计算机科学中的数学基础 Exercise11

陈昱衡 521021910939

2023 年 3 月 22 日

Warmups7

7 Ten people numbered 1 to 10 are lined up in a circle as in the Josephus problem, and every mth person is executed. (The value of m may be much larger than 10.) Prove that the first three people to go cannot be 10, k, and $k+1$ (in this order), for any k.

若第一个被删除的人是 10 号，那么 m 满足

$$m \bmod 10 = 0 \tag{1}$$

若紧接着第二个被删除时人是 k, 那么由于有十个人，而第一次删除的恰好是 10 号，那么第二轮相当于有九个人，从头开始删除，那么 m 满足

$$m \bmod 9 = k \tag{2}$$

若紧接着删除编号为 $k+1$ 的人，那么 m 满足

$$m \bmod 8 = 1 \tag{3}$$

而 m 若同时满足这些条件，就有 m 既为奇数，又为偶数，故不存在这样的 m。

Warmups8

8 The residue number system $(x \bmod 3, x \bmod 5)$ considered in the text has the curious property that 13 corresponds to $(1,3)$, which looks almost the same. Explain how to find all instances of such a coincidence, without calculating all fifteen pairs of residues. In other words, find all solutions to the congruences

$$10x + y \equiv x \pmod 3, \qquad 10x + y \equiv y \pmod 5.$$

Hint: Use the facts that $10u + 6v \equiv u \pmod 3$ and $10u + 6v \equiv v \pmod 5$.

根据题意，x, y 满足，

$$10x + y \equiv x \bmod 3 \tag{4}$$

$$10x + y \equiv y \bmod 5 \tag{5}$$

根据提示，

$$10x + 6y \equiv x \bmod 3 \tag{6}$$

$$10x + 6y \equiv y \bmod 5 \tag{7}$$

所以，两式相减，有

$$5y \equiv 0 \bmod 5 \tag{8}$$

$$\tag{9}$$

得到，$y=0$ 或 $y=3$ 代入，可得 $x=0$ 或 $x=1$.

Warmups9

9 Show that $(3^{77}-1)/2$ is odd and composite. *Hint:* What is $3^{77} \bmod 4$?

由二项式展开，有

$$\begin{aligned} 3^{77}-1 &= (4-1)^{77}-1 && (10)\\ &= 4^{77} - 77\times 4^{76} + \cdots + 77\times 4 - 4 + 3 && (11)\\ & && (12) \end{aligned}$$

故，根据提示，可以计算得，

$$3^{77} - 1 \bmod 4 = 3 \tag{13}$$

故，可以计算得到，$\frac{3^{77}-1}{2}$ 是奇数。同时，由等差数列求和公式，

$$\begin{aligned} \frac{3^{77}-1}{2} &= 1+3+3^2+3*3+\cdots+3^{77} && (14)\\ &= (1+3+3^2+\cdots+3^7)+3^8\times(1+3+3^2+\cdots+3^7)+\cdots+3^{70}\times(1+3+3^2+\cdots+3^7) && (15)\\ &= (1+3+3^2+\cdots+3^7)\times(1+3^8+\cdots+3^{70}) && (16) \end{aligned}$$

故，$\frac{3^{77}-1}{2}$ 是奇的合数。

Basics17

17 Let f_n be the "Fermat number" $2^{2^n}+1$. Prove that $f_m \perp f_n$ if $m<n$.

观察费马数，猜测，

$$f_n = f_{n-1}\times f_{n-2}\times f_0 + 2 \tag{17}$$

现用数学归纳法证明。易证，当 $n=1$ 时, 有

$$f_1 = 5 = 4+1 = 3+2 = f_0+2 \tag{18}$$

假设，当第 $n-1$ 项满足时，有

$$\begin{aligned} f_n &= 2^{2^n}+1 && (19)\\ f_{n-1} &= 2^{2^{n-1}}+1 && (20)\\ &= f_{n-2}\times f_0 + 2 && (21)\\ f_{n-2}\times\cdots f_0 &= 2^{2^{n-1}}-1 && (22)\\ f_{n-1}\times f_{n-2}\times\cdots\times f_0 &= (2^{2^{n-1}}-1)\times(2^{2^{n-1}}+1) && (23)\\ &= 2^{2^n}-1 && (24)\\ &= f_n - 2 && (25) \end{aligned}$$

故，

$$f_n = f_0 \times f_1 \times \cdots \times f_{n-1} + 2 \tag{26}$$

故，因为 $m \leq n$

$$f_n \bmod f_m \equiv 2 \tag{27}$$

由

$$gcd(n, m) = gcd(n \bmod m, m) \tag{28}$$

得，

$$\begin{aligned} gcd(f_n, f_m) &= gcd(f_n \bmod f_m, f_m) && (29)\\ &= gcd(2, f_m) && (30)\\ &= 1 && (31) \end{aligned}$$

故, 得到 f_m 和 f_m 互素。