MATH 135 Algebra, Solutions to Assignment 4

1: For each of the following pairs (a, b), find integers q and r with $0 \leq r < |b|$ such that $a = bq + r$.

(a) $a = 753$, $b = 21$

Solution: Using long division (or using a calculator) we find that $753 = 21 \cdot 35 + 18$, so $q = 35$ and $r = 18$.

(b) $a = -5124$, $b = 316$

Solution: Using long division (or using a calculator) we find that $5124 = 316 \cdot 16 + 68$, and so we have $-5124 = 316(-16) - 68 = 316(-17) + 316 - 68 = 316(-17) + 248$. Thus $q = -17$ and $r = 248$.

(c) $a = 4137$, $b = -152$

Solution: Using long division (or using a calculator) we find that $4137 = 152 \cdot 27 + 33 = (-152)(-27) + 33$, and so $q = -27$ and $r = 33$.

2: For each of the following pairs (a, b), find $\gcd(a, b)$.

(a) $a = 78$, $b = 34$

Solution: Applying the Euclidean Algorithm gives

$$\begin{aligned} 78 &= 2 \cdot 34 + 10 \\ 34 &= 3 \cdot 10 + 4 \\ 10 &= 2 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

and so $\gcd(a, b) = 2$.

(b) $a = 456$, $b = 1273$

Solution: The Euclidean Algorithm gives

$$\begin{aligned} 1273 &= 2 \cdot 456 + 361 \\ 456 &= 1 \cdot 361 + 95 \\ 361 &= 3 \cdot 95 + 76 \\ 95 &= 1 \cdot 76 + 19 \\ 76 &= 4 \cdot 19 + 0 \end{aligned}$$

and so $\gcd(a, b) = \gcd(1273, 456) = 19$.

(c) $a = -1205$, $b = 2501$

Solution: The Euclidean Algorithm gives

$$\begin{aligned} 2501 &= 2 \cdot 1205 + 91 \\ 1205 &= 13 \cdot 91 + 22 \\ 91 &= 4 \cdot 22 + 3 \\ 22 &= 7 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

so we have $\gcd(a, b) = \gcd(2501, 1205) = 1$.

3: For each of the following pairs (a, b), find $d = \gcd(a, b)$ then find integers s and t such that $as + bt = d$.

(a) $a = 60$, $b = 35$

Solution: The Euclidean Algorithm gives

$$60 = 1 \cdot 35 + 25 \ , \quad 35 = 1 \cdot 25 + 10 \ , \quad 25 = 2 \cdot 10 + 5 \ , \quad 10 = 2 \cdot 5 + 0$$

so we have $d = \gcd(a, b) = 5$. Back-Substitution then gives rise to the sequence

$$1 \ , \quad -2 \ , \quad 3 \ , \quad -5$$

so we have $60 \cdot 3 - 35 \cdot 5 = 5$ and can take $s = 3$ and $t = -5$. Alternatively, the Extended Euclidean Algorithm gives rise to the table

$$\begin{array}{ccc} 1 & 0 & 60 \\ 0 & 1 & 35 \\ 1 & -1 & 25 \\ -1 & 2 & 10 \\ 3 & -5 & 5 \end{array}$$

so we have $60 \cdot 3 - 35 \cdot 5 = 5$ and can take $s = 3$ and $t = -5$.

(b) $a = 239$, $b = 759$

Solution: The Euclidean Algorithm gives

$$759 = 3 \cdot 239 + 42 \ , \quad 239 = 5 \cdot 42 + 29 \ , \quad 42 = 1 \cdot 29 + 13 \ , \quad 29 = 2 \cdot 13 + 3 \ , \quad 13 = 4 \cdot 3 + 1 \ , \quad 3 = 3 \cdot 1 + 0$$

so we have $d = \gcd(a, b) = 1$. Back-Substitution then gives rise to the sequence

$$1 \ , \quad -4 \ , \quad 9 \ , \quad -13 \ , \quad 74 \ , \quad -235$$

so we have $759 \cdot 74 - 239 \cdot 235 = 1$ and can take $s = -235$ and $t = 74$. Alternatively, the Extended Euclidean Algorithm gives rise to the table

$$\begin{array}{ccc} 1 & 0 & 759 \\ 0 & 1 & 239 \\ 1 & -3 & 42 \\ -5 & 16 & 29 \\ 6 & -19 & 13 \\ -17 & 54 & 3 \\ 74 & -235 & 1 \end{array}$$

so we have $759 \cdot 74 - 239 \cdot 235 = 1$ and can take $s = -235$ and $t = 74$.

