MTH 505 Homework 2

Roy Howie

February 20, 2017

Fix $a, b \in \mathbb{N}$ with $ab \neq 0$ and let $R_{a,b,c} = \{\, (x, y) \in \mathbb{N}^2 \mid ax + by = c \,\}$.

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

(a) Let $d \nmid c$, then there exists $q, r \in \mathbb{Z}$ such that $c = qd + r$ and $0 < r < d$. Note that $ax + by = c = qd + r$, or that $d(a'x + b'y - q) = r$. This implies $d \mid r$, a contradiction, as $0 < r < d$. Hence, $R_{a,b,c} = \varnothing$.

(b) Let $d \mid c$ with $c = dc'$ and let $R_{a',b',c'} = \{\, (x, y) \in \mathbb{N}^2 \mid a'x + b'y = c' \,\}$.

Suppose $(x, y) \in R_{a,b,c}$, then $ax + by = c$. This implies $d(a'x + b'y) = dc'$, or that $a'x + b'y = c'$, meaning $(x, y) \in R_{a',b',c'}$. Hence, $R_{a,b,c} \subset R_{a',b',c'}$.

Conversely, suppose $(x', y') \in R_{a',b',c'}$, then $a'x' + b'y' = c'$, implying $d(a'x' + b'y') = dc'$. Therefore, $ax' + by' = c$, so $(x', y') \in R_{a,b,c}$. Hence, $R_{a',b',c'} \subset R_{a,b,c}$

Thus, $R_{a,b,c} = R_{a',b',c'}$. □

2.2 Let $a, b, c \in \mathbb{N}$ with $ab \neq 0$ and $\gcd(a, b) = 1$. If $R_{a,b,c}$ is nonempty, prove there exists unique $(u, v) \in R_{a,b,c}$ such that $0 \leq u < b$.

Existence. Let $(x, y) \in R_{a,b,c,}$, then there exists unique $q, r \in \mathbb{N}$ such that $x = qb + r$ and $0 \leq r < b$. If $q = 0$, then $x < b$, so $(u, v) = (x, y)$. Otherwise, $ax + by = c$ implies $a(qb + r) + by = c$, or that $ar + b(y + aq) = c$, meaning $(u, v) = (r, y + aq)$.

Uniqueness. Suppose (x, y) can be reduced to two pairs (u, v) and $(\tilde{u}, \tilde{v})$ with $0 \leq u, \tilde{u} < b$. Then $au + bv = c$ and $a\tilde{u} + b\tilde{v} = c$, implying $au \equiv c \pmod{b}$ and $a\tilde{u} \equiv c \pmod{b}$. But a and b are coprime, so $u \equiv c \equiv \tilde{u} \pmod{b}$. Furthermore, $0 \leq u, \tilde{u} < b$, so u and $\tilde{u}$ inhabit the same residue class and are therefore equal. □

2.3 Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. If $c = ab - a - b$, prove $R_{a,b,c} = \varnothing$.

Note that, in **2.2**, we have existence iff $R_{a,b,c}$ is nonempty. Uniqueness, however, is a result of the Division Algorithm. That is, there is only one pair $(u, v) \in \mathbb{Z}^2$ satisfying $au + bv = ab - a - b$ with $0 \leq u < b$.

Next, note that $(u, v) = (b - 1, -1)$ is a solution to $au + bv = ab - a - b$. Thus, if $R_{a,b,c}$ is nonempty, then it contains a pair (x, y) without a corresponding (u, v) satisfying the conditions laid out in **2.2**. But for all (x, y) in $R_{a,b,c}$, (u, v) existed and was unique! Hence, $R_{a,b,c}$ is empty. □

2.4 Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. Prove every number $c > ab - a - b$ is (a, b)-representable.

(a) Suppose $a = 1$ or $b = 1$. Without loss of generality, let $a = 1$. We wish to show every number $c > 1 * b - 1 - b = -1$ is (a, b)-representable. This is clearly the case, as, for all $n \in \mathbb{N}$, $n = a * n$.

