# GOLDBACH VARIATIONS: PROBLEMS WITH PRIME NUMBERS

# Alessandro Zaccagnini

#### PRAELUDIUM

We will call prime numbers the integers  $n \ge 2$  which are divisible only by 1 and themselves. Euclid (fourth century B. C.) first showed that there exist infinitely many prime numbers. His proof is an excellent example of a mathematical argument: if 2, 3, 5, ..., p were the only prime numbers, we could construct the number  $2 \cdot 3 \cdot 5 \cdots p + 1$ , which has the property of leaving the remainder 1 when divided by any of our former prime numbers. Since every integer larger than 1 is either a prime number, or is divisible by at least a prime, our list can not be complete. According to the great British mathematician G. H. Hardy, this proof "is as fresh and significant as when it was discovered-two thousand years have not written a wrinkle on it."

The following is a short list of prime numbers.

| 2   | 3   | 5   | 7   | 11  | 13  | 17  | 19  | 23  | 29  | 31  | 37  | 41  | 43  |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 47  | 53  | 59  | 61  | 67  | 71  | 73  | 79  | 83  | 89  | 97  | 101 | 103 | 107 |
| 109 | 113 | 127 | 131 | 137 | 139 | 149 | 151 | 157 | 163 | 167 | 173 | 179 | 181 |
| 191 | 193 | 197 | 199 | 211 | 223 | 227 | 229 | 233 | 239 | 241 | 251 | 257 | 263 |
| 269 | 271 | 277 | 281 | 283 | 293 | 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 |
| 353 | 359 | 367 | 373 | 379 | 383 | 389 | 397 | 401 | 409 | 419 | 421 | 431 | 433 |
| 439 | 443 | 449 | 457 | 461 | 463 | 467 | 479 | 487 | 491 | 499 | 503 | 509 | 521 |
| 523 | 541 | 547 | 557 | 563 | 569 | 571 | 577 | 587 | 593 | 599 | 601 | 607 | 613 |
| 617 | 619 | 631 | 641 | 643 | 647 | 653 | 659 | 661 | 673 | 677 | 683 | 691 | 701 |
| 709 | 719 | 727 | 733 | 739 | 743 | 751 | 757 | 761 | 769 | 773 | 787 | 797 | 809 |
| 811 | 821 | 823 | 827 | 829 | 839 | 853 | 857 | 859 | 863 | 877 | 881 | 883 | 887 |
| 907 | 911 | 919 | 929 | 937 | 941 | 947 | 953 | 967 | 971 | 977 | 983 | 991 | 997 |

Table 1. The prime numbers below 1000.

Now that we know that there are infinitely many prime numbers, we might ask if there is a method to compute them, apart from trial division. Eratosthenes (second century B. C.) devised the so-called sieve that allows to separate the prime numbers from the composite ones: we show how it works by means of Table 2. Setting aside the number 1, which has a special status, we delete from the table below all multiples of 2 starting from  $2^2 = 4$ . Next, we look for the first uncancelled number, which is 3, and go on as before, starting from  $3^2 = 9$ . We repeat these operations with 5, starting from  $5^2 = 25$ , then with 7, from  $7^2 = 49$ , and finally with 11, from  $11^2 = 121$ . Now we can stop, since the first uncancelled number is 13 and  $13^2 = 169$  is outside our table, which now shows 1 and all prime numbers through 144. The lines help to cancel multiples of the same prime number.



Table 2. Eratosthenes' sieve.

Prime numbers go on forever, according to Euclid, but looking carefully at Table 1 one sees that their density seems to decrease slowly, and this can be checked building larger tables, as our Table 3 below shows. Can we explain this phenomenon? Performing the operations required by the sieve on the integers 1, 2, ..., N, (where N is a very large number) we can observe that only about one half of the integers survive the first step (when we deal with the prime number 2), and only  $\frac{2}{3}$  of them remain after the second step (p = 3), and so on. In other words, when dealing with the prime number p we cancel about 1/p-th of the integers in our table that have not been cancelled yet. Since every non-prime integer has at least a prime factor not exceeding its square root, at the end the proportion of surviving numbers in Table over their total should be roughly

