The GCD of m Linear Forms in n Variables

Ben Klein

Davidson, North Carolina, USA

beklein@davidson.edu

Harold Reiter

Department of Mathematics,

University of North Carolina Charlotte,

Charlotte, NC 28223, USA

hbreiter@uncc.edu

Arthur Holshouser

3600 Bullard St.

Charlotte, NC,

USA

Abstract. Suppose that $a, b, c, d \in Z$ are fixed, $\begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$ and at least one of $(a, b), (c, d), (a, c) (b, d)$ are relatively prime. Also, $(x, y) \in Z \times Z, (x, y) \neq (0, 0)$ and (x, y) are relatively prime. (x, y) is considered a variable.

Define $u = ax + cy, v = bx + dy$. In this paper we study the gcd (u, v) in great detail. We use matrix theory and also the Euclidean algorithm with row transformations on matrices to do this.

Also, three of the four main results in this paper can be extended to n-space by using the exact same arguments and we illustrate how this can be done. Due to a defect in the mathematics itself one of these extensions is not completely satisfactory. Near the end of the paper we generalize the theory further by defining derived matrices. Then the exact same theory holds for many other variations of u, v such as $u = -dx + cy, v = bx - ay$. In Section 10 we drop the condition that at least one of $(a, b), (c, d), (a, c), (b, d)$ are relatively prime and substitute the one condition that gcd $(a, b, c, d) = 1$. This is a vast improvement and much of the 2 variable material remains unchanged. In Section 13 we end the paper with a new idea. Then we can study m linear forms in n variables. Some of this work was motivated by the theory of generalized Stern-Brocot trees.

1 Introduction

The material in this paper arose naturally from our work on Farey fractions and Stern-Brocot trees. Suppose that $a, b, c, d \in Z$ are fixed, $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$ and at least one of $(a, b), (c, d), (a, c) (b, d)$ are relatively prime. Also, $(x, y) \in Z \times Z, (x, y) \neq (0, 0)$ and (x, y) are relatively prime. (x, y) is considered a variable. Define $u = ax + cy, v = bx + dy$. We show that for all $(x, y) \in Z \times Z$, if gcd $(x, y) = 1$ then gcd $(u, v) | \Delta$. Therefore, if $\Delta = \pm 1$ then gcd $(u, v) = 1$ is true for all (x, y) if gcd $(x, y) = 1$.

Also, we show that $\gcd(u,v) = 1$ is true for all $(x,y), \gcd(x,y) = 1$, if and only if $\Delta = \pm 1$.

We do this by showing that if $|\Delta| \geq 2$, then $\gcd(u,v) = |\Delta|$ for an infinite number of $(x,y), \gcd(x,y) = 1$, and we find all such (x,y). Also, if $\overline{\Delta} \in \{1,2,3,\cdots\}$ and $\overline{\Delta}|\Delta$, we show that. $\gcd(u,v) = \overline{\Delta}$ for an infinite number of $(x,y), \gcd(x,y) = 1$. Also, we find all such $(x,y), \gcd(x,y) = 1$.

Also, for all $\Delta \neq 0$, we show separately that there exists an infinite number of $(x,y), \gcd(x,y) = 1$, such that $\gcd(u,v) = 1$. Also, we find all such (x,y). Solving $\gcd(u,v) = 1$ is easier than solving $\gcd(u,v) = \overline{\Delta}$. Three of the above four results can be extended to n-space in a completely straightforward way by using the exact same proofs. We illustrate this for the $\gcd(u,v) = \Delta$ result. We do not generalize the $\gcd(u,v) = \overline{\Delta}$ result to n-space. Due to a defect in the mathematics itself the $\gcd(u,v) = \Delta$ generalization is not completely satisfactory and we state why in Section 8.

Also, in Section 8 we state the three n-space generalizations for 3-space.

In Section 9, we state some further extensions of our results by using derived matrices. Then the theory holds true completely unchanged for many other variations of u, v such as $u = -dx + cy, v = bx - ay$.

In Section 10, we drop the condition that at least one of $(a,b), (c,d), (a,c), (b,d)$ are relatively prime and we substitute the one condition that $\gcd(a,b,c,d) = 1$. This was a major breakthrough for us and much of the two variable theory holds true unchanged when we use $\gcd(a,b,c,d) = 1$. The n-space version using this new assumption is an open ended problem which we have not solved. Indeed, we continue to use the assumption that at least one of $(a,b), (c,d), (a,c), (b,d)$ are relatively prime mainly because the n-space version of this can be proved in almost exactly the same way that the 2-variable theory is proved. In Section 13, we end with a new idea. This new idea allows us to use the machinery in this paper to study the gcd of m linear forms in n variables, $m, n \in \{1,2,3,\cdots\}$. This includes one linear form in n variables which we deal with in Section 14.

2 Showing that $\gcd(u,v) | \Delta$

Theorem 1 and Problem 3 of Section 7 are the two major results in this paper.

Theorem 1 *Suppose that* $a,b,c,d \in Z$ *are fixed and* $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. *Also,* $(x,y) \in Z \times Z, (x,y) \neq (0,0)$ *and* (x,y) *are relatively prime.* (x,y) *is considered a variable. Define* $u = ax + cy, v = bx + dy$. *Then* $\gcd(u,v) | \Delta$. *Thus, if* $\Delta = \pm 1$, *we see that* (u,v) *are relatively prime for all* (x,y) *when* $\gcd(x,y) = 1$ *since* $\gcd(u,v) = 1$.

Note 1 In Theorem 1 we are not requiring at least one of $(a,b), (c,d), (a,c), (b,d)$ to be relatively prime. However, we are requiring $\gcd(x,y) = 1$. We will now illustrate in Theorem $1'$ how the two variable results can be extended unchanged to n-space. Theorem

$1'$ is a 3-space version of Theorem 1. In Section 13 we invite the reader to greatly extend Theorems $1, 1'$ by using a new idea. The proof of Theorem $1'$ also proves Theorem 1.

Theorem $1'$ Suppose that $a, b, c, d, e, f, g, h, i, x, y, z \in Z$ where Z is the set of all integers.

Also, $(x, y, z) \neq (0, 0, 0)$ and $\gcd(x, y, z) = 1$. This means that if $t \in \{1, 2, 3, \cdots\}$ and $t \,|x, t|\, y, t|z$ then $t = 1$.

Also, suppose $\Delta = \begin{vmatrix} a & d & g \\ b & e & h \\ c & f & i \end{vmatrix} \neq 0$.

Define $u = ax + dy + gz, v = bx + ey + hz, w = cx + fy + iz$. Then $\gcd(u, v, w) \,|\Delta$. This means that if $r \in \{1, 2, 3, \cdots\}$ and $r|u.r|v, r|w$ then $r|\Delta$.

Proof. Define $M = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}, M^{-1} = \frac{1}{\Delta} \begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix}$ where $\overline{a}, \overline{b}, \overline{c}, \cdots \in Z$.

Now $\begin{bmatrix} u \\ v \\ w \end{bmatrix} = M \begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

Therefore, $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = M^{-1} \begin{bmatrix} u \\ v \\ w \end{bmatrix}$ which implies $\begin{bmatrix} \Delta x \\ \Delta y \\ \Delta z \end{bmatrix} = \begin{bmatrix} \overline{a}u + \overline{d}v + \overline{g}w \\ \overline{b}u + \overline{e}v + \overline{h}w \\ \overline{c}u + \overline{f}v + \overline{i}w \end{bmatrix}$.

Since $\Delta, x, y, z, \overline{a}, \overline{b}, \overline{c}, \cdots, u, v, w \in Z$ we see that if $r|u, r|v, r|w$ where $r \in \{1, 2, 3, \cdots\}$ then $r|\Delta x, r|\Delta y, r|\Delta z$. However, if $t \in \{1, 2, 3, \cdots\}$ and $t|x, t|y, t|z$ then $t = 1$. Therefore, we see that $r|\Delta$. Therefore, $\gcd(u, v, w) \,|\Delta$. ■

Observation 1 If $\Delta = \pm 1$ then $\gcd(u, v, w) = 1$ is true for all $(x, y, z) \in Z \times Z \times Z, (x, y, z) \neq (0, 0, 0), \gcd(x, y, z) = 1$.

