110054809 易頡

1、設 $P(n)$ 為 $2^n < n!$

基礎步驟：$P(4)$ 為真，因為 $2^4 = 16 < 4! = 24$

歸納步驟：假設 $P(k)$ 為真，當 k 為任意大於等於 4 的固定整數

證明 $P(k+1)$ 為真，

$$2^{k+1} = 2 \cdot 2^k$$
$$< 2 \cdot k! \quad \text{(根據歸納假設)}$$
$$< (k+1)k!$$
$$= (k+1)!$$ 這樣便完成了歸納步驟

因此，$2^n < n!$ 成立，當 n 為任意大於等於4的固定整數

2、

a) 基礎步驟

b) $P(2)$ 成立，因為 $2! = 2 < 2^2 = 4$

c) 歸納步驟：假設 $P(k)$ 為真，$k! < k^k$，當 k 為任意大於 1 的固定整數

d) 證明 $P(k+1)$ 為真

e) $(k+1)! = (k+1)k!$
$$< (k+1)k^k \quad \text{(根據歸納假設)}$$
$$< (k+1)(k+1)^k$$
$$= (k+1)^{k+1}$$

f) 因此，$n! < n^n$ 成立，當 n 為任意大於 1 的固定整數

3、a)
$644 = 2 \cdot 322 + 0$

$322 = 2 \cdot 161 + 0$

$161 = 2 \cdot 80 + 1$

$80 = 2 \cdot 40 + 0$

$40 = 2 \cdot 20 + 0$

$20 = 2 \cdot 10 + 0$

$10 = 2 \cdot 5 + 0$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

$(644)_{10} = (10\ 1000\ 0100)_2$

1010000100 110054809 易頡

4. b) $i=0$ $a_0=0$ $X=1$ $power = 11^2 \bmod 645 = 121$

$i=1$ $a_1=0$ $X=1$ $power = 121^2 \bmod 645 = 451$

$i=2$ $a_2=1$ $X = 1\cdot 451 \bmod 645 = 451$ $power = 451^2 \bmod 645 = 226$

$i=3$ $a_3=0$ $X=451$ $power = 226^2 \bmod 645 = 121$

$i=4$ $a_4=0$ $X=451$ $power = 121^2 \bmod 645 = 451$

$i=5$ $a_5=0$ $X=451$ $power = 451^2 \bmod 645 = 226$

$i=6$ $a_6=0$ $X=451$ $power = 226^2 \bmod 645 = 121$

$i=7$ $a_7=1$ $X = 451\cdot 121 \bmod 645 = 391$ $power = 121^2 \bmod 645 = 451$

$i=8$ $a_8=0$ $X=391$ $power = 451^2 \bmod 645 = 226$

$i=9$ $a_9=1$ $X = 391\cdot 226 \bmod 645 = 1$

5. c)

$11^2 \bmod 645 = (11^1 \bmod 645)^2 \bmod 645 = 11^2 \bmod 645 = 121$

$11^4 \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^8 \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

$11^{16} \bmod 645 = (226 \bmod 645)^2 \bmod 645 = 226^2 \bmod 645 = 121$

$11^{32} \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^{64} \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

$11^{128} \bmod 645 = (226 \bmod 645)^2 \bmod 645 = 226^2 \bmod 645 = 121$

$11^{256} \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^{512} \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

6. d)

$$
\begin{aligned}
11^{644} \bmod 645 &= (11^{512} \bmod 645)\cdot(11^{128} \bmod 645)\cdot(11^4 \bmod 645) \\
&= [(226\cdot 121) \bmod 645]\cdot(11^4 \bmod 645) \\
&= (27346 \bmod 645)\cdot(11^4 \bmod 645) \\
&= (256\cdot 451) \bmod 645 \\
&= 115456 \bmod 645 \\
&= 1
\end{aligned}
$$

100054809 易頡

7.

a) finite, $X=\{-4,-3,-2,-1,0,1,2,3,4\} \Rightarrow size=9$

b) finite, 因為集合有四個元素, $size = 2^4 = 16$

c) infinite

d) finite, $|A|=5$, $|B|=3$ $size = 5\times 3 = 15$

e) finite, $9x^2=1$, 沒有正整數解 $size=0$

f) finite, 因為集合有三個元素, $size = 2^3 = 8$

g) finite, $|A|=3$ $|B|=0$ $A\times B=\varnothing$ $size=0$

h) finite, $4x^2=8$, $x^2=2$, 沒有正整數解 $size=0$

i) finite, $x^2=2$ 沒有整數解, $size=0$

j) finite, 因為集合有兩個元素 $size = 2^2 = 4$

k) infinite

l) finite, $|S|=3$, $|T|=5$ $size = 3\times 5 = 15$

m) finite, $X=\{-2,-1,0,1,2\}$ $size=5$

8.

