6.1 Through the Euclidean Algorithm (or otherwise),

(a) \( 12345 \cdot 11 = 67890 \cdot 3 = 15 = \gcd(12345, 67890) \)

[any solution will do]

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

6.2 (a) With the Euclidean Algorithm, we find an solution.

The rest come from adding/subtracting suitable multiple.

The answers are

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

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

Note that there are more answers than just

\[ + 67890k \quad \text{and} \quad -12345k. \]

We get the correct multiple by dividing by the \( \gcd \), e.g., \( \frac{12345}{15} = 823 \).

(c) \( (-1645 + 392k) \cdot 54321 + (9048 - 18107k) \cdot 9876 = 3 \).

Side Note: the work from 6.1 feeds into the work for 6.2.
The method looks like this:

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

Then \((6x + 15y)z = 3w\), and these 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 \((x, y, z) = (7, 3, 7(-1), -1) = (21, -7, -1)\).

Alternatively, \( 6 \cdot (7.3) + 15(7(-1)) = 7.3 = 2z \),

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 \( \gcd(A, B) \cdot 2 + C \cdot 2 \), 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 \( Ax + By + Cz = 0 \) has no sols of \( \gcd(A, B, C) \neq 0 \).

This gives solution \((x, y, z) = (298, -149, 12)\) to the question in \( CC \).
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 $a(vc) + b(vc) = c$.

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

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

$$(22, -23).$$

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

\[ \left\{ \text{Notice} \quad \frac{1442}{47} = 30.88 \approx 30 \text{ or } 31 \right\}. \]
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

\[
a x + b y = 1.
\]

Multiplying by \( c \) gives \( a c x + b c y = c \).

As \( a \mid a \), and \( a \mid b \), we know \( a \mid (ac x + b c y) = c \). \( \square \)

Notice that if \( p \) divides any 2 of \( st, \frac{s^2 + t^2}{2}, \frac{c^3 + t^2}{2} \),

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 \( p \mid s^2 \), \( p \mid s^3 \), we have \( p \mid (s^3 + t^3) - (s^3) = t^3 \),

so \( p \mid t^3 \). 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 \( \times 3 \).] \( \square \)
(a) 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 $\frac{n}{2}$ is an E-factorization.

On the other hand, if $\frac{n}{2}$ is odd, then exactly $1$ 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 $\text{ap, } 2q = \text{a, } 2pq$.

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 $\text{a, } 4p, \text{qr, } 2p, \text{a}, \text{qr, } \text{a, } 2p, \text{qr}$.

The smallest of this form is $4 \cdot 3^2 \cdot 5 = 180$.

One might try $4p^3r$, with factors $2p^3 \cdot 2r, 2p^2 \cdot 2r, 2p \cdot 2r, 2r, 2p$. The smallest is $4 \cdot 3^3 \cdot 5 = 540$.

Another attempt is $2^3 \cdot p^2 \cdot q$, with factors $2p^2 \cdot 2q, 2 \cdot 2p, 2q, 2p, 4r, 2p, 2r, a, 2r, a, 2p, 2r, a, 2r, a, 2p, 2r$.

The smallest is $2520$, and this is the actual smallest with $4$. \[\square\]