质数的余环以及基于石头数的整数分解法

左洪盛

April 5, 2012

1 质数的九

1.1 余数相邻关系的唯一性

余数相邻关系是指通过特定的乘积运算并对质数求余得到的余数序列。设质数p，整数$y < p$，n是任意大于0的整数，$y_1 \equiv y \times n \pmod p$，则$y$的右邻数$y_1$是唯一的；同理，$y_2 \times n \equiv y \pmod p$，则$y$的左邻数$y_2$也是唯一的，因此可得余数的相邻关系唯一性。

1.2 余环

设整数$t \geq 0$，p为质数(如未特别指明，本文之字符p均代表质数)，考察如下计算：

$$y_0 = t \times 10^0 \% p，y_1 = t \times 10^1 \% p，\cdots，y_n = t \times 10^n \% p，\cdots$$

y_0，y_1，$\cdots$，y_n都小于p，组成一个有限集合。另外，

$$y_1 = y_0 \times 10 \% p，\ y_2 = y_1 \times 10 \% p，\cdots$$

所以y_0，y_1，$\cdots$，y_n的部分相邻关系为：y_0-y_1-$\cdots$-y_n，其中只有y_0的左邻数和y_n的右邻数没有确定。根据相邻关系的唯一性，y_0的左邻数只能是y_n，y_n的右邻数只能是y_0，即这个余数序列是一个封闭的构造，这种构造为余环。

1.3 质数的九

上面的分析可知，$y_{n+1} \equiv y_0 \pmod p$，令$t = n+1$，所以有$10^t \equiv 1 \pmod p$。定义符号九，令九 $= 10^t - 1$，表示能被质数p整除的长度最短的一串9。对于任意质数P，存在对应的九，使下面的等式成立：

$$九 = P \cdot Ⓢ \tag{1.1}$$

其中Ⓢ叫做质数P的商数，九的长度用符号$\bar{九}$表示,显然，

$$10^{\underline{九}} \equiv 1 \pmod p \tag{1.2}$$

2 余环长度

2.1 质数的余环长度

定义 2.1 称包含余数1的余环为主余环，用(1)表示。

定理 2.1 若余数$y \in (1)$，则$y \cdot (1) = (1)$。

证：$y \in (1)$，则有$y \equiv 10^t \pmod p$，设y'是(1)中的任意余数，$y' \equiv 10^{t'} \pmod p$；则$y \cdot y' \equiv 10^{t+t'} \pmod p$，得证。

定理 2.2 若余数$y \notin (1)$,$y \cdot (1) \neq (1)$

证：设y'是(1)中的任意余数，$y \equiv 10^{t'} \pmod p$，则$y \cdot y' \equiv y \cdot 10^{t'} \pmod p$，假如，$y \cdot y' \% p \in (1)$成立，则$y \cdot y' \equiv y \cdot 10^{t'} \equiv 10^t \pmod p$，从而有$y \equiv 10^{t-t'} \pmod p$，与$y \notin (1)$矛盾，得证。

定理 2.3 质数p的所有余环的长度相等，等于$\underline{九}$。

证：根据1.3可知，(1)的长度等于$\underline{九}$。设$y \in (1)$，由2.1可知$y \cdot (1)$可得到一个不同于(1)的余环(y)，表示如下：

$$y \cdot (1) = (y) \tag{2.1}$$

设$y_1, y_2 \in (1)$，$y_1 \not\equiv y_2 \pmod p$，所以，$y \cdot y_1 \not\equiv y \cdot y_2 \pmod p$。由2.1, $y \cdot y_1, y \cdot y_2 \in y$，因此$y \cdot (1)$得到的$\underline{九}$个余数相互不同于，所以(y)的长度和(1)的长度相等，等于$\underline{九}$。

质数p共有$p-1$个余数，分布于多个长度相等的余环中，因此，$\underline{九} \mid (p-1)$。设X表示p的余环个数，则,

$$p - 1 = \underline{九} \cdot X \tag{2.2}$$

2.2 质数乘方的余环长度

设p^t对应$\overline{九}_{p^t}$，$y = Ⓢ\% p^t$，如果$y = 0$，则$\overline{九}_{p^{t+1}} = \overline{九}_{p^t}$；如果$y \neq 0$，则$\overline{九}_{p^{t+1}} = \overline{九}_{p^t} \cdot p$

