arXiv:2303.12523v1 [math.HO] 4 Jan 2023

关于多项式不变性的一项 Granville 结果的变体

Labib Haddad and Charles Helou

Abstract

2004年，Andrew Granville 证明了如下结论：关于变量 x, y, z 的多项式，在映射 $\varphi: z \to -(x+y+z)$ 下保持不变，当且仅当它是 $b = z(x+y+z)$ 的多项式。下面我们简要叙述其来历，随后给出这一主题的一个变体。

History

2004年3月，第二作者收到一位同事的询问，内容涉及两个或三个变量中含幂单项式的某些对称多项式的因式分解。当时有一个关于多项式$F_p(x,y) = (x+y)^p - x^p - y^p$在 $\mathbb{Z}[x,y]$ 中的因式分解的陈述，其中 $p > 3$为素数，具体如下：

$$F_p(x,y) = pxy(x+y)\left(x^2+xy+y^2\right)^e C_p(x,y),$$

其中，根据 $p \equiv -1$ 是 1 (mod 6) 还是 1， $e = 1$ 分别为 1 或 2；而 $C_p(x,y) \in \mathbb{Z}[x,y]$ 是所谓的柯西多项式，被描述为一个众所周知的初等结果。事实上， $F_p(x,y)$ 是一个次数为 p 的齐次多项式，除以 y^p 后得到关于 $t = \frac{x}{y}$ 的次数为 $p-1$ 的多项式 $K_p(t)$，即

$$\frac{F_p(x,y)}{y^p} = \left(\frac{x}{y}+1\right)^p - \left(\frac{x}{y}\right)^p - 1 = (t+1)^p - t^p - 1 = \sum_{k=1}^{p-1}\binom{p}{k}t^k = K_p(t).$$

显然， $K_p(0) = K_p(-1) = 0$ 且 $K_p'(0) = p$, $K_p'(-1) = -p \neq 0$, 因此 0 和 1 是 K_p 的单根，所以 K_p 在 $\mathbb{Z}[t]$ 中可被 $t(t+1)$ 整除，也可被 p 整除，因为当 $1 \le k \le p-1$ 时，二项式系数 $\binom{p}{k}$ 可被 p 整除。此外，令 $\zeta_3 = \exp\left(\frac{2i\pi}{3}\right)$ 为本原三次单位根，我们有

$$K_p(\zeta_3) = (\zeta_3+1)^p - \zeta_3^p - 1 = -(1+\zeta_3^p+\zeta_3^{2p}) = 0$$

and

$$K_p'(\zeta_3) = p((\zeta_3+1)^{p-1} - \zeta_3^{p-1}) = p\zeta_3^{p-1}(\zeta_3^{p-1}-1),$$

由 $\mathcal{AMS}$-TEX排版

因此， $K_p'(\zeta_3) = 0$ 当且仅当 $p \equiv 1 \pmod 3$，即 $p \equiv 1 \pmod 6$。所以 ζ_3 是 $K_p(t)$ 的根，并且当且仅当 $p \equiv 1 \pmod 6$ 时它是一个二重根；也就是说，若 $p \equiv -1 \pmod 6$，则 $K_p(t)$ 可被 t^2+t+1 整除；若 $p \equiv 1 \pmod 6$，则在 $\mathbb{Z}[t]$ 中可被 $(t^2+t+1)^2$ 整除。因此

$$K_p(t) = pt(t+1)(t^2+t+1)^e C_p(t),$$

其中

$$e = \begin{cases} 1, & \text{if } p \equiv -1 \pmod 6 \\ 2, & \text{if } p \equiv 1 \pmod 6, \end{cases}$$

而 $C_p(t) \in \mathbb{Z}[t]$（次数为 $p-3-2e$）称为柯西多项式，因为它由 A. L. Cauchy 于 1839年引入，并于 1841年 重新探讨（[2, 3, 5]）。D. Mirimanoff 于 1903年 研究了柯西多项式（[4]），并猜想它们在 $\mathbb{Q}$ 上不可约；这一猜想至今仍未解决。更多详情可参见 G. Ter- janian 1989年的论文（[6]）。 $K_p(t)$ 的这一因式分解意味着上文所引 $F_p(x,y)$ 的因式分解。准确地说，在 $K_p(t)$ 的因式分解中， $C_p(t)$ 应为 $C_p(t,1)$，但我们"滥用记号"，将二者视为相同。

