

**Problem.** Let  $x, y$  and  $a_0, a_1, a_2, \dots$  be integers satisfying  $a_0 = a_1 = 0$ , and

$$a_{n+2} = xa_{n+1} + ya_n + 1$$

for all integers  $n \geq 0$ . Let  $p$  be any prime number. Show that  $\gcd(a_p, a_{p+1})$  is either equal to 1 or greater than  $\sqrt{p}$ .

After trying to solve the problem on your own, you can find a possible solution on the next page.

**Problem.** Let  $x, y$  and  $a_0, a_1, a_2, \dots$  be integers satisfying  $a_0 = a_1 = 0$ , and

$$a_{n+2} = xa_{n+1} + ya_n + 1$$

for all integers  $n \geq 0$ . Let  $p$  be any prime number. Show that  $\gcd(a_p, a_{p+1})$  is either equal to 1 or greater than  $\sqrt{p}$ .

**Remark 1.** I presented a different solution in the video that uses only forward induction and no backward induction.

*Proof.* Let  $q$  be any prime dividing  $\gcd(a_p, a_{p+1})$ . We will show that  $q > \sqrt{p}$ , which implies the statement.

Note that  $p \geq 2$  and so  $0 = a_{p+1} = xa_p + ya_{p-1} + 1 = ya_{p-1} + 1 \in \mathbb{F}_q$  implying  $q \nmid y$ . Thus, we have

$$a_n = \frac{a_{n+2} - xa_{n+1} - 1}{y} \in \mathbb{F}_q, \quad (1)$$

which tells us that  $(a_{n+2}, a_{n+1}) \in \mathbb{F}_q^2$  uniquely determines  $a_n \in \mathbb{F}_q$ .

We have  $|\mathbb{F}_q^2| = q^2$ . By the pigeon hole principle, there exists  $0 \leq i < j \leq q^2$  with  $(a_i, a_{i+1}) = (a_j, a_{j+1}) \in \mathbb{F}_q^2$ . Take  $i, j$  such that  $d := j - i$  is minimal. Using recursion and [eq. \(1\)](#) inductively and by the minimality of  $d$ , we get

$$(a_s, a_{s+1}) = (a_t, a_{t+1}) \in \mathbb{F}_q^2 \iff d \mid t - s.$$

Since  $(a_1, a_2) = (0, 1) \neq (0, 0) = (a_0, a_1) \in \mathbb{F}_q^2$ , we have  $d > 1$ . From  $(a_0, a_1) = (a_p, a_{p+1}) = (0, 0) \in \mathbb{F}_q^2$ , we get  $d \mid p$ , which implies  $d = p$  since  $p$  is a prime. Thus,  $q^2 \geq d = p$ . Since  $p$  is prime, we cannot have equality. Thus,  $q > \sqrt{p}$ , as desired. q.e.d.