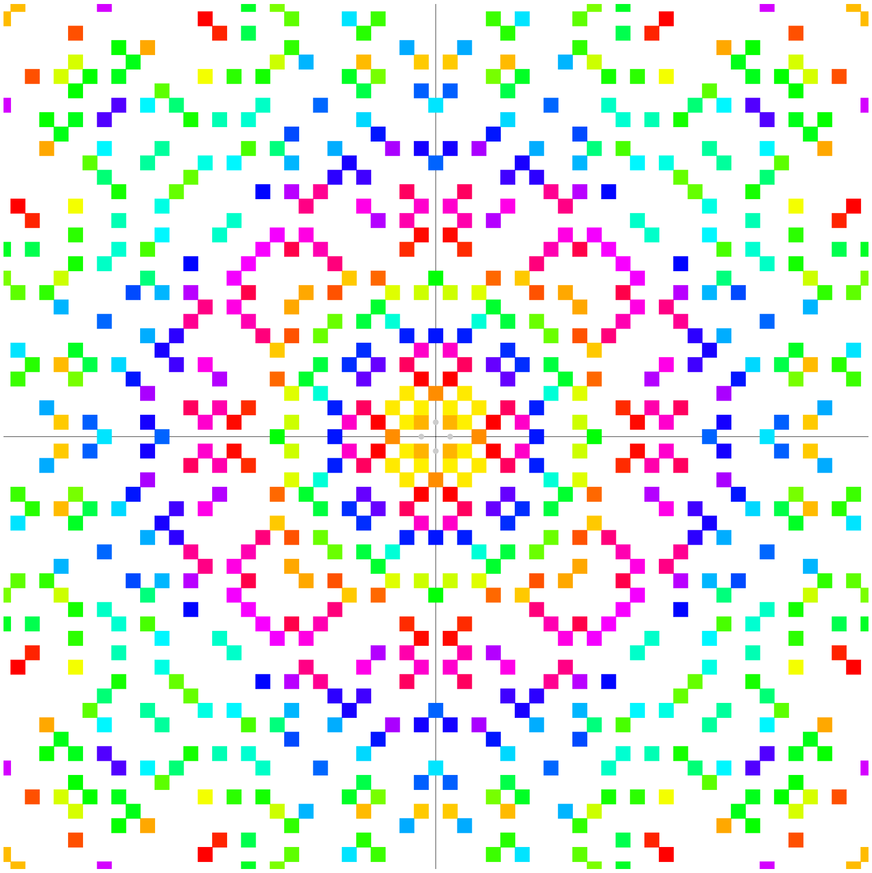


FIGURE 2. Gaussian primes.

3. A Hardy-Littlewood constant

The statistics of Gaussian primes on various rows has been of interest for almost 100 years, sometimes without addressing the Gaussian primes although. It is related to the fascinating story of a constant:

Hardy-Littlewood conjectured that the frequency ratio of primes on $\mathrm{im}(z) = 1$ and $\mathrm{im}(z) = 0$ is

$$C = C_1 = \prod_{p \in P_1} [1 - \frac{1}{p-1}] \prod_{p \in P_3} [1 + \frac{1}{p-1}] = 1.37279... ,$$

where P_k is the set of rational primes congruent to k modulo 4. More generally, in their conjecture H, they give explicit constants for all the other rations between rows $k+ia$ and $k+ib$ as C_a/C_b using the product $C_a = \prod_p (1 - (-a^2|p)/(p-1))$ over all odd primes p, where $(q|p)$ is the **Jacobi symbol**, assuming the empty product is $C_0 = 1$.

In 1962, [4] combine several conjectures of Hardy and Littlewood about density relations of sets. What is the ratio of the number of primes of the form $f(x)$ in $[0, \dots, n]$ and the number of primes the form $g(x)$ in $[0, \dots, n]$? We can write this in the limit $n \to \infty$ as C_f/C_g, where

$$C_f = \prod_p \frac{(1 - \omega_f(p)/p)}{(1 - 1/p)} .$$

This intuition works if f, g are irreducible polynomials of the same degree with positive leading coefficients and $\omega_f(p) \neq p$ for all p where $\omega_f(p)$ is the number of solutions $f(x) = 0$ modulo p. One can include $f(x) = x^n$, where $\omega_f(p) = 1$ and so set $C_f = 1$.

The constants C_k are then shorts cuts for C_{n^2+k}. But lets just focus on the constant C for $f(x) = x^2 + 1$ which is a nice prototype as in that case $\omega_f(p) = 1$ for $p \in P_3$ and $\omega_f(p) = 2$ for $p \in P_1$ by quadratic reciprocity so that $(1 - \omega_f(p)/p)/(1 - 1/p)) = 1 - \frac{1}{p-1}$ for $p \in P_1$ and $(1 + \frac{1}{p-1})$ for $p \in P_3$.

The intuition behind the constants C_f is of probabilistic nature. It is a bit hard to describe but once you see it, the “formulas open up” and become crystal clear. Lets try: we are interested in solutions $a^2 = -1$ modulo p because then, p is a factor of $a^2 + 1$ preventing the later of being prime. The key assumption is that the solution sets of equations like $a^2 = -1$ modulo p or then modulo q is pretty much independent events if p, q are different odd primes. This means that the chance being a solution to both becomes the product of the probabilities for each. To get the probability, start with the full set of integers on some large interval, then look at the probability changes, when primes are successively added to the list. Now, every time a new prime is added to the list, the size of the space changes by $(p-1)/p = (1 - 1/p)$ because we can only take numbers which are not multiples of p. The product of these size changes is $1/\zeta(1) = 0$ and reflects the infinitude of primes. But if we look at the **ratio** of solution sets for two polynomials f, g, we don't have to worry about this renormalization: it happens for both f and g in the same way. In particular, when looking at solutions of the form $x^2 + 1$, then whenever -1 is a quadratic residue, the probability decreases by $(1 - 1/(p-1))(1 - 1/p) = (p-2)/p$ but if -1 is not a quadratic residue, then the probability stays the same, as the prime has no chance of dividing $a^2 + 1$. Including again the volume change gives $(p-2)/p/(1-1/p) = 1 - 1/(p-1)$ in the residue case and $1/(1-1/p) = p/(p-1) = 1 + 1/(p-1)$ in the non-residue case. This explains the formula for C. The more general case is combined skillfully in [4]. Using this frame work, many of the formulas of [20] make sense, also density formulas for the estimated number of prime twins, where one takes $f(x) = x(x+2)$ as this is also a special case of the Paul Bateman and Roger Horn setup. This general statement generalizes many conjectures and is called the **Bateman-Horn** conjecture. For relations with Dirichlet series see [5] for generalizations to number fields see [17]. For computations of various constants related to patterns of Gaussian integers in particular, see [25].

Mathematicians were interested in these constants also for cryptological reasons. A major reason is because there is a **holy grail** for factoring large integers $n = pq$ known already to Pierre de Fermat: find solutions to quadratic equations like $x^2 = a$ modulo pq for small a. Since $x^2 - y^2$ is then zero modulo pq the greatest common divisor of $x - y$ and n is a factor. Essentially all advanced factorizaton methods like Morrison-Brillard or quadratic sieve are based on this [39]. Also in this setup, some heuristic randomness assumptions for pseudo random sequences are the key to estimate the time an algorithm needs to factor the integer. There were later computations by Daniel Shanks [41] and Marvin Wunderlich (1937-2013) [53] who was also a cryptologist. In 1973, Wunderlich checked the frequency ratio of primes up to 14'000'000 and compared it with the Hardy-Littlewood constant C. We profited from Moore's law on hardware advancement and computed up to 134143000000 up to which 2728969165 rational primes of the form $4k + 3$ exist and 3746378328 primes of the form $n^2 + 1$ which gives a fraction of 1.372818123... Fluctuations still happen.
By the way, the grandmasters of number theory, Godfrey Hardy and John Littlewood were not without assistance: we read on page 62 of [20] that "some of their conjectures have been tested numerically by Mrs. Streatfield, Dr. A.E. Western and Mr. O. Western". Much

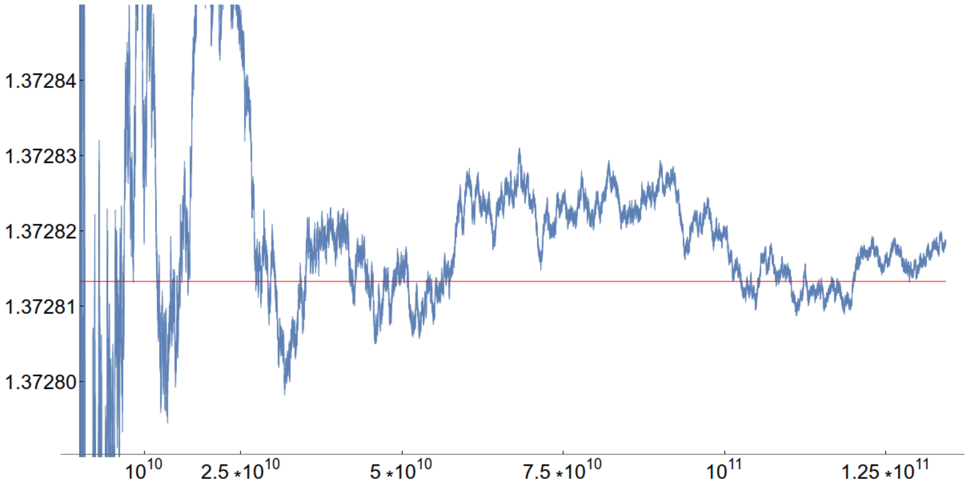


Figure 3. The convergence to the Hardy-Littlewood constant C giving the ratio of Gaussian prime density on $\mathrm{Im}(z) = 1$ and $\mathrm{Im}(z) = 0$. Shanks [41] gave $C = 1.37281346$. The constant C is almost prophetic as by an open Landau's problem (which currently appears theoretically beyond reach), one does not even know whether C is positive!

