FIBONACCI SEQUENCE MODULO a prime $p \equiv 3 \pmod 4$

GOTTFRIED BRUCKNER
DAW, Institut fur Reine Mathematik, Berlin-Adlershof, Germany

Shah [1] proved: For a prime $q > 7$ the Fibonacci sequence might contain a complete residue system mod q only if $q \equiv 3$ or $7 \pmod{20}$. Here we show the

Theorem. Let p be a prime, $p > 7$, $p \equiv 3 \pmod 4$, then in the Fibonacci sequence, a complete residue system mod p doesn't exist.

It follows from this and Shah's result: The only primes for which the Fibonacci sequence possesses a complete residue system are 2, 3, 5, and 7.

Let p be a prime, $p > 7$, $p \equiv 3 \pmod 4$. In the following all residues and congruences are meant mod p. For the Fibonacci sequences

$$u_{-1} = 0, \quad u_0 = 1, \quad u_1 = 1, \quad u_2 = 2, \cdots$$

is true:

$$(1) \quad u_n = u_a u_{n-a} + u_{a-1}u_{n-a-1}, \quad a = 0, \cdots, n; \quad n = 0, 1, \cdots$$

$$(2) \quad u_{k+b} \equiv \pm u_{k-b}, \quad b = 0, \cdots, k,$$

where $g = 2k + 1$ is the minimal index so that $p \mid u_g$ (for $p \equiv 3 \pmod 4$ g is uneven).

$$(3) \quad u_{x(g+1)+y} \equiv \pm u_y, \quad y = 0, \cdots, g; \quad x = 0, 1, 2, \cdots$$

(You verify these known facts by easy calculations.)

Lemma. The residues

$$u_s u_{s-1}^{-1}, \quad s = 1, \cdots, g,$$

are all different.

Proof. From

$$u_a u_{b-1} \equiv u_b u_{a-1}, \quad 1 \le a \le b \le g,$$

we define (putting $u_a = u_{a-1} + u_{a-2}$ and $u_b = u_{b-1} + u_{b-2}$)

$$u_{a-1} u_{b-2} \equiv u_{b-1} u_{a-2},$$

continuing this way, we get

$$u_1 u_{b-a} \equiv u_{b-a+1} u_0 ,$$

this means

$$u_{b-a} \equiv u_{b-a+1} ,$$

hence $u_{b-a-1} \equiv 0$, hence $b = a$.

Corollary 1. $g \le p$.

Corollary 2. The residues

$$u_s u_{s-e}^{-1}, \quad s = e, \cdots, g + e - 1,$$

are all different, e being a given number $1 \le e \le g$.

Proof. From

$$u_a u_{b-e} \equiv u_b u_{a-e},$$

we conclude with

$$u_a = u_e u_{a-e} + u_{e-1} u_{a-e-1}$$

and

$$u_b = u_e u_{b-e} + u_{b-e-1}$$

(from (1))

$$u_{a-e-1}u_{b-e} \equiv u_{b-e-1}u_{a-e}$$

and by the Lemma, $a - e = b - e$, $a = b$.

(The Lemma and Corollaries hold, of course, for all primes.)

Proof of the Theorem. From (2) and (3), it is clear that

$$u_n \equiv 0 \quad \text{or} \quad \pm u_c, \quad 1 \le c \le k$$

holds for all n. Therefore the question is whether

$$\{0, \pm u_c, 1 \le c \le k\}$$

forms a complete residue system or not. This might be the case only if k takes its maximum $(p-1)/2$. Hence to prove the Theorem, it suffices to prove: Is $g = p$ then there is a congruence

$$(\star)\ u_a \equiv \pm u_b$$

for at least one pair (a,b), $1 \le a < b \le (p-1)/2$.

Putting $e = 5$, Corollary 2 gives: The p residues

$$u_s u_{s-5}^{-1}, \quad s = 5, \cdots, p+4,$$

are all different. Hence there is a t, $5 \le t \le p+4$, satisfying

$$u_t u_{t-5}^{-1} \equiv 1 .$$

From this,

$$u_t \equiv u_{t-5} \quad \text{for one } t, \quad 5 \le t \le p+4 .$$

We differ 4 cases:

a) $$t \ge p,$$

b) $$p > t > t - 5 \ge (p-1)/2,$$

c) $t > (p-1)/2 > t-5$,

d) $(p-1)/2 \geq t$.

Case a) is impossible:

$$u_{p\pm4} \equiv \pm u_3, \quad u_{p\pm3} \equiv \pm u_2, \quad u_{p\pm2} \equiv \pm u_1, \quad u_{p\pm1} \equiv \pm u_0, \quad u_p \equiv 0$$

(from (2) and (3)). (Check the cases $t = p, \cdots, p+4$ one after the other and take into account $p > 5$.) While Case (d) is a congruence (*) itself, we easily get such a congruence in Case (b) by utilizing (2). In the remaining Case (c), we put

$$t = (p-1)/2 + r, \quad 1 \leq r \leq 4 .$$

We have

$$u_{(p-1)/2+r} \equiv u_{(p-1)/2-(5-r)} .$$

From (2), we conclude

$$u_{(p-1)/2+r} \equiv \pm u_{(p-1)/2-r} ,$$

hence

$$(**) \quad u_{(p-1)/2-(5-r)} \equiv \pm u_{(p-1)/2-r} .$$

$p > 7$ implies $(p-1)/2 > 4$, therefore in (**), both indices are ≥ 1, r and $5-r$ always being different (**) is a congruence (*). This finishes the proof of the Theorem.

REFERENCE

1. A. P. Shah, "Fibonacci Sequence Modulo m," Fibonacci Quarterly, Vol. 6 (1968), pp. 139-141.