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**.]

Proof. (a): Let $d \nmid c$ and assume for contradiction that $R_{a,b,c}$ is not empty, i.e., assume that there exists a pair of natural numbers $(x, y) \in \mathbb{N}^2$ such that $ax + by = c$. But then we have

$$\begin{aligned} c &= ax + by \\ &= (da')x + b(db') \\ &= d(a'x + b'y), \end{aligned}$$

which contradicts the fact that $d \nmid c$.

(b): Now suppose that $d|c$ so that $c = dc'$ for some $c' \in \mathbb{Z}$. Since c and d are both positive we must have $c' \in \mathbb{N}$. To show that $R_{a',b',c'} \subseteq R_{a,b,c}$ consider any $(x, y) \in \mathbb{N}^2$, so that $a'x + b'y = c'$. Then we have

$$\begin{aligned} a'x + b'y &= c' \\ d(a'x + b'y) &= d(c') \\ (da')x + (db')y &= (dc') \\ ax + by &= c, \end{aligned}$$

which says that $(x, y) \in R_{a,b,c}$ as desired. Conversely, consider any $(x, y) \in R_{a,b,c}$, so that $ax + by = c$. Then we have

$$\begin{aligned} ax + by &= c \\ (da')x + (db')y &= (dc') \\ d(a'x + b'y) &= d(c') \\ a'x + b'y &= c', \end{aligned}$$

which says that $(x, y) \in R_{a',b',c'}$. (The last step used multiplicative cancellation.) $\square$

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

$$0 \leqslant u < b.$$

[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.]

Proof. If $R_{a,b,c} \neq \varnothing$ then there exists some pair $(x, y) \in \mathbb{N}^2$ such that $ax + by = c$. Since $b \neq 0$ there exists a pair of **integers** $q, r \in \mathbb{Z}$ such that

$$\begin{cases} x = qb + r \\ 0 \leqslant r < x \end{cases}$$

Then substituting $x = qb + r$ gives

$$\begin{aligned} ax + by &= c \\ a(qb + r) + by &= c \\ ar + b(q + y) &= c. \end{aligned}$$

It only remains to check that $(u, v) := (r, q + y) \in \mathbb{N}^2$ and we already know that $r \in \mathbb{N}$. Since $r < x$ we also have $qb = (x - r) > 0$, which since $b > 0$ implies that $q > 0$. But then since $y \in \mathbb{N}$ we have $q + y \in \mathbb{N}$ as desired. This proves existence.

For uniqueness, assume that we have (u_1, v_1) and (u_2, v_2) in $R_{a,b,c}$ with $0 \leqslant u_1 < b$ and $0 \leqslant u_2 < b$. Then since $au_1 + bv_1 = c = au_2 + bv_2$ we see that

$$\begin{aligned} au_1 + bv_1 &= au_2 + bv_2 \\ a(u_1 - u_2) &= b(v_2 - v_1), \end{aligned}$$

which implies that b divides $a(u_1 - u_2)$. But then since $\gcd(a, b) = 1$, Euclid's Lemma says that $b|(u_1 - u_2)$. If $(u_1 - u_2) = 0$ then we are done. Otherwise, suppose without loss of generality that $u_1 - u_2 > 0$. Then the fact that $b|(u_1 - u_2)$ implies that

$$b \leqslant u_1 - u_2 \leqslant u_1$$

which contradicts the fact that $u_1 < b$. This contradiction shows that $(u_1 - u_2) = 0$ and then the equation $b(v_2 - v_1) = a(u_1 - u_2) = a \cdot 0 = 0$ together with the fact $b \neq 0$ implies that $(v_2 - v_1) = 0$ as desired. $\square$

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 $x < b$.]

Proof. Assume for contradiction that we have a representation $ax + by = (ab - a - b)$ with $(x, y) \in \mathbb{N}^2$. From 2.2 this implies that there exists a representation $au + bv = (ab - a - b)$

with $(u, v) \in \mathbb{N}^2$ and $0 \leqslant u < b$. Now observe that

$$\begin{aligned} au + bv &= ab - a - b \\ au + a &= ab - b - bv \\ a(u+1) &= b(a - 1 - v). \end{aligned}$$

The last equation says that b divides $a(u+1)$ and then since a and b are coprime we obtain $b|(u+1)$ from Euclid's Lemma. Since $u + 1 > 0$ this implies that $b \leqslant u + 1$ [this argument is in the notes] but we already know that $u < b$ (i.e., $u + 1 \leqslant b$) so we conclude that $u + 1 = b$. Finally, we substitute $u = b - 1$ to obtain

$$\begin{aligned} au + bv &= ab - a - b \\ a(b-1) + bv &= ab - a - b \\ ab - a + bv &= ab - a - b \\ bv &= -b \\ v &= -1, \end{aligned}$$

which contradicts the fact that $v \in \mathbb{N}$. □

[Sorry I didn't follow my own hint very closely.]

