THE CHINESE UNIVERSITY OF HONG KONG

DEPARTMENT OF MATHEMATICS

MMAT5510 Foundation of Advanced Mathematics 2017-2018

Suggested Solution to Assignment 3

1a. If $S = \emptyset$, it is trivial. Suppose $S \neq \emptyset$, we first claim that if $a \in S$, $S\backslash\{a\}$ is also finite. The argument is as follow:

As S is finite and non-empty, there exist bijective function $f : \mathbb{N}_n \to S$ for some $n \in \mathbb{N}^+$ and there exist unique $k \in \mathbb{N}_n$ such that $f(k) = a$. Then we define a function $g : \mathbb{N}_{n-1} \to S\backslash\{a\}$

$$g(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq k-1 \\ f(i-1) & \text{if } k \leq i \leq n-1 \end{cases}$$

Then we are going to show that g is a bijective function.

- Suppose $g(i) = g(j)$. Then either $1 \leq i, j \leq k-1$ or $k \leq i, j \leq n-1$. Otherwise, say $1 \leq i \leq k-1$ and $k \leq j \leq n-1$, then we have $f(i) = g(i) = g(j) = f(j+1)$. By the injectivity of f, we have $i = j+1$ which is a contradiction.

  Now, if $1 \leq i, j \leq k-1$, we have $f(i) = g(i) = g(j) = f(j)$ and so $i = j$; otherwise $k \leq i, j \leq n-1$, we have $f(i+1) = g(i) = g(j) = f(j+1)$ which implies $i+1 = j+1$ and so $i = j$. Therefore, g is an injective function.
- Let $y \in S\backslash\{a\}$. Firstly, $y \in S$, there exists $1 \leq j \leq n$ such that $f(j) = y$. Note that $y \neq a$ and so $j \neq k$. If $1 \leq j \leq k-1$, take $i = j$, then we have $i \in \mathbb{N}_{n-1}$ and $g(i) = f(i) = f(j) = y$; if $k+1 \leq j \leq n$, take $i = j-1$, then we have $k \leq i \leq n-1$ and so $i \in \mathbb{N}_{n-1}$ and $g(i) = f(i+1) = f(j) = y$.

  Therefore, g is a surjective function.

Therefore, g is a bijective function and $S\backslash\{a\}$ is finite.

Next, we will prove the statement by induction. When $n = 0$, it is trivial. Assume the statement is true for sets of n elements. Let S have $n+1$ elements. If $T = S$, it is done. Otherwise $\exists\, a \in S\backslash T$ and $T \subseteq S\backslash\{a\}$. Since $S\backslash\{a\}$ has n elements, T is finite.

1b. The statement is proved by the contrapositve of 1a.

2. The set of all prime number is a subset of $\mathbb{N}^+$ and so it is countable. It is also nonempty. We will prove the statement by contradiction. Suppose the set of prime number is finite and has n elements. let $p_1, p_2, \ldots, p_n$ be the elements. Consider $p = p_1 p_2 \cdots p_n + 1$. p can not be divided by p_i for any $1 \leq i \leq n$. By prime factorization, p is divided by some prime factor q which is not in the set. It leads to a contradiction. Therefore the set of all prime numbers is a countably infinite set.

3. Let $f : \mathbb{N}^+ \to A$ be a function defined by

$$f(n) = 5\Big[\frac{((-1)^{n-1} - 1)n}{4} + \frac{(1 + (-1)^{n-1})(n-1)}{4}\Big]$$

(When n is odd, the first term vanishes and we have $f(1) = 0$, $f(3) = 5$, $f(5) = 10$ and etc; when n is even, the second term vanishes and we have $f(2) = -5$, $f(4) = -10$, $f(6) = -15$ and etc.) Then we are going to show that f is bijective.

- If $f(m) = f(n)$,then either both m and n are even or both of them are odd (otherwise, when we compute $f(m)$ and $f(n)$, one is nonnegative while the other one is negative, which is a contradiction.)