$$\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\cdots\left(1-\frac{1}{p}\right),$$

where p is the largest prime number  $\leq \sqrt{N}$ . We can not even hint at a proof here, but it is known that the above product is approximately

$$\frac{c}{\log N} \tag{1}$$

where c = 1.1229197..., if N is a very large number. Here and in the sequel log denotes the *natural logarithm* function, in base e = 2.718281828... If N is a very large number, it may seem legitimate to expect that there should be approximately  $cN/\log N$  prime numbers  $\leq N$ , since (1) apparently represents the proportion of uncancelled numbers in Eratosthenes' sieve. Actually this is not the case, since for large N the proportion of the numbers cancelled by the prime  $p \leq \sqrt{N}$  is very rarely

exactly 1/p: this happens only exceptionally. The computations leading to (1) are not therefore fully justified, but using a different and rather intricate argument (too long and complicated to be summarized here), Jacques Hadamard and Charles de la Vallée Poussin proved independently in 1896 that

$$\pi(N) \sim \frac{N}{\log N},\tag{2}$$

where, traditionally,  $\pi(N)$  denotes the number of prime numbers not exceeding N. There is no danger of confusion with the other meaning of  $\pi$ : in this talk the number  $\pi = 3.14159...$  will never appear. The symbol  $\sim$  denotes an approximate equality: more precisely, (2) means that the ratio between the quantities  $\pi(N)$  and  $N/\log N$  is very close to 1 when N is very large. This is known as the Prime Number Theorem, and it is the result of more than a century of efforts of first-rate mathematicians, such as L. Euler, C. F. Gauss, P. L. Dirichlet, B. Riemann, P. Chebyshev.

Table 3 shows the value of  $\pi(N)$  when N is a small power of 10, the error in the approximation and the ratio between the quantities in (2).

| N         | $\pi(N)$  | $\pi(N) - \frac{N}{\log N}$ | $\frac{\pi(N)\log N}{N}$ |
|-----------|-----------|-----------------------------|--------------------------|
| 10        | 4         | 0                           | $0.921\ldots$            |
| $10^{2}$  | 25        | 3                           | 1.151                    |
| $10^{3}$  | 168       | 23                          | $1.161\ldots$            |
| $10^{4}$  | 1229      | 143                         | $1.132\ldots$            |
| $10^{5}$  | 9592      | 906                         | $1.104\ldots$            |
| $10^{6}$  | 78498     | 6116                        | $1.084\ldots$            |
| $10^{7}$  | 664579    | 44158                       | $1.071\ldots$            |
| $10^{8}$  | 5761455   | 332774                      | $1.061\ldots$            |
| $10^{9}$  | 50847534  | 2592592                     | $1.054\ldots$            |
| $10^{10}$ | 455052511 | 20758029                    | 1.048                    |

**Table 3.** Values of  $\pi(N)$  for  $N = 10^n$ , n = 1, ..., 10. The differences in the third column are rounded to the nearest integer.

#### THEMA: GOLDBACH'S PROBLEM

In 1742, the mathematician Christian Goldbach, in a letter to Euler, stated that every even integer larger than 4 can be written as a sum of two (not necessarily distinct) odd primes. In other words, if n is an even integer larger than 4 it is possible to find two odd prime numbers  $p_1$  and  $p_2$  so that

$$n = p_1 + p_2.$$
 (3)

For instance, 10 = 3 + 7 = 5 + 5 = 7 + 3. Today this is known as "Goldbach's binary problem," and no proof has been found yet. We give the number of solutions of equation (3) (denoted by r(n)) for even n through 200 in Table 4. Note that r(4) = 1 because 4 = 2 + 2, and that, as above for 10, solutions like 3 + 7 and 7 + 3 are considered as distinct.

