1. (a) The lexicographically least point is (2,3), so our list becomes

\[(4,4), (2,7), (3,1), (0,0), (-2,2), (2,0), (-1,6), (3,5), (1,5), (2,2)\]

(b) First note that the fractions \(x/y\) for each point \((x, y) \neq (0,0)\) in our list are sorted in decreasing order as follows:

\[2/0, 3/1, 2/2, 4/4, 3/5, 2/7, 1/5, -1/6, -2/2\,.

Thus the points are sorted in increasing polar angle (only retaining points furthest from \(P_0\) with the same polar angle) as follows:

\[(2,0), (3,1), (4,4), (3,5), (2,7), (1,5), (-1,6), (-2,2)\,.

(c) The above points are named \(P_1\) to \(P_8\) in that order and we initialize \(I = 2\).

Outer loop \(J = 3\):

\[\Delta_{P_1P_2P_3} = \begin{vmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 0 & 1 & 4 \end{vmatrix} = (12 - 4) - (8 - 0) + (2 - 0)\]

\[= 8 - 8 + 2 = 2 > 0\]

so \(\Delta_{P_1P_2P_3}\) is anticlockwise; increment \(I = 3\).

Outer loop \(J = 4\):

\[\Delta_{P_2P_3P_4} = \begin{vmatrix} 1 & 1 & 1 \\ 3 & 4 & 3 \\ 1 & 4 & 5 \end{vmatrix} = (20 - 12) - (15 - 3) + (12 - 4)\]

\[= 8 - 12 + 8 = 4 > 0\]

so \(\Delta_{P_2P_3P_4}\) is anticlockwise; increment \(I = 4\).

Outer loop \(J = 5\):

\[\Delta_{P_3P_4P_5} = \begin{vmatrix} 1 & 1 & 1 \\ 4 & 3 & 2 \\ 4 & 5 & 7 \end{vmatrix} = (21 - 10) - (28 - 8) + (20 - 12)\]

\[= 11 - 20 + 8 = -1 < 0\]

so \(\Delta_{P_3P_4P_5}\) is clockwise; decrement \(I = 3\), which will delete the point \((3,5)\).

\[\Delta_{P_2P_3P_5} = \begin{vmatrix} 1 & 1 & 1 \\ 3 & 4 & 2 \\ 1 & 4 & 7 \end{vmatrix} = (28 - 14) - (21 - 2) + (12 - 4)\]

\[= 14 - 19 + 8 = 3 > 0\]
so $\Delta P_2 P_3 P_5$ is anticlockwise; reassign $P_4 = (2, 7)$; increment $I = 4$.

Outer loop $J = 6$:

$$\Delta_{P_3 P_4 P_6} = \det \begin{bmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 4 & 7 & 5 \end{bmatrix} = (10 - 7) - (20 - 4) + (28 - 8)$$
$$= 3 - 16 + 20 = 7 > 0$$

so $\Delta P_3 P_4 P_6$ is anticlockwise; reassign $P_5 = (1, 5)$; increment $I = 5$.

Outer loop $J = 7$:

$$\Delta_{P_4 P_5 P_7} = \det \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & -1 \\ 7 & 5 & 6 \end{bmatrix} = (6 + 5) - (12 + 7) + (10 - 7)$$
$$= 11 - 19 + 3 = -5 < 0$$

so $\Delta P_4 P_5 P_7$ is clockwise; decrement $I = 4$, which will delete the point $(1, 5)$.

$$\Delta_{P_3 P_4 P_7} = \det \begin{bmatrix} 1 & 1 & 1 \\ 4 & 2 & -1 \\ 4 & 7 & 6 \end{bmatrix} = (12 + 7) - (24 + 4) + (28 - 8)$$
$$= 19 - 20 + 20 = 19 > 0$$

so $\Delta P_3 P_4 P_7$ is anticlockwise; reassign $P_5 = (-1, 6)$; increment $I = 5$.

Outer loop $J = 8$:

$$\Delta_{P_4 P_5 P_8} = \det \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -2 \\ 7 & 6 & 2 \end{bmatrix} = (-2 + 12) - (4 + 14) + (12 + 7)$$
$$= 10 - 18 + 19 = 11 > 0$$

so $\Delta P_4 P_5 P_8$ is anticlockwise; reassign $P_6 = (-2, 2)$; increment $I = 6$.

