Instances of a problem treated in general below were used to illustrate Mathematical Induction on pp. 198-9, p. 200 Ex. #19, 31-33, and p. 227 Ex. #9 in our text *Discrete Mathematics and Its Applications* 4th. ed. by K. Rosen (1999, McGraw-Hill). Every student is expected to be able to follow the proofs in this note but perhaps not to create them nor to reproduce them all.

Given two kinds of coins, one worth M¢ and the other worth N¢, what sums of money can be made up using various numbers of these coins and no others? Given two kinds of stamps, one worth M¢ and the other worth N¢, what postage can be made up using various numbers of these stamps and no others? In short, what set **$** is generated by the expression $x\cdot M + y\cdot N$ as x and y run through all nonnegative integers? This set **$** consists of certain nonnegative multiples of $d := GCD(M, N)$. In fact every multiple of d bigger than $L := LCM(M, N) – M – N$ turns out to lie in **$**, though this fact is not obvious; to prove it is the purpose of this note. The proof comes via Charles Holton from Yossi Fendel, who didn't remember where he got it.

Dividing d into L and into every member of **$** including M and N simplifies the problem. It becomes trivial if either of M or N is 1, so we assume henceforth that

$$M > 1, \quad N > 1 \quad \text{and} \quad GCD(M, N) = 1 .$$

Set **$** is still generated by the expression $x\cdot M + y\cdot N$ as x and y run through all nonnegative integers. Our task is to prove that the largest integer L *not* in **$** is

$$L := M\cdot N – M – N = (M–1)\cdot(N–1) – 1 .$$

First some terminology: For any nonnegative integer z we write " z **mod** $M\cdot N$ " for the *residue* (remainder) left when z is divided by $M\cdot N$. A set of $M\cdot N$ integers z is called a *complete nonredundant set of residues* just when every remainder 0, 1, 2, …, $M\cdot N–1$ turns up just once among the residues z **mod** $M\cdot N$. In particular every set of $M\cdot N$ consecutive nonnegative integers is a complete nonredundant set of residues; an example is the interval **T** of $M\cdot N$ integers t that satisfy $L < t \le L+M\cdot N$. This **T** will figure in the proof.

Consider now the subset **S** of **$** generated by the expression $x\cdot M + y\cdot N$ as x and y run through all integers that satisfy $0 \le x < N$ and $0 \le y < M$. The integers in **S** are not all consecutive; 0 and M and N belong to **S** but 1 does not. Still, **S** is a complete nonredundant set of residues, as we shall demonstrate now. Every member s of **S** determines its x and y uniquely because if $s = x\cdot M + y\cdot N = \bar{x}\cdot M + \bar{y}\cdot N$ then $(x–\bar{x})\cdot M = (\bar{y}–y)\cdot N$, but $GCD(M, N) = 1$ and therefore $|x–\bar{x}| \equiv 0$ **mod** N and $|y–\bar{y}| \equiv 0$ **mod** M; now the constraints $0 \le x < N$ and $0 \le \bar{x} < N$ imply $x = \bar{x}$, and similarly $y = \bar{y}$. Therefore the $M\cdot N$ pairs (x, y) generate $M\cdot N$ distinct members $s = x\cdot M + y\cdot N$ of **S**. No two members of **S** have the same residue **mod** $M\cdot N$ because, if $x\cdot M + y\cdot N \equiv \bar{x}\cdot M + \bar{y}\cdot N$ **mod** $M\cdot N$, then $(x–\bar{x})\cdot M + (y–\bar{y})\cdot N \equiv 0$ **mod** $M\cdot N$, whence follows $|x–\bar{x}| \equiv 0$ **mod** N and $|y–\bar{y}| \equiv 0$ **mod** M, and then $x = \bar{x}$ and $y = \bar{y}$ as before. Therefore the $M\cdot N$ elements of **S** provide all $M\cdot N$ distinct residues, which means that **S** is a complete nonredundant set of residues, as is **T**.

For example, if $M = 2$ and $N = 3$ then $L = 1$, **T** = {2, 3, 4, 5, *6*, 7} and **S** = {*0*, 2, 3, 4, 5, 7}. If $M = 2$ and $N = 5$ then $L = 3$, **T** = {4, 5, 6, 7, 8, 9, *10*, 11, *12*, 13} and **S** = (*0*, *2*, 4, 5, 6, 7, 8, 9, 11, 13}. If $M = 3$ and $N = 5$ then $L = 7$, **T** = {8, 9, 10, …, *20*, *21*, 22} and **S** = {*0*, *3*, *5*, *6*, 8, 9, 10, 11, 12, 13, 14, 16, 17, 19, 22}.

The sets **S** and **T** overlap; their largest elements are the same $(N–1)\cdot M + (M–1)\cdot N$, but the smallest element $L+1 = (M–1)\cdot(N–1)$ in **T** is rather bigger than the smallest element 0 in **S**.

