Goldbach Partitions and Sequences

Subhash Kak

Subhash Kak is Regents Professor at Oklahoma State University in Stillwater. His technical research is in the fields of information theory, neural networks, and quantum information and he has also written on archaeoastronomy and art. He is the author of twenty books that include *The Architecture of Knowledge.*

Properties of Goldbach partitions of numbers, as sums of primes, are presented and their potential applications to cryptography are described. The sequence of the number of partitions has excellent randomness properties. Goldbach partitions can be used to create ellipses and circles on the number line and they can also be harnessed for cryptographic applications.

Keywords
Number theory, cryptography, random sequences.

1. Introduction

The Goldbach conjecture, that every even integer can be expressed as a sum of two primes, is one of the most enduring unsolved problems of mathematics [1]. The conjecture was first made in a letter Christian Goldbach wrote to the Swiss mathematician Leonhard Euler on 7 June 1742. In his response on 30 June of the same year, Euler said: "Every even integer is a sum of two primes. I regard this as a completely certain theorem, although I cannot prove it." This has remained as one of the best known unsolved problems of mathematics to this day and is referred to as the 'strong' Goldbach conjecture.

There is another version of the conjecture that states that every odd number greater than 7 is a sum of three odd primes. This is called the 'weak' Goldbach conjecture. Computer experiments have shown that the conjectures are true for $n \leq 4 \times 10^{18}$.

A representation of a number as a sum of primes is a prime partition. Some examples of prime partitions are given in *Table* 1.

The prime partitions are a special case of partition function $p(n)$, that represents the number of possible parti-

Table 1.

Even Numbers	Odd Numbers
8 = 3+5	9 = 3+3+3 and 5+2+2
10 = 3+7 and 5+5	11 = 7+2+2 and 5+3+3
22 = 19+3, 17+5, 11+11	19 = 13+3+3, 11+5+3, 7+7+5
34 = 31+3, 29+5, 23+11, 17+17	37 = 17+17+3, 17+13+7, 13+13+11

tions of n. For example, $p(4) = 5$ since we can write it as 4, 3+1, 2+2, and 2+1+1, and 1+1+1+1. The prime partition function has applications in physics as properties of certain matter states can be seen to be related to the number of ways elementary particles states can be brought together.

Srinivasa Ramanujan famously proved the following identities for the general partition function $p(n)$:

$$p(5n+4) = 0 \bmod 5$$
$$p(7n+5) = 0 \bmod 7$$
$$p(11n+6) = 0 \bmod 11\,.$$

The line of research set in motion by Ramanujan has led to brilliant success in recent years and a formula that generates the partition function for any n has been found [2].

If the general partition function is of importance in physics, the prime partition function is of importance in cryptography. Specific partitions of very large numbers can serve as keys for secure digital communication. Let $g(n)$ be the number of unique ways n can be expressed as $p + q$, where p and q are primes. As the value of the number n increases, the number of pairs $g(n)$ that produces the sum also increases. The sender and the receiver of encrypted data can choose a key related to a

The line of research set in motion by Ramanujan has led to brilliant success "in recent years and a formula that generates the partition function for any *n* has been found.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$g(n)$	1	1	1	2	1	2	2	2	2	3	3	3	2	3	2	4	4	2	3	4	3	4	5	4	3	5	3

Table 2. Number of Goldbach partitions $g(n)$ of even number n.

specific partition of a large shared number, whereas, an eavesdropper will only discover the key by an exhaustive search, thus, defining an asymmetry in the process. *Table* 2 presents some values of $g(n)$.

Here, we are not interested in the general partition function $p(n)$ but rather the Goldbach partition function $g(n)$, or the different ways a number can be represented as a sum of two primes (for even numbers) and three primes (for odd numbers). We call this the Goldbach sequence $g(n)$, which may be converted into a binary sequence $b(n)$ by mapping each even number to 0 and each odd number to 1. The resulting binary sequences may be used as pseudorandom sequences in communications and computing and also in cryptography to generate random keys.

In this article, we present some elementary results on the Goldbach partitions and sequences. Then, we show how we can generate what we call Goldbach circles, ellipses and balloons. The sequences of these functions have excellent randomness properties [3, 4], which make their use in cryptographic applications possible. In this, they are similar to other mathematical functions that generate random sequences (e.g., [5, 6] which uses decimal expansions for coding). However, at this point, we need to generate all possible Goldbach partitions by a method that is basically equivalent to that of trial and error. If results similar to that obtained for Ramanujan's partitions are obtained for Goldbach partitions, it will have significant applications to coding and cryptography.

