一类具有素数公式的可换环

王 世 强

(北京师范大学数学系)

模型论一般被认为是一个比较抽象的数理逻辑分支,本文象文献[1]一样,也是为模型论中的结论在其它数学分支中寻找新事例的尝试之一. 在考查整数环 I 的某些剩余类环的基础上,引用模型论中的紧致性定理,我们可以证明:存在着 I 的各种扩环,它们分别具有各种多项式形状的"素数公式"(其含义见下列定理).

我们讨论如下的整系数多项式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \quad (a_0, \cdots, a_n \in I;\ a_0 \neq 0;\ n \geqslant 1),$$

它适合条件:

(A) $f(x)$在多项式环 $I[x]$ 中分解为整数与不可约本原多项式之积时,至少有一个次数$\geqslant$1 的单因式(即:非重因式)出现(易知:对于 $I[x]$ 中任给的 $f(x)$,它是否适合 (A) 是能够在有限步内有效地判定的. 不过这一点在本文的论证中并不需要).

本文的主要结果是:

定理 1 对每一个适合条件 (A) 的整系数多项式 $f(x)$,都存在整数环 I 的扩环 R_f,它具有下列诸性质:R_f 是有 1 的可换环. R_f 中有无限多个素元. R_f 中有无限多个合元. R_f 中每个非单位的元(特别地,每个素元)都可表示为 $f(x_1)$ $(x_1 \in R_f)$ 形状. 此外:R_f 中有无限多个单位. R_f 中每个非零非单位的元都是零因子.

我们知道,在整数论中,有很多关于素数形状的待解问题. 例如,我们不知道是否存在无限多个 $x_1^2 + 1 (x_1 \in I)$ 形状的素数,等等. 本文的结果,与这些问题的研究并无直接联系. 但是本文说明,利用有关整数环 I 的某些不难证明的性质,并引用模型论的结论,可以断定存在 I 的各种扩环,在这些扩环中,有着关于素数形状的强得多的结论成立. 这些不但是自身有趣的事实,也显示了模型论方法的一些作用(若不用模型论中的紧致性定理或超积方法,作者尚未见对定理 1 有其它证法).

为了证明定理 1,先证明一些引理.

引理 1 设 $g(x)$ 是任一个非常数的整系数多项式. 若把 $g(0), g(1), g(2), \cdots\cdots$ 中每个数的素因数都列举出来,则其中有无限多个互异的素数出现.

证 设 $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \quad (b_0, \cdots, b_m \in I;\ b_0 \neq 0;\ m \geqslant 1)$. 若 $b_m = 0$,则由 $g(x) = x(b_0x^{m-1} + \cdots + b_{m-1})$ 易见结论成立. 以下设 $b_m \neq 0$.

假若在 $g(0), g(1), g(2), \cdots$ 中只出现有限多个互异的素因数,设为

$$p_1, \cdots\cdots, p_r. \tag{1.1}$$

令 $q = p_1 \cdot \cdots \cdot p_r$,由 $b_0 \neq 0$ 可知当 x 甚大时,$|g(x)|$ 甚大,所以 $r \geqslant 1$,从而 $q > 1$.

本文 1981 年 8 月 26 日收到.

由此及 $b_m \neq 0$ 知可取正整数 l 足够大使 $|g(b_m^2q^l)| > |b_m|$. (1.2)

令 $q_1 = b_m^2q^l$，由(1.1)知 $g(q_1)$ 的每个素因数 π 都在 $p_1, \cdots, p_r$ 中，所以 $\pi|q$，再由 $\pi|g(q_1)$ 及 q_1，$g(x)$形状易见有 $\pi|b_m$. 故可知：存在 b_m 的幂 b_m^u 能使 $g(q_1)|b_m^u$. 设 u_1 为此种 u 中之最小者(由(1.2)式及 $b_m \neq 0$ 可知 $u_1 > 1$)，则有

$$g(q_1)|b_m^{u_1},\ g(q_1)\nmid b_m^{u_1-1}, \tag{1.3}$$

所以，存在 $v \in I$ 能使

$$b_m^{u_1} = g(q_1)\cdot v = (b_0(b_m^2q^l)^m + \cdots + b_{m-1}(b_m^2q^l) + b_m)\cdot v. \tag{1.4}$$

如果 $b_m|v$，设 $v = b_mv_1(v_1 \in I)$，则由(1.4)式有 $b_m^{u_1-1} = g(q_1)\cdot v_1$，此与(1.3)式不合. 所以

$$b_m\nmid v. \tag{1.5}$$

又由(1.4)式有

$$b_m^{u_1-1} = b_m(b_0b_m^{2m-2}q^{lm} + \cdots + b_{m-1}q^l)\cdot v + v, \tag{1.6}$$

且由上有 $u_1 - 1 > 0$，故由(1.6)式易见有 $b_m|v$，此与(1.5)式矛盾. 故引理得证.

引理 2 设整系数多项式 $f(x)$ 适合条件 (A)，则存在无限多个素数 p 能适合下列条件 (B) 存在 $a \in I$ 能使 $p|f(a)$ 而 $p\nmid f'(a)$(注意：a 与 p 有关).