3 Applying the Euclidean Algorithm to Linear Forms

Suppose $a, b, c, d, x, y \in Z$,

$\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0, (x, y) \neq (0, 0)$ and (x, y) are relatively prime.

We apply the Euclidean Algorithm to compute $\gcd(ax + cy, bx + dy)$.

We represent $ax + cy, bx + dy$ by the matrix $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ since we have $\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + cy \\ bx + dy \end{bmatrix}$.

We first review the Euclidean Algorithm to compute $\gcd(a, b)$ where $a, b \in Z, (a, b) \neq (0, 0)$. Our approach is slightly different from the usual approach.

We note that $\gcd(a, b) = \gcd(a, b \pm a) = \gcd(a \pm b, b)$.

First, suppose $1 \leq |a| \leq |b|$. Then $\gcd(a, b) = \gcd(a, b \pm a)$ where the $\pm$ sign is chosen so that $|b \pm a| < |b|$.

Second, suppose $|a| \geq |b| \geq 1$. Then $\gcd(a,b) = \gcd(a \pm b, b)$ where the $\pm$ sign is chosen so that $|a \pm b| < |a|$. If $|a| = |b| \neq 0$ we have $\gcd(a,b) = |a| = |b|$ since $\gcd(a,b) = \gcd(a, b \pm a) = (a,0) = \gcd(a \pm b, b) = \gcd(0,b) = |a| = |b|$.

Starting with (a,b) and repeating the above algorithm we will eventually arrive at $\gcd(a,b) = \gcd(\overline{a},0) = |\overline{a}|$ or $\gcd(a,b) = \gcd\left(0,\overline{b}\right) = \left|\overline{b}\right|$.

For example, $\gcd(15,21) = \gcd(15, 21-15) = \gcd(15,6) = \gcd(15-6,6) = \gcd(9,6) = \gcd(9-6,6) = \gcd(3,6) = \gcd(3,6-3) = \gcd(3,3) = \gcd(3,0) = \gcd(0,3) = 3$. We now apply the Euclidean Algorithm to compute $\gcd(u,v)$ where $u = ax + cy, v = bx + dy$ and where $a,b,c,d,x,y \in Z, \Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0, (x,y) \neq (0,0)$ and $\gcd(x,y) = 1$.

Now

$$\begin{aligned} &\gcd\left(\overline{a}x + \overline{c}y, \overline{b}x + \overline{d}y\right) \\ &\qquad = \gcd\left(\overline{a}x + \overline{c}y, \left(\overline{b}x + \overline{d}y\right) \pm \left(\overline{a}x + \overline{c}y\right)\right) \\ &\qquad = \gcd\left(\overline{a}x + \overline{c}y, \left(\overline{b} \pm \overline{a}\right)x + \left(\overline{d} \pm \overline{c}\right)y\right) \\ &\qquad = \gcd\left(\left(\overline{a}x + \overline{c}y\right) \pm \left(\overline{b}x + \overline{d}y\right), \overline{b}x + \overline{d}y\right) \\ &\qquad = \gcd\left(\left(\overline{a} \pm \overline{b}\right)x + \left(\overline{c} \pm \overline{d}\right)y, \left(\overline{b}x + \overline{d}y\right)\right). \end{aligned}$$

Also, $\begin{vmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{vmatrix} = \begin{vmatrix} \overline{a} & \overline{c} \\ \overline{b} \pm \overline{a} & \overline{d} \pm \overline{c} \end{vmatrix} = \begin{bmatrix} \overline{a} \pm \overline{b} & \overline{c} \pm \overline{d} \\ \overline{b} & \overline{d} \end{bmatrix}$.

Using the matrix representation $\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix}$ of $\overline{a}x + \overline{c}y, \overline{b}x + \overline{d}y$ we can now apply the following row transformations to $\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix}$. $\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} \to \begin{bmatrix} \overline{a} \pm \overline{b} & \overline{c} \pm \overline{d} \\ \overline{b} & \overline{d} \end{bmatrix}$ or $\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} \to \begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} \pm \overline{a} & \overline{d} \pm \overline{c} \end{bmatrix}$. Using these row transformations we use the Euclidean Algorithm in the standard way on the first column $\begin{bmatrix} a \\ b \end{bmatrix}$ of the initial matrix $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ to reduce $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ to $\begin{bmatrix} \overline{g} & \overline{c} \\ 0 & \overline{d} \end{bmatrix}$ or $\begin{bmatrix} a & c \\ b & d \end{bmatrix} \to \begin{bmatrix} 0 & \overline{c} \\ \overline{g} & \overline{d} \end{bmatrix}$ where $|\overline{g}| = \gcd(a,b)$ and $\overline{g}, \overline{c}, \overline{d} \in Z$.

Thus, if $\gcd(a,b) = 1$ we see that $\overline{g} = \pm 1$. We now see that $\gcd(u,v) = \gcd(ax + cy, bx + dy) = \gcd\left(\overline{g}x + \overline{c}y, \overline{d}y\right)$ or $\gcd(ax + cy, bx + dy) = \gcd\left(\overline{c}y, \overline{g}x + \overline{d}y\right)$. Also, note that $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = \begin{vmatrix} \overline{g} & \overline{c} \\ 0 & \overline{d} \end{vmatrix} \neq 0$ or $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = \begin{vmatrix} 0 & \overline{c} \\ \overline{g} & \overline{d} \end{vmatrix} \neq 0$. Thus, $\Delta = \overline{g}\overline{d}$ or $\Delta = -\overline{g}\overline{c}$. The algorithm can also be used on the 2nd column in the same way.

All the material in Section 3 generalizes to n-space in a completed straight forward way. We give examples of the row transformations in Sections 5, 10.

4 A Standard Set

Suppose $d \in Z \backslash \{0\}, g \in \{1,2,3,\cdots\}$ and $g|d$. In this paper the set $S(d,g) = \{x : x \in Z, \gcd(d,x) = g\}$ is considered to be a standard set which can easily be computed in its entirety.

If $g = 1$ we call $S(d,g) = S(d,1) = S(d)$ where $S(d) = \{x : x \in Z, \gcd(d,x) = 1\}$. $S(d)$ can be called the Euler set of d. Also, $S(d) = S(-d)$ and $S(d,g) = S(-d,g)$.

Also, if $d \in \{1,2,3,\cdots\}$, then $S(d) = \overline{S}(d) + nd, n \in Z$,
where $\overline{S}(d) = \{x : x \in \{1,2,\cdots,d\}, \gcd(x,d) = 1\}$.

Also, if $d, g \in \{1,2,3,\cdots\}$, $g|d$, then $S(d,g) = \overline{S}(d,g) + nd, n \in Z$, where $\overline{S}(d,g) = \{x : x \in \{1,2,\cdots,d\}, \gcd(x,d) = g\}$.

Of course, if $\overline{S}(d)^{\#}$ is the number of elements in $\overline{S}(d)$, then $\overline{S}(d)^{\#} = \phi(d)$ where $\phi(d)$ is Euler's ϕ-function.

Also, $\overline{S}(d,g) = \{x : x \in \{1,2,3,\cdots,d\}, \gcd(x,d) = g\} = \left\{g \cdot x : x \in \left\{1,2,\cdots,\frac{d}{g}\right\}, \gcd\left(x,\frac{d}{g}\right) = 1\right\}$.

Also, $\overline{S}(d,g)^{\#} = \phi\left(\frac{d}{g}\right)$. Concluding this section we note that $\gcd(x,d_1,d_2,\cdots d_n) = \gcd(x,\gcd(d_1,d_2,\cdots d_n))$.

5 Finding all $(x,y) \in Z \times Z, \gcd(x,y) = 1$, such that $u = ax + cy, v = bx + dy$ are Relatively Prime

Problem 1 Suppose $a,b,c,d \in Z$ are fixed, and $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. Also, at least one of $(a,b),(c,d),(a,c),(b,d)$ are relatively prime. Find all of the $(x,y) \in Z \times Z, (x,y) \neq (0,0), (x,y)$ are relatively prime and show that there are an infinite number of such (x,y) such that $u = ax + cy, v = bx + dy$ are relatively prime. Of course, $\gcd(u,v) = 1$ implies $\gcd(x,y) = 1$.