If results similar to that obtained "for Ramanujan's partitions are obtained for Goldbach partitions, it will"have significant applications to coding and cryptography.

2. Number of Partitions

The theory of partitions provides estimates on the function $g(n)$. Here, we confine ourselves to partitions of even numbers only, for convenience. *Figures* 1 and 2 provide

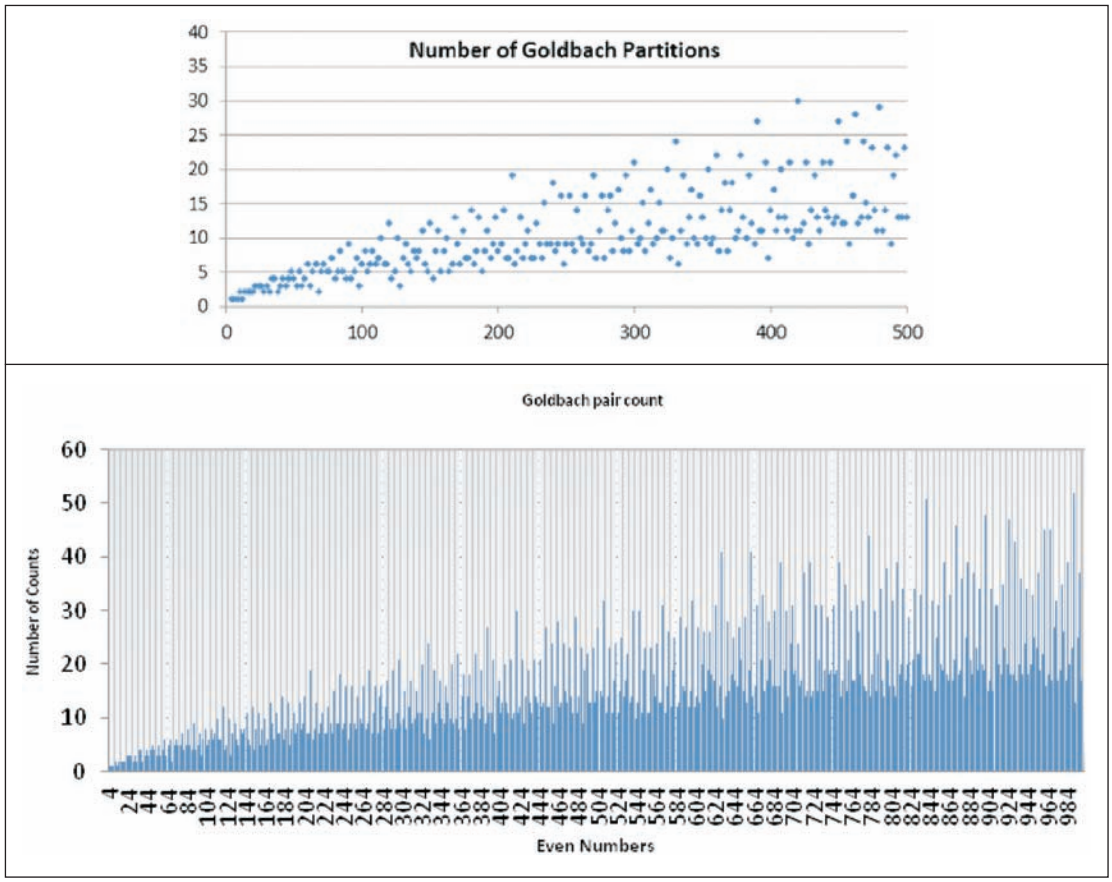

Figure 1 (top). Number of Goldbach partitions $g(n)$ for $n \leq 500$.

Figure 2 (bottom). Number of Goldbach partitions $g(n)$ for $n \leq 1000$.

examples of the function to the values 500 and 1000. The function grows in the form of a band.

A formula estimating $g(n)$ may be derived using statistical considerations. For large n and m between 3 and $n/2$, the probability of m and $n-m$ being prime is given by $1/[\ln m \ln(n-m)]$. Thus, the number of ways a large even number n can be expressed as a sum of two odd primes is approximately equal to

$$\sum_{m=3}^{n/2} \frac{1}{\ln m \ln(n-m)} \approx \frac{n}{2\ln^2 n} .$$

However, this expression may in general, not include dependencies among numbers. For example, for an even

number n that is divisible by 3, and m prime, $n-m$ is co-prime to 3 and thus more likely to be prime rather than a general number. If corrections are used, we obtain the estimate [7]:

$$2\pi_2 \left(\prod_{p|n;p\geq 3} \frac{p-1}{p-2} \right) \frac{n}{\ln^2 n},$$

where π_2 is the twin prime constant $\prod_{p\geq 3} \left(1 - \frac{1}{(p-1)^2}\right) = 0.6601618158\ldots$.

