CS1231(S) Tutorial 7: Number Theory II

National University of Singapore

2019/20 Semester 1

1. Compute $\gcd(a, b)$ for the following pairs of a and b, and express $\gcd(a, b)$ in the form $ax + by$ where $x, y \in \mathbb{Z}$.
   (a) $a = 17$, $b = 5$;
   (b) $a = 275$, $b = 407$.

2. Prove the following statement:
$$\forall a, b, c \in \mathbb{Z}\ \Big(\big((a \mid c) \wedge (b \mid c) \wedge (\gcd(a, b) = 1)\big) \rightarrow (ab \mid c)\Big)$$

3. Let $a, b \in \mathbb{Z}$. Prove that if $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$, then ($\gcd(x, y)$ exists and) $\gcd(x, y) = 1$.

4. Let $a, b \in \mathbb{Z}$, not both zero. Show that for all $n \in \mathbb{Z}$, n is an integer linear combination of a and b (i.e. there exist $x, y \in \mathbb{Z}$ such that $ax + by = n$) if and only if $\gcd(a, b) \mid n$. (Hint: use Bézout's Identity for the 'if' direction).

5. Find integers x, y and z such that $12x - 15y + 50z = 1$.
   (Hint: What is $\gcd(\gcd(12, 15), 50)$? Use Bézout's Identity.)

6. Let $a, b \in \mathbb{Z}$, not both zero. Show that
$$\gcd\left(\tfrac{a}{\gcd(a,b)}, \tfrac{b}{\gcd(a,b)}\right) = 1.$$

7. Determine the prime factorisation of each of the following integers:
   (a) 14351;
   (b) 14369.

8. For each of the following pairs of a and n, find a multiplicative inverse (if any) of a modulo n.
   (a) $a = 3$, $n = 8$;
   (b) $a = 6$, $n = 14$;
   (c) $a = 31$, $n = 24$.

9. Find all integers x (if any) that satisfy each of the following congruence equations:
   (a) $5x \equiv 2 \pmod{32}$;
   (b) $4x \equiv 6 \pmod{48}$.

   [Hint: For part (b), you may find Qn 4 helpful.]

10. Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$ with $\gcd(m, n) = 1$. Consider the following simultaneous congruence equations:

$$x \equiv a \pmod{m};$$
$$x \equiv b \pmod{n}.$$

(a) Let $my + nz = 1$, where $y, z \in \mathbb{Z}$ (which exist since $\gcd(m, n) = 1$), and let $x_0 = anz + bmy$. Verify that $x = x_0$ is a solution of the above simultaneous congruence equations.

(b) Prove further that x is a solution of the above simultaneous congruence equations if and only if $x \equiv x_0 \pmod{mn}$. [Hint: Qn 2 may be useful.]