证 任取 $f(x)$在 $I[x]$中的一个次数 $\geqslant 1$ 的不可约本原单因式 $q(x)$(由(A)知 $q(x)$存在)，设

$$f(x) = f_1(x)\cdot q(x),\ (f_1(x) \in I[x]). \tag{2.1}$$

由 $q(x)$ 为单因式知 $q(x)\nmid f_1(x)$，再由 $q(x)$不可约可知存在 $u(x), v(x) \in I[x]$ 能使

$$u(x)q(x) + v(x)f_1(x) = c,\ (c \in I,\ c \neq 0). \tag{2.2}$$

又由 $q(x)$次数 $\geqslant 1$ 知 $q(x)\nmid q'(x)$，仿上可知存在 $w(x), w_1(x) \in I[x]$ 能使

$$w(x)q(x) + w_1(x)q'(x) = d,(d \in I, d \neq 0). \tag{2.3}$$

又由(2.1)式有

$$f'(x) = f_1'(x)q(x) + f_1(x)q'(x). \tag{2.4}$$

由引理1知，在 $q(0), q(1), q(2), \cdots\cdots$中有无限多个素因数，其中大于 $\max(|c|,|d|)$ 的显然仍有无限多个，任取一个这样的素因数 p 来看：

由 p 的取法知，$p\nmid c$；$p\nmid d$；并且存在 $a \in I$ 能使 $p|q(a)$. (2.5)

由(2.5)及(2.1)可知 $p|f(a)$. (2.6)

由(2.5)及(2.2)可知 $p\nmid f_1(a)$；由(2.5)及(2.3)式可知 $p\nmid q'(a)$；从而由 p 为素数知 $p\nmid f_1(a)q'(a)$；再由(2.5)及(2.4)式可知 $p\nmid f'(a)$. (2.7)

由(2.6)及(2.7)即知 p 适合条件(B).

引理 3 设 p 为任一素数，I' 为整数环 I 对于模 p^3 的剩余类环 $I/(p^3)$. 取 I' 中诸剩余类的代表元为：$0, 1, 2, \cdots, p^3 - 1$. 则 I' 的 $p^3 - 1$ 个非零元为如下情况：I' 中的单位(指：有逆元的元)为一切 $m(0 < m < p^3)$ 之适合 $p\nmid m$ 者，共有 $p^3 - p^2$ 个. I' 中的素元(指：非零，非单位，且无真分解的元)为一切 $mp(0 < m < p^2)$ 之适合 $p\nmid m$ 者，共有 $p^3 - p$ 个. I' 中的合元(指：非零，非单位，也非素元的元)为一切 $mp^2(0 < m < p)$，共有 $p - 1$ 个.

证明从略.

引理 4 设整系数多项式 $f(x)$ 适合条件(A)，素数 p 及 $f(x)$适合条件(B). 则在 I 的剩余类环 $I' = I/(p^3)$ 中，每个非单位的元都能表示为 $f(x_1)$ 形状 $(x_1 \in I')$.

证 取 I' 中诸剩余类的代表元为：$0, 1, 2, \cdots, p^3 - 1$.

由(B)知存在 $a \in I$ 能使 $p|f(a)$ 而 $p\nmid f'(a)$. (4.1)

由 $p|f(a)$ 知对任何 $k \in I$ 都有 $p|f(a + kp)$. (4.2)

现在证明：当 k 取值 $0, 1, 2, \cdots, p^2-1$ 时，诸 $f(a+kp)$ 对模 p^3 互不同余。 (4.3)

设 $$0 \leqslant k_1, k_2 \leqslant p^2-1, \tag{4.4}$$

若有 $$f(a+k_1p) \equiv f(a+k_2p) \pmod{p^3},$$

则有(用 Taylor 公式)：

$$f(a)+k_1pf'(a)+\frac{1}{2!}k_1^2p^2f''(a)+\frac{1}{3!}k_1^3p^3f'''(a)+\cdots$$
$$\equiv f(a)+k_2pf'(a)+\cdots, \pmod{p^3},$$

注意到每个 $\frac{1}{r!}f^{(r)}(x)$ 的系数都是整数，即可得

$$(k_1-k_2)pf'(a)+(k_1^2-k_2^2)p^2\left(\frac{1}{2}f''(a)\right) \equiv 0, \pmod{p^3},$$

从而可有 $$p^2 \mid (k_1-k_2)\left[f'(a)+(k_1+k_2)p\left(\frac{1}{2}f''(a)\right)\right],$$

但由 (4.1) 式可知 $p \nmid f'(a)+(k_1+k_2)p\left(\frac{1}{2}f''(a)\right)$，所以 $p^2 \mid k_1-k_2$，再由 (4.4) 式即知 $k_1=k_2$. 所以 (4.3) 式成立.

由 (4.2)、(4.3) 式可知，诸 $f(a+kp)$ $(k=0, 1, 2, \cdots, p^2-1)$ 对模 p^3 的最小非负剩余恰好就是 I' 中的全部 (p^2 个)形状为 mp 的元，从而由引理 3 即知它们包括了 I' 中全部非单位的元.

定理 1 的证明. 令语言 $\mathscr{L}=\{+, \times, 0, 1\}$，令 T_f 为 $\mathscr{L}$ 中如下的理论 (以下为简便，用普通语言描述 T_f 的公理)：

T_f 的公理：
- 可换环公理.
- 1 是乘法单位元.
- 存在无限多个单位(指："至少存在一个单位"，"至少存在 2 个互异的单位"，"至少存在 3 个互异的单位"，……等无限多条公理. 以下仿此).
- 存在无限多个素元.
- 存在无限多个合元.
- 对每个非单位的元 α，都存在元 β 能使 $\alpha=f(\beta)$.
- 每个非零非单位的元都是零因子.
- $1 \neq 0$, $1+1 \neq 0$, $1+1+1 \neq 0$, $\cdots$.

任取 T_f 的有限子集 S. 则由引理 2、3、4 易知能找到足够大的素数 p，使 I 对于模 p^3 的剩余类环 I' 适合 S. 故由紧致性定理可知 T_f 有模型. 显见 T_f 的每一模型 R_f 都具有定理 1 中所说的性质.

参 考 文 献

[1] 王世强，北京师范大学学报，1982，1；科学通报，26 (1981)，18：1149.