CS1231(S) Tutorial 7: Number Theory 2
Solutions

National University of Singapore

2020/21 Semester 1

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 $b = 407$.

   Solution.

   (a)
$$
\begin{aligned}
17 \,\underline{\mathrm{mod}}\, 5 &= 2 & \dashleftarrow \quad 2 &= 17 - 5 \times 3 & (1)\\
5 \,\underline{\mathrm{mod}}\, 2 &= 1 & \dashleftarrow \quad 1 &= 5 - 2 \times 2 & (2)\\
2 \,\underline{\mathrm{mod}}\, 1 &= 0
\end{aligned}
$$

   Hence
$$
\begin{aligned}
\gcd(17, 5) = 1 &= 5 - 2 \times 2 && \text{by (2);}\\
&= 5 - (17 - 5 \times 3) \times 2 && \text{by (1);}\\
&= 17 \times (-2) + 5 \times 7.
\end{aligned}
$$

   (b)
$$
\begin{aligned}
407 \,\underline{\mathrm{mod}}\, 275 &= 132 & \dashleftarrow \quad 132 &= 407 - 275 \times 1 & (3)\\
275 \,\underline{\mathrm{mod}}\, 132 &= 11 & \dashleftarrow \quad 11 &= 275 - 132 \times 2 & (4)\\
132 \,\underline{\mathrm{mod}}\, 11 &= 0
\end{aligned}
$$

   Hence
$$
\begin{aligned}
\gcd(407, 275) = 11 &= 275 - 132 \times 2 && \text{by (4);}\\
&= 275 - (407 - 275 \times 1) \times 2 && \text{by (3);}\\
&= 407 \times (-2) + 275 \times 3.
\end{aligned}
$$

2. Let $a, b, c \in \mathbb{Z}$. Suppose a and b divide c, and $\gcd(a, b) = 1$. Prove that ab divides c.

   Solution.

   1. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $c = ka$ and $c = \ell b$.
   2. Apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b) = 1$.
   3. Then $c = c(as + bt)$ as $as + bt = 1$;
   4. $= cas + cbt$
   5. $= (\ell b)as + (ka)bt$ by line 1;
   6. $= ab(\ell s + kt)$, where $\ell s + kt \in \mathbb{Z}$.
   7. So $ab \mid c$ by the definition of divisibility. □

   This can also be proved by considering the prime factorizations of a, b, and c.

3. Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = 1$. Show that $\gcd(a, b) = 1$.

   Solution.

   1. If $a = 0 = b$, then $1 = as + bt = 0s + 0t = 0$, which is a contradiction.
   2. So $a \neq 0$ or $b \neq 0$.
   3. This implies $\gcd(a, b)$ exists and $\gcd(a, b) \geqslant 1$.
   4. Let $d = \gcd(a, b)$.

5. Then $d \mid a$ and $d \mid b$ by the definition of gcd.
6. $\therefore \quad d \mid as+bt$ by the Closure Lemma.
7. $\therefore \quad d \mid 1$ as $as+bt=1$ by assumption.
8. $\therefore \quad d \leqslant |d| \leqslant |1| = 1$ by Theorem 7.4.
9. So $\gcd(a,b) = d = 1$ by line 3. □

4. Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$. Prove that $\gcd(s, t) = 1$.

   Solution.

   1. The definition of $\gcd(a, b)$ tells us $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$.
   2. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $a = k \gcd(a, b)$ and $b = \ell \gcd(a, b)$.
   3. Then $k \gcd(a,b) \cdot s + \ell \gcd(a,b) \cdot t = \gcd(a,b)$ as $as + bt = \gcd(a, b)$ by assumption.
   4. $\therefore \quad ks + \ell t = 1$ as $\gcd(a, b)$ is positive if it exists.
   5. $\therefore \quad \gcd(s, t) = 1$ by Question 3. □

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

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

   Solution.