(b) Assume $a, b \geq 2$.

As $\gcd(a, b) = 1$, there exist $x', y' \in \mathbb{Z}$ such that $ax' + by' = 1$. Furthermore, as in **2.2**, we may further constrain x' to $0 \leq x' < b$. Next, note that $x' > 0$, as $x = 0$ implies $b = 1$, but we assumed $b \geq 2$. Hence, $(x' - 1) \in \mathbb{N}$.

Likewise, assume $(y' + a - 1) < 0$. This implies $y' \leq -a$. But then $ax' + by' = 1 \leq ax' + b(-a) = a(x' - b)$, meaning $x' > b$. This is a contradiction, so $(y' + a - 1) \in \mathbb{N}$.

Therefore, $(1-a-b+ab)$ is (a,b)-representable. Indeed, $a(x'-1)+b(y'+a-1) = 1-a-b+ab$.

(c) Let $n \geq ab-a-b+1$ and assume n is (a,b)-representable. Let x' and y' be as in **(b)**. Then there exist $x, y \in \mathbb{N}$ such that $ax+by=n$ and $0 \leq x < b$.

Note that $a(x+x')+b(y+y') = n+1$. If $y+y' \geq 0$, then we are done. Otherwise, we wish to show $(x+x'-b, y+y'+a) \in \mathbb{N}^2$.

Suppose $y+y'+a < 0$ and recall from **(b)** that $y'+a \geq 1$. We then have $y+y' < -a \leq y'-1$, or that $y < -1$. However, this implies

$$\begin{aligned} ab-a-b+1 \leq n = ax+by &< ax+b(-1) \\ a(b-1)-b+1 &< ax-b \\ a(b-1) &< ax \\ b &\leq x \end{aligned}$$

But we assumed $0 \leq x < b$, so this is a contradiction! Hence, $(y+y'+a) \in \mathbb{N}$.

Next, note that $ab-a-b < n$ by assumption. Furthermore, $n+1 = a(x+x')+b(y+y') \leq a(x+x')-b$, as $y+y' < 0$. Since $n < n+1$, it follows that

$$\begin{aligned} ab-a-b &< a(x+x')-b \\ a(b-1) &< a(x+x') \\ b-1 &< x+x' \\ b &\leq x+x' \end{aligned}$$

Hence, $(x+x'-b) \in \mathbb{N}$ and $(x+x'-b,\ y+y'+a)$ is indeed a valid representation of $n+1$. □

2.5 Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. Prove $|R_{a,b,c}| = \lfloor \frac{c}{ab} \rfloor$.

Note that all solutions (x,y) to the equation $ax+by=c$ are of the form $(cx'+kb, cy'-ka)$ for all $k \in \mathbb{Z}$ and for (x',y') solving $ax'+by'=1$. Furthermore, if a solution $(u,v) \in R_{a,b,c}$, then $u, v \geq 0$.

Thus, $cx'+kb \geq 0$ implies $k \geq -\frac{cx}{b}$ and $cy'-ka \geq 0$ implies $k \leq \frac{cy'}{a}$. Hence,

$$|R_{a,b,c}| = \left\lfloor \frac{cy'}{a} - \frac{-cx'}{b} \right\rfloor = \left\lfloor \frac{c}{ab}(y'b+x'a) \right\rfloor = \left\lfloor \frac{c}{ab} \right\rfloor \qquad \square$$

2.6 Let $a, b \in \mathbb{N}$ be coprime with $ab \neq 0$. Given $c \in \mathbb{N} \cap (0, ab)$ such that a and b do not divide c, prove $|R_{a,b,c}| + |R_{a,b,ab-c}| = 1$.

Define $\{\, x \,\}$ as $x - \lfloor x \rfloor$ and note $|R_{a,b,c}| = \frac{c}{ab} - \{\, \frac{cy'}{a} \,\} - \{\, \frac{cx'}{b} \,\} + 1$ for $ax'+by'=1$. Then,

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

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