(c) $a = -5083$, $b = 1656$

Solution: The Euclidean Algorithm gives

$$5083 = 3 \cdot 1656 + 115 \ , \quad 1656 = 14 \cdot 115 + 46 \ , \quad 115 = 2 \cdot 46 + 23 \ , \quad 46 = 2 \cdot 23 + 0$$

so we have $d = \gcd(a, b) = 23$. Back-Substitution then gives rise to the sequence

$$1 \ , \quad -2 \ , \quad 29 \ , \quad -89$$

so we have $5083 \cdot 29 - 1656 \cdot 89 = 23$ and can take $s = -29$ and $t = -89$. Alternatively, the Extended Euclidean Algorithm gives rise to the table

$$\begin{array}{ccc} 1 & 0 & 5083 \\ 0 & 1 & 1656 \\ 1 & -3 & 115 \\ -14 & 43 & 46 \\ 29 & -89 & 23 \end{array}$$

so we have $5083 \cdot 29 - 1656 \cdot 89 = 23$ and can take $s = -29$ and $t = -89$.

4: Prove each of the following statements.

(a) For all integers a, b we have $\gcd(a, b) = \gcd(2a + b, 3a + 2b)$.

Solution: We provide two proofs. For the first proof, let $d = \gcd(a, b)$ and let $e = \gcd(2a + b, 3a + 2b)$. Since $d = \gcd(a, b)$ we have $d\big|a$ and $d\big|b$ and so $d\big|(ax + by)$ for any integers x, y by Proposition 2.11(ii). In particular, $d\big|2a+b$ and $d\big|3a+2b$. Since d is a common divisor of $2a+b$ and $3a+2b$, e is the greatest common divisor of $2a + b$ and $3a + 2b$, we must have $d \leq e$. On the other hand, since $e = \gcd(2a + b, 3a + 2b)$, we have $e\big|(2a + b)$ and $e\big|(2a + 3b)$ and so $e\big|(2a + b)x + (3a + 2b)y$ for any integers x, y, by Proposition 2.11(ii). In particular $e\big|2(2a + b) - 1(3a + 2b)$, that is $e\big|a$, and $e\big| - 3(2a + b) + 2(3a + 2b)$, that is $e\big|b$. Since e is a common divisor of a and b, and d is the greatest common divisor of a and b, we must have $e \leq d$. We have shown that $d \leq e$ and that $e \leq d$, so we must have $d = e$.

We now give a second proof. Taking $a = x$, $b = y$, $q = -1$ and $r = a - bq = x + y$ in Proposition 2.21 gives $\gcd(x, y) = \gcd(y, x + y)$, or equivalently $\gcd(x, y) = \gcd(x + y, y)$. Reversing the roles of x and y gives $\gcd(x, y) = \gcd(y, x) = \gcd(x, x + y)$. Thus we obtain the following two rules: for all integers x and y,

$$\gcd(x, y) = \gcd(x, x + y) \text{ , and } \gcd(x, y) = \gcd(x + y, y) .$$

Using these two rules, we have

$$\begin{aligned} \gcd(a, b) &= \gcd(a, a + b) \\ &= \gcd\big(a + (a + b), a + b\big) = \gcd(2a + b, a + b) \\ &= \gcd\big(2a + b, (a + b) + (2a + b)\big) = \gcd(2a + b, 3a + 2b), . \end{aligned}$$

(b) For all integers a, b, c with $c > 0$ we have $\gcd(ac, bc) = c \gcd(a, b)$.

Solution: Let $d = \gcd(a, b)$ and let $e = \gcd(ac, bc)$. We must show that $e = dc$. Since $c\big|ac$ and $c\big|bc$ we have $c\big|e$ (by Proposition 2.29), say $e = kc$. Since $e\big|ac$, so $kc\big|ac$, we have $k\big|a$, and since $e\big|bc$, so $kc\big|bc$, we have $k\big|b$, and so k is a common divisor of a and b. Since d is the greatest common divisor of a and b, we must have $k \leq d$, and hence $kc \leq dc$, that is $e \leq dc$. On the other hand, we have $d\big|a$ so $dc\big|ac$, and we have $d\big|b$ so $dc\big|bc$, and so dc is a common divisor of ac and bc. Since e is the greatest common divisor of ac and bc, we must have $dc \leq e$. We have shown that $e \leq dc$ and that $dc \leq e$, so we have $e = dc$, as required.

(c) For all integers a, b, c we have $\gcd(ab, c) = 1$ if and only if $\gcd(a, c) = \gcd(b, c) = 1$.

