质数的余环以及基于石头数的整数分解法

左洪盛

April 13, 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固定整数求余得到的余数序列。设整数N，整数$y < p$， n是任意大于0的整数，$y_1 \equiv y \times n \pmod N$，则$y$的右邻数$y_1$是唯一的；同理，$y_2 \times n \equiv y \pmod N$，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$t \geq 1$，N为个位是1,3,7,9的整数,

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

y_0，y_1，$\cdots$，y_n都小于N，组成一个有限集合。显然，

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

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：

$$\text{九} = P \cdot \text{Ⓢ} \tag{1.1}$$

其中Ⓢ叫做质数P的商数，九的长度用符号$\bar{\text{九}}$表示,显然，

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

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

定理 2.4 设p^t对应九$_{[p^t]}$，即九$_{[p^t]}$是能被p^t整除的长度最短的一串9，$\textcircled{S} = 九_{[p^t]}/p$, $y = \textcircled{S} \% p^t$，如果$y = 0$，则$\overline{九_{[p^{t+1}]}} = \overline{九_{[p^t]}}$；如果$y \neq 0$，则$\overline{九_{[p^{t+1}]}} = \overline{九_{[p^t]}} \cdot p$

证：当$y = 0$时，结论显然成立,
当$y \neq 0$时，$\{y \cdot 10^{\overline{九_{[p^t]}}} + \textcircled{S}\} \equiv 2y \pmod p$，$\{2y \cdot 10^{\overline{九_{[p^t]}}} + \textcircled{S}\} \equiv 3y \pmod p$,
…，$\{(y \cdot (p-1)) \cdot 10^{\overline{九_{[p^t]}}} + \textcircled{S}\} \equiv p \cdot y \pmod p$，得证。

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$(y)^4 \neq (y)^3 \neq (y)^2 \neq (y)$ …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： $d_1 = \frac{x}{a} \cdot b_1$,$d_2 = \frac{x}{a} \cdot b_2$,…,$d_t = \frac{x}{a} \cdot b_t$。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：

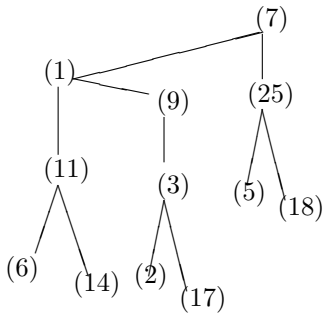
$$x = \sum_{m \mid x} \varphi(m) \tag{3.1}$$

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：

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

$\varphi(X)$：表示底层余环(阶等于X)的余环个数

4 基于石头数的整数分解法

4.1 石头数及其计算

定义 4.1 本征质数——根据1.3，任意质数p都有对应的九，称p是九的本征质数。

定义 4.2 本征积——九的所有本征质数的乘积,用符号R表示。

定义 4.3 本征幂数——质数的乘方p^t有对应的九（即九是能被p^t整除的长度最短的一串9），称p^t是九的本征幂数。

如果$p^t = 九$,则必有$p = 3$,除了$九 = 2$, 不知是否有更大的九满足此式。

定义 4.4 本征幂余——p^t是九的本征幂数，t'是使得$九_{[p^{t'}]} \neq 九_{[p^t]}$的小于$t$的最大整数，则$p^{t-t'}$为九的本征幂余,用符号$V$表示。

对于$3^3 = 9$,不存在t',所以$V_1 = 1$; 并且$R_1 = 3$。

定理 4.1 幂数集合$A = \{p^2, p^3, \ldots, p^t\}$，对应的九集合$B = \{九_{[p^2]}, 九_{[p^3]}, \ldots, 九_{[p^t]}\}$, 对应的本征幂余$C = \{V_{[p^2]}, V_{[p^3]}, \ldots, V_{[p^t]}\}$；则

$$\prod_{i=2}^{t} V_{[p^i]} = p^{t-1}$$

。

证：$\prod_{i=2}^{t} V_{[p^i]} = p^{t-t'} \cdot p^{t'-t''} \ldots p^{t-1} = p^{t-1}$

定义 4.5 石头数——九的所有本征质数和本征幂余的乘积，称作九的石头数，用符号S表示，$S = B \cdot V$。

定理 4.2 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:

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

定理 4.3

$$S = \frac{I}{\prod\limits_{m \mid \overline{九}, m < \overline{九}} S_m} \tag{4.2}$$

证：

$$I = \prod_i p_i^{t_i} = \prod_i p_i \cdot \prod_i p_i^{t_i - 1}$$

前半部分代表I的所有质因子的乘积，后半部分表示其余乘积; 根据定理4.1, 如果$p_i \mid I$则$I_{[p_i]} \mid I$, 进而有$R_{[p_i]} \mid I$，所以：

$$\prod_i p_i = \prod_{m \mid \overline{九}} R_m$$

根据定理4.1以及4.1可知，

$$\prod_i p_i^{t_i - 1} = \prod_{m \mid \overline{九}} V_m$$

所以，

$$I = \prod_{m \mid \overline{九}} (R_m \cdot V_m) = \prod_{m \mid \overline{九}} S_m$$

由上式变形即得公式。

4.2 石头数的分解

我们的目的是得到石头数包含的所有本征质数。　对于石头数S,对应九,如果p是九的本征质数，根据公式??得$\overline{九} \mid (p-1)$，所以，设$n = k \cdot \overline{九} + 1, k \geq 1$,用$n$试除$S$，并滤除本征质数的乘积，就能得到的所有的本征质数。

stone_son.py是基于此算法的计算机程序,程序利用了多进程技术，对n的无效取值进行了过滤，能够限定n的最大值。

4.3 基于石头数的整数分解法

根据本文前面探讨的各种结果，特别是石头数，可以形成个位是1,3,7,9的整数的分解方法：

1.求整数N的$\overline{九_{[}N]}$,方法有两种，详见-

2.分解$\overline{九_{[}N]}$,得其因子集合A。

3.以A中数据作为九的长度,求其对应的石头数;得到石头数集合B。

4.对B中所有石头数，求其对应的所以本征质数; 得到本征质数集合C。

5.用C中的所有本征质数试除N,得到N的质因子。

5 一种基于九的整数筛法

5.1 合数的余环群

默认合数个位等于1,3,7,9，设合数$N = \prod_i p_i$,对应$\overline{九_{[}N]} = lcm(\overline{九_{[}p_1]}, \overline{九_{[}p_2]}, \ldots, \overline{九_{[}p_t]})$。考察余环乘法：$(p_i) = (1) \cdot p_i, p_i \mid N$, 设$y \in (1), y \cdot p_i \% N = p_i \cdot y \%(N/p_i)$, 所以$len[(p_i)] = lcm(\overline{九_{[}p_1]}, \overline{九_{[}p_2]}, \ldots, \overline{九_{[}p_{i-1}]}, \overline{九_{[}p_{i+1}]}, \ldots, \overline{九_{[}p_t]}$,

定理 5.1 任意个位等于1,3,7,9的合数$N = p_1 \cdot p_2 \ldots \cdot p_t$, N的同余余环共有$\sum_i p_i$个余数。

证：同余余环是

5.2 一种整数的筛法

定理 5.2 任意个位等于1,3,7,9的整数，$\overline{九_{[}N]}$是N对应的九的长度，如果$\overline{九_{[}N]} \mid (N-1)$，则N是：

1. 质数
2. 本征积
3. 具有如下性质的合数：$N = p_1 \cdot p_2 \ldots p_t$,

$$\overline{九} \mid \sum_i (p_i - 1), \text{其中} p_i \text{是} N \text{的质因子}$$

证：