Halt and output the new $P_0, P_1, \ldots, P_6$:

$$(0, 0), (2, 0), (3, 1), (4, 4), (2, 7), (-1, 6), (-2, 2).$$

(d) Adding the coordinates $(2, 3)$ yields the convex hull of $X$ as a polygon in standard form:

$$(2, 3), (4, 3), (5, 4), (6, 7), (4, 10), (1, 9), (0, 5).$$

2. (a) Observe that $190 = 3(55) + 25$, so $q = 3$ and $r = 25$.

(b) Observe that $1001 = 58(17) + 15$, so $q = 58$ and $r = 15$.

(c) Observe that $-1001 = 59(-17) + 2$, so $q = 59$ and $r = 2$. 

3. Consider first $b > 0$. We have

$$\frac{a}{b} = \left\lfloor \frac{a}{b} \right\rfloor + c$$

for some $c$ satisfying $0 \leq c < 1$, giving

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + cb$$

where we have $0 \leq cb < b$, giving $r = cb$ and $q = \lfloor a/b \rfloor$.

Now consider $b < 0$. We have

$$\frac{a}{b} = \left\lceil \frac{a}{b} \right\rceil - c$$

for some $c$ satisfying $0 \leq c < 1$, giving

$$a = \left\lceil \frac{a}{b} \right\rceil b - cb$$

where we have $0 \leq -cb < -b$, giving $r = -cb$ and $q = \lceil a/b \rceil$.

These observations combine to give the formula

$$q = \begin{cases} 
\lfloor a/b \rfloor & \text{if } b > 0 \\
\lceil a/b \rceil & \text{if } b < 0.
\end{cases}$$

4. (a) The algorithm produces the following steps:

$$
\begin{align*}
190 & = 3(55) + 25 \\
55 & = 2(25) + 5 \\
25 & = 5(5) + 0
\end{align*}
$$

so the greatest common divisor is 5.

(b) The algorithm produces the following steps:

$$
\begin{align*}
1001 & = 38(17) + 15 \\
17 & = 15 + 2 \\
15 & = 7(2) + 1 \\
2 & = 2(1) + 0
\end{align*}
$$

so the greatest common divisor is 1.
(c) The algorithm produces the following steps:

\[
egin{align*}
100011 & = 9(10011) + 9912 \\
10011 & = 9912 + 99 \\
9912 & = 100(99) + 12 \\
99 & = 8(12) + 3 \\
12 & = 4(3) + 0
\end{align*}
\]

so the greatest common divisor is 3.

(d) The algorithm produces the following steps:

\[
egin{align*}
2^{20} & = 1048576 = 2621(400) + 176 \\
400 & = 2(176) + 48 \\
176 & = 3(48) + 32 \\
48 & = 32 + 16 \\
32 & = 2(16) + 0
\end{align*}
\]

so the greatest common divisor is 16.

5. The algorithm produces the following steps:

\[
egin{align*}
987 & = 610 + 377 \\
610 & = 377 + 233 \\
377 & = 233 + 144 \\
233 & = 144 + 89 \\
144 & = 89 + 55 \\
89 & = 55 + 34 \\
55 & = 34 + 21 \\
34 & = 21 + 13 \\
21 & = 13 + 8 \\
13 & = 8 + 5 \\
8 & = 5 + 3 \\
5 & = 3 + 2 \\
3 & = 2 + 1 \\
2 & = 2(1) + 0
\end{align*}
\]

so the greatest common divisor is 1. The remainders are Fibonacci numbers.

6. My (fictional!) staff number is 1001943. Suppose for argument’s sake that the
student number is 0345678. Then the algorithm produces the following steps:

\[
\begin{align*}
1001943 & = 2(345678) + 310587 \\
3454678 & = 310587 + 35091 \\
310587 & = 8(35091) + 29859 \\
35091 & = 29859 + 5232 \\
29859 & = 3699 + 1533 \\
3699 & = 2(1533) + 633 \\
1533 & = 2(633) + 267 \\
633 & = 2(267) + 99 \\
267 & = 2(99) + 69 \\
99 & = 69 + 30 \\
69 & = 2(30) + 9 \\
30 & = 3(9) + 3 \\
9 & = 3(3) + 0
\end{align*}
\]

so the greatest common divisor is 3, and the numbers are not coprime.

