arXiv:2302.00459v2 [math.NT] 3 Dec 2023

Jacobsthal 函数的多项式类比

Alexander Kalmynin *† Sergei Konyagin †邮箱：alkalb1995cd@mail.ru 邮箱：konyagin23@gmail.com

摘要

对于多项式 $f(x) \in \mathbb{Z}[x]$，我们研究 Jacobsthal 函数的一种类比，其定义公式为

$$j_f(N) = \max_m \{\text{对于某些 } x \in \mathbb{N}, \text{不等式 } (x+f(i), N) > 1 \text{对所有 } i \le m\}\text{均成立}$$

我们证明了一个下界

$$j_f(P(y)) \gg y(\ln y)^{\ell_f - 1} \left(\frac{(\ln\ln y)^2}{\ln\ln\ln y}\right)^{h_f} \left(\frac{\ln y \ln\ln\ln y}{(\ln\ln y)^2}\right)^{M(f)},$$

其中，$P(y)$是所有小于 y的素数 p 的乘积，ℓ_f 是 $f(x)$的一次因子个数，h_f 是非线性不可约因子的个数，而 $M(f)$是映射$f\colon \mathbb{F}_p \to \mathbb{F}_p$下一个点的最大原像的平均大小。量 $M(f)$根据某些伽罗瓦群计算得出。

关键词：Jacobsthal 函数、筛法、多项式、伽罗瓦群 MSC 分类：
11N25；11N32

1 引言与主要结果

设 N 为一个自然数。Jacobsthal 函数 $j(N)$定义为与 N互素的数之间最大间隔的长度。换言之，

$$j(N) = \max_m\{\text{For some } x \in \mathbb{N} \text{ the inequality } (x+i, N) > 1 \text{ holds for all } i \le m\}$$

用于估计 $j(N)$ 的估计被用于建立关于连续素数之间大间隔的结果。例如，目前关于 $p_{n+1} - p_n$ 的最佳下界是

*俄罗斯国立高等经济大学，俄罗斯莫斯科
†俄罗斯科学院斯捷克洛夫数学研究所，俄罗斯莫斯科

定理（[1]）。设 $y \geq 19$ 且

$$P(y) = \prod_{p \leq y} p.$$

Then

$$j(P(y)) \gg y \frac{\ln y \ln\ln\ln y}{\ln\ln y} = (1 + o_{y\to\infty}(1)) \ln P(y) \frac{\ln\ln P(y) \ln\ln\ln\ln P(y)}{\ln\ln\ln P(y)}.$$

特别是，对于 $X \geq e^{16}$

$$\max_{p_{n+1} \leq X} (p_{n+1} - p_n) \gg \ln X \frac{\ln\ln X \ln\ln\ln\ln X}{\ln\ln\ln X}.$$

至于 $j(N)$ 的上界，H. Iwaniec 证明了 [2]

定理。对于所有自然数 N，不等式

$$j(N) \ll \ln^2 N$$

成立。

本文将研究 Jacobsthal 函数的一个多项式类比。具体而言，设 $f(x)$ 是一个具有整数系数的非常数多项式。通过下式定义函数 $j_f(x)$:

$$j_f(N) = \max_m \{\text{For some } x \in \mathbb{N} \text{ the inequality } (x + f(i), N) > 1 \text{ holds for all } i \leq m\}.$$

因此，我们不再考察不含与 N 互素的数的区间，而是研究多项式数列的平移。本文将给出 $j_f(P(y))$ 的一个下界，类似于经典的 Rankin 上界 [3]。为表述所得结论，我们先定义一个数 $M(f)$；可以将其称为映射 $f\colon \mathbb{F}_p \to \mathbb{F}_p$ 下非零点的最大原像的平均大小。

