Notes about mod

First we'll define divisibility. We say that a | b if and only if there is some integer c such that b = ac. In English, "a | b" would be read as "b is divisible by a."

For example, 6 | 18, 197 | 0 and 34 | 34.

Now, let's define mod:

$a \equiv b \pmod{n}$ if and only if n | (a – b). (This just means there exists some integer c such that a – b = nc.)

In essence, this is true if n divides evenly into the difference of a and b. Alternatively, we can think of it as follows: when a and b are divided by n, they leave the same remainder.

In our class, typically we will make some mathematical calculation and then we'd like to know what letter a particular number corresponds to. What we really want is give some integer a, we want to find a value b such that $0 \le b < 26$ and $a \equiv b \pmod{26}$.

For example, if we get 194 after some calculation and want to know what letter it is, our goal is to find the unique value of b such that

$$194 \equiv b \pmod{26}, \text{ with } 0 \le b < 26$$

We can determine that $194 \equiv 12 \pmod{26}$. We can verify this because 194 – 12 = 182 and 182 = 26x7. The easy way to find b when the starting value is greater than 26 is to divide 26 into the number. When we divide 26 into 194, it goes in 7 times, leaving a remainder of 12, which is our desired value.

Consider a second example:

$$-85 \equiv b \pmod{26}, \text{ with } 0 \le b < 26$$

By dividing, we find that $-85 \equiv -7 \pmod{26}$, since -85 – (-7) = -78 and -78 = 26x(-3), but we also see that we haven't gotten the desired value of b either. We can simply add 26 to -7 to do that, since adding or subtracting multiples of 26 will "create" other values equivalent to the original. Thus, we have:

$$-85 \equiv -7 \equiv 26 - 7 \equiv 19 \pmod{26}$$

Now, let's look at some rules with mod:

if $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$
if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ and $ac \equiv bc \pmod{cn}$,
but this latter fact is rarely used
if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$
if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$, and
$ac \equiv bd \pmod{n}$

These are fairly straight-forward to apply. However, division rules are tricky since we are now dealing with integers. If we have a situation such as

$$3a \equiv 16 \pmod{26}$$

we deal with it by multiplying through by the inverse of 3 (mod 26) which is 9, to yield the following equation:

$$9(3a) \equiv 9(16) \pmod{26}$$
$$27a \equiv 144 \pmod{26}$$
$$a \equiv 14 \pmod{26}$$

Here is a list of the inverses mod 26:

1
3, 9
5, 21
7, 15
11, 19
17, 23
25

(Note: 1 is an inverse of itself as is 25. The rest are pairs, so 3 is the inverse of 9 and 9 is the inverse of 3 (mod 26), etc.)

But what about an equation like

$4a \equiv 14 \pmod{26}$ or $4a \equiv 7 \pmod{26}$

This literally means:

$4a - 14 = 26c$, for some int c.
$2a - 7 = 13c$, so
$2a \equiv 7 \pmod{13}$ is all we can ascertain, the following above implies that $a \equiv 10 \pmod{13}$, which can be determined by multiplying through by 7.

$4a - 7 = 26c$, for some int c
$7 = 4a - 26c$
$7 = 2(2a - 13c)$, which is impossible since 7 is NOT divisible by 2.

If we find that a ≡ 10 (mod 13), that means that a ≡ 10 (mod 26) or a ≡ 23 (mod 26).

We can see this because if a – 10 = 13c for some integer c, then setting c = 0, 1 shows that a could be 10 or 23. Setting c = 2 shows that a could be 36, but 36 is equivalent to 10 mod 26.

This information is relevant in the following situations:

1) Solving for the inverse of a matrix
2) Solving for a key in a known plaintext attack on the Hill cipher

For the former, if it is known that the matrix does have an inverse, then there will be a unique solution that satisfies all of the given equations. To take an example from the notes (chapter 4), when solving the equation $\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 26$, we found that c ≡ 8 (mod 26). We could have used that and substituted into the equation

6a + 5c ≡ 0 (mod 26), yielding
6a + 5(8) ≡ 0 (mod 26)
6a ≡ -40 (mod 26)
6a ≡ 12 (mod 26)
3a ≡ 6 (mod 13)
a ≡ 2 (mod 13), which means a ≡ 2 (mod 26) or a ≡ 15 (mod 26)

Which of these two is correct can only be ascertained by plugging into the other relevant equation:

3a + c ≡ 1 (mod 26)

For #2, it may be the case that the equations formed don't provide a unique solution for the key. This was illustrated in the notes for chapter 4. Here we can narrow the key down to a few options and from there we can simply try out all of the candidates.