| In this case, an analysis of Table 4 seems to show that the number of solution      | ns |
|---|----|
| r(n) grows with n, but in an extremely irregular fashion: for example, $r(180) = 2$ | 8, |
| while $r(182) = 12$ . Can we try and explain this phenomenon, too?                  |    |

| n  | r(n)   | n  | r(n)  | n  | r(n)  | n  | r(n)  | n  | r(n)   |
|--|--|--|---|--|---|--|---|--|--|
| $     \begin{array}{r}       2 \\       12 \\       22 \\       32 \\       42     \end{array} $       | $\begin{array}{c} 0\\ 2\\ 5\\ 4\\ 8\end{array}$  | $ \begin{array}{r}     4 \\     14 \\     24 \\     34 \\     44 \end{array} $ | $egin{array}{c} 1 \ 3 \ 6 \ 7 \ 6 \end{array}$  | $     \begin{array}{r}       6 \\       16 \\       26 \\       36 \\       46     \end{array} $       | $\begin{array}{c}1\\4\\5\\8\\7\end{array}$  | $     \begin{array}{r}       8 \\       18 \\       28 \\       38 \\       48     \end{array} $       | $\begin{array}{c}2\\4\\3\\10\end{array}$  | $     \begin{array}{r}       10 \\       20 \\       30 \\       40 \\       50     \end{array} $      | $\begin{array}{c} 3\\ 4\\ 6\\ 6\\ 8\end{array}$  |
| 52     62     72     82     92 $     92     $  | $\begin{array}{c} 6\\ 5\\ 12\\ 9\\ 8\end{array}$   | $54 \\ 64 \\ 74 \\ 84 \\ 94$   | $     \begin{array}{r}       10 \\       10 \\       9 \\       16 \\       9     \end{array} $   | $56 \\ 66 \\ 76 \\ 86 \\ 96$   | $     \begin{array}{r}       6 \\       12 \\       10 \\       9 \\       14     \end{array} $   | $     58 \\     68 \\     78 \\     88 \\     98   $   | $\begin{array}{c} 7\\ 4\\ 14\\ 8\\ 6\end{array}$  | $ \begin{array}{c} 60 \\ 70 \\ 80 \\ 90 \\ 100 \end{array} $   | $     \begin{array}{c}       12 \\       10 \\       8 \\       18 \\       12     \end{array} $ |
| $     \begin{array}{r}       102 \\       112 \\       122 \\       132 \\       142     \end{array} $ | $     \begin{array}{r}       16 \\       14 \\       7 \\       18 \\       15     \end{array} $ | $104 \\ 114 \\ 124 \\ 134 \\ 144$  | $     \begin{array}{r}       10 \\       20 \\       10 \\       11 \\       22     \end{array} $ | $     \begin{array}{r}       106 \\       116 \\       126 \\       136 \\       146     \end{array} $ | $     \begin{array}{r}       11 \\       12 \\       20 \\       10 \\       11     \end{array} $ | $     \begin{array}{r}       108 \\       118 \\       128 \\       138 \\       148     \end{array} $ | $     \begin{array}{r}       16 \\       11 \\       6 \\       16 \\       10 \\     \end{array} $ | $     \begin{array}{r}       110 \\       120 \\       130 \\       140 \\       150     \end{array} $ | $     12 \\     24 \\     14 \\     14 \\     24   $   |
| $     \begin{array}{r}       152 \\       162 \\       172 \\       182 \\       192     \end{array} $ |  | $154 \\ 164 \\ 174 \\ 184 \\ 194$  | $16 \\ 10 \\ 22 \\ 16 \\ 13$  | $     156 \\     166 \\     176 \\     186 \\     196   $  | $22 \\ 11 \\ 14 \\ 26 \\ 18$  | $     158 \\     168 \\     178 \\     188 \\     198   $  | $9 \\ 26 \\ 13 \\ 10 \\ 26$   | $     \begin{array}{r}       160 \\       170 \\       180 \\       190 \\       200     \end{array} $ | $16 \\ 18 \\ 28 \\ 16 \\ 16$   |

**Table 4.** Values of r(n) for even n through 200.

First of all, it is rather reasonable that r(n) grows somehow, since the larger n, the larger the number of primes that can appear as summands in (3). Furthermore, we can use (2) to obtain an expected "order of magnitude" for r(n).