has been written about the influence of computers in mathematical research [52]. The story of the Hardy-Littlewood constant C illustrates that already early in the 20th century, when humans were still doing the computations by hand, the experimental part has been important. We were especially intrigued by the constant C because Streatfield, Western, Western already got a 5 digit agreement. This was later in the century confirmed by Shanks and Wunderlich. As we have much faster computers now, how accurate can we get now? Surprisingly, even for $n = 2^{36}$, the fluctuations remain of the order 10^{-5}. Surprised, we started to believe initially that the Hardy-Littlewood conjecture could be too strong and some small fluctuations could remain. There is no reason for alarm however. Theory predicts a slow convergence: if the Riemann hypothesis holds, an error of the order $(\log(x))^2/\sqrt{x}$ is expected. While this converges to zero, it happens very slowly in the range we do currently compute: for $x = 2^{36}$, this is still $2 \cdot 10^{-3}$ only. So, the constant is already in better agreement than expected. Just to get an idea about the computing culture: Daniel Shanks (1917-1996) [41] reports in 1959 that A.E. Western rewrote the constant using zeta and beta function values as

$$C = \frac{6}{4}\frac{\zeta(6)}{\beta(2)\zeta(3)} \prod_{p \in P_1} (1 + \frac{2}{p^3-1})(1 - \frac{2}{p(p-1)^2})$$

which gives 4 decimal places already when summing over three primes $p = 5, 13, 17$: the value is then $\frac{478543065\pi^6}{304368582656\beta(2)\zeta(3)} = 1.37283...$, where $\beta(2) = 0.915966$ is the Catalan number and $\zeta(3) = 1.20206$ is a zeta value. A bit earlier, in 1922, even before the Hardy-Littlewood article appeared, A.E. Western [50] computed the constant C using further sophisticated identities involving various zeta values so that one can use two primes $5, 13$ only to get C to 4 decimal places! Western was a giant in computation who also published mathematical tables like [51]. Anyway, this episode illustrates the culture in which the almost prophetic paper [20] was written in.

Its maybe important to remember that the mathematicians one hundred years ago had no access to computers; and this situation remained essentially until the mid century. Zuse Z3 was built 1941, Colossus and Mark I appeared only in 1944 but all of them were slow: Mark I for example needed 6 seconds to multiply two numbers [37]. Shanks in 1960 used an IBM 704 with a 32K high-speed memory. Today we have access to machines which give each user 500 GBybes of RAM and hundreds of CPUs. The program of Shanks needed on the Vaccuum tube computer 10 minutes to factor all n^2+1 from $n = 1$ to $n = 180000$. Today, a tiny laptop weighting 2 pounds with 8 GBytes of RAM reports it done in less than 4 seconds.

4. More questions

Much about the structure of Gaussian integers is still a mystery. One does not know for example whether there are some rows without primes. This is the **frogger problem**: the complex plane is the freeway, the rows are the car lanes, the non-primes are the cars. Can the frog hop to infinity on primes, which are the car gaps? The **Gaussian moat problem** has attracted a lot of attention: does a bounded step size suffices to hop to infinity on primes? [27, 16, 11, 49, 32, 44]. The **twin prime conjecture** for Gaussian primes asks for the existence of infinitely many **Gaussian primes twins**, pairs of primes for which the Euclidean distance is $\sqrt{2}$ [22]. While one does not know whether infinitely many Gaussian prime twins exist, one can estimate that there are asymptotically $Cr/\log^2(r)$ of them in a ball of radius r [25] which is a Hardy-Littlewood type estimate and now part of the Bateman-Horn conjecture. Virtually any question known for rational integers can be ported to Gaussian primes. This includes Diophantine problems or Waring type problems. Here is an other question: what is the regularity of the sequence defined by the unique angle $\theta(p_k) \in (0, \pi/4)$ if p_k is the k'th Gaussian prime in that sector? The sequence behaves very much like a random number generator. Is the topological entropy positive for the shift on the compact hull generated by the sequence?

While the numerical evidence for Hardy-Littlewood is strong, one has to get reminded that even the existence of infinitely many primes on the Gaussian line $\{\mathrm{Im}(z) = 1\}$ is open. It is one of the four problems presented by **Edmund Landau** at the 1912 International congress of mathematicians. The statement beats even Goldbach in simplicity: are there infinitely many primes p for which $p-1$ is a square? Hardy and Littlewood have also formulas for the density of Gaussian primes of the form $\{a + ib_0\}$ for fixed b_0. We looked experimentally at correlations between primes in different rows or at matrices and constructed graphs defined by Gaussian primes: take as the vertex set the positive integers and connect a, b if $a+ib$ is a Gaussian prime. We also applied the game of life to Gaussian prime configurations and believe that **Gaussian life** exists arbitrary far away from the origin. It could be "prime twins" blinking from far, far away. An other question is if we look at Gaussian or Eisenstein primes on the orbifold $\mathbb{C}/D_4$ or $\mathbb{C}/D_6$ factoring out the symmetry and let the ones with integer norm (not the ones with integer radius) move with uniform speed on those cones (like planets circling the sun). Is there any positive time for which 4 primes $a + ib$ with prime $ar + b^2$ are on the same line? It is likely that such **exceptional prime alignments** do not exist for Gaussian primes and similarly for Eisenstein primes away from the symmetry axes. Also, when factoring out the symmetry group given by the units and conjugation in the Hurwitz or Octonion case, one gets prime constellations on compact manifolds. In the Hurwitz case, there is a compact 3 manifold which is diffeomorphic to $M(p) = (\mathbb{H} \cap S_p)/G$, where S_p is the sphere in $\mathbb{R}^4$ of radius p and G is the group generated by the action of multiplying with a units and conjugation. $M(p)$ plays the role of the circles through the primes centered at the origin on the cone in the Gaussian case. Hurwitz showed that there are exactly $p+1$ primes on $M(p)$. We expect the distribution of this **prime cloud** on on M to converge weakly to an absolutely continuous volume measure on M, when the rational prime p goes to infinity.

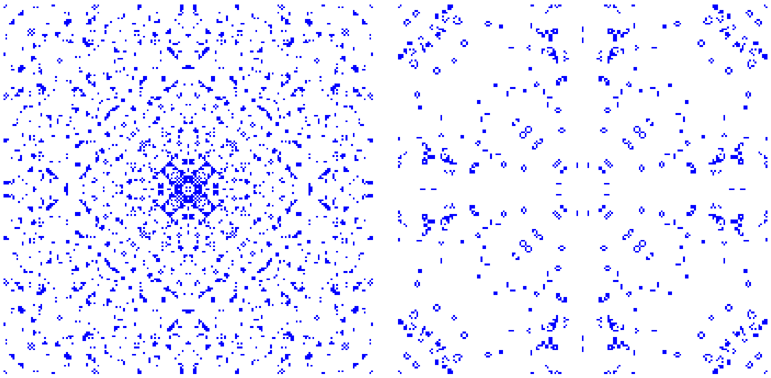


Figure 4. Gaussian primes are a configuration in A^{Z^2}, where $A = \{0,1\}$ is the two letter alphabet. We can therefore apply cellular automata on it. The left picture shows it after applying the Conway game of life rule once, the second after three times. In light of the prime twin conjecture for Gaussian primes, there should be life arbitrary far away from the origin. "Life" in a region is a configuration which "moves" when applying the time map.

But there are not only open problems about Gaussian primes. Quite many results are known. There is an analogue of Dirichlet's theorem on arithmetic progressions: for an arbitrary finite set in $\mathbb{Z}[i]$, there exist infinitely many $a \in \mathbb{Z}[i]$ and $r \in \mathbb{R}^+$ such that $a + r\sum_{f \in F} v_f$ is a Gaussian prime [43]. An other example is that the density of the **prime quotients** p/q in R^+ generalizes to the statement that the Gaussian prime quotients p/q are dense in the complex plane [14]. Patterns are explored in [11, 49, 26, 25]. The Goldbach conjecture is not the only statement which involves the additive structure and primes (which inherently rely on the multiplicative structure of the ring): any additive function $f(zw) = f(z) + f(w)$ which satisfies $f(p+1) = 0$ for all Gaussian primes is 0 [34]. Gaussian primes and friends are an Eldorado for new questions. We got dragged into this area while doing an exercise in section 5 of [33]. The addictive topic of primes totally ruined our original summer plans, just like it did for the boy in the Doxiadis novel [10].

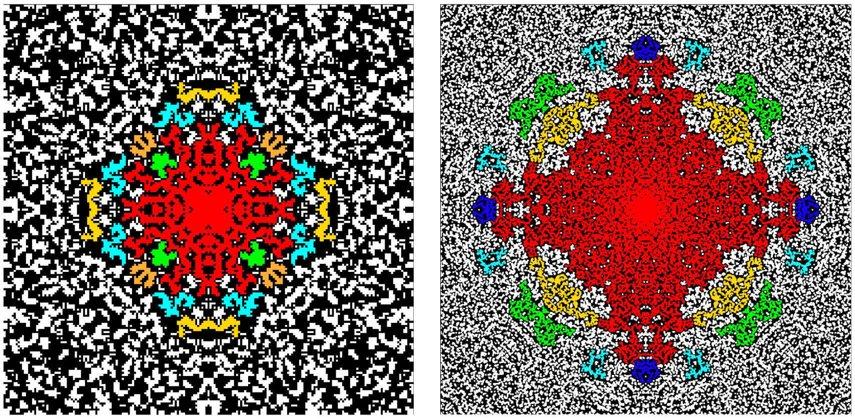


FIGURE 5. To illustrate the moat problem we applied a cellular automaton map and looked at the central connected component. The first picture is a screen shot after applying the map once, the second after applying the map two times. In principle, one can compute moats like that. But it is not very efficient.

5. Eisenstein primes

Given the cube root $w = (1+\sqrt{-3})/2$ of -1, an **Eisenstein integer** is a complex number $a+bw$ for which a, b are rational integers. The norm $p = N(z)$ of $z = a+bw$ is a^2+b^2+ab. One usually writes the Eisenstein integers with the cube root of 1. For Goldbach statements however, it is more convenient to work with w which is in the first quadrant. This ring of integers has been investigated first by Gotthold Eisenstein (1823-1852) [13]. The basic structure of **Eisenstein primes** is well known [42]. Either p is prime and congruent $0, 1$ modulo 3 or then $\sqrt{p}$ is prime and congruent to 2 modulo 3. The later class are the primes on the six symmetry axes.

