110054809 易頎

1. Let $P(n)$ be the proposition that $2^n < n!$

Basis step: $P(4)$ is true since $2^4 = 16 < 4! = 24$

Inductive step: Assume $P(k)$ holds. $2^k < k!$ for an arbitrary integer, $k \geq 4$

To show that $P(k+1)$ holds:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! \quad \text{(by the inductive hypothesis)} \\ &< (k+1)k! \\ &= (k+1)! \end{aligned}$$

Therefore, $2^n < n!$ holds, for every integer $n \geq 4$

2. $n! < n^n$

a) Basis step

b) $P(2)$ is true, since $2! = 2 < 2^2 = 4$

c) Inductive step: Assume $P(k)$ holds, $k! < k^k$ for an arbitrary integer $k > 1$

d) prove that $P(k+1)$ holds

e) $$\begin{aligned} (k+1)! &= (k+1)k! \\ &< (k+1)k^k \quad \text{(by the inductive hypothesis)} \\ &< (k+1)(k+1)^k \\ &= (k+1)^{k+1} \end{aligned}$$

f) Therefore, $n! < n^n$ holds, for every integer $n > 1$

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

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

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

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

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

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

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

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

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

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

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) $11^{644} \bmod 645 = (11^{512} \bmod 645) \cdot (11^{128} \bmod 645) \cdot (11^4 \bmod 645)$

$= [(226 \cdot 121) \bmod 645] \cdot (11^4 \bmod 645)$

$= (27346 \bmod 645) \cdot (11^4 \bmod 645)$

$= (256 \cdot 451) \bmod 645$

$= 115456 \bmod 645$

$= 1$

110054809 易頡

7.

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

b) finite, since the set has 4 element size of the set $=2^4=16$

c) infinite

d) finite, $|A|=5$, $|B|=3$ size $=5\times3=15$

e) finite, $9x^2=1$, no positive integer can be solution, size $=0$

f) finite, since the set has 3 elements size of the set $=2^3=9$

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

h) finite, $4x^2=8$, $x^2=2$ no positive integer can be solution, size $=0$

i) finite, no integer can be solution to $x^2=2$, size $=0$

j) finite, since the set has 2 elements size of the set $=2^2=4$

k) infinite

l) finite, $|S|=3$, $|T|=5$ size $=3\times5=15$

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

8.

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

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

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

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

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

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

$23^{40} \bmod 41 = (23^{32} \bmod 41)\cdot(23^8 \bmod 41) = (37\cdot10) \bmod 41 = 1$

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. First we go through the Euclidean algorithm computation that $\gcd(34, 89) = 1$

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

then we reverse our step and write 1 as the desired linear combination:

$1 = 3 - 2$
$= 3 - (5-3) = 2 \cdot 3 - 5$
$= 2 \cdot (8-5) - 5 = 2 \cdot 8 - 3 \cdot 5$
$= 2 \cdot 8 - 3(13-8) = 5 \cdot 8 - 3 \cdot 13$
$= 5 \cdot (21-13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$
$= 5 \cdot 21 - 8(34-21) = 13 \cdot 21 - 8 \cdot 34$
$= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34$

Thus $s = -34$, so an inverse of 34 modulo 89 is -34, which can also be written as 55

11. First we go through the Euclidean algorithm computation that $\gcd(144, 233) = 1$

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

then we reverse our step and write 1 as the desired linear combination

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

Thus $s = 89$, so an inverse of 144 mod 233 is 89