Algebraic structures*

Solutions by Alex Loiko

Problem 1

Definition 1. *Define*

$$S(a,b) = \{xa + yb | x \in \{0, 1 \ldots\}, y \in \{0, 1 \ldots\}\}$$

e.g.

$$S(2,3) =$$

$$\begin{aligned}\{0 \cdot 2 + 0 \cdot 3 &= 0, \\ 1 \cdot 2 + 0 \cdot 3 &= 2, \\ 0 \cdot 2 + 1 \cdot 3 &= 3, \\ 1 \cdot 2 + 1 \cdot 3 &= 5, \\ &\vdots, \\ &\ldots, \}\end{aligned}$$

Prove that if $\gcd(a,b) = 1$*, then* $\mathbb{N} \setminus S(a,b)$ *is a finite set.*

Consider congruences $\mod ab$, in particular the set of congruences

$$T = \{xa + yb \mod ab | x \in \{0, 1, \ldots, b-1\}, y \in \{0, 1, \ldots, a-1\}\}$$

I claim that all numbers of that form ($xa + yb$ for $x \in \{0, \ldots, b-1\}$ and $y \in \{0, \ldots, a-1\}$) are distinct $\mod ab$. Indeed, assume $n = xa + yb$ and $m = x'a + y'b$ are two numbers of that form. Then

$$\begin{aligned} n &\equiv m && \Leftrightarrow \\ xa + yb &\equiv x'a + y'b && \Leftrightarrow \\ a(x' - x) &\equiv b(y' - y) \end{aligned}$$

which, since $\gcd(a,b) = 1$ and $|x' - x| < b$, $|y' - y| < a$ only can be true when $x' - x = 0$ and $y - y' = 0$ that is, when $x' = x$ and $y' = y$. All of

*Well, at least the title of the problem set said algebraic structures :)

them are distinct $\mod ab$ and there are ab of them. It can only mean that $T = \{0, 1, \ldots, ab-1\}$. Now, if

$$n \in S(a,b), n \equiv k \mod ab$$

it is clear that all other numbers $m \equiv k \mod ab$ with $m > n$ also lie in $S(a,b)$ because you can always add $b \cdot a$ to $n \in S(a,b)$ and the result will still be in $S(a,b)$.

Because of the above any number greater than $\max T$ lies in $S(a,b)$ because it must be possible to write it as $n + kab$ where $n \in T$ (remember that T contains all congruence classes $\mod ab$). That means that there are only finitely many numbers **not** in $S(a,b)$, all of them less than $\max T$. This proves the claim.

Problem 2

Definition 2. *Define the* ***Frobenius number*** *of $S(a,b)$ to be the largest positive integer not in $S(a,b)$.*
e.g. the Frobenius number of

$$S(3,5) = \{0, 3, 5, 6, 9, 10, 11, 12, 13, 14, 15, 16, 17, \ldots\}$$

is 7 because any number greater than 7 is in $S(a,b)$

Prove that the Frobenius number of $S(a,b)$ is $ab - a - b$.

Turns out most of the work was done in the previous problem. Let's play around with this for a while. The set T defined in **Problem 1** turned out to be quite useful. Let's call it $T(a,b)$ instead and study it closer and calculate some numeric examples. But just some small modification, instead of defining it as

$$T(a,b) = \{xa + yb \mod ab | x \in \{0, 1, \ldots, b-1\}, y \in \{0, 1, \ldots, a-1\}\}$$

let's skip the $\mod ab$ part and just write

$$T(a,b) = \{xa + yb | x \in \{0, 1, \ldots, b-1\}, y \in \{0, 1, \ldots, a-1\}\}$$

Say that we want to calculate $T(3,5)$ and write it in increasing order.

```
> let t a b = sort [a*x + b*y | x <- [0..(b-1)], y <- [0..(a-1)]]
> t 3 5
> [0,3,5,6,8,9,10,11,12,13,14,16,17,19,22]
```

Ok. A long list of numbers. The largest number in $T(a,b)$ is always $a(b-1)+b(a-1) = 2ab-a-b$. Since every number greater than $\max T(a,b)$ lies in $S(a,b)$ we have found at least some bound on the Frobenius number.