Define Q as the set of Eisenstein integers $a + bw$ with $a > 0, b > 0$. These are the integers in the fundamental region, the first sextant of the complex plane. After doing some experiments, we experienced two surprises: first of all, the Eisenstein primes appear so dense that no **evenness** condition is necessary for writing an integer as a sum of two primes. The second surprise was that the extreme boundary case appears less constraining than the nearest next boundary case. There are two isolated "ghosts" Eisenstein primes.

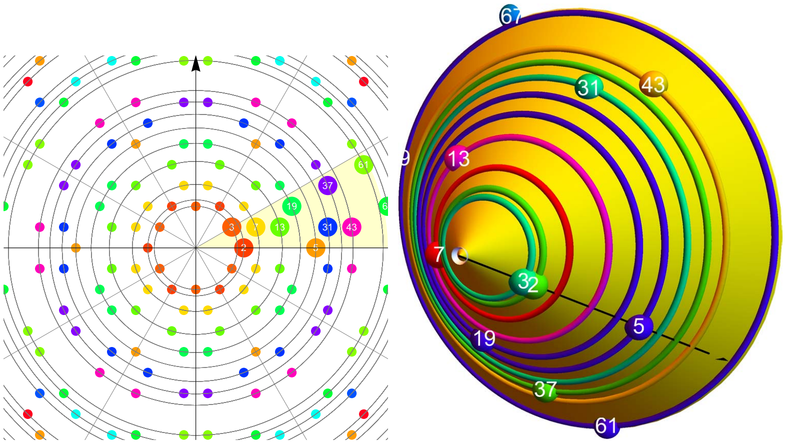


FIGURE 6. Eisenstein primes also cover the rational primes. The order is different as in the Gaussian case. The dihedral D_6 symmetry of the primes hides that on the fundamental domain $\mathbb{C}/D_6$, the angle distribution is pretty random, apart from the prime 3 and the $3k+2$ primes confined to the real axes.

Conjecture: Every Eisenstein integer $a+bw$ with $a>3, b>3$ is the sum of two Eisenstein primes in Q.

This would especially imply that infinitely many primes exist which are of one of the three forms $n^2+n+1, n^2+2n+4, n^2+3n+9$. Since in the second case, n has to be odd so that $a=n+m$ is even, we need for odd a a decomposition in the form $(n+w)+(m+3w)$ which means:

Remark: Eisenstein Goldbach implies the Bunyakowsky conjecture on the infinitude of primes of the form n^2+n+1.

We originally got the impression that the condition $a>1, b>1$ works and not only $a>3, b>3$, as stated. Here is a tale of caution: as we looked at the toughest case $z=2+nw$, where the problem is to write an integer n as a sum $n=a+b$ where a^2+a+1, b^2+b+1 are both prime, then this problem appears always to have a solutions up to $n=10^7$ and with better and better margins. Since everything looked good at the boundary $b=2$, why look further? But in the row just adjacent to the boundary, there appeared two exceptional cases, $3+109w$ and $3+121w$ which we call the **Eisenstein ghost twins** as they appeared out of nothing as the bad guys in the "matrix" of computations. These Eisenstein integers can not be written as a sum of two primes in Q. They appear topologically isolated, surrounded by "good rows" of the

Gaussian integer matrix. So, they appear completely unique of this kind:

Conjecture: Except for the two Eisenstein ghosts $109w + 3, 121 + 3w$, every Eisenstein integer $a + bw$ with $a > 1, b > 1$ is the sum of two Eisenstein primes in Q.

Lets look at the boundary case $z = 2 + nw$, where we look for two primes $p = 1 + aw$. Since $x^2 + x + 1$ is a cyclotomic polynomial, the Bunyakowski conjecture asking that there are infinitely many primes of the form $x^2 + x + 1$ kicks in. Lets just formulate the boundary case too. It is a special case of enhanced Eisenstein Goldbach statement and it isolates the Eisenstein ghost twins.

Conjecture: Every integer $n > 1$ can be written as a sum $n = a + b$ where $a^2 + a + 1, b^2 + b + 1$ are both prime.

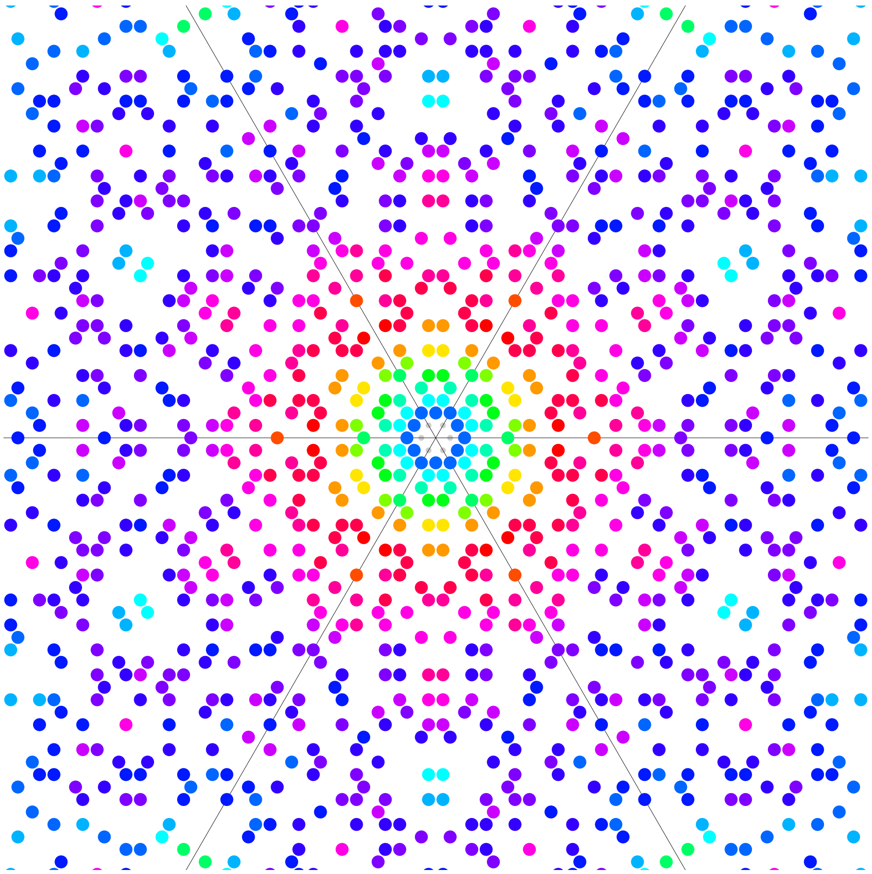


Figure 7. The Eisenstein primes.

Lets state the Mitsui type statement also, as it is so elegant.

Conjecture: Every Eisenstein integer can be written as a sum of two Eisenstein primes.

A possible calculus formulation is that the smooth two-periodic function $f(s,t) = \sum_{p=a+wb} e^{iat}/a! e^{ibs}/b!$ has the property that all Fourier coefficients of $g(x,y) = f(x,y)^2$ are positive, if the sum is over all Eisenstein primes.

6. Quaternion primes

Discovered by William Hamilton (1805-1865), the quaternions $z = a + ib + jc + kd = (a,b,c,d)$ have the norm $N(z) = a^2 + b^2 + c^2 + d^2$. Their arithmetic is determined by $i^2 = j^2 = k^2 = ijk = -1$, identities infamously found on October 16, 1843. The set of lattice points with integer values a, b, c, d do not form a maximal order. As Adolf Hurwitz (1859-1919) noticed, one needs to include “half integers”. Today, integers of the form (a,b,c,d) with integer a,b,c,d are called **Lipschitz integers**, and the additional integers of the form $(a+1/2, b+1/2, c+1/2, d+1/2)$ with integer a,b,c,d are called the **Hurwitz integers**. The union of Lipschitz and Hurwitz integers are then the **Quaternion integers** [24].

The quaternion integers form a lattice in R^4 which is known to be the densest lattice sphere packing in $\mathbb{R}^4$, the D_4 lattice [31] proven by Alex Korkin and Yegor Zolotarev (who is also known for the Zolotarev lemma in quadratic reciprocity). The group of units is the binary tetrahedron group which forms a regular 4-polytop, the **24 cell**, when drawn on the 3-sphere. This is the unit sphere in the discrete D_4 lattice. Despite the lack of commutativity and prime factorization which depends on the order in which the primes are arranged, the norm property of division algebra still allows to define **quaternion primes** as quaternion integers p which can not be divided by any other quaternion integer q different from a unit and having smaller norm $N(q) < N(p)$. As noticed also again by Hurwitz, their structure is easier: they are just the integers for which $N(q)$ is a rational prime. As the integers, also the Quaternion primes come now in two classes, the **Lipschitz primes** and the **Hurwitz primes** depending on whether they are Lipschitz integers or Hurwitz integers.

Define the region $Q = \{(a,b,c,d) \mid a > 0, b > 0, c > 0, d > 0\}$.

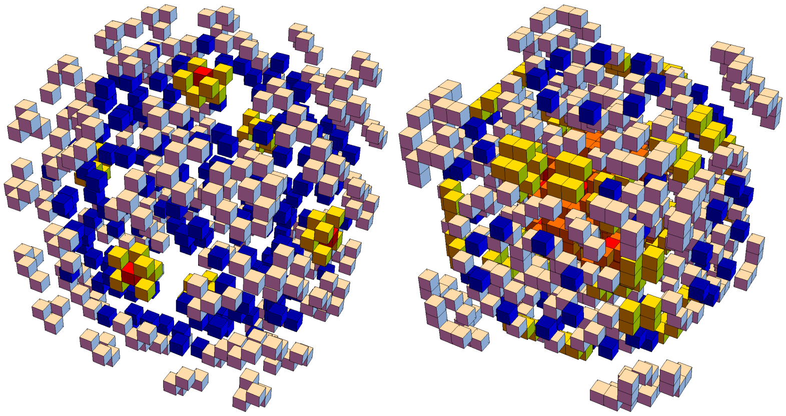


FIGURE 8. A slice through all the Lipschitz primes (a, x, y, z) for $a = 701$. They are given by the integer vectors (a, x, y, z) for which $a^2 + x^2 + y^2 + z^2$ is a rational prime. To the right, we see the Hurwitz primes $(1 + 2a, 1 + 2x, 1 + 2y, 1 + 2z)/2$ for $a = 3001$. They are given by the integer vectors $(a, x, y, z) + (1, 1, 1, 1)/2$ for which the sum of the squares is a rational prime.

