

$$\begin{aligned}
 1) \ a) \ \gcd(14039, 152) \\
 &= \gcd(1529, 278) \\
 &= \gcd(278, 139) \\
 &= \gcd(139, 0) \\
 &= 139
 \end{aligned}$$

$$14039 = 9 \cdot 1529 + 278$$

$$1529 = 5 \cdot 278 + 139$$

$$\begin{aligned}
 \Rightarrow 139 &= 1529 - 5 \cdot 278 \\
 &= 1529 - 5 \cdot (14039 - 9 \cdot 1529) \\
 &= 1529 + 45 \cdot 1529 - 5 \cdot 14039 \\
 &= 46(1529) - 5(14039)
 \end{aligned}$$

$$s = -5 \quad t = 46$$

$$\begin{aligned}
 b) \ 1528x &\equiv 1 \pmod{14039} \\
 x &\equiv \frac{1}{1528} \pmod{14039} \\
 x &\equiv 1528^{-1} \pmod{14039}
 \end{aligned}$$

$$\Rightarrow 14039 = 1528(9) + 287$$

$$1528 = 287(5) + 93$$

$$287 = 93(3) + 8$$

$$93 = 8(11) + 5$$

$$8 = 5(1) + 3$$

$$5 = 3(1) + 2$$

$$3 = 2(1) + 1$$

$$\Rightarrow 1 = 3 - 2$$

$$= 3 - (5 - 3)$$

$$= 2 \cdot 3 - 5$$

$$= 2 \cdot (8 - 5) - 5 = 2(8) - 3(5)$$

$$= 2(8) - 3(93 - 11(8))$$

$$= 2(8) - 3(93) + 33(8)$$

$$= 35(8) - 3(93)$$

$$= 35(287 - 3(93)) - 3(93)$$

$$= 35(287) - 108(93)$$

$$= 35(14039 - 9(1528)) - 108(1528 - 5(287))$$

$$\begin{aligned}
&= 35(14039) - 315(1528) - 108(1528) \\
&\quad + 540(287) \\
&= 35(14039) - 423(1528) + 540(287) \\
&\geq 35(14039) - 423(1528) + 540(14039 - 9(1528)) \\
&= 35(14039) - 423(1528) + 540(14039) - \\
&\quad 4860(1528) \\
&= \cancel{575(14039)} - 5283(1528)
\end{aligned}$$

$$1528^{-1} \pmod{14039} \equiv -5283 \equiv 8756$$

$$1528x \equiv 1 \pmod{14039}$$

$$x = 8756 \quad \underline{953}$$

$$C) \quad 2x \equiv 3 \pmod{5}$$

$$5x \equiv 2 \pmod{6}$$

$$CRT \quad 4x \equiv 8 \pmod{11}$$

$$\Rightarrow x \equiv 4 \pmod{5}$$

$$x \equiv 4 \pmod{6}$$

$$x \equiv 2 \pmod{11}$$

$$1. \quad 2x \equiv 3 \pmod{5}$$

$$2x \equiv 3+5 \pmod{5}$$

$$x \equiv \frac{7}{2} \pmod{5}$$

$$\hookrightarrow \gcd(2, 5) = 1$$

$$x \equiv 4 \pmod{5}$$

$$6x - 1x$$

$$2. \quad 5x \equiv 2 \pmod{6}$$

$$-1x \equiv 2 \pmod{6}$$

$$x \equiv -2 \pmod{6}$$

$$x \equiv 4 \pmod{6}$$

$$3. \quad 4x \equiv 8 \pmod{11}$$

$$x \equiv \frac{7}{4} \pmod{11}$$

$$\hookrightarrow \gcd(4, 11) = 1$$

$$x \equiv 2 \pmod{11}$$

$$1) m = 5 \cdot 6 \cdot 11 = 330$$

$$2) m_1 = \frac{m}{m_1} = 66$$

$$m_2 = 55$$

$$m_3 = 30$$

$$3) y_1 = m_1^{-1} = 1 \pmod{5}$$

$$y_2 = m_2^{-1} = 1 \pmod{6}$$

$$y_3 = m_3^{-1} = 7 \pmod{11}$$

$$4) X = 1 \cdot 4 \cdot 66 + 1 \cdot 4 \cdot 55 + 7 \cdot 2 \cdot 30 \\ = 904 \equiv 224 \pmod{330}$$

$$X = 224 + 330y$$

- 2) 1) Paris
2) Bordeaux
3) Lyon
4) Marseille
5) Nice
6) Cannes

- 3) 1) Argo
2) Alien
3) Chicago
4) Grease
5) Titanic

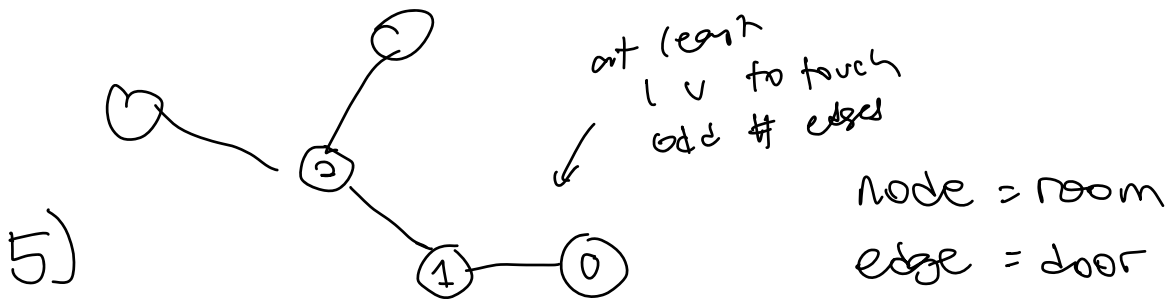
4) Eve has: c is a message r to
 $m^e \pmod n$ encrypt as $z = r^e \pmod n$
 and given to Bob; Bob
 will return $X^d \pmod n$
 let $X = c \cdot z$

- $a^b \pmod c = (a \pmod c)^b \pmod c$
- $xy \pmod z = x \pmod z \cdot y \pmod z$
- $\phi(n) = \phi(pq)$
 $= \phi(p) \phi(q) = (p-1)(q-1)$
- $\gcd(e, (p-1)(q-1)) = 1$
- $de \equiv 1 \pmod{(p-1)(q-1)}$

$$\begin{aligned}
 X^d \pmod n &= (m^e \pmod n \cdot r^e \pmod n)^d \pmod n \\
 &= (m^e r^e)^d \pmod n \quad \cancel{\pmod n} \\
 &= (mr)^{de} \pmod n \\
 &= (mr)^{1+k(p-1)(q-1)} \pmod n \\
 &= (mr) (mr)^{k(p-1)(q-1)} \pmod n \\
 &= (mr) (mr)^{k\phi(n)} \pmod n \\
 &= (mr) \left[\cancel{(mr)^{\phi(n)}}^k \right] \pmod n \\
 &\quad \quad \quad \downarrow -1 \\
 &= mr \pmod n
 \end{aligned}$$

$$\Rightarrow m \pmod n = \frac{mr \pmod n}{r}$$

\Rightarrow Eve should construct X to be
 Alice's ciphertext times some ciphertext
 z of a message r using Bob's encryption
 method.



Given that the mansion has one entrance (door, edge) and assigning edges to be doors and nodes to be rooms, and using the Handshake Lemma, which states that the number of vertices that touches an odd number of edges in a finite undirected graph is even, there is at least one room (vertex; one of two (even) of the rooms that touches the door (edge; one (odd))) that is the entrance to the mansion which touches an odd # of doors and has no ghost.

Issac Zheng