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.]

Proof. (a): Since the problem is symmetric in a and b we will assume without loss of generality that $b = 1$. Now we want to show that every number $c > (a - a - 1) = -1$, i.e., every number $c \geqslant 0$ is $(a, 1)$-representable. But this is certainly true because $a(0) + 1(0) = 0$ is a valid representation of $c = 0$ and $a(1) + 1(c - 1) = c$ is a valid representation of $c > 0$. This solves the problem when $a = 1$ or $b = 1$ so from now on we will assume that $a \geqslant 2$ and $b \geqslant 2$.

(b): **Base Case.** Since $\gcd(a, b) = 1$ the Euclidean Algorithm gives integers $x', y' \in \mathbb{Z}$ such that $ax' + by' = 1$ and from 2.2 we can assume that $0 \leqslant x' < b$. [Actually this is a bit easier than 2.2 because we don't require $y' \geqslant 0$.] If $x' = 0$ then we have $by' = ax' + by' = 1$ which implies that $b = 1$, contradicting the fact that $b \geqslant 2$. Thus we must have $x' \geqslant 1$, i.e., $x' - 1 \in \mathbb{N}$. To complete the proof, assume for contradiction that $(y' + a - 1) < 0$, i.e., $y' + a \leqslant 0$. This implies that $y' \leqslant -a$ and hence $by' \leqslant -ab$. Finally, since $(x' - b) < 0$ we obtain the desired contradiction:

$$1 = ax' + by' \leqslant ax' - ab = a(x' - b) < 0.$$

We conclude that $(x' - 1)$ and $(y' + a - 1)$ are natural numbers, so

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

is a valid (a, b)-representaiton of $(ab - a - b + 1)$.

(c): **Induction Step.** Let $n \geqslant (ab - a - b + 1)$ and assume for induction that there exist natural numbers $(x, y) \in \mathbb{N}^2$ such that $ax + by = n$. In this case we want to show that $n + 1$ is also (a, b)-representable. To do this, recall from part (b) that we have integers $x', y' \in \mathbb{Z}$ with the following properties:

- $ax' + by' = 1$,
- $1 \leqslant x' \leqslant b - 1$,
- $y' + a \geqslant 1$.

Now add the equations $ax + by = n$ and $ax' + by' = 1$ to obtain

$$a(x + x') + b(y + y') = n + 1,$$

where $x + x' \geqslant 0$. If we also have $y + y' \geqslant 0$ then we are done, so assume that $y + y' < 0$. Since $y' + a \geqslant 1$ and $y \geqslant 0$ we have $(y + y' + a) \geqslant 1$. It only remains to check that $(x + x' - b) \geqslant 0$. To see this we use the assumptions $(n + 1) \geqslant (ab - a - b + 2)$ and $(y + y' + 1) \leqslant 0$ to obtain

$$\begin{aligned}
n + 1 = a(x + x') + b(y + y') &> ab - a - b + 2 \\
a(x + x') &\geqslant ab - a - b - b(y + y') + 2 \\
&> ab - a - b(y + y' + 1) + 2 \\
&\geqslant ab - a - b(0) + 2 \\
&> ab - a \\
&= a(b - 1) > 0.
\end{aligned}$$

By cancelling $a > 0$ from both sides of $a(x + x') > a(b - 1)$ we obtain $(x + x') > (b - 1)$ and hence $(x + x' - b) \geqslant 0$ as desired. It follows that

$$a(x + x' - b) + b(y + y' + a) = (ax + by) + (ax' + by') + (-ab + ab) = n + 1 + 0$$

is a valid (a, b)-representation of $n + 1$. $\square$

[That was tricky.]

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

$$(x, y) = (cx' - kb, cy' + ka) \quad \forall k \in \mathbb{Z},$$

where $x', y' \in \mathbb{Z}$ are some specific integers satisfying $ax' + by' = 1$. Now prove that the **natural number solutions** correspond to values of $k \in \mathbb{Z}$ such that

$$\frac{-cy'}{a} \leqslant k \leqslant \frac{cx'}{b}.$$

Counting these integers is delicate but you should be able to give a rough bound.]

