SOME RESULTS CONCERNING PYTHAGOREAN TRIPLETS

R. M. STERNHEIMER
Brookhaven National Laboratory, Upton, NY 11973
(Submitted December 1983; revised August 1984)

I. INTRODUCTION

In connection with the discussion in my earlier paper [1] entitled: "A Corollary to Iterated Exponentiation," in which I have presented a new conjecture concerning Fermat's Last Theorem, it occurred to me that it is of interest to make a systematic study of the sets of three integers x, y, z which satisfy the condition

$$x^2 + y^2 = z^2. \tag{1}$$

Such a triplet of integers (x, y, z) is commonly referred to as a "Pythagorean triplet," for which we shall also use the abbreviation P-triplet.

The actual motivation of the present work is to explore as thoroughly as possible the two cases, $n = 1$ and $n = 2$, for which the Diophantine equation of Fermat has solutions, namely,

$$x^n + y^n = z^n \qquad (n = 1, 2). \tag{2}$$

This interest is, in turn, derived from my earlier conjecture [1] that because $n = 1$ and $n = 2$ are the only two positive integers that are smaller than e, (2) holds only for $n = 1$ and $n = 2$ when x, y, and z are restricted to being positive integers. Most of the discussion in the present paper will be devoted to the case in which $n = 2$.

II. PYTHAGOREAN DECOMPOSITIONS

By using a computer program devised by M. Creutz, we were able to determine all Pythagoeran triplets for which $z \leqslant 300$. At this point, a distinction must must be made between P-triplets for which x, y, and z have no common divisor [the so-called "primitive solutions" of (1)] and P-triplets which are related to the primitive solutions by multiplication by a common integer factor k. So, if x_i, y_i, z_i are relatively prime and obey (1), it is obvious that the derived triplet (kx_i, ky_i, kz_i) will also satisfy (1).

The original computer program was therefore modified to print out only the primitive solutions, and was extended up to $z \leqslant 3000$. To anticipate one of my results, the number of primitive solutions in any interval of 100 in z is approximately constant and equal to ≈ 16. Thus there are 80 primitive solutions (PS) between $z = 1$ and 500, and 477 PS in the entire interval $1 \leqslant z \leqslant 3000$. We

---

The manuscript was authored under Contract No. DE-AC02-76CH00016 with the U.S. Department of Energy. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

will make the convention to denote by x the larger of the two numbers in the left-hand side of (1), i.e., $x > y$.

In Table 1, I have tabulated all primitive solutions for $1 \leqslant z \leqslant 500$. The triplets are presented in the order x_i, y_i, z_i. When a value of z_i is underlined, this indicates that it is not prime. The nonunderlined z_i values are primes which we will call "Pythagorean primes" or P-primes. In this work, and also for the region $501 \leqslant z \leqslant 2000$, the tables of primes and prime factors given in the *Handbook of Chemistry and Physics* [2] were essential.

When the z_i of the primitive solution is not a prime, I have underlined it, and the underlined number is usually followed by a subscript 1 or 2, which has the following significance. Already in the work for $z \leqslant 300$ (with all triplets listed), I have noticed the following rule: If $z_{p,i}$ and $z_{p,j}$ belong to two different primitive solutions, the product

$$z_{p,k} = z_{p,i} z_{p,j} \tag{3}$$

belongs to two new primitive solutions, namely,

$$(x_{1,k},\ y_{1,k},\ z_{p,k}) \quad \text{and} \quad (x_{2,k},\ y_{2,k},\ z_{p,k}). \tag{4}$$

These two new P decompositions are relatively prime and are also prime with respect to the expected decomposition obtained by taking the product of $z_{p,j}$ with the decomposition $(x_{p,i},\ y_{p,i},\ z_{p,i})$ and that obtained by taking the product of $z_{p,i}$ with the decomposition $(x_{p,j},\ y_{p,j},\ z_{p,j})$. Thus, there are ***four*** linearly independent P decompositions for the number $z_{p,k}$ of (3). To take an example, according to Table 1, the number 65 has the decompositions (56, 33, 65) and (63, 16, 65), and, in addition, (52, 39, 65) and (60, 25, 65) obtained from (4, 3, 5) and (12, 5, 13), respectively.

This rule is satisfied in all decompositions of products $z_{p,i} z_{p,j}$ provided that the prime factors of $z_{p,i}$ and $z_{p,j}$ are different. On the other hand, if $z_{p,i}$ and $z_{p,j}$ are merely powers of the same prime p_i, then there will be just *one* additional linearly independent Pythagorean decomposition for

$$z_{p,k} = p_i^{\alpha_i} p_i^{\alpha_{i'}} = p_i^{\alpha_i + \alpha_{i'}}. \tag{5}$$

As an example, the number $25 = 5^2$ has one additional P decomposition, namely, (24, 7, 25) besides that derived from (4, 3, 5), namely, (20, 15, 25). Similarly, the number $125 = 5^3$ has one new P decomposition, namely, (117, 44, 125) in addition to the two decompositions derived from the P decompositions for 5 and 25, namely, (100, 75, 125) and (120, 35, 125), respectively.

We may notice that the square $5^2 = 25$ has *two* P decompositions and the cube $5^3 = 125$ has *three* P decompositions. Thus, in general, a power $p_i^{\alpha_i}$ will have α_i Pythagorean decompositions, where p_i is a Pythagorean prime (such as 5, 13, 17, etc.). In Table 1, I have indicated the factors $z_{p,i}$ and $z_{p,j}$ which give rise to the new double primitive solution, when $z_{p,k}$ is a product of two different $z_{p,i}$ and $z_{p,j}$ which are relatively prime to each other. When a single power $p_i^{\alpha_i}$ is involved, this has also been noted, e.g., $13^2 = 169$ has the new P decomposition (120, 119, 169), in addition to the one expected from (12, 5, 13), namely, (156, 65, 169).

The total number of primitive solutions in the successive intervals of 100 in Table 1 are: 16 from 1 to 100, 16 from 101 to 200, 15 from 201 to 300, 16 from 301 to 400, and 17 from 401 to 500, giving a total of

$$\Sigma n_p = 16 + 16 + 15 + 16 + 17 = 80. \tag{6}$$

Table 1. Listing of the Pythagorean primitive decompositions for the integers in the range $1 \leqslant N \leqslant 500$. The values of z which are not prime numbers are underlined, and the subscripts 1 and 2 indicate the two new primitive solutions associated with such numbers. An exception occurs when the number N_i is a power of a single P-prime number, $p_i^{\alpha_i}$, in which case only one new primitive solution arises. For the numbers which are underlined (non-primes), the prime decomposition is indicated.

ν_i	x_i, y_i, z_i	ν_i	x_i, y_i, z_i	ν_i	x_i, y_i, z_i	ν_i	x_i, y_i, z_i
1	4,3,5	21	105,88,137	41	247,96,$\underline{265}_1 = 5 \times 53$	61	352,135,$\underline{377}_2 = 13 \times 29$
2	12,5,13	22	143,24,$\underline{145}_1 = 5 \times 29$	42	264,23,$\underline{265}_2 = 5 \times 53$	62	340,189,389
3	15,8,17	23	144,17,$\underline{145}_2 = 5 \times 29$	43	260,69,269	63	325,228,397
4	24,7,$\underline{25} = 5^2$	24	140,51,149	44	252,115,277	64	399,40,401
5	21,20,29	25	132,85,157	45	231,160,281	65	391,120,409
6	35,12,37	26	120,119,$\underline{169} = 13^2$	46	240,161,$\underline{289} = 17^2$	66	420,29,421
7	40,9,41	27	165,52,173	47	285,68,293	67	304,297,$\underline{425}_1 = 5 \times 85$
8	45,28,53	28	180,19,181	48	224,207,$\underline{305}_1 = 5 \times 61$	68	416,87,$\underline{425}_2 = 5 \times 85$
9	60,11,61	29	153,104,$\underline{185}_1 = 5 \times 37$	49	273,136,$\underline{305}_2 = 5 \times 61$	69	408,145,433
10	56,33,$\underline{65}_1 = 5 \times 13$	30	176,57,$\underline{185}_2 = 5 \times 37$	50	312,25,313	70	396,203,$\underline{445}_1 = 5 \times 89$
11	63,16,$\underline{65}_2 = 5 \times 13$	31	168,95,193	51	308,75,317	71	437,84,$\underline{445}_2 = 5 \times 89$
12	55,48,73	32	195,28,197	52	253,204,$\underline{325}_1 = 5 \times 65$	72	351,280,449
13	77,36,$\underline{85}_1 = 5 \times 17$	33	156,133,$\underline{205}_1 = 5 \times 41$	53	323,36,$\underline{325}_2 = 5 \times 65$	73	425,168,457
14	84,13,$\underline{85}_2 = 5 \times 17$	34	187,84,$\underline{205}_2 = 5 \times 41$	54	288,175,337	74	380,261,461
15	80,39,89	35	171,140,$\underline{221}_1 = 13 \times 17$	55	299,180,349	75	360,319,$\underline{481}_1 = 13 \times 37$
16	72,65,97	36	220,21,$\underline{221}_2 = 13 \times 17$	56	272,225,353	76	480,31,$\underline{481}_2 = 13 \times 37$
17	99,20,101	37	221,60,229	57	357,76,$\underline{365}_1 = 5 \times 73$	77	476,93,$\underline{485}_1 = 5 \times 97$
18	91,60,109	38	208,105,233	58	364,27,$\underline{365}_2 = 5 \times 73$	78	483,44,$\underline{485}_2 = 5 \times 97$
19	112,15,113	39	209,120,241	59	275,252,373	79	468,155,$\underline{493}_1 = 17 \times 29$
20	117,44,$\underline{125} = 5^3$	40	255,32,257	60	345,152,$\underline{377}_1 = 13 \times 29$	80	475,132,$\underline{493}_2 = 17 \times 29$

In Table 1 the numbers z_i that are not underlined are the primes for which a Pythagorean decomposition is possible. We will call them Pythagorean primes or P primes. The other primes (which are not P-decomposable) will be called non-Pythagorean primes or NP primes, e.g., 2, 3, 7, 11, 19, 23, 31, 43, and 47 are the NP primes below $N = 50$.

