Problem 2. **Separating Functions**

France 1 — ITYM 2010

Abstract

In this problem, we will first prove an important lemma that shows that it is enough to obtain all residues modulo a_1 by positive combinations of a_1, a_2, ..., a_n to be able to write all sufficiently large integers by positive combinations. Besides, this also shows our strategy: the "last residue" argument will be very much used.

Then we will answer to all the questions in order.

In the first question, we proceed by induction on n to obtain the desired result.

In the second question, which is our base step for the induction in question 1, we look modulo a_2. Using the lemma and the fact that a_1 is a generator modulo a_2, we obtain $F(a_1, a_2) = (a_1 - 1)(a_2 - 1)$.

In the third question:

a We consider $2k + 1$, the smallest odd integer such that from this integer on, we can get all odd integers by positive combination of a_1, a_2 and a_3. Then we show that $2k$ is a positive combination of a_1, a_2 and a_3 and conclude.

b Given that a_3 is very large compared to the other two, we can give an explicit procedure to obtain all residues modulo a_1: we use a_2 to obtain multiples of d, and a_3 only to obtain the residues modulo d. Then we show that the bound we obtained by this method is the minimum one.

The fourth and fifth questions are extensions of the results of question 3 to all n, in fact noticing that the methods we use can be generalized.

Finally, we propose a further result in relation to the structure of positive combinations. We prove that, if S is a non-empty set included in $\mathbb{N}$, stable by addition, then we can find a positive integer K such that all sufficiently large elements of S are exactly the multiples of K. Furthermore, we show that $K = pgcd(a_1, a_2, \dots)$. This is in analogy with the Bezout property in $\mathbb{Z}$.

Introduction

Definition 1. *A* positive combination *of $a_1, \ldots, a_n$ is a number of the form $\sum_{i=1}^{n} n_i a_i$ where $n_i \in \mathbb{N}$.*

In this problem, we will use this

Lemma 1. *If we can obtain all residues modulo a_1 by positive combinations of the positive integers $a_1, a_2, \ldots, a_n$, then there is $N > 0$ such that, $\forall n > N$, n is a positive combination of $a_1, \ldots, a_n$.*

Proof. Let $x_1, \ldots, x_{a_1}$ be positive combinations of $a_1, \ldots, a_n$ such that $x_i \equiv i \mod a_1$. Let $N = \max(x_1, \ldots, x_{a_1})$. Then $\forall n > N$, $n - x_{(n \mod a_1)} > 0$ and $n - x_{(n \mod a_1)}$ is a multiple of a_1. Therefore $n = (n - x_{(n \mod a_1)}) + x_{(n \mod a_1)}$ is a positive combination of $a_1, \ldots, a_n$. □

We see that in fact the proof gives more: one can choose the maximum of the given residues as the bound.

1st question

We proceed by induction. The initial step, for $n = 2$ will be proven in question 2, when we find explicitly the values for $F(a_1, a_2)$.

Induction step:

Let $d = gcd(a_1, \ldots, a_{n-1})$. We have $gcd(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}) = 1$.

By the induction hypothesis, there is $N > 0$ such that every $n > N$ is a positive combination of $\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}$. Therefore, every multiple of d bigger than Nd is a positive combination of $a_1, \ldots, a_{n-1}$. Furthermore, $gcd(a_1, \ldots, a_n) = 1$, so $gcd(d, a_n) = 1$. Therefore d is an additive generator modulo a_n and we can consequently obtain every residue modulo a_n with positive combinations of $a_1, \ldots, a_n$ and the conclusion follows by lemma 1.

2nd question

We have $gcd(a_1, a_2) = 1$. Then a_1 is an additive generator modulo a_2. Therefore, we can define r_i which is the smallest integer such that r_i is a positive combination of a_1 and a_2 and such that $r_i = i$ modulo a_2.

Let r be the maximum of the r_i ($i \in \{0, 1, \ldots, a_2 - 1\}$). We have $r = na_1 + ma_2$. So $r - ma_2 = na_1 > 0$, because $r_0 = 0$ and then r is not a multiple of a_2, and $r - ma_2 = r$ modulo a_2. By definition of r, we have $r - ma_2 \geq r$ so $m = 0$. Then we have $r = (a_2 - 1)a_1$: to obtain all a_2 residues modulo a_2 with multiples of a_1, the smallest we can take are $0 \times a_1$, a_1, $2a_1$, $\ldots$, $(a_2 - 1)a_1$.

