Assignment 4 **LE, Nhat Hung**

MATH 240 February 20, 2018

1. (a)

$$\begin{array}{lllll} 243 & = 235 & + & 8 \\ 235 & = 29 \cdot 8 & + & 3 \\ 8 & = 2 \cdot 3 & + & 2 \\ 3 & = 2 & + & 1 \end{array}$$

$gcd(235, 243) = 1$

$$\begin{aligned} 3 = 2 + 1 \quad & \Rightarrow 3 - 2 = 1 \\ & \Rightarrow 235 - 29 \cdot 8 - (8 - 2 \cdot 3) = 1 \\ & \Rightarrow 235 - 30 \cdot 8 + 2 \cdot 3 = 1 \\ & \Rightarrow 235 - 30(243 - 235) + 2(235 - 29 \cdot 8) = 1 \\ & \Rightarrow 33 \cdot 235 - 30 \cdot 243 - 58 \cdot 8 = 1 \\ & \Rightarrow 33 \cdot 235 - 30 \cdot 243 - 58(243 - 235) = 1 \\ & \Rightarrow 91 \cdot 235 - 88 \cdot 243 = 1 \\ & \Rightarrow 235^{-1} = 91 \pmod{243} \end{aligned}$$

$$\begin{aligned} 235x \equiv 12 \pmod{243} \quad & \Rightarrow x \equiv 12 \cdot 91 \pmod{243} \\ & \Rightarrow x \equiv 1092 \equiv 120 \pmod{243} \\ & \Rightarrow x = 120 \end{aligned}$$

(b) $235 = 5 \cdot 47$
$245 = 5 \cdot 7^2$
$gcd(234, 245) = 5$

Suppose $235x \equiv 12 \pmod{245}$ has a solution.

$$\begin{aligned} 235x \equiv 12 \pmod{245} \quad & \Rightarrow 235x = 245q + 12,\ q \in \mathbb{Z} \\ & \Rightarrow 235x - 245q = 12 \\ & \Rightarrow gcd(235, 245) \mid 12 \\ & \Rightarrow 5 \mid 12 \end{aligned}$$

But $5 \nmid 12$.
Thus, $235x \equiv 12 \pmod{245}$ has no solutions.

(c) $235x \equiv 10 \pmod{245} \Leftrightarrow 47x \equiv 2 \pmod{49}$

$$\begin{array}{llll} 49 & = 47 & + & 2 \\ 47 & = 23 \cdot 2 & + & 1 \end{array}$$

$gcd(47, 49) = 1$

$$\begin{aligned} 47 = 23 \cdot 2 + 1 \quad & \Rightarrow 47 - 23 \cdot 2 = 1 \\ & \Rightarrow 47 - 23(49 - 47) = 1 \\ & \Rightarrow 24 \cdot 47 - 23 \cdot 49 = 1 \\ & \Rightarrow 47^{-1} = 24 \pmod{49} \end{aligned}$$

$$\begin{aligned}
235x \equiv 10 \pmod{245} \quad &\Rightarrow 47x \equiv 2 \pmod{49} \\
&\Rightarrow x \equiv 2 \cdot 24 \pmod{49} \\
&\Rightarrow x \equiv 48 \pmod{49} \\
&\Rightarrow x = 48 + 49k,\ k \in \mathbb{Z} \text{ and } 0 \leq x < 245 \\
&\Rightarrow x = 48, 97, 146, 195 \text{ or } 244
\end{aligned}$$

2. Let $d_0, ..., d_{k-1}$ digits of $n \in \mathbb{Z}$.

$$n = \overline{d_{k-1}d_{k-2}...d_1d_0}$$

$$\begin{aligned}
n \equiv \overline{d_{k-1}d_{k-2}...d_1d_0} \pmod{11} \quad &\Rightarrow n \equiv 10^{k-1}d_{k-1} + 10^{k-2}d_{k-2} + ... + 10d_1 + d_0 \pmod{11} \\
&\Rightarrow n \equiv (-1)^{k-1}d_{k-1} + (-1)^{k-2}d_{k-2} + ... + (-1)d_1 + d_0 \pmod{11} \\
&\Rightarrow n \equiv d_{k-1} + (-d_{k-2}) + ... + (-d_1) + d_0 \pmod{11} \\
&\quad \text{or, if last digit's label is odd:} \\
&\quad n \equiv (-d_{k-1}) + d_{k-2} + ... + (-d_1) + d_0 \pmod{11}
\end{aligned}$$