As mentioned above, all of the primitive solutions up to $N = 3000$ have been obtained with the computer program. (The total running time on the CDC-7600 Computer was less than 30 seconds.) However, I have limited the main analysis to the numbers $N \leqslant 2000$.

In the discussion below, I will derive a general formula for the number n_d of Pythagorean decompositions for an arbitrary integer.

In connection with the results of (3) and (4), it was noted and proved by M. Creutz [3] that when the triplets (x_1, y_1, z_1) and (x_2, y_2, z_2) are multiplied by each other, the additional primitive solutions mentioned in (4) have the following form:

$$X_1 = x_1y_2 + y_1x_2, \qquad Y_1 = |x_1x_2 - y_1y_2|; \tag{7}$$

$$X_2 = |x_1y_2 - y_1x_2|, \qquad Y_2 = x_1x_2 + y_1y_2. \tag{8}$$

Here we have omitted the subscript p for simplicity of notation. To prove the validity of (7) and (8), we note that

$$\begin{aligned} X_1^2 + Y_1^2 &= x_1^2y_2^2 + y_1^2x_2^2 + 2x_1x_2y_1y_2 + x_1^2x_2^2 + y_1^2y_2^2 - 2x_1x_2y_1y_2 \\ &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) = z_1^2z_2^2 = (z_1z_2)^2 = Z^2, \end{aligned} \tag{9}$$

thus verifying that $Z \equiv z_1z_2$ has the P decomposition (X_1, Y_1, Z). A similar equation is obtained by calculating $X_2^2 + Y_2^2 = z_1^2z_2^2 = Z^2$, thus confirming the new P triplet (X_2, Y_2, Z).

As an example, for $Z = 65$, we have $x_1 = 4$, $y_1 = 3$, $z_1 = 5$ and $x_2 = 12$, $y_2 = 5$, $z_2 = 13$, which gives $X_1 = 56$, $Y_1 = 33$, leading to the triplet (56, 33, 65) listed in Table 1. Furthermore, equations (8) give $X_2 = 16$, $Y_2 = 63$, which is equivalent to the second triplet, (63, 16, 65), also listed in Table 1.

It is also obvious from (7) and (8) that if $x_1 = x_2$, $y_1 = y_2$, i.e., $z_{p,k} = z_{p,i}^2$ in the notation of (3), then

$$X_1 = 2x_1y_1, \qquad Y_1 = |x_1^2 - y_1^2|,$$

which gives rise to only one new P triplet, since for the other solution, $X_2 = 0$, $Y_2 = x_1^2 + y_1^2 = z_{p,i}^2 = z_{p,k}$. For the case $x_1 = x_2 = 4$, $y_1 = y_2 = 3$, we have

$$X_1 = 2x_1y_1 = 24, \qquad Y_1 = 4^2 - 3^2 = 7,$$

giving the one new triplet, (24, 7, 25).

In Table 2, all the Pythagorean primes from $N = 1$ to $N = 2000$ are listed. Successive intervals of 100 are separated by semicolons.

Table 2. List of all Pythagorean primes for $1 \leqslant N \leqslant 2000$, i.e., primes which satisfy (1) where x and y are positive integers. Those primes which are underlined belong to a set of twin primes, i.e., primes p_i and p_j such that $|p_i - p_j| = 2$. For each set of twin primes p_i, p_j, *one and only one* is a P-prime. The primes in successive intervals of 100 are separated by a semicolon.

$\underline{5}$, $\underline{13}$, $\underline{17}$, $\underline{29}$, 37, $\underline{41}$, 53, $\underline{61}$, $\underline{73}$, 89, 97; $\underline{101}$, $\underline{109}$, $\underline{113}$, $\underline{137}$, $\underline{149}$, 157, 173, $\underline{181}$, $\underline{193}$, $\underline{197}$; $\underline{229}$, 233, $\underline{241}$, 257, $\underline{269}$, 277, $\underline{281}$, 293; $\underline{313}$, 317, 337, $\underline{349}$, 353, 373, 389, 397; 401, 409, $\underline{421}$, $\underline{433}$, 449, 457, $\underline{461}$;

509, $\underline{521}$, 541, 557, $\underline{569}$, 577, 593; $\underline{601}$, 613, $\underline{617}$, $\underline{641}$, 653, $\underline{661}$, 673, 677; 701, 709, 733, 757, 761, 769, 773, 797; $\underline{809}$, $\underline{821}$, $\underline{829}$, 853, $\underline{857}$, 877, $\underline{881}$; 929, 937, 941, 953, 977, 997;

1009, 1013, $\underline{1021}$, $\underline{1033}$, $\underline{1049}$, $\underline{1061}$, 1069, $\underline{1093}$, 1097; 1109, 1117, 1129, $\underline{1153}$, 1181, 1193; 1201, 1213, 1217, $\underline{1229}$, 1237, 1249, $\underline{1277}$, $\underline{1289}$, 1297; $\underline{1301}$, $\underline{1321}$, 1361, 1373, 1381; 1409, $\underline{1429}$, 1433, $\underline{1453}$, $\underline{1481}$, $\underline{1489}$, 1493;

1549, 1553, 1597; 1601, $\underline{1609}$, 1613, $\underline{1621}$, 1637, 1657, $\underline{1669}$, 1693, $\underline{1697}$; 1709, $\underline{1721}$, 1733, 1741, 1753, 1777, $\underline{1789}$; 1801, 1861, $\underline{1873}$, $\underline{1877}$, 1889; 1901, 1913, $\underline{1933}$, $\underline{1949}$, 1973, 1993, $\underline{1997}$.

III. CONNECTIONS WITH THE TWIN PRIMES

Note that many of the Pythagorean primes in Table 2 are underlined. These are the primes which belong to a set of twin primes, i.e., primes p_i and p_j, which are separated by 2, i.e., such that $|p_i - p_j| = 2$. As an example, 17 is part of the twin prime set (17, 19); similarly, 41 is part of the twin prime set (41, 43). By a survey of all twin primes $N_i < 2000$, it was found that in all cases, for each set of twin primes, *one* of them is a P-prime (P-decomposable), while the other is a non-P-prime. This result can be shown to follow naturally from a theorem due to Fermat, according to which all primes $p_i \equiv 1 \pmod 4$ are P-primes, while all primes $q_j \equiv 3 \pmod 4$ are non-P-primes. Actually, what Fermat proved is that all primes $p \equiv 1 \pmod 4$ can be written in the form $p_i = a^2 + b^2$, and this is, according to an elementary theorem due to Diophantos, the necessary and sufficient condition for $p_i^2 = x_i^2 + y_i^2$ to be satisfied [4]. Here, $x_i = a^2 - b^2$ and $y_i = 2ab$, and the result follows naturally from the following equation:

$$p_i^2 \equiv (a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2 = a^4 + b^4 - 2a^2b^2 + 4a^2b^2. \quad (10)$$

Obviously, $p_i \equiv 1 \pmod 4$ means that p_i can be written as $4n + 1$. Then, if p_j is either 2 units larger or smaller than p_i, it is given by $4n' + 3$, and $p_j \equiv 3 \pmod 4$.

Of the 147 P-primes listed in Table 2, 60 are twin primes. The remaining $87 = 147 - 60$ P-primes are "isolated" primes, i.e., they do not belong to a twin set. If we consider successive intervals of 500, we find a total of 44 P-primes between 1 and 500; 36 P-primes between 501 and 1000; 36 P-primes between 1001 and 1500; and 31 P-primes between 1501 and 2000. Incidentally, there is a total of 302 prime numbers between 1 and 2000, so that the overall fraction of P-primes is $147/302 = 0.487 \approx 49\%$, close to 50%, as would be expected from Fermat's Theorem concerning $p_i \equiv 1 \pmod 4$.

The approximate equality of the number n_P of P-primes and n_{NP} of non-P-primes indicates that the Pythagorean primes have an intimate connection with the entire system of positive integers and, in addition, this connection indicates that we may expect that very approximately on the order of one-half of all integers are P-decomposable in at least one way ($n_d \geqslant 1$), while the other half is not Pythagorean-decomposable. These integers will be called P-numbers and non-P or NP-numbers, respectively. Numerical results for the fractions of P-numbers in three different intervals for $N \leqslant 2000$ will be given below. Obviously, for an integer N_i to be P-decomposable in at least one way, it is necessary and sufficient that N_i can be written as

$$N_i = p_i J, \quad (11)$$

where p_i is an arbitrary P-prime and J is a positive integer.