Table 3 presents the number of Goldbach partitions for numbers up to 104. Over this range, the number varies between 1 and 14. For numbers less than 2000, the largest number of partitions is 91 for $n = 1890$.

Let the partitions of even number n be g_1 and g_2. If n is divisible by 4, then $g_1 + g_2 = 0 \bmod 4$. Now assume

Table 3. Number of partitions up to $n = 104$.

n	$g(n)$	n	$g(n)$	n	$g(n)$
4	1	38	2	72	6
6	1	40	3	74	5
8	1	42	4	76	5
10	2	44	3	78	7
12	1	46	4	80	4
14	2	48	5	82	5
16	2	50	4	84	8
18	2	52	3	86	5
20	2	54	5	88	4
22	3	56	3	90	9
24	3	58	4	92	4
26	3	60	6	94	5
28	2	62	3	96	7
30	3	64	5	98	3
32	2	66	6	100	6
34	4	68	2	102	8
36	4	70	5	104	5

$g_1 - g_2 = 0 \bmod 4$. Then, $2g_1 = 0 \bmod 4$, which means that g_1 is even which is impossible since it is a prime partition. This means that if $g_1 + g_2 = 0 \bmod 4$, then $g_1 - g_2 \neq 0 \bmod 4$.

The partition function $g(n)$ has a local peak for multiples of primes. We obtain local peaks at multiples of $2 \times 3 = 6$; $2 \times 3 \times 5 = 30$; $2 \times 3 \times 5 \times 7 = 210$; $2 \times 3 \times 5 \times 11 = 330$; $2 \times 3 \times 5 \times 13 = 390$; $2 \times 3 \times 5 \times 7 \times 11 = 2310$; $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$; $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 = 510510$; $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 = 9699690$, etc. Owing to these peaks, we obtain other conditions such as $g(6k) > g(6k+2)$, $g(30k) > g(30k+2)$, $g(210k) > g(210k+2)$ and so on.

Table 4 illustrates the difference between multiples of these numbers and their adjacent values. The difference between the peak and the next values ranges from more than twice to four times.

For $n = 6$, 30, and 210, all primes in the range $[n/2, n-2]$ are among the partitions. The number $n = 210$ is the largest such number possible.

The Goldbach partitions of 30 are (23,7), (19, 11) and

The partition function $g(n)$ has a local peak for multiples of primes.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
200	8	320	11	380	13	2300	49
202	9	322	11	382	10	2302	32
204	14	324	20	384	19	2304	68
206	7	326	7	386	12	2306	34
208	7	328	10	388	9	2308	34
210	19	330	24	390	27	2310	114
212	6	332	6	392	11	2312	35
214	8	334	11	394	11	2314	40
216	13	336	19	396	21	2316	66
218	7	338	9	398	7	2318	38

Table 4. The number of partitions near 210, 330, 390 and 2310.

The Goldbach partitions of 420 cover all primes in the range [*n*/2, *n*–2] excepting 277, 251 and 233.

(17, 13); and that of 210 are

(199, 11), (197, 13), (193, 17), (191, 19), (181, 29), (179, 31), (173, 37), (167, 43), (163, 47), (157, 54), (151, 59), (149, 61), (139, 71), (137, 73), (131, 79), (127, 83), (113, 97), (109, 101), (107, 103).

The Goldbach partitions of 420 cover all primes in the range $[n/2, n-2]$ excepting 277, 251 and 233. In the case of $n=630$, all primes in the corresponding range are covered excepting these eight cases: 509, 487, 461, 443, 421, 409, 383, and 331.

3. Goldback Circles and Ellipses

Let $2n = p + q$, as sum of two primes and so, $n - p = q - n$. The Goldbach radius of the number n is then the smallest $n - p$ associated with the number. For example, consider $n=14$. The number 28 can be expressed in two ways as sum of primes that are equidistant from 14: $5+23$ and $11+17$. The Goldbach radius of 14 is then the smaller of the two sets, which is 3. This radius, therefore, picks one of the Goldbach partitions associated with the number and it associates a circle with the number.

