Problem 2: Separating Functions

Team Germany

Abstract

In our solution to this problem, we first solve Problem 2.2 by stating that $F(a_1, a_2)$ exists and equals $(a_1 - 1)(a_2 - 1)$ for any two coprime integers a_1 and a_2, and then use this to prove that $F(a_1, \dots, a_n)$ exists for any coprime integers $a_1, \dots, a_n$.

We then prove some facts about separating functions and parity, generalizing the result of Problem 2.3.a. In Problem 2.5, we generalize the statement of problem 2.3.a: If $a_1, \dots, a_n$ are coprime and $d = \gcd(a_1, \dots, a_{n-1})$, then $F(a_1, \dots, a_n) \equiv 1 - a_n \mod d$.

We also proved the formula stated in Problem 2.3.b; the "natural" generalization of this formula for higher values of n also holds, as was proved by us in Theorem 3.

We denote by $\mathbb{N}$ the set of nonnegative integers (this notation was also used in the problem statement).
We begin by solving Problem 2.2, as we will use results from this problem in Problem 2.1. In the two first problems, we first have to show that $F(a_1, a_2)$ is well-defined. To simplify the notation of the proofs, we add a number ∞ to the integers that has the property that $z < \infty$ for any integer z and that the sum or the product of ∞ with any positive integer yields ∞ again. For any n coprime integers $a_1, \dots, a_n$, we then set $F(a_1, \dots, a_n) = \infty$ if there is no number f such that any integer which is greater than f can be represented as a sum $x_1a_1 + \dots + x_na_n$ with nonnegative integers $x_1, \dots, x_n$, and if there are such numbers, then we declare $F(a_1, \dots, a_n)$ to be the minimal such number (in this case, our definition coincides with the original definition). Our goal is of course to show that $F(a_1, \dots, a_n) < \infty$ for any coprime integers $a_1, \dots, a_n$.

Problem 2.2

Answer: For every pair (a_1, a_2) of coprime positive integers, we have

$$F(a_1, a_2) = (a_1 - 1)(a_2 - 1) = a_1a_2 - a_1 - a_2 + 1.$$

Proof. Let a_1 and a_2 be coprime, and let $S = \{x_1a_1 + x_2a_2; x_1, x_2 \in \mathbb{N}\}$. We show that $a \in S$ for every $a \geq (a_1 - 1)(a_2 - 1)$. This shows that $F(a_1, a_2) \leq (a_1 - 1)(a_2 - 1)$, so in particular, $F(a_1, a_2) < \infty$. Let $a \geq (a_1 - 1)(a_2 - 1)$. As a_1 and a_2 are coprime, there exist integers x_1 and x_2 such that $x_1a_1 + x_2a_2 = a$ (this is a well-known fact, sometimes called the lemma of Bézout). Then for every integer k, we also have $(x_1 + ka_2)a_1 + (x_2 - ka)a_2 = a$, so we can assume that $0 \leq x_1 \leq a_2 - 1$ by finding a suitable value for k. It follows that $x_1a_1 \leq a_1a_2 - a_1$, so

$$x_2a_2 = a - x_1a_1 \geq a_1a_2 - a_1 - a_2 + 1 - a_1a_2 + a_1 = -a_2 + 1 > -a_2$$

and thus $x_2 > -1$, i.e. $x_2 \geq 0$.
It now remains to show that $F(a_1, a_2) \geq (a_1 - 1)(a_2 - 1)$, which is equivalent to showing that $(a_1 - 1)(a_2 - 1) - 1 \notin S$. Note that $(a_1 - 1)(a_2 - 1) - 1 = a_1a_2 - a_1 - a_2$: Suppose that

$$a_1a_2 - a_1 - a_2 = x_1a_1 + x_2a_2$$

with $x_1, x_2 \geq 0$. We get that $a_2(x_2 + 1) = a_1(a_2 - 1 - x_1)$ is divisible by a_1, and as a_1 and a_2 are coprime, it follows that a_1 divides $x_2 + 1$. As $x_2 + 1 > 0$, we get $x_2 + 1 \geq a_1$, or $x_1 \geq a_1 - 1$. Similarly, $x_2 \geq a_2 - 1$. Thus,

$$x_1a_1 + x_2a_2 \geq (a_2 - 1)a_1 + (a_1 - 1)a_2 = a_1a_2 - a_1 - a_2 + a_1a_2 > a_1a_2 - a_1 - a_2,$$

contradiction! □

Problem 2.1

We prove the claim in the statement of the theorem by proving the following lemma, which will also help us in Problem 2.3.b:

Lemma 1. If $a_1, \dots, a_n$ are coprime integers, and $d = \gcd(a_1, \dots, a_{n-1})$, then d and a_n are coprime and

$$F(a_1, \dots, a_n) \le d\, F(\frac{a_1}{d}, \dots, \frac{a_{n-1}}{d}) + F(d, a_n).$$

Proof. It is obvious that d and a_n have to be coprime, as a common divisor of d and a_n divides all the a_i and thus $\gcd(a_1, \dots, a_n) = 1$.
By Problem 2.2, we get that $F(d, a_n) < \infty$. If $F(a_1/d, \dots, a_{n-1}/d) = \infty$, then we are done. So suppose that $F(a_1/d, \dots, a_{n-1}/d) < \infty$.
Now, let $a \ge dF(a_1/d, \dots, a_{n-1}/d)+F(a_n, d)$. Then $a-dF(a_1/d, \dots, a_{n-1}/d) \ge F(a_n, d)$, so there are $x_n, x \in \mathbb{N}$ such that $a - dF(a_1/d, \dots, a_{n-1}/d) = xd + x_n a_n$. Now, as $x \ge 0$, we can find nonnegative integers $x_1, \dots, x_{n-1}$ such that

$$x_1 \cdot \frac{a_1}{d} + \ldots + x_n \cdot \frac{a_{n-1}}{d} = F(a_1/d, \dots, a_{n-1}/d) + x,$$

and then we have

$$\begin{aligned} a &= dF(a_1/d, \dots, a_{n-1}/d) + xd + x_n a_n \\ &= d \cdot \left(\frac{a_1}{d} + \ldots + x_n \cdot \frac{a_{n-1}}{d}\right) + x_n a_n \\ &= x_1 a_1 + \ldots + x_n a_n. \end{aligned}$$

Thus, every number which is at least $dF(a_1/d, \dots, a_{n-1}/d)+F(a_n, d)$ can be represented as a weighted sum of the a_i as required, and thus $F(a_1, \dots, a_n) \le dF(a_1/d, \dots, a_{n-1}/d) + F(a_n, d)$. □

Note that we have already shown in Problem 2.2 that $F(a_1, a_2) < \infty$ for any two coprime numbers a_1 and a_2. Thus, it follows easily by induction on n that $F(a_1, \dots, a_n) < \infty$ for any n coprime integers $a_1, \dots, a_n$.

Problems 2.3.a and 2.4

The following theorem is a generalization of the result of Problem 3.b:

Theorem 1. Suppose that among the n coprime integers $a_1, \ldots, a_n$, at most one is odd. Then $F(a_1, \ldots, a_n)$ is even.

Proof. Suppose that $a_1, \ldots, a_{n-1}$ are even. Then a_n has to be odd as the integers are coprime. As $a_n - 1 \geq 0$, there are nonnegative integers $x_1, \ldots, x_n$ such that

$$F(a_1, \ldots, a_n) + a_n - 1 = x_1 a_1 + \ldots + x_n a_n.$$

Now, suppose that $F(a_1, \ldots, a_n)$ is odd. As $a_n - 1$ is even, $F(a_1, \ldots, a_n)$ will also be odd, so as $2 \mid a_1, \ldots, a_n$, $x_n a_n$ must be odd. It follows that x_n is odd, hence $x_n \geq 1$ and

$$F(a_1, \ldots, a_n) - 1 = x_1 a_1 + \ldots + x_{n-1} a_{n-1} + (x_n - 1) a_n$$

can be represented as a weighted sum of the a_i with nonnegative integral weights, contradicting the definition of $F(a_1, \ldots, a_n)$. $\square$