Solution: Suppose first that $\gcd(ab, c) = 1$. Using Back Substitution, or the Extended Euclidean Algorithm, we can find integers x and y so that $abx + cy = 1$. By Proposition 2.27, since $a(bx) + c(y) = 1$ we have $\gcd(a, c) = 1$, and since $b(ax) + c(y) = 1$ we have $\gcd(b, c) = 1$.

Conversely, suppose that $\gcd(a, c) = \gcd(b, c) = 1$. By Back Substitution, or by the Extended Euclidean Algorithm, we can choose integers s, t, u and v such that $as + ct = 1$ and $bu + cv = 1$. Then we have $1 = (as + ct)(bu + cv) = ab(su) + c(asv + tbu + tcv)$, and so $\gcd(ab, c) = 1$ by Proposition 2.27.

5: Use long division of polynomials to solve the following problems. (You may find it useful to read part of section 9.1 in the text. An example of long division of polynomials is on page 229, and the statement and proof of the Division Algorithm for Polynomials is on page 230).

(a) Let $a(x) = 4x^5 - x^3 + 2x^2 - 3x + 5$ and $b(x) = 2x^2 + x + 3$. Find polynomials $q(x)$ and $r(x)$ with $\deg(r(x)) < \deg(b(x))$ such that $a(x) = b(x)q(x) + r(x)$.

Solution: Long division of polyomials gives

$$\begin{array}{rr}
 & 2x^3 - x^2 - 3x + 4 \\
\hline
2x^2 + x + 3 \;\big)\; & 4x^5 + 0x^4 - 1x^3 + 2x^2 - 3x + 5 \\
 & \underline{4x^5 + 2x^4 + 6x^3} \\
 & -2x^4 - 7x^3 + 2x^2 \\
 & \underline{-2x^4 - x^3 - 3x^2} \\
 & -6x^3 + 5x^2 - 3x \\
 & \underline{-6x^3 - 3x^2 - 9x} \\
 & 8x^2 + 6x + 5 \\
 & \underline{8x^2 + 4x + 12} \\
 & 2x - 7
\end{array}$$

Thus we can take $q(x) = 2x^3 - x^2 - 3x + 4$ and $r(x) = 2x - 7$.

(b) Let $a(x) = 2x^3 - 3x^2 - 2x + 8$ and $b(x) = x^2 - 3x + 3$. Find polynomials $s(x)$ and $t(x)$ such that $a(x)s(x) + b(x)t(x) = 1$.

Solution: Notice that the proofs of Euclidean Algorithm, Back Substitution, and the Extended Euclidean Algorithm can all modified so that they can be applied in the case that $a = a(x)$ and $b = b(x)$ are polynomials. The Euclidean Algorithm gives

$$\begin{array}{rr}
 & 2x + 3 \\
\hline
x^2 - 3x + 3 \;\big)\; & 2x^3 - 3x^2 - 2x + 8 \\
 & \underline{2x^3 - 6x^2 + 6x} \\
 & 3x^2 - 8x + 8 \\
 & \underline{3x^2 - 9x + 9} \\
 & x - 1
\end{array}
\qquad\qquad
\begin{array}{rr}
 & x - 2 \\
\hline
x - 1 \;\big)\; & x^2 - 3x + 3 \\
 & \underline{x^2 - x} \\
 & -2x + 3 \\
 & \underline{-2x + 2} \\
 & 1
\end{array}$$

and so we have $d(x) = \gcd\big(a(x), b(x)\big) = 1$. Back-Substitution gives rise to the sequence

$$1\ ,\quad -(x-2)\ ,\quad 1 + (x-2)(2x+3) = 2x^2 - x - 5$$

so we have $(x^2 - 3x + 3)(2x^2 - x - 5) - (2x^3 - 3x^2 - 2x + 8)(x - 2) = 1$, and we can take $s(x) = -x + 2$ and $t(x) = 2x^2 - x - 5$. Alternatively, the Extended Euclidean Algorithm gives rise to the table

$$\begin{array}{cccc}
1 & 0 & 2x^3 - 3x^2 - 2x + 8 \\
0 & 1 & x^2 - 3x + 3 \\
1 & -(2x+3) & x - 1 \\
-(x-2) & 2x^2 - x - 5 & 1
\end{array}$$

so we have $(x^2 - 3x + 3)(2x^2 - x - 5) - (2x^3 - 3x^2 - 2x + 8)(x - 2) = 1$, and we can take $s(x) = -x + 2$ and $t(x) = 2x^2 - x - 5$.