CSC3001 离散数学 :教程 6

由 Rybin Dmitry主持
dmitrybin@link.cuhk.edu.cn

香港中文大学（深圳）

2022 年 10 月 26 日

无聊学生的棘手问题

1. 什么时候是 $6^{n-2} + 3n-2 + 2n-2 - 1$ 能被 n 整除?

2. 证明

$$x^3 + 是^4 = z^5$$

有无限多个正整数解。相同的

$$x^{k} {}^{k+1} + y = z^{k+2},$$

其中k是正整数。

是否同样适用

$$x^{2k} + y^{2k+2} = z^{2k+4}?$$

数论回顾

1 由于乘法是可逆的,因此乘以数

a置换残基1, 2, ..., p − 1。因此是数字的乘积

1, 2, ..., p − 1 模p等于数字的乘积

a, 2a, 3a, ...,(p - 1)a。因此

$$一个^{p-1} = 1 \text{ 模}p$$

2

数论回顾

1. (GCD作为线性组合)最重要的性质

   d = gcd(a, b) 两个数a, b是a和b组成的最小正整数组合

$$d = ma + nb = \min\{x > 0 | x = ma + nb, n, m \in Z\}$$

2. 特别是,对于互质数a, b我们有gcd(a, b) = 1,因此

$$1 = ma + nb$$

   意思是

$$1 = ma \bmod b$$

3. (模 b 乘法)先前的恒等式表明,如果a与b互质,则a 模b是可逆的　(模素p 乘法)特别是,数字

4.

   1, 2, ..., p − 1 都是模p 可逆的。

练习 1

做模乘

$$12345 \cdot 67890 \text{ 模型 } 17$$

$$2^{7}9 \text{ 模 } 17$$

练习 1 的解法

为了简化计算,我们只需要不断找到能被 17 整除的数字

$$12345 = 123 \cdot 100+45 = (119+4) \cdot 100+45 = 4 \cdot 15+11 = 71 = 3 \bmod 17$$

$$67890 = 68000 - 110 = -110 = 9 \bmod 17$$

$$3 \cdot 9 = 27 = 10 \bmod 17$$

答案是 10。

$$2^{79} = 280-1 = (216)\, 5 \cdot 2^{-1} = 1 \cdot 9 = 9 \bmod 17$$

练习 2

计算

$$(2p)!/p2 \bmod p$$

练习 2 的解法

首先,没有除以p ^{2} 答案显然等于 0

$$(2便士)! = 0 模p$$

我们将使用威尔逊定理

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = -1 \bmod p$$

这意味着

$$(p+1) \cdot (p+2) \cdot (p+3) \cdot \cdots \cdot (2p-1) = -1 \bmod p$$

我们现在只需要注意

$$(p \cdot 2p)/p2 = 1 \cdot 2。$$

那么整个答案是

$$(1 \cdot 2 \cdot \ldots \cdot (p-1)) \cdot 1 \cdot ((p+1) \cdot (p+2) \cdot (p+3) \cdot \ldots \cdot (2p-1)) \cdot 2 = 2 \bmod p$$

练习 3

证明对于任何余数p、q、r以 3、5 和 7 为模，总有整数n使得

$$n = p \bmod 3$$

$$n = q \bmod 5$$

$$n = r \bmod 7$$

练习 3 的解法

这是中国剩余定理的陈述。让我们考虑一下
定理更多。

1. 显然,考虑n模 3 × 5 × 7 = 105就足够了
2. 我们想要显示地图

$$Z105 \to Z3 \times Z5 \times Z7$$

$$n\ 7\!\to (n \bmod 3, n \bmod 5, n \bmod 7)$$

涵盖所有三胞胎。

3. 我们证明两个集合的大小都是105（很明显）
4. 我们证明只有0映射到(0, 0, 0)（很明显）
5. 由于映射是线性的,它是单射的,因此是双射的（有点明显）。

练习 4

绘制一个由残差 mod 7 给出的顶点的有向图：

$$0, 1, 2, 3, ..., 6$$

和边缘由

$$x \mapsto 3x$$

你能从这张图中得出什么结论？

练习 4 的解法

该图是一个循环

$$1 \to 3 \to 2 \to 6 \to 4 \to 5 \to 1$$

加上一个孤立的循环 $0 \to 0$。它遵循

$$3^6 = 1 \text{ 模式 } 7$$

它还遵循 3 的幂生成所有余数 mod 7。

谢谢你

感谢您的关注！