CS1231(S) Tutorial 7: Number Theory 2

National University of Singapore

2020/21 Semester 1

Background

Definition 8.5.1. Let $m, n \in \mathbb{Z}$. An *integer linear combination* of m and n is a number of the form $ms + nt$, where $s, t \in \mathbb{Z}$.

Theorem 8.5.2 (Bézout's Lemma). Let $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $\gcd(m, n)$ is an integer linear combination of m and n.

Questions for discussion on the LumiNUS Forum

Answers to these questions will not be provided.

D1. Prove or disprove the following sentence:

> There is a prime number p such that $p + 2$ and $p + 4$ are also prime.

D2. Show that 15 is a multiplicative inverse of 7 modulo 26.

D3. Use the Euclidean Algorithm to find

- (a) $\gcd(1, 5)$,
- (b) $\gcd(100, 101)$,
- (c) $\gcd(123, 277)$,
- (d) $\gcd(1529, 14039)$,
- (e) $\gcd(1529, 14038)$, and
- (f) $\gcd(11111, 111111)$.

D4. Prove or disprove the following sentence:

> If d is an integer linear combination of two integers a and b, then $d = \gcd(a, b)$.

Tutorial questions

1. Compute $\gcd(a, b)$ for the following pairs of a and b, and express $\gcd(a, b)$ in the form of $ax + by$ where $x, y \in \mathbb{Z}$:
   - (a) $a = 17$ and $b = 5$;
   - (b) $a = 275$ and $b = 407$.
2. Let $a, b, c \in \mathbb{Z}$. Suppose a and b divide c, and $\gcd(a, b) = 1$. Prove that ab divides c.
3. Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = 1$. Show that $\gcd(a, b) = 1$.
4. Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$. Prove that $\gcd(s, t) = 1$.

   (Hint: you may find Question 3 helpful.)

5. Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Prove that

$$\gcd\Big(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\Big) = 1.$$

(Hint: you may find Question 3 helpful.)

6. Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Prove that an integer n is an integer linear combination of a and b if and only if $\gcd(a, b) \mid n$.

   (Hint: Bézout's Lemma may be helpful for the "if" direction.)

7. Find $x, y, z \in \mathbb{Z}$ such that $12x - 15y + 50z = 1$.

   (Hint: What is $\gcd(\gcd(12, 15), 50)$? Bézout's Lemma may be helpful here.)

8. Determine the prime factorization of each of the following integers:

   (a) 14351;

   (b) 14369.

9. For each of the following pairs of a and n, determine whether a has a multiplicative inverse modulo n, and find one if it has any:

   (a) $a = 3$ and $n = 8$;

   (b) $a = 6$ and $n = 14$;

   (c) $a = 31$ and $n = 24$.

10. For each of the congruence equations below, find all integers x, if any, that satisfy it:

    (a) $5x \equiv 2 \pmod{32}$;

    (b) $4x \equiv 6 \pmod{48}$.

    (Hint: you may find Question 6 helpful for (b).)

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

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

    Apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $ms + nt = 1$. Let $c_0 = ant + bms$.

    (a) Verify that $x = c_0$ is a solution to the system of simultaneous congruence equations above.

    (b) Let $c \in \mathbb{Z}$. Prove that $x = c$ is a solution to the system of simultaneous congruence equations above if and only if $c \equiv c_0 \pmod{mn}$.
    (Hint: you may find Question 2 useful.)