IV. THE DECOMPOSITION FORMULA FOR n_d

The most general integer can be written as

$$\begin{aligned} N_k &= p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots \\ &= \prod_{i=1}^{n_a} p_i^{\alpha_i} \prod_{j=1}^{n_b} q_j^{\beta_j} \equiv A_k B_k, \end{aligned} \quad (12)$$

where the p_i and P-primes are the α_i are the corresponding powers, and similarly, the q_j are the non-P-primes and the β_j are the corresponding powers. In the second row of (12), n_a denotes the number of different P-primes in N_k and n_b denotes the number of different non-P-primes in the prime decomposition of N_k; finally, A_k and B_k represent the two products involving $p_i^{\alpha_i}$ and $q_j^{\beta_j}$, respectively.

Theorem: The total number of Pythagorean decompositions n_d corresponding to N_k of (12) is given by:

$$n_d = \sum_{i=1}^{n_a} \alpha_i + 2\sum_{i<j}^{n_a} \alpha_i\alpha_j + 4\sum_{i<j<k}^{n_a} \alpha_i\alpha_j\alpha_k + 8\sum_{i<j<k<\ell}^{n_a} \alpha_i\alpha_j\alpha_k\alpha_\ell + \cdots$$
$$+ 2^{n_a - 1}\alpha_1\alpha_2\alpha_3 \cdots \alpha_{n_a}. \tag{13}$$

Here, the first sum extends over all α_i, the second sum extends over all possible products of pairs of α_i, the third sum extends over all possible products $\alpha_i\alpha_j\alpha_k$, where three α_i's are involved, etc. As an example, for the number 65 of Table 1, we have $65 = 5^1 \times 13^1$, so that $\alpha_1 = \alpha_2 = 1$, and (13) gives

$$n_d = 1 + 1 + 2(1)(1) = 4. \tag{14}$$

Similarly, for $N_k = 325 = 5^2 \times 13$, with $\alpha_1 = 2$, $\alpha_2 = 1$, we find

$$n_d = 2 + 1 + 2(2)(1) = 7. \tag{15}$$

In order to illustrate equation (13), we consider the number $1625 = 5^3 \times 13$. First, we will count the number of ways in which 1625 can be written without mixing up the 5's and the 13 in the decomposition. We use the notation $(p_i^{\alpha_i})$ *with parentheses* to indicate the decomposition of $p_i^{\alpha_i}$. Now, there are clearly $\alpha_1 = 3$ decompositions pertaining to the powers of 5 alone; they are (5^3), (5^2), and (5), where (5^3) stands for (117, 44, 125) (see Table 1), (5^2) stands for (24, 7, 25), and $(5) \equiv (4, 3, 5)$. Thus, three decompositions of 1625 can be written as $(5^3) \times 13$, $(5^2) \times 65$, and $(5) \times 325$, where the multiplication applies to the three integers x_i, y_i, and z_i listed above for each case. In addition, there is the decomposition $(13) \times 125$, where $(13) \equiv (12, 5, 13)$. These four decompositions correspond to $\alpha_1 + \alpha_2 = 3 + 1 = 4$. Next, we consider the cases in which a product of a power of 5 times 13 appears inside the parentheses. These cases are $(5^3 \times 13)$, $(5^2 \times 13) \times 5$, and $(5 \times 13) \times 25$. According to the rule of equations (3) and (4) for $z_{p,i}$ and $z_{p,j}$ having different prime factors, there are two new primitive solutions for each such case, e.g.,

$$(325) \times 5 = (253,\ 204,\ 325) \times 5 \quad \text{and} \quad (323,\ 36,\ 325) \times 5,$$

where $325 = 5^2 \times 13$ (see Table 1). There are $\alpha_1\alpha_2 = (3)(1) = 3$ such cases, and they contribute $2\alpha_1\alpha_2 = 6$ decompositions. Thus, the total

$$n_d = 4 + 6 = 10 = \alpha_1 + \alpha_2 + 2\alpha_1\alpha_2$$

as given by (13). This illustration can be generalized to give the various terms of (13) and to provide the proof by induction. In each case, the factor 2, 4, 8 in the second, third, and fourth terms, respectively, of (13) corresponds to the doubling of the primitive solutions described above, where more than one prime is involved. For another example of (13), consider the number

$$N = (5^2)(13)(17) = 5525. \tag{16}$$

It has 22 decompositions of the type

$$5525^2 = x^2 + y^2, \tag{17}$$

since $\alpha_1 = 2$, $\alpha_2 = \alpha_3 = 1$, and, from (13),

$$n_d = (2 + 1 + 1) + 2(2 + 2 + 1) + 4(2) = 4 + 10 + 8 = 22. \tag{18}$$

Using (13), we have obtained the number of decompositions n_d for three sets of 51 integers, namely those extending from $N = 50$ to $N = 100$, those extending from $N = 950$ to 1000, and those extending from $N = 1950$ to 2000. The results are presented in Table 3, which lists n_P, the number of Pythagorean numbers (for which $n_d \geqslant 1$), n_{NP}, the number of non-P-prime numbers (for which $n_d = 0$), the total $\Sigma n_d/n_P$ and, finally, the ratio of n_P to the total number 51. It is seen that while n_P/all $N = 0.49$ for the first set (50-100), for the other two sets, n_P/all N is constant at a value of ≈ 0.61. However, the total number of decompositions, Σn_d, increases from 34 (for $N = 50$-100) to 58 (for $N = 1950$-2000), and the average $\Sigma n_d/n_P$ also increases from 1.36 to 1.87 per Pythagorean number. It thus appears that the fraction of all numbers that are P-decomposable reaches a plateau value of ~0.61 for large N, at least in the range of $N = 1000$-2000.

Table 3. For three ranges of N: 50-100, 950-1000, 1950-2000, I have tabulated the total number of Pythagorean numbers n_P, the total number of non-P-numbers n_{NP}, the total number of P-decompositions Σn_d, and the ratios $\Sigma n_d/n_P$ and $n_P/51$, where 51 is the total number of integers in each range.

N range	n_P	n_{NP}	Σn_d	$\Sigma n\ /n_P$	$n_P/51$
50-100	25	26	34	1.36	0.490
950-1000	31	20	53	1.71	0.608
1950-2000	31	20	58	1.87	0.608

We note that for very large numbers N_k (say $N_k \sim 10^{20}$) which have many factors $p_i^{\alpha_i}$ [see (12)], the use of (13) for n_d becomes cumbersome. For this reason, I have derived a simpler formula for n_d which can be readily evaluated for large N_k. This formula is presented in Appendix A of this paper [see equation (A25)].

As a final remark regarding (12), we note that we may define a *Pythagorean congruence* (*P-congruence*) as follows: Referring to (12), it is seen that the product A_k determines completely the type and the number n_d of P-decompositions as given by (13). Therefore, we can write

$$N_k \equiv A_k(P), \tag{19}$$

and all numbers N_{k_i} with the same product A_k (but different values of B_k) will have the same P-decompositions, except for a different cofactor B_{k_i}. The congruence (19) holds under the operation of multiplication, i.e., if we have two integers N_k and $N_{k'}$ with different values of A_k and B_k, then the product $N_k N_{k'}$ can be written as follows,

$$N_k N_{k'} = (A_k A_{k'}) B_k B_{k'}, \tag{20}$$

and the P-decompositions of $N_k N_{k'}$ will be uniquely determined by the product $A_k A_{k'}$, except for the cofactor $B_k B_{k'}$ which multiplies all decompositions (x_i, y_i, z_i). Therefore, $N_k N_{k'}$ is P-congruent to $A_k A_{k'}$:

$$N_k N_{k'} \equiv A_k A_{k'} (P). \tag{21}$$

As examples of Pythagorean congruence, we mention three cases: $84 \equiv 1(P)$, since 84 is not P-decomposable, and $84 = 2^2 \times 3 \times 7$ is a product of non-P-primes only; similarly, $6630 \equiv 1105(P) = 5 \times 13 \times 17(P)$, where 5, 13, and 17 are P-primes. Finally, $929 \equiv 929(P)$, since 929 is a P-prime.