Theorem 1 cannot be improved: For every integer $n > 2$, there are coprime integers $a_1, a_2, \ldots, a_n$ out of which exactly two are odd such that $F(a_1, \ldots, a_n)$ is odd. More generally, for any number k with $2 \leq k \leq n$, there are numbers $a_1, a_2, \ldots, a_n$ out of which exactly k are odd such that $F(a_1, \ldots, a_n)$ is odd, and there are also coprime integers $a_1, \ldots, a_n$ out of which exactly k are odd such that $F(a_1, \ldots, a_n)$ is even.
The second statement is very easy to prove: Just note that for two coprime numbers a_1 and a_2, at least one will be odd, so $F(a_1, a_2) = (a_1 - 1)(a_2 - 1)$ will always be even. By choosing a_1 and a_2 with suitable parity and then choosing integers $a_3, \ldots, a_n > F(a_1, a_2)$ with suitable parities, we will get a tuple $(a_1, \ldots, a_n)$ with an arbitrary distribution of even and odd numbers and such that $F(a_1, \ldots, a_n)$ is odd.
For the first statement, we can't begin with two arbitrary numbers a_1 and a_2, so we have to give starting triples (a_1, a_2, a_3) with exactly three and exactly two odd numbers such that $F(a_1, a_2, a_3)$ is odd. But this is also easy: We have $F(3, 7, 11) = 9$ and $F(3, 4, 5) = 3$.

Problem 2.5

There is a simple generalization of Theorem 1:

Theorem 2. Let $a_1, \ldots, a_n$ be coprime integers, and let $d = \gcd(a_1, \ldots, a_{n-1})$. Then $F(a_1, \ldots, a_n) \equiv 1 - a_n \mod d$.

Proof. The proof is the same as for Theorem 1: Consider the number $F(a_1, \ldots, a_n) + a_n - 1$. This number has a representation

$$F(a_1, \ldots, a_n) + a_n - 1 = x_1 a_1 + \ldots + x_n a_n$$

with $x_i \geq 0$ for all i. Note that this implies

$$F(a_1, \ldots, a_n) - 1 = x_1 a_1 + \ldots + x_{n-1} a_{n-1} + (x_n - 1) a_n$$

and so $x_n - 1 < 0$, i.e. $x_n = 0$, by definition of $F(a_1, \ldots, a_n)$. It follows that d divides $F(a_1, \ldots, a_n) + a_n - 1$, implying that $F(a_1, \ldots, a_n) \equiv 1 - a_n \mod d$. □

Problem 2.3.b

We will show a more general theorem from which the solution of Problem 2.3.b can be obtained by setting $n = 3$:

Theorem 3. Suppose that $a_1, \ldots, a_n$ are coprime integers, $d = \gcd(a_1, \ldots, a_{n-1})$ and $a_n \geq F(a_1/d, \ldots, a_{n-1}/d)$. Then we have

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

Proof. We have already proved in Lemma 1 that

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

Thus, it remains to prove that $d\, F(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}) + F(d, a_n) - 1$ can't be written as a sum $x_1 a_1 + \ldots + x_n a_n$ with nonnegative integers x_i. Suppose that

$$d\, F(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}) + F(d, a_n) - 1 = x_1 a_1 + \ldots + x_n a_n.$$

By Problem 2.2, we have $F(a_n, d) = a_n d - a_n - d + 1 \equiv -a_n + 1 \mod d$. As d divides $a_1, a_2, \ldots, a_{n-1}$, we get that $x_n a_n \equiv -a_n \mod d$ and thus, as d and a_n are coprime, $x_n \equiv d - 1 \mod d$.
If $x_n = d - 1$, then it follows that

$$\begin{aligned} d\left(x_1 \cdot \frac{a_1}{d} + \ldots + x_{n-1} \cdot \frac{a_{n-1}}{d}\right) &= x_1 a_1 + \ldots + x_{n-1} a_{n-1} \\ &= dF(a_1/d, \ldots, a_{n-1}/d) + (a_n - 1)(d - 1) - 1 - (d - 1) a_n \\ &= d\left(F(a_1/d, \ldots, a_{n-1}/d) - 1\right) \end{aligned}$$

and thus $x_1 \cdot \frac{a_1}{d} + \ldots + x_{n-1} \cdot \frac{a_{n-1}}{d} = F(a_1/d, \ldots, a_{n-1}/d) - 1$, contradicting the definition of $F(a_1/d, \ldots, a_{n-1}/d)$.
Otherwise, we must have $x_n \geq 2d - 1$, yielding

$$\begin{aligned} x_1 a_1 + \ldots + x_{n-1} a_{n-1} &\leq dF(a_1/d, \ldots, a_{n-1}/d) + (a_n - 1)(d-1) - 1 - (2d-1)a_n \\ &= dF(a_1/d, \ldots, a_{n-1}/d) - da_n - d \\ &= d\left(F(a_1/d, \ldots, a_{n-1}/d) - a_n\right) - d \leq -d < 0, \end{aligned}$$

contradiction! □