by Lemma 4, $D = 1$. If $p \equiv 21$ or $29 \pmod{40}$, then $\sigma \mid p - 1$ implies that $\sigma \not\equiv 0 \pmod 8$. By Lemma 4, $D \neq 2$. This concludes the proof of the second part of the theorem. By Theorems 2 and 6, a formula for $D(n)$ is obtained:

$$D(n) = \frac{[D(2^{r_0})\rho(2^{r_0}),\ D(p_1^{r_1})\rho(p_1^{r_1}),\ \ldots,\ D(p_1^{r_m})\rho(p_m^{r_m})]}{[\rho(2^{r_0}),\ \rho(p_1^{r_1}),\ \ldots,\ \rho(p_m^{r_m})]}.$$

For an odd prime p, we have, by Theorems 3 and 7,

$$\sigma(p^r)/\rho(p^r) = p^{r-s}\sigma(p)/p^{r-t}\rho(p) = p^{t-s}\sigma(p)/\rho(p).$$

Since this value is either 1, 2, or 4, it must be the case that $s = t$, and hence, $D(p^r) = D(p)$. The formula above reduces to

$$D(n) = \frac{[D(2^{r_0})\rho(2^{r_0}),\ D(p_1)\rho(p_1),\ \ldots,\ D(p_m)\rho(p_m)]}{[\rho(2^{r_0}),\ \rho(p_I),\ \ldots,\ \rho(p_m)]}.$$

A routine checking of all cases—using Lemma 4, the formula above, and the formulas for $\sigma(2^r)$ and $\rho(2^r)$—verifies the remainder of Theorem 8. □

Theorem 9 is now an immediate consequence of Theorems 4 and 8.

4. RELATED TOPICS

Several questions remain open. We would like to know, for example, whether a formula for $D(p)$ is possible when $p \equiv 1$ or $9 \pmod{20}$.

One may also ask whether $\sigma(p^2) \neq \sigma(p)$ for all odd primes p. If so, our formulas of Theorems 3 and 7 would be simplified so that $s = t = 1$. This question has been asked earlier by D. D. Wall [6]. Penny & Pomerance claim to have verified it for $p \leq 177{,}409$ [4]. Using Theorem 1, the conjecture is equivalent to $\varepsilon^{p^2-1} \neq 1$ in $\mathbf{Z}_{p^2}^*[\sqrt{5}]$. A similar equality $2^{p-1} = 1$ in $\mathbf{Z}_{p^2}^*$ has been extensively studied, and the first counterexample is $p = 1093$. The analogy between the two makes the existence of a large counterexample to $\sigma(p^2) \neq \sigma(p)$ seem likely.

REFERENCES

1. Z. Borevich & I. Shafarevich, *Number Theory* (New York: Academic Press, 1966).
2. S. Lang, *Algebra* (Reading, Mass.: Addison-Wesley, 1965).
3. W. LeVeque, *Topics in Number Theory*, I (Reading, Mass.: Addison-Wesley, 1956).
4. Penny & Pomerance, *American Math. Monthly*, Vol. 83 (1976), pp. 742-743.
5. N. Vorob'ev, *Fibonacci Numbers* (New York: Blaisdell, 1961).
6. D. D. Wall, *American Math. Monthly*, Vol. 67 (1960), pp. 525-532.

*****

CONGRUENT PRIMES OF FORM $(8r + 1)$

J. A. H. HUNTER

An integer e is congruent if there are known integral solutions for the system $X^2 - eY^2 = Z^2$, and $X^2 + eY^2 = Z^2$. At present, we can be sure that a particular number is congruent only if corresponding X, Y values have been determined.

However, it has been stated and accepted that integers of certain forms cannot be congruent. Proofs exist for most of those excluding conditions, but not for all—no counterexamples having been discovered as regards the latter. For example, a prime of form $(8r + 3)$, or the product of two such primes, cannot be congruent.

L. Bastien and others have stated that a prime of form $(8r + 1)$, representable as $(k^2 + t^2)$ cannot be congruent if $(k + t)$ is not a quadratic residue of that prime. But no proof of this has been known to exist in the literature.

The necessary proof will be developed in this paper.