3 余环间关系

3.1 余环的阶

约定$(y)_1 \cdot (y)_2$表示任意$y_1 \in (y)_1$,$y_2 \in (y)_2$的乘积对质数p求余所得的余数集合。

定理 3.1 设两个余环，$(y)_1 \neq (1)$,$(y)_2 \neq (1)$，则$(y)_1 \cdot (y)_2$是一个余环，并且$(y)_1 \cdot (y)_2 \neq (y)_1 \neq (y)_2$成立。

证：任意$y_{11}, y_{12} \in (y)_1$,$y_{12} \equiv y_{11} \cdot 10^{t_1} \pmod p$, $y_{21}, y_{22} \in (y)_2$，$y_{22} \equiv y_{21} \cdot 10^{t_2} \pmod p$, 则,$y_{12} \cdot y_{22} \equiv y_{11} \cdot 10^{t_1} \cdot y_{21} \cdot 10^{t_2} \equiv y_{11} \cdot y_{22} \cdot 10^{t_1+t_2} \pmod p$，得证。

任意$y_1 \in (y)_1$,$y_2 \in (y)_2$，若结论不成立，假设$(y)_1 \cdot (y)_2 = (y)_1$,则: $y_1 \cdot y_2 \equiv y_1 \cdot 10^t \pmod p$，即，$y_2 \equiv 10^t \pmod p$成立，和$(y)_2 \neq (1)$矛盾。得证。

定理 3.2 对于质数p的任意一个余环(y)，必存在整数$t \leq X$，使$(y)^t = (1)$成立

证：由3.1，设$(y) \neq (1)$，则：$(y)^2 \neq (y)$ 若$(y)^2 \neq (1)$,则$(y)^3 \neq (y)^2 \neq (y)$ 若$(y)^3 \neq (1)$,则$(y)^4 \neq (y)^3 \neq (y)^2 \neq (y)$ $\cdots$因为余环最多有X个，所以必有$t \leq X$，使$(y)^t = (1)$成立。满足等式的最小t称为余环的阶,用符号$\overline{(y)}$表示。

3.2 任意正整数的欧拉表示

x表示任意正整数。

定理 3.3 对于任意正整数$d < x$,存在正整数a, b，$a \mid x$,$(a, b) = 1$，$b < a < x$,使等式$d = \frac{x}{a} \cdot b$成立。

证：令$m = (d, x)$，$a = \frac{x}{m}$,显然a是小于x的整数。令$b = \frac{d}{m}$，显然，b是小于d的整数，且有$b < a$。$d = (d, x) \cdot \frac{d}{(d,x)} = m \cdot b = \frac{x}{a} \cdot b$，得证。

定理 3.4 小于x，和x的最大公约数等于m的数共有$\varphi(\frac{x}{m})$个，φ为欧拉函数。

证：设$d_1, d_2, \ldots, d_t$是所有小于x，和x的最大公约数等于m的数，则：$d_1 = \frac{x}{a} \cdot b_1$,$d_2 = \frac{x}{a} \cdot b_2$,$\cdots$,$d_t = \frac{x}{a} \cdot b_t$。根据3.2,可知$b_1, b_2, \ldots, b_t$是和$a$互质的$t$个数，所以$t = \varphi(a) = \varphi(\frac{x}{m})$。

定义 3.1 同约集合m为：若$d \in m$则$(d, x) = m$。由3.2，集合的长度等于对应最大公约数的欧拉函数值

显然，对于任意$d, 1 \leq d \leq x$，一定属于且只能属于一个m。因此1到x分属于多个同约集合，可得公式：

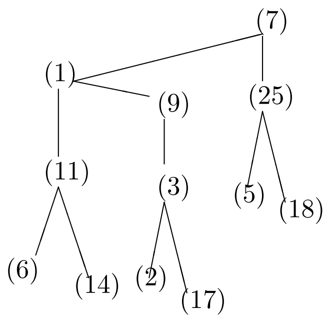
$$x = \sum_{m|x} \varphi(m) \tag{3.1}$$

3.3 同阶余环的数目

设(y)的阶数等于T，设$k < T$，并且$(k, T) = 1$，$(y)_k = (y)^k$，易证，$(y)_k$的阶数也等于T；因此至少有$\varphi(T)$个余环的阶数等于T。
根据公式3.2，如果m_1阶的余环的个数大于$\varphi(m_1)$，则必会导致另外一个m_2阶的余环个数小于$\varphi(m_2)$。综上得，阶数等于T的余环的个数等于$\varphi(T)$。

