MATH 135: Extra Practice Set 5
January 11^{th} 2017
Jay Ching Lim

Question 1. *(a) Use the Extended Euclidean Algorithm to find three integers x, y and $d = gcd(1112, 768)$ such that $1112x + 768y = d$. (b) Determine integers s and t such that $768s - 1112t = gcd(768, -1112)$.*

(a) We have $1112x + 768y = \gcd(1112, 768) = d$. By EEA,

x	y	r	q
1	0	1112	0
0	1	768	0
1	-1	344	1
-2	3	80	2
9	-13	24	4
-29	42	8	3
96	-139	0	3

From the second last row, we have

$$1112(-29) + 768(42) = \gcd(1112, 768) = 8.$$

Thus, $x = -29$, $y = 42$, and $d = 8$.

(b) Observe that $\gcd(768, -1112) = \gcd(-1112, 768) = \gcd(1112, 768)$.

Let $s = y$ and $t = -x$. Then we need to determine integers s and t such that $768y + 1112x = \gcd(1112, 768)$, which is the same equation as before. Since we have $1112(-29) + 768(42) = \gcd(1112, 768) = 8$, we can deduce that $s = 42$ and $t = -(-29) = 29$.

Question 2. *Prove that for all $a \in \mathbb{Z}$, $gcd(9a + 4, 2a + 1) = 1$.*

Proof. Let $a \in \mathbb{Z}$. We will apply GCD WR repeatedly.

Since $9a + 4 = 4(2a + 1) + a$, $\gcd(9a + 4, 2a + 1) = \gcd(2a + 1, a)$.
Since $2a + 1 = 2(a) + 1$, $\gcd(2a + 1, a) = \gcd(a, 1)$.
Since $a = a(1) + 0$, $\gcd(a, 1) = \gcd(1, 0) = |1| = 1$.

By the chain of equalities, we get

$$\begin{aligned}\gcd(9a+4, 2a+1) &= \gcd(2a+1, a)\\ &= \gcd(a, 1)\\ &= \gcd(1, 0)\\ &= |1|\\ &= 1, \text{ as required.}\end{aligned}$$

□

Question 3. *Let gcd$(x, y) = d$. Express gcd$(18x+3y, 3x)$ in terms of d and prove that you are correct.*

We know that $18x+3y = 6(3x)+3y$. So by GCD WR, $\gcd(18x+3y, 3x) = \gcd(3x, 3y) = 3 \cdot \gcd(x, y) = 3d$.

Proof. Since $d = gcd(x, y)$, $d|x$ and $d|y$ by the definition of gcd. By the definition of divisibility, $\exists k \in \mathbb{Z}$ such that $dk = x$. Multiplying this by 3, we get $(3d)k = 3x$. Since $k \in \mathbb{Z}$, $3d|3k$. Also, $\exists h \in \mathbb{Z}$ such that $dh = y$ and a similar argument shows that $3d|3y$.

By BL, $\exists x_1, y_1 \in \mathbb{Z}$ such that

$$xx_1 + yy_1 = d.$$

Multiplying the equation by 3 yields

$$(3x)x_1 + (3y)y_1 = 3d.$$

Using our previous results, i.e. $3d|3x$ and $3d|3y$ together with the fact that $\exists x_1, y_1 \in \mathbb{Z}$ such that $(3x)x_1+(3y)y_1 = 3d$, we can apply GCD CT to deduce that $\gcd(18x + 3y, 3x) = 3d$, as required.

□

Question 4. *Prove that if $gcd(a, b) = 1$, then $gcd(2a + b, a + 2b) \in \{1, 3\}$.*

Proof. Assume that $gcd(a, b) = 1$. Let $d = gcd(2a + b, a + 2b)$. By the definition of gcd, $d|(2a + b)$ and $d|(a + 2b)$. By DIC,

$$d|[2(2a + b) + (-1)(a + 2b)] \implies d|3a.$$

Again, by DIC,

$$d|[(-1)(2a + b) + 2(a + 2b)] \implies d|3b.$$

By GCD OO, $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying this equation by 3, we get $(3a)x+(3b)y = 3$. By the definition of divisibility, $\exists k \in \mathbb{Z}$ such that $dk = 3a$ and $\exists h \in \mathbb{Z}$ such that $dh = 3b$. Substituting $3a = dk$ and $3b = dh$ into the previous equation, we get $(dk)x + (dh)y = 3 \iff d(kx + hy) = 3$. Since $k, x, h, y \in \mathbb{Z}$, $kx + hy \in \mathbb{Z}$. So by definition of divisibility, $d|3$. The only possible values of d are 1 and 3, i.e. $d = gcd(2a + b, a + 2b) \in \{1, 3\}$, as required.

$\square$

Question 5. *Prove that for every integer k, $gcd(a, b) \leq gcd(ak, b)$.*

Proof. Let $k \in \mathbb{Z}$, $d_1 = gcd(a, b)$ and $d_2 = gcd(ak, b)$. By definition of gcd, $d_1|a$ and $d_1|b$. Clearly, $a|ak$. By TD, since $d_1|a$ and $a|ak$, $d_1|ak$. Applying the definition of gcd on d_2, we know that $\forall c \in \mathbb{Z}$, if $c|ak$ and $c|b$, then $c \leq gcd(ak, b) = d_2$. Since $d_1|ak$ and $d_1|b$, we can let $c = d_1$ to deduce that $d_1 \leq d_2$. Thus, $gcd(a, b) \leq gcd(ak, b)$, as required.

$\square$

Question 6. *Given a rational number r, prove that there exist coprime integers p and q, with $q \neq 0$, so that $r = \frac{p}{q}$.*

Question 7. *Prove that: if $a \mid c$ and $b \mid c$ and $gcd(a, b) = 1$, then $ab \mid c$.*

Question 8. *Let $a, b, c \in \mathbb{Z}$. Prove that if $gcd(a, b) = 1$ and $c \mid a$, then $gcd(b, c) = 1$.*

Question 9. *Prove that if $gcd(a, b) = 1$, then $gcd(a^m, b^n) = 1$ for all $m, n \in \mathbb{N}$. You may use the result of an example in the notes.*

Question 10. *Suppose a, b and n are integers. Prove that $n \mid gcd(a, n) \cdot gcd(b, n)$ if and only if $n \mid ab$.*