Conjecture: Every Lipschitz integer quaternion with entries > 1 is the sum of two Hurwitz primes in Q.

Again, this could be rewritten analytically as the property that

$$f(x, y, z, w) = \sum_{p=a+ib+jc+kd \in Q} x^{2a} y^{2b} z^{2c} w^{2d} ,$$

summing over all Hurwitz primes in Q has the property that $g = f^2$ has nonzero derivatives $g^{(k,l,m,n)}$ for $k, l, m, n > 1$.

Already for $z = (2, 2, 2, 2)$, there are 14 possibilities: either $(3, 1, 1, 1)/2 + (1, 3, 3, 3)/2$ (8 cases) or $(1, 1, 3, 3)/2 + (3, 3, 1, 1)/2$ (6 cases). In the special case, when the Lipschitz integer is $z = (2, 2, 2, n)$, the two primes must have up to permutation the form $p = (1, 1, 1, x)/2, q = (3, 3, 3, n - x)/2$, or then $p = (1, 1, 3, x)/2, q = (3, 3, 1, 2n - x)/2$ for an unknown odd integer x. In the first case, we need simultaneously to have $(3 + x^2)/4$ and $(27 + (2n - x)^2)/4$ to be rational primes. In the second case, we need simultaneously to have $(11 + x^2)/4$ and $(19 + (2n - x)^2)/4$ to be prime. Since x needs to be odd for p to be a Hurwitz prime, we can write $x = 2k + 1$. Now $(3 + x^2)/4 = 1 + k + k^2$ and $(27 + (2n - x)^2)/4 = 7 - (n - k) + (n - k)^2$. In the second case

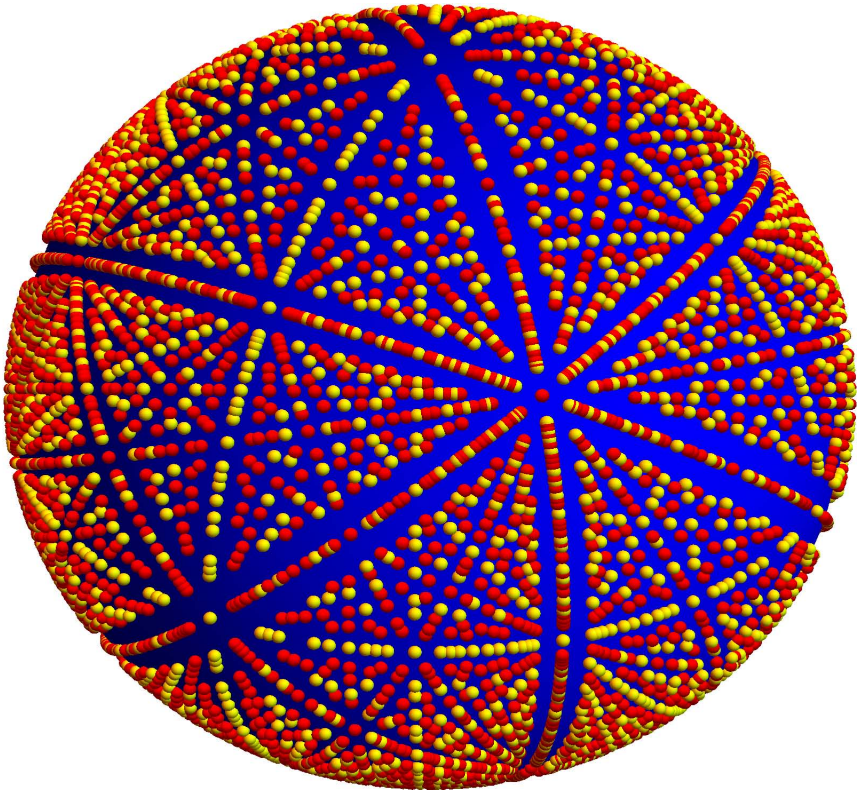


Figure 9. The **Hurwitz prime sphere** shows the quaternion primes inside the cube $\{|a|,|b|,|c|,|d| \leq 8\}$ projected onto the first three coordinates and then projected onto the unit sphere. Since Hurwitz primes can not be on coordinate planes, some grand circles of Lipschitz primes appear. Apart from the symmetry imposed by units and conjugation, both Hurwitz and Lipschitz prime sets appear to be uniformly distributed on the sphere.

$3+k+k^2$ and $5-(n-k)+(2n-k)^2$. We see: If the Hurwitz Goldbach conjecture holds, then for any n, there exists $k < n$ for which both $3+k+k^2$ and $7+k+k^2-n-2kn+n^2$ are prime or for which both $1+k+k^2$ and $5+k+k^2-n-2kn+n^2$ are prime. Now, if Goldbach is true and if there existed only finitely many primes of the form $3+k+k^2$ and $1+k+k^2$, then for all $m=n-k$ large enough, $7-m+m^2$ and $5-m+m^2$ would always have to be prime. This is obviously not true if m is a multiple of 7 or 5. We see that quaternion Goldbach again implies a special case of the Bunyakovsky conjecture, which like Landau's problem is likely not so easy to prove:

Remark: If the quaternion Goldbach conjecture is true, then one of the sequences $1 + k + k^2$ or $3 + k + k^2$ contains infinitely many primes.

Let us quickly verify the **Bunyakovsky conditions** which enter the **Bunyakovsky conjecture**. First, $\phi_3(k) = 1 + k + k^2$ is already the cyclotomic polynomial and also k^2+k+3 satisfies the conditions of the Bunyakovsky conjecture: the maximal coefficient of the polynomial f is positive, the coefficients have no common divisor and there is a pair of integers n, m such that $f(n), f(m)$ have no common divisor. The set of k for which $k^2 + k + 1$ is prime is the sequence $A002384$ in [1].

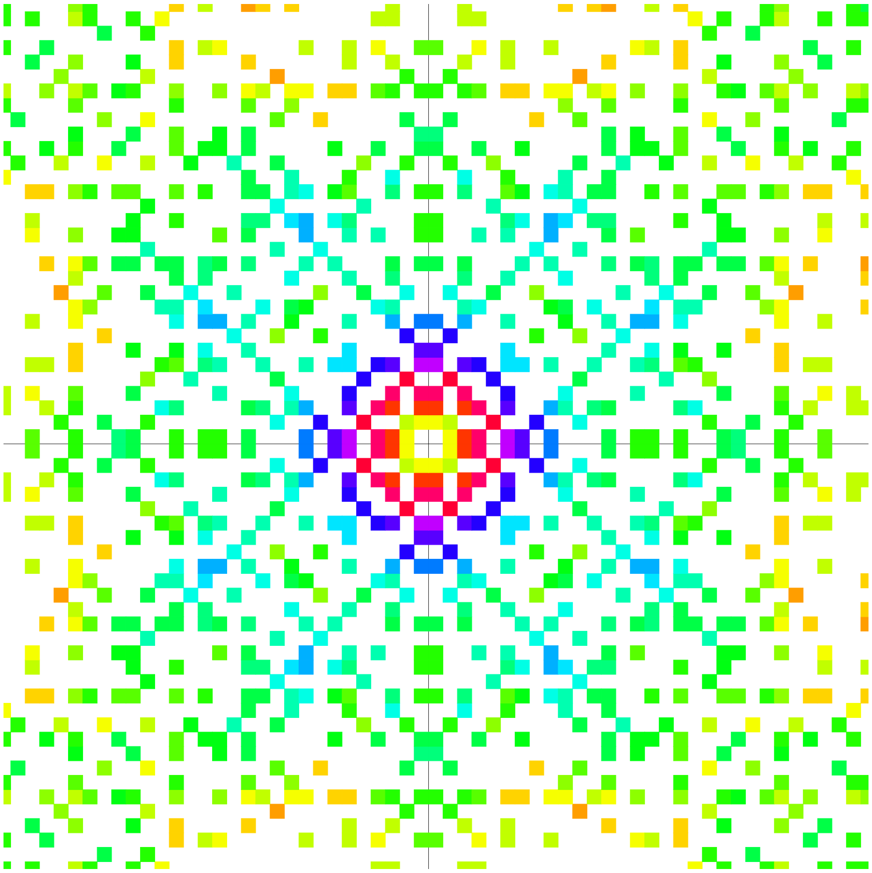


FIGURE 10. Hurwitz primes of the form $(1/2, 1/2, a + 1/2, b + 1/2)$.

We also see experimentally

Conjecture: Every Hurwitz integer quaternion with entries > 2 is the sum of a Hurwitz and Lipschitz primes in Q.

The Hurwitz integer $(3/2, 3/2, 3/2, 3/2)$ is not the sum of a Hurwitz and Lipschitz prime because the only decomposition would be $(1, 1, 1, 1) + (1, 1, 1, 1)/2$ but both are not prime. Together:

Conjecture: Every integer quaternion with entries > 2 is the sum of two quaternion primes in Q.

7. Octavian primes

Besides $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$, there is a fourth normed division algebra $\mathbb{O}$, the space of **Octonions**. Also called the space of **Cayley numbers** or **Hypercomplex numbers**, they were discovered by John Graves and not only lack commutativity but have no associativity. The members of $\mathbb{O}$ can either be written as a linear combination of a basis $1, i, j, k, l, m, n, o$ or then, according to a suggestion of Arthur Cayley and Leonard Dickson, as pairs (z, w) of quaternions, defining $(z, w)\cdot(u, v) = (zu - v^*w, vz + wu^*)$. The algebra is no more associative.