定义。假设 $f(x) \in \mathbb{Z}[x]$。若 p是素数，则用 $M_p(f)$ 表示方程 $f(x) = y$在固定 $y \in \mathbb{F}_p \backslash \{0\}$ 时的解的最大数量 $x \in \mathbb{F}_p$。量 $M(f)$ 定义为满足下式的唯一 M

$$\sum_{p \leq X} \frac{M_p(f)}{p} = M \ln\ln X + O(1)$$

对所有实数 $X \geq 2$均成立，前提是这样的数 M 存在。

容易看出，如果 $f_d(x) = x^d$，那么 $M(f_1) = 1$ 且 $M(f_2) = M(f_3) = 2$。在第三节中，我们将用与 $f(x)$ 相关的某些伽罗瓦群来表示 $M(f)$。我们将对所有 d 以及一个次数为 d 的典型多项式，明确计算 $M(f_d)$。第二节专门证明关于 $j_f(P(y))$ 的以下界

定理 1。设对于一个多项式 $f \in \mathbb{Z}[x]$, f 的因式分解包含 ℓ_f 个不同的一次因子和 h_f 个不同的非线性因子。那么对于 $y \geq 19$，不等式

$$j_f(P(y)) \gg y(\ln y)^{\ell_f - 1} \left(\frac{(\ln \ln y)^2}{\ln \ln \ln y} \right)^{h_f} \left(\frac{\ln y \ln \ln \ln y}{(\ln \ln y)^2} \right)^{M(f)} =$$

$$(1 + o_{y \to \infty}(1)) \ln P(y) (\ln \ln P(y))^{\ell_f - 1} \left(\frac{(\ln \ln \ln P(y))^2}{\ln \ln \ln \ln P(y)} \right)^{h_f} \left(\frac{\ln \ln P(y) \ln \ln \ln \ln P(y)}{(\ln \ln \ln P(y))^2} \right)^{M(f)}$$

成立。

注 1. 注意到，j_f 的值在加上常数平移后保持不变，即对所有 $n \in \mathbb{Z}$，都有 $j_f = j_{f+n}$。取 $n = -f(0)$，我们总能使多项式被 x整除。特别地，对于次数至少为 2 的多项式 f，我们总能得到

$$j_f(P(y)) \gg y \frac{(\ln \ln y)^2}{\ln \ln \ln y} \frac{\ln y \ln \ln \ln y}{(\ln \ln y)^2} = y \ln y.$$

事实上，由于 $M(f) \geq 1$，对于 $\ell_f \geq 2$或 $\ell_f = 1$以及 $h_f \geq 1$，我们便得到所需的不等式。剩下的最后一种情形是 $\ell_f = 1, h_f = 0$，即对于某些 $a, b, c \in \mathbb{Z}$, $ac \neq 0$，有 $f = c(ax + b)^d$。在最后一节中，我们证明对于 $f_d(x) = x^d$, $d \geq 2$，有 $M(f_d) = \tau(d) \geq 2$；因此在此情形下，我们得到$M(f) = M(f_d) \geq 2$，不等式得证。

$M(f)$ 的值总是存在且为有理数。为了表述关于 $M(f)$ 的结果，我们先引入量 $m(G, H; X)$。

定义。设有限群 G 作用于集合 X，且 H 是 G 的子群。对于 $g \in G$，用 X^g 表示 g 的不动点集合。那么

$$m(G, H; X) = \frac{1}{|G|} \sum_{g \in G} \max_{h \in H} |X^{hg}|.$$

定理 2。设 L 为一个域，令 L_f 表示多项式 $f(x) - y$ 在有理函数域 $L(y)$（以 L 为底域）上的分裂域。用 K 表示 $\mathbb{Q}_f$ 与 $\overline{\mathbb{Q}}$ 的交，即 $\mathbb{Q}_f$ 的最大常数子域。设 G_f 和 G_f^+ 分别为 $\mathbb{Q}_f = K_f$ 在 $\mathbb{Q}(y)$ 和 $K(y)$ 上的伽罗瓦群。这些群自然地作用于 X，即 $f(x) = y$ 的所有解所成的集合，而 G_f^+ 可视为固定 K 的 G_f 的子群。我们有

$$M(f) = m(G_f, G_f^+; X).$$

我们对 j_f 的研究受到文献 [4]中定理 5 的启发。该结果给出了最小整数 $\gamma_k > 0$ 的上界，使得对于 $1 \leq j \leq k$，所有数 $\gamma_k + j^d$ 都不是两个平方数之和。估计 γ_k 的问题由前两位作者提出。