V. CONCLUDING COMMENTS

Of particular interest among the P-triplets, are those for which $x = z - 1$ (see Table 1 for examples). In this case, it is easily seen that y must be an odd integer, which can therefore be written as

$$y = 2\nu + 1, \tag{22}$$

where ν is an arbitrary positive integer. We can now write:

$$\begin{aligned} x^2 + y^2 &= (z - 1)^2 + (2\nu + 1)^2 \\ &= z^2 - 2z + 1 + 4\nu^2 + 4\nu + 1 = z^2. \end{aligned} \tag{23}$$

Upon subtracting z^2 from the last two expressions in (23), and dividing by 2, we obtain

$$-z + 1 + 2\nu^2 + 2\nu = 0, \tag{24}$$

which gives

$$z = 2\nu(\nu + 1) + 1, \tag{25}$$

and, therefore, $x = z - 1 = 2\nu(\nu + 1)$, and a suitable (x, y, z) triplet exists for any choice of ν (> 0), i.e., for any odd integer except $y = 1$. [In the latter case, $x = 0$ and equation (1) is trivially satisfied.] Thus, the ensemble of numbers y includes all odd numbers $\geqslant 3$, and hence, obviously, all prime numbers except $y = 1$ and $y = 2$. An example of such a triplet (from Table 1) is (40, 9, 41), in which case $\nu = 4$, $z = (2)(4)(5) + 1 = 41$, $x = z - 1 = 40$. Thus, the set of y's for $x = z - 1$ contains all prime numbers larger than e. We see again the privileged position of the numbers $y = 1$ and $y = 2$ (cf. [1]) that are *not* included among the y_i's in the P-triplets, in complete similarity to the exponents $n = 1$ and $n = 2$ for which Fermat's Last Theorem is satisfied [i.e., equation (2)]. I should also note that I can amplify the statement made in [1] concerning the Diophantine equation

$$F(x, y) \equiv x^y - y^x = 0. \tag{26}$$

In [1], I stated that the only nontrivial solution of (26) for integer x and y is $x = 2$, $y = 4$. However, if we do not demand that y be an integer, but if we consider a limiting process for x and y, then another nontrivial solution exists for $x \to 1$, i.e., the limit of y as x approaches 1 from above ($x = 1 + \varepsilon$, $\varepsilon \to 0$) is $y = \infty$. Specifically, I have calculated the values of y determined by (26) for $x = 1.1$, $x = 1.01$, and $x = 1.001$, with the following results:

$$y(x = 1.1) = 43.56, \quad x^y = y^x = 63.53; \tag{27}$$

$$y(x = 1.01) = 658.81, \quad x^y = y^x = 703.0; \tag{28}$$

$$y(x = 1.001) = 9133.4, \quad x^y = y^x = 9217.05. \tag{29}$$

It is clear from these results that the limit of y as x approaches 1 from above is infinity, i.e.,

$$\lim_{x \to 1} y = \infty. \tag{30}$$

Thus, equation (26) is essentially satisfied for both $x = 1$ and $x = 2$, analogous to Fermat's Last Theorem, which is satisfied only for $n = 1$ and $n = 2$.

Parenthetically, I may note that for $x = 0$, (26) *cannot* be satisfied for any positive y, since

$$F(0, y) = 0^y - y^0 = -1 \tag{31}$$

for all y. Analogous to this result, Fermat's Last Theorem, equation (2), also has no solution for $n = 0$, since the left-hand side $x^0 + y^0 = 2$, whereas the right-hand side $z^0 = 1$.

In summary, I have shown that the Pythagorean decompositions of z according to (1) provide a new classification of the number system into: (a) P-numbers $N_{P,i}$ [see (11)] that are P-decomposable in at least one way ($n_d \geqslant 1$); (b) non-P-numbers $N_{NP,i}$ that cannot be decomposed according to (11) and (12), i.e., for which all of the α_i exponents of (12) are zero. The system of integers is approximately evenly divided between P-numbers and non-P-numbers in the range $50 < N_i < 100$, although for large N_i in the range of ~ 900-2000, the P-numbers predominate slightly, to the extent of 60% of all integers.

The set of P-primes p_i and products or powers of the p_i, i.e., $p_i p_j$ or $p_i^{\alpha_i}$ give rise to the primitive solutions (x_i, y_i, z_i) for which (1) is satisfied. As described by equations (3) and (4), and (7)-(9), for each pair of primitive solutions ($x_{p,i}, y_{p,i}, z_{p,i}$) and ($x_{p,j}, y_{p,j}, z_{p,j}$), the product $z_{p,k} \equiv z_{p,i} z_{p,j}$ contributes *two* new primitive solutions (provided the prime factors of $z_{p,i}$ and $z_{p,j}$ are different).

The total number of Pythagorean decompositions for a given P-number $N_{p,i}$ increases rapidly with the number n_a of p_i primes [see equation (12)] and with the powers α_i associated with each p_i. I have obtained a general expression for n_d in terms of the α_i and n_a [see equation (13)]. Furthermore, (13) has been proven by induction in the discussion which follows (15). An equivalent formula for (13) will be derived in Appendix A. The results given in Appendix A provide the means for a rapid evaluation of n_d when the integer N_k [see (12)] is large, so that there is a large number n_a of P-primes p_i in the prime decomposition of N_k.

Concerning the primitive solutions, I have noticed empirically from the decomposition tables that the density of primitive solutions, i.e., their frequency, is almost constant in going from N ~ 0-100 to $N = 3000$. Thus, generally, for each additional interval of 100 in N, we obtain sixteen additional primitive solutions. As an example, the total number of primitive solutions included in Table 1 for $1 \leqslant N \leqslant 500$ is exactly $80 = 5 \times 16$ [equation (6)]. For $1 \leqslant N \leqslant 1000$, the total number of primitive solutions is 158, and for the entire sample with $1 \leqslant N \leqslant 3000$, the total number of primitive solutions is 477, almost equal to the expected number $16 \times 30 = 480$. At present, I have no explanation for the remarkable constancy of the density (frequency) of primitive solutions as a function of N.

As a final comment, it is not clear at present to what extent the results reported in this paper for the case $n = 2$ will help in the ultimate proof of Fermat's Last Theorem. Nevertheless, my previous suggestion about the values of $n > e$ [1] and its amplification as presented in this paper [equations (26)-(30)] may offer a guideline to a complete proof. In any case, the interesting discovery of the doubling of the primitive solutions [equations (3), (4)] and the derivation of the resulting decomposition formula [equation (13)] will perhaps shed new light on the nature of our integer number systme. Additional results on the evaluation of (13) and on the case $n = 1$ in (2) will be given in Appendix A and Appendix B, respectively.

APPENDIX A

EVALUATION OF EQUATION (13)

In connection with (13) for the number n_d of Pythagorean decompositions of an arbitrary integer N_k as given by (12), it seems of interest to tabulate typical values of n_d for integers with relatively low values of the exponents α_i. Table 4 shows a systematic listing of the numbers of decompositions n_d for all cases for which $\Sigma\alpha_i \leqslant 6$. Obviously, the table can be subdivided into subtables pertaining to those cases for which any given number of P-primes p_i are involved. Thus, the top part of the table pertains to $\alpha_1 > 0$, $\alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 = 0$ (i.e., the case $n_a = 1$). The next panel of the table pertains to cases for which two Pythagorean primes occur ($n_a = 2$) in the decomposition of N_k [equation (12)], and these will be denoted α_1 and α_2, i.e., $\alpha_3, \ldots, \alpha_6 = 0$. In this panel I have arbitrarily assumed that $\alpha_1 \geqslant \alpha_2$ and, of course, all cases are subject to the limitation that $\alpha_1 + \alpha_2 \leqslant 6$. The third, fourth, fifth, and sixth panels of the table are similarly constructed.

The next-to-the-last column of the table lists the values of n_d, while the last column lists the values of $N_{\min}$, the smallest integer N_k for which the particular decomposition as given in the first six columns exists. In addition, the prime decomposition of $N_{\min}$ is listed after the value of $N_{\min}$. Obviously, in order to obtain the lowest N_k value consistent with the set $\{\alpha_i\}$, we must assume that all of the β_j in (12) are zero, i.e., $B_k = 1$. Furthermore, it is necessary to choose for the P-prime with the largest α_i the value 5, then the value 13 for the P-prime with the next largest α_i, and so forth.

Several results are apparent from a study of Table 4 and of (13):

1. Consider equation (13) and a particular α_i, say $\alpha_{i,0}$. Because the particular $\alpha_{i,0}$ appears linearly in all of the terms of (13), n_d depends linearly on $\alpha_{i,0}$, and in particular, for equally spaced values of α_i, e.g.,

$$\alpha_{i,0},\quad \alpha_{i,0} + 1, \quad \text{and} \quad \alpha_{i,0},\quad \alpha_{i,0} - 1,$$

we find

$$n_d(\alpha_{i,0} + 1) - n_d(\alpha_{i,0}) = n_d(\alpha_{i,0}) - n_d(\alpha_{i,0} - 1), \tag{A1}$$

Table 4. Listing of special cases of (13) for the number of Pythagorean decompositions as a function of the α_i's and n_a. I have tabulated all cases for which $\sum_{i=1}^{6}\alpha_i \leqslant 6$. The seventh column of the table gives the values of $n_d\{\alpha_i\}$ as obtained from (13). The last column gives the smallest number $N_{\min}$ for which the listed exponents $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$, and α_6 are realized. The prime decomposition of $N_{\min}$ is listed for each $N_{\min}$. The blank spaces in the columns for α_i correspond to values of $\alpha_i = 0$.

