Section 05: Number Theory

1. GCD
   (a) Calculate gcd(100, 50).

   (b) Calculate gcd(17, 31).

   (c) Find the multiplicative inverse of 6 \text{(mod 7)}.

   (d) Does 49 have a multiplicative inverse \text{(mod 7)}?

2. Extended Euclidean Algorithm
   (a) Find the multiplicative inverse $y$ of $7 \text{mod 33}$. That is, find $y$ such that $7y \equiv 1 \text{ (mod 33)}$. 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 $\text{gcd}(p, a) = 1$, 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))

4. Have we derived yet?

Each of the following proofs has some mistake in its reasoning - identify that mistake.

   (a) Proof. If it is sunny, then it is not raining. It is not sunny. Therefore it is raining. \(\square\)

   (b) Prove that if $x + y$ is odd, either $x$ or $y$ is odd but not both.

---

\(^1\)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!
Proof. Suppose without loss of generality that $x$ is odd and $y$ is even. Then, $\exists k \ x = 2k + 1$ and $\exists m \ y = 2m$. Adding these together, we can see that $x + y = 2k + 1 + 2m = 2k + 2m + 1 = 2(k + m) + 1$. Since $k$ and $m$ are integers, we know that $k + m$ is also an integer. So, we can say that $x + y$ is odd. Hence, we have shown what is required.

(c) Prove that $2 = 1$. :)

Proof. Let $a, b$ be two equal, non-zero integers. Then,

\[
\begin{align*}
    a &= b \\
    a^2 &= ab & \text{[Multiply both sides by a]} \\
    a^2 - b^2 &= ab - b^2 & \text{[Subtract $b^2$ from both sides]} \\
    (a - b)(a + b) &= b(a - b) & \text{[Factor both sides]} \\
    a + b &= b & \text{[Divide both sides by $a - b$]} \\
    b + b &= b & \text{[Since $a = b$]} \\
    2b &= b & \text{[Simplify]} \\
    2 &= 1 & \text{[Divide both sides by $b$]}
\end{align*}
\]

(d) Prove that $\sqrt{3} + \sqrt{7} < \sqrt{20}$

Proof.

\[
\begin{align*}
    \sqrt{3} + \sqrt{7} &< \sqrt{20} \\
    (\sqrt{3} + \sqrt{7})^2 &< 20 \\
    3 + 2\sqrt{21} + 7 &< 20 \\
    19.165 &< 20
\end{align*}
\]

It is true that $19.165 < 20$, hence, we have shown that $\sqrt{3} + \sqrt{7} < \sqrt{20}$