Problem 2: Separating Functions

Team: France 2

June 21, 2010

Abstract

For the first question, we show that there exists an integer $f \in \mathbb{N}$ such that for all $a \geq f$, $a \in S$. And, if a sequence of a_1 consecutive integers starting from f is in S, then all integers larger than f are in S.

For the second question, in the case n = 2 : The condition of the question implies that such a polynomial p vanishes for $a_1 = 1$ or $a_2 = 1$. Let $p(X, Y) = (X-1)(Y-1) = XY - X - Y + 1 \in \mathbb{R}[X, Y]$. Then, for every pair of coprime positive integers a_1, a_2, $F(a_1, a_2) = p(a_1, a_2)$ Without loss of generality, we assume $a_1 < a_2$: let $k \in [1, a_1 - 1]$ be the remainder of the division of a_2 by a_1. We will show that with two lemmas:

- $p(a_1, a_2) - 1 \notin S$
- for $0 \leq r < a_1$, there exists $u \in S$ such that $u \leq p(a_1, a_2)$ and $u = r[a_1]$. This clearly implies that, for $0 \leq r < a_1$, $p(a_1, a_2) + r \in S$.

In the case n = 3 after showing that if a_1, a_2 are even and a_3 is odd, then $F(a_1, a_2, a_3)$ is even, we will show that if $d = a_1 \wedge a_2$ we have $F(a_1, a_2, a_3) = dF(\frac{a_1}{d}, \frac{a_2}{d}) + F(d, a_3)$. Indeed, we will see two lemmas:

- $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d \notin S$
- $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 \notin S$

In the fourth question, we will show that F can have only one residue modulo d.

Notation

- $a \wedge b$ means $\gcd(a; b)$
- $a \equiv b[c]$ means $a \equiv b (\mathrm{mod}\ c)$

Question 1

Proposition 1.1

There exists an integer $f \in \mathbb{N}$ such that for all $a \geq f$, $a \in S$.

Proof 1.1

The result is clear for $n = 1$. We shall assume $n \geq 2$ in the following slides. Without a loss of generality, we assume that all the a_k are distinct, then ordered from the smallest to the largest $a_1 < a_2 \ldots < a_n$.

Remark
If a_1 consecutive integers starting from f are in S, all integers larger than f are in S. Indeed, $m \in S$

$$\begin{aligned} &\Rightarrow \quad \exists (x_1, \ldots, x_n) \in \mathbb{N}^n, \quad m = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \\ &\Rightarrow \quad \exists (x_1, \ldots, x_n) \in \mathbb{N}^n, \quad m + a_1 = a_1(x_1 + 1) + \ldots + a_n x_n \\ &\Rightarrow \quad m + a_1 \in S \end{aligned}$$

Proposition 1.2

Therefore, we shall prove that the existence of $f_0 \in N$ such that

$$\{f_0, f_0 + 1, \ldots, f_0 + a_1 - 1\} \in S.$$

Proof 1.2

From Bezout identity, there exists $(b_1, b_2, \ldots, b_3) \in \mathbb{Z}^n$ such that

$$a_1 b_1 + a_2 b_2 + \ldots + a_n b_n = 1.$$

Let $B = \min_k |b_k| > 0$ and consider $f_0 = a_1 B \left(\sum_{k=1}^{n} a_k \right) \geq 0$.
Thus, for all $j \in 0, a_1 - 1$,

$$\begin{aligned} f_0 + j &= a_1 B. \sum_{k=1}^{n} (a_k) + j \sum_{k=1}^{n} (a_k b_k) \\ &= \sum_{k=1}^{n} (B a_1 + j b_k) a_k. \end{aligned}$$

We check that, for all $j \in 0, a_1 - 1$, $x_j \geq 0$ since $j < a_1$ and $b_i \geqslant -B$.

Question 2

The condition of the question implies that such a polynomial p vanishes for $a_1 = 1$ or $a_2 = 1$.
Let $p(X, Y) = (X - 1)(Y - 1) = XY - X - Y + 1 \in \mathbb{R}[X]$. Then, for every pair of coprime positive integers a_1, a_2, $F(a_1, a_2) = p(a_1, a_2)$ Without a loss of generality, we assume $a_1 < a_2$: let $k \in 1, a_1 - 1$ be the remainder of the division of a_2 by a_1 (therefore $a_2 = k[a_1]$).

Lemma 2.1

$p(a_1, a_2) - 1 = (a_1 - 1)a_2 - a_1 \notin S$.

