# On the Sum of the Squares of Two Consecutive Integers

By Edward L. Cohen†

**I. Introduction.** Solutions of $n^2 + (n+1)^2 = q^k$ are examined, where $q$ is a prime $\leq 109$, and $k$ is an integer $\geq 1$. Note from Hardy and Wright [1, p. 219, Theorem 252] that if $e$ has in its factorization any prime $\equiv 3 \pmod 4$, then $n^2 + (n+1)^2 \neq e^l$ for any $l$ (positive). So only the numbers that have prime factors $\equiv 1 \pmod 4$, have to be considered. Here, we deal only with primes $q \equiv 1 \pmod 4$, where $q \leq 109$, and a few other primes with $109 < q < 1000$. L. Aubry [2] proved that $x^2 + (x+1)^2 \neq m^k$ if $k$ is not a power of 2.

Notice that $1^2 + 2^2 = 5$, $3^2 + 4^2 = 5^2$, $2^2 + 3^2 = 13$, $119^2 + 120^2 = 13^4$, $20^2 + 21^2 = 29^2$, $4^2 + 5^2 = 41$, and $5^2 + 6^2 = 61$. Excluding these possibilities, there is the

THEOREM. *$n^2 + (n+1)^2 \neq q^k$ for all primes $q \leq 109$.*

The theorem [3] was previously proven (in a slightly different manner) for $q = 5$.

Observe that

$$n^2 + (n+1)^2 = q^k \tag{1}$$

is equivalent to

$$Z^2 = 2 \cdot q^k - 1\,, \tag{2}$$

for if $Z = 2n + 1$, (1) comes from (2), and if $n = (Z-1)/2$, (2) comes from (1).

Some facts are stated about Gaussian integers. The integers are of the form $a + bi$, where $a$ and $b$ are natural integers. Unique factorization holds, and the only units are $+1$, $-1$, $+i$, $-i$.

**II. Case 1: 41, 5, 13, 29, 37, 53, 61, 101, and 109.** A special solution is required for every prime $q$ in Case 1. We select 41; the results for all the primes in Case 1 are in Table I, and their results can be compared with those of 41.

Let us factor (1) for $q = 41$: $[(n+1) + ni][(n+1) - ni] = (5 + 4i)^k(5 - 4i)^k = \mu^k \cdot \bar{\mu}^k$, with the possible inclusion of some units. Should $(n+1) + ni$ or $(n+1) - ni$ have as factors both $5 + 4i$ and $5 - 4i$, it would have a factor of 41. Hence, its real and imaginary parts, $n + 1$ and $n$, would both be divisible by 41, which is impossible. (A similar argument shall be omitted later.)

Now, $4^2 + 5^2 = 41$, so solutions with $k \geq 2$ must be sought. The following lemma must first be proven.

LEMMA. *$n$ is a solution* $\langle\!=\!\rangle$ $n = 651$ or $-652 \pmod{41^2}$.

*Proof.* If $n$ runs through the integers mod 41, namely 0, 1, 2, $\cdots$, 40, then $n^2 + (n+1)^2 \equiv 0 \pmod{41}$ $\langle\!=\!\rangle$ $n = 4$ or $n = 36$ (i.e., $-5$) $\pmod{41}$.

Received August 25, 1966. Revised November 21, 1966.

† Present address: University of Ottawa, Ottawa 2, Canada.