Take a very large number N, and consider the  $\pi(N) - 1$  odd primes less than or equal to N, and all of their possible sums. Obviously, if both  $p_1$  and  $p_2$  are  $\leq N$ , we can only conclude that  $p_1 + p_2 \leq 2N$ , but this is not very important, since we are content with an approximate result. By (2) the possible sums  $p_1 + p_2$  are

$$(\pi(N) - 1)^2 \sim \frac{N^2}{(\log N)^2},$$

so that, on average, every even integer  $n \leq 2N$  has about  $N/(\log N)^2$  representations of the type (3) with  $p_1$  and  $p_2 \leq N$ , since there are exactly N even integers  $\leq 2N$ . This average argument does not yet explain the remarkable irregularities in Table 4, but it suggests that r(n) should be close to

$$\frac{n}{(\log n)^2}.$$
(4)

Can we give a convincing explanation of what we observe? In other words, does (4) really give the right order of magnitude of r(n)? And, assuming the answer to be positive, how do we explain the irregularities of r(n)? In Table 5 we give the

solutions of the equations a + b = n for n = 60 and n = 62, where a and b are odd integers and  $a \le b$  (these are inessential simplifications that we introduce in order to keep the Table within reasonable size).

| 1 + 59     | 1 + 61    |
|------------|-----------|
| * 3 + 57 * | * 3 + 59  |
| 5 + 55     | 5 + 57 *  |
| 7 + 53     | 7 + 55    |
| * 9 + 51 * | * 9 + 53  |
| 11 + 49    | 11 + 51 * |
| 13 + 47    | 13 + 49   |
| *15 + 45 * | *15 + 47  |
| 17 + 43    | 17 + 45 * |
| 19 + 41    | 19 + 43   |
| *21 + 39 * | *21 + 41  |
| 23 + 37    | 23 + 39 * |
| 25 + 35    | 25 + 37   |
| *27 + 33 * | *27 + 35  |
| 29 + 31    | 29 + 33 * |
|            | 31 + 31   |
|            |           |

**Table 5.** How to obtain the solutions of equation (3) for n = 60 or n = 62. The stars mark the multiples of 3.

Now we perform a sort of double sieve, deleting from the potential solutions of equation (3) those with a summand divisible by 3, which are marked by stars. We immediately note an important difference between the two cases: when n = 60 the stars appear at the same height, so that when we consider the prime number 3 we only cancel 1/3 of the solutions of the equation a + b = 60 listed at the beginning, and 1 - 1/3 = 2/3 of them survive. On the contrary, when n = 62 we cancel about 2/3 of the solutions of the equation a + b = 62, leaving just 1 - 2/3 = 1/3 of the total.

How do we tell the two situations apart? It is not very difficult to see that the difference lies in the fact that 3 divides 60 but not 62. Obviously the prime number 3 itself is not special: the same argument holds for all odd primes  $p \leq \sqrt{n}$ . Hence, arguing by analogy with the earlier problem, we are tempted to modify the previous conjecture that r(n) is about (4), replacing it by

$$n \cdot \frac{1}{2} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \cdot \left(1 - \frac{2}{q_1}\right) \cdot \left(1 - \frac{2}{q_2}\right) \cdots \left(1 - \frac{2}{q_s}\right), \quad (5)$$

where  $p_1, \ldots, p_r$  are the distinct odd prime factors of n, while  $q_1, \ldots, q_s$  are the other odd primes below  $\sqrt{n}$ , and we inserted the factor  $\frac{1}{2}$  in order to take into account the fact that there is no even summand in (3) if  $n \neq 4$ .

Luckily it is not difficult to simplify the expression (5) somewhat: recalling the differences between (1) and (2), after a short computation, our conjecture takes the shape

$$r(n) \sim c' \cdot \frac{p_1 - 1}{p_1 - 2} \cdot \frac{p_2 - 1}{p_2 - 2} \cdots \frac{p_r - 1}{p_r - 2} \cdot \frac{n}{(\log n)^2},$$
 (6)

for a suitable constant c' = 1.3203... called "twin-prime constant" for a reason we shall presently see. We remark that, for instance, when n = 60 the product over

the prime factors in (6) is 8/3 = 2.6666... while for n = 62 it is only 30/29 = 1.03448... Hence, if our argument is correct, the reason why r(60) = 12 is more than twice r(62) = 5 is not mysterious anymore.