Proof 2.1

Assume that $(a_1 - 1)a_2 - a_1 \in S$, i.e.

$$\exists (x, y) \in \mathbb{N}^2, \qquad (a_1 - 1)a_2 - a_1 = xa_1 + ya_2.$$

Then

$$\begin{aligned} (a_1 - 1)a_2 - a_1 &\equiv (a_1 - 1)k[a_1] \\ xa_1 + ya_2 &\equiv ky[a_1]. \end{aligned}$$

so, $ky = k(a_1 - 1)[a_1]$. Furthermore, $k \wedge a_1 = 1$ (since $a_1 \wedge a_2 = 1$), so $y = a_1 - 1[a_1]$. Since $y \geq 0$, this equality entails $y \geq a_1 - 1$ and then $xa_1 + ya_2 \geq a_1 - 1)a_2$ ($x \geq 0$, $a_1 > 0$ and $a_2 > 0$). As a consequence, $(a_1 - 1)a_2 > (a_1 - 1)a_2 - a_1$: contradiction.

Lemma 2.2

For all $r \in 0, a_1 - 1$, there exists $y \in 0, a_1 - 1$ such that

$$ky = r[a_1].$$

In other words, $\left\{ \begin{array}{ccc} \mathbb{Z}/a_1\mathbb{Z} & \to & \mathbb{Z}/a_1\mathbb{Z} \\ y & \mapsto & ky \end{array} \right.$ is a bijection.

Proof 2.2
Consider $y, z \in 0, a_1 - 1$, such that $ky = kz[a_1]$. Then

$$k(y - z) = 0[a_1].$$

Since $k \wedge a_1 = 1$, $y - z = 0[a_1]$ thus $y = z$.

Lemma 2.3

For $0 \leq r < a_1$, there exists $u \in S$ such that $u \leq p(a_1, a_2)$ and $u = r[a_1]$.

Proof 2.3

Let $r \in 0, a_1 - 1$ and $y \in 0, a_1 - 1$ such that $ky = r[a_1]$ (the existence has been proved in the preceding lemma). Then

- $0a_1 + ya_2 \in S$,
- $0a_1 + ya_2 \leq (a_1 - 1)a_2 \leq p(a_1, a_2)$,
- $0a_1 + ya_2 = ky[a_1] = r[a_1]$.

Question 3

Partie A

Lemma 3.1

Let $(x, y, z) \in \mathbb{N}^3$.
If a_1, a_2 are even, a_3 is odd and $xa_1 + ya_2 + za_3 \in S$ is odd, then $z \geq 1$.

Proof 3.1

Since $f = xa_1 + ya_2 + za_3$ is odd and $xa_1 + ya_2$ is even, za_3 is odd, so z is odd and $z \geq 1$.

Proposition 3.1

If a_1, a_2 are even and a_3 is odd, then $F(a_1, a_2, a_3)$ is even.

Proof 3.2

Let us assume $F = F(a_1, a_2, a_3)$ odd. The integer $F + (a_3 - 1)$ is odd and greater than F so

$$\exists (X, Y, Z) \in \mathbb{N}^3, \qquad F = Xa_1 + Ya_2 + Za_3.$$

We deduce from the preceding lemma that $Z \geq 1$.
Therefore $(X, Y, (Z - 1)) \in \mathbb{N}^3$, so $Xa_1 + Ya_2 + (Z - 1)a_3 \in S$ and smaller than F: contradiction.

Lemma 3.2

Let $d = a_1 \wedge a_2$.
Forall $f \in S$, there exists $(x, y, z) \in \mathbb{N} \times \mathbb{N} \times 0, d - 1$ such that

$$f = xa_1 + ya_2 + za_3.$$

Proof 3.3

Since $f \in S$, there exists $(x, y, z) \in \mathbb{N}^3$ such that

$$f = xa_1 + ya_2 + za_3 = d\left(\frac{x}{d}a_1 + \frac{y}{d}a_2\right) + za_3.$$

Let $z = qd + r$ with $r \in 1, d-1$, the euclidean division of z by d.
Since $a_3 \geq F(\frac{a_1}{d}, \frac{a_2}{d})$, there exists $(u, v) \in \mathbb{N}^2$ such that

$$a_3 = u\frac{a_1}{d} + v\frac{a_2}{d}.$$

Combining these equations, we obtain

$$f = (x + qu)a_1 + (y + qv)a_2 + ra_3.$$

Partie B

Proposition 3.2
Let $d = a_1 \wedge a_2$.

$$F(a_1, a_2, a_3) = dF(\frac{a_1}{d}, \frac{a_2}{d}) + F(d, a_3).$$

Lemma 3.3
$dF(\frac{a_1}{d}, \frac{a_2}{d}) - d \notin S$

Proof 3.4

Let us assume $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d \in S$, i.e. there exists $(x', y', z') \in \mathbb{N} \times \mathbb{N} \times 0, d-1$ such that

$$dF(\frac{a_1}{d}, \frac{a_2}{d}) - d = x'a_1 + y'a_2 + z'a_3.$$

Reducing modulo d, we obtain $z'a_3 = 0[d]$. But $a_3 \wedge d = 1$ and $z' \in 0, d-1$, so $z' = 0$.