We first show that the situations regarding primes of form $(8r + 1)$, and those of form $(8r + 5)$, are not the same. For this we use the Collins analysis method.

It is well known that every congruent number must be of form $uv(u^2 - v^2)/g^2$. Then, if e be a prime of form $(8r + 5)$ or $(8r + 1)$, for congruent e we must have solutions to $uv(u^2 - v^2) = eg^2$: from which it follows that one of u, v, $(u - v)$, $(u + v)$ must be ea^2, say, and the other three must all be squares.

Consider each of the four possibilities.

(1) $u + v = ea^2$, $u - v = b^2$, $u = c^2$, $v = d^2$.

Then, $b^2 - 2c^2 = -ea^2$:
possible with $e = 8r + 1$; impossible with $e = 8r + 5$.

Similarly, $b^2 + 2d^2 = ea^2$:
possible with $e = 8r + 1$; impossible with $e = 8r + 5$.

Also, $c^2 + d^2 = ea^2$, and $c^2 - d^2 = b^2$:
both possible for $e = 8r + 1$ and for $e = 8r + 5$.

Hence, this case (1) applies to $e = 8r + 1$, but not to $e = 8r + 5$.

(2) $u - v = ea^2$, $u + v = b^2$, $u = c^2$, $v = d^2$.

Then, $b^2 - 2c^2 = -ea^2$:
possible with $e = 8r + 1$; impossible with $e = 8r + 5$.

Similarly, $b^2 - 2d^2 = ea^2$:
possible with $e = 8r + 1$; impossible with $e = 8r + 5$.

Also, $c^2 - d^2 = ea^2$, and $c^2 + d^2 = b^2$:
both possible for $e = 8r + 1$ and for $e = 8r + 5$.

Hence, this case (2) applies to $e = 8r + 1$, but not to $e = 8r + 5$.

(3) $u = ea^2$, $u + v = b^2$, $u - v = c^2$, $v = d^2$.

Then, $b^2 + c^2 = 2ea^2$, $b^2 - c^2 = 2d^2$, $b^2 - d^2 = ea^2$, and $c^2 + d^2 = ea^2$:
All possible for both $e = 8r + 1$ and $e = 8r + 5$.

Hence, this case (3) applies to both.

(4) $v = ea^2$, $u + v = b^2$, $u - v = c^2$, $u = d^2$.

Then, $b^2 - c^2 = 2ea^2$, $b^2 + c^2 = 2d^2$, $b^2 - d^2 = ea^2$, and $d^2 - c^2 = ea^2$:
All possible for both $e = 8r + 1$ and $e = 8r + 5$.

Hence, this case (4) applies to both.

So, for $e = 8r + 5$, we have possible:

$$\text{Case (3)}\quad \left.\begin{aligned} x^2 + y^2 &= 2ez^2 \\ x^2 - y^2 &= 2w^2 \end{aligned}\right\} \qquad \text{Case (4)}\quad \left.\begin{aligned} x^2 + y^2 &= 2z^2 \\ x^2 - y^2 &= 2ew^2 \end{aligned}\right\}$$

But, for $e = 8r + 1$, we have possible:

$$\text{Case (1)}\quad \left.\begin{aligned} x^2 + y^2 &= ez^2 \\ x^2 - y^2 &= w^2 \end{aligned}\right\} \qquad \text{Case (2)}\quad \left.\begin{aligned} x^2 + y^2 &= z^2 \\ x^2 - y^2 &= ew^2 \end{aligned}\right\}$$

$$\text{Case (3)}\quad \left.\begin{aligned} x^2 + y^2 &= 2ez^2 \\ x^2 - y^2 &= 2w^2 \end{aligned}\right\} \qquad \text{Case (4)}\quad \left.\begin{aligned} x^2 + y^2 &= 2z^2 \\ x^2 - y^2 &= 2ew^2 \end{aligned}\right\}$$

We now show that each of the subsidiary-equation systems (1), (2), and (3) will provide a solution for the system (4) for any congruent number prime $(8r + 1)$.

From (1) to (4):

Say $x^2 + y^2 = ez^2$, $x^2 - y^2 = w^2$, and $A^2 + B^2 = 2C^2$, $A^2 - B^2 = 2eD^2$.

