



English (eng), day 1

*Tuesday, July 18, 2017*

**Problem 1.** For each integer  $a_0 > 1$ , define the sequence  $a_0, a_1, a_2, \dots$  by:

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{if } \sqrt{a_n} \text{ is an integer,} \\ a_n + 3 & \text{otherwise,} \end{cases} \quad \text{for each } n \geq 0.$$

Determine all values of  $a_0$  for which there is a number  $A$  such that  $a_n = A$  for infinitely many values of  $n$ .

**Problem 2.** Let  $\mathbb{R}$  be the set of real numbers. Determine all functions  $f: \mathbb{R} \rightarrow \mathbb{R}$  such that, for all real numbers  $x$  and  $y$ ,

$$f(f(x)f(y)) + f(x+y) = f(xy).$$

**Problem 3.** A hunter and an invisible rabbit play a game in the Euclidean plane. The rabbit's starting point,  $A_0$ , and the hunter's starting point,  $B_0$ , are the same. After  $n-1$  rounds of the game, the rabbit is at point  $A_{n-1}$  and the hunter is at point  $B_{n-1}$ . In the  $n^{\text{th}}$  round of the game, three things occur in order.

- (i) The rabbit moves invisibly to a point  $A_n$  such that the distance between  $A_{n-1}$  and  $A_n$  is exactly 1.
- (ii) A tracking device reports a point  $P_n$  to the hunter. The only guarantee provided by the tracking device to the hunter is that the distance between  $P_n$  and  $A_n$  is at most 1.
- (iii) The hunter moves visibly to a point  $B_n$  such that the distance between  $B_{n-1}$  and  $B_n$  is exactly 1.

Is it always possible, no matter how the rabbit moves, and no matter what points are reported by the tracking device, for the hunter to choose her moves so that after  $10^9$  rounds she can ensure that the distance between her and the rabbit is at most 100?

*Language: English**Time: 4 hours and 30 minutes  
Each problem is worth 7 points*



English (eng), day 2

Wednesday, July 19, 2017

**Problem 4.** Let  $R$  and  $S$  be different points on a circle  $\Omega$  such that  $RS$  is not a diameter. Let  $\ell$  be the tangent line to  $\Omega$  at  $R$ . Point  $T$  is such that  $S$  is the midpoint of the line segment  $RT$ . Point  $J$  is chosen on the shorter arc  $RS$  of  $\Omega$  so that the circumcircle  $\Gamma$  of triangle  $JST$  intersects  $\ell$  at two distinct points. Let  $A$  be the common point of  $\Gamma$  and  $\ell$  that is closer to  $R$ . Line  $AJ$  meets  $\Omega$  again at  $K$ . Prove that the line  $KT$  is tangent to  $\Gamma$ .

**Problem 5.** An integer  $N \geq 2$  is given. A collection of  $N(N+1)$  soccer players, no two of whom are of the same height, stand in a row. Sir Alex wants to remove  $N(N-1)$  players from this row leaving a new row of  $2N$  players in which the following  $N$  conditions hold:

- (1) no one stands between the two tallest players,
- (2) no one stands between the third and fourth tallest players,
- ⋮
- ( $N$ ) no one stands between the two shortest players.

Show that this is always possible.

**Problem 6.** An ordered pair  $(x, y)$  of integers is a *primitive point* if the greatest common divisor of  $x$  and  $y$  is 1. Given a finite set  $S$  of primitive points, prove that there exist a positive integer  $n$  and integers  $a_0, a_1, \dots, a_n$  such that, for each  $(x, y)$  in  $S$ , we have:

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \cdots + a_{n-1}xy^{n-1} + a_ny^n = 1.$$

Language: English

Time: 4 hours and 30 minutes  
Each problem is worth 7 points

## Solutions

1. For each integer  $a_0 > 1$ , define the sequence  $a_0, a_1, a_2, \dots$  by:

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{if } \sqrt{a_n} \text{ is an integer,} \\ a_n + 3 & \text{otherwise,} \end{cases} \quad \text{for each } n \geq 0.$$

Determine all values of  $a_0$  for which there is a number  $A$  such that  $a_n = A$  for infinitely many values of  $n$ .