α_1	α_2	α_3	α_4	α_5	α_6	$n_d\{\alpha_i\}$	$N_{\min}$
1						1	5
2						2	25
3						3	125
4						4	625
5						5	3125
6						6	15,625
1	1					4	65 = 5 × 13
2	1					7	325 = 25 × 13
2	2					12	4225 = 25 × 169
3	1					10	1625 = 125 × 13
3	2					17	21,125 = 125 × 169
3	3					24	274,625 = 125 × 2197
4	1					13	8125 = 625 × 13
4	2					22	105,625 = 625 × 169
5	1					16	40,625 = 3125 × 13
1	1	1				13	1105 = 5 × 13 × 17
2	1	1				22	5525 = 25 × 13 × 17
2	2	1				37	71,825 = 25 × 169 × 17
2	2	2				62	1,221,025 = 25 × 169 × 289
3	1	1				31	27,625 = 125 × 13 × 17
3	2	1				52	359,125 = 125 × 169 × 17
4	1	1				40	138,125 = 625 × 13 × 17
1	1	1	1			40	32,045 = 5 × 13 × 17 × 29
2	1	1	1			67	160,225 = 25 × 13 × 17 × 29
2	2	1	1			112	2,082,925 = 25 × 169 × 17 × 29
3	1	1	1			94	801,125 = 125 × 13 × 17 × 29
1	1	1	1	1		121	1,185,665 = 5 × 13 × 17 × 29 × 37
2	1	1	1	1		202	5,928,325 = 25 × 13 × 17 × 29 × 37
1	1	1	1	1	1	364	48,612,265 = 5 × 13 × 17 × 29 × 37 × 41

and, indeed, for any two values of α_i which differ by 1, the differences

$$n_d(\alpha_i) - n_d(\alpha_i - 1)$$

will be the same. Of course, in applying (A1), one must keep all of the other

α_j values constant. Equation (A1) can be used to check the correctness of the entries of Table 4. As an example,

$$n_d(2,\ 2) - n_d(2,\ 1) = 12 - 7 = n_d(2,\ 1) - n_d(2,\ 0)$$
$$= 7 - 2 = 5. \tag{A2}$$

Similarly,

$$n_d(3,\ 1,\ 1,\ 1) - n_d(2,\ 1,\ 1,\ 1) = 94 - 67$$
$$= n_d(2,\ 1,\ 1,\ 1) - n_d(1,\ 1,\ 1,\ 1)$$
$$= 67 - 40 = 27. \tag{A3}$$

Here I have used the notation $n_d(\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4)$ and $n_d(\alpha_1,\ \alpha_2)$ for the corresponding entries in Table 4.

2. Next, we consider the cases where all of the α_i are 1, e.g.,

$$n_d(1,\ 1,\ 1) = 13, \quad n_d(1,\ 1,\ 1,\ 1,\ 1) = 121, \text{ etc.}$$

For simplicity, $n_d(1,\ 1,\ \ldots,\ 1)$ with ξ 1's will be simply denoted by $n_d[1_\xi]$. We note that the $n_d[1_\xi]$ satisfy the recursion relations

$$n_d[1_{\xi+1}] = 3n_d[1_\xi] + 1. \tag{A4}$$

As an example, $n_d[1_6] = 364$; $n_d[1_5] = 121$, and we have

$$n_d[1_6] = 3n_d[1_5] + 1 = 364 = (3 \times 121) + 1. \tag{A5}$$

Equation (A4) together with the additional condition $n_d[1_1] = 1$ can be used to derive all of the $n_d[1_\xi]$ values of Table 4, namely, 4 $\{= n_d[1_2]\}$, 13, 40, 121, and 364.

I also note that the difference $n_d[1_\xi + 1] - n_c[1_\xi]$ obeys the equation

$$n_d[1_{\xi+1}] - n_d[1_\xi] = 3^\xi. \tag{A6}$$

As an example: $n_d[1_6] - n_d[1_5] = 364 - 121 = 243 = 3^5$.

Therefore, I find:

$$n_d[1_\xi] = \sum_{\eta=0}^{\xi-1} 3^\eta. \tag{A7}$$

3. A similar relation is obtained when we calculate differences between values of $n_d(2,\ 1,\ \ldots,\ 1)$. For simplicity, we write $n_d(2,\ 1,\ \ldots,\ 1)$ with γ 1's as $n_d[2,\ 1_\gamma]$. We note that

$$n_d(2,\ 1,\ 1) - n_d(2,\ 1) = 22 - 7 = 15, \tag{A8}$$

$$n_d(2,\ 1,\ 1,\ 1) - n_d(2,\ 1,\ 1) = 67 - 22 = 45, \tag{A9}$$

and also

$$n_d(2,\ 1) - n_d(2) = 7 - 2 = 5. \tag{A10}$$

These results suggest the relation:

$$n_d[2,\ 1_\gamma] - n_d[2,\ 1_{\gamma-1}] = 5 \times 3^{\gamma-1}. \tag{A11}$$

In fact, for $\gamma = 4$, we find

$$n_d[2,\ 1_4] - n_d[2,\ 1_3] = 5 \times 3^3 = 135 = 202 - 67. \tag{A12}$$

Moreover, I have found that

$$n_d[2,\ 1_\gamma] - n_d[1,\ 1_\gamma] = 3^\gamma, \tag{A13}$$

and, therefore, in view of (A7), and generalizing to $n_d[k,\ 1_\gamma]$,

$$n_d[k,\ 1_\gamma] = \sum_{\eta=0}^{\gamma} 3^\eta + (k - 1)3^\gamma, \tag{A14}$$

where k is an arbitrary positive integer.

Finally, as a generalization of (A7), I have found that the $n_d[k_\xi]$ for an arbitrary number ξ of integers k, e.g., $n_d[2,\ 2,\ 2] = n_d[2_3]$, are given by the following expression:

$$n_d[k_\xi] = k\sum_{\eta=0}^{\xi-1}(2k + 1)^\eta. \tag{A15}$$

As an example: $n_d[2,\ 2,\ 2] = n_d[2_3]$ is given by

$$n_d[2_3] = 2\sum_{\eta=0}^{2}(5)^\eta = 2(1 + 5 + 5^2) = 62, \tag{A16}$$

in agreement with the corresponding entry in Table 4. The generalized recursion relation which pertains to (A15) is

$$n_d[k_{\xi+1}] = (2k + 1)n_d[k_\xi] + k. \tag{A17}$$

A more general formula which is based on (A14) and (A15) gives

$$n_d[k,\ k'_\gamma] = k'\sum_{\eta=0}^{\gamma-1}(2k' + 1)^\eta + k(2k' + 1)^\gamma. \tag{A18}$$

(A18) gives n_d for γ powers α_i equal to k' and a single power α_j equal to k.

In an attempt to simplify the evaluation of (A15) and (A18), we note that the sum in (A18) can be written as follows:

$$\sum_{\eta=0}^{\gamma-1}(2k'+1)^\eta = (2k'+1)^{\gamma-1}\left[1 + \frac{1}{2k'+1} + \frac{1}{(2k'+1)^2} + \cdots + \frac{1}{(2k'+1)^{\gamma-1}}\right]. \tag{A19}$$

The expression in square brackets is the major part of the infinite series

$$\frac{1}{1 - 1/(2k'+1)} = 1 + \frac{1}{2k'+1} + \frac{1}{(2k'+1)^2} + \cdots\ . \tag{A20}$$

The left-hand side of (A20) can be rewritten as follows:

$$\frac{1}{1 - 1/(2k'+1)} = \frac{2k'+1}{2k'}. \tag{A21}$$

Therefore, the sum of (A19) is approximately given by

$$\sum_{\eta=0}^{\gamma-1}(2k'+1)^{\eta} \cong (2k'+1)^{\gamma}/2k'. \tag{A22}$$

The part of the expression (A20) which is not included in the sum of (A19) can be shown to result in a negative contribution to $n_d[k, k_j']$, which is given by

$$\Delta n_d = -k'\left[\frac{1}{1-1/(2k'+1)} - 1\right] = -k'\left(\frac{2k'+1}{2k'} - 1\right) = -\frac{1}{2}. \tag{A23}$$

Upon inserting these results in (A18), we obtain:

$$\begin{aligned} n_d[k, k_\gamma'] &= k'(2k'+1)^{\gamma}/2k' - \frac{1}{2} + k(2k'+1)^{\gamma} \\ &= \frac{1}{2}(2k'+1)^{\gamma}(2k+1) - \frac{1}{2}. \end{aligned} \tag{A24}$$

Equation (A24) suggests a natural generalization to an arbitrary number of different k_i's, since each k_i gives rise to a power $(2k_i + 1)^{\gamma_i}$ in the expression for n_d. We therefore obtain:

$$n_d(\{\alpha_i\}) = \frac{1}{2}\prod_{i=1}^{i_{\max}}(2k + 1)^{\gamma_i} - \frac{1}{2}. \tag{A25}$$

This equation permits a rapid evaluation of $n_d(\{\alpha_i\})$ and is completely equivalent to the much more complicated equation (13) from which it is ultimately derived. I may note that we have the additional relation

$$\sum_{i=1}^{i_{\max}} \gamma_i = n_a, \tag{A26}$$

where n_a is the number of different P-primes, as used in (12). As an example, I consider the following number,

$$\begin{aligned} N[2, 1_{13}] &\equiv 5^2 \times 13 \times 17 \times 29 \times 37 \times 41 \times 53 \times 61 \times 73 \times 89 \times 97 \times 101 \times 109 \times 113 \\ &\cong 6.1605 \times 10^{23}, \end{aligned} \tag{A27}$$

which is close to Avogadro's number

$$N_{\text{Av}} = 6.02204 \times 10^{23}.$$

The notation $N[2, 1_{13}]$ obviously means that the lowest P-prime, $p_1 = 5$, was squared and the next 13 P-primes (power $k_i = 1$) were multiplied in the order of increasing p_i (see Table 2).