Now, remark that $r - a_2$ is not a positive combination of a_1 and a_2, because $r - a_2 < r$ and $r - a_2 \equiv r \mod a_2$, which would contradict the definition of r. But we can obtain $r-1, r-2, \ldots, r-(a_2-1)$. Indeed, if $j \in \{1, \ldots, a_2 - 1\}$, $r - j \equiv r_{(r-j \mod a_2)} \mod a_2$.

Moreover, $r - j \geq r_{(r-j \mod a_2)}$, because if $r - j < r_{(r-j \mod a_2)}$ then $r_{(r-j \mod a_2)} \geq a_2 + r - j > r$, contradiction. Therefore $r - j - r_{(r-j \mod a_2)} = ka_2$, where $k \geq 0$, and then $r - j = r_{(r-j \mod a_2)} + ka_2$ is a positive combination of a_1 and a_2. Therefore $F(a_1, a_2) = r - (a_2 - 1) = (a_1 - 1)(a_2 - 1)$.

3rd question

a)

WLOG, we consider that a_1 and a_2 are even, and a_3 is necessarily odd. Consider $2k+1$ the smallest odd positive integer such that we can obtain every greater odd integer with a positive combination of a_1, a_2 and a_3.

We write: $2k + 1 = xa_1 + ya_2 + za_3$, where z is greater than 0. As z must be odd, $z \geq 1$.

As a consequence, $2k + 1 - a_3 = xa_1 + ya_2 + (z - 1)a_3$ is a positive combination of a_1, a_2 and a_3, since $z - 1$ is a nonnegative integer. Similarly, if m is odd and greater than $2k + 1$, then the even integer $m - a_3$ can be obtained by a linear combination of a_1, a_2 and a_3.

Therefore we can obtain by a linear combination of a_1, a_2 and a_3 all even integers $\geq 2k + 1 - a_3$ (because $2k + 1 - a_3 + 2m = (2(k + m) + 1) - a_3$), and $2k + 1 - a_3 \leq 2k$. In particular, we can obtain $2k$ but we can't obtain $2k - 1$. Then $F(a_1, a_2, a_3) = 2k$ is even.

b)

We have to obtain all residues modulo a_1 with positive combination of a_2 and a_3.

We can obtain all residues modulo a_1 by the following method: we obtain all multiples of d modulo a_1 using 0, a_2, $2a_2$, ..., $(\frac{a_1}{d} - 1)a_2$, and we obtain the residues modulo d with 0, a_3, $2a_3$, ..., $(d-1)a_3$. (Just imagine a partition by blocs of length d modulo a_1). With this method, the last class modulo a_1 is obtained by the integer $(d - 1)a_3 + (\frac{a_1}{d} - 1)a_2$.

Like in question 1, we can then obtain every integer $\geq (d-1)a_3 + (\frac{a_1}{d} - 1)a_2 - (a_1 - 1)$ by positive combinations of a_1, a_2 and a_3. So we have $F(a_1, a_2, a_3) \leq (d - 1)a_3 + (\frac{a_1}{d} - 1)a_2 - (a_1 - 1)$.

Let's show that we have equality. We have to obtain the class $(d - 1)a_3 + (\frac{a_1}{d} - 1)a_2$ modulo a_1 with a positive combination of a_2 and a_3, as adding a_1 will only increase it. Therefore, let m and n be such that $ma_3 + na_2 = (d - 1)a_3 + (\frac{a_1}{d} - 1)a_2$ modulo a_1. We have, modulo d, $ma_3 = (d - 1)a_3$, so $m = kd + (d - 1)$, where $k \geq 0$ (because $gcd(a_3, d) = 1$).

And we know that $a_3 \geq F\left(\frac{a_1}{d}, \frac{a_2}{d}\right)$. Therefore there is $A, B \geq 0$ such that $da_3 = Aa_1 + Ba_2$. But we have $ma_3 + na_2 \equiv (d - 1)\, a_3 + \left(\frac{a_1}{d} - 1\right) a_2 \mod a_1$, so $k\,(Aa_1 + Ba_2) + na_2 \equiv \left(\frac{a_1}{d} - 1\right) a_2 \mod a_1$. Therefore, $a_2\,(kB + n) \equiv \left(\frac{a_1}{d} - 1\right) a_2 \mod a_1$, and then $kB + n = \frac{a_1}{d} - 1$ modulo $\frac{a_1}{d}$. So $kB + n \geq \frac{a_1}{d} - 1$, as it must be non-negative. Therefore $k(Aa_1 + Ba_2) + na_2 \geq \left(\frac{a_1}{d} - 1\right) a_2$.