*Solution by Clarence Chew.*

*Lemma 1.* If  $a_k \equiv 2 \pmod{3}$  for some  $k \geq 0$ , then no number  $A$  exists such that  $a_n = A$  for infinitely many values of  $n$ .

*Proof.* Since no square is congruent to 2 (mod 3),  $a_k$  is not a square. For  $\ell \geq 0$ ,  $a_{k+\ell} \equiv 2 \pmod{3} \Rightarrow a_{k+\ell}$  is not a square  $\Rightarrow a_{k+\ell+1} = a_{k+\ell} + 3 \equiv 2 \pmod{3}$ . Thus  $a_k, a_{k+1}, a_{k+2}, \dots$  are all congruent to 2 (mod 3) and  $a_k < a_{k+1} < a_{k+2} < \dots$ . This implies that result.

*Lemma 2.* If  $a_k \not\equiv 2 \pmod{3}$  and  $a_k \geq 9$ , then at least one of  $a_{k+1}, a_{k+2}, a_{k+3}, \dots$  is less than  $a_k$ .

*Proof.* If  $a_k$  is a square, then  $a_{k+1} = \sqrt{a_k} < a_k$ . So we may suppose  $a_k$  is not a square. Consider the next 3 consecutive squares after  $a_k$ :  $(\lfloor \sqrt{a_k} \rfloor + 1)^2$ ,  $(\lfloor \sqrt{a_k} \rfloor + 2)^2$ ,  $(\lfloor \sqrt{a_k} \rfloor + 3)^2$ . They are all less than  $(\sqrt{a_k} + 3)^2$ . One of them is congruent to  $a_k \pmod{3}$ . Let that square be  $a_m$ , where  $m > k$ . Then  $a_{m+1} = \sqrt{a_m} < \sqrt{a_k} + 3 < a_k$  as  $a_k \geq 9$ .

*Lemma 3.*  $a_0 \equiv 0 \pmod{3}$  if and only if  $a_n \equiv 0 \pmod{3}$  for all  $n$ .

*Proof.* If  $a_k \equiv 0 \pmod{3}$ , then either  $a_{k+1} = a_k + 3 \equiv 0 \pmod{3}$ , or  $a_{k+1} = \sqrt{a_k} \equiv 0 \pmod{3}$ , where  $a_k$  is a square. Similarly, the converse is true. Thus by induction, the lemma is proved.

(Case 1).  $a_0 \equiv 0 \pmod{3}$ .

By lemma 3,  $a_n \equiv 0 \pmod{3}$  for all  $n$ . By lemma 2, we can find successively small terms until  $a_k < 9$ . That is  $a_k = 3$  or 6. From then on, the sequence becomes 3, 6, 9, 3,  $\dots$ , thus it is periodic.

(Case 2).  $a_0 \equiv 1 \pmod{3}$ .

Suppose  $a_k \not\equiv 2 \pmod{3}$  for all  $k$ . By lemma 2, we can find successively small terms until there is a term  $a_k < 9$ . By lemma 3,  $a_k \not\equiv 0 \pmod{3}$  as  $a_0 \not\equiv 0 \pmod{3}$ . We must have  $a_k = 2, 4, 5, 7, 8$ . For  $a_k = 2, 5, 8$ , it contradicts the assumption that  $a_k \not\equiv 2 \pmod{3}$ . For  $a_k = 4$  or 7, it eventually gives a term 2. Again, it contradicts the assumption that  $a_k \not\equiv 2 \pmod{3}$ . Thus some  $a_k \equiv 2 \pmod{3}$ , then by lemma 1, no such  $A$  exist.

Thus the answers are all positive multiples of 3.