Setting $A = x^4 + 2x^2y^2 - y^4$, $B = x^4 - 2x^2y^2 - y^4$, we have

$$A^2 + B^2 = 2(x^4 + y^4)^2,\quad A^2 - B^2 = 2e \cdot (2xyzw)^2.$$

As an example,

$$\left.\begin{aligned} 5^2 + 4^2 &= 41 \cdot 1^2 \\ 5^2 - 4^2 &= 3^2 \end{aligned}\right\} \qquad \left.\begin{aligned} 1169^2 + 431^2 &= 2 \cdot 881^2 \\ 1169^2 - 431^2 &= 2 \cdot 41 \cdot 120^2 \end{aligned}\right\}$$

From (2) to (4):

Say $x^2 + y^2 = z^2$, $x^2 - y^2 = ew^2$, and $A^2 + B^2 = 2C^2$, $A^2 - B^2 = 2eD^2$.

Setting $A = x^4 + 2x^2y^2 - y^4$, $B = x^4 - 2x^2y^2 - y^4$, we have

$$A^2 + B^2 = 2(x^4 + y^4)^2,\quad A^2 - B^2 = 2e \cdot (2xyzw)^2.$$

As an example,

$$\left.\begin{aligned} 21^2 + 20^2 &= 29^2 \\ 21^2 - 20^2 &= 41 \cdot 1^2 \end{aligned}\right\} \qquad \left.\begin{aligned} 387281^2 + 318319^2 &= 2 \cdot 354481^2 \\ 387281^2 - 318319^2 &= 2 \cdot 41 \cdot 24360^2 \end{aligned}\right\}$$

From (3) to (4):

Say $x^2 + y^2 = 2ez^2$, $x^2 - y^2 = w^2$, and $A^2 + B^2 = 2C^2$, $A^2 - B^2 = 2eD^2$.

Setting $A = (ez^2)^2 + 2ez^2w^2 - w^4$, $B = (ez^2)^2 - 2ez^2w^2 - w^4$, we have

$$A^2 + B^2 = 2[(ez^2)^2 + w^4]^2,\quad A^2 - B^2 = 2e \cdot (2xyzw)^2.$$

As an example,

$$\left.\begin{aligned} 33^2 + 31^2 &= 82 \cdot 5^2 \\ 33^2 - 31^2 &= 2 \cdot 8^2 \end{aligned}\right\} \qquad \left.\begin{aligned} 1177729^2 + 915329^2 &= 2 \cdot 1054721^2 \\ 1177729^2 - 915329^2 &= 2 \cdot 41 \cdot 81840^2 \end{aligned}\right\}$$

We may also consider the system (4) itself:

Say $x^2 + y^2 = 2z^2$, $x^2 - y^2 = 2ew^2$.

From the first of the two equations we require

$$x = u^2 + 2uv - v^2,\quad y = u^2 - 2uv - v^2,\quad z = u^2 + v^2.$$

Then $x^2 - y^2 = (2u^2 - 2v^2)4uv$,
whence, $4uv(u^2 - v^2) = ew^2$, which we know has solutions if e is a congruent number.

Now, having shown that each of the four possible systems of subsidiary equasions, for prime e of form $8r + 1$, must have solutions if e is to be congruent—and that system (4) is linked to each of the other three systems—a proof that any one of the four systems will not have solutions for any particular value of e must be proof that no other of the four systems can have solutions. Accordingly, we now show that e cannot be congruent if $e = k^2 + t^2$, and $(k + t)$ is not a quadratic residue of e. For this we investigate the subsidiary-equation system (1).

Say e is a prime of form $(8r + 1)$, represented uniquely as $k^2 + t^2$.