  Now, suppose that both m and n are even. Then,

$$\begin{aligned} f(m) &= f(n) \\ 5\Big[\frac{((-1)^{m-1}-1)m}{4} + \frac{(1+(-1)^{m-1})(m-1)}{4}\Big] &= 5\Big[\frac{((-1)^{n-1}-1)n}{4} + \frac{(1+(-1)^{n-1})(n-1)}{4}\Big] \\ \frac{5(-2m)}{4} &= \frac{5(-2n)}{4} \\ m &= n \end{aligned}$$

  Suppose that both m and n are odd. Then,

$$\begin{aligned} f(m) &= f(n) \\ 5\Big[\frac{((-1)^{m-1}-1)m}{4} + \frac{(1+(-1)^{m-1})(m-1)}{4}\Big] &= 5\Big[\frac{((-1)^{n-1}-1)n}{4} + \frac{(1+(-1)^{n-1})(n-1)}{4}\Big] \\ \frac{10(m-1)}{4} &= \frac{10(n-1)}{4} \\ m &= n \end{aligned}$$

  Therefor, f is an injective function.

- Let $q \in A$.

  Suppose that $q \geq 0$, we take $n = \frac{2q}{5} + 1 \in \mathbb{N}^+$. Then,

$$f(n) = f(\frac{2q}{5}+1) = 5\Big[\frac{((-1)^{\frac{2q}{5}}-1)(\frac{2q}{5}+1)}{4} + \frac{(1+(-1)^{\frac{2q}{5}})(\frac{2q}{5})}{4}\Big] = 5\Big[\frac{2(\frac{2q}{5})}{4}\Big] = q$$

  Suppose that $q < 0$, we take $n = -\frac{2q}{5} \in \mathbb{N}^+$. Then,

$$f(n) = f(-\frac{2q}{5}) = 5\Big[\frac{((-1)^{-\frac{2q}{5}-1}-1)(-\frac{2q}{5})}{4} + \frac{(1+(-1)^{-\frac{2q}{5}-1})(-\frac{2q}{5}-1)}{4}\Big] = \frac{5(-2)(-\frac{2q}{5})}{4} = q$$

  Therefore, f is surjective function.

Therefore, f is a bijective function and A is a countably infinite set.

4. Let d =gcd(a, b).

   ($\Rightarrow$)

   Suppose $c = as + bt$. Since $d \mid a$, then $d \mid as$. Since $d \mid b$, then $d \mid bt$. Therefore $d \mid as + bt = c$.

   ($\Leftarrow$)

   Suppose $d \mid c$. First $\exists\ s_0,\ t_0 \in \mathbb{Z}$ s.t. $d = as_0 + bt_0$. Since $d \mid c$, $c = nd$ for some $n \in \mathbb{Z}$. Then $c = n(as_0 + bt_0) = a(ns_0) + b(nt_0)$.

5a. By Extended Euclidean Algorithm, we have

$$\begin{aligned} 27 &= 3 \times 8 + 3 & \gcd(27, 8) = 1 &= 3 - 2 \\ 8 &= 2 \times 3 + 2 & &= 3 - (8 - 2 \times 3) \\ 3 &= 2 + 1 & &= 3 \times 3 = 8 \\ & & &= 3 \times (27 - 3 \times 8) - 8 \\ & & &= 3 \times 27 - 10 \times 8 \end{aligned}$$

Therefore,

$$\begin{aligned} 8x &\equiv 3 \pmod{27} \\ (-10)(8x) &\equiv (-10)3 \pmod{27} \\ x &\equiv 24 \pmod{27} \end{aligned}$$

5b. By Extended Euclidean Algorithm, we have

$$\begin{aligned} 18 &= 2 \times 7 + 4 & \gcd(18, 7) = 1 &= 4 - 3 \\ 7 &= 4 + 3 & &= 4 - (7 - 4) \\ 4 &= 3 + 1 & &= 2 \times 4 - 7 \\ & & &= 2 \times (18 - 2 \times 7) - 7 \\ & & &= 2 \times 18 - 5 \times 7 \end{aligned}$$