According to (A25), the number of Pythagorean decompositions of $N[2, 1_{13}]$ is

$$n_d(\{\alpha_i\}) = \frac{1}{2}(5)(3^{13}) - \frac{1}{2} = 3{,}985{,}807. \tag{A28}$$

In general, we may try to calculate numbers N_k which in a given range have the largest number of P-decompositions n_d. This is usually accomplished by multiplying an appropriate number γ_1 of P-primes, all taken linearly ($k_1 = 1$), i.e., to the first power. This conclusion was derived from the results of Table 4 which show, for example, that $N[1, 1, 1, 1, 1] = N[1_5] = 1{,}185{,}665$ has

$n_d = 121$ P-decompositions, whereas the slightly larger $N[2, 2, 2] = N[2_3] = 1,221,025$ has only $n_d = 62$ P-decompositions.

In view of this result, I have made a study of the numbers $N[1_\gamma]$, where $N[1_\gamma]$ denotes the product of the first γ primes in Table 2. As an example,

$$N[1_{14}] = 5 \times 13 \times 17 \times 29 \times 37 \times 41 \times 53 \times 61 \times 73 \times 89 \times 97 \times 101 \times 109 \times 113 \cong 1.2321 \times 10^{23} \tag{A29}$$

has $n_d[1_{14}]$ Pythagorean decompositions, where [from (A25)]:

$$n_d[1_{14}] = \frac{1}{2}(3^{14} - 1) = 2,391,484. \tag{A30}$$

For several values of γ up to $\gamma = 25$, Table 5 gives the values of $N[1_\gamma]$, the corresponding $n_d[1_\gamma]$ [cf. (A30)], and the exponent $\sigma(\gamma)$, which will be defined presently. I noticed that $n_d[1_\gamma]$ is, in all cases, of the order of

$$\{N[1_\gamma]\}^{1/3} \text{ to } \{N[1_\gamma]\}^{1/4},$$

so that an accurate inverse power, denoted by $1/\sigma$, can be defined for each γ, such that

$$n_d[1_\gamma] = \{N[1_\gamma]\}^{1/\sigma}. \tag{A31}$$

$\sigma(\gamma)$ is a slowly varying function of γ that increases from $\sigma = 2.732$ for $\gamma = 3$ to $\sigma = 4.145$ for $\gamma = 25$. Below $\gamma = 3$, $\sigma(\gamma)$ increases to $\sigma = 3.011$ for $\gamma = 2$ and to ∞ for $\gamma = 1$, since the first P-prime, $p_1 = 5$, has a single P-decomposition, and $5^0 = 1$. The resulting curve of $\sigma(\gamma)$ *vs* γ is shown in Figure 1.

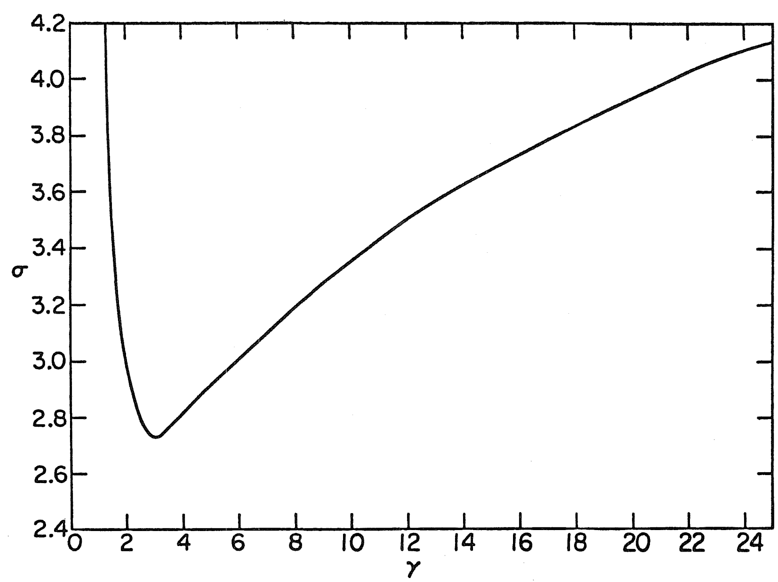

Figure 1. The inverse exponent σ as a function of γ for the n_d values pertaining to $N[1_\gamma]$ [see (A31)].

Table 5. Values of $\sigma(\gamma)$, $N[1_\gamma]$, and $n_d[1_\gamma]$ for selected values of γ in the range $1 \leqslant \gamma \leqslant 25$ [see (A31)].

γ	$\sigma(\gamma)$	$N[1_\gamma]$	$n_d[1_\gamma]$
1	∞	5	1
2	3.011	65	4
3	2.732	1105	13
4	2,813	32,045	40
5	2.916	1,185,665	121
6	3.001	48,612,265	364
8	3.184	1.572×10^{11}	3,280
10	3.358	1.021×10^{15}	29,524
12	3.503	1.004×10^{19}	265,720
14	3.620	1.232×10^{23}	2,391,484
17	3.789	3.949×10^{29}	64,570,081
20	3.936	2.286×10^{36}	1.743×10^{9}
22	4.024	1.076×10^{41}	1.569×10^{10}
25	4.145	1.553×10^{48}	4.236×10^{11}

APPENDIX B

THE CASE $n = 1$ OF EQUATION (2) AND COMMENTS ABOUT GOLDBACH'S CONJECTURE

It is obvious that the case $n = 1$ of (2), namely

$$x + y = z \tag{B1}$$

always has a solution with integers x, y, and z. We will assume, for definiteness, that $x \geqslant y$. Then (B1) has $z/2$ linearly independent solutions when z is even, and $(z - 1)/2$ linearly independent solutions when z is odd. As an example for $z = 11$, we have the following $(11 - 1)/2 = 5$ linear decompositions of z: $10 + 1$, $9 + 2$, $8 + 3$, $7 + 4$, and $6 + 5$.

There is a well-known conjecture, namely Goldbach's Conjecture, that any even z can be written as the sum of two prime numbers x and y. To my knowledge, this conjecture has not yet been proven in the general case, i.e., for an arbitrary even z. In this Appendix I have made a systematic study of the linear decompositions [equation (B1)] of all the even numbers $z \leqslant 100$ in terms of sums of two primes x and y.

It can be shown that the total number of linearly independent decompositions of an even z into a sum of two odd numbers according to (B1) is $z/4$ for $z = 4\nu$ (divisible by 4) and $(z + 2)/4$ for $z = 4\nu + 2$ (not divisible by 4). According to the above-mentioned program, I am led to consider all of the linear decompositions of z as a sum $x + y$, where x and y are restricted to being prime numbers. It will be seen shortly that in this endeavor, the concepts of a Pythagorean prime (P-prime) and a non-P-prime are of great importance.

In Table 6, I have listed all of the prime decompositions for even z in the range from 2 to 100. The number z is also denoted by N. In the prime decompositions, I have underlined the value of x_i or y_i in those cases where x_i or y_i is a Pythagorean prime. The most striking result of this table (aside from the large number of prime decompositions as $z = N$ increases) is that there are two types of cases, depending upon whether N is or is not divisible by 4: (a) If N is divisible by 4, i.e., $N = 4\nu$ (ν = positive integer), then each decomposition is the sum of a P-prime and a non-P-prime. (The only apparent exception occurs for $4 = 2 + 2$, and this decomposition will be discussed further below.) (b) If N is not divisible by 4, i.e., for $N = 4\nu + 2$, the prime decompositions involve either the sum of two P-primes (both x and y underlined) or the sum of two non-P-primes (neither x nor y underlined). As an example, $N = 16 = \underline{13} + 3 = 11 + \underline{5}$. By contrast, $N = 10 = 7 + 3 = \underline{5} + \underline{5}$.

These two rules can be derived from the theorem of Fermat [see the discussion preceding equation (10)] that all primes $p_i \equiv 1 \pmod 4$ are Pythagorean primes, while all primes $q_i \equiv 3 \pmod 4$ are non-P-primes. Thus, we can write:

$$p_i = 4\nu_i + 1, \tag{B2}$$

$$q_j = 4\nu_j - 1, \tag{B3}$$

from which it follows that

$$p_i + q_j = 4(\nu_i + \nu_j) = 4\nu \tag{B4}$$

for numbers $N = 4\nu$ that are divisible by 4. On the other hand,

$$p_i + p_{i'} = 4\nu_i + 4\nu_{i'} + 2 = 4(\nu_i + \nu_{i'}) + 2 = 4\nu + 2, \tag{B5}$$

$$q_j + q_{j'} = 4\nu_j + 4\nu_{j'} - 2 = 4(\nu_j + \nu_{j'} - 1) + 2 = 4\bar{\nu} + 2, \tag{B6}$$

for even numbers that are not divisible by 4, i.e., $N = 4\nu + 2$ or $4\bar{\nu} + 2$.