Note 2 If $S \subseteq Z$ is a set and $a \in Z$ then $S - a = \{x - a : x \in S\}$. We note from Theorem 1 that if $\Delta = \pm 1$ then (u,v) are relatively prime for all $(x,y) \in Z \times Z$, $(x,y) \neq (0,0), (x,y)$ are relatively prime. Also the n-space solution to Problem 1 is almost exactly the same. Also, in Section 10 we solve Problem 1 when we use the condition that $\gcd(a,b,c,d) = 1$.

Solution We first assume that at least one of $(a,b),(c,d)$ are relatively prime. By symmetry we may assume that (a,b) are relatively prime. We deal later with one of $(a,c),(b,d)$ are relatively prime. Since $\gcd(a,b) = 1$, we can apply the Euclidean algorithm and the row transformations of Section 3 to the linear forms $u = ax + cy, v = bx + dy$ to show that $\gcd(ax + cy, bx + dy) = \gcd\left(\pm x + \overline{c}y, \overline{d}y\right)$ where $(\pm 1)\left(\overline{d}\right) = \Delta$ or $\gcd(ax + cy, bx + dy) = \gcd\left(\overline{c}y, \pm x + \overline{d}y\right)$, where $(\mp 1)(\overline{c}) = \Delta$.

Since $\gcd\left(\pm x + \overline{c}y, \overline{d}y\right) = \gcd\left(\pm x + \overline{c}y, \pm\overline{d}y\right) = \gcd\left(\mp x - \overline{c}, \pm\overline{d}y\right)$, by symmetry, suppose that $\gcd(ax + cy, bx + dy) = \gcd\left(x + \overline{c}y, \overline{d}y\right)$ where $\overline{d} \in \{1,2,3,\cdots\}, \overline{d} = |\Delta|, \Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0, \overline{c} \in Z$.

Let $y \in Z \backslash \{0\}$ be arbitrary, but fixed.

Now $\gcd(ax+cy, bx+dy) = \gcd\left(x+\overline{c}y, \overline{d}y\right) = 1$ if and only if $x+\overline{c}y \in S\left(\overline{d}y\right)$ where $S\left(\overline{d}y\right)$ is defined in Section 4 and where $S\left(\overline{d}y\right)$ can easily be computed in its entirety.

Therefore, $x \in S\left(\overline{d}y\right) - \overline{c}y$. Of course, $x+\overline{c}y \in S\left(\overline{d}y\right)$ implies that $\gcd(x,y) = 1$. Also of course $\gcd(ax+cy, bx+dy) = 1$ implies $\gcd(x,y) = 1$. Suppose now that at least one of (a,c) or (b,d) are relatively prime. By symmetry, we suppose that (a,c) are relatively prime. For $(x,y) \in Z \times Z$, $\gcd(x,y) = 1$ we know that $u = ax+cy, v = bx+dy$ are relatively prime if and only if there exists $m, n \in Z$ such that $mu + nv = 1$. Of course, this implies $\gcd(m,n) = 1$.

Now $mu + nv = 1$ is true if and only if $m[ax+cy] + n[bx+dy] = x[ma+nb] + y[mc+nd] = 1$. Of course, this implies $\gcd(x,y) = 1$ and also $\gcd(ma+nb, mc+nd) = 1$. Since (a,c) are relatively prime and also $\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$, we can use the above solution to compute all $(m,n) \in Z \times Z, (m,n) \neq (0,0), \gcd(m,n) = 1$ so that $ma+nb, mc+nd$ are relatively prime. For each such $(m,n) \in Z \times Z$ it is a standard problem in number theory to compute all $(x,y) \in Z \times Z, (x,y) \neq (0,0), \gcd(x,y) = 1$ such that $x[ma+nb] + y[mc+nd] = 1$. This takes care of $\gcd(a,c) = 1$ which completes the solution.■

Note 3. Some readers may not like the way that we took care of the case where at least one of (a,c) or (b,d) are relatively prime. For these readers we point out that in Section 7 we develop a different technique for handling this case. Also, in Section 10 we give the complete solution to Problem 1 where we have only one case namely $\gcd(a,b,c,d) = 1$.

However, when we generalize Problem 1 to n-space we are still stuck with the above solution since this is the only way that we know how to handle n-space.

Example 1 Find all $(x,y) \in Z \times Z, (x,y) \neq (0,0), \gcd(x,y) = 1$ so that $u = 3x+7y, v = 2x+3y$ are relatively prime.

Solution We use the fact that $\gcd(3,2) = 1$.

Now $\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \Delta = \begin{vmatrix} 3 & 7 \\ 2 & 3 \end{vmatrix} = -5. \quad \begin{bmatrix} 3 & 7 \\ 2 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 3-2 & 7-3 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 4 \\ 1 & -1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 4 \\ 0 & -5 \end{bmatrix}$.

Therefore, $\gcd(u,v) = \gcd(x+4y, -5y) = \gcd(x+4y, 5y) = 1$. Now $y \in Z \backslash \{0\}$ is arbitrary but fixed.

As an example, let $y = 3$. Now $\gcd(x+12, 15) = 1$ if and only if $x+12 \in S(15) = \{1,2,4,7,8,11,13,14\} + 15n, n \in Z, = \{16,17,19,22,23,26,28,29\} + 15\overline{n}, \overline{n} \in Z$. Therefore, $x \in S(15) - 12$ which implies that $x \in \{4,5,7,10,11,14,16,17\} + 15\overline{n}, \overline{n} \in Z$. That is, $x \in \{1,2,4,5,7,10,11,14\} + 15\overline{n}, \overline{n} \in Z$. ■

6 Finding All $(x,y) \in Z \times Z, \gcd(x,y) = 1$ such that $\gcd(u,v) = \gcd(ax+cy, bx+dy) = |\Delta|$

Problem 2 *Suppose* $a,b,c,d \in Z$ *are fixed and* $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. *Also, at least one of* $(a,b),(c,d),(a,c),(b,d)$ *are relatively prime. Also,* $(x,y) \in Z \times Z, (x,y) \neq (0,0)$ *and* (x,y) *are relatively prime.* (x,y) *is considered to be a variable. Define* $u = ax+cy, v = bx+dy$. *Find all* $(x,y) \in Z \times Z$ *where* $\gcd(x,y) = 1$ *such that* $\gcd(u,v) = |\Delta|$ *and also show that there are an infinite number of such* (x,y). *Of course, from Theorem 1, this implies that* $\gcd(u,v) = 1$ *for all* $(x,y) \in Z \times Z$,$(x,y) \neq (0,0), \gcd(x,y) = 1$ *if and only if* $\Delta = \pm 1$.

Note 4 We generalize both Problems 1, 2 in Problem 3 of Section 7. The n-space versions of Problems 1, 2 are solved almost exactly the same way that Problems 1, 2 are solved. However, we do not generalize Problem 3 to n-space and this is why we solve Problems 1, 2 separately from Problem 3 even though Problem 3 generalizes both Problems 1, 2.

Also, it is fairly easy to see that the more advanced machinery developed later in Section 10 can be used to solve a slightly modified Problem 2 when we only use the one simple condition on a,b,c,d that $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. If $\gcd(a,b,c,d) = \theta$, we can show that $\gcd(u,v) = \dfrac{|\Delta|}{\theta}$ for an infinite number of $(x,y) \in Z \times Z, \gcd(x,y) = 1$. We mention this again in Section 14 after we have studied Section 10.

Solution Define $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}, M^{-1} = \dfrac{1}{\Delta}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$. Of course, Theorem 1 takes care of the case where $|\Delta| = 1$.

Suppose now that $|\Delta| \geq 2$. We compute an infinite number of $(x,y) \in Z \times Z, (x,y) \neq (0,0), (x,y)$ are relatively prime and we also find all such (x,y) so that $u = \Delta\theta, v = \Delta\phi$ where $(\theta,\phi) \in Z \times Z, (\theta,\phi) \neq (0,0)$ and (θ,ϕ) are relatively prime. Of course, this implies that $\gcd(u,v) = \gcd(\Delta\theta, \Delta\phi) = |\Delta|$ since (θ,ϕ) are relatively prime.

From $\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \Delta\theta \\ \Delta\phi \end{bmatrix} = M\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$ and $M^{-1}\begin{bmatrix} \Delta\theta \\ \Delta\phi \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$ and $M^{-1} = \dfrac{1}{\Delta}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$ and $\dfrac{1}{\Delta}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} \Delta\theta \\ \Delta\phi \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$ we have $\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} \theta \\ \phi \end{bmatrix} = \begin{bmatrix} d\theta - c\phi \\ -b\theta + a\phi \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$.