Therefore, $x'\frac{a_1}{d} + y'\frac{a_2}{d} = F(\frac{a_1}{d}, \frac{a_2}{d}) - 1$: contradiction!

As a consequence, $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d \notin S$.

Lemma 3.4
of $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 \notin S$

Proof 3.5

Let us assume $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 \in S$, i.e. there exists $(x', y', z') \in \mathbb{N} \times \mathbb{N} \times 0, d-1$ such that

$$dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 = x'a_1 + y'a_2 + z'a_3.$$

As before, we obtain that $z' = d-1$ by reducing modulo d and using $d \wedge a_3 = 1$.
Therefore, $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d = x'a_1 + y'a_2 \in S$: contradiction.
As a consequence, $dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 \notin S$

Proof 3.6 : proof of the proposition 3.2

Using question 2, we just showed that

$$\begin{aligned} F(a_1, a_2, a_3) &\geq dF(\frac{a_1}{d}, \frac{a_2}{d}) - d + (d-1)a_3 + 1 \\ &\geq dF(\frac{a_1}{d}, \frac{a_2}{d}) + F(d, a_3). \end{aligned}$$

Moreover, forall $f = dF(\frac{a_1}{d}, \frac{a_2}{d}) + r$ with $r \geq F(d, a_3)$, there exists

- $(u, z) \in \mathbb{N}^2$ such that $ud + za_3 = r$ since $r \geq F(d, a_3)$;
- $(x, y) \in \mathbb{N}^2$ such that $x\frac{a_1}{d} + y\frac{a_2}{d} = F(\frac{a_1}{d}, \frac{a_2}{d}) + r$.

Then, $f = xa_1 + ya_2 + za_3 \in S$.
In conclusion,

$$F(a_1, a_2, a_3) = dF(\frac{a_1}{d}, \frac{a_2}{d}) + F(d, a_3).$$

Question 4

Lemma 4.1
$f \in S$

$$f \equiv 0[d] \Leftrightarrow x_n \equiv 0[d]$$

Proof 4.1
By definition,

$$\exists (x_1, \ldots, x_n) \in \mathbb{N}^n, \quad f = a_1x_1 + a_2x_2 + \ldots + a_nx_n$$
$$sof \equiv a_nx_n[d]$$

It is trivial to say that :
$x_n \equiv 0[d] \Rightarrow f \equiv 0[d]$
We will show the reverse by using Gauss theorem :
$f \equiv 0[d] \Leftrightarrow a_nx_n \equiv 0 \times a_n[d] \Leftrightarrow x_n \equiv 0[d]$

In conclusion,

$$f \equiv 0[d] \Leftrightarrow x_n \equiv 0[d]$$

Proposition 4.2
If d divide $a_1, ..., a_{n-1}$, also $F \equiv 1 - a_n[d]$

Proof 4.2
We have $F + a_n - 1 \geq F$, so $\exists(x_1, \ldots, x_n) \in \mathbb{N}^n$, such that $F + a_n - 1 = a_1X_1 + a_2X_2 + \ldots + a_nX_n$
So, $F + a_n - 1 \in S$
If X_n is not congruent 0 modulo d, $X_n \neq 0$, so X_n 1
Let be $X_n - 1 \in \mathbb{N}$, $a_1X_1 + a_2X_2 + \ldots + a_n(X_n - 1) \in S$ so $F - 1 \in S$ It is a contradiction
So, $X_n \equiv 0[d]$ so $F + a_n - 1 \equiv 0[d]$
In conclusion $F \equiv 1 - a_n[d]$

Question 5

We can easily prove in a similar way (question 3.b)) :
Proposition 5. Let n positive integers $a_1, \ldots, a_n$ which are coprime and consider $d = a_1 \wedge a_2 \wedge \ldots \wedge a_{n-1}$.

$$F(a_1, \ldots, a_n) = dF(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}) + F(d, a_n).$$