2. Let  $\mathbb{R}$  be the set of real numbers. Determine all functions  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that, for all real numbers  $x$  and  $y$ ,

$$f(f(x)f(y)) + f(x+y) = f(xy).$$

*Solution by Bryan Wang.* We will show that the only such functions are  $f(x) = 0$ ,  $f(x) = x - 1$  or  $f(x) = -(x - 1)$ . Clearly these functions satisfy the given functional equation:

$$f(f(x)f(y)) + f(x+y) = f(xy). \quad (2.0)$$

Letting  $y = 0$  into (2.0), we get

$$f(f(x)f(0)) + f(x) = f(0). \quad (2.1)$$

Letting  $x = 0$  into (2.1), we get

$$f(f(0)^2) = 0. \quad (2.2)$$

Letting  $xy = x + y \Leftrightarrow (x - 1)(y - 1) = 1$  into (2.0), we get

$$f(f(x)f(y)) = 0. \quad (2.3)$$

From (2.1), if  $f(0) = 0$ , then  $f(x) = 0$  for all  $x \in \mathbb{R}$ , which is a solution.

Next we suppose  $f(0) \neq 0$ . Then for all  $x \neq 1$ , if  $f(x) = 0$ , then by taking  $y = \frac{1}{x-1} + 1$  in (2.3) it gives  $f(0) = 0$ , a contradiction. Thus

$$f(x) = 0 \Rightarrow x = 1. \quad (2.4)$$

Thus, by (2.2), we have  $f(0)^2 = 1$  so that  $f(0) = \pm 1$ .

Suppose  $f(0) = 1$ . If we let  $g(x) = -f(x)$ , then the same equation  $g(g(x)g(y)) + g(x+y) = g(xy)$  is satisfied with  $g(0) = -1$ . So we need only consider the case  $f(0) = -1$  and  $-f$  gives another solution.

From now on, we focus on  $f(0) = -1$ . By (2.2), we have  $f(1) = 0$ . Letting  $x = 1$  and  $y = 1$  in (2.0), we have for all  $x \in \mathbb{R}$ ,

$$f(x+1) = f(x) + 1. \quad (2.5)$$

As  $f(0) = -1$ , (2.1) becomes  $f(-f(x)) = -1 - f(x)$ . Adding this to (2.5), we obtain  $f(x+1) + f(-f(x)) = 0$ , which by (2.5) is equivalent to

$$f(x) + 1 + f(-f(x)) = 0 \quad (2.6)$$

and also to

$$f(x) + f(1 - f(x)) = 0. \quad (2.7)$$

In (2.7), we replace  $x$  by  $1 - f(x)$  to get  $f(1 - f(x)) + f(1 - f(1 - f(x))) = 0$ , which by (2.7) is equivalent to  $f(1 - f(x)) + f(1 + f(x)) = 0$ . By (2.5), this equivalent to

$f(-f(x)) + f(f(x)) = -2$ . By (2.6), this is equivalent to  $-f(x) - 1 + f(f(x)) = -2$ . That is

$$f(f(x)) = f(x) - 1. \quad (2.8)$$

By (2.5),  $f(2) = 1$ . In (2.0), we let  $y = 2$  to get  $f(f(x)f(2)) + f(x + 2) = f(2x)$ . Using (2.5), we get  $f(f(x)) + f(x) + 2 = f(2x)$ . Substituting this into (2.8) to eliminate the term  $f(f(x))$ , we get

$$f(2x) = 2f(x) + 1. \quad (2.9)$$

By (2.5),  $f(-1) = -2$ . In (2.0), let  $y = -1$  and use (2.5) to get  $f(-2f(x)) + f(x) - 1 = f(-x)$ . By (2.9), this is equivalent to  $2f(-f(x)) + 1 + f(x) - 1 = f(-x)$ , which by (2.6) becomes  $2(-f(x) - 1) + 1 + f(x) - 1 = f(-x)$ . That is

$$f(x) + f(-x) = -2. \quad (2.10)$$

Now let's prove that  $f$  is injective. Suppose  $f(a) = f(b)$ . Then by (2.10),  $f(-a) = f(-b)$ . In (2.0), letting  $(x, y) = (a, -b)$  and  $(b, -a)$  respectively, we obtain  $f(a-b) = f(b-a)$ . By (2.10),  $f(a-b) = f(b-a) = -1$ . By (2.5), this gives  $f(a-b+1) = 0$ . By (2.4),  $a-b+1 = 1$  so that  $a = b$ . This proves that  $f$  is injective.