The Problem we now face is to compute an infinite number of $(\theta,\phi) \in Z \times Z, (\theta,\phi) \neq (0,0), (\theta,\phi)$ are relatively prime and also compute all such (θ,ϕ) so that (x,y) are relatively prime. Note that θ,ϕ are now playing the role of x,y in Problem 1. Also, note that $\Delta = \begin{vmatrix} d & -c \\ -b & a \end{vmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$ where $\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$ is used in the place of $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$. In other words, we are just calling a,b,c,d by the new names $d,-b,-c,a$ respectively.

Also, we note that if at least one of $(a,b),(c,d),(a,c),(b,d)$ are relatively prime then at least one of $(d,-b),(-c,a),(d,-c),(-b,a)$ are also relatively prime.

The problem we now face is the same problem as Problem 1 and from Problem 1 we know how to compute all $(\theta,\phi)\in Z\times Z,(\theta,\phi)\neq(0,0),(\theta,\phi)$ are relatively prime such that $x=d\theta-c\phi,y=-b\theta+a\phi$ are relatively prime. Also, we know that there are an infinite number of such (θ,ϕ). ■

7 Finding All $(u,v)=(ax+cy,bx+dy),\gcd(x,y)=1$, Such that $\gcd(u,v)=\overline{\Delta}$ where $\overline{\Delta}|\Delta$.

Problem 3 *Suppose that* $a,b,c,d\in Z$ *are fixed and* $\Delta=\begin{vmatrix} a & c \\ b & d \end{vmatrix}\neq 0$. *Also,* $\overline{\Delta}\in\{1,2,3,\cdots\},\overline{\Delta}|\Delta$. *Also at least one of* $(a,b),(c,d),(a,c),(b,d)$ *are relatively prime. Also* $(x,y)\in Z\times Z,(x,y)\neq(0,0)$ *and* (x,y) *are relatively prime.*

Define $u=ax+cy,v=bx+dy$.

Find all $(x,y)\in Z\times Z,(x,y)\neq(0,0),(x,y)$ *are relatively prime and show that there are an infinite number of such* (x,y) *such that* $\gcd(u,v)=\overline{\Delta}$.

From Theorem 1 we know $\gcd(u,v)|\Delta$. *Using the ideas of Section 10, it may be possible to solve Problem 3 when we use the condition that* $\gcd(a,b,c,d)=1$.

Solution First, assume that at least one of $(a,b),(c,d)$ are relatively prime. By symmetry we may suppose that $\gcd(a,b)=1$.

Since $\gcd(a,b)=1$ we can apply the Euclidean Algorithm and the row transformations of Section 3 to the linear forms $u=ax+cy,v=bx+dy$ to show that $\gcd(ax+cy,bx+dy)=\gcd\left(\pm x+\overline{c}y,\overline{d}y\right)$ where $(\pm1)\left(\overline{d}\right)=\Delta$ or $\gcd(ax+cy,bx+dy)=\gcd\left(\overline{c}y,\pm x+\overline{d}y\right)$ where $(\mp1)(\overline{c})=\Delta$. As in Section 6, by symmetry we may suppose that $\gcd(ax+cy,bx+dy)=\gcd\left(x+\overline{c}y,\overline{d}y\right)$ where $\overline{d}=|\Delta|,\Delta=\begin{vmatrix} a & c \\ b & d \end{vmatrix}\neq 0,\overline{c}\in Z$. That is, $\gcd(ax+cy,bx+dy)=\gcd(x+\overline{c}y,\Delta y),\overline{c}\in Z$.

Therefore, we want to compute all $(x,y)\in Z\times Z,\gcd(x,y)=1$ such that $\gcd(ax+cy,bx+dy)=\gcd(x+\overline{c}y,\Delta y)=\overline{\Delta}$. Suppose that p is a prime and $p|\overline{\Delta}$. Now $\gcd(x+\overline{c}y,\Delta y)=\overline{\Delta}$. Therefore, $p|\overline{\Delta}$ implies $p|(x+\overline{c}y)$. Therefore, if $p|\overline{\Delta}$ and also $p|y$ then $p|(x+\overline{c}y)$ implies $p|x$. But $p|x$ and $p|y$ is impossible since $\gcd(x,y)=1$.

Therefore, p does not divide y when $p|\overline{\Delta}$ and from this we know that $\gcd\left(y,\overline{\Delta}\right)=1$.

Let $y\in Z\backslash\{0\},\gcd\left(y,\overline{\Delta}\right)=1$, be arbitrary but fixed.

Now $\gcd(x+\overline{c}y,\Delta y)=\overline{\Delta}$ where $\overline{\Delta}\in(1,2,3,\cdots),\overline{\Delta}|\Delta$ and $\overline{\Delta}|\Delta y$ is true if and only if $x+\overline{c}y\in S\left(\Delta y,\overline{\Delta}\right)=\left\{t:t\in Z,\gcd(\Delta y,t)=\overline{\Delta}\right\}$. $S\left(\Delta y,\overline{\Delta}\right)$ was defined in Section 4.

Now if $\gcd(x+\overline{c}y,\Delta y)=\overline{\Delta}$ is true then $\gcd(x,y)=1$ must also be true.

To see this suppose $\gcd(x,y)\neq1$. Then there exists a prime p, such that $p|x,p|y$. Now $p\nmid\overline{\Delta}$ since $\gcd\left(y,\overline{\Delta}\right)=1$. However, $p|x,p|y$ implies $p|\gcd(x+\overline{c}y,\Delta y)$ and this implies $p|\overline{\Delta}$

since we know that $\gcd(x+\bar{c}y, \Delta y) = \overline{\Delta}$. This is a contradiction since $p \nmid \overline{\Delta}$.

Therefore, (x, y) are relatively prime and $\gcd(ax+cy, bx+dy) = \gcd(x+\bar{c}y, \Delta y) = \overline{\Delta}$ when $x + \bar{c}y \in S\left(\Delta y, \overline{\Delta}\right)$. This is equivalent to $x \in S\left(\Delta y, \overline{\Delta}\right) - \bar{c}y$.

Next, suppose one of $(a, c), (b, d)$ are relatively prime.

As always, define $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}, M^{-1} = \frac{1}{\Delta}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix} = \frac{1}{\overline{\Delta}\Delta'}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$ where $\Delta = \overline{\Delta}\Delta'$ since $\overline{\Delta}|\Delta$.

Also, $\begin{bmatrix} u \\ v \end{bmatrix} = M\begin{bmatrix} x \\ y \end{bmatrix}$. Therefore, $\begin{bmatrix} x \\ y \end{bmatrix} = M^{-1}\begin{bmatrix} u \\ v \end{bmatrix} = \frac{1}{\Delta}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} u \\ v \end{bmatrix}$.

We want to find all $(x, y) \in Z \times Z, (x, y) \neq (0, 0), \gcd(x, y) = 1$ so that $u = \overline{\Delta}\theta, v = \overline{\Delta}\phi$ where $(\theta, \phi), \in Z \times Z, (\theta, \phi) \neq (0, 0), (\theta, \phi)$ are relatively prime. Of course, this is equivalent to $\gcd(u, v) = \overline{\Delta}$ since (θ, ϕ) must be relatively prime.

From $\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \overline{\Delta}\theta \\ \overline{\Delta}\phi \end{bmatrix} = M\begin{bmatrix} x \\ y \end{bmatrix}$ and $M^{-1}\begin{bmatrix} \overline{\Delta}\theta \\ \overline{\Delta}\phi \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$ and $M^{-1} = \frac{1}{\overline{\Delta}\Delta'}\begin{bmatrix} d-c \\ -ba \end{bmatrix}$ and $\frac{1}{\overline{\Delta}\Delta'}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} \overline{\Delta}\theta \\ \overline{\Delta}\phi \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$ we have $\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\begin{bmatrix} \theta \\ \phi \end{bmatrix} = \begin{bmatrix} d\theta - c\phi \\ -b\theta + a\phi \end{bmatrix} = \begin{bmatrix} \Delta' x \\ \Delta' y \end{bmatrix}$.

