Assignment 4 **LE, Nhat Hung**
MATH 240 February 15, 2018

1. **Division algorithm:**

$$\forall a, b \in \mathbb{Z}\ (b \neq 0), \begin{cases} a = qb + r \\ 0 \leq r < |b| \end{cases} \text{ with } q, r \in \mathbb{Z}$$

Case of $a = 0,\ b \neq 0 : q, r = 0$

Case of $a, b < 0$:
Having proven the algorithm for $a, b > 0$, we know $-a = q(-b) + r$.

$$\begin{aligned} -a = q(-b) + r \quad &\Rightarrow a = qb - r \\ &\Rightarrow a = qb + b - b - r \\ &\Rightarrow a = (q+1)b - b - r \\ &\Rightarrow \begin{cases} a = q'b + r' \\ q' = q + 1,\ r' = -b - r \\ 0 \leq |b| - r < |b| \end{cases} \\ &\Rightarrow \begin{cases} a = q'b + r' \\ 0 \leq -b - r < |b| \end{cases} \\ &\Rightarrow \begin{cases} a = q'b + r' \\ 0 \leq r' < |b| \end{cases} \end{aligned}$$

Case of $a < 0,\ b > 0$:

$$\begin{aligned} -a = qb + r \quad &\Rightarrow a = -qb - r \\ &\Rightarrow a = -qb - b + b - r \\ &\Rightarrow a = -(q+1)b + b - r \\ &\Rightarrow \begin{cases} a = q'b + r' \\ q' = -(q+1),\ r' = b - r \\ 0 \leq b - r < |b| \end{cases} \\ &\Rightarrow \begin{cases} a = q'b + r' \\ 0 \leq r' < |b| \end{cases} \end{aligned}$$

Case of $a > 0,\ b < 0$:

$$\begin{aligned} a = q(-b) + r \quad &\Rightarrow a = -qb + r \\ &\Rightarrow \begin{cases} a = q'b + r \\ q' = -q \\ 0 \leq r < |b| \end{cases} \\ &\Rightarrow \begin{cases} a = q'b + r \\ 0 \leq r < |b| \end{cases} \end{aligned}$$

2. (a)

$$\begin{array}{lcllll} 2018 & = & 8 \cdot 240 & + & 98 \\ 240 & = & 2 \cdot 98 & + & 44 \\ 98 & = & 2 \cdot 44 & + & 10 \\ 44 & = & 4 \cdot 10 & + & 4 \\ 10 & = & 2 \cdot 4 & + & 2 \\ 4 & = & 2 \cdot 2 \end{array}$$

$gcd(2018, 240) = 2$

$$
\begin{aligned}
10 = 2 \cdot 4 + 2 \quad &\Rightarrow 10 - 2 \cdot 4 = 2 \\
&\Rightarrow (98 - 2 \cdot 44) - 2(44 - 4 \cdot 10) = 2 \\
&\Rightarrow 98 - 4 \cdot 44 + 8 \cdot 10 = 2 \\
&\Rightarrow 2018 - 8 \cdot 240 - 4(240 - 2 \cdot 98) + 8(98 - 2 \cdot 44) = 2 \\
&\Rightarrow 2018 - 12 \cdot 240 + 16 \cdot 98 - 16 \cdot 44 = 2 \\
&\Rightarrow 2018 - 12 \cdot 240 + 16(2018 - 8 \cdot 240) - 16(240 - 2 \cdot 98) = 2 \\
&\Rightarrow 17 \cdot 2018 - 156 \cdot 240 + 32 \cdot 98 = 2 \\
&\Rightarrow 17 \cdot 2018 - 156 \cdot 240 + 32(2018 - 8 \cdot 240) = 2 \\
&\Rightarrow 49 \cdot 2018 - 412 \cdot 240 = 2
\end{aligned}
$$

(b) $gcd(a, b) = 1 \Rightarrow la + mb = 1,\ l, b \in \mathbb{Z}$

$$
\begin{aligned}
&\begin{cases} la(k^2 - 1) = kl(b + ka) - klb - la \\ mb(k^2 - 1) = km(a + kb) - kma - mb \end{cases} \quad \Rightarrow \quad (k^2 - 1)(la + mb) = kl(a + kb) + km(b + ka) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad -klb - la - kma - mb \\
&\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow \quad (k^2 - 1) \cdot 1 = kl(a + kb) + km(b + ka) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad -l(a + kb) - m(b + ka) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow \quad (k^2 - 1) = (kl - m)(a + kb) + (km - l)(b + ka) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow \quad \begin{cases} d \mid (k^2 - 1) \\ d = gcd(a + kb, b + ka) \end{cases}
\end{aligned}
$$

(c)

$$
\begin{aligned}
&\begin{cases} p \text{ prime} \\ p \mid n \\ p \nmid m \end{cases} \quad \Rightarrow \begin{cases} gcd(p, m) = 1 \\ p \mid (m \cdot \frac{n}{m}) \end{cases} \\
&\qquad\qquad\quad \Rightarrow p \mid \tfrac{n}{m}
\end{aligned}
$$

3. (a)

$ka \equiv kb \pmod{kn}$	$a \equiv b \pmod{n}$
$\Rightarrow kn \mid (ka - kb)$	$\Rightarrow n \mid (a - b)$
$\Rightarrow ka - kb = l(kn),\ l \in \mathbb{Z}$	$\Rightarrow a - b = mn,\ m \in \mathbb{Z}$
$\Rightarrow a - b = ln$	$\Rightarrow ka - kb = m(kn)$
$\Rightarrow n \mid (a - b)$	$\Rightarrow kn \mid (ka - kb)$
$\Rightarrow a \equiv b \pmod{\text{n}}$	$\Rightarrow ka \equiv kb \pmod{\text{kn}}$

Thus, $ka \equiv kb \pmod{kn} \Leftrightarrow a \equiv b \pmod{n}$

(b) $a \equiv b \pmod{n} \Rightarrow a - b = kn,\ k \in \mathbb{Z}$
Let $c = gcd(a, n)$, $d = gcd(b, n)$.

$$
\begin{aligned}
a - b = kn \quad &\Rightarrow \tfrac{a}{c} - \tfrac{n}{c}k = \tfrac{b}{c} \\
&\Rightarrow c \mid b \\
&\Rightarrow c \leq d
\end{aligned}
$$

Similarly, $d \mid a$ and $d \leq c$.
Thus, c = d, or $gcd(a, n) = gcd(b, n)$.

(c)

$$
\begin{aligned}
1806 \equiv 4 \pmod{17} \quad &\Rightarrow 1806^2 \equiv 16 \equiv -1 \pmod{17} \\
&\Rightarrow (1806^2)^{3118} \equiv (-1)^{3118} \pmod{17} \\
&\Rightarrow 1806^{6236} \equiv 1 \pmod{17}
\end{aligned}
$$