We said above that Goldbach's problem has not been settled, yet: there are radically different arguments which suggest the correctness of (6), itself a very strong form of the Goldbach conjecture, but nobody has been able to give a rigorous proof as of now. Actually, this conjecture has been checked by means of computers up to  $n = 4 \cdot 10^{14}$ , but obviously this can not be considered a proof. A part of the difficulty lies in the fact that the approximation given by (2) is not sufficiently precise. Anyway, several "approximate" results have been proved, but they are not easy to describe here. The easiest to talk about among them is now the subject of our ...

#### VARIATIO PRIMA

In (3) we considered the problem of representing large enough even numbers (where large enough means greater than 4) in the form  $p_1 + p_2$ , where  $p_1$  and  $p_2$  are odd primes. We now ask: what is the corresponding problem for the odd integers? Since every prime apart from 2 is odd, we have to sum three odd primes in order to get another odd integer. Hence, we call "ternary Goldbach conjecture" the following statement: for every sufficiently large odd integer n there exist three odd primes  $p_1$ ,  $p_2$  and  $p_3$ , not necessarily distinct, such that

$$n = p_1 + p_2 + p_3. (7)$$

Of course it is possible to work by analogy with the previous cases, performing a triple sieve. Furthermore it may be expected that this should be an easier problem, since the "average" argument leading to (4) now gives the much larger number  $n^2/(\log n)^3$ . Actually, in 1937 the Russian mathematician I. M. Vinogradov proved that for any sufficiently large odd integer n, the equation (7) has always at least one solution. Moreover Vinogradov proved that there is a formula similar to (6) for the number of solutions, which we call  $r_3(n)$ . If n is a large odd number

$$r_3(n) \sim c'' \cdot \frac{(p_1 - 1)(p_1 - 2)}{p_1^2 - 3p_1 + 3} \cdot \frac{(p_2 - 1)(p_2 - 2)}{p_2^2 - 3p_2 + 3} \cdots \frac{(p_r - 1)(p_r - 2)}{p_r^2 - 3p_r + 3} \cdot \frac{n^2}{(\log n)^3}, \quad (8)$$

where c'' is another positive constant, and  $p_1, p_2, \ldots, p_r$  are the prime factors of n.

At the time, Vinogradov could not say precisely what "sufficiently large" means, but later researches showed that every odd  $n > 3^{3^{15}}$  is sufficiently large. Unfortunately this is an enormous number (it has almost 7 million digits) which has been reduced over time, though it is still impossible to check the remaining cases by computer. Recently the French mathematician O. Ramaré proved that for any integer  $n \ge 2$ , the equation

$$n = p_1 + p_2 + \dots + p_r$$

is soluble with the p's prime numbers, and  $r \leq 7$ .

#### VARIATIO SECUNDA

We now change equation (3) turning the + sign into a - sign:

$$n = p_1 - p_2. (9)$$

The most important consequence is that while equation (3) could only have finitely many solutions, we can not say the same thing for equation (9). In order to compare the two situations, we consider a large number N, and we count the solutions of equation (9) with  $p_2 \leq N$ . Table 6 gives the number of solutions of (9) (denoted by  $\pi_n(N)$ ) for even n through 100, and N = 10000. We immediately see that all numbers in the Table are rather large, but once again there are visible irregularities: going back to our previous example,  $\pi_{60}(10000)$  is more than twice  $\pi_{62}(10000)$ . We ask: is it possible to find a simple explanation to this phenomenon?

