Section 05: Number Theory

1. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Find the multiplicative inverse of 6 $\pmod 7$.

(d) Does 49 have an multiplicative inverse $\pmod 7$?

2. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2 (\text{mod } 33)$ for all of its integer solutions z.

3. Euclid's Lemma[1]

(a) Show that if an integer p divides the product of two integers a and b, and $\gcd(p, a) = 1$, then p divides b.

(b) Show that if a prime p divides ab where a and b are integers, then $p \mid a$ or $p \mid b$. (Hint: Use part (a))

[1] these proofs aren't much longer than proofs you've seen so far, but it can be a little easier to get stuck – use these as a chance to practice how to get unstuck if you do!