Proof. Consider $a, b, c \in \mathbb{N}$ with $\gcd(a, b) = 1$. From 2.2 there exist integers $x', y' \in \mathbb{Z}$ such that $ax' + by' = 1$ and $0 \leqslant x' < b$. We know from class that the complete integer solution to the equation $ax + by = c$ is given by

$$(x, y) = (cx' - kb, cy' + ka) \quad \forall k \in \mathbb{Z},$$

and our job is to discover which of these solutions are non-negative. That is, we need to find all integers $k \in \mathbb{Z}$ such that the following two inequalities hold:

$$\begin{aligned} cx' - kb &\geqslant 0 \\ cy' + ka' &\geqslant 0. \end{aligned}$$

These two inequalities can be written in terms of fractions to obtain

$$\frac{-cy'}{a} \leqslant k \leqslant \frac{cx'}{b}.$$

Each such value of $k \in \mathbb{Z}$ corresponds to a non-negative solution of $ax + by = c$, so we conclude that $|R_{a,b,c}|$ is equal to the number of integers in the closed real number interval $[-cy'/a, cx'/b]$. The exact count is tricky, but the floor of the length of the interval provides a lower bound:

$$\begin{aligned} |R_{a,b,c}| &\geqslant \left\lfloor \frac{cx'}{b} - \frac{-cy'}{a} \right\rfloor \\ &= \left\lfloor \frac{cax' + cby'}{ab} \right\rfloor \\ &= \left\lfloor \frac{c(ax' + by')}{ab} \right\rfloor = \left\lfloor \frac{c}{ab} \right\rfloor. \end{aligned}$$

$\square$

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 $x \notin \mathbb{Z}$.]

Proof. Consider $a, b, c \in \mathbb{N}$ with $\gcd(a, b) = 1$, $0 < c < ab$, and where a and b do not divide c. Then for any integers $ax' + by' = 1$ Popoviciu's formula gives

$$\begin{aligned} |R_{a,b,(ab-c)}| &= \frac{ab-c}{ab} - \left\{\frac{(ab-c)y'}{a}\right\} - \left\{\frac{(ab-c)x'}{b}\right\} + 1 \\ &= 2 - \frac{c}{ab} - \left\{by' - \frac{cy'}{a}\right\} - \left\{ax' - \frac{cx'}{b}\right\}. \end{aligned}$$

But now observe that for all integers $n \in \mathbb{Z}$ and non-integer rationals $x \in \mathbb{Q}$ we have

$$\{n - x\} = \{-x\} = 1 - \{x\}.$$

Thus the above formula becomes

$$\begin{aligned} |R_{a,b,(ab-c)}| &= 2 - \frac{c}{ab} - \left\{by' - \frac{cy'}{a}\right\} - \left\{ax' - \frac{cx'}{b}\right\} \\ &= 2 - \frac{c}{ab} - \left(1 - \left\{\frac{cy'}{a}\right\}\right) - \left(1 - \left\{\frac{cx'}{b}\right\}\right) \\ &= 1 - \left(\frac{c}{ab} - \left\{\frac{cy'}{a}\right\} - \left\{\frac{cx'}{b}\right\} + 1\right) \\ &= 1 - |R_{a,b,c}|. \end{aligned}$$

□

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.