TABLE I

| *prime* | *Gaussian Integer* | *power* | $n \equiv$ | $k$ | *addendum* | $Z_k$ | $Z_{k-1}$ | $Z_{k-2}$ | *quasi-periodic* | *mod* | *nonsquare* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | $2+i$ | 3 | 28 | 7 | 25 | $-28$ | 8 | $-38$ | $-1$ | 101 | 2 |
| 13 | $2+3i$ | 5 | 114124 | 6595 | 85683 | $-114125$ | 13228 | $-44273$ | $-1$ | | See Table II |
| 29 | $2+5i$ | 3 | 5066 | 1626 | 5887 | $-5067$ | $-10409$ | 6308 | $-1$ | 105967 | 92809 |
| 37 | $6+i$ | 2 | 58 | 104 | 333 | 59 | 45 | 568 | $+1$ | 149 | 11 |
| 41 | $5+4i$ | 2 | 651 | 71 | 205 | $-651$ | 431 | 244 | $+1$ | 83 | 53 |
| 53 | $2+7i$ | 1 | 11 | 10 | 13 | 12 | 3 | 14 | $-1$ | | See Table III |
| 61 | $6+5i$ | 3 | 87784 | 3811 | 55815 | 87785 | 946 | $-94278$ | $+1$ | 1116301 | 5405 |
| 101 | $10+i$ | 1 | 45 | 13 | 25 | $-46$ | 28 | $-39$ | $-1$ | 151 | 6 and $-8$ |
| 109 | $10+3i$ | 1 | 16 | 15 | 27 | 17 | 39 | 51 | $-1$ | 73 | $-17$ and 15 |

Suppose $n \equiv 4 \pmod{41}$. Then $n = 41r + 4$. Substituting this in $n^2 + (n+1)^2 = 41^k$, the following is obtained:

$$2 \cdot 41r^2 + 18r + 1 = 41^{k-1}, \tag{3}$$

or $r \equiv -16 \pmod{41}$, $r = 41l - 16$, and hence $n = 41^2 l - 652$. So $n \equiv -652 \pmod{41^2}$.

If $n \equiv -5 \pmod{41}$, the same type of calculation shows that $n \equiv 651 \pmod{41^2}$. Q.E.D.

The above lemma can also be proved by using [4, p. 79]. In fact, [4] can be used to prove the lemma in the general case for a prime of the form $4t + 1$.

Now, $(5 + 4i)^k = X_k + iY_k$, so

$$(X_{k+1} + iY_{k+1}) = (X_k + iY_k)(5 + 4i) = (5X_k - 4Y_k) + (4X_k + 5Y_k)i \; ; \tag{4}$$

therefore, $X_{k+1} = 5X_k - 4Y_k$, and $Y_{k+1} = 4X_k + 5Y_k$. It can be seen that both $X_k$ and $Y_k$ satisfy

$$Z_{k+2} = 10Z_{k+1} - 41Z_k \, . \tag{5}$$

Let $Z_j = (\mu^j + \bar{\mu}^j)/2 = [(5 + 4i)^j + (5 - 4i)^j]/2$. (Since $[(n+1) + ni][(n+1) - ni] = [n + (n+1)i][n - (n+1)i]$, we could have the possibility that $Z_k$ either $= \pm n$ or $\pm(n+1) \bmod 41^2$; i.e., $Z_k = \pm 651$ or $\pm 652 \pmod{41^2}$.) Thus, $Z_0 = 1$, $Z_1 = 5$. We use $Z_0$, $Z_1$, and the formula $Z_{j+2} = 10Z_{j+1} - 41Z_j \pmod{41^2}$.

We say that a sequence is *quasi-periodic* when two successive residue classes repeat except possibly with a change of sign. By (5), the sequence is quasi-periodic, since $Z_1 \equiv Z_{206} \pmod{41^2}$ and $Z_2 \equiv Z_{207} \pmod{41^2}$. The sequence repeats with a quasi-period of 205. Also, of $Z_0, Z_1, \cdots, Z_{205}$ only $Z_{71} = \pm 651$ or $\pm 652$. The table below indicates what we are interested in:

| $k$ | *addendum* | $Z_k$ | $Z_{k-1}$ | $Z_{k-2}$ |
|---|---|---|---|---|
| 71 | | $-651$ | 431 | 244 |
| 276 | 205 | $-651$ | 431 | 244 |
| 481 | 205 | $-651$ | 431 | 244 |
| 686 | 205 | $-651$ | 431 | 244 |
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |

(Actually the sequence connected with 41 is periodic, but the sequences connected with 5, 13, 29, 53, 101, and 109 are quasi-periodic. Also, note that if $\mu = 4 + 5i$ were used the same $k$ and addendum would be obtained.)