| n  | $\pi_n$ | n  | $\pi_n$ | n  | $\pi_n$ | n  | $\pi_n$ | n   | $\pi_n$ |
|----|---------|----|---------|----|---------|----|---------|-----|---------|
| 2  | 205     | 4  | 203     | 6  | 411     | 8  | 208     | 10  | 270     |
| 12 | 404     | 14 | 245     | 16 | 200     | 18 | 417     | 20  | 269     |
| 22 | 226     | 24 | 404     | 26 | 240     | 28 | 248     | 30  | 536     |
| 32 | 196     | 34 | 215     | 36 | 404     | 38 | 213     | 40  | 267     |
| 42 | 489     | 44 | 227     | 46 | 201     | 48 | 409     | 50  | 270     |
| 52 | 221     | 54 | 410     | 56 | 240     | 58 | 212     | 60  | 535     |
| 62 | 206     | 64 | 201     | 66 | 458     | 68 | 209     | 70  | 318     |
| 72 | 401     | 74 | 206     | 76 | 220     | 78 | 428     | 80  | 272     |
| 82 | 205     | 84 | 493     | 86 | 207     | 88 | 217     | 90  | 531     |
| 92 | 218     | 94 | 208     | 96 | 400     | 98 | 232     | 100 | 260     |

**Table 6.** Values of  $\pi_n(10000)$  for even *n* through 100.

Once we fix n = 60 and N = 10000, for instance, we can construct a the analogous of Table 5, where in the first column we write the odd numbers  $1, 3, \ldots$ , 9999, and in the second the numbers  $1 + 60, 3 + 60, \ldots$ , 9999 + 60. Removing as above the multiples of 3 from each column, we see that in this case as well they appear at the same height, whereas for n = 62 they appear at different heights. Hence we are led to conjecture that for  $\pi_n(N)$  a relation like

$$\pi_n(N) \sim c' \cdot \frac{p_1 - 1}{p_1 - 2} \cdot \frac{p_2 - 1}{p_2 - 2} \cdots \frac{p_r - 1}{p_r - 2} \cdot \frac{N}{(\log N)^2}$$
(10)

should hold, where, as above,  $p_1, \ldots, p_r$  are the odd prime factors of n (which we consider as fixed), N is a very large number, and c' is the same constant as in (6). We can explain its name, at last; the problem had originally been stated thus: is it true that there exist infinitely many "twin primes," that is, primes having a difference of 2 like 11 and 13? We conclude by remarking that the smallest values in Table 6 occur when n is a power of 2, while the largest are those for n's having lots of small, odd prime factors, like 6, 30, ..., in good agreement with (10). This problem, just like Goldbach's, is still open, although some "approximate" results are known, but again they are too difficult to describe here.

#### VARIATIONES AD LIBITUM

We said that the twin-prime problem may be stated in a slightly different fashion, which suggests a new variation: if there are really infinitely many prime numbers p such that p + 2 is prime as well, is it true that there are infinitely many primes p such that both p + 2 and p + 4 are prime numbers? Looking up Table 1 we discover that this happens only once, when p = 3. It is not too difficult to understand where the problem lies: for any integer n, one among the numbers n, n + 2 and n + 4 is a multiple of 3. But modifying our demand and looking at the numbers p, p + 2 and p + 6, we discover that these are simultaneously prime in a large number of cases: actually, there are 55 prime numbers p < 10000 such that both p + 2 and p + 6 are again primes.

We are thus led to consider what some mathematicians call constellations of primes: given k distinct positive integers  $a_1, a_2, \ldots, a_k$ , we ask if there are infinitely many primes p such that  $p+a_1, \ldots, p+a_k$  are all simultaneously prime. Evidently, the twin primes correspond to the case k = 1 and  $a_1 = 2$ . In order to simplify the argument, we set  $a_0 = 0$  and write in compact form  $(a_0, \ldots, a_k)$  the set of k + 1integers  $a_0, a_1, \ldots, a_k$ , thus identifying the constellation itself. The problem we face immediately is how to tell the situation with k = 2,  $a_1 = 2$  and  $a_2 = 4$  (that is, the constellation (0, 2, 4)), apart from k = 2,  $a_1 = 2$  and  $a_2 = 6$  (i. e., the constellation (0, 2, 6)), which as we saw are radically different.