In order to do number theory, one has to specify what the **integers** are in $\mathbb{O}$. There are now three classes of integers, the **Gravesian integers** (a, b, c, d, e, f, g), the **Kleinian integers** $(a, b, c, d, e, f, g) + (1, 1, 1, 1, 1, 1, 1, 1)/2$ as well as the **Kirmse integers** which includes elements for which 4 of the entries are half integers. There are 7 maximal orders which Johannes Kirmse classified in 1925 [29, 7]. They are all equivalent and produce the class of **Octonion integers** or **Cayley integers** or then more catchy, the **Octavian integers**. See [6, 3]. The condition $N(zw) = N(z)N(w)$ which assures that the algebra a **division algebra**, is also called the **Degen eight square identity** named after Carl Ferdinand Degen. The identity allows to define Octavian primes as the set of Octavian integers for which the sum of the squares is a rational square.
Primes can now be called **Gravesian**, **Kleinian** or **Kirmse** primes. All three distinct classes together form the **Octavian primes**. Their **units**, the unit norm integral Octonions, are remarkable. They they do not form a multiplicative **group**, as multiplication is not associative, they form a finite **loop** of 240 elements. A loop is an algebraic structure which is more primitive and so general than a group in which one does not insist on associativity. The units form what is one calls a **Moufang loop** [36] named after German mathematician **Ruth Moufang** (1905-1977) who was a student of Max Dehn (1878-1952), who is known for the Dehn-Sommerville relations or Dehn twists. There is a smaller loop of 16 unit octonions containing the Gravesian integers like

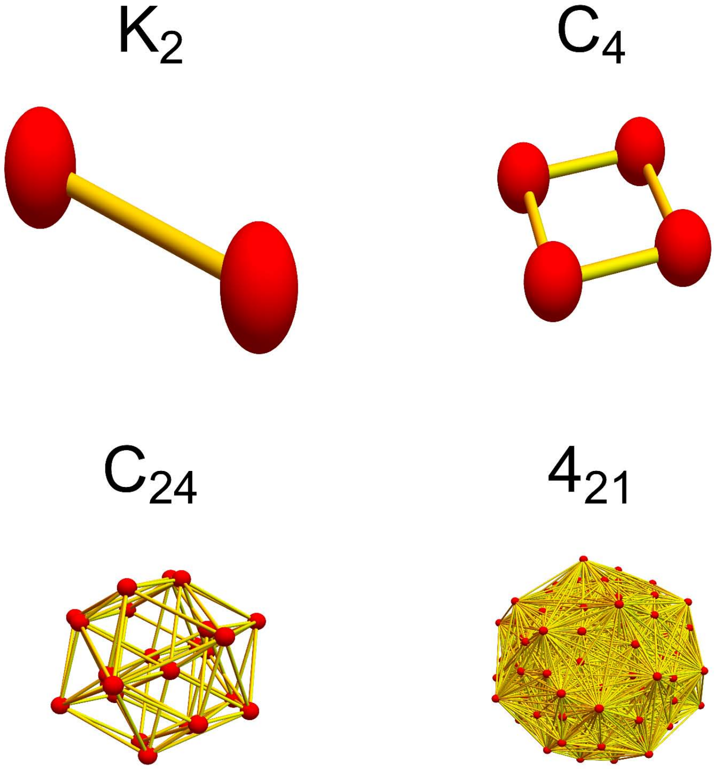


Figure 11. The units in the four normed division algebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$: We see the K_2 for $\{\pm 1\} \subset \mathbb{R}$, $C_4 = \{1, i, -1, -i\} \subset \mathbb{C}$, the 24 cell in $\mathbb{H}$ and the Gosset polytop in $\mathbb{Q}$ generating the E_8 lattice. The all are known to generate the densest sphere packings, except for $\mathbb{C}$, where one has to look at the Eisenstein integers instead.

$(\pm 1, 0, 0, 0, 0, 0, 0, 0, 0)$. The units placed in the unit sphere of R^8 form the **Gosset polytope** 4_{21} which was discovered by Thorold Gosset (1869-1962), who as a lawyer without much clients amused himself as an amateur mathematician and also helped proofreading [8] which has a note on Gosset on page 164. The vertices of 4_{21} are the roots of the exceptional Lie algebra E_8 belonging to the 248 dimensional Lie group E_8. As the dimension of the maximal torus is 8, the root system lives in R^8. One can write points on the sphere of radius 2 taking vertices $(a, b, 0, 0, 0, 0, 0, 0)$ with $a, b \in \{-1, 1\}$ or (a, b, c, d, e, f, g, h) with with entries in $\{-1/2, 1/2\}$ summing up to an even number. This lattice E_8

has just recently been verified by Maryna Viazovska to be the densest sphere packing in R^8 [47].

In the Octavian case, it appears that it is not obvious how to come up with a conjecture which both convinces and is justifiably difficult. Brute force searches are difficult as the volume of a box of size r grows like r^8. Here is a first attempt of get to a conjecture. We formulate as a question since our experiments did not get far yet, nor do we have an idea how difficult the statement could be. Anyway, lets denote by Q again the set of all integer octonions, for which all coordinates are positive.

Question: Is there a constant K such that every Octavian integer Z with coordinates $\geq K$ is a sum of two Octavian primes P, Q in Q ?

While $(1,1,1,1,1,1,1,1)$ as a sum of $p+p$ with Kleinian prime $p = (1,1,1,1,1,1,1,1)/2$ of norm 2, already the Kleinian $(1,1,1,1,1,1,1,2)$ can not be written as a sum of two primes and the Kirmse integer $(2,2,3,3,3/2,3/2,3/2,3/2)$ can not be written as as sum of two primes the constant has to be at least 2. Lets look at some small examples using the notation $\overline{a}$ for a block of 4 numbers a. The Kleinian $(\overline{3},\overline{3})/2$ is the sum of the two Kirmse primes $(\overline{1/2},\overline{1}) + (\overline{1},\overline{1/2})$ of norm 5. The Kirmse integer $(\overline{1},\overline{3/2})$ is the sum $(\overline{1/2},\overline{1/2}) + (\overline{1/2},\overline{1})$ of a Kleinian prime of norm 2 and a Krimse prime of norm 5. The integer $(\overline{2},\overline{2})$ can be written as a sum $(\overline{1/2},\overline{1})$+$(\overline{3/2},\overline{1})$ of two Kirmse primes with norm 5 and 13. And $(\overline{2},\overline{3/2})$ can be written as a sum $(\overline{1/2},\overline{1/2})$+ $(\overline{3/2},\overline{1})$ of a Kleinian and Krimse prime of norm 2 and 13. The Kleinian integer $n = (\overline{3},\overline{3})$ already can be written in 64 ways as a sum of two positive Gravesian primes, like $n = p+q$ with $p = (\overline{2},2,2,2,1)$ and $q = (\overline{1},2,2,2,1)$ and then for example 6 more ways as a sum of Kirmse primes like $p = (1,1,2,2,\overline{3/2})$ and $q = (2,2,1,1,\overline{3/2})$. For $(\overline{3},3,3,3,4)$ we have a decomposition like $(1,2,2,1,3/2,3/2,3/2,5/2)$,$(2,1,1,2,\overline{3/2})$.

To simplify, one can take the Cayley-Dickson point of view and see an Octonion as a pair (z,w) of quaternions and $(z,w)\cdot(u,v) = (zu - v^*w, vz + wu^*)$, where $z^* = (a,-b,-c,-d)$ is the conjugate quaternion of $z = (a,b,c,d)$. A subclass of Octonion prime are now pairs (z,w) of quaternion integers for which $N(z)+N(w)$ is prime. These could already be enough to work with and get the sum. We then don't even have to touch the multiplication of Octonions as the prime property is visible from the norm. One certainly has to distinguish cases. In the simplest case, within Gravesian integers if (z, w), we want to find a Gravesian prime $(x, y) = (x, y)$ such that both $p = \sum_i x_i^2 + y_i^2$ and $q = \sum_i (z_i - x_i)^2 + (w_i - y_i)^2$ are prime. One can also just look at two dimensional slices in the 8-dimensional space and notice that the primes are quite "dense". For Figure (12) for example, we show at all pairs (a, b) for which $a^2 + b^2 + a + b + 5$ is prime. Note that they appear dense but proving even that some exist in each row is a Landau-Bunyakovsky type problem.

Maybe there is a trick to write down the primes p, q directly using the Lagrange 4 square theorem so that they add up to n. Maybe also that in the higher dimensional situation the original **Schnirelman density** approach works. This density α is a quantity of a set A such that for $X = [-M, M]^8$ satisfies $|A \cap X(M)| \geq \alpha |X(M)| = \alpha(2M + 1)^8$ for every $M > 1$. Schnirelman showed in the one dimensional case that the density of the set sum $P + P$ of primes P is positive. In the higher dimensional case, a similar argument could be used. In any way, the intuitive argument given by Hardy and Littlewood for primes makes things plausible: in all cases, the probability to find a prime in the box $Q(n)$ is $1/\log(n)$. To hit two primes has probability $1/\log(n)^2$, but we have $|Q(n)|$ chances. The chance to miss in higher dimensions shrinks even faster with n in higher dimensions.

But we don't even have scratched the surface with experimental investigations in the case of Octavian integers.

Acknowledgements: Some computations were run on the Odyssey cluster supported by the FAS Division of Science, Research Computing Group at Harvard University.