However, whenever s lies in $\mathbf{S}$ but not in $\mathbf{T}$, which implies $s \le L$, then $t := s + M\cdot N$ must lie in $\mathbf{T}$ (because $L < M\cdot N \le t \le L+M\cdot N$) but not in $\mathbf{S}$ since no residue **mod** $M\cdot N$ occurs more than once in $\mathbf{S}$. In short, $\mathbf{T}–\mathbf{S} \supseteq (\mathbf{S}–\mathbf{T}) + M\cdot N$. (Here the "–" is the set-difference operator and the "+" adds $M\cdot N$ to every element of $\mathbf{S}–\mathbf{T}$.) Since, like $\mathbf{S}$ and $\mathbf{T}$, the sets $\mathbf{S}–\mathbf{T}$ and $\mathbf{T}–\mathbf{S}$ have equally many elements, actually $\mathbf{T}–\mathbf{S} = (\mathbf{S}–\mathbf{T}) + M\cdot N$.

This set's every element $t = s + M\cdot N = x\cdot M + y\cdot N + M\cdot N = (x+N)\cdot M + y\cdot N$ lies in $\$$ and so, since $\$ \supset \mathbf{S}$ too, $\$ \supset \mathbf{S} \cup (\mathbf{T}–\mathbf{S}) = \mathbf{S} \cup \mathbf{T} \supset \mathbf{T}$. Now that we know $\$ \supset \mathbf{T}$, we can prove that every integer bigger than L lies in $\$$ by induction as follows:

Partition the integers bigger than L into consecutive subsets $\mathbf{T} + j\cdot M\cdot N$ for $j = 0, 1, 2, 3, \ldots$, and let our induction hypothesis be that $\$ \supset \mathbf{T} + j\cdot M\cdot N$ for some integer $j \ge 0$. We know this hypothesis to be true for $j = 0$. For each integer t in $\mathbf{T} + (j+1)\cdot M\cdot N$ we find that $s := t – M\cdot N$ belongs to $\mathbf{T} + j\cdot M\cdot N$ which is contained in $\$$, according to the induction hypothesis, whence follows that $s = x\cdot M + y\cdot N$ for some integers $x \ge 0$ and $y \ge 0$. Then $t = (x+N)\cdot M + y\cdot N$ must lie in $\$$ too, and therefore $\$ \supset \mathbf{T} + (j+1)\cdot M\cdot N$ too. By induction $\$ \supset \mathbf{T} + j\cdot M\cdot N$ for every integer $j \ge 0$. (This part of the proof is the only part presented in our text.)

So, every integer bigger than L lies in $\$$. Now where does L lie? L cannot lie in the subset $\mathbf{S}$ because its largest element is $(N–1)\cdot M + (M–1)\cdot N = L + M\cdot N \equiv L$ **mod** $M\cdot N$, and no residue **mod** $M\cdot N$ can occur in $\mathbf{S}$ more than once. L cannot lie in the subset

$$\$–\mathbf{S} = \{x\cdot M + y\cdot N : (x \ge 0 \text{ and } y \ge M) \text{ or } (x \ge N \text{ and } y \ge 0)\}$$

because its least element is $M\cdot N > L$. Therefore L cannot lie in $\$$, which therefore consists of every integer greater than L together with a scattering of integers less than L. End of proof.

. . . . . .

" A challenging exercise:"

Prove that exactly half the integers between 0 and L inclusive lie in $\$$.

Note why $L+1 = (M–1)\cdot(N–1)$ is even: GCD(M, N) = 1 so $M–1$ and $N–1$ cannot both be odd. Now let $\mathbf{J}$ be the interval of $L+1$ integers j that satisfy $0 \le j \le L$. To prove that exactly half these integers lie in $\$$ we shall show that, whenever an integer s lies in $\mathbf{J}\cap\$$, then $L–s$ lies in $\mathbf{J}–\$$, so there must be exactly $(L+1)/2$ such pairs $\{s, L–s\}$ in $\mathbf{J}$.

$\mathbf{J}\cap(\$–\mathbf{S}) = \mathbf{Ø}$ (is empty) because, as was explained above, the least element of $\$–\mathbf{S}$ is $M\cdot N > L$; therefore $\mathbf{J}\cap\$ = \mathbf{J}\cap(\mathbf{S} \cup (\$–\mathbf{S})) = \mathbf{J}\cap\mathbf{S}$. Since every integer s in $\mathbf{J}\cap\$$ lies in $\mathbf{S}$ too, every such $s = x\cdot M + y\cdot N$ for some integers satisfying $0 \le x < N$ and $0 \le y < M$. Then $M\cdot N + L–s = (N–1)\cdot M + (M–1)\cdot N - x\cdot M – y\cdot N = (N–1–x)\cdot M + (M–1–y)\cdot N$ lies in $\mathbf{S}$, in which each of the $M\cdot N$ residues **mod** $M\cdot N$ occurs just once. Since $M\cdot N + L–s \equiv L–s$ **mod** $M\cdot N$, we conclude that $\mathbf{S}$ cannot contain $L–s$ which, however, does lie in $\mathbf{J}$. Therefore $L–s$ lies in $\mathbf{J}–\mathbf{S}$ which, since $\mathbf{J}\cap\$ = \mathbf{J}\cap\mathbf{S}$, implies $L–s$ lies in $\mathbf{J}–\$$ as claimed. End of proof.