   1. On the one hand, apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.
   2. On the other hand, we know $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ by the definition of gcd.
   3. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $a = k \gcd(a, b)$ and $b = \ell \gcd(a, b)$.
   4. Combining the two, we have $\gcd(a, b) = as + bt = k \gcd(a, b) \cdot s + \ell \gcd(a, b) \cdot t$.
   5. So $1 = ks + \ell t$.
   6. This implies, by Question 3 and the choice of k and ℓ,

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

   This can also be proved by considering the prime factorizations of a and b.

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 $\gcd(a, b) \mid n$.

   Solution.

   1. Let $n \in \mathbb{Z}$.
   2. ("Only if")
      - 2.1. Let $s, t \in \mathbb{Z}$ such that $n = as + bt$.
      - 2.2. By the definition of gcd, we know $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$.
      - 2.3. So $\gcd(a, b) \mid as + bt$ by the Closure Lemma.
      - 2.4. This means $\gcd(a, b) \mid n$.
   3. ("If")
      - 3.1. Suppose $\gcd(a, b) \mid n$.
      - 3.2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = k \gcd(a, b)$.
      - 3.3. Apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.
      - 3.4. Then $n = k \gcd(a, b)$ by line 3.2;
      - 3.5. $\quad = k(as + bt)$ by line 3.3;
      - 3.6. $\quad = a(ks) + b(kt)$ where $ks, kt \in \mathbb{Z}$.
      - 3.7. So n is an integer linear combination of a and b. □

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

   Solution. Observe that $\gcd(12, 15) = 3$ and $\gcd(\gcd(12, 15), 50) = \gcd(3, 50) = 1$. Thus Bézout's Lemma tells us that 3 is an integer linear combination of 12 and 15, and that 1 is an integer linear combination of 3 and 50. By observation, we have

   $$3 = 15 - 12 = 15 \times 1 + 12 \times (-1), \tag{5}$$
   $$1 = 51 - 50 = 50 \times (-1) + 3 \times 17. \tag{6}$$

   (One can also use the Euclidean Algorithm here.) So

   $$\begin{aligned} 1 &= 50 \times (-1) + 3 \times 17 && \text{by (6);} \\ &= 50 \times (-1) + \big(15 \times 1 + 12 \times (-1)\big) \times 17 && \text{by (5);} \\ &= 12 \times (-17) - 15 \times (-17) + 50 \times (-1). \end{aligned}$$

   Thus, we can let x, y, z be $-17, -17, -1$ respectively. (Note: there are other solutions.)

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

   (a) 14351;
   (b) 14369.

   Solution.

   (a) $14351 = 113 \times 127$.
   (b) $14369 = 14369$, i.e., 14369 is prime.

   This exercise is to illustrate the difficulty of factorizing large numbers.

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 $n = 24$.

   Solution.

   (a) Note that $\gcd(3, 8) = 1$. So 3 has a multiplicative inverse modulo 8 by Theorem 8.7. One readily observes that

   $$1 = 9 - 8 = 3 \times 3 - 8 \equiv 3 \times 3 \pmod{8}.$$

   Thus 3 is a multiplicative inverse of 3 modulo 8.

   (b) Note that $\gcd(6, 14) = 2 \neq 1$. So 6 does not have a multiplicative inverse modulo 14 by Theorem 8.7.

   (c) Note that $\gcd(31, 24) = 1$. So 31 has a multiplicative inverse modulo 24 by Theorem 8.7. By the Euclidean Algorithm,

   $$\begin{aligned} 31 \mathbin{\underline{\text{mod}}} 24 &= 7 & \dashleftarrow\quad 7 &= 31 - 24 \times 1 && (7) \\ 24 \mathbin{\underline{\text{mod}}} 7 &= 3 & \dashleftarrow\quad 3 &= 24 - 7 \times 3 && (8) \\ 7 \mathbin{\underline{\text{mod}}} 3 &= 1 & \dashleftarrow\quad 1 &= 7 - 3 \times 2 && (9) \\ 3 \mathbin{\underline{\text{mod}}} 1 &= 0 \end{aligned}$$

   Hence
   $$\begin{aligned} \gcd(31, 24) = 1 &= 7 - 3 \times 2 && \text{by (9);} \\ &= 7 - (24 - 7 \times 3) \times 2 && \text{by (8);} \\ &= 24 \times (-2) + 7 \times 7 \\ &= 24 \times (-2) + (31 - 24 \times 1) \times 7 && \text{by (7);} \\ &= 31 \times 7 + 24 \times (-9) \\ &\equiv 31 \times 7 \pmod{24}. \end{aligned}$$

   Thus 7 is a multiplicative inverse of 31 modulo 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) $4x \equiv 6 \pmod{48}$.

