SOLUTION OF THE SYSTEM
$a^2 \equiv -1 \pmod{b}$, $b^2 \equiv -1 \pmod{a}$

JAMES C. OWINGS, Jr.
University of Maryland, College Park, MD 20742

(Submitted August 1985)

INTRODUCTION

On page 64 of *Introduction to Number Theory* by Adams and Goldstein [1], problem number 7 asks: "Does $x^2 \equiv -1 \pmod{65}$ have a solution?" An obvious solution is $x = 8$, but if one first solves the congruences $x^2 \equiv -1 \pmod{5}$ and $x^2 \equiv -1 \pmod{13}$ and then applies the Chinese Remainder Theorem, one finds that $x^2 \equiv -1 \bmod (5 \cdot 13) \iff x \equiv \pm 5 \pm \pm 3 \bmod (5 \cdot 13)$. This leads to the following obvious question. For which pairs of numbers a, b do we have $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$? This is equivalent to $ab \mid a^2 + b^2 + 1$ which, in turn, is equivalent to the pair of conditions $a \mid b^2 + 1$ & $b \mid a^2 + 1$ (if the latter conditions hold, it is clear that a and b are relatively prime).

Let

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_n + F_{n+1},\ F_{n-2} = F_n - F_{n-1}$$

so that F_n, the n^{th} Fibonacci number, is defined for all integers n. Clearly $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$ is equivalent to $(a - b)^2 \equiv -1 \pmod{ab}$. We will show that $(a - b)^2 \equiv -1 \pmod{ab}$, where $1 \leqslant a \leqslant b$, iff for some $n \geqslant 0$, $a = F_{2n-1}$ & $b = F_{2n+1}$. Thus, the solutions are (1, 1), (1, 2), (2, 5), (5, 13), (13, 34), (34, 89), (89, 233), (233, 610), ... Since we are also interested in the equation $(a - b)^2 \equiv +1 \pmod{ab}$, we shall carry out many of our calculations with ± 1 in place of -1.

1. EQUIVALENCE TO THE DIOPHANTINE EQUATION $z^2 - (x^2 - 4)y^2 = \pm 4$

Since $(a - b)^2 \equiv \pm 1 \pmod{ab}$, we write $(a - b)^2 \mp 1 = rab$, that is,

$$a^2 - (2 + r)ab + b^2 \mp 1 = 0.$$

Let $k = 2 + r$. If b and k are given, then there will exist an a satisfying $a^2 - kab + b^2 \pm 1 = 0$ iff

$$\frac{1}{2}(kb \pm \sqrt{(k^2 - 4)b^2 \pm 4})$$

is an integer. By examining the cases k even, b even, k and b both odd, we see that this is equivalent to $(k^2 - 4)b^2 \pm 4 = z^2$, for some z. We let $x = k$, $y = b$, and obtain the Diophantine equation

$$z^2 - (x^2 - 4)y^2 = \pm 4.$$

Every solution of this equation except for $(z, x, y) = (0, 0, \pm 1)$ corresponds to two solutions of $(a - b)^2 = \pm 1 + (x - 2)ab$, namely,

$$b = y,\ a = \frac{xy \pm z}{2}.$$

Here 4 corresponds to +1 and −4 corresponds to −1.

2. THE EQUATION $z^2 - (x^2 - 4)y^2 = -4$

We now concentrate on the -1 case. First, we prove a useful lemma.

Lemma 1: $z^2 - (x^2 - 4)y^2 = -4$ is solvable in integers iff $z^2 - (x^2 - 4)y^2 = -1$ is solvable in integers. One direction is easy, since $z^2 - (x^2 - 4)y^2 = -1$ implies $(2z^2) - (x^2 - 4)(2y)^2 = -4$. So suppose $z^2 - (x^2 - 4)y^2 = -4$ is solvable. If x were even, then 4 would divide $x^2 - 4$, so 2 would divide z, and we would obtain

$$\left(\frac{z}{2}\right)^2 - \left(\left(\frac{x}{2}\right)^2 - 1\right)y^2 = -1.$$

Since -1 is not a square (mod 4), y is odd. Thus,

$$\left(\frac{z}{2}\right)^2 = -1 + \left(\left(\frac{x}{2}\right)^2 - 1\right)y^2 \equiv \left(\frac{x}{2}\right)^2 - 2 \equiv 2, 3 \pmod{4},$$

which is impossible. Therefore, x is odd.