3.4 余环归枝图

余环归枝图是表示余环的乘法运算环境中的余环位置关系的立体图。图中节点代表余环，连线代表一个幂次为X的质因子的幂运算。例如：下图是质数271对应的归枝图



3.5 原根在归枝图中的分布

原根是 ，原根所在余环的阶数等于X，关于原根的分布有如下表达式：

$$\varphi(p-1) = \varphi(X) \cdot \varphi(\overline{\text{九}}) \cdot \frac{(X, \overline{\text{九}})}{\varphi((X, \overline{\text{九}}))} \tag{3.2}$$

$\varphi(X)$：表示底层余环(阶等于X)的余环个数

4 石头数

4.1 石头数及其计算

定义 4.1 本征质数——质数p对应九，则称p是九的本征质数。

定义 4.2 本征幂数——质数的乘方p^t对应九，则称p^t是九的本征幂数。

定理 4.1 A、B是大于1的并且个位是1、3、7、9的整数，如果数A整除B，则A对应的九能整除B对应的九，表示为:

$$A \mid B \Rightarrow \text{九}_A \mid \text{九}_B \text{或} \overline{\text{九}_A} \mid \overline{\text{九}_B} \tag{4.1}$$

定理 4.2 定义如下公式：

$$S = \frac{I}{3^m \cdot \prod_{i|\overline{九},1<i<\overline{九}} S_i} \tag{4.2}$$

其中$\overline{九} > 1, I = 九/9$, $3|\overline{九}$时$m = \frac{\overline{九}}{3}$, $3 \not| \overline{九}$时$m = 0$；式中S_i也是满足上式的S。则，S一定是整数，我们称S是九的石头数。

证： I的质因子分解表示为：$I = \prod p^i$, 其中p是质数,$i \geq 1$; 质因子可以分为三种情况：$t = 1$,$t > 1$并且$p^t \mid 九$,$t > 1$并且$p^t \not| 九$，下面对三种情况分别讨论。

当$p \mid 九$, $p^2 \not| 九$时, 由定理4.1，$九_{[p]} \mid 九$。如果$九_{[p]} \neq 九$，则$p \mid S_i$, S_i是$九_{[p]}$对应的石头数；又, 由$p \mid 九$得$p \mid I$; 因此 $p \not| S$ 。 如果$九_{[p]} = 九$, 则p不能整除公式的分母，必有$p \mid S$。因此可知九的本征质数都能整除S，不属于九的本征质数不都能整除S。

当$t > 1, p^t \mid 九$时, 如果p^t是九的本征幂数, 倘若p同时也是九的本征质数, 则p的任意次方都不能整除$\prod_{i|\overline{九}} S_i$, 从而使$p^t \mid S$；倘若$p$是$九_i, i \in A$的本征质数,$p^2$是$九_j, j \in A$的本征幂数,等等,有$t_1 < t$,使$p^{t_1} \mid \prod_{i|\overline{九}} S_i$，进而使$p^{t-t_1} \mid S$。因此可知，$p^t$是九的本征幂数时，有$p^{t'} \mid S, t' \leq t$。 如果$p^t$不是九的本征幂数,

集合A=$\{p^1, p^2, p^3, \ldots, p^t\}$对应B=$\{九_{[}p], 九_{[}p^2], 九_{[}p^3], \ldots, 九_{[}p^t]\}$,由B通过公式得到对应的C=$\{S_{[}p], S_{[}p^2], S_{[}p^3], \ldots, S_{[}p^t]\}$。B和C总是一一对应的，一般A和B是一一对应的，但有时会有多对一的关系，比如$p = 487$时,$九_{[}p] = 九_{[}p^2] = 486$。 当AC一一对应时，如果t=2, $p \mid S_{[}p]$, 由公式得$p \mid S_{[}p^2]$; 如果t=3, $p \mid S_{[}p]$, 由公式得$p \mid S_{[}p^2]$,以及$p \mid S_{[}p^3]$;等等；总之，p整除C中的所有石头数. 并且

$$p^t \mid \prod_{S \in C} S \tag{4.3}$$

当AC多对一对应时，假设$p^m \to S_{[}p^{m+1}]$, $p^{m+1} \to S_{[}p^{m+1}]$,则$p^2 \mid S_{[}p^{m+1}]$; 即，如果两个幂运算映射到一个石头数，则这个石头数可以被质数的平方整数，以此类推，可知映射关系数等于整除石头数的质数乘方的幂数。所以，多对一映射时，上式仍然成立。

定理 4.3 若$九_1$整除$九_2$，则$九_1$的石头数能整除$九_2$。