Hence, it is shown that only $71, 71 + 1 \cdot 205, 71 + 2 \cdot 205, \cdots$ can yield solutions of $n^2 + (n+1)^2 = 41^k$. We prove that this cannot happen.

Notice that $k \equiv 71 \pmod{205}$. If $2 \cdot 41^k - 1$ is a square, then it is a quadratic residue for any modulus. This is an immediate consequence of the definition of a quadratic residue. Since $41^{205} \equiv 1 \pmod{83}$, $2 \cdot 41^{71} \cdot 41^{205 \cdot s} - 1 \equiv 53 \pmod{83}$, $s \geq 0$. As 53 is a nonsquare (mod 83), it is proven that $2 \cdot 41^k - 1 \equiv 53 \pmod{83}$ is a nonsquare for the relevant cases. This completes the proof.

Tables II and III deal with 13 and 53 respectively. It was not possible to find one prime (like 83 above) with a corresponding nonsquare. Therefore, with 13 and

TABLE II

| $2 \cdot 13^{6595} \cdot 13^{85683 \cdot s} - 1$ where | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $s =$ | *0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* | *12* | *13* | *14* | *15* | *16* | *17* | *18* | *19* | *20* |
| mod 11 | 8 *N* | 5 *S* | 3 *S* | 9 *S* | 2 *N* | 1 *S* | 4 *S* | 6 *N* | 0 *S* | 7 *N* | 8 *N* | 5 *S* | 3 *S* | 9 *S* | 2 *N* | 1 *S* | 4 *S* | 6 *N* | 0 *S* | 7 *N* | 8 |
| mod 421 | 57 *N* | 283 *S* | 25 *S* | 286 *S* | 301 *N* | 418 *S* | 236 *N* | 332 *N* | 323 *N* | 337 *S* | 362 *N* | 136 *N* | 394 *S* | 133 *N* | 118 *S* | 1 *S* | 183 *N* | 87 *N* | 96 *N* | 82 *S* | 57 |
| mod 1171 | 447 *S* | 745 *N* | 708 *N* | 913 *S* | 695 *S* | 447 *S* | 745 *N* | 708 *N* | 913 *S* | 695 *S* | 447 *S* | 745 *N* | 708 *N* | 913 *S* | 695 *S* | 447 *S* | 745 *N* | 708 *N* | 913 *S* | 695 *S* | 447 |
| mod 342733 | *f** *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* *S* | *g* *N* | *f* |

* Where $f = 338304$ is a square, $S$, and $g = 4427$ is a nonsquare, $N$.

TABLE III

*S a square, N a nonsquare*

| $2 \cdot 53^{10} \cdot 53^{13 \cdot s} - 1$ where | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $s =$ | *0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* | *12* | *13* | *14* | *15* | *16* | *17* | *18* |
| mod 19 | 7 *S* | 3 *N* | 1 *S* | 0 *S* | 9 *S* | 4 *S* | −8 *S* | 5 *S* | 2 *N* | −9 *N* | −5 *N* | −3 *S* | −2 *S* | 8 *N* | −6 *N* | 6 *S* | −7 *N* | −4 *N* | 7 |
| mod 79 | 21 *S* | −33 *S* | 24 *N* | −23 *N* | 31 *S* | −26 *N* | 21 *S* | −33 *S* | 24 *N* | −23 *N* | 31 *S* | −26 *N* | 21 *S* | −33 *S* | 24 *N* | −23 *N* | 31 *S* | −26 *N* | 21 |
| mod 163 | −58 *N* | 6 *S* | 1 *S* | −47 *N* | 79 *N* | −48 *S* | −61 *N* | 75 *N* | 44 *N* | −58 *N* | 6 *S* | 1 *S* | −47 *N* | 79 *N* | −48 *S* | −61 *N* | 75 *N* | 44 *N* | −58 |

53 several primes were used. To check whether a number is a square or a nonsquare modulo a prime, one can use quadratic residue theory [1, Chapter VI].

