Encryption via Multiplication

Reading

- Section 8.5

Notes

Instead of adding a number to encode, we could instead multiply by a number. In order to do that, we need to make sure that we can properly decrypt, which would amount to multiplying by the inverse. So we need to have an inverse to begin with, so we should only multiply by invertible elements.

Let's give that a go. We are working modulo 26 to have enough space for all the letters, so we need a number that's relatively prime to 26. Since $26 = 2 \times 13$, numbers like 3, 5 and 7 would do. Let's use 3.

We will use the word NUMBER again as our plaintext. In terms of numbers this becomes "14 21 13 2 5 18". We multiply these by 3 then reduce modulo 26: "42 63 39 6 15 54" or "16 11 13 6 15 2". In terms of letters this would be: PKMFOB. So that is our cyphertext that we would transmit.

In order to decrypt this at the other end, we would need to figure out what the multiplicative inverse of 3 is. Since $3 \cdot 9 = 27 \equiv 1 (\mathrm{mod} 26)$, we see that 9 is the multiplicative inverse. So to decrypt the message, we need to take the numbers "16 11 13 6 15 2", multiply them with 9 and reduce modulo 26: "144 99 117 54 135 18" or "14 21 13 2 5 18", which is what we started with.

To practice this some more, decrypt the message ILYEV which was encrypted by multiplying by 5.