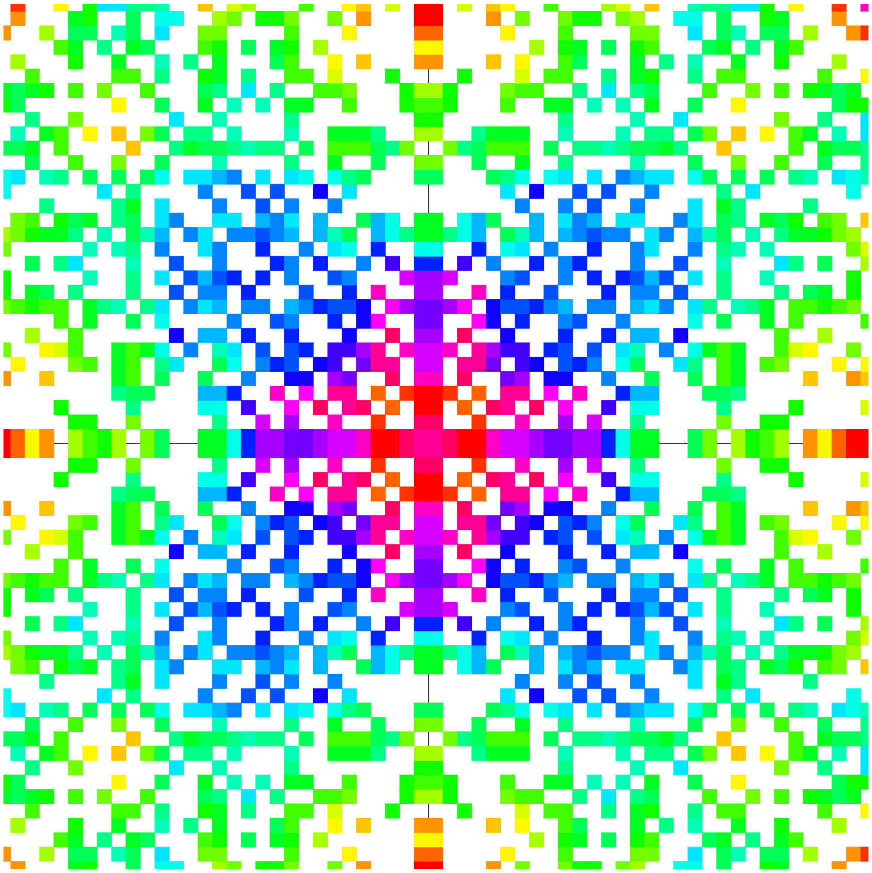


FIGURE 12. Kirmse primes $(1, 1, 1, 1, 3/2, 3/2, a + 1/2, b + 1/2)$. They are given by all pairs (a, b) for which $17 + a^2 + b^2 + a + b$ is a rational prime.

APPENDIX: GOLDBACH COMETS AND GHOSTS IN THE MATRIX

For Gaussian Goldbach, things look comfortable. It looks even possible that one can chose for every row a small set of rows.
We next now pictures illustrating **Eisenstein ghost twins** with "ghost" added, not to confuse with Eisenstein prime twins, which are neighboring Eisenstein primes.

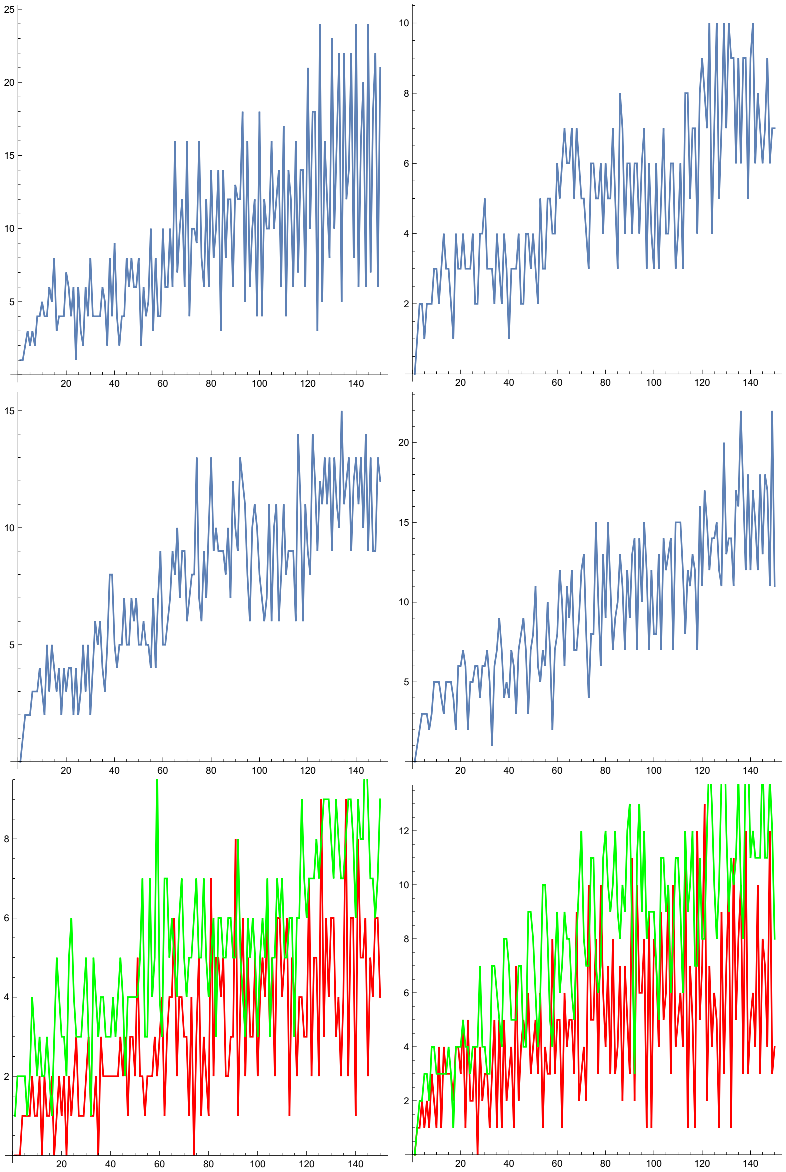


FIGURE 13. The number of times, a Gaussian integer $a + ib$ can be written as a sum of Gaussian primes. We see cases $b = 2, b = 3, b = 4, b = 5, b = 6, b = 7$. In the last two cases, one can not force a prime from the first row.

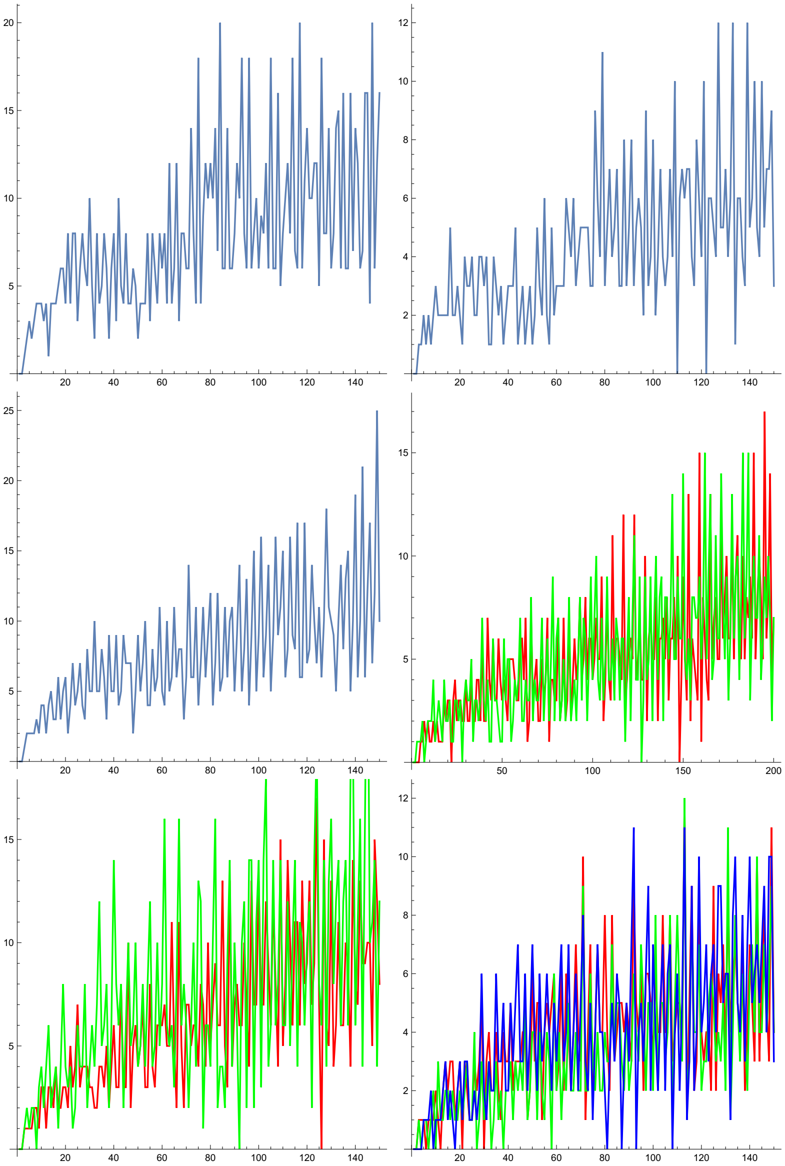
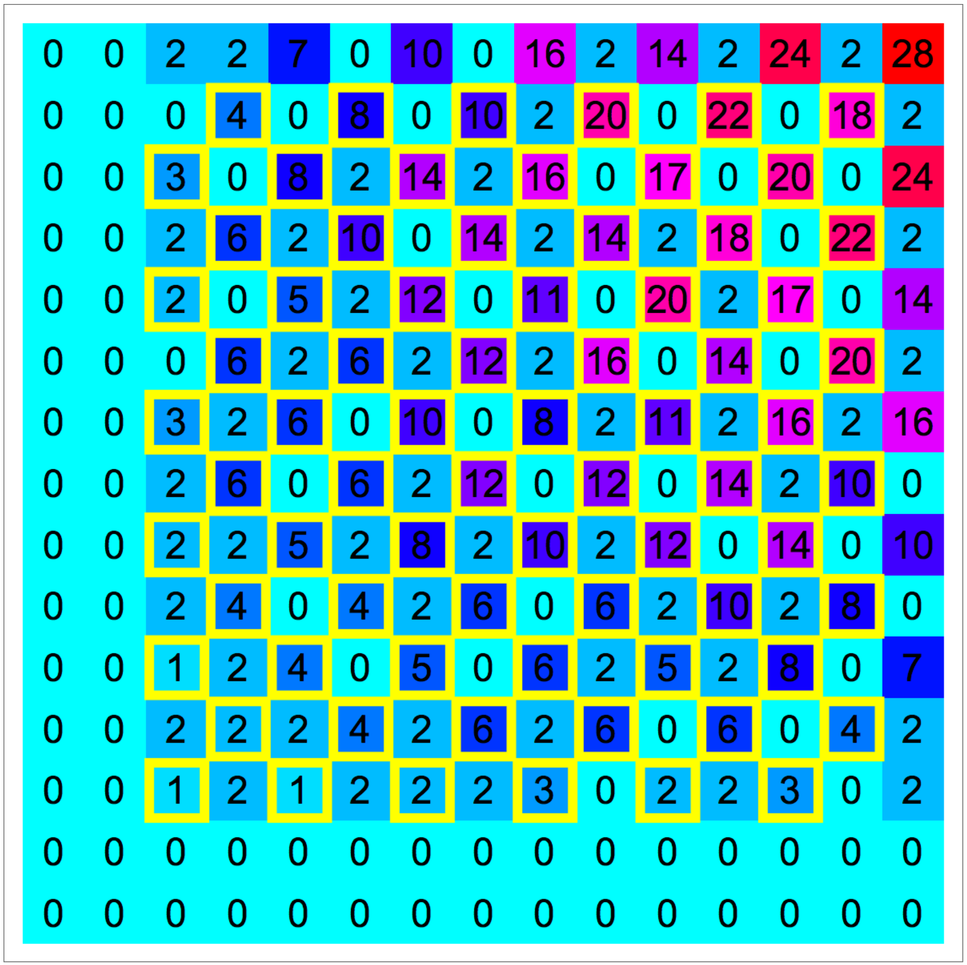
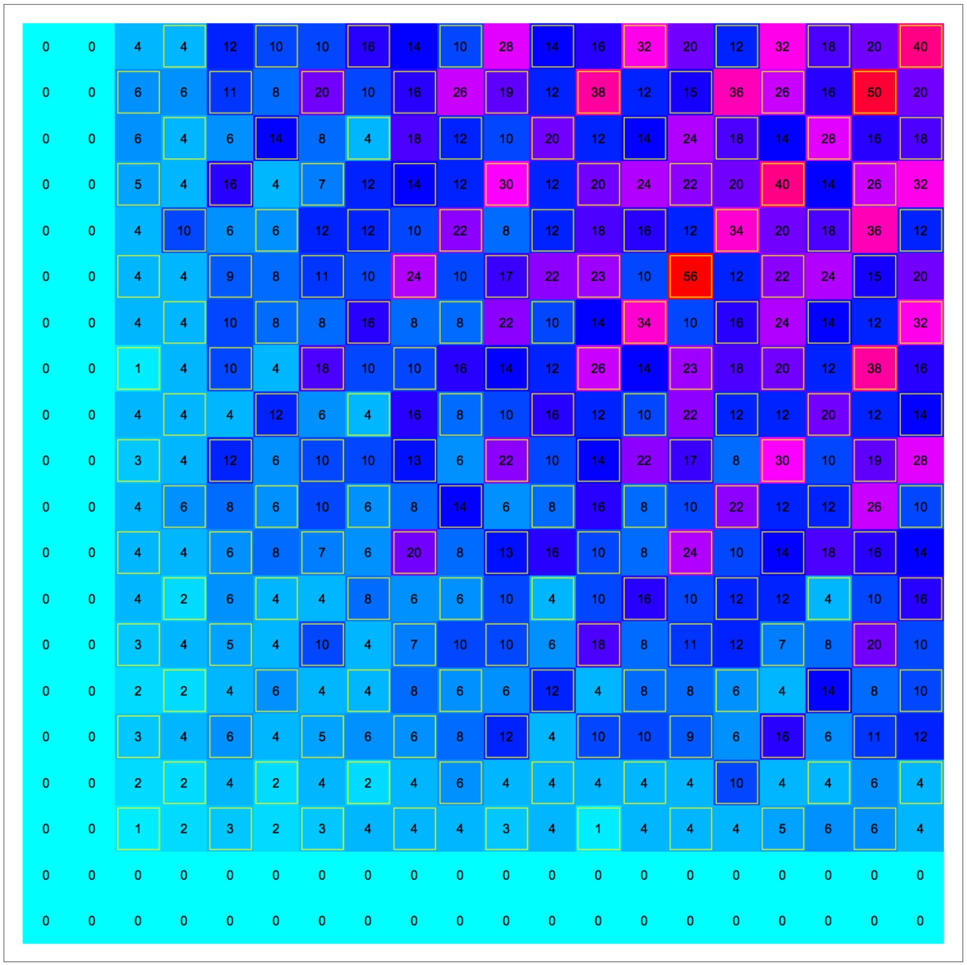