由此引入多项式

$$E_2 = \frac{(x+y)^p - x^p - y^p}{pxy(x+y)} = \left(x^2+xy+y^2\right)^e C_p(x,y),$$

它属于 $Z[x,y]$；类似地，在三个变量 x, y, z 的情形下，多项式

$$E_3 = \frac{(x+y+z)^p - x^p - y^p - z^p}{p(x+y)(y+z)(z+x)},$$

它位于 $Z[x,y,z]$ 中。事实上，令

$$H_p(x,y,z) = (x+y+z)^p - x^p - y^p - z^p = \sum_{\substack{0 \le j,k,l < p \\ j+k+l=p}} \frac{p!}{j!k!l!} x^j y^k z^l,$$

不难看出， H_p 的所有系数都能被 p 整除，并且 $H_p(x,-x,z) = H_p(x,y,-y) = H_p(x,y,-x) = 0$，因此 H_p 能被 p、 $x+y$、 $y+z$ 和 $z+x$ 整除，它们在 $Z[x,y,z]$ 中两两互素。因此， H_p 能被它们的乘积 $p(x+y)(y+z)(z+x)$ 整除，也就是说， E_3 的系数属于 $\mathbb{Z}$。此外，注意到

$$E_3 = E_2 + Q(x,y,z),$$

其中 $Q \in z\mathbb{Z}[x,y,z]$。事实上，

$$E_3 - E_2 = \frac{(x+y+z)^p - x^p - y^p - z^p}{p(x+y)(y+z)(z+x)} - \frac{(x+y)^p - x^p - y^p}{pxy(x+y)} =$$

$$= \frac{xy((x+y+z)^p - x^p - y^p - z^p) - (y+z)(z+x)((x+y)^p - x^p - y^p)}{pxy(x+y)(y+z)(z+x)} =$$

$$= \frac{xy\left(\left(\sum_{k=1}^{p-1} \binom{p}{k}(x+y)^k z^{p-k} + (x+y)^p - x^p - y^p\right) - (xy+xz+yz+z^2)((x+y)^p - x^p - y^p)\right.}{pxy(x+y)(y+z)(z+x)} =$$

$$= \frac{xy\sum_{k=1}^{p-1} \binom{p}{k}(x+y)^k z^{p-k} - z(x+y+z)((x+y)^p - x^p - y^p)}{pxy(x+y)(y+z)(z+x)},$$

它是一个关于 $\mathbb{Z}[x,y,z]$ 的多项式，且其所有项都是 z 的倍数。

随后，核心问题出现了。令 $b = z(x+y+z)$，我的通信者观察到

$E_3 = a_n + b(a_{n-1} + b(a_{n-2} + \cdots + b(a_2 + b(a_1 + b)) \cdots)) = b^n + a_1 b^{n-1} + \cdots a_{n-2} b^2 + a_{n-1} b + a_n$，其中 $n = \frac{p-3}{2}$，且所有 $a_k \in \mathbb{Z}[x,y]$，满足 $a_n = E_2$。这相当于说明 E_3 是一个关于 b 的多项式，其系数属于 $\mathbb{Z}[x,y]$，并要求给出证明。

2004年4月，又收到第二条消息，对第一条消息作了补充。在这条消息中，他指出 $a_n + xya_{n-1} = (x+y)^{p-3}$，并猜想，对于 $0 \le m \le n-1$，其中 $n = \frac{p-3}{2}$，

$$a_{n-m} + xya_{n-m-1} = a_{n-m}^{(1)} (x+y)^{p-2m-3},$$

其中，$a_k^{(j)}$ 是多项式 a_k中第 j项的系数。接着，文中声称，L. E. Dickson 所著《数论史》第二卷引用的 E. Catalan 的一项结果给出了 $C_p(x,y) = \sum_{k=0}^{p-3-2e} c_k x^{p-3-2e-k} y^k$的系数，即（经修正后）

$$c_k = \frac{1}{p}\left(\binom{p-1}{k} - (-1)^k\right).$$

随后，他声称可以推导出 $a_{n-1}^{(1)} = a_n^{(2)}$和 $a_n^{(2)} = \frac{p-3}{2}$。所有计算均使用 Mathematica 完成。