By assumption, we know that at least one of $(d, -b), (-c, a)$ are relatively prime. Also, we want to find all $(\theta, \phi) \in Z \times Z, (\theta, \phi) \neq (0, 0), \gcd(\theta, \phi) = 1$ so that (x, y) are relatively prime.

This is equivalent to $\gcd(d\theta - c\phi, -b\theta + a\phi) = |\Delta'|$ where $\gcd(\theta, \phi) = 1$ and this is the exact same problem that we just solved with θ, ϕ now playing the role of x, y and with a, b, c, d renamed $d, -b, -c, a$, and $\overline{\Delta}$ renamed $|\Delta'|$. Also, $\begin{vmatrix} d & -c \\ -b & a \end{vmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = \Delta \neq 0$ and $|\Delta'|\,|\Delta$. Therefore, Problem 3 is solved. ■

8 n-space Generalizations

Theorem 1 and Problems 1, 2 can be generalized to n-space.

We have not solved the generalization of Problem 3 to n-space. We now state the 3-space versions of Problems 1, 2.

The 3-space and n-space solutions are almost exactly the same as the 2-space versions. Of course, Theorem 1′ generalizes Theorem 1 to 3-space and the n-space theorem and proof is exactly the same.

Problem 1′ Suppose that $a, b, c, d, e, f, g, h, i \in Z$ are fixed and $\Delta = \begin{vmatrix} a & d & g \\ b & e & h \\ c & f & i \end{vmatrix} \neq 0$. Also, $\gcd(a, b, c) = 1$ or $\gcd(d, e, f) = 1$ or $\gcd(g, h, i) = 1$ or $\gcd(a, d, g) = 1$ or $\gcd(b, e, h) . = 1$ or $\gcd(c, f, i) = 1$.

Also, $(x, y, Z) \in Z \times Z \times Z, (x, y, z) \neq (0, 0, 0)$ and $\gcd(x, y, z) = 1$; x, y, z are variables.

Define $u = ax + dy + gz, v = bx + ey + hz, w = cx + fy + iz$. Find all of the $(x, y, z) \in Z \times Z \times Z, (x, y, z) \neq (0, 0, 0), \gcd(x, y, z) = 1$ and show that there are an infinite number of

such (x,y,z) such that $\gcd(u,v,w)=1$. Of course, $\gcd(u,v,w)=1$ implies $\gcd(x,y,z)=1$.

Note 5 Of course, from Theorem 1′ if $\Delta=\pm1$ then $\gcd(u,v,w)=1$ for all (x,y,z) where $\gcd(x,y,z)=1$. Also, we are far from solving Problem 1′ if we drop the condition that $\gcd(a,b,c)=1$ or $\gcd(d,e,f)=1$, etc, and substitute $\gcd(a,b,c,d,e,f,g,h,i)=1$. This last condition comes from Section 10.

Problem 2′ Suppose that $a,b,c,d,e,f,g,h,i\in Z$ are fixed.

Define $M=\begin{bmatrix} a & d & g\\ b & e & h\\ c & f & i\end{bmatrix}$ and assume that $\Delta=\begin{vmatrix} a & d & g\\ b & e & h\\ c & f & i\end{vmatrix}\neq 0$.

Define $M^{-1}=\dfrac{1}{\Delta}\begin{bmatrix} \overline{a} & \overline{d} & \overline{g}\\ \overline{b} & \overline{e} & \overline{h}\\ \overline{c} & \overline{f} & \overline{i}\end{bmatrix}$ where $\overline{a},\overline{b},\overline{c},\overline{d},\overline{e},\overline{f},\overline{g},\overline{h},\overline{i}\in Z$. Also assume that $\gcd\left(\overline{a},\overline{b},\overline{c}\right)=1$ or $\gcd\left(\overline{d},\overline{e},\overline{f}\right)=1$ or $\gcd\left(\overline{g},\overline{h},\overline{i}\right)=1$ or $\gcd\left(\overline{a},\overline{d},\overline{g}\right)=1$ or $\gcd\left(\overline{b},\overline{e},\overline{h}\right)=1$ or $\gcd\left(\overline{c},\overline{f},\overline{i}\right)=1$.

Also, $(x,y,z)\in Z\times Z\times Z, (x,y,z)\neq(0,0,0)$ and $\gcd(x,y,z)=1$. x,y,z are variables.

Define $u=ax+dy+gz, v=bx+ey+hz, w=cx+fy+iz$.

Find all $(x,y,z)\in Z\times Z\times Z, (x,y,z)\neq(0,0,0), \gcd(x,y,z)=1$ and show that there are an infinite number of (x,y,z) such that $\gcd(u,v,w)=|\Delta|$.

Of course, this implies that $\gcd(u,v,w)=1$ for all $(x,y,z)\in Z\times Z\times Z, (x,y,z)\neq(0,0,0), \gcd(x,y,z)=1$, if and only if $\Delta\pm1$. At the end of our solution we show why this generalization is not completely satisfactory.

Solution. The solution that we give is nearly the same as Problem 2. We wish to compute all $(x,y,z), \gcd(x,y,z)=1$ so that $u=\Delta\theta, v=\Delta\phi, w=\Delta\psi$ where $(\theta,\phi,\psi)\in Z\times Z\times Z, (\theta,\phi,\psi)\neq(0,0,0), \gcd(\theta,\phi,\psi)=1$. This implies that $\gcd(u,v,w)=|\Delta|$ since $\gcd(\theta,\phi,\psi)=1$.

From $\begin{bmatrix} u\\ v\\ w\end{bmatrix}=\begin{bmatrix} \Delta\theta\\ \Delta\phi\\ \Delta\psi\end{bmatrix}=M\begin{bmatrix} x\\ y\\ z\end{bmatrix}=\begin{bmatrix} a & d & g\\ b & e & h\\ c & f & i\end{bmatrix}\begin{bmatrix} x\\ y\\ z\end{bmatrix}$ and $M^{-1}\begin{bmatrix} \Delta\theta\\ \Delta\phi\\ \Delta\psi\end{bmatrix}=\begin{bmatrix} x\\ y\\ z\end{bmatrix}$

and $M^{-1}=\dfrac{1}{\Delta}\begin{bmatrix} \overline{a} & \overline{d} & \overline{g}\\ \overline{b} & \overline{e} & \overline{h}\\ \overline{c} & \overline{f} & \overline{i}\end{bmatrix}$ and $\dfrac{1}{\Delta}\begin{bmatrix} \overline{a} & \overline{d} & \overline{g}\\ \overline{b} & \overline{e} & \overline{h}\\ \overline{c} & \overline{f} & \overline{i}\end{bmatrix}\begin{bmatrix} \Delta\theta\\ \Delta\phi\\ \Delta\psi\end{bmatrix}=\begin{bmatrix} x\\ y\\ z\end{bmatrix}$ we have $\begin{bmatrix} \overline{a} & \overline{d} & \overline{g}\\ \overline{b} & \overline{e} & \overline{h}\\ \overline{c} & \overline{f} & \overline{i}\end{bmatrix}\begin{bmatrix} \theta\\ \phi\\ \psi\end{bmatrix}=$

$\begin{bmatrix} \overline{a}\theta+\overline{d}\phi+\overline{g}\psi\\ \overline{b}\theta+\overline{e}\phi+\overline{h}\psi\\ \overline{c}\theta+\overline{f}\phi+\overline{i}\psi\end{bmatrix}=\begin{bmatrix} x\\ y\\ z\end{bmatrix}$.

The problem we now face is to compute all $(\theta,\phi,\psi)\neq(0,0,0), \gcd(\theta,\phi,\psi)=1$ and show that there are an infinite number of such (θ,ϕ,ψ) such that $\gcd(x,y,z)=1$. We note that $\begin{vmatrix} \overline{a} & \overline{d} & \overline{g}\\ \overline{b} & \overline{e} & \overline{h}\\ \overline{c} & \overline{f} & \overline{i}\end{vmatrix}=\Delta^2\neq 0$.

The problem we now face is solved in Problem 1′. ■

The matrices $\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix} = \begin{bmatrix} 2 & -2 & 0 \\ 0 & 2 & -4 \\ 0 & 0 & 4 \end{bmatrix}$ show that $\gcd(a,b,c) = 1$ or $\gcd(d,e,f) = 1$, etc. does not imply that $\gcd\left(\overline{a},\overline{b},\overline{c}\right) = 1$ or $\gcd\left(\overline{d},\overline{e},\overline{f}\right) = 1$, etc.