$$23^{1002} = (23^{40})^{25}\cdot 23^2 \equiv 1^{25}\cdot 529 = 529 \equiv 37 \pmod{41}$$

$$23^2 \bmod 41 = 529 \bmod 41 = 37$$

$$23^4 \bmod 41 = (37 \bmod 41)^2 \bmod 41 = 16$$

$$23^8 \bmod 41 = (16 \bmod 41)^2 \bmod 41 = 10$$

$$23^{16} \bmod 41 = (10 \bmod 41)^2 \bmod 41 = 18$$

$$23^{32} \bmod 41 = (18 \bmod 41)^2 \bmod 41 = 37$$

$$23^{40} \bmod 41 = (23^{32} \bmod 41)\cdot(23^8 \bmod 41) = (37\cdot 10) \bmod 41 = 1$$

110654809 易頡

9. a) $3^{302} = (3^4)^{75} \cdot 3^2 \equiv 1^{75} \cdot 9 = 9 \equiv 4 \pmod 5$ $81 \bmod 5 = 1$

b) $3^{302} = (3^6)^{50} \cdot 3^2 \equiv 1^{50} \cdot 9 = 9 \equiv 2 \pmod 7$ $729 \bmod 7 = 1$

c) $3^{302} = (3^{10})^{30} \cdot 3^2 \equiv 1^{30} \cdot 9 = 9 \equiv 9 \pmod{11}$

d) Let $m = 5 \cdot 7 \cdot 11 = 385$

$M_1 = \frac{385}{5} = 77$ $y_1 = 3$ is an inverse of $M_1 = 77 \bmod 5$ since $77 \cdot 3 \equiv 1 \pmod 5$

$M_2 = \frac{385}{7} = 55$ $y_2 = 6$ is an inverse of $M_2 = 55 \bmod 7$ since $55 \cdot 6 = 330 \equiv 1 \pmod 7$

$M_3 = \frac{385}{11} = 35$ $y_3 = 6$ is an inverse of $M_3 = 35 \bmod 11$ since $35 \cdot 6 = 210 \equiv 1 \pmod{11}$

Hence, $x = 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 9 \cdot 35 \cdot 6 = 3474 \equiv 9 \pmod{385}$

10. 用歐幾里德演算法，先算出 $\gcd(34, 89) = 1$

$89 = 2 \cdot 34 + 21$
$34 = 1 \cdot 21 + 13$
$21 = 1 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

反轉步驟，算出結果是1的線性組合

$$
\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3(13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8(34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34
\end{aligned}
$$

因此 $s = -34$，34 mod 89 的其中一個數論倒數為 -34，也可寫為 55

11. 用歐幾里德演算法，先算出 $\gcd(144, 233) = 1$

$233 = 1 \cdot 144 + 89$
$144 = 1 \cdot 89 + 55$
$89 = 1 \cdot 55 + 34$
$55 = 1 \cdot 34 + 21$
$34 = 1 \cdot 21 + 13$
$21 = 1 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

反轉步驟，算出結果是1的線性組合

$$
\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3(13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot 21 - 8(34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13(55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21(89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\
&= 34(144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\
&= 34 \cdot 144 - 55(233 - 144) \\
&= 89 \cdot 144 - 55 \cdot 233
\end{aligned}
$$