**III. Case 2: 17, 73, 89, 97, and Others Under 1000.** A special solution is required for every prime in Case 2. We select 17; the others are proved in the same manner.

Let us factor (1) for $q = 17$: $[(n + 1) + ni][(n + 1) - ni] = (4 + i)^k (4 - i)^k = \mu^k \cdot \bar{\mu}^k$ with the possible inclusion of some units. The following lemma is first proven.

LEMMA. *$n$ is a solution* $\langle = \rangle$ $n \equiv 6$ or $-7 \pmod{17}$.

*Proof.* If $n$ runs through the integers mod 17, namely 0, 1, 2, $\cdots$, 16, then $n^2 + (n + 1)^2 \equiv 0 \pmod{17}$ $\langle = \rangle$ $n \equiv 6$ or 10 (i.e., $-7$) $\pmod{17}$. Q.E.D.

Now, $(4 + i)^k = X_k + iY_k$, so

$$(6) \quad (X_{k+1} + iY_{k+1}) = (X_k + iY_k)(4 + i) = (4X_k - Y_k) + (X_k + 4Y_k)i \ ;$$

therefore, $X_{k+1} = 4X_k - Y_k$, and $Y_{k+1} = X_k + 4Y_k$. It can be seen that both $X_k$ and $Y_k$ satisfy

$$(7) \qquad Z_{k+2} = 8Z_{k+1} - 17Z_k \ .$$

Let $Z_j = (\mu^j + \bar{\mu}^j)/2 = [(4 + i)^j + (4 - i)^j]/2$. These give $Z_0$ and $Z_1$. We use $Z_0$, $Z_1$, and the formula $Z_{j+2} = 8Z_{j+1} - 17Z_j \pmod{17}$. The sequence is quasi-periodic with quasi-period 4. We have

| $Z_0$ | $Z_1$ | $Z_2$ | $Z_3$ | $Z_4$ | $Z_5$ | $Z_6$ | $Z_7, \cdots$ |
|---|---|---|---|---|---|---|---|
| 1 | 4 | $-2$ | 1 | 8 | $-4$ | 2 | $-1, \cdots$ |

which does not give $\pm 6$, $\pm 7$.

*Other Primes in Case 2.* Other primes $q$ in Case 2 $\leq 109$ are 73, 89, and 97. The primes in Case 2 with $109 < q < 1000$ are 157, 193, 233, 241, 257, 281, 337, 349, 353, 401, 409, 433, 449, 461, 541, 577, 601, 617, 641, 661, 673, 709, 769, 821, 881, 929, 937, and 977. The proofs are omitted.

**IV. Acknowledgments.** An IBM 7030 computer was used extensively in the calculations. I am grateful to Paul Hamburger of MITRE, who shortened the output of one of my programs considerably.

The MITRE Corporation
Bedford, Massachusetts

1. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 3rd ed., Clarendon Press, Oxford, 1954, 1962. MR **16**, 673.
2. L. AUBRY, *L'intermédiaire des math.*, 18, 1911, pp. 8–9, errata pp. 112–113; *Sphinx-Oedipe*, numero special, March 1914, pp. 15–16, errata p. 39.
3. C. ENGLEMAN, "On close-packed double error-correcting codes on $p$ symbols," *IRE Trans. Inform. Theory*," v. IT-7, 1961, pp. 51–52. MR **23** #B3075.
4. D. SHANKS, "A sieve method for factoring numbers of the form $n^2 + 1$," *MTAC*, v. 13, pp. 78–86. MR **21** #4520.