It is at most $2ab - a - b$. But that number is ab from the one we want! I write the output again:

$$T(3,5) = \{0, 3, 5, 6, 8, 9, 10, 11, 12, 13, 14, \boxed{16,17,19,22}\}$$

Note that I have put a box around those numbers that are greater than ab and colored one special number green. Let's write them $\mod ab$.

```
> let tMod a b = map (flip mod (a*b)) $ t a b
> tMod 4 5
> [0,4,5,8,9,10,12,13,14,15,16,17,18,19,1,2,3,6,7,11]
```

And again, but in math:

$$T(4,5) = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, \boxed{1,2,3,6,7,11}\}$$

Now we are (more or less) ready to prove the bound. But first, let's prove a property of the numbers in $T(a,b)$.

---

*Every number in $T(a,b)$ is **minimal** in the sense that it is the minimal number in $S(a,b)$ in it's congruence class $\mod ab$.*
Or, more simple, if $n, m \in S(a,b)$ and $n \in T(a,b)$ and $n \equiv m$ then $m \geq n$.

For the proof, assume that $n, m \in S(a,b)$, $n \in T(a,b)$ and $n \equiv m$. Then we have $n = xa + yb$ for $0 \leq x < b, 0 \leq y < a$ since $n \in T(a,b)$. Now write

$$m = x'a + y'b \geq (x' \mod b)a + (y' \mod a)b \in T(a,b)$$

Observe that the later number is $\equiv m \mod ab$ because

$$a(x - x \mod b) \equiv 0 \mod ab$$

and

$$b(y - y \mod a) \equiv 0 \mod ab$$

(it follows from $x - x \mod b \equiv 0 \mod b$). That can only mean that

$$(x' \mod b)a + (y' \mod a)b = n$$

and we are done with that part of the proof.

Take another look at the pretty colored list of $T(4,5)$ and $T(3,5)$. The green number is in the first case $2ab-a-b$ and in the second $ab-a-b$. We want to prove that all numbers above that lie in $S(a,b)$. Well, assume some does not and call it x! Let $x \equiv k \in T(a,b)$ be it's congruence class i $T(a,b)$. Because of the minimal property of T we must have $x < k$. But then $k \geq x + ab$. Actually, we must have $k = x + ab$ because $k \geq x + 2ab$ would imply $k \geq 2ab > 2ab - a - b$ which is the largest number in $T(a,b)$. Then we have

$$ab - a - b < x = k - ab \Rightarrow k > 2ab - a - b$$

and $k \notin T(a,b)$. Contradiction! Hurray! The theorem is proven!

Umm... The theorem is proven and I have still got **haskell** code left. Here comes some I couldn't find any use for:

Say we are interested in the (x,y) pair of the numbers in $T(a,b)$. Let's write a function that shows us it!

```
> let tShow a b = [(a*x + b*y, (x,y)) | x <- [0..(b-1)], y<-[0..(a-1)]]
> tShow 2 3
> [(0,(0,0)),(3,(0,1)),(2,(1,0)),(5,(1,1)),(4,(2,0)),(7,(2,1))]
```

Now we want them in order.

```
> sort $ tShow 2 3
> [(0,(0,0)),(2,(1,0)),(3,(0,1)),(4,(2,0)),(5,(1,1)),(7,(2,1))]
```

Now we want them mod ab but still in the same order as before

```
> let tShowMod a b = zip (map ((flip mod (a*b)) . fst) $ tShow a b) (map snd $ tShow a
> tShowMod 2 3
> [(0,(0,0)),(3,(0,1)),(2,(1,0)),(5,(1,1)),(4,(2,0)),(1,(2,1))]
```

For more info and generalizations of this problem read
http://en.wikipedia.org/wiki/Coin_problem

For a **haskell** tutorial, read
http://learnyouahaskell.com/

For a very nice intoduction to LaTeXin shedish, read
http://www.ddg.lth.se/perf/handledning/

If you already know LaTeX, maybe you can explain why the horizontal line separators doesn't work? They are supposed to be centered with

```
\newcommand{\smallLine}{
  \begin{center}
    \line(1,0){100}
  \end{center}
}
```

but for some reason they are not...

Oh! Wait!!

I also have a problem for you!

Recall **Problem 2**, the second box with numbers ($\boxed{1,2,3,6,7,11}$). Prove that those are the only numbers that **can't** be written as positive linear combinations of a and b. Formally:

Another problem

Define

$$D(a,b) = \{x - ab | x > ab \wedge x \in T(a,b)\}$$

Now prove that

$$\mathbb{N} \setminus S(a,b) = D(a,b)$$

It shouldn't be that hard if you have read and understood this text.

/Alex