By (2.5) and (2.8),  $f(f(x)) = f(x-1)$ . Using injectivity, we get  $f(x) = x-1$ .

3. A hunter and an invisible rabbit play a game in the Euclidean plane. The rabbit's starting point,  $A_0$ , and the hunter's starting point,  $B_0$ , are the same. After  $n-1$  rounds of the game, the rabbit is at point  $A_{n-1}$  and the hunter is at point  $B_{n-1}$ . In the  $n$ th round of the game, three things occur in order:
- (i) The rabbit moves invisibly to a point  $A_n$  such that the distance between  $A_{n-1}$  and  $A_n$  is exactly 1.
  - (ii) A tracking device reports a point  $P_n$  to the hunter. The only guarantee provided by the tracking device to the hunter is that the distance between  $P_n$  and  $A_n$  is at most 1.
  - (iii) The hunter moves visibly to a point  $B_n$  such that the distance between  $B_{n-1}$  and  $B_n$  is exactly 1.

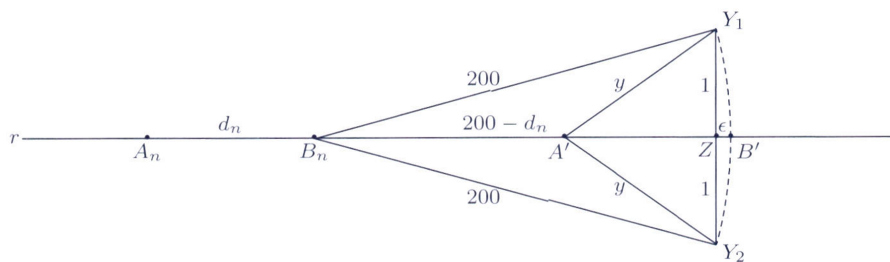
Is it always possible, no matter how the rabbit moves, and no matter what points are reported by the tracking device, for the hunter to choose her moves so that after  $10^9$  rounds she can ensure that the distance between her and the rabbit is at most 100?

*Official Solution.* The answer is No. If the answer were "yes", the hunter would have a strategy that would "work", no matter how the rabbit moved or where the position  $P_n$  reported by tracking device was. We will show the opposite: with bad luck from the positions reported by tracking device, there is no strategy for the hunter that guarantees that the distance stays below 100 in  $10^9$  rounds.

Let  $d_n$  be the distance between the hunter and the rabbit after  $n$  rounds. Of course, if  $d_n \geq 100$  for any  $n < 10^9$ , the rabbit has won - it just needs to move straight away from the hunter, and the distance will be kept at or above 100 thereon.

We will show that, while  $d_n < 100$ , whatever given strategy the hunter follows, the rabbit has a way of increasing  $d_n^2$  by at least  $\frac{1}{2}$  every 200 rounds (as long as the positions reported by the tracking device are lucky enough for the rabbit). This way,  $d_n^2$  will reach  $10^4$  in less than  $2 \cdot 10^4 \cdot 200 = 4 \cdot 10^6 < 10^9$  rounds, and the rabbit wins.

Suppose the hunter is at  $A_n$  and the rabbit is at  $B_n$ . Suppose even that the rabbit *reveals* its position at this moment to the hunter (This allows us to ignore all information from the previous positions reported by the tracking device). Let  $r$  be the line  $A_n B_n$ , and  $Y_1$  and  $Y_2$  be points which are 1 unit away from  $r$  and 200 units away from  $B_n$ , as in the figure.



The rabbit's plan is simply to choose one of the points  $Y_1$  or  $Y_2$  and hop 200 rounds straight towards it. Since all hops stay within 1 distance unit from  $r$ , it is possible that all positions reported by the tracking device stay on  $r$ . In particular, in this case, the hunter has no way of knowing whether the rabbit chose  $Y_1$  or  $Y_2$ .

