HW # 3 Solutions

$\boxed{6.1}$ Through the Euclidean Algorithm (or otherwise),

(a) $12345 \cdot 11 - 67890 \cdot 2 = 15 = \gcd(12345, 67890)$

[Any solution will do]

(b) $54321 \cdot (-1645) + 9876 \cdot 9048 = 3 = \gcd(54321, 9876)$.

$\boxed{6.2}$ (a) With the Euclidean Algorithm, we find one solution. The rest come from adding/subtracting suitable multiples.

The answers are

$$105 \cdot (-53 + 121k) + 121(46 - 105k) = 1 \quad \text{for any } k \text{ in } \mathbb{Z}.$$

(b) $(11 + 4526k) \cdot 12345 + (-2 - 823k) \cdot 67890 = 15$.

Note that there are more answers than just

$+67890k$ and $-\cancel{}\ 12345k$.

We get the correct multiples by dividing by the gcd, e.g. $\frac{12345}{15} = 823$.

(c) $(-1645 + 3292k) \cdot 54321 + (9048 - 18107k) 9876 = 3$.

Side Note: the work from 6.1 feeds into the work for 6.2.

$\boxed{6.4}$ The method looks like this.

Solve $6x + 15y = \gcd(6,15) = 3$. One solution is $(3,-1)$.

Then $(6x+15y) * w = 3w$, and those numbers expressible as a linear combination of 6 and 15 are exactly multiples of 3.

Now we solve $3w + 20z = 1$. A solution is $(7,-1)$

In other words,

$$7 \cdot (6x + 15y) + 20 \cdot (-1) = 1$$

has solution $(x,y,z) = (7\cdot 3, 7\cdot(-1), -1)$
$= (21, -7, -1)$.

$\{$ Alternately, $6\cdot(7\cdot 3) + 15(7\cdot(-1)) = 7\cdot 3 = 21$,
so we get our $x = 21$, $y = -7$ from here.

In this method, we see that those numbers expressible as

$Ax + By + Cz$ are those numbers expressible as

$\gcd(A,B)\cdot w + C\cdot z$, which are those multiples of $\gcd(\gcd(A,B), C) = \gcd(A,B,C)$.

So $Ax + By + Cz = \gcd(A,B,C)$ has sols, while

$Ax + By + Cz = D$ has no sols if $\gcd(A,B,C) \nmid D$.

This gives solution $(x,y,z) = (298, -149, 12)$ to the question in (c). ▨

$\boxed{6.5}$ We now use this in class a lot.

Take a solution to $av + bu = 1$, (that we get from the Euclidean Algorithm), and multiply through by c to get the solution $a(vc) + b(uc) = c$.

For $37x + 47y = 103$, we first solve ~~$37x + 47y = 1$.~~ $37u + 47v = 1$.

This has solution $(u, v) = (14, -11)$.

Multiplying by 103 gives solution $(1442, -1133)$.

Of course, all solutions come from

$$(1442 + 47k, -1133 - 37k).$$

Taking $k = -30$ gives the "smaller" solution

$$(32, -23).$$

Taking $k = -31$ gives $(-15, 14)$.

$\left\{ \text{Notice} \quad \frac{1442}{47} = 30.68 \approx 30 \text{ or } 31 \right\}$. ∎

7.1 We replicate the proof for $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

So as $\gcd(a,b)=1$, there are solutions to

$$ax+by=1.$$

Multiplying by c gives $acx+bcy=c$.

As $a \mid a$, and $a \mid bc$, we know $a \mid (acx+bcy)=c$. ∎

7.3 Notice that if p divides any 2 of st, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$, then in fact p divides all three of them, as the third is a linear combination of the other 2.

So it suffices to prove that any 2 are relatively prime.

Say $p \mid st$ and $p \mid \frac{s^2-t^2}{2}$.

If $p \mid \frac{s^2-t^2}{2}$, then $p \mid s^2-t^2$ too.

As $p \mid st$, we have $p \mid s$ or $p \mid t$. Let's say $p \mid s$. $*$

Then $p \mid s^2$ too.

As $p \mid s^2$, $p \mid s^2-t^2$, we have $p \mid (s^2-t^2)-(s^2) = -t^2$, & so $p \mid t^2$. But then $p \mid t$ as well.

We've shown $p \mid s$ and $p \mid t$. But $\gcd(s,t)=1$ by our starting point, so $p=1$. [It's almost identical for when $p \mid t$ at $*$]. ∎

7.5

(a) $\mathbb{E}$-primes are exactly those even numbers n for which $\frac{n}{2}$ is odd. It's clear that $\frac{n}{2}$ must be odd, as otherwise

$$2 \cdot \frac{n}{2} \text{ is an } \mathbb{E}\text{-factorization.}$$

On the other hand, if $\frac{n}{2}$ is odd, then exactly 1 2 appears in the prime factorization of n. So it cannot possibly split into 2 even numbers. //

(b) It's actually the exact same as the proof for integers. //

(c) The smallest is $36 = 2 \cdot 18 = 6 \cdot 6$.

More generally, if p, q are distinct odd primes, $4pq$ will have the two factorizations $2p \cdot 2q = 2 \cdot 2pq$.

A number of the form $4p^2q$ will have the three factorizations

$$4p^2q = 2 \cdot 2p^2q = 2p^2 \cdot 2q = 2pq \cdot 2p.$$

The smallest such number is $4 \cdot 3^2 \cdot 5 = 180$.

There are many different ways to get four factorizations. One that works is $4pqr$, which has factors

$$2 \cdot 2pqr, \quad 2p \cdot 2qr, \quad 2pq \cdot 2r, \quad 2q \cdot 2pr.$$

The smallest of this form is $4 \cdot 3 \cdot 5 \cdot 7 = 420$.

One might try $4p^3r$, with factors $2p^3 \cdot 2r$, $2p^2 \cdot 2pr$, $2p \cdot 2p^2r$, $2 \cdot 2p^3r$.

The smallest is $4 \cdot 3^3 \cdot 5 = 540$.

Another attempt is $2^3 p^2 \cdot q$, with factors $2p \cdot 2p \cdot 2q$, $2 \cdot 2pq \cdot 2p$, $2 \cdot 2p^2 \cdot 2p$, and $2 \cdot 2 \cdot 2p^2q$.

The smallest is 360, and this is the actual smallest with 4. ∎