FIGURE 14. The number of times an Eisenstein integer $a+bw$ can be written as a sum of Eisenstein primes. For $b=2$, this appears always possible as $p+q$ with form $p=x+w, q=y+w$. For $b=3$, two **Eisenstein ghost twins** which are $109+3w$ and $121+3w$ appear. Later we have still gaps when forcing individual rows but they don't intersect.



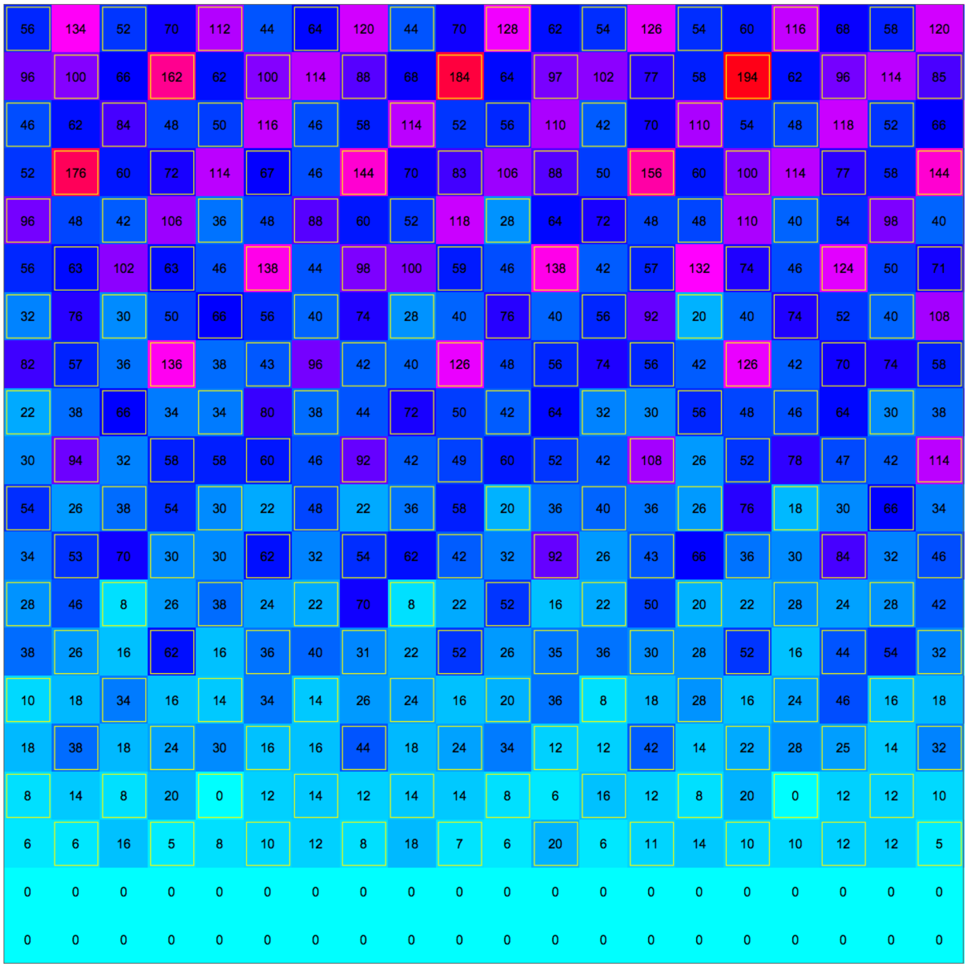
0	0	2	2	7	0	10	0	16	2	14	2	24	2	28
0	0	0	4	0	8	0	10	2	20	0	22	0	18	2
0	0	3	0	8	2	14	2	16	0	17	0	20	0	24
0	0	2	6	2	10	0	14	2	14	2	18	0	22	2
0	0	2	0	5	2	12	0	11	0	20	2	17	0	14
0	0	0	6	2	6	2	12	2	16	0	14	0	20	2
0	0	3	2	6	0	10	0	8	2	11	2	16	2	16
0	0	2	6	0	6	2	12	0	12	0	14	2	10	0
0	0	2	2	5	2	8	2	10	2	12	0	14	0	10
0	0	2	4	0	4	2	6	0	6	2	10	2	8	0
0	0	1	2	4	0	5	0	6	2	5	2	8	0	7
0	0	2	2	2	4	2	6	2	6	0	6	0	4	2
0	0	1	2	1	2	2	2	3	0	2	2	3	0	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

FIGURE 15. The matrix entries in the picture show how many times a Gaussian integer can be written as a sum of two Gaussian primes in Q. We see that the evenness condition is clearly necessary.



0	0	4	4	12	10	10	16	14	10	28	14	16	32	20	12	32	18	20	40
0	0	6	6	11	8	20	10	16	26	19	12	38	12	15	36	26	16	50	20
0	0	6	4	6	14	8	4	18	12	10	20	12	14	24	18	14	28	16	18
0	0	5	4	16	4	7	12	14	12	30	12	20	24	22	20	40	14	26	32
0	0	4	10	6	6	12	12	10	22	8	12	18	16	12	34	20	18	36	12
0	0	4	4	9	8	11	10	24	10	17	22	23	10	56	12	22	24	15	20
0	0	4	4	10	8	8	16	8	8	22	10	14	34	10	16	24	14	12	32
0	0	1	4	10	4	18	10	10	16	14	12	26	14	23	18	20	12	38	16
0	0	4	4	4	12	6	4	16	8	10	16	12	10	22	12	12	20	12	14
0	0	3	4	12	6	10	10	13	6	22	10	14	22	17	8	30	10	19	28
0	0	4	6	8	6	10	6	8	14	6	8	16	8	10	22	12	12	26	10
0	0	4	4	6	8	7	6	20	8	13	16	10	8	24	10	14	18	16	14
0	0	4	2	6	4	4	8	6	6	10	4	10	16	10	12	12	4	10	16
0	0	3	4	5	4	10	4	7	10	10	6	18	8	11	12	7	8	20	10
0	0	2	2	4	6	4	4	8	6	6	12	4	8	8	6	4	14	8	10
0	0	3	4	6	4	5	6	6	8	12	4	10	10	9	6	16	6	11	12
0	0	2	2	4	2	4	2	4	6	4	4	4	4	4	10	4	4	6	4
0	0	1	2	3	2	3	4	4	4	3	4	1	4	4	4	5	6	6	4
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 16. Here we see how many times an Eisenstein integer $a + wb$ can be written as a sum of two Eisenstein primes in Q. It looks as if we can write any $a + bw$ with $a > 1, b > 1$ as a sum of two Eisenstein primes in Q. But it only appears so at first.