Plugging back, $ma_3 + na_2 \geq \left(\frac{a_1}{d} - 1\right) a_2 + (d-1)a_3$ and finally

$$F(a_1, a_2, a_3) \geq \left(\frac{a_1}{d} - 1\right) a_2 + (d-1)a_3 - (a_1 - 1). \qquad \square$$

4th Question

We consider the case when a_1, a_2, ..., a_{n-1} are even, and a_n is necessarily odd. We obtain the same result as for 3.a, with the same proof: just remplace the expression $xa_1 + ya_2 + za_3$ by

$$x_1a_1 + x_2a_2 + \cdots + x_na_n,$$

where the x_i are positive integers, and x_n is strictly positive. Considering now the integer $2k+1$ as before, we get that $2k$ will be a positive combination, but not $2k-1$, and we're done.

5th Question

We consider the case when we have n positive integers a_1, a_2, ..., a_n with $n \geq 3$ and there is an integer $p \geq 2$ such that

$$gcd(a_1, a_2, \ldots, a_{n-1}) = p.$$

By Lemma 1, to obtain all sufficiently large integers by positive combinations of a_1, a_2, $\ldots a_n$, we must obtain all residues modulo p, and then by question 2 for $\frac{a_i}{p}$, this is a sufficient condition.

Suppose now, in analogy to question 3b, that

$$a_n \geq s = F\left(\frac{a_1}{p}, \frac{a_2}{p}, \ldots \frac{a_{n-1}}{p}\right),$$

so that a_n is not useful for generating multiples of p, but only its residues. We obtain the last residue R modulo p with $(p-1)a_n$.

Then ps is the smallest integer such that we can get all greater multiples of p by a positive combination of $a_1, a_2, \ldots a_{n-1}$. We then have, using the same arguments from question 3b:

$ps + (p-1)a_n$	is the smallest integer such that we can get all greater integers $\equiv R \pmod{d}$
$ps + (p-1)a_n - p$	is the greatest integer that we can't obtain by a positive combination of a_1, a_2, $\ldots a_n$
then $F(a_1, a_2, \ldots, a_n)$	$= ps + (p-1)a_n - p + 1$
that is $F(a_1, a_2, \ldots, a_n)$	$= pF(\frac{a_1}{p}, \ldots, \frac{a_{n-1}}{d}) + F(p, a_n)$.

Further results

We make a first generalization:

Proposition 1. *If S is a non-empty set included in $\mathbb{N}$, stable by addition, then we can find positive integers K and m such that all elements of S greater than m are exactly the multiples of K greater than m.*

This is analogous to the statement of Bézout's Theorem, in which we restrict ourselves to positive numbers.

Proof. If $S = \{0\}$, the property is obvious.

Else, let a_1, a_2, ..., a_{n-1}, a_n, a_{n+1}, ..., be the strictly positive elements of S in growing order. Put $d_n = gcd(a_1, a_2, \ldots, a_{n-1}, a_n) \geq 1$. The sequence (d_n) is decreasing, because for all integers a_1, a_2, ..., a_{n-1}, a_n, we have:

$$gcd(a_1, a_2, \ldots, a_{n-1}, a_n) \leq gcd(a_1, a_2, \ldots, a_{n-2}, a_{n-1})$$

with equality if and only if a_n is a multiple of $gcd(a_1, a_2, \ldots, a_{n-2}, a_{n-1})$.

This shows that (d_n) admits a limit. Let k be this limit. As d_n takes only discrete values, there is n_0 such that $\forall n \geq n_0$, $d_n = k$.

First let's do the case where $k = 1$. We have $gcd(a_1, \ldots, a_{n_0}) = 1$, and all positive combinations of a_1, ..., a_{n_0} are in S. Therefore, by question 1, there exists m such that all integers $\geq m$ are in S, and the conclusion follows with $K = k = 1$.

Else, if $k > 1$, we define $S' = \frac{1}{k}S = \{\frac{x}{k}, x \in S\}$. S' verifies the hypothesis of the problem, and with the same notations as previously, we have $k' = 1$. Then $\exists m' > 0$ such that S' contains every integer $\geq m'$. But $S = kS'$, so every element in $S \geq km'$ is a multiple of k greater than km'. The conclusion follows.

□