Looking at such positions reported by the tracking device, what is the hunter going to do? If the hunter's strategy tells him to go 200 rounds straight to the right, he ends up at the point  $A'$  in the figure. Note that the hunter does not have a better alternative! Indeed, after these 200 rounds he will always end up at a point to the left of  $A'$ . If his strategy took him to a point above  $r$ , he would end up even further from  $Y_2$ ; and if his strategy took him below  $r$ , he would end up further from  $Y_1$ . In other words, no matter what strategy the hunter follows, he can never be sure his distance to the rabbit will be less than  $y \stackrel{\text{def}}{=} A'Y_1 = A'Y_2$  after these 200 rounds.

To estimate  $d_n^2$ , we take  $Z$  as the midpoint of the segment  $Y_1 Y_2$ , and  $B'$  the point 200 units to the right of  $B_n$  along  $r$  and define  $\epsilon = ZB'$  (note that  $A'B' = d_n$ ). Then

$$y^2 = 1 + A'Z^2 = 1 + (d_n - \epsilon)^2,$$

where  $\epsilon = 200 - B_n Z = 200 - \sqrt{200^2 - 1} = \frac{1}{200 + \sqrt{200^2 - 1}} > \frac{1}{400}$ .

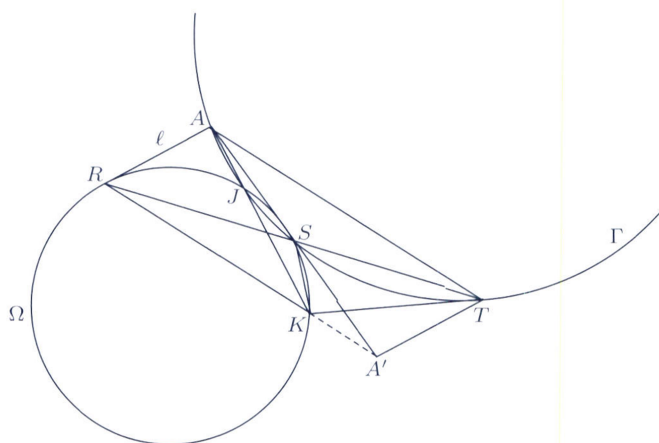
Next we can calculate  $\epsilon$  as follow. Let  $Q$  be the foot of the perpendicular from  $B_n$  onto  $Y_1 B'$ . Then the triangles  $ZY_1 B'$  and  $QB_n Y_1$  are similar. From this, we obtain  $\epsilon^2 + 1 = 400\epsilon$ , so

$$y^2 = d_n^2 - 2\epsilon d_n + \epsilon^2 + 1 = d_n^2 + \epsilon(400 - 2d_n).$$

Since  $\epsilon > \frac{1}{400}$  and we assume  $d_n < 100$ , this shows that  $y^2 > d_n^2 + \frac{1}{2}$ . So, as we claim, with this list of positions reported by the tracking device, no matter what the hunter does, the rabbit might achieve  $d_{n+200}^2 > d_n^2 + \frac{1}{2}$ . The rabbit wins.

4. Let  $R$  and  $S$  be different points on a circle  $\Omega$  such that  $RS$  is not a diameter. Let  $\ell$  be the tangent line to  $\Omega$  at  $R$ . Point  $T$  is such that  $S$  is the midpoint of the line segment  $RT$ . Point  $J$  is chosen on the shorter arc  $RS$  of  $\Omega$  so that the circumcircle  $\Gamma$  of triangle  $JST$  intersects  $\ell$  at two distinct points. Let  $A$  be the common point of  $\Gamma$  and  $\ell$  that is closer to  $R$ . Line  $AJ$  meets  $\Omega$  again at  $K$ . Prove that the line  $KT$  is tangent to  $\Gamma$ .