Let (z_0, y_0) be a solution of $z^2 - (x^2 - 4)y^2 = -4$. Then $z_0 \equiv y_0 \pmod{2}$. If z_0 and y_0 are both even, then

$$\left(\frac{z_0}{2}\right)^2 - (x^2 - 4)\left(\frac{y_0}{2}\right)^2 = -1$$

and we are done. Therefore, we assume that z_0, y_0 are odd. We now quote the following easy and well-known result.

Multiplication Principle: If $u_0^2 - Dv_0^2 = A$ and $u_1^2 - Dv_1^2 = B$, then $u_2^2 - Dv_2^2 = AB$ where

$$u_2 + \sqrt{D}v_2 = (u_0 + \sqrt{D}v_0)(u_1 + \sqrt{D}v_1) = (u_0u_1 + Dv_0v_1) + \sqrt{D}(u_0v_1 + u_1v_0).$$

$(x, \pm 1)$ are solutions of $z^2 - (x^2 - 4)y^2 = 4$; so, by the Multiplication Principle with $D = x^2 - 4$, (z_i, y_i), $i = 1, 2$, are solutions of

$$z^2 - (x^2 - 4)y^2 = (-4)(4) = -16,$$

where

$$(z_i, y_i) = (z_0x + (-1)^i Dy_0,\ xy_0 + (-1)^i z_0).$$

Since $4^2 \mid 16$, it is clear that $4 \mid z_i$ iff $4 \mid y_i$. Also, since x, z_0, y_0, and D are all odd, z_1, y_1, z_2, and y_2 are even. Also,

$$z_2 - z_1 = 2Dy_0 \equiv 2 \pmod{4} \quad \text{and} \quad y_2 - y_1 = 2z_0 \equiv 2 \pmod{4}.$$

So, for some i, $z_i \equiv y_i \equiv 0 \pmod{4}$. Hence,

$$\left(\frac{z_i}{4}\right)^2 - (x^2 - 4)\left(\frac{y_i}{4}\right)^2 = -1$$

and Lemma 1 is proved.

Lemma 2: $z^2 - (x^2 - 4)y^2 = -1$ is solvable only when $x = \pm 3$.

When $x = \pm 3$, we may take $z = 2$, $y = 1$. Suppose $z^2 - (x^2 - 4)y^2 = -1$ is solvable. Then x is odd. Suppose $x > 0$ and $x \neq 3$. Then $x > 3$ since, otherwise,

$$z^2 - (x^2 - 4)y^2 \geqslant 0.$$

Let (z^*, y^*) be that solution characterized by $z^* > 0$, $y^* > 0$, and y^* is minimal (the so-called *fundamental* solution). Since $x > 3$, $x^2 - 4$ is not a perfect square; so, by the general theory of Pell equations (see [1], p. 201, Theorem

106), if (z, y) is any solution of $z^2 - (x^2 - 4)y^2 = +1$ with $z > 0$, $y > 0$, then

$$z + \sqrt{x^2 - 4}y = (z^* + \sqrt{x^2 - 4}y^*)^n,$$

where n is an even positive integer.

In order to arrive at a contradiction, we need to find a small solution of $z^2 - (x^2 - 4)y^2 = 1$ with x odd. We have two obvious solutions of

$$z^2 - (x^2 - 4)y^2 = 4,$$

namely, $(x, 1)$ and $(x^2 - 2, x)$. Therefore,

$$(x(x^2 - 2) + (x^2 - 4)x, x^2 + (x^2 - 2)) = (2(x^3 - 3x), 2(x^2 - 1))$$

is a solution of $z^2 - (x^2 - 4)y^2 = 16$, by the Multiplication Principle. Since x is odd, $x^3 - 3x$ and $x^2 - 1$ are even. Hence,

$$\left(\frac{x^3 - 3x}{2}\right)^2 - (x^2 - 4)\left(\frac{x^2 - 1}{2}\right)^2 = 1.$$