It may be noted that, in constructing Table 6, I have underlined the number 1, i.e., I have treated 1 as a Pythagorean prime (with the decomposition $1^2 = 1^2 + 0^2$). This is essentially a matter of definition, but it is mandated by the result that the decompositions which involve 1 obey the rules (a) and (b) described above, provided that 1 is regarded as a P-prime for the present purposes. I will also note that to regard 1 as a P-prime in cases where a direct addition is involved makes good sense, whereas in the arguments leading to the decomposition formula, (13), if I had introduced an arbitrary factor 1^{α_0} in the expression for N_k of (12), this would have invalidated (13) for the total number of decompositions n_d, unless $\alpha_0 = 0$.

The decomposition $4 = 2 + 2$ is an apparent exception to rules (a) and (b) given above. It does not seem to conform to the rule that one of the pair (x, y) be a P-prime, whereas the other of the pair (x, y) should be a non-P-prime. One way to obviate this contradiction is to specify that rules (a) and (b) apply only when the prime numbers x and y are odd. Another way of looking at the situation with respect to both 1 and 2 is that, as was emphasized repeatedly in [1] and in this paper, both 1 and 2 are special integers to which some of the rules governing other primes ($\geqslant 3$) do not apply; see especially the last two paragraphs of [1] and the discussion following (26) above. This privileged position of 1 and 2 has been correlated with the special properties of the powers $n = 1$ and $n = 2$ in the original Fermat equation, (2). Finally, a third and more speculative way to describe the status of the integer 2 in connection with $4 = 2 + 2$ is that just as $y = 1$ had to be defined as a P-prime in connection with Table 6, but as a non-P-prime in connection with (13), so $x = 2$ or $y = 2$ behaves half of the time as a P-prime (with the decomposition $2^2 = 2^2 + 0^2$) and half of the time as a non-P-prime which has no decomposition $2^2 = x^2 + y^2$, where $x, y > 0$. According to this interpretation, we could write $4 = 3 + \underline{1} = 2 + \underline{2}$ in Table 6.

Table 6. Linear decompositions of all even numbers $2 \leqslant N \leqslant 100$. For each $N = z$, all of the linear decompositions into a sum of prime numbers $z = x + y$ are listed. Values of x and y which correspond to Pythagorean primes are underlined; the nonunderlined values correspond to non-P-primes. Note that when N is divisible by 4, i.e., $N = 4\nu$ (ν = positive integer), one of the pair (x, y) is a P-prime whereas the other number in the sum is a non-P-prime. When N is divisible by 2, but not by 4, i.e., for $N = 4\nu + 2$, either both x and y are P-primes, or both x and y are non-P-primes. A possible exception occurs for the decomposition of $4 = 2 + 2$ (see discussion in text). We assume that $x \geqslant y$.

N	$x_i + y_i$
2	$\underline{1}+\underline{1}$
4	$3+\underline{1}$, $2+2$
6	$\underline{5}+\underline{1}$, $3+3$
8	$7+\underline{1}$, $\underline{5}+3$
10	$7+3$, $\underline{5}+\underline{5}$
12	$11+\underline{1}$, $7+\underline{5}$
14	$\underline{13}+\underline{1}$, $11+3$, $7+7$
16	$\underline{13}+3$, $11+\underline{5}$
18	$\underline{17}+\underline{1}$, $\underline{13}+\underline{5}$, $11+7$
20	$19+\underline{1}$, $\underline{17}+3$, $\underline{13}+7$
22	$19+3$, $\underline{17}+\underline{5}$, $11+11$
24	$23+\underline{1}$, $19+\underline{5}$, $\underline{17}+7$, $\underline{13}+11$
26	$23+3$, $19+7$, $\underline{13}+\underline{13}$
28	$23+\underline{5}$, $\underline{17}+11$
30	$\underline{29}+\underline{1}$, $23+7$, $19+11$, $\underline{17}+\underline{13}$
32	$31+\underline{1}$, $\underline{29}+3$, $19+\underline{13}$
34	$31+3$, $\underline{29}+\underline{5}$, $23+11$, $\underline{17}+\underline{17}$
36	$31+\underline{5}$, $\underline{29}+7$, $23+\underline{13}$, $19+\underline{17}$
38	$\underline{37}+\underline{1}$, $31+7$, $19+19$
40	$\underline{37}+3$, $\underline{29}+11$, $23+\underline{17}$
42	$\underline{41}+\underline{1}$, $\underline{37}+\underline{5}$, $31+11$, $\underline{29}+\underline{13}$, $23+19$
44	$43+\underline{1}$, $\underline{41}+3$, $\underline{37}+7$, $31+\underline{13}$

Table 6. continued

N	$x_i + y_i$
46	$43+3,\ \underline{41}+\underline{5},\ \underline{29}+\underline{17},\ 23+23$
48	$47+\underline{1},\ 43+\underline{5},\ \underline{41}+7,\ \underline{37}+11,\ 31+\underline{17},\ \underline{29}+19$
50	$47+3,\ 43+7,\ \underline{37}+\underline{13},\ 31+19$
52	$47+\underline{5},\ \underline{41}+11,\ \underline{29}+23$
54	$\underline{53}+\underline{1},\ 47+7,\ 43+11,\ \underline{41}+\underline{13},\ \underline{37}+\underline{17},\ 31+23$
56	$\underline{53}+3,\ 43+\underline{13},\ \underline{37}+19$
58	$\underline{53}+\underline{5},\ 47+11,\ \underline{41}+\underline{17},\ \underline{29}+\underline{29}$
60	$59+\underline{1},\ \underline{53}+7,\ 47+\underline{13},\ 43+\underline{17},\ \underline{41}+19,\ \underline{37}+23,\ 31+\underline{29}$
62	$\underline{61}+\underline{1},\ 59+3,\ 43+19,\ 31+31$
64	$\underline{61}+3,\ 59+\underline{5},\ \underline{53}+11,\ 47+\underline{17},\ \underline{41}+23$
66	$\underline{61}+\underline{5},\ 59+7,\ \underline{53}+\underline{13},\ 47+19,\ 43+23,\ \underline{37}+\underline{29}$
68	$67+\underline{1},\ \underline{61}+7,\ \underline{37}+31$
70	$67+3,\ 59+11,\ \underline{53}+\underline{17},\ 47+23,\ \underline{41}+\underline{29}$
72	$71+\underline{1},\ 67+\underline{5},\ \underline{61}+11,\ 59+\underline{13},\ \underline{53}+19,\ 43+\underline{29},\ \underline{41}+31$
74	$\underline{73}+\underline{1},\ 71+3,\ 67+7,\ \underline{61}+\underline{13},\ 43+31,\ \underline{37}+\underline{37}$
76	$\underline{73}+3,\ 71+\underline{5},\ 59+\underline{17},\ \underline{53}+23,\ 47+\underline{29}$
78	$\underline{73}+\underline{5},\ 71+7,\ 67+11,\ \underline{61}+\underline{17},\ 59+19,\ 47+31,\ \underline{41}+\underline{37}$
80	$79+\underline{1},\ \underline{73}+7,\ 67+\underline{13},\ \underline{61}+19,\ 43+\underline{37}$
82	$79+3,\ 71+11,\ 59+23,\ \underline{53}+\underline{29},\ \underline{41}+\underline{41}$
84	$83+\underline{1},\ 79+\underline{5},\ \underline{73}+11,\ 71+\underline{13},\ 67+\underline{17},\ \underline{61}+23,\ \underline{53}+31,\ 47+\underline{37},\ 43+\underline{41}$
86	$83+3,\ 79+7,\ \underline{73}+\underline{13},\ 67+19,\ 43+43$
88	$83+\underline{5},\ 71+\underline{17},\ 59+\underline{29},\ 47+\underline{41}$
90	$\underline{89}+\underline{1},\ 83+7,\ 79+11,\ \underline{73}+\underline{17},\ 71+19,\ 67+23,\ \underline{61}+\underline{29},\ 59+31,\ \underline{53}+\underline{37},\ 47+43$
92	$\underline{89}+3,\ 79+\underline{13},\ \underline{73}+19,\ \underline{61}+31$
94	$\underline{89}+\underline{5},\ 83+11,\ 71+23,\ \underline{53}+\underline{41},\ 47+47$
96	$\underline{89}+7,\ 83+\underline{13},\ 79+\underline{17},\ \underline{73}+23,\ 67+\underline{29},\ 59+\underline{37},\ \underline{53}+43$
98	$\underline{97}+\underline{1},\ 79+19,\ 67+31,\ \underline{61}+\underline{37}$
100	$\underline{97}+3,\ \underline{89}+11,\ 83+\underline{17},\ 71+\underline{29},\ 59+\underline{41},\ \underline{53}+47$

The number of prime linear decompositions $n_{\ell d}$, (B1), varies somewhat sporadically in going from a specific N, N_i, to its neighbors $N_i + 2$, $N_i + 4$, etc. However, there is a definite trend of an increasing number of prime decompositions $n_{\ell d}$ with increasing N, as would be expected because of the increasing number of integers x, y which are smaller than N, as N increases. We note, in particular, that $n_{\ell d} = 10$ for $N = 90$ (see Table 6). Since the total number of all linear decompositions of $N = 90$ into a sum of two odd numbers is

$$(N + 2)/4 = 23,$$

we see that the percentage of the linear decompositions which consist of sums of primes is $10/23 = 43\%$.

