# Exercise of Chapter 1

Written by Hsin-Jung, Wu.

## Section 1.1

1. Since $[a_n a_{n-1} \dots a_1 a_0]_{10} = a_2a_1a_0 + a_5a_4a_3 \times 1000 + a_8a_7a_6 \times 1000^2 + \dots$ But $1000 \equiv -1 \pmod{k}$, for $k = 7, 11, 13$.

   So $[a_n a_{n-1} \dots a_1 a_0]_{10}] \equiv a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 + \dots \pmod{k}$. where $k = 7, 11, 13$

2. If $\overline{r_i + s} = \overline{r_j + s}$ for $i < j$, then $\overline{r_i - r_j} \equiv 0 \pmod{n}$. Thus we have a contradiction that $\overline{r_i} = \overline{r_j}$. So $\{\overline{r_1 + s} \dots \overline{r_n + s}\} = \mathbb{Z}_n$

3. Consider $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, then $A^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

4. $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, but $AB = 0$

5. 本題參考自Fermat Number

$$
\begin{aligned}
F_5 &= 4294967297 \\
&= 641 \times 6700417 \\
F_7 &= 340282366920938463463374607431768211457 \\
&= 59649589127497217 \times 5704689200685129054721
\end{aligned}
$$

## Section 1.2

1. (a)

$$
355 = 113 \times 3 + 16
$$

$$
113 = 16 \times 7 + 1
$$

Then $1 = 113 - 16 \times 7 = 113 - (355 - 113 \times 3) \times 7 = 113 \times 22 - 355 \times 7$.

So $x = 44 - 355t$, $y = -14 + 113t$, where $t$ is an integer. ■

(b) It is equivalent to solve $23x + 5y = 9$.

$$23 = 5 \times 4 + 3$$
$$5 = 3 \times 1 + 2$$
$$3 = 2 \times 1 + 1$$

Then $1 = 3-2 = 3-(5-3) = 3\times2-5 = (23-5\times4)\times2-5 = 23\times2-5\times9$.

So $x = 18 - 5t$, $y = -81 + 23t$, where $t$ is an integer. ■

(c) Since $25x+15y \equiv 0 \pmod 5$ but $8 \equiv 3 \pmod 5$. Hence it has no solution.

2. It is easy to see that $(-1-\sqrt{2})^n = a_n - b_n\sqrt{2}$. So we have that ${a_n}^2 - 2{b_n}^2 = \big((-1-\sqrt{2})(-1+\sqrt{2})\big)^n = -1^n$. Hence we complete the proof.

3. May assume $c$ is positive. Consider $S = \{\overline{a+b}, \overline{a+2b}, \ldots, \overline{a+cb}\}$. If $S = \mathbb{Z}_c$, there exists some $i$ such that $a + bi \equiv 1 \pmod c$, say $a + bi = kc + 1$, where $k$ is some integer. Let $d$ is the great common divisor of $a + bi$ and $c$, then $d|(a+bi) - kc \Rightarrow d|1$, so $d = 1$. Hence we are done. Otherwise, there exists $i > j$ such that $a+bi \equiv a+bj \pmod c$. Then we have $c|(a+bi)-(a+bj)$ thus $c|b(i-j)$. Since $0 < i-j < c$, then $c|b$, say $b = kc$, where $k$ is some integer. Let $d$ is the great common divisor of $a+b$ and $c$, then $d|(a+b) - kc \Rightarrow d|a$. Thus $d$ is a common divisor of $a$ and $b$, so $d = 1$. Hence we are done.

## Section 1.3

1. It is easy to see that

$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv 4 \pmod{11}$$

So $x = 2 \times 35 + 77 + 4 \times 55 + 385t = 367 + 385t$, where $t$ is any integer.

## Section 1.4

1. (1). Since $sx \equiv sy \pmod{n}$, then $sx - sy = kn$ for some integer $k$. But $s, n$ are relative prime, so $k/s$ must be an integer. Hence $x - y \equiv 0 \pmod{n}$, i.e. $x \equiv y \pmod{n}$.

   (2). Since for each $i < j$, $\overline{r_i} \neq \overline{r_j}$, then by (1) we know that $\{\overline{sr_1}, \ldots, \overline{sr_n}\}$ are distinct, then $\mathbb{Z}_n = \{\overline{sr_1}, \ldots, \overline{sr_n}\}$