We can work as follows: we consider the primes p which do not exceed k + 1 (k+1) being the number of primes in the constellation), and for each of these primes we compute the remainders of  $a_0, a_1, \ldots, a_k$  when divided by p. If for any of these primes it happens that the remainders, in some order, are  $0, 1, \ldots, p-1$ , then the numbers  $p = p + a_0, p + a_1, \ldots, p + a_k$  can be simultaneously prime for at most one value of p, and we call the constellation  $(a_0, \ldots, a_k)$  non-admissible. On the other hand, if for every prime  $\leq k+1$  at least one remainder is missing, the constellation is called admissible.

| a  | b  | $\pi_{(0,a,b)}$         | a                                       | b                      | $\pi_{(0,a,b)}$                             | a                                       | b  | $\pi_{(0,a,b)}$          | a                                       | b  | $\pi_{(0,a,b)}$        |
|--|--|-------------------------|---|------------------------|---|---|--|--------------------------|---|--|------------------------|
| $\begin{array}{c}2\\2\\2\\4\end{array}$        | $     \begin{array}{r}       6 \\       18 \\       30 \\       10     \end{array} $ | $55 \\ 66 \\ 112 \\ 91$ | $\begin{array}{c}2\\2\\2\\4\end{array}$ |                        | $57 \\ 82 \\ 85 \\ 62$                      | $\begin{array}{c}2\\2\\2\\4\end{array}$ | $12 \\ 24 \\ 36 \\ 16$   | $92 \\ 59 \\ 65 \\ 57$   | $\begin{array}{c}2\\2\\4\\4\end{array}$ | $\begin{array}{c} 14\\ 26\\ 6\\ 18\end{array}$   | $73 \\ 68 \\ 57 \\ 71$ |
| $\begin{bmatrix} 6\\ 6\\ 8\\ 30 \end{bmatrix}$ | 8<br>18<br>14<br>60  |                         |   | $12 \\ 20 \\ 18 \\ 90$ | $     118 \\     106 \\     88 \\     221 $ |   | $     \begin{array}{r}       14 \\       22 \\       60 \\       120     \end{array} $ | $76 \\ 62 \\ 166 \\ 219$ |   | $     \begin{array}{r}       16 \\       12 \\       30 \\       120     \end{array} $ |                        |

**Table 7.** Computations for some admissible constellations of primes with N = 10000.

Going back to our previous example, in the case (0, 2, 4) we see at once that for p = 2 all the remainders are 0, while if p = 3 they are 0, 2, 1, respectively. When (0, 2, 6) and p = 2 all the remainders are 0, but for p = 3 they are 0, 2, 0, respectively.

The ideas explained above suggest the conjecture that for any given admissible constellation  $(a_0, \ldots, a_k)$ , there are infinitely many primes p such that  $p + a_1, \ldots, p + a_k$  are all primes, although the formula corresponding to (10) is rather complicated. But why should we just consider constellations of primes, which have, so to speak, a fixed distance? Actually, the same method can be used to study

the problem of the distribution of the primes p such that 2p + 1 is another prime, and we might even choose more complicated relations. This suggests that there are infinitely many problems of this type, but we stop here since our time has ran out.

#### Coda

These last few words are for those who insist on knowing the whole truth. The constant c in (1) is  $2e^{-\gamma}$ ,  $\gamma$  being the Euler-Mascheroni constant, defined by

$$\gamma = \lim_{n \to \infty} \left( \sum_{i=1}^{n} \frac{1}{i} - \log n \right) = 0.5772156649 \dots$$

The proof is far from easy. From a numerical point of view,  $N/(\log N - 1)$  is a better approximation to  $\pi(N)$  than  $N/\log N$ : This can be explained by the general theory. A still closer approximation is given by the *logarithmic integral* function, defined by

$$\operatorname{li}(N) = \int_2^N \frac{\mathrm{d}t}{\log t}.$$

With this function, the difference  $\pi(N) - \operatorname{li}(N)$  turns out to be much smaller than the one in the third column of Table 3. It is conjectured that there exists a positive constant A such that for large N we have

$$\left|\pi(N) - \operatorname{li}(N)\right| \le A\sqrt{N}\log N,$$

but the best estimates known today are extremely weaker.

It has been proved that both r(n) and  $\pi_n(N)$  do not exceed four times the expression on the right in (6) and (10) respectively. More generally, it has been proved that all quantities we dealt with do not exceed some fixed multiple of the expected quantity. Furthermore, it is now known that the even integers n such that r(n) is significantly smaller than (6) are rather rare. The precise statement is technical.