So we must assume that $\gcd\left(\overline{a},\overline{b},\overline{c}\right) = 1$ or $\gcd\left(\overline{d},\overline{e},\overline{f}\right) = 1$ or $\gcd\left(\overline{g},\overline{h},\overline{i}\right) = 1$, etc.

Indeed suppose we try to use the matrix $\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$ to solve Problem $2'$.

In the step $\begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix} \begin{bmatrix} \theta \\ \phi \\ \psi \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ we have $\begin{bmatrix} 2 & -2 & 0 \\ 0 & 2 & -4 \\ 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} \theta \\ \phi \\ \psi \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

It is obvious that $\gcd(x,y,z) = 1$ cannot be true. Therefore, no solution exists for Problem $2'$ when we use this matrix. This example tells us that both Problems 2, 3 cannot be generalized to n-space in a completely satisfactory way.

Thus, it appears that some of the two variable mathematics cannot be generalized to n-space in a completely satisfactory way. In other words, we must use artificial conditions in the hypothesis to get n-space generalizations.

9 Transforming the Matrix

We Illustrate the Transformations of the Matrices for 3×3 Matrices. These new matrices can be called derived matrices.

Define $M = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}, a,b,c,d,e,f,g,h,i \in Z$. Also, $\Delta = \begin{vmatrix} +a+d+g \\ +b+e+h \\ +c+f+i \end{vmatrix} \neq 0$.

We wish to transform M into a new matrix $\overline{M} = \begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix}$ where $\{a,b,c,d,e,f,g,h,i\} = \left\{\pm\overline{a},\pm\overline{b},\pm\overline{c},\pm\overline{d},\pm\overline{e},\pm\overline{f},\pm\overline{g},\pm\overline{h},\pm\overline{i}\right\}$ such that $\begin{vmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{vmatrix} = \pm\Delta$.

The following standard transformations (which have redundancies) will accomplish this. We take arbitrary combinations of these four transformations.

1. Reversing the algebraic signs in a row and reversing the algebraic signs in a column.
2. Interchanging two rows and interchanging two columns.
3. Interchanging the rows and columns by flipping the matrix about one of the two diagonals. The tranpose M^T of M is defined by flipping the matrix M about the main

diagonal.

4. Rotating the matrix 90° clockwise or counter clockwise. Once we have a new matrix $M = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} \rightarrow \overline{M} = \begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix}$ where $\Delta = |M|, \overline{\Delta} = \left|\overline{M}\right| = \pm\Delta$ we can use the matrix $\overline{M}$ in the exact same way as matrix M in Theorem 1, $1'$ or Problem $1, 1'$ or Problem $2, 2'$ or Problem 3. In other words, the theory is completely unchanged. The reason for this is that $a, b, c, \cdots \in Z$ and $\overline{a}, \overline{b}, \overline{c}, \cdots \in Z$ and also the hypothesis of Theorem $1, 1'$ or Problem $1, 1,'$ or Problem $2, 2'$ or Problem 3 is unchanged as we go from $M = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} \rightarrow \overline{M} = \begin{bmatrix} \overline{a} & \overline{d} & \overline{g} \\ \overline{b} & \overline{e} & \overline{h} \\ \overline{c} & \overline{f} & \overline{i} \end{bmatrix}$.

Theorem $\overline{1}$ is an example of this.

Theorem $\overline{1}$ Suppose $a, b, c, d \in Z$, are fixed and $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. Also, $(x, y) \in Z \times Z, (x, y) \neq (0, 0)$ and (x, y) are relatively prime. Define $u = dx - cy, v = -bx + ay$. Then $\gcd(u, v) | \Delta$. Therefore, if $\Delta = \pm 1$ we know that (u, v) are relatively prime for all $(x, y) \in Z \times Z$ if (x, y) are also relatively prime.

Proof. Define $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$. We let the reader show that $\overline{M} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$ can be derived from M by using the above transformations 1 and 3. We can now use Theorem 1 with this new matrix $\overline{M}$ to prove Theorem $\overline{1}$. ■

10 Dropping the Condition that at least one of $(a, b), (c, d), (a, c), (b, d)$ are Relatively Prime

In Problems 1, 2, 3 we assumed that at least one of $(a, b), (c, d), (a, c), (b, d)$ are relatively prime. We now give the complete solution to Problem 1 when we drop this condition that at least one of $(a, b), (c, d), (a, c), (b, d)$ are relatively prime. However, this complete solution to Problem 1 may be an empty set. In Theorem 2 and Observation 3 we show that $\gcd(a, b, c, d) = 1$ is the necessary and sufficient condition on a, b, c, d so that this complete solution to Problem 1 is not an empty set and we state exactly what this complete solution is when $\gcd(a, b, c, d) = 1$.

Problem 1^* Suppose that $a, b, c, d \in Z$ are fixed and $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. Find all $(x, y) \in Z \times z, x, y$ $(x, y) \neq (0, 0), (x, y)$ are relatively prime such that $u = ax + cy, v = bx + dy$ are relatively prime.

Solution. As in the solution to Problem 1 of Section 5, by using the Euclidean Algorithm and the matrix row transformations of Section 3, by symmetry it is obvious that $\gcd(ax+cy, bx+dy) = \gcd\left(\overline{a}x+\overline{c}y, \overline{d}y\right) = 1$ where $\overline{a}, \overline{c}, \overline{d} \in Z, |\overline{a}| = \gcd(a,b)$ and $\overline{a}\overline{d} = \pm\Delta \neq 0$. However, since $\gcd(\theta,\phi) = \gcd(\pm\theta, \pm\phi)$ we will now assume that $\overline{a}, \overline{d} \in \{1,2,3,\cdots\}$, and $\overline{a} = \gcd(a,b)$ and $\overline{a}\overline{d} = |\Delta|$. Also, $\overline{c} \in Z$ and $\gcd(c,d) = \gcd\left(\overline{c}, \overline{d}\right)$. Let $y \in Z \setminus \{0\}$ be arbitrary but fixed. Then the complete solution to Problem 1^* is $\overline{a}x + \overline{c}y \in S\left(\overline{d}y\right)$ which is equivalent to $\overline{a}x \in S\left(\overline{d}y\right) - \overline{c}y$ where $S\left(\overline{d}y\right)$ is the Euler set defined in Section 4. ■

We note that this final set $\overline{a}x$ may be an empty set for some or all y. In Theorem 2 and Observation 3 we give the necessary and sufficient condition on a, b, c, d such that this final set $\overline{a}x$ is not empty for some $y \in Z \setminus \{0\}$ and we also specify precisely for which $y \in Z \setminus \{0\}$, this final set $\overline{a}x = s\left(\overline{d}y\right) - \overline{c}y$ is not empty.

Observation 2 It is obvious that Problem 1^* has no solutions for $(x,y) \in Z \times Z, \gcd(x,y) = 1$ if $\gcd(a,b,c,d) \neq 1$. Also, from the above solution, we can assume that $\gcd(ax+cy, bx+dy) = \gcd\left(\overline{a}x+\overline{c}y, \overline{d}y\right)$ where $\overline{a}, \overline{d} \in \{1,2,3,\cdots\}, \overline{a} = \gcd(a,b), \overline{a}\overline{d} = |\Delta|, \overline{c} \in Z$ and $\gcd\left(\overline{c}, \overline{d}\right) = \gcd(c,d)$. Therefore, $\gcd(a,b,c,d) = \gcd(\gcd(a,b), \gcd(c,d)) = \gcd\left(\overline{a}, \overline{c}, \overline{d}\right)$.

Theorem 2. Suppose $a, b, c, d \in Z$ are fixed and $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. Also, assume that $\gcd(a,b,c,d) = 1$. Let $\gcd(ax+cy, bx+dy) = \gcd\left(\overline{a}x+\overline{c}y, \overline{d}y\right)$ where $\overline{a}, \overline{d} \in \{1,2,3,\cdots\}, \overline{a} = \gcd(a,b), \overline{a}\overline{d} = |\Delta|, \overline{c} \in Z$ and $\gcd\left(\overline{c}, \overline{d}\right) = \gcd(c,d)$. Also, let $y = 1$.