In Table 7 I have tabulated the total number of linear prime decompositions (ℓd) $n_{\ell d}$ for all even numbers N in the range $2 \leqslant N \leqslant 100$. For the cases where N is not divisible by 4, I have also listed the partial $n_{\ell d}$'s for *two* P-primes (x, y), denoted by $n_{\ell d, 2}$, and for *no* P-prime, denoted by $n_{\ell d, 0}$. Obviously, when N is not divisible by 4, we have

$$n_{\ell d} = n_{\ell d, 2} + n_{\ell d, 0}. \tag{B7}$$

At the bottom of the table, I have listed the total number of ℓd's $\Sigma n_{\ell d}$ in the range $2 \leqslant N \leqslant 50$ and $52 \leqslant N \leqslant 100$, and for the complete range $2 \leqslant N \leqslant 100$. It is seen that $\Sigma n_{\ell d}$ increases from 78 for the first half of the table ($N \leqslant 50$) to $\Sigma n_{\ell d} = 135$ for the second half of the table ($52 \leqslant N \leqslant 100$), showing the increase of the average $\Sigma n_{\ell d}/25$ from 3.12 to 5.40.

Similar tabulations have been made for $\Sigma n_{\ell d, 0}$ and $\Sigma n_{\ell d, 2}$. It is seen that the total number of ℓd's with $n_{P\text{-primes}} = 0$ slightly predominates over the total number of ℓd's with $n_{P\text{-primes}} = 2$. The ratio for the complete sample of 108 decompositions (up to $N = 100$) is $60/48 = 1.25$.

I have also written down the prime decompositions for eight even integers in the range $102 \leqslant N \leqslant 200$. The results are:

$$n_{\ell d}(N = 116) = 6,\quad n_{\ell d}(130) = 7,\quad n_{\ell d}(150) = 13,\quad n_{\ell d}(164) = 6,$$
$$n_{\ell d}(180) = 15,\quad n_{\ell d}(182) = 7,\quad n_{\ell d}(184) = 8,\ \text{and}\ n_{\ell d}(200) = 9.$$

Finally, I wish to point out an important correlation which is as simple as the one derived by Fermat concerning $p_i = 4\nu + 1$ for a P-prime and $q_j = 4\nu + 3$ for a non-P-prime. It is well known that any prime number p_i can be written in the form

$$p_i = 6\nu_i + 1 \quad \text{or} \quad 6\nu_i - 1, \tag{B8}$$

where ν_i is an arbitrary positive integer. (This equation does not, however, apply to the prime numbers 2 and 3, and for $p_i = 1$ we must use $\nu_i = 0$.) The argument for (B8) goes as follows: Consider a specific ν_i. Then $6\nu_i + 1$ is divisible by neither 2 nor 3, and therefore *may* be a prime; $6\nu_i + 2$ is divisible by 2; $6\nu_i + 3$ is divisible by 3; $6\nu_i + 4$ is again divisible by 2; $6\nu_i + 5 = 6(\nu_i + 1) - 1$ is divisible by neither 2 nor 3, and therefore is a candidate for being a prime number.

Table 7. For all even integers N in the range from 2 to 100, $n_{\ell d}$ is the number of linear decompositions of N into a sum of primes $N = x_i + y_i$, as given in Eq. (B1). For the integers N which are divisible by 2 but not by 4, i.e., for values $N = 4\nu + 2$, I have also listed the number of linear decompositions into a sum of two P-primes, denoted by $n_{\ell d,2}$, and the number of linear decompositions into a sum of two non-P-primes, denoted by $n_{\ell d,0}$. Obviously, for values of $N = 4\nu + 2$, we have $n_{\ell d} = n_{\ell d,2} + n_{\ell d,0}$. The sum of all $n_{\ell d}$ and $n_{\ell d,\alpha}$ ($\alpha = 0$ or 2) is listed at the end of the table for the intervals $2 \leqslant N \leqslant 50$ and $52 \leqslant N \leqslant 100$, and also for the total range $2 \leqslant N \leqslant 100$.

N	$n_{\ell d}$	$n_{\ell d,2}$	$n_{\ell d,0}$	N	$n_{\ell d}$	$n_{\ell d,2}$	$n_{\ell d,0}$
2	1	1	0	52	3		
4	2			54	6	3	3
6	2	1	1	56	3		
8	2			58	4	3	1
10	2	1	1	60	7		
12	2			62	4	1	3
14	3	1	2	64	5		
16	2			66	6	3	3
18	3	2	1	68	3		
20	3			70	5	2	3
22	3	1	2	72	7		
24	4			74	6	3	3
26	3	1	2	76	5		
28	2			78	7	3	4
30	4	2	2	80	5		
32	3			82	5	2	3
34	4	2	2	84	9		
36	4			86	5	1	4
38	3	1	2	88	4		
40	3			90	10	4	6
42	5	3	2	92	4		
44	4			94	5	2	3
46	4	2	2	96	7		
48	6			98	4	2	2
50	4	1	3	100	6		
$\Sigma n_{\ell d}$ $(2 \leqslant N \leqslant 50)$					78	19	22
$\Sigma n_{\ell d}$ $(52 \leqslant N \leqslant 100)$					135	29	38
$\Sigma n_{\ell d}$ $(2 \leqslant N \leqslant 100)$					213	48	60

Now the correlation which can be derived from Fermat's $p_i = 4\nu + 1$ theorem is that all Pythagorean primes are of the form

$$p_i = 6\nu_i + 1, \quad \text{if } \nu_i \text{ is even,} \tag{B9}$$

and

$$p_i = 6\nu_i - 1, \quad \text{if } \nu_i \text{ is odd.} \tag{B10}$$

Thus, $37 = (6)(6) + 1$ is an example of (B9) (even $\nu_i = 6$); $89 = (6)(15) - 1$ is an example of (B10).

In view of (B9) and (B10), the non-P-primes (except 2 and 3) are of the form

$$q_j = 6\nu_j - 1, \quad \text{if } \nu_j \text{ is even,} \tag{B11}$$

and

$$q_j = 6\nu_j + 1, \quad \text{if } \nu_j \text{ is odd.}$$

It should perhaps be noted that *not all* ν_i or ν_j give rise to P- or non-P-primes. The first few ν_i values which do *not* give rise to a prime number are: $\nu_i = 20, 24, 31, 34, 36, 41$, etc. The preceding equations signify only that *if* a given number is a P-prime p_i or a non-P-prime q_j, then it can be expressed by (B9) or (B10), and (B11) or (B12), respectively.

Referring to the results of Table 7, I wish to note that the total number $n_{\ell d}$ of prime decompositions has maxima when N is divisible by 6 ($N = 6\nu$), at least starting with $N = 24$. This trend is particularly noticeable when N lies in the range from 72 to 96. Thus, $n_{\ell d}(90) = 10$ is considerably larger than $n_{\ell d}(88) = 4$ and $n_{\ell d}(92) = 4$. Similarly, $n_{\ell d}(84) = 9$ characterizes a peak in the $n_{\ell d}$ values as a function of N since, for the neighboring $N = 82$ and $N = 86$, we find $n_{\ell d}(82) = 5$ and $n_{\ell d}(86) = 5$. This property may be caused by the fact that, when $N = 6\nu$, we have two primes such that one of them is of the form $6\nu_1 + 1$ and the other prime can be written as $6\nu_2 - 1$, and in taking the sum, we obtain $N = 6(\nu_1 + \nu_2) = 6\nu$. It is also interesting that in several cases, particularly for $N = 6\nu$, both members of each of two twin prime sets are involved, e.g.,

$$78 = \underline{73} + \underline{5} = 71 + 7 = \underline{61} + \underline{17} = 59 + 19.$$

Note also that

$$84 = \underline{73} + 11 = 71 + \underline{13} = \underline{41} + 43$$

and

$$90 = \underline{73} + \underline{17} = 71 + 19 = \underline{61} + \underline{29} = 59 + 31.$$

ACKNOWLEDGMENTS

I would like to thank Dr. Michael Creutz for several helpful discussions, for a critical reading of the manuscript, and for devising the computer program designed to list the primitive solutions of equation (1). I am also indebted to Dr. Sidney Heller for a critical reading of the manuscript.

REFERENCES

1. R. M. Sternheimer. "A Corollary of Iterated Exponentiation." *The Fibonacci Quarterly 23* (1985):146-148.
2. *Handbook of Chemistry and Physics*. 44th ed., pp. 244-251. Cleveland, Ohio: Chemical Rubber Publishing Co., 1963.
3. M. Creutz. Private communication.
4. See also W. J. Le Veque. *Elementary Theory of Numbers*, p. 108. Reading, Mass: Addison-Wesley Publishing Co., 1962; and A. F. Horadam. "Fibonacci Number Triples." *Amer. Math. Monthly 68* (1961):751-753.

◆◇◆◇◆