MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 141
JANUARY 1978, PAGES 293–295

A Note on Congruent Numbers

By H. J. Godwin

Abstract. The list of known congruent numbers less than 1000 is extended by a proof that 19 primes of the form $8k + 7$ are congruent.

The positive rational integer a is called congruent if and only if there exist rational nonzero integers x, y, z, t such that $x^2 - ay^2 = z^2$, $x^2 + ay^2 = t^2$. (This is the definition in [3] where the history of early work on such numbers is given; Sierpiński [4] requires, unusually, that y should be 1.) The most recent work on congruent numbers appears to be that of Alter and Curtz [1], who list the numbers < 1000 known to be congruent or incongruent. In [1] 457 appears in both lists but, as noted later by the same authors [2], is in fact congruent.

In the present note a simple method, which enables a number of additions to be made to the list of congruent numbers, is described.

In what follows p denotes a prime congruent to 7 (mod 8).

If p is congruent, we have $2x^2 = z^2 + t^2 = 2((\frac{1}{2}z + \frac{1}{2}t)^2 + (-\frac{1}{2}z + \frac{1}{2}t)^2)$, $2py^2 = t^2 - z^2$.

Hence, $x = l^2 + m^2$, $z + t = 2(l^2 - m^2)$, $t - z = 4lm$, or $x = l^2 + m^2$, $z + t = 4lm$, $t - z = 2(l^2 - m^2)$; whence $py^2 = lm(l^2 - m^2)$.

Hence, just one of $l, m, l - m, l + m$ is p times a square, and the rest are squares. Also, since we may suppose that $(x, y) = 1$, we have $(t, z) = 1$ and so no two of the squares have a common factor.

Consideration of congruences modulo 8 gives either

I. $l = a^2$, $m = pb^2$, $l - m = c^2$, $l + m = d^2$, or

II. $l = a^2$, $m = b^2$, $l - m = pc^2$, $l + m = d^2$.

In case I we have $a^2 - pb^2 = c^2$, $a^2 + pb^2 = d^2$ and $a \leqslant a^2 = l \leqslant l^2 < x$ so that, by the method of descent, case I does not arise.

In case II we have, again by congruences modulo 8, that a is even and b odd; and since $a^2 + b^2 = d^2$, we have

$$a = 2ef, \quad b = e^2 - f^2, \quad \text{whence } pc^2 = (2ef - e^2 + f^2)(2ef + e^2 - f^2).$$

Since $(l, m) = 1$, we have $(e, f) = 1$ and so, since e, f cannot both be odd because b is odd, we have either

(i) $2ef - e^2 + f^2 = pg^2$, $2ef + e^2 - f^2 = h^2$, or

(ii) $2ef - e^2 + f^2 = g^2$, $2ef + e^2 - f^2 = ph^2$.

(i) gives $(e + f)^2 = h^2 + 2f^2$ and since $(e + f, f) = 1$ we have

---

Received November 9, 1976.
AMS (MOS) subject classifications (1970). Primary 10B05; Secondary 65A05.
Key words and phrases. Congruent numbers, Diophantine equations.

$$e + f = r^2 + 2s^2, \quad f = 2rs,$$

$$\text{whence } pg^2 = (r^2 + 2s^2)^2 - 2(r^2 - 2rs + 2s^2)^2 = f(r, s) \quad \text{say.}$$

Case (ii) leads to the same result.

We now search for pairs (r, s) such that the squarefree part of $f(r, s)$ is p.

Since $f(2s, r) = 4f(r, s)$, it is sufficient to consider $r/s < \sqrt{2}$, and we have also

$$r/s > t = \frac{\sqrt{2} - 2\sqrt{(\sqrt{2} - 1)}}{\sqrt{2} - 1} = .3066\ldots,$$

the smaller zero of $f(x, 1)$. Since 2 is a quadratic residue of p, say $2 \equiv n^2 \pmod{p}$, we have

$$f(r, s) \equiv ((r^2 + 2s^2) - n(r^2 - 2rs + 2s^2))((r^2 + 2s^2) + n(r^2 - 2rs + 2s^2)) \pmod{p}.$$

Since -1 is a quadratic nonresidue of p, just one of the quadratic factors is reducible modulo p, and so $r/s \equiv r_1$ or $r_2 \pmod{p}$.

We now consider, for each s, the values $f(r, s)$ where $r = r_1 s - kp$ or $r_2 s - kp$ for

$$t < r_i - k(p/s) < \sqrt{2}, \qquad i = 1, 2.$$

A search, mainly by computer, gave the following values of p, r, s and so each of the primes p listed is congruent.

p	r	s
103	38	119
127	136	443
167	14	27
191	60	193
199	26	49
223	256	301
263	4017	12767
271	49	106
311	705	2061
359	23	75
383	153	138
431	61	114
439	130	127
463	67	146
487	751	1973
631	2615	1927
839	25	21
919	142	143
991	211	670

The primes $p < 1000$ not in the above list are 367, 503, 599, 607, 647, 727, 743, 823, 863, 887, 911, 967, 983, and for each of these a search for $s \leqslant 40{,}000$

yielded no value of r. However, the wide variation in the values of s in the table does not preclude the existence of solutions with $s > 40000$ and the conjecture (see [1]) that all numbers $\equiv 5$, 6 or 7 (mod 8) are congruent is not refuted.

Department of Statistics and Computer Science
Royal Holloway College
Egham Hill,
Egham, Surrey TW20 0EX, England

1. R. ALTER & T. B. CURTZ, "A note on congruent numbers," *Math. Comp.*, v. 28, 1974, pp. 303–305.

2. R. ALTER & T. B. CURTZ, Corrigendum, *Math. Comp.*, v. 30, 1976, p. 98.

3. L. E. DICKSON, *History of the Theory of Numbers*, Vol. 2, New York, 1952, pp. 459–472. (Reprint.)

4. W. SIERPIŃSKI, *Elementary Theory of Numbers*, PWN, Warsaw, 1964.