2004年5月，第三封邮件发来，称他已将问题发给 Andrew Granville；Granville 回复说，任何在映射 $\varphi\colon\ z \mapsto -(x+y+z)$下保持不变的多项式 $F(x,y,z)$（例如 E_3），都可以写成关于 $b = z(x+y+z)$的多项式，并给出了一个按 F的次数归纳的简单证明。具体而言，令 $a_0 = F(x,y,0)$，Granville 指出，a_0和 $F(x,y,z) - a_0$在 φ下保持不变。但是，$F(x,y,z) - a_0$能被 z整除；应用 φ后，它也能被 $-(x+y+z)$整除，因此能被 b 整除。注意到 b在 φ下也保持不变，他推导出 $G(x,y,z) = F(x,y,\frac{b}{z} - a_0)$在 ϕ~~下保持不变~~，且次数低于 F。因此，根据归纳假设，G 可以写成关于 b的多项式，从而 F也可以。

下面我们尝试推广 Granville 这一绝妙而简洁的论证。

注。此后，为强调这些多项式对 p的依赖关系，将 E_2 和 E_3 所表示的多项式分别记作$E_{2,\,p}$ 和$E_{3,\,p}$。请注意，

$$\frac{(x+y)^p - (x^p+y^p)}{x+y} = (x+y)^{p-1} - \frac{x^p+y^p}{x+y} = \sum_{k=0}^{p-1}\binom{p-1}{k}x^k y^{p-1-k} - \sum_{k=0}^{p-1}(-1)^k x^k y^{p-1-k}$$

$$= \sum_{k=0}^{p-1}\left(\binom{p-1}{k} - (-1)^k\right)x^k y^{p-1-k} = \sum_{k=1}^{p-2}\left(\binom{p-1}{k} - (-1)^k\right)x^k y^{p-1-k},$$

因为 $\binom{p-1}{k} - (-1)^k = 0$ 对于 $k=0$ 和 $k=p-1$。因此

$$E_{2,p}(x,y) = \frac{(x+y)^p - (x^p+y^p)}{pxy(x+y)} = \frac{1}{pxy}\sum_{k=1}^{p-2}\left(\binom{p-1}{k} - (-1)^k\right)x^k y^{p-1-k} =$$

$$= \sum_{k=1}^{p-2}\frac{\binom{p-1}{k} - (-1)^k}{p}x^{k-1}y^{p-k-2},$$

其中系数 $\binom{p-1}{k}_p^{-(-1)^k}$ 是整数，对于 $1 \le k \le p-2$，因为

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!} \equiv \frac{(-1)^k k!}{k!} \equiv (-1)^k \pmod{p}.$$

另一方面，

$$H_p(x,y,z) = (x+y+z)^p - (x^p+y^p+z^p) = \sum_{m=0}^{p} \binom{p}{m}(x+y)^m z^{p-m} - (x^p+y^p+z^p) =$$

$$= \sum_{m=1}^{p} \binom{p}{m}(x+y)^m z^{p-m} - (x^p+y^p),$$

因此

$$E_{3,p}(x,y,z) = \frac{H_p(x,y,z)}{p(x+y)(y+z)(z+x)} = \frac{1}{p(y+z)(z+x)}\left(\sum_{m=1}^{p}\binom{p}{m}(x+y)^{m-1}z^{p-m} - \frac{x^p+y^p}{x+y}\right)$$

$$= \frac{1}{p(y+z)(z+x)}\left(\sum_{m=1}^{p}\binom{p}{m}(x+y)^{m-1}z^{p-m} - \sum_{k=0}^{p-1}(-1)^k x^k y^{p-1-k}\right) =$$

$$= \frac{1}{p(y+z)(z+x)}\sum_{k=0}^{p-1}\left(\binom{p}{k+1}(x+y)^k z^{p-k-1} - (-1)^k x^k y^{p-k-1}\right),$$

最后一个 e 通过在前两个求和式中的第一个求和式里令 $k = m-1$，得到该性质 .

