

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

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

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

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, $x \equiv 52 \pmod{89}$, $x = 52, 141, 230, \dots$ 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

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

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

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, $x \equiv 123 \pmod{233}$,

$$x = 123, 356, 589, \dots \text{ 和 } -110, -343, \dots$$

14.

$$i=0 \quad a_0 = 1 \quad x = 19 \cdot 1 \pmod{2537} = 19 \quad \text{power} = 19^2 \pmod{2537} = 361$$

$$i=1 \quad a_1 = 0 \quad x = 19 \quad \text{power} = 361^2 \pmod{2537} = 934$$

$$i=2 \quad a_2 = 1 \quad x = 19 \cdot 934 \pmod{2537} = 2524 \quad \text{power} = 934^2 \pmod{2537} = 2165$$

$$i=3 \quad a_3 = 1 \quad x = 2524 \cdot 2165 \pmod{2537} = 2299$$

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

$$\begin{array}{r} 2537 \overline{) 5464460} \\ \underline{5074} \\ 3904 \\ \underline{2537} \\ 13676 \\ \underline{12685} \\ 9910 \\ \underline{7611} \\ 2299 \end{array}$$

$$\begin{array}{r} 2524 \\ \underline{2165} \\ 15144 \\ \underline{2524} \\ 5048 \\ \underline{5464460} \end{array}$$

$$\begin{array}{r} 2537 \overline{) 17746} \\ \underline{1522} \\ 2524 \\ \underline{343} \\ 2537 \overline{) 17746} \\ \underline{17611} \\ 1125 \\ \underline{10148} \\ 9776 \\ \underline{7611} \\ 2165 \end{array}$$

$$\begin{array}{r} 934 \\ \underline{19} \\ 8906 \\ \underline{934} \\ 17746 \end{array}$$