数学新星网 ※ 学生专栏
www.nsmath.cn/xszl

# 一次完整多项式

任建宇

(合肥市第一中学, 230601)

在 2018 年上海新星数学夏令营中, 冯跃峰老师提出了如下"完整多项式"问题:

**问题** 设 $f(x)$ 为多项式, 如果对给定的正整数 $n$, 存在 $x_0 \in \mathbb{N}$ 使

$$f(x_0), f^{(2)}(x_0), \cdots, f^{(n)}(x_0)$$

构成模 $n$ 的完系, 则称 $f(x)$ 为模 $n$ 的完整多项式. 试问: 对给定的正整数 $n$, 哪些多项式 $f(x)$ 是模 $n$ 的完整多项式?

这是一个容量很大的问题. 本文解决了一次完整多项式的情形, 得到如下定理:

**定理** 对给定正整数 $n \geq 4$, 设 $n$ 的标准分解式为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, 则 $f(x) = ax + b (a, b \in \mathbb{N}^*)$ 是模 $n$ 的完整多项式当且仅当 $(b, n) = 1$, 且

$$\begin{cases} a \equiv 1 \, (\mathrm{mod} p_1 p_2 \cdots p_r), \text{ 若 } 4 \nmid n \\ a \equiv 1 \, (\mathrm{mod} 2 p_1 p_2 \cdots p_r), \text{ 若 } 4 | n \end{cases}.$$

**证明** 原题等价于: 对给定的正整数 $n \geq 4$, 求所有正整数对 $(a, b)$, 使存在 $m \in \mathbb{N}$, 数列 $\{x_k \mid x_1 = m, x_l = a x_{l-1} + b, \, l \geq 2\}$ 的前 $n$ 项构成模 $n$ 的完系.

当 $a = 1$ 时, 问题等价于存在 $m \in \{1, 2, \cdots, n\}$, 使 $m+b, m+2b, \cdots, m+nb$ 构成模 $n$ 的完系, 这又等价于 $(b, n) = 1$, 所以结论成立.

当 $a \geq 2$ 时, 易知若正整数对 $(a, b)$ 满足上述条件, 则必有 $(a, n) = 1$ (否则 , $(a, n) = d > 1$, 则 $\{x_k\}$ 中除第一项外都在模 $d$ 余 $b$ 的剩余类中, 不可能构成模 $n$ 的完系), 故以下证明中均假设 $(a, n) = 1$.

我们熟知 $(a, n) = 1$ 时, $\{x_k\}$ 关于 $n$ 的模数列是纯周期数列, 故存在 $m \in \mathbb{N}$,

修订日期: **2019-05-09.**

数列 $\{x_k \mid x_1 = m, x_n = ax_{n-1} + b\}$ 的前 $n$ 项构成模 $n$ 的完系等价于数列 $\{x_k \mid x_1 = 1, x_l = ax_{l-1} + b,\ l \geq 2\}$ 的前 $n$ 项构成模 $n$ 的完系.

下面先考虑 $b = 1$ 的情形, 此时问题转化为求所有正整数 $a$, 使得

$$\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^n-1}{a-1}$$

模 $n$ 互不同余.

① $n = p, p$ 为素数.

此时若正整数 $a$ 满足上述条件, 则有

$$p \nmid \frac{a^j-1}{a-1} - \frac{a^i-1}{a-1}, \forall 1 \leq i < j \leq p,$$

结合 $(a, p) = (a, n) = 1$, 有

$$p \nmid \frac{a^{j-i}-1}{a-1}, \forall 1 \leq i < j \leq p.$$

又 $\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^p-1}{a-1}$ 模 $n$ 互不同余, 则只能有 $p \mid \frac{a^p-1}{a-1}$.

若 $a \not\equiv 1 \pmod{p}$, 则 $p \mid a^p - 1, a \equiv a^p \equiv 1 \pmod{p}$, 矛盾!

若 $a \equiv 1 \pmod{p}$, 则易验证其满足要求.

综上, 此时正整数 $a$ 满足条件当且仅当 $a \equiv 1 \pmod{p}$.

② $n = p^\alpha, p$ 为素数, $\alpha \geq 2$.

