§ 4.1

recall:

$a \equiv b \pmod m \Rightarrow m \mid (a-b)$

$\underbrace{7 \equiv 3 \pmod 2} \Rightarrow 2 \mid (7-3) \Rightarrow 2 \mid 4 \Rightarrow 4 = 2\times 2 + 0$

Theorem: $a \equiv b \pmod m$ iff $a \bmod m = b \bmod m$

$7 \equiv 3 \pmod 2$ iff $\underbrace{7 \bmod 2}_{1} = \underbrace{3 \bmod 2}_{1}$

Theorem 5. let $m$ be a positive integer. if $a \equiv b \pmod m$ and $c \equiv d \pmod m$.

then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$

Pf. $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow a - b = m \cdot k \quad k \in \mathbb{Z}$

$a = b + mk$ ①

$c \equiv d \pmod m \Rightarrow m \mid (c-d) \Rightarrow c - d = m \cdot p \quad p \in \mathbb{Z}$

$c = d + mp$ ②

Backward Reasoning

$a + c \equiv (b+d) \pmod m$

$\downarrow$

$m \mid [(a+c) - (b+d)]$

$\downarrow$

$(a+c) - (b+d) = m \cdot Q$

① + ② $\Rightarrow a + c = b + mk + d + mp$

$(a+c) = (b+d) + m(k+p)$

$(a+c) - (b+d) = m \cdot (k+p)$

$k, p \in \mathbb{Z}, \quad k + p \in \mathbb{Z}$

$m \mid (a+c) - (b+d)$

$(a+c) \equiv (b+d) \pmod m$

Backward Reasoning

$ac \equiv bd \pmod m$

$\downarrow$

$m \mid (ac - bd)$

$\downarrow$

$\boxed{ac} - \boxed{bd} = m \cdot \mathbb{Z}$

① · ② $= a \cdot c = (b + mk) \cdot (d + mp)$

$ac = bd + bmp + dmk + m^2kp$

$ac - bd = m(bp + dk + mkp)$

$b, p, d, k, m \in \mathbb{Z}$

$m \mid (ac - bd)$

$ac \equiv bd \pmod m$

Corollary: let $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$

(Come from theorem 5)

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$(ab) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m \;\Leftarrow$$

Ex $(19^3 \bmod 31)^4 \bmod 23$

$19^3 \bmod 31$

$= ((19 \bmod 31) \cdot (19 \bmod 31)) (19 \bmod 31) \bmod 31$

$= 19^3 \bmod 31$

---

$41^2 \bmod 31 = [(41 \bmod 31) \cdot (41 \bmod 31)] \bmod 31$

$= [\underline{10} \cdot \underline{10}] \bmod 31$

$= 100 \bmod 31$

$= 7$

$41^3 = 68921 \div 31 = \underline{2223}. \cdots$

$68921 - 31 \times 2223 =$

$41^3 \bmod 31 = [(41 \bmod 31)(41 \bmod 31)(41 \bmod 31)] \bmod 31$

$8$

$= [10 \cdot 10 \cdot 10] \bmod 31$

$= 1000 \bmod 31$

$= 8$

$1000 \div 31 = 32. \cdots$

$1000 - 31 \times 32 = 1000 - 992 = 8$

$(19^3 \bmod 31)^4 \bmod 23$

$= 8^4 \bmod 23$

$= (8^2 \cdot 8^2) \bmod 23$

$= (64 \cdot 64) \bmod 23$

$= [(64 \bmod 23)(64 \bmod 23)] \bmod 23$

$= [18 \cdot 18] \bmod 23$

$= (324) \bmod 23$

$= 2$

$19^3 = 6859 \bmod 31$

$6859 \div 31 = 221. \cdots$

Remainder $= 6859 - 31 \times 221$

$= 8$

$19^3 < \begin{matrix} 19^2 \\ 19 \end{matrix}$

$19^3 \bmod 31 = (19^2 \cdot 19) \bmod 31$

$= [(19^2 \bmod 31)(19 \bmod 31)] \bmod 31$

$= [(361 \bmod 31)(19)] \bmod 31$

$= [(20)(19)] \bmod 31$

$= 380 \bmod 31$

$= \ldots$