*Solution by Bryan Wang and Ng Yu Peng.* Extend  $AS$  to  $A'$  so that  $S$  is the midpoint of  $AA'$ . Then  $ARA'T$  is a parallelogram so that  $AT \parallel A'R$ . Also  $\angle SRK = \angle SJK = \angle ATS$  so that  $AT \parallel RK$ . This implies that  $R, K, A'$  are collinear. Thus  $\angle STA' = \angle ART = \angle SKR$  so that  $SKA'T$  are concyclic. Therefore,  $\angle STK = \angle SA'K = \angle SAT$  so that  $KT$  is tangent to  $\Gamma$ .



5. An integer  $N \geq 2$  is given. A collection of  $N(N + 1)$  soccer players, no two of whom are of the same height, stand in a row. Sir Alex wants to remove  $N(N - 1)$  players from this row leaving a new row of  $2N$  players in which the following  $N$  conditions hold:
- (1) no one stands between the two tallest players,
  - (2) no one stands between the third and fourth tallest players,
  - $\vdots$
  - ( $N$ ) no one stands between the two shortest players.

Show that this is always possible.

*Official Solution.* Split the people into  $N$  groups by height: group  $G_1$  has the  $N + 1$  tallest ones, group  $G_2$  has the next  $N + 1$  tallest, and so on, up to group  $G_N$  with the  $N + 1$  shortest people.

Now scan the original row from left to right, stopping as soon as you have scanned two people (consecutively or not) from the same group, say  $G_i$ . Since we have  $N$  groups, this must happen before or at the  $(N + 1)^{\text{th}}$  person of the row. Choose this pair of people, removing all the other people from the same group  $G_i$ , and also all people that have been scanned so far. The only people that could separate this pair's heights were in  $G_i$  (and they are gone); the only people that could separate this pair's positions were already scanned (and they are gone too).

We now left with  $N - 1$  groups (all except  $G_i$ ). Since each of them lost at most one person, each one has at least  $N$  unscanned people left in the row. Repeat the scanning process from left to right, choosing the next two people from the same group, removing this group and everyone scanned up to that point. Once again we end up with two people who are next to each other in the remaining row and whose heights cannot be separated by anyone else who remains (since the rest of their group is gone). After picking these 2 pairs, we still have  $N - 2$  groups with at least  $N - 1$  people each.

If we repeat the scanning process a total of  $N$  times, it is easy to check that we will end up with 2 people from each group, for a total of  $2N$  people remaining. The height order is guaranteed by the grouping, and the scanning construction from left to right guarantees that each pair from a group stand next to each other in the final row.

6. An ordered pair  $(x, y)$  of integers is a primitive point if the greatest common divisor of  $x$  and  $y$  is 1. Given a finite set  $S$  of primitive points, prove that there exist a positive integer  $n$  and integers  $a_0, a_1, \dots, a_n$  such that, for each  $(x, y)$  in  $S$ , we have:

$$a_0x_n + a_1x_{n-1}y + a_2x_{n-2}y^2 + \dots + a_{n-1}xy_{n-1} + a_ny_n = 1.$$

*Official Solution.* Label the primitive points in  $S$  as  $(x_1, y_1), \dots, (x_n, y_n)$ . Firstly, it is enough to construct a homogeneous polynomial  $f(x, y)$  such that  $f(x, y) = \pm 1$  for all  $(x, y) \in S$  because we then have  $f^2(x, y) = 1$  for all  $(x, y) \in S$ . Secondly, if any two of the primitive points  $(x_i, y_i)$  and  $(x_j, y_j)$  lie on the same line through the origin, then  $(x_i, y_i) = (-x_j, -y_j)$  because both of the points are primitive. We then have  $f(x_j, x_j) = \pm f(x_i, y_i)$  whenever  $f$  is homogeneous. Therefore we may assume no two of the points in  $S$  are collinear with the origin by ignoring the extra lattice points. We induct on  $n$  to construct a homogeneous polynomial  $f(x, y)$  such that  $f(x_i, y_i) = 1$  for all  $1 \leq i \leq n$ .

If  $n = 1$ , then because  $x_1, y_1$  are relatively prime, there exist some integers  $a, b$  such that  $ax_1 + by_1 = 1$ . Then  $f(x, y) = ax + by$  is suitable.