Without loss of generality, let the last digit's label be even.
Want to prove:

$$\textbf{(1)}\ 11 \mid [(d_0 + d_2 + ... + d_{k-1}) - (d_1 + d_3 + ... + d_{k-2})] \Leftrightarrow 11 \mid n\ \textbf{(2)}$$

$$\begin{aligned}
\textbf{(1)} \quad &\Rightarrow (d_0 + d_2 + ... + d_{k-1}) - (d_1 + d_3 + ... + d_{k-2}) \equiv 0 \pmod{11} \\
&\Rightarrow d_{k-1} + (-d_{k-2}) + ... + (-d_3) + d_2 + (-d_1) + d_0 \equiv 0 \pmod{11} \\
&\Rightarrow n \equiv 0 \pmod{11} \\
&\Rightarrow 11 \mid n
\end{aligned}$$

$$\begin{aligned}
\textbf{(2)} \quad &\Rightarrow n \equiv 0 \pmod{11} \\
&\Rightarrow d_{k-1} + (-d_{k-2}) + ... + (-d_3) + d_2 + (-d_1) + d_0 \equiv 0 \pmod{11} \\
&\Rightarrow (d_0 + d_2 + ... + d_{k-1}) - (d_1 + d_3 + ... + d_{k-2}) \equiv 0 \pmod{11} \\
&\Rightarrow 11 \mid [(d_0 + d_2 + ... + d_{k-1}) - (d_1 + d_3 + ... + d_{k-2})] \qquad \square
\end{aligned}$$

Thus, $11 \mid [(d_0 + d_2 + ... + d_{k-1}) - (d_1 + d_3 + ... + d_{k-2})] \Leftrightarrow 11 \mid n$.

3. (a) $p = 13, q = 17$.
   (b) $(p-1)(q-1) = 192$

$$\begin{aligned}
192 &= 113 &+&\ 79 \\
113 &= 79 &+&\ 34 \\
79 &= 2 \cdot 34 &+&\ 11 \\
34 &= 3 \cdot 11 &+&\ 1
\end{aligned}$$

$$\begin{aligned}
34 = 3 \cdot 11 + 1 \quad &\Rightarrow 34 - 3 \cdot 11 = 1 \\
&\Rightarrow 113 - 79 - 3(79 - 2 \cdot 34) = 1 \\
&\Rightarrow 113 - 4 \cdot 79 + 6 \cdot 34 = 1 \\
&\Rightarrow 113 - 4 \cdot (192 - 113) + 6 \cdot (113 - 79) = 1 \\
&\Rightarrow 11 \cdot 113 - 4 \cdot 192 - 6 \cdot 79 = 1 \\
&\Rightarrow 11 \cdot 113 - 4 \cdot 192 - 6 \cdot (192 - 113) = 1 \\
&\Rightarrow 17 \cdot 113 - 10 \cdot 192 = 1
\end{aligned}$$

$e^{-1} \equiv 113^{-1} \equiv 17 \pmod{192}$

Then, $d = 17$

Let M be E decoded.

$$\begin{aligned} M &\equiv E^d \pmod{221} \\ &\equiv 2^{17} \pmod{221} \\ &\equiv 19 \pmod{221} \end{aligned}$$

(c) $p - 1 = 12$
$q - 1 = 16$

$$\begin{array}{lll} 113 & = 9 \cdot 12 & + \quad 5 \\ 12 & = 2 \cdot 5 & + \quad 2 \\ 5 & = 2 \cdot 2 & + \quad 1 \end{array}$$

$$\begin{aligned} 5 = 2 \cdot 2 + 1 \quad &\Rightarrow 5 - 2 \cdot 2 = 1 \\ &\Rightarrow 113 - 9 \cdot 12 - 2(12 - 2 \cdot 5) = 1 \\ &\Rightarrow 113 - 11 \cdot 12 + 4(113 - 9 \cdot 12) = 1 \\ &\Rightarrow 5 \cdot 113 - 47 \cdot 12 = 1 \end{aligned}$$

$e^{-1} \equiv 113^{-1} \equiv 5 \pmod{12}$
Let $d_1 = 5$.

$113 = 7 \cdot 16 + 1 \Rightarrow 113 - 7 \cdot 16 = 1$
$e^{-1} \equiv 113^{-1} \equiv 1 \pmod{16}$
Let $d_2 = 1$.

$$\begin{aligned} \begin{cases} x \equiv E^{d_1} \pmod{p} \\ x \equiv E^{d_2} \pmod{q} \end{cases} \quad &\Rightarrow \begin{cases} x \equiv 2^5 \pmod{13} \\ x \equiv 2^1 \pmod{17} \end{cases} \\ &\Rightarrow \begin{cases} x \equiv 6 \pmod{13} \\ x \equiv 2 \pmod{17} \end{cases} \end{aligned}$$

$$\begin{array}{ll} 17 & = 13 + 4 \\ 13 & = 3 \cdot 4 + 1 \end{array}$$

$$\begin{aligned} 13 = 3 \cdot 4 + 1 \quad &\Rightarrow 13 - 3 \cdot 4 = 1 \\ &\Rightarrow 13 - 3(17 - 13) = 1 \\ &\Rightarrow 4 \cdot 13 - 3 \cdot 17 = 1 \end{aligned}$$

By the Chinese Remainder Theorem,

$$\begin{aligned} M &\equiv x \pmod{221} \\ &\equiv 6(-3 \cdot 17) + 2(4 \cdot 13) \pmod{221} \\ &\equiv -202 \pmod{221} \\ &\equiv 19 \pmod{221} \end{aligned}$$