Let

$$(A, B) = \left(\frac{x^3 - 3x}{2}, \frac{x^2 - 1}{2}\right).$$

(A, B) is probably the fundamental solution of $z^2 - (x^2 - 4)y^2 = 1$, but we do not have a proof [William Adams has shown, using the theory of continued fractions, that (A, B) is the fundamental solution]. In any case,

$$A + \sqrt{x^2 - 4}B = (z^* + \sqrt{x^2 - 4}y^*)^n, \text{ where } n \text{ is even.}$$

Therefore, there exist positive numbers U and V such that

$$A + \sqrt{x^2 - 4}B = (U + \sqrt{x^2 - 4}V)^2.$$

Let $D = \sqrt{x^2 - 4}$. Then $A = U^2 + DV^2$, $B = 2UV$. Hence,

$$A = U^2 + D\left(\frac{B}{2U}\right)^2.$$

Let $W = U^2$. Then $4W^2 - 4AW + DB^2 = 0$. So $(2W - A)^2 = A^2 - DB^2 = 1$, and

$$U^2 = W = \frac{A \pm 1}{2} = \frac{x^3 - 3x \pm 2}{4}.$$

Thus,

$$U = \frac{1}{2}\sqrt{x^3 - 3x \pm 2} = \frac{1}{2}\sqrt{(x \mp 1)^2(x \pm 2)} = \frac{x \mp 1}{2}\sqrt{x \pm 2}$$

and

$$V = \frac{B}{2U} = \frac{x^2 - 1}{2(x \mp 1)\sqrt{x \pm 2}} = \frac{x \pm 1}{2\sqrt{x \pm 2}}.$$

It turns out that if $2W = A - 1$, then $U^2 - DV^2 = -1$, while if $2W = A + 1$, then $U^2 - DV^2 = +1$. We do not, however, need this information. We have shown

Proposition: If $z^2 - (x^2 - 4)y^2 = -1$ is solvable in integers, then either

$$x - 2 \text{ is a perfect square and } \sqrt{x - 2} \mid x - 1$$

or

$$x + 2 \text{ is a perfect square and } \sqrt{x + 2} \mid x + 1.$$

Suppose that $x - 2 = t^2$ and $t \mid x - 1$. Then $t \mid t^2 + 1$. So $t = 1$. Therefore $x = 3$, a contradiction. Suppose that $x + 2 = t^2$ and $t \mid x + 1$. Then $t \mid t^2 - 1$. So $t = 1$. Thus $x = -1$, a contradiction. This completes the proof of Lemma 2.

Putting Lemmas 1 and 2 together, we see that $z^2 - (x^2 - 4)y^2 = -4$ is solvable in integers iff $x = \pm 3$.

3. SOLUTION OF $a^2 - 3ab + b^2 = \pm 1$

In solving the congruence $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$, it clearly suffices to find all solutions (a, b) with $a, b \geq 1$. Also, the equation is equivalent to $(a - b)^2 \equiv -1 \pmod{ab}$, i.e., $(a - b)^2 + 1 = rab$, where, because $a, b > 0$, we know $r > 0$. By §2, $2 + r = k = \pm 3$. Therefore, $k = 3$ and $r = 1$. So, if $a, b \geq 1$, the congruence $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$ is equivalent to the equation

$$a^2 - 3ab + b^2 = -1.$$

Theorem: Let a and b be any two integers. Then

1) $a^2 - 3ab + b^2 = -1$ iff $(a, b) = \pm(F_n, F_{n\pm 2})$ where n is odd, and

2) $a^2 - 3ab + b^2 = 1$ iff $(a, b) = \pm(F_n, F_{n\pm 2})$ where n is even.

Proof: We could reduce our equations to the Pell equation $u^2 - 5v^2 = 1$ using well-known methods. However, it is easier to apply the methods developed in [3]. Consider the equation $a^2 - 3ab + b^2 = -1$. The idea is that any solution (a, b) generates two other solutions (a, b') and (a', b), where a' and b' are determined by the recurrences $a' = 3b - a$, $b' = 3a - b$. If we apply these recurrences over and over, we develop a two-way infinite chain $\ldots b'\,a\,b\,a'\ldots$ of integers in which any adjacent pair represents a solution. According to ([3], p. 56), every chain of solutions to our equation must contain an a-value in the set $\{0, \pm 1\}$ or a b-value in the set $\{0, \pm 1\}$. The only solutions (a, b) having this property are $\pm(1, 1)$, $\pm(1, 2)$, and $\pm(2, 1)$. So, except for changes of sign, every solution lies in the single chain