此外，将分子和分母同乘以 $(x+y)$，展开分子，并令 $l = k+1$，可得

$$E_{3,p}(x,y,z) = \frac{1}{p(x+y)(y+z)(z+x)}\left(\sum_{l=1}^{p}\binom{p}{l}(x+y)^l z^{p-l} + \sum_{l=1}^{p}(-1)^l x^l y^{p-l} - \sum_{k=0}^{p-1}(-1)^k x^k y^{p-k}\right)$$

$$= \frac{1}{p(x+y)(y+z)(z+x)}\left(\sum_{l=0}^{p}\binom{p}{l}(x+y)^l z^{p-l} - x^p - y^p - z^p)\right).$$

展开二项式 $(x+y)^l$，并将所有二项式系数替换为其定义式，然后反转求和顺序并提出公因子，可得

$$E_{3,p}(x,y,z) = \frac{1}{p(x+y)(y+z)(z+x)}\left(p!z^p\sum_{k=0}^{p}\frac{1}{k!}\left(\frac{x}{y}\right)^k\sum_{l=k}^{p}\frac{1}{(p-l)!(l-k)!}\left(\frac{y}{z}\right)^l - x^p - y^p - z^p\right).$$

因此，前面已证明的关于 $E_{3,p}$ 的以下两个表达式，

$$E_{3,p}(x,y,z) = \frac{1}{p(y+z)(z+x)}\sum_{k=0}^{p-1}\left(\binom{p}{k+1}(x+y)^k z^{p-k-1} - (-1)^k x^k y^{p-k-1}\right) =$$

$$= \frac{1}{p(x+y)(y+z)(z+x)}\left(p!z^p\sum_{k=0}^{p}\frac{1}{k!}\left(\frac{x}{y}\right)^k\sum_{l=k}^{p}\frac{1}{(p-l)!(l-k)!}\left(\frac{y}{z}\right)^l - x^p - y^p - z^p\right).$$

同理，分别交换 $x+y$ 与 $y+z$，再交换 $x+y$ 与 $x+z$，可得

$$E_{3,p}(x,y,z)=\frac{1}{p(x+y)(x+z)}\sum_{k=0}^{p-1}\left(\binom{p}{k+1}(y+z)^k x^{p-k-1}-(-1)^k y^k z^{p-k-1}\right)=$$
$$=\frac{1}{p(x+y)(y+z)(z+x)}\left(p!x^p\sum_{k=0}^{p}\frac{1}{k!}\left(\frac{y}{z}\right)^k\sum_{l=k}^{p}\frac{1}{(p-l)!(l-k)!}\left(\frac{z}{x}\right)^l-x^p-y^p-z^p\right),$$

and

$$E_{3,p}(x,y,z)=\frac{1}{p(x+y)(y+z)}\sum_{k=0}^{p-1}\left(\binom{p}{k+1}(x+z)^k y^{p-k-1}-(-1)^k x^k z^{p-k-1}\right)=$$
$$=\frac{1}{p(x+y)(y+z)(z+x)}\left(p!y^p\sum_{k=0}^{p}\frac{1}{k!}\left(\frac{z}{x}\right)^k\sum_{l=k}^{p}\frac{1}{(p-l)!(l-k)!}\left(\frac{x}{y}\right)^l-x^p-y^p-z^p\right).$$