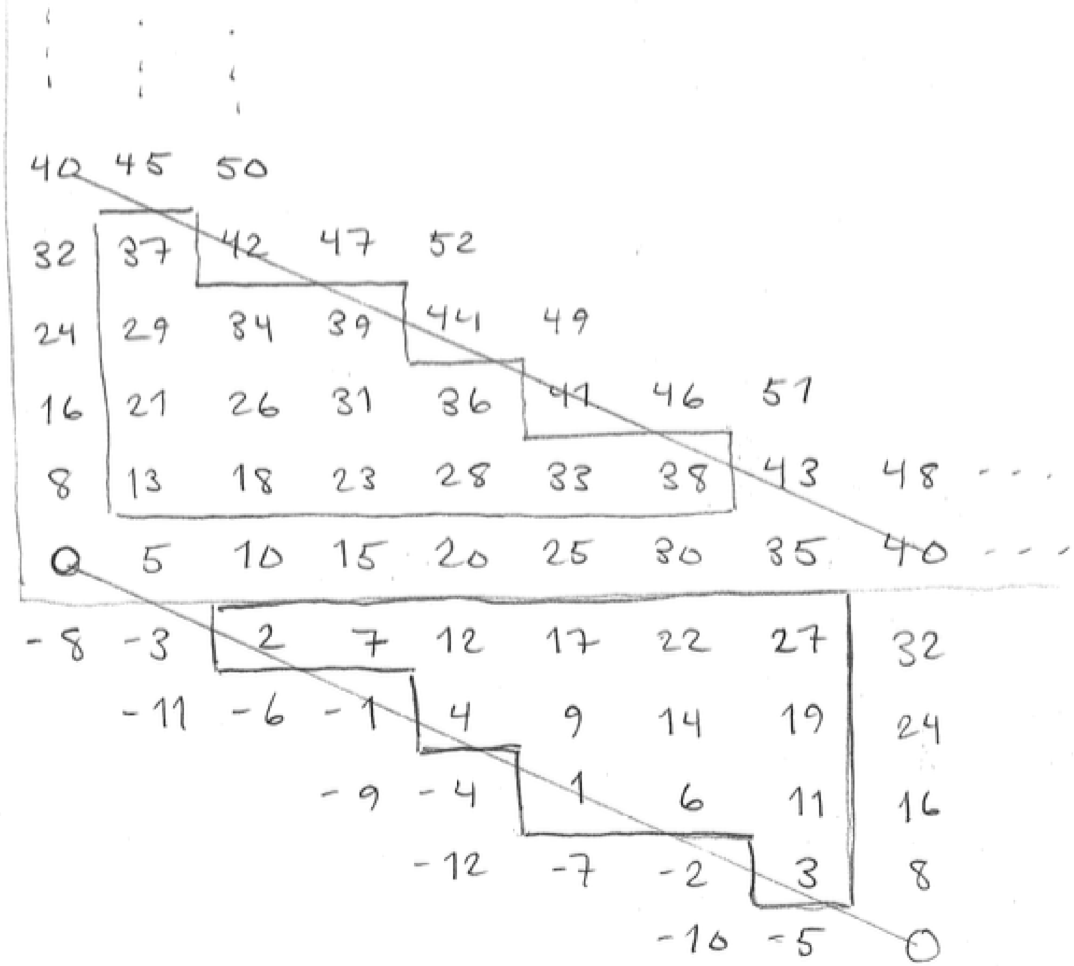
Proof. I didn't ask you to show this, but here's the proof. Let $\gcd(a, b) = 1$. Then we know that every integer $c \geqslant ab$ is (a, b)-representable. [In fact we know that every integer $c > (ab - a - b)$ is representable, but we don't need this right now.] Of the $ab + 1$ elements of the set $\{c \in \mathbb{Z} : 0 \leqslant c \leqslant ab\}$ we know that b elements are multiples of a, and a elements are multiples of b. Furthermore, since $\gcd(a, b) = 1$ we know that the only elements that are multiples of both a and b are 0 and ab. We conclude that there are exactly

$$(ab + 1) - (a + b - 2) = (ab - a - b + 1) = (a - 1)(b - 1)$$

elements of the set that are **not** a multiple of a or b. The result of Problem 2.6 says that exactly **half** of these numbers are (a, b)-representable. □

Epilogue: The proofs above are *algebraic*, but there is also a beautiful *geometric* way to think about the Frobenius coin problem. Consider $a, b \in \mathbb{N}$ with $ab \neq 0$ and $\gcd(a, b) = 1$. Label each point $(x, y) \in \mathbb{Z}^2$ of the integer lattice by the number $ax + by$. Note that points on the same line of slope $-a/b$ receve the same label. The problem is to count the integer points on the line $ax + by = c$ that lie in the first quadrant.

For example, here is the labelling corresponding to the coprime pair $(a, b) = (5, 8)$:



I have drawn the lines $5x + 8y = 5 \cdot 8 = 40$ and $5x + 8y = 0$. It was relatively easy to show that every label $c \geqslant 40$ occurs in the first quadrant, but the numbers below 40 are more tricky. I have outlined the numbers below 40 are are not multiples of 5 or 8 but are still $(5, 8)$-representable. We observe that there are $(5-1)(8-1)/2 = 14$ such numbers, as expected.

I have also outlined the numbers in the fourth quadrant that are **not** $(5, 8)$-representable. Observe that these two shapes are congruent up to 180° rotation, and in fact this is the transformation $c \mapsto (ab - c)$. Observe further that the two shapes fit together perfectly to make an $(a-1) \times (b-1)$ rectangle. This is the geometric explanation for Sylvester's formula

$$\frac{(a-1)(b-1)}{2}.$$