A generalization of the circle is the ellipse, where the distances between the components on two sides of the even number are different. An ellipse can be constructed around an even number n on the number line, where, the distance of the two extreme points from n is j and k, respectively. This will, in general, be represented by the (j, k) ellipse. For example, the (3,5) ellipse around 22 consists of the partitions 19 and 37.

The circle sequence associated with a set of even numbers is the corresponding values of the radii. The ellipse sequence $(1, k)$ is the set of random numbers m associated with the given natural numbers n so that $n - m$ and $n + km$ are primes. These numbers are reduced to 1 and -1 by computing their mod 4 value.

n	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
r	1	9	3	5	9	3	1	3	15	5	3	9	7	3	15	1	9	3
r mod 4	1	1	-1	1	1	-1	1	-1	-1	1	-1	1	-1	-1	-1	1	1	-1

Table 5 (top). Circle sequence of random numbers, r, for n between 30 and 64.

n	16	18	22	24	26	28	32	34	36	38	42	44	46	48	52	54	56
m	3	1	3	1	3	5	1	5	5	1	1	3	3	1	5	7	3
m mod 4	-1	1	-1	1	-1	1	1	1	1	1	1	-1	-1	1	1	-1	-1

Table 6 (bottom). Ellipse sequence for $k = 5$.

Example 1. *Table* 5 consists of the circle sequence for numbers between 30 and 64. The r numbers are the random sequence and they can only be odd numbers. These may be converted to binary sequence by the mapping r mod 4.

Example 2. The ellipse sequence generated for $k = 5$, where n ranges from 16 to 56 is shown in *Table* 6. Note that, multiples of $k = 5$ do not figure in the list of n for ellipse sequences, since for such values the upper partition will not be prime. As explanation, the value for $n = 16$ is 3 since $16-3 = 13$ and $16 + 3 \times 5 = 31$ are primes.

It is clear that by proper choice of the starting point of the circle sequence and by doing this as well as picking values of k, any number of Goldbach random sequences can be generated.

4. Concentric Circles

Figure 3 provides a graphical example of concentric circles for small values of n. In particular, one can see

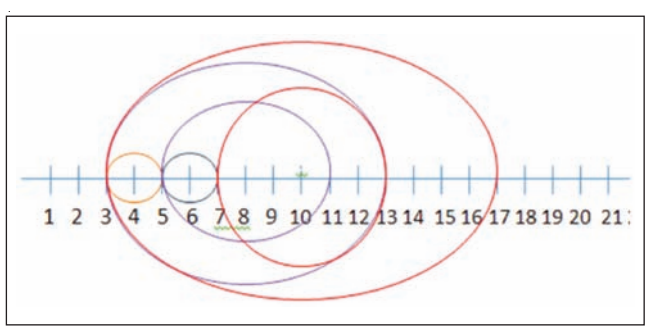

Figure 3. Concentric circles around $n = 4$, 6, 8, and 10.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
$k(n)$	1	1	2	2	3	2	2	4	3	3	5	3	3	6	5	2	6
$k(n)$ mod 2	1	1	0	0	1	0	0	0	1	1	1	1	1	0	1	0	0

n	202	204	206	208	210	212	214	216	218	220	222	224	226
$k(n)$	11	20	11	10	30	12	9	19	11	14	21	13	12
$k(n)$ mod 2	1	0	1	0	0	0	1	1	1	0	1	1	0

Table 7 (top). Number of concentric circles $k(n)$, n from 4 to 36.

Table 8 (bottom). Number of concentric circles $k(n)$, n from 202 to 226.

the two concentric circles about $n = 8$ and 10, and 12, although the larger ones have been shown somewhat squished.

Let the count of concentric circles for the number n be given by $k(n)$. *Tables* 7 and 8 provide some examples of $k(n)$. Note that what we called the circle sequence in the previous section represented merely the first circle information for each of the number points.

There are two circles for $n = 10$, namely (7, 13) and (3, 17), and likewise for $n = 24$, the five circles are (5, 43), (7, 41), (11, 37), (17, 31) and (19, 29).