    Solution.

    (a) Note that $\gcd(32, 5) = 1$. So 5 has a multiplicative inverse modulo 32 by Theorem 8.7. One readily observes that

    $$1 = 65 - 64 = 5 \times 13 + 32 \times (-2) \equiv 5 \times 13 \pmod{32}.$$

    So 13 is a multiplicative inverse of 5 modulo 32. Therefore, for all $x \in \mathbb{Z}$,

    $$5x \equiv 2 \pmod{32} \quad \Leftrightarrow \quad x \equiv 13 \times 2 = 26 \pmod{32}$$

    by Theorem 8.8.

    (b) We prove that no $x \in \mathbb{Z}$ makes $4x \equiv 6 \pmod{48}$ by contradiction.

    1. Let $x \in \mathbb{Z}$ such that $4x \equiv 6 \pmod{48}$.
    2. Use the alternative definitions of congruence to find $k \in \mathbb{Z}$ such that $4x = 48k + 6$.
    3. Note then 6 is an integer linear combination of 4 and 48 as $6 = 4x + 48(-k)$.
    4. Thus Question 6 tells us $\gcd(4, 48) \mid 6$.
    5. However, we know $\gcd(4, 48) = 4$ and $4 \nmid 6$ by Definition 7.1, as $6/4 = 1.5 \notin \mathbb{Z}$.
    6. This is the required contradiction. □

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 $c \equiv c_0 \pmod{mn}$.

    Solution.

    (a)
    $$\begin{aligned} c_0 &= ant + bms && \text{by the definition of } c_0; \\ &= a(1 - ms) + bms && \text{by the choice of } s \text{ and } t; \\ &= a + m(-as + bs) \\ &\equiv a \pmod{m} && \text{as } -as + bs \in \mathbb{Z}. \\ c_0 &= ant + bms && \text{by the definition of } c_0; \\ &= ant + b(1 - nt) && \text{by the choice of } s \text{ and } t; \\ &= b + n(at - bt) \\ &\equiv b \pmod{n} && \text{as } at - bt \in \mathbb{Z}. \end{aligned}$$

    (b) 1. ("Only if")

    1.1. Suppose $x = c$ is a solution to the system of simultaneous congruence equations.

    1.2. This means $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$.

1.3. As congruence is symmetric and transitive, we deduce that $c \equiv c_0 \pmod{m}$ and $c \equiv c_0 \pmod{n}$ by part (a).

1.4. So $m \mid (c - c_0)$ and $n \mid (c - c_0)$ by the alternative definitions of congruence.

1.5. As $\gcd(m, n) = 1$ by assumption, this implies $mn \mid (c - c_0)$ by Question 2.

1.6. Hence the alternative definitions of congruence tell us $c \equiv c_0 \pmod{mn}$.

2. ("If")

2.1. Suppose $c \equiv c_0 \pmod{mn}$.

2.2. Use the alternative definitions of congruence to find $k \in \mathbb{Z}$ such that $c = k(mn) + c_0$.

2.3. Then $\quad c = c_0 + m(kn)$

2.4. $\qquad\quad \equiv c_0 \pmod{m}$

2.5. $\qquad\quad \equiv a \pmod{m} \quad$ by part (a).

2.6. Similarly, $\quad c = c_0 + n(km)$

2.7. $\qquad\qquad\quad \equiv c_0 \pmod{n}$

2.8. $\qquad\qquad\quad \equiv b \pmod{n} \quad$ by part (a).

2.9. So $x = c$ is a solution to the system of simultaneous congruence equations.