MTH 505: Number Theory — Spring 2017
Homework 2 — Drew Armstrong

The Frobenius Coin Problem. Consider the equation

$$ax + by = c$$

where a, b, c, x, y are **natural numbers**. We can think of \$$a$ and \$$b$ as two denominations of coins and \$$c$ as some value that we want to pay. The equation has a solution $(x, y) \in \mathbb{N}^2$ if and only if we can make change for \$$c$, and in this case we say that c is (a, b)-*representable*. More generally, we will consider the set of (a, b)-*representations of* c:

$$R_{a,b,c} := \{(x, y) \in \mathbb{N}^2 : ax + by = c\}.$$

The problem is trivial when $ab = 0$ so we will always assume that $ab \neq 0$, i.e., that a and b are both nonzero.

2.1. Consider natural numbers $a, b, c \in \mathbb{N}$ with $d = \gcd(a, b)$, where $a = da'$ and $b = db'$.

(a) If $d \nmid c$ prove that $R_{a,b,c} = \varnothing$.

(b) If $d|c$ with $c = dc'$ prove that $R_{a,b,c} = R_{a',b',c'}$. [Unlike the case of Diophantine equations, it is possible that both of these sets could be **empty**.]

The previous result allows us to restrict our attention to coprime a and b.

2.2. Let $a, b, c \in \mathbb{N}$ with $ab \neq 0$ and $\gcd(a, b) = 1$. If $R_{a,b,c} \neq \varnothing$ (i.e., if c is (a, b)-representable) prove that there exists a **unique representation** $(u, v) \in R_{a,b,c}$ with the property

$$0 \leqslant u < b - 1.$$

[Hint: For existence, let $(x, y) \in R_{a,b,c}$ be an arbitrary solution. Since $b \neq 0$ there exists a quotient and remainder of x mod b. For uniqueness, use the coprimality of a and b to apply Euclid's Lemma.]

2.3. Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. If $c = (ab - a - b)$ prove that $R_{a,b,c} = \varnothing$. That is, prove that **the number** $(ab - a - b)$ **is not** (a, b)**-representable**. [Hint: Let $c = (ab - a - b)$ and assume for contradiction there exists a representation $(x, y) \in R_{a,b,c}$. Show that the cases $x < b$ and $x \geqslant b$ both lead to the contradiction $y < 0$. You can use 2.2 for the case $x < b$.]

2.4. Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. In this exercise you will prove by induction that **every number** $c > (ab - a - b)$ **is** (a, b)**-representable**.

(a) Prove the result when $a = 1$ or $b = 1$.

(b) From now on we will assume that $a \geqslant 2$ and $b \geqslant 2$. In this case prove that the number $(ab - a - b + 1)$ is (a, b)-representable. [Hint: From the Euclidean Algorithm and 2.2 there exist $x', y' \in \mathbb{Z}$ with $ax' + by' = 1$ and $0 \leqslant x' < b - 1$. Prove that $(x' - 1) \in \mathbb{N}$ and $(y' + a - 1) \in \mathbb{N}$, and hence

$$a(x' - 1) + b(y' + a - 1) = (ab - a - b + 1)$$

is a valid representation.]

(c) Let $n \geqslant (ab - a - b + 1)$ and assume for induction that n is (a, b)-representable. In this case prove that $n + 1$ is also (a, b)-representable. [Hint: Let x', y' be as in part (b). By the induction hypothesis and 2.2 there exist $x, y \in \mathbb{N}$ with $ax + by = n$ and $0 \leqslant x < b$. Note that
$$a(x + x') + b(y + y') = (n + 1).$$
If $y + y' \geqslant 0$ then you are done. Otherwise, show that
$$a(x + x' - b) + b(y + y' + a) = (n + 1)$$
is a valid representation.]

Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. So far you have proved that $|R_{a,b,(ab-a-b)}| = 0$ and
$$|R_{a,b,c}| \geqslant 1 \text{ for all } c > (ab - a - b).$$
The next problem gives a rough lower bound for the **total number** of (a, b)-representations.

2.5. Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. Prove that
$$|R_{a,b,c}| \geqslant \left\lfloor \frac{c}{ab} \right\rfloor = \max\{n \in \mathbb{N} : n \leqslant c/(ab)\}.$$
[Hint: We know from class that the **integer solutions** of $ax + by = c$ have the form
$$(x, y) = (x' + kb', y' - ka') \quad \forall k \in \mathbb{Z},$$
where $x', y' \in \mathbb{Z}$ are some specific integers satisfying $ax' + by' = 1$. By 2.2 you can assume that $x' > 0$ and $y' < 0$. Now prove that the **natural number solutions** correspond to values of $k \in \mathbb{Z}$ such that
$$\frac{c(-y')}{a} \leqslant k \leqslant \frac{cx'}{b}.$$
Counting these integers is delicate but you should be able to give a rough bound.]

Unfortunately this rough bound gives us no information when $c < ab$, i.e., when $\lfloor c/(ab) \rfloor = 0$. With a bit more work one could compute the exact formula: for any $ax' + by' = 1$ we have

$$(*) \qquad |R_{a,b,c}| = \frac{c}{ab} - \left\{ \frac{cy'}{a} \right\} - \left\{ \frac{cx'}{b} \right\} + 1,$$

where $\{x\} := x - \lfloor x \rfloor$ is the **fractional part** of the rational number $x \in \mathbb{Q}$. This formula is due to Tiberiu Popoviciu in 1953.

2.6. Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. Given an integer $0 < c < ab$ such that $a \nmid c$ and $b \nmid c$, use Popoviciu's formula $(*)$ to show that
$$|R_{a,b,c}| + |R_{a,b,(ab-c)}| = 1.$$
[Hint: Use the fact that $\{-x\} = 1 - \{x\}$ when $x \notin \mathbb{Z}$.]

In conclusion, one can show from 2.6 that there exist exactly $\frac{(a-1)(b-1)}{2}$ natural numbers that are not (a, b)-representable. This fact was first proved by James Joseph Sylvester in 1884.