We have the system: $x^2 + y^2 = ez^2$, $x^2 - y^2 = w^2$. Thence,

$$(kz)^2 = x^2 + y^2 - (tz)^2,$$

with solution

$$\left.\begin{aligned} kz &= a^2 + b^2 - c^2 \\ tz &= 2ac \end{aligned}\right\} \qquad \left.\begin{aligned} x &= a^2 - b^2 + c^2 \\ y &= 2ab \end{aligned}\right\} \quad \ldots (M)$$

hence,

$$2kac = ta^2 + tb^2 - tc^2,$$

making

$$t^2c^2 + 2ktac - t^2a^2 = t^2b^2$$

whence,

$$(tc + ka)^2 - (ka)^2 - (ta)^2 = (tb)^2$$

so

$$(tc + ka)^2 - ea^2 = (tb)^2,$$

with solution

$$\left.\begin{aligned} tc + ka &= m^2 + en^2 \\ ka &= 2kmn \end{aligned}\right\} \qquad \left.\begin{aligned} tc &= m^2 - 2kmn + en^2 \\ tb &= m^2 - en^2 \end{aligned}\right\}$$

Without loss of generality, that becomes

$$a = 2tmn,\ b = m^2 - en^2,\ c = m^2 - 2kmn + en^2.$$

Substituting in (M), and omitting the common term $4mn$, we get

$$x = km^2 - 2emn + ken^2,\ y = t(m^2 - en^2),$$

whence

$$x + y = (k + t)m^2 - 2emn + (k - t)^2$$

and

$$x - y = (k - t)m^2 - 2emn + (k + t)^2.$$

Now, since we have $x^2 + y^2 = ez^2$, with e an odd prime, x and y cannot be of same parity. Hence, each of $(x + y)$ and $(x - y)$ must be a square.

So, say, $x + y = p^2$. Then,

$$[(k + t)m - en]^2 - 2e(tn)^2 = (k + t)p^2,$$

which is possible only if $(k + t)$ is a quadratic residue of e.

That completes the proof that a prime of form $(8r + 1)$, uniquely represented as $(k^2 + t^2)$, cannot be congruent if $(k + t)$ is a quadratic nonresidue of e.

BIBLIOGRAPHY

L. Bastien, *Nombres Congruents*, l'Intermediare des Mathematiciens, Vol. 22, (1915).

A. H. Beiler, *Recreations in the Theory of Numbers* (1966), pp. 155-157.

Matthew Collins, *A Tract on the Possible and Impossible Cases of Quadratic Duplicate Equalities* (Dublin: Trinity College, 1858).
A. Gérardin, *Nombres Congruents*, 1'Intermédiare des Mathématiciens, Vol. 22, (1915).
S. Roberts, *Proceedings of the London Mathematical Society*, Vol. 11 (1879).

*****

SOME CLASSES OF FIBONACCI SUMS

LEONARD CARLITZ
Duke University, Durham, North Carolina 27706

1. INTRODUCTION

Layman [3] recalled the formulas [2]

$$F_{2n} = \sum_{k=0}^{n} \binom{n}{k} F_k, \tag{1.1}$$

$$2^n F_{2n} = \sum_{k=0}^{n} \binom{n}{k} F_{3k}, \tag{1.2}$$

$$3^n F_{2n} = \sum_{k=0}^{n} \binom{n}{k} F_{4k}, \tag{1.3}$$

where, as usual, the F_n are the Fibonacci numbers defined by

$$F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1} \qquad (n \geq 1).$$

As Layman remarks, the three identities suggest the possibility of a general formula of which these are special instances. Several new sums are given in [2]. Many additional sums occur in [1].

Layman does not obtain a satisfactory generalization; however, he does obtain a sequence of sums that include (1.1), (1.2), and (1.3). In particular, the following elegant formulas are proved:

$$5^n F_{2n} = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} F_{5k}, \tag{1.4}$$

$$8^n F_{2n} = \sum_{k=0}^{n} \binom{n}{k} 3^{n-k} F_{6k}, \tag{1.5}$$

$$F_{3n} = (-1)^n \sum_{k=0}^{n} \binom{n}{k} (-2)^k F_{2k}, \tag{1.6}$$

$$5^n F_{3n} = (-1)^n \sum_{k=0}^{n} \binom{n}{k} (-2)^k F_{5k}. \tag{1.7}$$

He notes also that each of the sums he obtains remains valid when F_n is replaced by L_n, where the L_n are the Lucas numbers defined by

$$L_0 = 2,\ L_1 = 1,\ L_{n+1} = L_n + L_{n-1} \qquad (n \geq 1).$$