此外，在搜寻上述提到的 E. Catalan 的结果后，我们在一篇文章（[1]）中找到了它。该文最初发表于 1861 年，后来 Catalan 于 1885 年再次提及并加以补充，其中给出了以下多项式的显式表达式

$$E_{3,n}(x,y,z)=\frac{(x+y+z)^n-x^n-y^n-z^n}{(x+y)(y+z)(z+x)},$$

适用于奇整数 $n>3$。他将系数全为 1、次数为 $m\geq 0$ 的齐次多项式定义为

$$H_m=H_m(x,y,z)=\sum_{j,k,l\in\mathbb{N}:j+k+l=m}x^j y^k z^l=\sum_{j=0}^{m}\sum_{k=0}^{m-j}x^j y^k z^{m-j-k},$$

with $H_0=1$，他设定了 $P=x+y+z$，并证明，对于奇数 $n>3$ ，

$$E_{3,n}(x,y,z)=\sum_{m=0}^{n-3}H_m(x,y,z)P^{n-3-m}+2H_{\frac{n-3}{2}}(x^2,y^2,z^2).$$

The variation

设 K 为交换域。取 $n+1$ 个变量 $x=(x_1,...,x_n)$ 和 z，然后考虑由多项式 $A = K[x,z]$ 构成的 $K[x]$-代数。选取一个多项式 $p(x,z)$，属于 A，并定义如下从 A 到 A 的变换 T：对于每个多项式 $F(x,z)$，将其对应到多项式

$$TF(x,z) = F(x,p(x,z)). \tag{1}$$

这个变换 T 是代数 A 到其自身的 $K[x]$-同态。令 B 为在 T下不变的多项式集合，即，

$$B = \{F \in A : TF = F\}. \tag{2}$$

显然， B 是 A 的一个 $K[x]$-子代数，并且包含 $K[x]$。那么 se t

$$C = B \setminus K[x]. \tag{3}$$

如何刻画 B 的元素?
要使 C 非空，需要满足什么条件?
情形 $p(x,z) = z$ 很平凡，因为 $T = \mathrm{id}_A$ 和 $B = A$。

当满足以下条件时，我们称多项式 $p(x,z)$ 为 `Granville 式

$$p(x,z) = -z + r(x). \tag{4}$$

在这种情况下， T是一个对合（即 $T^2 = \mathrm{id}_A$），因为此时有 $Tp(x,z) = z$。Granville 研究的是 $p(x,z) = -(x+y+z)$ 的情形。

现在，进入“变体”!

1 准备。引入变换 T 的 T^k ot 次迭代序列，以及相关的多项式序列 $p_k(x,z) = T^k z$。

当然， T^0 是 id_A，并且 $T^1 = T$。

类似地， $p_0(x,z) = z$，而 $p_1(x,z)$ 本身就是 $p(x,z)$。

简言之，当 $p(x,z) = z$ 时，我们称 $p(x,z)$ 为 1-适当。

设 $m > 1$ 为整数。此后，我们假设 K 包含所有 m 次单位根。当多项式 $p(x,z)$ 具有以下形式时，我们称其为 m-适当：

$$p(x,z) = qz + r(x), \tag{*}$$

其中 q 是一个本原 m 次单位根，且 $r(x)$ 属于 $K[x]$。

因此，当且仅当 $p(x,z)$ 是 2-适当时，它才是“Granville 式”的。

当对于某个 $m \geq 1$， $p(x,z)$ 是 m-适当的时，简称其为适当。

2 注。当 $p(x,z)$ 是 m-适当的时，我们有 $p_m(x,z) = z$，因此有 $T^m = \mathrm{id}_A$。更准确地说，我们有

$$
\begin{aligned}
&p_0(x,z) = z\\
&p_1(x,z) = qz + r(x)\\
&p_2(x,z) = q^2 z + (q+1).r(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&p_k(x,z) = q^k z + (q^{k-1} + \cdots + q + 1).r(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&p_m(x,z) = z.
\end{aligned}
$$

当 $r(x) \neq 0$ 时，多项式 p_0、p_1、.....、p_{m-1} 两两互素。

令 $d(P)$ 为每个多项式 $P(x,z)$ 关于 z 的次数。]

3 定理。设 $p(x,z)$ 是 m-adequat。令 b 为多项式 $\{p_k$ 的乘积：$0 \leq k < m\}$。多项式 $F(x,z)$ 属于 B 当且仅当它具有以下形式：

$$F(x,z) = G(b), \text{ with } G(y) \in K[x][y]. \tag{6}$$

证明。注意到多项式 b 属于 B，因此 $TG(b) = G(b)$，而所有具有形式 (6) 的多项式都属于 B。

对于逆命题，分两种情况讨论。

若 $r(x) = 0$，则 F属于 B意味着 $F(x,z) = F(x,qz)$；由于 $q^m = 1$，我们得出 F是 z^m的多项式。

否则，对 z中的 F，按其次数 $d(F)$ 归纳。

The case $d(F) = 0$ is trivial.