**7.** The equations which appear in the Euclidean Algorithm are

\[
\begin{align*}
 a & = q_1 r_1 + r_2 & (b = r_1) \\
 r_1 & = q_2 r_2 + r_3 \\
 r_2 & = q_3 r_3 + r_4 \\
 & \vdots \\
 r_{s-2} & = q_{s-1} r_{s-1} + r_s \\
 r_{s-1} & = q_s r_s + 0
\end{align*}
\]

We claim that each remainder \( r_i \) can be expressed as an integer linear combination of \( a \) and \( b \). The induction begins because

\[
\begin{align*}
 r_1 & = 0(a) + 1(b) & \text{and} & & r_2 & = 1(a) - q_1(b) .
\end{align*}
\]

Suppose as inductive hypothesis that \( 2 < i \leq s \) and

\[
\begin{align*}
 r_{i-1} & = x a + y b & \text{and} & & r_{i-2} & = z a + w b
\end{align*}
\]

for some \( x, y, z, w \). But

\[
\begin{align*}
 r_{i-2} & = q_{i-1} r_{i-1} + r_i ,
\end{align*}
\]

so

\[
\begin{align*}
 r_i & = r_{i-2} - q_{i-1} r_{i-1} \\
 & = z a + w b - q_{i-1} (x a + y b) \\
 & = (z - q_{i+1} x) a + (w - q_{i-1} y) b ,
\end{align*}
\]
which is an integer linear combination of \( a \) and \( b \), completing the inductive step. The claim follows now by induction. In particular the greatest common divisor \( r \) is an integer linear combination of \( a \) and \( b \).

*8. From the previous question,

\[
c = xa + yb
\]

for some \( y, b \), and

\[
a = zd \quad \text{and} \quad b = wd
\]

for some \( z, w \), so that

\[
c = xzd + ywd = (xz + yw)d,
\]

which is a multiple of \( d \).

9. (a) \( \text{l.c.m.}(2, 3) = 6, \text{l.c.m.}(4, 12) = 12, \text{l.c.m.}(4, 10) = 20, \text{l.c.m.}(6, 15) = 30. \)

*(b) Suppose \( m = ax = by \) for some \( x, y \). Put \( \ell = \text{l.c.m.}(a, b) \) so \( \ell = az = bw \) for some \( z, w \). But \( m = q\ell + r \) for some \( q, r \) with \( 0 \leq r < \ell \), so

\[
r = m - q\ell = ax - qaz = a(x - qz)
\]

and

\[
r = m - q\ell = by - qbw = b(y - qw).
\]

Thus \( r \) is a multiple of \( a \) and \( b \). If \( r > 0 \) then \( r \geq \ell \), a contradiction. Hence \( r = 0 \), so \( m = q\ell \) is a multiple of \( \ell \).

*(c) Put \( \ell = \text{l.c.m.}(a, b) \) and \( g = \gcd(a, b) \). Then \( gx = a, gy = b, \ell = az = bw \) for some \( x, y, z, w \). Hence \( ab/g = xb = ya \) is a multiple of \( a \) and \( b \), so \( ab/g \geq \ell \). By (b), \( ab/\ell \) is an integer and we have \( (ab/\ell)z = b, (ab/\ell)w = a \), so \( ab/\ell \) divides \( a \) and \( b \), whence \( ab/\ell \leq g \). Hence \( ab \geq \ell g \geq ab \), so \( \ell g = ab \).

An algorithm, therefore, for finding least common multiples, is to first apply the Euclidean Algorithm to find \( g \) and then compute \( \ell = ab/g \).

*(d) If \( a, b \) are coprime then in (a), \( g = 1 \) so \( \ell = ab \); but by (b), \( \ell | c \), so \( c \) is a multiple of \( ab \).

**10. Suppose \( p|ab \), say \( ab = pq \). Suppose \( p \nmid a \). Then \( \gcd(p, a) = 1 \) since \( p \) is prime. By an earlier question, \( 1 = ax + by \) for some \( x, y, \) so

\[
b = b(ax + py) = abx + bpy = pqx + pby = p(qx + by),
\]

which shows \( p|b \).