对素数 $p$, 正整数 $m$, 若 $p^k \mid m, p^{k+1} \nmid m$, 则记为 $v_p(m) = k$. 由定义易知 $m_2 \mid m_1$ 时,

$$v_p\left(\frac{m_1}{m_2}\right) = v_p(m_1) - v_p(m_2).$$

(1) $p$ 为奇素数时.

若 $a \not\equiv 1 \pmod{p}$, 则由 ① 知 $\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^p-1}{a-1}$ 无法构成模 $p$ 的完系, 更不可能构成模 $p^\alpha$ 的完系.

若 $a \equiv 1 \pmod{p}$, 由著名的升幂定理 (即 LTE 引理), 知

$$\begin{aligned} v_p\left(\frac{a^k-1}{a-1}\right) &= v_p\left(a^k-1\right) - v_p(a-1) \\ &= v_p(a-1) + v_p(k) - v_p(a-1) \\ &= v_p(k), \end{aligned}$$

也即 $p^\alpha \mid \frac{a^k-1}{a-1}$ 当且仅当 $p^\alpha \mid k$.

故若存在 $1 \leq i < j \leq p^\alpha, p^\alpha \mid \frac{a^j-1}{a-1} - \frac{a^i-1}{a-1}$, 则 $p^\alpha \mid \frac{a^{j-i}-1}{a-1}$, 于是 $p^\alpha \mid j - i$, 与 $j - i \leq p^\alpha - 1$ 矛盾! 从而

$$\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \ldots, \frac{a^{p^\alpha}-1}{a-1}$$

模 $p^\alpha$ 互不同余.

(2) $p=2$ 时.

由 $(a,2^\alpha)=1$ 知 $a$ 为奇数.

若 $a\equiv 3\pmod 4$, 则

$$v_2\left(\frac{a^{2^{\alpha-1}}-1}{a-1}\right)=v_2\left(a^{2^{\alpha-1}}-1\right)-v_2(a-1)=\sum_{i=0}^{\alpha-2}v_2\left(a^{2^i}+1\right)\geq\alpha.$$

于是 $2^\alpha\mid\frac{a^{2^{\alpha-1}}-1}{a-1}$, 则 $2^\alpha\mid\frac{a^{2^{\alpha-1}+1}-1}{a-1}-\frac{a-1}{a-1}$,

$$\frac{a-1}{a-1},\frac{a^2-1}{a-1},\cdots,\frac{a^{2^\alpha}-1}{a-1}$$

中有模 $2^\alpha$ 同余的两项, 不符题意.

若 $a\equiv 1\pmod 4$, 则 $k$ 为奇数时,

$$v_2\left(a^k-1\right)=v_2(a-1)+v_2\left(1+a+\cdots+a^{k-1}\right).$$

而 $1+a+\cdots+a^{k-1}$ 是奇数个奇数相加, 是一个奇数, 故

$$v_2\left(1+a+\cdots+a^{k-1}\right)=0,$$

即 $v_2\left(a^k-1\right)=v_2(a-1)$. 又

$$v_2\left(a^2-1\right)=v_2(a-1)+v_2(a+1)=v_2(a-1)+1,$$

由数学归纳法可知

$$v_2\left(a^m-1\right)=v_2(a-1)+v_2(m),\forall m\in\mathbb{N}^+.$$

于是同 $p$ 为奇素数的情况可知, 此时

$$\frac{a-1}{a-1},\frac{a^2-1}{a-1},\cdots,\frac{a^{2^\alpha}-1}{a-1}$$

模 $2^\alpha$ 互不同余.

综上, 此时 $a$ 满足要求当且仅当

$$\begin{cases}a\equiv 1\pmod p, p\text{ 为奇素数}\\ a\equiv 1\pmod 4,\ p=2\end{cases}.$$

③ $n$ 的标准分解式为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$.