分四步进行。

引理1. 若 $F(x,z)$ 属于 B，则 $p_k(x,z)$、$k \geq 0$中的每一个都整除多项式 $W(x,z)$：$=F(x,z) - F(x,0)$。

事实上，$W(x,z)$ 也属于 B，并且可被 z整除。因此，我们必有 $W(x,z) = z.U(x,z)$，而对于 $k \geq 1$，有

$$W(x,z) = T^k U(x,z) = p_k(x,z).T^k U(x,z).$$

如果 $F(x,z)$ 属于 B，多项式 $F(x,z) - F(x,0)$ 可被 b 整除，即有 $F(x,z) - F(x,0) = b(x,z).V(x,z)$。因此，$V(x,z)$ 属于 B，此外还有 $d(V) < d(F)$。由此得出结论。□

补充。以下三个条件等价。

(i) 集合 C 非空。(ii) 存在一个整数 $m \geq 1$，使得 $T^m = \mathrm{id}_A$。(iii) 多项式 $p(x, z)$ 是适当的。

证明. 如果 $p(x, z)$ 是 m-适当的，我们已经知道 C 非空，且 $T^m = \mathrm{id}_A$。□

引理 2. 如果 $d(p) \neq 1$，那么 $B = K[x]$。

事实上，$d(TF) = d(F).d(p)$。如果 F 属于 B，即 $TF = F$，则有 $d(F) = d(F).d(p)$；而且，如果 $d(p) \neq 1$，那么 $d(F) = 0$。□

引理 3. 如果 C 非空，则多项式 $p(x, z)$ 是适当的。

证明。根据前一个引理，我们知道 $p(x, z)$ 具有以下形式：

$$p(x, z) = q(x).z + r(x), \text{ with } q(x) \neq 0. \tag{7}$$

取 $F \in B$，使得 $d(F) = m \geq 1$。
按 z 的幂次降序排列 F，写作
$F = u.z^m + v.z(m - 1) + \cdots$
由此可得
$TF = u.(qz + r)^m + v.(qz + r)^{m-1} + \cdots$
$= u.q^m z^m + (u.m.q^{m-1}.r + v.q^{m-1} z^{m-1} + \cdots$
然后令前两个系数相等，得到两个等式

$$q^m = 1 \tag{8}$$

$$q^{m-1}.(m.r + v) = v. \tag{9}$$

因此，对于 $q = 1$，我们有 $r = 0$。□

引理 4. 若 $T^m = \mathrm{id}_A$ 对于某个 $m \geq 1$，则 $\{p_k$ 中多项式的乘积 b : $0 \leq k < m\}$ 在 T 下保持不变，并且 $d(b) \geq 1$。

证明到此结束 □ □

References

1. E. Catalan, *Sur le dernier théorème de Fermat (1861)*, M´em. Soc. Roy. Sci. Li`ege (2) 12 (1885), 179-187。2. A. L. Cauchy, *Rapport sur un Mémoire de M. Lamé, relatif au dernier théorème de Fermat*, 巴黎科学院会议记录 9 (1839年), 359-363。3. A. L. Cauchy, *Note sur Quelques Théorèmes d'Algèbre*, 《分析与数学物理练习》, 第2卷, Bachelier, 巴黎, 1841年, 第137-144页。4. D. Mirimanoff, *Sur l'équation* $(x+1)^l - x^l - 1 = 0$, 《新数学年刊》3 (1903年), 385-397。5. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1979年。6. G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes*, 《算术学报》54 (1989年), 87-125。

120 Rue de Charonne, 75011 Paris, France; email: labib.haddad@wanadoo.fr

Penn State Univ., 25 Yearsley Mill Rd, Media, PA 19063, USA; e-mail: cxh22@psu.edu