Then there exists $x \in Z$ such that $\gcd(ax+cy, bx+dy) = \gcd(ax+c, bx+d) = \gcd\left(\overline{a}x+\overline{c}y, \overline{d}y\right) = \gcd\left(\overline{a}x+\overline{c}, \overline{d}\right) = 1$.

Proof. Now $\gcd(a,b,c,d) = 1$ is given and also $\gcd(a,b,c,d) = 1$ is true if and only if $\gcd(\gcd(a,b), \gcd(c,d)) = 1$. Since $\gcd(a,b) = \overline{a}, \gcd(c,d) = \gcd\left(\overline{c}, \overline{d}\right)$ we see that $\gcd(a,b,c,d) = 1$ is true if and only if $\gcd\left(\overline{a}, \overline{c}, \overline{d}\right) = 1$.

Define $\overline{d} = d'd^*, d', d^* \in \{1,2,3,\cdots\}$, where d', d^* are defined by the following two properties.

First, if p is a prime and $p|d'$ then $p|\overline{a}$. Also, $\gcd(\overline{a}, d^*) = 1$.

Therefore, if $y = 1$ we have $\gcd(ax+c, bx+d) = \gcd\left(\overline{a}x+\overline{c}, \overline{d}\right) = \gcd\left(\overline{a}x+\overline{c}, d'd^*\right)$.

Now $\gcd\left(\overline{a}, \overline{c}, \overline{d}\right) = \gcd(\overline{a}, \overline{c}, d'd^*) = 1$.

If p is a prime and $p|d'$ then $p|\overline{a}$. Therefore, $\gcd(\overline{a}, \overline{c}, d') = 1$ implies $\gcd(d', \overline{c}) = 1$.

Also, $\gcd(\overline{a}, d^*) = 1$ by definition. We need to find $x \in Z$ such that $\gcd\left(\overline{a}x+\overline{c}, \overline{d}\right) = \gcd(\overline{a}x+\overline{c}, d'd^*) = 1$. Now for every $x \in Z$ we see that $\gcd(\overline{a}x+\overline{c}, d') = 1$ since if p is a prime and $p|d'$ then $p|\overline{a}$ and $p \nmid \overline{c}$. We now find $x \in \{0,1,2,\cdots,d^*-1\}$ such that $\gcd(\overline{a}x+\overline{c}, d^*) = 1$. We know that $\gcd(\overline{a}, d^*) = 1$. Therefore, the remainders of $\dfrac{\overline{a}x+\overline{c}}{d^*}$ as x ranges over the set $x \in \{0,1,2,\cdots,d^*-1\}$ must all be different. To see this suppose that $x \neq \overline{x}, x, \overline{x} \in \{0,1,2,\cdots,d^*-1\}$ and the remainder of $\dfrac{\overline{a}x+\overline{c}}{d^*}$ equals the remainder of $\dfrac{\overline{a}\overline{x}+\overline{c}}{d^*}$.

This implies that $d^* | (\overline{a}x+\overline{c}) - (\overline{a}\overline{x}+\overline{c})$ which implies that $d^*|\overline{a}(x-\overline{x})$. However, since $\gcd(d^*, \overline{a}) = 1$ and $|x-\overline{x}| \in \{1,2,3,\cdots d^*-1\}$ it is impossible for $d^*|\overline{a}(x-\overline{x})$.

Therefore, there exists $x' \in \{0, 1, 2, \cdots, d^* - 1\}$ such that the remainder of $\dfrac{\overline{a}x' + \overline{c}}{d^*}$ equals 1. Therefore, for this x' $\gcd(\overline{a}x' + \overline{c}, d^*) = 1$.

For this x' we know that $\gcd(\overline{a}x' + \overline{c}, d^*) = 1$. Also of course $\gcd(\overline{a}x' + \overline{c}, d') = 1$.

Therefore, $\gcd(\overline{a}x' + \overline{c}, d'd^*) = 1$. ■

Observation 3 In Problem 1^* we showed that $\gcd(ax + cy, bx + dy) = \gcd\left(\overline{a}x + \overline{c}y, \overline{d}y\right)$ where $\overline{a}, \overline{d} \in \{1, 2, 3, \cdots\}, \overline{c} \in Z$. In the proof of Theorem 2 we showed that $\gcd\left(\overline{a}, \overline{c}, \overline{d}\right) = 1$ and there exists $x \in Z$ such that $\gcd\left(\overline{a}x + \overline{c}, \overline{d}\right) = 1$. Now if $\gcd(\overline{a}, y) \neq 1, y \in Z \setminus \{0\}$, then obviously $\gcd\left(\overline{a}x + \overline{c}y, \overline{d}y\right) \neq 1$ for all $x \in Z, \gcd(x, y) = 1$.

However, if $\gcd(\overline{a}, y) = 1$, where $y \neq 0$, and $\gcd\left(\overline{a}, \overline{c}, \overline{d}\right) = 1$ then obviously $\gcd\left(\overline{a}, \overline{c}y, \overline{d}y\right) = 1$. Therefore, if $\gcd(\overline{a}, y) = 1, y \neq 0$, we can apply Theorem 2 to $\overline{a}, \overline{c}y, \overline{d}y$ to compute $x \in Z$ such that $\gcd\left(\overline{a}x + \overline{c}y, \overline{d}y\right) = 1$. In other words we need $\gcd(\overline{a}, y) = 1$ where $\overline{a} = \gcd(a, b)$ in order for $\gcd(ax + cy, bx + dy) = 1$ for some $x \in Z$. By symmetry we know that $x \in Z \setminus \{0\}$ must satisfy $\gcd(x, \gcd(c, d)) = 1$ in order for $\gcd(ax + cy, bx + dy) = 1$ for some $y \in Z$.

In Section 6, we used Problem 1 to solve Problem 2. If in Problem 2 we now use the assumption that $\gcd(a, b, c, d) = 1$ we can now solve Problem 2 by using Problem 1^*, Theorem 2 and Observation 3 exactly the same way that we used Problem 1 in Section 6 to solve Problem 2. In Section 14, we comment on Problem 2 again when we give the reader a problem to solve.

11 An Example for the Reader

Example 2. Find all $(x, y) \in Z \times Z, (x, y) \neq (0, 0), \gcd(x, y) = 1$ such that $u = 6x + 3y, v = 2x + 6y$ are relatively prime. From the above two conditions $\gcd(x, \gcd(c, d)) = 1$ and $\gcd(\gcd(a, b), y) = 1$, we note that $\gcd(x, \gcd(3, 6)) = \gcd(x, 3) = 1$ and $\gcd(\gcd(6, 2), y) = \gcd(2, y) = 1$.

12 Two Unsolved Problems

Problem 1^* of Section 12 is very easy to extend to n-space. However, we have not extended Theorem 2 and Observation 3 of Section 10 to n-space. Also, we have not solved Problem 3 of Section 7 when we use the new assumption that $\gcd(a, b, d, c) = 1$. This means that we have a two variable problem that we have not solved.

13 A Different Idea

Suppose that $a, b, c, d, e, f \in Z$ are fixed and the rank of $\begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}$ is two.

Also, $(x, y) \in Z \times Z, (x, y) \neq (0, 0)$ and (x, y) are relatively prime.

Define $u = ax + dy, v = bx + ey, w = cx + fy$.

Analogous to Section 3, we can use the Euclidean algorithm on the first column and row transformations to transform the above matrix into $\begin{bmatrix} \overline{a} & \overline{d} \\ 0 & \overline{e} \\ 0 & 0 \end{bmatrix}$. We note that $|\overline{a}| = \gcd(a,b,c)$, $\gcd\left(\overline{d},\overline{e}\right) = \gcd(d,e,f)$ and $\gcd\left(\overline{a},\overline{d},\overline{e}\right) = \gcd(a,b,c,d,e,f)$. Also, we note that $\gcd\left(\left|\begin{matrix} a & d \\ b & e \end{matrix}\right|, \left|\begin{matrix} a & d \\ c & f \end{matrix}\right|, \left|\begin{matrix} b & e \\ c & f \end{matrix}\right|\right)$ is invariant under the following type of transformations.