56	134	52	70	112	44	64	120	44	70	128	62	54	126	54	60	116	68	58	120
96	100	66	162	62	100	114	88	68	184	64	97	102	77	58	194	62	96	114	85
46	62	84	48	50	116	46	58	114	52	56	110	42	70	110	54	48	118	52	66
52	176	60	72	114	67	46	144	70	83	106	88	50	156	60	100	114	77	58	144
96	48	42	106	36	48	88	60	52	118	28	64	72	48	48	110	40	54	98	40
56	63	102	63	46	138	44	98	100	59	46	138	42	57	132	74	46	124	50	71
32	76	30	50	66	56	40	74	28	40	76	40	56	92	20	40	74	52	40	108
82	57	36	136	38	43	96	42	40	126	48	56	74	56	42	126	42	70	74	58
22	38	66	34	34	80	38	44	72	50	42	64	32	30	56	48	46	64	30	38
30	94	32	58	58	60	46	92	42	49	60	52	42	108	26	52	78	47	42	114
54	26	38	54	30	22	48	22	36	58	20	36	40	36	26	76	18	30	66	34
34	53	70	30	30	62	32	54	62	42	32	92	26	43	66	36	30	84	32	46
28	46	8	26	38	24	22	70	8	22	52	16	22	50	20	22	28	24	28	42
38	26	16	62	16	36	40	31	22	52	26	35	36	30	28	52	16	44	54	32
10	18	34	16	14	34	14	26	24	16	20	36	8	18	28	16	24	46	16	18
18	38	18	24	30	16	16	44	18	24	34	12	12	42	14	22	28	25	14	32
8	14	8	20	0	12	14	12	14	14	8	6	16	12	8	20	0	12	12	10
6	6	16	5	8	10	12	8	18	7	6	20	6	11	14	10	10	12	12	5
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

FIGURE 17. There are two integers $(3 + 109w)$ and $(3 + 121w)$ (as well as their mirrors) which can not be written as the sum of two positive Eisenstein primes $a + bw + (c + dw)$ with positive a, b, c, d. These are the bad **Eisenstein ghost twins**. Can you find the ghosts in the matrix? We believe they are the only ones.

References

[1] A002384. The on-line encyclopedia of integer sequences. https://oeis.org.

[2] A110673. The on-line encyclopedia of integer sequences. https://oeis.org.

[3] John C. Baez. The octonions. *Bull. Amer. Math. Soc. (N.S.)*, 39(2):145–205, 2002.

[4] P.T. Bateman and R.A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[5] K. Conrad. Hardy-Littlewood constants. In *Mathematical properties of sequences and other combinatorial structures (Los Angeles, CA, 2002)*, pages 133–154. Kluwer Acad. Publ., Boston, MA, 2003.

[6] J.H. Conway and D.A. Smith. *On Quaternions and Octonions*. A.K. Peters, 2003.

[7] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math. J.*, 13:561–578, 1946.

[8] H.S.M. Coxeter. *Regular Polytopes*. Dover Publications, New York, 1973.

[9] L.E. Dickson. *History of the theory of numbers. Vol. I:Divisibility and primality.* Chelsea Publishing Co., New York, 1966.

[10] A. Doxiadis. *Uncle Petros and Goldbach's Conjecture*. Bloomsbury, USA, New York, 2000.

[11] S. Wagon E. Gethner and B. Wick. A stroll through the Gaussian primes. *Amer. Math. Monthly*, 105(4):327–337, 1998.

[12] T. Oliveira e Silva, S. Herzog, and S. Pardi. Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$. *Math. Computation*, 83:2033–2060, 2014.

[13] G. Eisenstein. *Mathematische Werke*. Chelsea, New York, 1975.

[14] S. R. Garcia. Quotients of Gaussian primes. *Amer. Math. Monthly*, 120(9):851–853, 2013.

[15] C. F. Gauss. Theoria residuorum biquadraticorum. commentatio secunda. *Comm. Soc. Reg. Sci. Gttingen*, 7:1–34, 1832.

[16] E. Gethner and H.M. Stark. Periodic Gaussian moats. *Experiment. Math.*, 6(4):289–292, 1997.

[17] R. Gross and J.H. Smith. A generalization of a conjecture of Hardy and Littlewood to algebraic number fields. *Rocky Mountain J. Math.*, 30(1):195–215, 2000.

[18] Richard K. Guy. *Unsolved Problems in Number Theory*. Springer, Berlin, 3 edition, 2004.

[19] G. H. Hardy and S. Ramanujan. Asymptotic formulæ in combinatory analysis [Proc. London Math. Soc. (2) **17** (1918), 75–115]. In *Collected papers of Srinivasa Ramanujan*, pages 276–309. AMS Chelsea Publ., Providence, RI, 2000.

[20] G.H. Hardy and J.E. Littlewood. Partitio numerorum III: On the expression of a number as a sum of primes. *Acta. Math*, 44:1–70, 48, 1923.

[21] H.A. Helfgott. Numerical verification of the Ternary Goldbach Conjecture up to $8.875 \cdot 10^{30}$. https://arxiv.org/pdf/1305.3062, 2014.

[22] C. A. Holben and J. H. Jordan. The twin prime problem and Goldbach's conjecture in the Gaussian integers. *Fibonacci Quart.*, 6(5):81–85, 92, 1968.

[23] L.K. Hua. *Introduction to Number theory.* Springer Verlag, Berlin, 1982.

[24] A. Hurwitz. *Zahlentheorie der Quaternionen*. Springer, 1919.

[25] S. Wagon J. Renze and B. Wick. The Gaussian zoo. *Experiment. Math.*, 10(2):161–173, 2001.

[26] J. H. Jordan and J. R. Rabung. Local distribution of Gaussian primes. *J. Number Theory*, 8(1):43–51, 1976.

[27] J.H. Jordan and J.R. Rabung. A conjecture of Paul Erdoös concerning Gaussian primes. *Math. Comp.*, 24:221–223, 1970.

[28] A.P. Juskevic and J.K. Kopelievic. *Christian Goldbach, 1690-1764*, volume 8. Vita Mathematica, 1994.

[29] J. Kirmse. Über die darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten und über ein mit diesem Problem zusammenhängendes nichtkommutatives und nichtassoziatives Zahlensystem. *Berichte Verhandlungen Sächs. Akad. Wiss. Leipzig. Math. Phys. Kl*, 76:63–82, 1925.

[30] H. Koch. Der briefwechsel von Leonhard Euler und Christian Goldbach. *Elem. Math*, 62:155–166, 2007.

[31] A. Korkin and G. Zolotareff. Sur les formes quadratique positive quaternaires. *Math Ann.*, 5:581–583, 1872.

[32] P. Loh. Stepping to infinity along Gaussian primes. *Amer. Math. Monthly*, 114(2):142–151, 2007.

[33] B. Mazur and W. Stein. *Prime Numbers and the Riemann Hypothesis*. Cambridge University Press, 2016.

[34] J. Mehta and G.K. Viswanadham. Set of uniqueness of shifted Gaussian primes. *Funct. Approx. Comment. Math.*, 53(1):123–133, 2015.

[35] T. Mitsui. On the Goldbach problem in an algebraic number field I. *J. Math. Soc. Japan*, 12(3), 1960.

[36] R. Moufang. Alternativkörper und der Satz vom vollständigen Vierseit (D_9). *Abhandlungen aus dera Mathematischen Seminar der Hamburgischen Universität*, 9:207–222, 1933.

[37] P.J. Nahin. *Number Crunching*. Princeton University Press, 2011.

[38] J. Pintz. Landau's problems on primes. *Journal de Theorie des Nombres de Bordeaux*, 21:357–404, 2009.

[39] H. Riesel. *Prime numbers and computer methods for factorization*, volume 57 of *Progress in Mathematics*. Birkhäuser Boston Inc., 1985.

[40] B. Schechter. *My brain is open*. Simon & Schuster, New York, 1998. The mathematical journeys of Paul Erdős.

[41] Daniel Shanks. On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$. *Math. Comp.*, 14:320–332, 1960.

[42] J. Stillwell. *Elements of Number Theory*. Springer, 2003.

[43] T. Tao. The Gaussian primes contain arbitrarily shaped constellations. *J. Anal. Math.*, 99:109–176, 2006.

[44] I. Vardi. Prime percolation. *Experiment. Math.*, 7(3):275–289, 1998.

[45] R.C. Vaughan. Recent work in additive prime number theory. In *Proceedings of the international congress of Mathematicians*, pages 389–394, 1978.

[46] R.C. Vaughan. *The Hardy-Littlewood Method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, second edition, 1997.

[47] M. Viazovsaka. The sphere packing problem in dimension 8. http://arxiv.org/abs/1603.04246, 2016.

[48] I.M. Vinogradov. *The Method of Trigonometric Sums in the Theory of Numbers*. Dover Publications, 1954.

[49] S. Wagon. *Mathematica in Action*. Springer, third edition, 2010.

[50] A.E. Western. Note on the number of primes of the form $n^2 + 1$. *Cambridge Phil. Soc., Proc.*, 21:108–109, 1922.

[51] A.E. Western and J.C.P. Miller. *Tables of indices and primitive roots. Royal Society Mathematical Tables*, volume 9. Royal Society at the Cambridge University Press, London, 1968.

[52] H.C. Williams. The influence of computers in the development of number theory. *Comp. and Maths. with Applications*, 8(2):75–93, 1982.

[53] M.C. Wunderlich. On the Gaussian primes on the line $\text{Im}(X) = 1$. *Math. Comp.*, 27:399–400, 1973.

[54] D. Zagier. A one-sentence proof that every prime p = 1 mod 4 is a sum of two squares. *Amer. Math. Monthly*, 97:144, 1990.

Department of Mathematics, Harvard University, Cambridge, MA, 02138