If  $n \geq 2$ , we have by induction hypothesis that there exists a homogeneous polynomial  $g(x, y)$  with  $g(x_1, y_1) = \dots = g(x_{n-1}, y_{n-1}) = 1$ . Let  $j = \deg g$ ,

$$g_n(x, y) = \prod_{k=1}^{n-1} (y_kx - x_ky),$$

and  $a_n = g_n(x_n, y_n)$ . By the assumption that no two of the points in  $S$  are collinear with the origin, we know  $a_n \neq 0$ . Let  $c, d$  be integers such that  $cx_n + dy_n = 1$ . we will construct  $f(x, y)$  in the form

$$f(x, y) = g(x, y)^K - C \cdot g_n(x, y) \cdot (cx + dy)^L,$$

where  $K$  and  $L$  are some positive integers  $C$  is some integer. We assume  $L = Kj - n + 1$  so that  $f$  is homogeneous.

Due to  $g(x_1, y_1) = \dots = g(x_{n-1}, y_{n-1}) = 1$  and  $g_n(x_1, y_1) = \dots = g_n(x_{n-1}, y_{n-1}) = 0$ , the property that  $f(x_1, y_1) = \dots = f(x_{n-1}, y_{n-1}) = 1$  is automatically satisfied with any choice of  $K, L$  and  $C$ .

Furthermore,

$$f(x_n, y_n) = g(x_n, y_n)^K - C \cdot g_n(x_n, y_n) \cdot (cx_n + dy_n)^L = g(x_n, y_n)^K - Ca_n.$$

If we have an exponent  $K$  such that  $g(x_n, y_n)^K \equiv 1 \pmod{a_n}$ , then we may choose  $C$  such that  $f(x_n, y_n) = 1$ . we now choose such a  $K$ .

Consider an arbitrary prime divisor  $p$  of  $a_n$ . By

$$p \mid a_n = g_n(x_n, y_n) = \prod_{k=1}^{n-1} (y_k x_n - x_k y_n),$$

there is some  $1 \leq k < n$  such that  $x_k y_n \equiv x_n y_k \pmod{p}$ . We first show that  $x_k x_n$  or  $y_k y_n$  is relatively prime with  $p$ . This is trivial in the case  $x_k y_n \equiv x_n y_k \not\equiv 0 \pmod{p}$ . In the other case, we have  $x_k y_n \equiv x_n y_k \equiv 0 \pmod{p}$ . If say  $p \mid x_k$ , then  $p \nmid y_k$  because  $(x_k, y_k)$  is primitive, so  $p \mid x_n$ ; then  $p \nmid y_n$  because  $(x_n, y_n)$  is primitive. In summary,  $p \mid x_k$  implies  $p \nmid y_k y_n$ . Similarly,  $p \mid y_n$  implies  $p \nmid x_k x_n$ .

By the homogeneity of  $g$  we have the congruences

$$x_k^d \cdot g(x_n, y_n) = g(x_k x_n, x_k y_n) \equiv g(x_k x_n, y_k x_n) = x_n^d \cdot g(x_k, y_k) = x_n^d \pmod{p} \quad (6.1)$$

and

$$y_k^d \cdot g(x_n, y_n) = g(y_k x_n, y_k y_n) \equiv g(x_k y_n, y_k y_n) = y_n^d \cdot g(x_k, y_k) = y_n^d \pmod{p}. \quad (6.2)$$

If  $p \nmid x_k x_n$ , then take the  $(p-1)^{st}$  power of (6.1); otherwise take the  $(p-1)^{st}$  power of (6.2); by Fermat's theorem, in both cases we get

$$g(x_n, y_n)^{p-1} \equiv 1 \pmod{p}.$$

If  $p^\alpha \mid a_n$ , then

$$g(x_n, y_n)^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

which implies that the exponent  $K = n \cdot \varphi(a_n)$ , which is a multiple of all  $p^{\alpha-1}(p-1)$ , is a suitable choice. Here the factor  $n$  is added to ensure  $K \geq n$  so that  $L > 0$ .