Figure 4 presents the concentric circle count for small

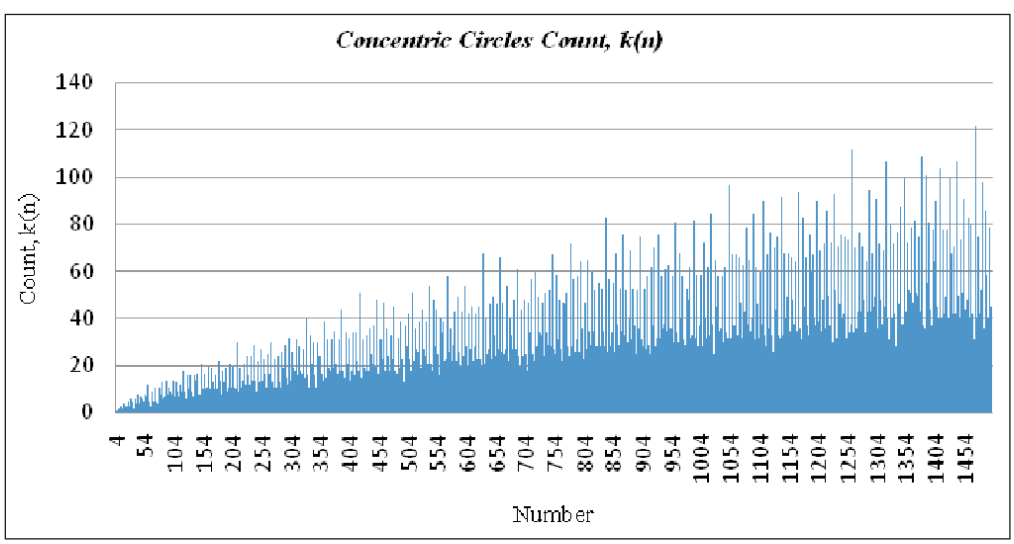

Figure 4. Concentric circles count, $k(n)$.

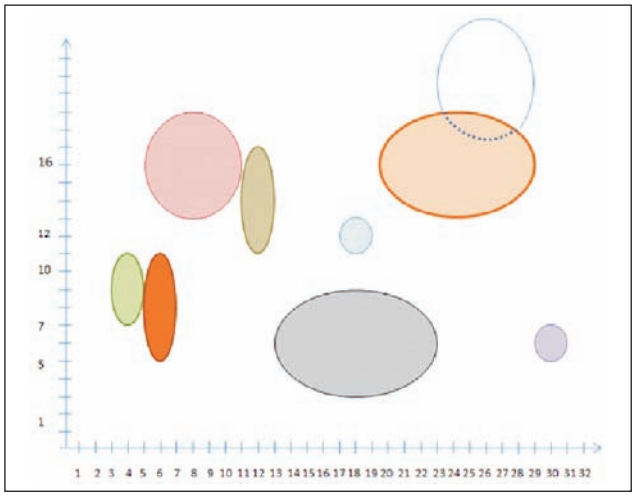

Figure 5. Goldbach balloons: circles and ellipses in two dimensions.

values of n. As in the case of the Goldbach partition count, the count $k(n)$ has peaks at multiples of 210.

Figure 5 is a representation of such sequences in two dimensions. We call these circles and ellipses as Goldbach balloons.

Goldbach partitions and sequences are fascinating objects to explore for their potential use in cryptography and computing. They are also of interest to number theorists.

Suggested Reading

[1] L E Dickson, Goldbach's Empirical Theorem: Every Integer is a Sum of Two Primes. In *History of the Theory of Numbers*, Vol.1, Divisibility and Primality, New York: Dover, pp.421–424, 2005.

[2] Ken Ono, The Last Words of a Genius, *Notices of the American Mathematical Society*, Vol.57, pp.1410–1419, 2010.

[3] K R Kanchu and S Kak, *Goldbach sequences for cryptographic applications*, arXiv:1208.1984

[4] D Cherlopalle and S Kak, *Goldbach triples and key distribution*, arXiv: 1209.0135

[5] S Kak and A Chatterjee, On decimal sequences, *IEEE Transactions on Information Theory*, Vol.IT-27, pp.647–652, 1981.

[6] S Kak, Encryption and error-correction coding using D sequences, *IEEE Transactions on Computers*, Vol.C-34, pp.803–809, 1985.

[7] G H Hardy and J E Littlewood, Some problems of partitio numerorum; III: on the expression of a number as a sum of primes, *Acta Mathematica* Vol.44, pp.1–70, 1922.

Acknowledgement

This research was supported in part by research grant #1117068 from the National Science Foundation, USA. I am thankful to K R Kanchu for his assistance.

Address for Correspondence
Subhash Kak
School of Electrical and Computer Engineering
Oklahoma State University
Stillwater, OK 74078, USA
Email:
subhash.kak@okstate.edu