Discussion Notes: Homework 3

Modular Inverses and Linear Congruences

We know that if $\gcd(a, m) = 1$ for $m > 1$, then there exists an inverse of a mod m. (This is theorem 3 in your book on page 234.)

Let $a = 19$ and $m = 141$. Does 19 mod 141 have an inverse?

Step 1: Find the gcd(141, 19).

We do this using the **Euclidean Algorithm** introduced on pages 227-228 of your book. This takes advantage of the fact that if $a = bq + r$ for $a, b, q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, r)$.

Using this algorithm we get:

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 & \gcd(141, 19) &= \gcd(19, 8) \\ 19 &= 2 \cdot 8 + 3 & &= \gcd(8, 3) \\ 8 &= 2 \cdot 3 + 2 & &= \gcd(3, 2) \\ 3 &= 1 \cdot 2 + 1 & &= \gcd(2, 1) \\ 2 &= 2 \cdot 1 + 0 & &= 1 \end{aligned}$$

Therefore, 141 and 19 are relatively prime and 19 mod 141 has an inverse.

Step 2: Finding the inverse.

So how do we find this inverse? The final goal is to get something in the form $1 = sa + tm$, since then we can conclude that s is our modular inverse. (See the proof at the bottom of page 234 in your book for this result.)

We can actually use the work we have already done in the Euclidean Algorithm to get this. Notice there pattern of repeating remainders in the Euclidean Algorithm:

$$\begin{aligned} a &= b * q_1 + r_1 \\ b &= r_1 * q_2 + r_2 \\ r_1 &= r_2 * q_3 + r_3 \\ r_2 &= r_3 * q_4 + r_4 \\ &\dots \\ r_i &= r_{i+1} * q_{i+2} + r_{i+2} \end{aligned}$$

So our repeating remainders are:

$$\begin{aligned} 141 &= 7 \cdot \boxed{19} + 8 & 141 &= 7 \cdot 19 + \boxed{8} & 141 &= 7 \cdot 19 + 8 & 141 &= 7 \cdot 19 + 8 \\ \boxed{19} &= 2 \cdot 8 + 3 & 19 &= 2 \cdot \boxed{8} + 3 & 19 &= 2 \cdot 8 + \boxed{3} & 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 & \boxed{8} &= 2 \cdot 3 + 2 & 8 &= 2 \cdot \boxed{3} + 2 & 8 &= 2 \cdot 3 + \boxed{2} \\ 3 &= 1 \cdot 2 + 1 & 3 &= 1 \cdot 2 + 1 & \boxed{3} &= 1 \cdot 2 + 1 & 3 &= 1 \cdot \boxed{2} + 1 \end{aligned}$$

I'm going to replace these remainders with variables to make things easier later. First, we have $a = 19$ and $m = 141$. Let's put those variables back in:

$$\begin{aligned} m &= 7 \cdot a + 8 \\ a &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Now lets assign the repeating 8s with r_1:

$$\begin{aligned} m &= 7 \cdot a + \boxed{r_1} \\ a &= 2 \cdot \boxed{r_1} + 3 \\ \boxed{r_1} &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Next assign the repeating 3s with r_2:

$$\begin{aligned} m &= 7 \cdot a + r_1 \\ a &= 2 \cdot r_1 + \boxed{r_2} \\ r_1 &= 2 \cdot \boxed{r_2} + 2 \\ \boxed{r_2} &= 1 \cdot 2 + 1 \end{aligned}$$

And finally the repeating 2s with r_3:

$$\begin{aligned} m &= 7 \cdot a + r_1 \\ a &= 2 \cdot r_1 + r_2 \\ r_1 &= 2 \cdot r_2 + \boxed{r_3} \\ r_2 &= 1 \cdot \boxed{r_3} + 1 \end{aligned}$$

Weird right? But we need to do a strange back-substitution to find the inverse, and this will make the math easier. You do have to be careful. Notice that there are some 2s that I did not replace:

$$\begin{aligned} m &= 7 \cdot a + r_1 \\ a &= \boxed{2} \cdot r_1 + r_2 \\ r_1 &= \boxed{2} \cdot r_2 + r_3 \\ r_2 &= 1 \cdot r_3 + 1 \end{aligned}$$

These boxed 2s are not part of the repeating remainders, and do not get replaced with variables.