因此 $s = 89$，144 mod 233 其中一個數論倒數為 89

110054809 易頡

12 根據第10題的計算 $\gcd(34,89)=1$，55為 34 modulo 89 的一個數論倒數

$34x \equiv 77 \pmod{89}$，兩邊同乘 55，$55\cdot 34x \equiv 55\cdot 77 \pmod{89}$

$1870x \equiv 4235 \pmod{89}$

因為 $1870 \equiv 1 \pmod{89}$，而 $4235 \equiv 52 \pmod{89}$，

若 x 是一個解的話，$x \equiv 4235 \equiv 52 \pmod{89}$

確認每個 $x \equiv 52 \pmod{89}$ 都是解，假設 $x \equiv 52 \pmod{89}$

$34x \equiv 34\cdot 52 = 1768 \equiv 77 \pmod{89}$

可以發現所有 x 都符合同餘，$x \equiv 52 \pmod{89}$，$x = 52, 141, 230, \ldots$ 和 $-37, -126$

13、根據第11題的計算 $\gcd(144,233)=1$，89為 144 modulo 233 的一個數論倒數

$144x \equiv 4 \pmod{233}$，兩邊同乘 89，$89\cdot 144x \equiv 89\cdot 4 \pmod{233}$

$12816x \equiv 356 \pmod{233}$

因為 $12816 \equiv 1 \pmod{233}$，而 $356 \equiv 123 \pmod{233}$

若 x 是一個解的話，$x \equiv 356 \equiv 123 \pmod{233}$

確認每個 $x \equiv 123 \pmod{233}$ 都是解，假設 $x \equiv 123 \pmod{233}$

$144x \equiv 144\cdot 123 = 17712 \equiv 4 \pmod{233}$

可以發現所有 x 都符合同餘，$x \equiv 123 \pmod{233}$，

$x = 123, 356, 589, \ldots$ 和 $-110, -343, \ldots$

14.

$i=0 \quad a_0 = 1 \quad x = 19\cdot 1 \bmod 2537 = 19 \quad power = 19^2 \bmod 2537 = 361$

$i=1 \quad a_1 = 0 \quad x = 19 \quad power = 361^2 \bmod 2537 = 934$

$i=2 \quad a_2 = 1 \quad x = 19\cdot 934 \bmod 2537 = 2524 \quad power = 934^2 \bmod 2537 = 2165$

$i=3 \quad a_3 = 1 \quad x = 2524\cdot 2165 \bmod 2537 = 2299$

return $x = 2299 = 19^{13} \bmod 2537$

110054809 易頡

15.

$i=0 \quad a_0=1 \quad X=1900\cdot 1 \bmod 2537=1900 \quad power=1900^2 \bmod 2537=2386$

$i=1 \quad a_1=0 \quad X=1900 \quad power=2386^2 \bmod 2537=2505$

$i=2 \quad a_2=1 \quad X=1900\cdot 2505 \bmod 2537=88 \quad power=2505^2 \bmod 2537=1024$

$i=3 \quad a_3=1 \quad X=88\cdot 1024 \bmod 2537=1317$

return $X=1317=1900^{13} \bmod 2537$

16.

$i=0 \quad a_0=1 \quad X=210\cdot 1 \bmod 2537=210 \quad power=210^2 \bmod 2537=971$

$i=1 \quad a_1=0 \quad X=210 \quad power=971^2 \bmod 2537=1614$

$i=2 \quad a_2=1 \quad X=210\cdot 1614 \bmod 2537=1519 \quad power=1614^2 \bmod 2537=2034$

$i=3 \quad a_3=1 \quad X=1519\cdot 2034 \bmod 2537=2117$

17. 將ATTACK轉為數字表示 00 19 19 00 02 10

$n=43\cdot 59=2537$，將轉換換後的數字4位為一組

因為 $2525<2537<252525$

第一組 0019 密文 $C=(0019)^{13} \bmod 2537=2299$（根據第14題）

第二組 1900 密文 $C=(1900)^{13} \bmod 2537=1317$（根據第15題）

第三組 0210 密文 $C=(0210)^{13} \bmod 2537=2117$（根據第16題）

因此 ATTACK經RSA加密後為 2299 1317 2117

18.

$X\equiv 2 \pmod 3 \quad a_1=2 \quad m_1=3$

$X\equiv 1 \pmod 4 \quad a_2=1 \quad m_2=4 \quad m=m_1\cdot m_2\cdot m_3=60$

$X\equiv 3 \pmod 5 \quad a_3=3 \quad m_3=5$

$M_1=\dfrac{m_1\cdot m_2\cdot m_3}{m_1}=20 \quad M_2=\dfrac{m_1\cdot m_2\cdot m_3}{m_2}=15 \quad M_3=\dfrac{m_1\cdot m_2\cdot m_3}{m_3}=12$

inverse y_1 of M_1 modulo $m_1=2 \quad 40\equiv 1 \pmod 3$

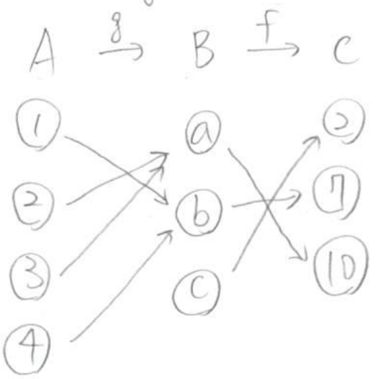
inverse y_2 of M_2 modulo $m_2=3 \quad 45\equiv 1 \pmod 4$

inverse y_3 of M_3 modulo $m_3=3 \quad 36\equiv 1 \pmod 5$

$X=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3=80+45+108=233\equiv 53 \pmod{60}$