Hardy & Littlewood in their famous paper [3] give a history of conjecture (6), proving that similar formulae conjectured before (which, essentially, had a different constant in place of c', or a product over odd prime factors of n of a different shape) are certainly wrong. Their paper contains an accurate criticism of the "probabilistic" methods leading to these incorrect formulae, which use arguments resembling the one that leads to (1), as well as several tables. Furthermore, they describe a revolutionary new method to tackle this and similar problems, and almost all of the strongest results obtained since (including Vinogradov's) have been proved using their method. It is impossible even to vaguely hint at the ideas involved: we would need a deep knowledge of real and complex analysis.

The constants c' and c'' are respectively

$$c' = 2 \prod_{p \neq 2} \left( 1 - \frac{1}{(p-1)^2} \right)$$
 and  $c'' = \prod_{p \neq 2} \left( 1 + \frac{1}{(p-1)^3} \right)$ ,

where the products are over the odd primes. The number  $3^{3^{15}}$  has been reduced to  $e^{100000}$ , but this is still enormous (it has more than 43000 digits).

As far as the constellation of primes are concerned, let us call  $\rho(p)$  the number of *distinct* remainders of the numbers  $a_0, \ldots, a_k$  when divided by p. Rephrasing the above argument, it is not difficult to prove that the constellation  $(a_0, \ldots, a_k)$  is admissible if and only if  $\rho(p) < p$  for every prime number p. The expected number of prime numbers  $p \leq N$  such that also  $p + a_1, \ldots, p + a_k$  are prime numbers is given by the formula

$$\pi_{(a_0,a_1,\dots,a_k)}(N) \sim \prod_p \left(1 - \frac{1}{p}\right)^{-1-k} \left(1 - \frac{\rho(p)}{p}\right) \cdot \frac{N}{(\log N)^{k+1}},$$

which contains both (2) and (10) as special cases. For example, in the case k = 2 shown in Table 7 we have  $\rho(p) = 3$  for all prime numbers not dividing ab(b-a).

Note. This talk owes much to the first one in Lang's book [5], while the title is clearly inspired by the dialogue "Aria with Diverse Variations" in Hofstadter's book [4]. Finally, the data in Table 3 are taken from Tables 5.2 and 26 respectively of the books by Conway & Guy [1], and by Ribenboim [7], while all other data were computed by the author. For further information see also the references below, and the following web pages:

# http://www.inesca.pt/~tos/goldbach.html

Goldbach Conjecture numerical verification results by Tomás Oliveira e Silva.

http://www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html Verifying Goldbach's Conjecture up to  $4 \cdot 10^{14}$  by Jörg Richstein.

# http://purl.oclc.org/NET/TRN/

Enumeration of the twin primes and Brun's constant to  $10^{14}$  by Thomas Nicely.

I am indebted to Keith Matthews for these links. This text is available online at the address

http://www.math.unipr.it/~zaccagni/psfiles/Goldbach\_E.ps and in Italian at

http://www.math.unipr.it/~zaccagni/psfiles/Goldbach\_I.ps

### References

- [1] J. H. Conway & R. K. Guy, The Book of Numbers, Springer, Berlin, 1997.
- [2] G. H. Hardy, A Mathematician's Apology, Cambridge U. P., Cambridge, 1940.
- [3] G. H. Hardy & J. E. Littlewood, Some problems of "Partitio Numerorum"; III: On the expression of a number as a sum of primes, Acta Math. 44 (1923), 1–70.
- [4] D. R. Hofstadter, Gödel, Escher, Bach: an Eternal Golden Braid, Basic Books, New York, 1979.
- [5] S. Lang, The Beauty of Doing Mathematics, Springer, Berlin, 1985.
- [6] C. Pomerance, The Search for Prime Numbers, Scientific American 247 (Dec. 1982), 122–130.
- [7] P. Ribenboim, The New Book of Prime Number Records, Springer, Berlin, 1996.

Dipartimento di Matematica, Università degli Studi di Parma, via Massimo d'Azeglio 85/A, 43100 Parma, Italy.

*E-mail address*: zaccagni@prmat.math.unipr.it *URL*: http://www.math.unipr.it/~zaccagni/home.html