$\begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix} \rightarrow \begin{bmatrix} a & d \\ b \pm a & e \pm d \\ c & f \end{bmatrix}$. Therefore, $\left\| \begin{matrix} \overline{a} & \overline{d} \\ 0 & \overline{e} \end{matrix} \right\| = \left| \ \overline{ae} \ \right| = \gcd\left(\left|\begin{matrix} a & d \\ b & e \end{matrix}\right|, \left|\begin{matrix} a & d \\ c & f \end{matrix}\right|, \left|\begin{matrix} b & e \\ c & f \end{matrix}\right|\right)$.

Also, $|\overline{a}| = \gcd(a,b,c)$. As in Section 10 we can show that there exists $(x,y) \in Z \times Z, \gcd(x,y) = 1$, such that $\gcd(u,v,w) = \gcd\left(\overline{a}x + \overline{d}y, \overline{e}y\right) = 1$ if and only if $\gcd(a,b,c,d,e,f) = \gcd\left(\overline{a},\overline{d},\overline{e}\right) = 1$. Also, when $\gcd(a,b,c,d,e,f) = 1$ we can find all $(x,y), \gcd(x,y) = 1$, such that $\gcd(u,v,w) = 1$ and show that there are an infinite number of such (x,y). Using $\gcd(a,b,c,d,e,f) = 1$ or $\gcd(a,b,c) = 1$ or $\gcd(d,e,f) = 1$ the reader can use the above ideas to extend the theorems and problems in this paper where $\Delta = \gcd\left(\left|\begin{matrix} a & d \\ b & e \end{matrix}\right|, \left|\begin{matrix} a & d \\ c & f \end{matrix}\right|, \left|\begin{matrix} b & e \\ c & f \end{matrix}\right|\right)$ plays the role of $\Delta = \left|\begin{matrix} a & c \\ b & d \end{matrix}\right|$.

Also, Theorem $1'$ and the 3-space Problem $1'$ can be extended in an analogous way. As an example, Theorem 1 now states that $\gcd(u,v,w) \,|\Delta$ when $\gcd(x,y) = 1$ and $\Delta = \gcd\left(\left|\begin{matrix} a & d \\ b & e \end{matrix}\right|, \left|\begin{matrix} a & d \\ c & f \end{matrix}\right|, \left|\begin{matrix} b & e \\ c & f \end{matrix}\right|\right)$.

The reader can also extend Theorem $1'$ in an analogous way. The idea in this section allows us to use the machinery in this paper to study the gcd for m linear forms in n variables, $m, n \in \{1,2,3,\cdots\}$.

As an example of $n > m$ consider $u = ax+cy+ez, v = bx+dy+fz$, where $a,b,c,d,e,f,x,y,z \in Z, (x,y,z) \neq (0,0,0)$ and $\gcd(x,y,z) = 1$. Also, $\gcd(a,b,c,d,e,f) = 1$ and the rank of $\begin{bmatrix} a & c & e \\ b & d & f \end{bmatrix}$ is two. We want $\gcd(u,v) = 1$. Now u, v are relatively prime if and only if there exists $m, n \in Z$ such that $m[ax + cy + ez] + n[bx + dy + fz] = 1$. This is equivalent to $x[ma + nb] + y[mc + nd] + z[me + nf] = 1$. Since the rank of the above matrix is two and $\gcd(a,b,c,d,e,f) = 1$, we can find all $(m,n) \in Z \times Z, (m,n) \neq (0,0), \gcd(m,n) = 1$ such that $\gcd(ma + nb, mc + nd, me + nf) = 1$.

For each (m,n) we can find all $(x,y,z) \in Z \times Z \times Z, \gcd(x,y,z) = 1$, such that $x(ma + nb) + y(mc + nd) + z(me + nf) = 1$.

14 Final Remarks

As stated previously in Note 4 of Section 6 it is fairly easy to see that a slightly modified Problem 2 of Section 6 can be solved by using the machinery developed in Section 10 when we only use the one single condition on $a, b, c, d \in Z$ that $\Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$. Then we show that $\gcd(u, v) = \dfrac{|\Delta|}{\theta}$ for some $(x, y) \in Z \times Z, \gcd(x, y) = 1, \theta = \gcd(a, b, c, d)$. We leave this as an easy problem for the reader.

Of course, if $\gcd(a, b, c, d) = \theta$ then $\theta^2 | \Delta$. Also, it is now very easy to see that for $u = ax + cy, v = bx + dy$, where $a, b, c, d \in Z, \Delta = \begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$ that $\gcd(u, v) = 1$ for all $(x, y) \in Z \times Z, (x, y) \neq (0, 0), \gcd(x, y) = 1$ if and only if $\gcd(a, b, c, d) = 1$ and $\Delta = \pm 1$.

Of course, $\gcd(a, b, c, d) = 1$ is redundant since $\Delta \pm 1$ implies $\gcd(a, b, c, d) = 1$. Also, as stated previously we are not completely satisfied with the n-space generalization of Problem 2. However, as pointed out in Section 8 this appears to be a defect in the mathematics itself. Also, as a final remark the reader might like to think about one linear form in n variables. An example would be $ax + by$. As a specific example of what we can do the reader might like to use Sections 3, 4 to solve the following.

Suppose $a, b, c \in Z \setminus \{0\}$ and $\gcd(a, b) = 1$. Show that there exists an infinite number of $(x, y) \in Z \times Z, (x, y) \neq (0, 0), \gcd(x, y) = 1$ such that $ax + by = c$. Also, find all such (x, y). It is easy to find $(x, y) \in Z \times Z$ such that $ax + by = c$. Also, we note that if $ax + by = c$ then $a[x + tb] + b[y - ta] = c, t \in Z$ are all of the solutions to $ax + by = c$ if we require $x, y \in Z$. In solving $ax + by = c$, we are requiring $\gcd(x, y) = 1$. Therefore, we need $\gcd(x + tb, y - ta) = 1$. Using Sections 3, 4 we can easily compute all such $t \in Z$ since $\gcd(a, b) = 1$ and $\Delta = \begin{vmatrix} x & b \\ y & -a \end{vmatrix} = -ax - by = -c \neq 0$. As another example, suppose that $a, b, c, d \in Z \setminus \{0\}, \gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. Find an infinite number of $(x, y, z) \in Z \times Z \times Z, (x, y, z) \neq (0, 0, 0), \gcd(x, y, z) = 1$ such that $bcx + acy + abz = d$. We note that $\gcd(bc, ac, ab) = 1$. Therefore, there exists $(x, y, z) \in Z \times Z \times Z$ such that $bcx + acy + abz = d$. If $bcx + acy + abz = d$ then $bc[x + ra] + ac[y + sb] + ab[z + tc] = d$ where $r, s, t \in Z, r + s + t = 0$.

Indeed, if $bcx + acy + abz = d$ and $bc[x + \overline{x}] + ac[y + \overline{y}] + ab(z + \overline{z}) = d$ where $\overline{x}, \overline{y}, \overline{z} \in Z$ then $bc\overline{x} + ac\overline{y} + ab\overline{z} = 0$. Now $a | bc\overline{x}, b | ac\overline{y}, c | ab\overline{z}$. Since $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$ we see that $\overline{x} = ar, \overline{y} = bs, \overline{z} = ct, r, s, t \in Z$ and $r + s + t = 0$. We now let $r = -2t, s = t$. We want $t \in Z$ so that $\gcd(x - 2a\overline{r}, y + bt, z + ct) = 1$. Also, we want to find an infinite number of t.

We now represent $x - 2at, y + bt, z + ct$ by the matrix $\begin{bmatrix} x & -2a \\ y & b \\ z & c \end{bmatrix}$. Noting that $\gcd(2a, b, c) = 1$, we now use Sections 3, 4 with this matrix after we show that the rank of this matrix is two.

To show that the rank is two suppose that $yc-bz=0, xc+2az=0$. Then $bcx+acy+abz=d$ becomes $-2abz+abz+abz=0=d\neq 0$, which is a contradiction. Therefore, the rank of the matrix is two. We can extend the above pattern arbitrarily far.

References

[1] https://en.wikipedia.org/wiki/Matrix

[2] https://en.wikipedia.org/wiki/Euclidean_algorithm

[3] H. Reiter and A. Holshouser, Generating Stern-Brocot type Rational Numbers with Mediants, Missouri J of Mathematical Sciences. Vol. 30, No. 1, Spring, 2018.