110054809 易頡

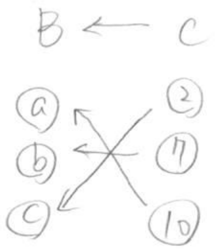
19. a) $f \circ g$



$f \circ g : A \to C$

$\{(1,7), (2,10), (3,10), (4,2)\}$

b) f^{-1}



$f^{-1}(2) = c$

$f^{-1}(7) = b$

$f^{-1}(10) = a$

20. $[p \wedge (p \to q)] \to p \equiv \neg[p \wedge (p \to q)] \vee q$ by the conditional-disjunction equivalence

$\equiv [\neg p \vee \neg(p \to q)] \vee q$ by a De Morgan's law

$\equiv (\neg p \vee q) \vee \neg(p \to q)$ by commutativity and associativity

$\equiv (\neg p \vee q) \vee \neg(\neg p \vee q)$ by the conditional-disjunction equivalence

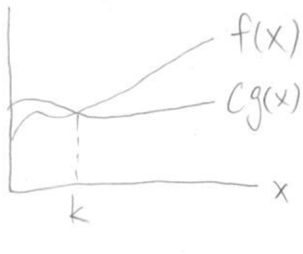
$\equiv T$ by a negation law

21.

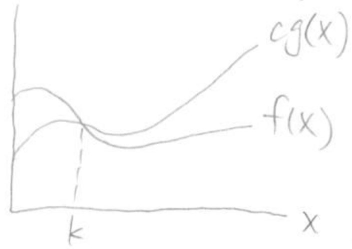
Step		Reason
1	$\neg t$	Hypothesis
2	$s \to t$	Hypothesis
3	$\neg s$	Modus tollens using (1) and (2)
4	$(\neg r \vee \neg f) \to (s \wedge l)$	Hypothesis
5	$(\neg(s \wedge l) \to \neg(\neg r \vee \neg f)$	contrapositive of (4)
6	$(\neg s \vee \neg l) \to (r \wedge f)$	De Morgan's law and double negative
7	$\neg s \vee \neg l$	Addition, using (3)
8	$r \wedge f$	Modus ponens using (6) and (7)
9	r	simplification using (8)

110054809 易頡

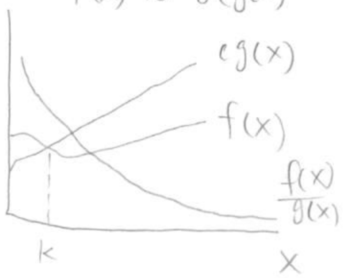
22 a) $f(x) \in \Omega(g(x))$



b) $f(x) \in O(g(x))$

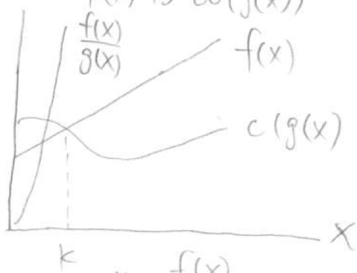


23 a) $f(x)$ is $o(g(x))$



$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$$

b) $f(x)$ is $\omega(g(x))$



$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = \infty$$

24. 基礎步驟：

$l(1) = i(1)+1$，零個內部節點時，1個葉子

遞迴步驟：

完整二元樹時每個內部節點皆有2個葉子，每個向下分支皆

葉子，而多一個內部節點，多$(2-1)$片葉子

$l(k) = i(k) + (2-1)$

25. $A_1 \times A_2 \times A_3 = \{$(竈門炭治郎，鱗滝左近次，吾峠呼世晴)，
(竈門炭治郎，鱗滝左近次，竈門禰豆子)，
(竈門炭治郎，鱗滝左近次，鬼頭明里)，
(竈門炭治郎，冨岡義勇，吾峠呼世晴)，
(竈門炭治郎，冨岡義勇，竈門禰豆子)，
(竈門炭治郎，冨岡義勇，鬼頭明里)，
(我妻善逸，鱗滝左近次，吾峠呼世晴)，(嘴平伊之助，鱗滝左近次，吾峠呼世晴)
(我妻善逸，鱗滝左近次，竈門禰豆子)，(嘴平伊之助，鱗滝左近次，竈門禰豆子)，
(我妻善逸，鱗滝左近次，鬼頭明里)，(嘴平伊之助，鱗滝左近次，鬼頭明里)，
(我妻善逸，冨岡義勇，吾峠呼世晴)，(嘴平伊之助，冨岡義勇，吾峠呼世晴)，
(我妻善逸，冨岡義勇，竈門禰豆子)，(嘴平伊之助，冨岡義勇，竈門禰豆子)，
(我妻善逸，冨岡義勇，鬼頭明里)，(嘴平伊之助，冨岡義勇，鬼頭明里)$\}$