Now, we are going to rewrite these equations again. (Yeah, this is a tedious algorithm. At least you don't have to code it!) Why? Remember, we want an equation that looks like $1 = sa + tm$. Notice that the last equation can be rewritten $1 = r_2 - 1 \cdot r_3$. We might be able to do something with that! So lets start rewriting:

$$\begin{aligned} m &= 7 \cdot a + r_1 && \text{becomes} && r_1 &= m - 7a \\ a &= 2 \cdot r_1 + r_2 && \text{becomes} && r_2 &= a - 2r_1 \\ r_1 &= 2 \cdot r_2 + r_3 && \text{becomes} && r_3 &= r_1 - 2r_2 \\ r_2 &= 1 \cdot r_3 + 1 && \text{becomes} && 1 &= r_2 - r_3 \end{aligned}$$

Now, we start the backwards substitution and something magical occurs!

$$\begin{aligned}
1 &= r_2 - r_3 \\
&= r_2 - (r_1 - 2r_2) && \text{substitute in } r_3 \\
&= 3r_2 - r_1 && \text{simplify} \\
&= 3(a - 2r_1) - r_1 && \text{substitute in } r_2 \\
&= 3a - 6r_1 - r_1 && \text{simplify} \\
&= 3a - 7r_1 && \text{simplify} \\
&= 3a - 7(m - 7a) && \text{substitute in } r_1 \\
&= 3a - 7m + 49a && \text{simplify} \\
&= 52a - 7m
\end{aligned}$$

Somehow, we end up with an equation in the form $1 = sa + tm = 52a - 7m$ where $s = 52$. Therefore, the modular inverse of 19 mod 141 is 52.

If we did this the more traditional way, without creating variables, we end up with:

$$\begin{aligned}
141 &= 7 \cdot 19 + 8 && \text{becomes} && 8 = 141 - 7 \cdot 19 \\
19 &= 2 \cdot 8 + 3 && \text{becomes} && 3 = 19 - 2 \cdot 8 \\
8 &= 2 \cdot 3 + 2 && \text{becomes} && 2 = 8 - 2 \cdot 3 \\
3 &= 1 \cdot 2 + 1 && \text{becomes} && 1 = 3 - 2
\end{aligned}$$

Do not over simplify! Keep in tack any of the "repeating numbers." The backwards subtitution looks like:

$$\begin{aligned}
1 &= 3 - (2) \\
&= 3 - (8 - 2 \cdot (3)) && \text{substitute in (2)} \\
&= 3 - 8 + 2 \cdot (3) && \text{simplify} \\
&= 3 \cdot (3) - 8 && \text{combine "(3)" terms} \\
&= 3 \cdot (19 - 2 \cdot (8)) - 8 && \text{substitute in (3)} \\
&= 3 \cdot 19 - 6 \cdot (8) - 8 && \text{simplify} \\
&= 3 \cdot 19 - 7 \cdot (8) && \text{combine "(8)" terms} \\
&= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot (19)) && \text{substitute in (8)} \\
&= 3 \cdot 19 - 7 \cdot 141 + 49 \cdot (19) && \text{simplify} \\
&= 52 \cdot (19) - 7 \cdot 141 && \text{combine "(19)" terms}
\end{aligned}$$

Again we end up with something in the form $1 = sa + tm = 52(19) - 7(141)$ making our inverse 52. However, it is really hard to keep track what you need to simplify, and what you need to substitute. If you can figure out how to use the variable method I recommend that!

There are a couple of resources on the web if you don't quite understand how to go through this agorithm. Just do a google search on "modular inverse"