1

(1) 最小正原根

$$ \varphi(23)=22,\quad (\mathbb Z/23\mathbb Z)^\times \text{ 为阶 }22\text{ 的循环群。} $$ 检验可得模 (23) 的最小正原根为 $$ g=5. $$

(2) 以 (5) 为底的指数表（幂表）与指标表（对数表）

幂表（$(k=0,1,\dots,21)$）：$$ 5^k \pmod{23}: $$

(k)	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
$(5^k\bmod 23)$	1	5	2	10	4	20	8	17	16	11	9	22
(k)	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**		
$(5^k\bmod 23)$	18	21	13	19	3	15	6	7	12	14		

定义指标（离散对数）：$$ \operatorname{ind}_5(a)=k \iff 5^k\equiv a\pmod{23}. $$ 例如从表读出 $$ \operatorname{ind}_5(2)=2,\quad \operatorname{ind}_5(3)=16,\quad \operatorname{ind}_5(14)=21. $$

(3) 用指数表解

令 $$ x\equiv 5^t\pmod{23}. $$ 由表：$$ 3\equiv 5^{16}\pmod{23},\qquad 2\equiv 5^2\pmod{23}. $$ 代入：$$ 3x^{14}\equiv 2 \iff 5^{16}\cdot (5^t)^{14}\equiv 5^2 \iff 5^{16+14t}\equiv 5^2\pmod{23}. $$ 由于 (5) 为原根，指数同余（模 (22)）：$$ 16+14t\equiv 2\pmod{22} \iff 14t\equiv -14\equiv 8\pmod{22}. $$ $$ \gcd(14,22)=2\Rightarrow 7t\equiv 4\pmod{11}. $$ 在模 (11) 下 $$ 7^{-1}\equiv 8\pmod{11}\quad(\text{因 }7\cdot 8=56\equiv 1\pmod{11}), $$ 所以 $$ t\equiv 4\cdot 8\equiv 32\equiv 10\pmod{11}. $$ 因此（模 (22)）有两解：$$ t\equiv 10,;21\pmod{22}. $$ 对应 $$ x\equiv 5^{10}\equiv 9\pmod{23},\qquad x\equiv 5^{21}\equiv 14\pmod{23}. $$ 结论：$$ {x\equiv 9\pmod{23}\ \text{或}\ x\equiv 14\pmod{23}.} $$

2

$$ m=3\cdot 13\cdot 17=663. $$ 令 $$ m_1=3,\ m_2=13,\ m_3=17,\qquad M_i=\frac{m}{m_i}. $$ 则 $$ M_1=221,\quad M_2=51,\quad M_3=39. $$ 求逆元：

- $(221\equiv 2\pmod 3)，(2^{-1}\equiv 2\pmod 3)$，取 $$ e_1=M_1\cdot 2=442. $$
- $(51\equiv 12\pmod{13})，(12^{-1}\equiv 12\pmod{13})$，取 $$ e_2=M_2\cdot 12=612. $$
- $(39\equiv 5\pmod{17})，(5^{-1}\equiv 7\pmod{17})$，取 $$ e_3=M_3\cdot 7=273. $$

取各模的既约剩余系：$$ R_3={1,2},\quad R_{13}={1,2,\dots,12},\quad R_{17}={1,2,\dots,16}. $$ 则模 (663) 的一个既约剩余系可写为 $$ { R_{663}= \left{ \bigl(442a+612b+273c\bigr)\bmod 663 \ \middle| a\in R_3,\ b\in R_{13},\ c\in R_{17} \right}. } $$ 其大小：$$ \varphi(663)=\varphi(3)\varphi(13)\varphi(17)=2\cdot 12\cdot 16=384. $$

3.

设 (g) 是模 (m) 的原根，则 $$ (\mathbb Z/m\mathbb Z)^\times=\langle g\rangle,\qquad |\langle g\rangle|=\varphi(m). $$ 所以任意单位都可表示为 $$ g^k\pmod m. $$ 由于 (m>2)，有 $$ -1\not\equiv 1\pmod m, $$ 且 $$ (-1)^2\equiv 1\pmod m, $$ 所以 (-1) 在该乘法群中的阶为 (2)。

在阶为 (n) 的循环群 $\langle g\rangle$ 中，阶为 (2) 的元素只能是 $g^{n/2}$。取 $n=\varphi(m)$，得 $$ -1\equiv g^{\varphi(m)/2}\pmod m. $$ 所以以任一原根 (g) 为底的指标满足 $$ {\operatorname{ind}_g(-1)=\frac{\varphi(m)}{2}.} $$

4.

记 $$ \langle a_0,a_1,\dots,a_n\rangle=[a_0;a_1,\dots,a_n]. $$

(a)

$$ [1;2,3]=1+\frac{1}{2+\frac{1}{3}} =1+\frac{1}{\frac{7}{3}} =1+\frac{3}{7} =\frac{10}{7}. $$ 渐进分数（逐步截断）： $$ {\frac{1}{1},\ \frac{3}{2},\ \frac{10}{7}.} $$

(b)

计算可得 $$ [2;1,1,4,1,1]=\frac{51}{20}. $$ 渐进分数： $$ {\frac{2}{1},\ \frac{3}{1},\ \frac{5}{2},\ \frac{23}{9},\ \frac{28}{11},\ \frac{51}{20}.} $$

5.

(a)

$$ \frac{121}{21}=5+\frac{16}{21} =5+\frac{1}{\frac{21}{16}} =5+\frac{1}{1+\frac{5}{16}} =5+\frac{1}{1+\frac{1}{\frac{16}{5}}} = [5;1,3,5]. $$ 因此 $$ {\frac{121}{21}=\langle 5,1,3,5\rangle.} $$ 渐进分数： $$ {\frac{5}{1},\ \frac{6}{1},\ \frac{23}{4},\ \frac{121}{21}.} $$

(b)

欧几里得算法给出 $$ \frac{177}{292}=[0;1,1,1,1,5,1,8]. $$ 因此 $$ {\frac{177}{292}=\langle 0,1,1,1,1,5,1,8\rangle.} $$ 渐进分数： $$ {\frac{0}{1},\ \frac{1}{1},\ \frac{1}{2},\ \frac{2}{3},\ \frac{3}{5},\ \frac{17}{28},\ \frac{20}{33},\ \frac{177}{292}.} $$