$$\ldots\underline{34}\ 13\ \underline{5}\ 2\ \underline{1}\ 1\ \underline{2}\ 5\ \underline{13}\ 34\ldots,$$

where we have underlined the a-values. Since $F_{-1} = 1$ and $F_1 \equiv 1$, and since

$$3F_n - F_{n-2} = 2F_n + F_{n-1} = F_n + F_{n+1} = F_{n+2}$$

holds for every integer n, we see that this sequence of numbers is

$$\ldots F_{-5}\ F_{-3}\ F_{-1}\ F_1\ F_3\ F_5\ldots\ .$$

Therefore $a^2 - 3ab + b^2 = -1$ iff, for some odd number n, $(a, b) = \pm(F_n, F_{n\pm 2})$. The equation $a^2 - 3ab + b^2 = +1$ is handled in a similar fashion.

Corollary: If $0 \leq a \leq b$, then $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$ iff, for some $n \geq 0$,

$$(a, b) = (F_{2n-1}, F_{2n+1}).$$

4. DISCUSSION OF $(\pm a \pm b)^2 \equiv 1 \pmod{ab}$

We shall briefly discuss the equation $(\pm a \pm b)^2 \equiv 1 \pmod{ab}$, equivalent to $(a - b)^2 \equiv 1 \pmod{ab}$, which we rewrite as $a^2 - kab + b^2 = 1$. In §1 we showed that this equation is solvable iff $z^2 - (k^2 - 4)y^2 = +4$ is solvable. The latter equation has an obvious solution, namely $(z, y) = (k, 1)$. So we have solutions of $a^2 - kab + b^2 = 1$ for every k, not just $k = 3$. When $k = 3$, we have only the solutions given by the Theorem of §3, but when $k = 4$ we have, for example, $(a, b) = (1, 4)$, and when $k = 5$ we have, for example, $(a, b) = (5, 24)$. When $k = 2$, we get the infinite class $(a, b) = (n, n \pm 1)$. Clearly,

$$n^2 - 2n(n \pm 1) + (n \pm 1)^2 = 1,$$

and if $a^2 - 2ab + b^2 = 1$, then $b = a \pm 1$. A complete classification for all k would be an interesting project.

5. WHEN a AND b ARE PRIMES

If a and b are distinct primes, or if one is an odd prime and the other is twice another odd prime, the congruence $x^2 \equiv -1 \pmod{ab}$, if solvable, will have precisely four solutions. Therefore,

$$x^2 \equiv -1 \pmod{ab} \iff x = \pm a \pm b$$

holds for the following pairs (a, b):

$$(2, 5), (5, 13), (13, 34), (34, 89), (89, 233).$$

However, it does not hold for the pair (233, 610). There are eight solutions of $x^2 \equiv -1 \bmod (233 \cdot 610)$, four of which are $\pm 233 \pm 610 = \pm 377, \pm 843$. The other four are $\pm 121 \cdot 233 \pm 610 = \pm 27583, \pm 28803$. Thus, the question arises: How many pairs of primes a, b are there satisfying $(\pm a \pm b)^2 = -1 \pmod{ab}$? Since n is prime whenever F_n is prime, if there are finitely many twin primes, there are only finitely many such pairs. However, it is generally believed that the set of twin primes is infinite. Nevertheless, based on separate probabilistic considerations, Daniel Shanks has conjectured that (89, 233) is the last such pair.

ACKNOWLEDGMENT

We should like to acknowledge the role of Daniel Shanks in the development of this paper. It was he who first noticed that the sequence

$$2, 5, 13, 34, 89, 233, \ldots$$

provides infinitely many solutions to the congruence $(\pm a \pm b)^2 \equiv -1 \pmod{ab}$.

REFERENCES

1. William W. Adams & Larry J. Goldstein. *Introduction to Number Theory*. Englewood Cliffs, NJ.: Prentice-Hall, 1976.
2. Trygve Nagell. *Introduction to Number Theory*. New York: Chelsea Publishing Co., 1964.
3. James C. Owings, Jr. "Diophantine Chains." *Rocky Mountain Journal of Mathematics 13*, no. 1 (1983):55-60.

◆◇◆◇◆