关于费马小定理的课堂笔记

Author 邓力铭
2016.10.14

引论

首先,我们定义这样一种表,大小为$(n-1)*(n-1)(n \in N+)$, 第i行第j列为$(i*j) \bmod n$
当我们通过给定程序打印足够多的表时,我们会发现以下规律:
若给定的数n为素数,那么表中的每一行构成集合$\{x|x \in [1, n-1], x \in N+\}$

推理 (假设给定的数n为素数p)

1.在$(n-1)$行中,我们任意选定第a行.
对于从左到右依次排列的元素,我们有:
$a*1 \equiv b_1 \pmod n$
$a*2 \equiv b_2 \pmod n$
$a*3 \equiv b_3 \pmod n$
...
$a*(p-1) \equiv b_i \pmod n$

2.根据同余性质,我们将各式相乘可得:

$$a^{p-1}*(p-1)! \equiv \prod_{i=1}^{p} b_i \equiv (p-1)! \pmod p$$

3.现考虑p 是否与 $(p-1)!$ 互素
a.分析$(p-1)!$的任意质因数我们可知其一定小于等于$p-1$,所以p除1外与$(p-1)!$没有公因数;
b.综上,p与$(p-1)!$互素

3.所以2所得的同余式等价于:

$$a^{p-1} \equiv 1 \pmod p$$

4.得到了特殊情况下的费马小定理.

费马小定理的一般证明

1. 通过上述推理,当素数p为a的质因数是费马小定理显然成立.
2. 当a与p互素的时候,我们也可利用上述推理过程实现一般性证明.
3. 现给定一个序列和一个集合
   $b_i = (a * i) \bmod p, p\text{为素数}, i \in [1, p-1], i \in N+\}$
   $B = \{x | x \in [1, p-1]\}$
4. 假设两个$i, j \in [1, p-1], i, j \in N+, i \neq j$
   且有

$$a * i \equiv a * j \pmod p$$

   但是,此时a,p互素,所以

$$i \equiv j \pmod p$$

   等价于

$$i = j$$

   与给定条件矛盾.
   5.所以序列b_i中每一项都能在集合B中找到对应元素,且他们互不相等.
   所以我们证明了,表中每一行在引论中的性质,据此,我们即可证明费马小定理.