由①②可知若 $a$ 不满足

$$\begin{cases}a\equiv 1\pmod{p_1p_2\cdots p_r},\text{ 若 }4\nmid n\\ a\equiv 1\pmod{2p_1p_2\cdots p_r},\text{ 若 }4\mid n\end{cases}.$$

且存在 $1\leq i<j\leq n, n\mid\frac{a^j-1}{a-1}-\frac{a^i-1}{a-1}$, 则

$$\forall p_i\in\{p_1,p_2,\cdots,p_r\},p_i^{\alpha_i}\mid\frac{a^{j-i}-1}{a-1},$$

又可知此时

$$\begin{cases} a \equiv 1 \pmod{p_i}, p_i \text{ 为奇素数} \\ a \equiv 1 \pmod{4},\ p_i = 2 \end{cases}.$$

有 $p_i^{\alpha_i} \mid j-i$. 从而 $n \mid j-i$, 与 $1 \le j-i \le n-1$ 矛盾!

故此时

$$\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \cdots, \frac{a^n-1}{a-1}$$

模 $n$ 互不同余, 满足条件.

下面考虑一般情形. 易知数列 $\{x_k \mid x_1 = 1, x_l = ax_{l-1} + b,\ l \ge 2\}$ 的前 $n$ 项即为

$$1, a+b, \cdots, a^{n-1} + b\frac{a^{n-1}-1}{a-1}.$$

由条件可知其中任意两项模 $n$ 不同余, 也即

$$\forall 1 \le i < j \le n, a^{i-1} + b\frac{a^{i-1}-1}{a-1} \not\equiv a^{j-1} + b\frac{a^{j-1}-1}{a-1} \pmod{n},$$

即

$$\forall 1 \le i < j \le n, (a-1+b)\frac{a^{j-i}-1}{a-1} \not\equiv 0 \pmod{n}.$$

这首先要求 $\forall 1 \le i < j \le n, \frac{a^{j-i}-1}{a-1} \not\equiv 0 \pmod{n}$, 即

$$\begin{cases} a \equiv 1 \pmod{p_1 p_2 \cdots p_r}, \text{ 若 } 4 \nmid n \\ a \equiv 1 \pmod{2p_1 p_2 \cdots p_r}, \text{ 若 } 4 \mid n \end{cases}.$$

且若 $(b, n) > 1$, 设 $p_k \in \{p_1, p_2, \cdots, p_r\}$, $p_k \mid (b, n)$, 则 $p_k \mid a-1+b$. 又此时

$$\frac{a-1}{a-1}, \frac{a^2-1}{a-1}, \cdots, \frac{a^n-1}{a-1}$$

模 $n$ 互不同余, 故存在 $1 \le s \le n-1$, 使 $p_k^{\alpha_k - 1} \mid \frac{a^s-1}{a-1}$. 取 $j-i = s$, 则有

$$(a-1+b)\frac{a^{j-i}-1}{a-1} \equiv 0 \pmod{n},$$

不符合要求.

而若 $(b, n) = 1$, 则此时 $(a-1+b, n) = 1$, 且

$$\forall 1 \le i < j \le n, \frac{a^{j-i}-1}{a-1} \not\equiv 0 \pmod{n}.$$

故

$$\forall 1 \le i < j \le n, (a-1+b)\frac{a^{j-i}-1}{a-1} \not\equiv 0 \pmod{n},$$

符合要求.

综上, 对给定的正整数 $n \ge 4$, 记 $n$ 的标准分解式 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, 则

$f(x)=ax+b(a,b\in\mathbb{N}^*)$ 是模 $n$ 的完整多项式当且仅当 $(b,n)=1$, 且

$$\begin{cases} a\equiv 1\,(\mathrm{mod}p_1p_2\cdots p_r)\,, \text{ 若 } 4\nmid n \\ a\equiv 1\,(\mathrm{mod}2p_1p_2\cdots p_r)\,, \text{ 若 } 4|n \end{cases}.$$

**注** $n=2$ 时, $f(x)=ax+b(a,b\in\mathbb{N}^*)$ 是完整多项式当且仅当 $a\equiv 0\pmod 2$ 或 $b\equiv 1\pmod 2$.

$n=3$ 时, $f(x)=ax+b(a,b\in\mathbb{N}^*)$ 是完整多项式当且仅当 $a\equiv 1\pmod 3$ 且 $b\not\equiv 0\pmod 3$.

**致谢** 本文得到了冯跃峰老师的支持与指导.