初等数论三大定理

这篇和算法没什么关系，纯粹是基础知识。

初等数论三大定理，指将整个初等数论框架支撑起来的三个定理，分别是Fermat-Euler（费马欧拉）定理、Wilson（威尔逊）定理和Chinese-Residue（中国剩余）定理。

其中，FE定理说明取模意义下缩系（简化剩余系/缩剩余系）集合的乘法构成群，Wilson定理揭示了模为素数的乘法群的结构，而CR定理阐述了怎样将群和群结合起来，即多素因子模数乘法群的结构问题。

它们三者的本质，都是解释缩系乘法群的结构问题。而研究缩系乘法群的结构，最终结论的形式是：奇素数幂次群结构、2的幂次群结构、CR定理，三个定理作为最终的最高结论。

Fermat-Euler定理

内容

设欧拉函数$\varphi(n)$是0到n-1里与n互素的数（缩剩余系）的个数，即缩系乘法群的阶。对于缩系中任一元素a，有：

$$a^{\varphi(n)}\equiv 1\quad \bmod n$$

特别地，当n是单个素数p的时候，$\varphi(p)$是p-1，即：（费马小定理）

$$a^{p-1}\equiv 1\quad \bmod p$$

这其实是群论里的定理。任意一个群，群里任意一个元素，自乘群的阶次，一定会回到单位元。即：元素的阶整除群的阶。

证明也简单：对缩系所有元素同时进行乘法操作，构成缩系元素的一个置换。（也可以采用群论中陪集的方法）

这个定理在数学题或者算法中，一般用于简化幂次。例如快速幂函数。

推广

将研究对象转移到缩系以外。在完系（完全剩余系）中，任一元素a，有相似结论：

$$a^{t+\varphi\left(\frac{n}{(a^t,n)}\right)}\equiv a^{t}\quad \bmod n$$

对于足够大的整数t成立。意思是，a本身自乘很多次后，也会落入循环中，循环节是n去除a^t与n最大公约数的缩系元素个数的约数。

并且这个足够大的t，一般要求a与n重合的那部分素因数被“ 消除 ”干净了，即a^t这部分素因数的幂次已经达到或超过了n中的相应幂次。

这个证明是显然的，分素因数讨论即可。

由于欧拉函数的积性，循环节显然是$\varphi(n)$的约数。因此弱化一下就是这样：

$$a^{t+\varphi\left(n\right)}\equiv a^{t}\quad \bmod n$$

这个更方便理解和使用。

Wilson定理

内容

对于任一素数p，1到p-1的乘积，模p余-1。即：

$$(p-1)!\equiv -1\quad \bmod p$$

或写为比较常见（方便使用）的形式：

$$(n-2)!\equiv \begin{cases}1\quad \bmod n&n\ is\ prime\\0\quad \bmod n&others\end{cases}$$

等价条件，显然可以用于判定素数，像费马小定理都还有无数个特例存在。但是由于阶乘太大了，且判断余数没有速算法，导致时间复杂度比正常因数分解还要高，所以没人选择这么做。

既然要研究缩系乘法群，那么缩系所有元素乘积自然很重要，Wilson定理说明它是-1。

证明也特别简单：数论倒数两两配对即可。只有两个无法配对的数，1和-1，因此最终结果是-1。

这个定理常用于解决剩余问题，在算法中基本不会遇到。

推广

模不是素数的时候，缩系中所有元素的乘积如何？

对于奇素数的幂次：

$$\prod\limits_{(a,p)=1}a\equiv (-1)\quad \bmod p^t$$

对于2的幂次：4以下仍然是-1，但是8以上全是1。

对于一般的整数n，情形如何？只要8不整除n，结论仍然会是-1。当8整除n的时候，情形就非常复杂了，这需要借助中国剩余定理。

设2在n中的幂次为v，下面的不定方程有整数解x和y，

$$\frac{n}{2^v}x-2^vy=1$$

那么最终结果为：

$$\prod\limits_{(a,n)=1}a\equiv \begin{cases}\frac{n}{2^v}x+2^vy=1+2^{v+1}y\quad \bmod n&n \equiv 0 \bmod 8\\-1\quad \bmod n&others\end{cases}$$

中国剩余定理

很简单，不同素因子幂乘起来，对应于缩系乘法群的笛卡尔积。因此缩系乘法群的总体构成一个空间，各

个素因子的缩系乘法群互不相干，分别构成相应的维度。

当已知这个数在各个维度的坐标，想求这个数的时候，利用线性代数的知识，先求各个维度上的单位向量，然后向量点乘即可。

单位向量的求法，就是一次不定方程。

模为奇素数幂的缩系乘法群的结构

构成循环群。生成元叫做原根。

不止这类模有原根，事实上1、2、4、奇素数的幂、2倍奇素数的幂都有，也就是说这些缩系乘法群也是循环群，而其余的模都没有。

模为2的幂的缩系乘法群的结构

是循环群与{-1,1}乘法群的笛卡尔积。