Therefore,

$$\begin{aligned} 7x + 32 &\equiv 6 \pmod{18} \\ 7x &\equiv -26 \pmod{18} \\ 7x &\equiv 10 \pmod{18} \\ (-5)(7x) &\equiv -50 \pmod{18} \\ x &\equiv 4 \pmod{18} \end{aligned}$$

6a. $\varphi(15) = \varphi(3 \cdot 5) = (3 - 1)(5 - 1) = 8$

6b. Since $\gcd(8, 15) = 1$, by Euler's theorem, we have $8^{\varphi(15)} \equiv 1 \pmod{15}$, so $8^8 \equiv 1 \pmod{15}$. Then

$$\begin{aligned} 8^{2017} &\equiv 8^{8 \cdot 127} \cdot 8 \pmod{15} \\ &\equiv 1^{125} \cdot 8 \pmod{15} \\ &\equiv 8 \pmod{15} \end{aligned}$$

7. Find all integer x such that $x \equiv 3 \pmod{11}$, $x \equiv 4 \pmod{13}$. By Extended Euclidean Algorithm,

$$\begin{aligned} 13 &= 11 + 2 & \gcd(13, 11) = 1 &= 11 - 5 \times 2 \\ 11 &= 5 \times 2 + 1 & &= 11 - 5 \times (13 - 11) \\ & & &= 6 \times 11 - 5 \times 13 \end{aligned}$$

By Chinese Reminder Theorem,

$$\begin{aligned} x &\equiv 3 \cdot 13 \cdot (-5) + 4 \cdot 11 \cdot 6 \pmod{143} \\ x &\equiv 69 \pmod{143} \end{aligned}$$

8. (a) i. $\varphi(17 \cdot 23) = (17-1)(23-1) = 16 \cdot 22 = 352$. Then we choose $e = 3$ and the public key is $(391, 3)$.

   ii. By Extended Euclidean Algorithm, we have $gcd(352, 3) = 1 = 352 - 117 \times 3$. Then we find the private key d by solving $ed \equiv 1 \pmod{\varphi(n)}$,

$$\begin{aligned} 3d &\equiv 1 \pmod{352} \\ (-177)(3d) &\equiv -177 \pmod{352} \\ d &\equiv 175 \pmod{352} \end{aligned}$$

   iii. The ciphertext c can be found by $c \equiv m^e \pmod{n}$. Hence

$$\begin{aligned} c &\equiv 33^3 \pmod{391} \\ c &\equiv 356 \pmod{391} \end{aligned}$$

   Therefore, $c = 356$.

   (b) i. By Extended Euclidean Algorithm, we have $\gcd(352, 29) = 1 = 85 \times 29 - 7 \times 352$. Then we find the private key d.

$$\begin{aligned} 29d &\equiv 1 \pmod{352} \\ 85(29d) &\equiv 85 \pmod{352} \\ d &\equiv 85 \pmod{352} \end{aligned}$$

   Therefore, if $e = 29$, the private key $d = 85$.

   ii. The orrginal message m is given by $m \equiv c^d \pmod{n}$. Since $18^{85} \equiv 154 \pmod{391}$, we have $m = 154$.

9. Given a ciphertext $c = 125$ and a public key $(n, e) = (28459, 109)$. First, $28459 = 149 \cdot 191$ and $\varphi(28459) = (149-1) \cdot (191-1) = 148 \cdot 190 = 28120$. Then by Extended Euclidean Algorithm, we have $\gcd(28120, 109) = 1 = 54 \times 28120 - 13931 \times 109$. Next we find the private key d.

$$\begin{aligned} 109d &\equiv 1 \pmod{28120} \\ (-13931)(109d) &\equiv -13931 \pmod{28120} \\ d &\equiv 14189 \pmod{28120} \end{aligned}$$

   Finally, we find m by $m \equiv c^d \pmod{28459}$

$$125^{14189} \equiv 10320 \pmod{28459}$$

   Therefore, the original message $m = 10320$.