2 主定理的证明

为证明我们的主要结果，我们将选择一个值 x，使得对于 i 的许多最小取值，通过为所有 $p \leq y$ 选择模 p 的剩余类 x_p，$x + f(i)$ 与 $P(y)$ 不互素。我们将选择 x_p

模 p，其中 $p \le y$ 为素数，使得对于所有 $i = 1, \dots, m$，都存在某个 $p \le y$，使得 $f(i) + x_p \equiv 0$(模 p)。然后我们令 x 为同时同余式 $x \equiv x_p$ (模 p)（对 $p \le y$）的一个解。于是可得 $j_f(P(y)) \ge m$。在证明中，我们将使用以下关于筛过集合的著名结果

引理 1. 设 $\kappa > 0, z \ge 2$。假设 $\{a_n\}$ 是一个非负实数序列，使得对所有 $d \mid P(z)$，我们都有

$$\sum_{n \equiv 0 \pmod d} a_n = g(d)X/d + r_d,$$

其中 $g(d)$ 是一个积性函数，满足 $g(p) \le \kappa, g(p) < p$ 对所有素数 p, $|r_d| \le g(d)$ 和 $z \ll X$均成立。于是我们有

$$\mathcal{S}(a, z) = \sum_{(n, P(z))=1} a_n \ll_\kappa XV(z),$$

其中

$$V(z) = \prod_{p \le z} \left(1 - \frac{g(p)}{p}\right).$$

证明. 这是筛法理论基本引理的一个版本。例如，参见 [5,定理 2.2]

□

特别地，我们得到以下推论

推论 1. 设 $\kappa, z, g(d)$ $V(z)$ 和 X如上所述。假设对任意 $p \le z$，集合 $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$ 包含 $g(p)$ 个元素。令 $S(X,\Omega)$ 表示满足以下条件的 $n \le X$ 的个数：对所有 $p \le z$， n模 $p \notin \Omega_p$。于是

$$S(X, \Omega) \ll XV(z).$$

证明。为此，对任意 $p \le z$，令

$$P(z; p) = \frac{P(z)}{p}$$

并令 $Q(z; p)$ 为满足以下同余式的最小正整数解

$$Q(z; p) \equiv P(z; p) \pmod p \text{ and } Q(z; p) \equiv -1 \pmod{P(z; p)}.$$

令

$$a_m = \begin{cases} 1 \text{ if } m = \prod_{p \le z} \prod_{r \in \Omega_p} (P(z; p)n + rQ(z; p)) \text{ for some } n \le X \\ 0 \text{ otherwise} \end{cases}$$

容易看出，当且仅当相应的 n不属于任何 Ω_p （对 $p \le z$），有 $(m, P(z)) = 1$ 且 $a_m = 1$。引理 1 的条件也显然成立。 □

此外, 我们需要切博塔廖夫密度定理的以下一个众所周知的推论

引理 2. 设 f 是一个具有整数系数的不可约多项式。若 $r_p(f)$ 表示 f 在 $\mathbb{F}_p$ 中的根的数量，则存在两个常数 c_1、$c_2 > 0$，使得对于 $x \geq 3$

$$\sum_{p \leq x} \frac{r_p(f)}{p} = \ln \ln x + c_1 + O(e^{-c_2\sqrt{\ln x}}).$$

证明。设 K 是 f 在 $\mathbb{Q}$ 上的分裂域。K 在 $\mathbb{Q}$ 上的伽罗瓦群 G 作用于 f 的根集上，且该作用是传递的。容易看出，当 p 足够大时，数目 $r_p(f)$ 等于相应弗罗贝尼乌斯共轭类在该作用下的不动点数。因此，根据切博塔廖夫定理，使得 $r_p(f) = k$ 成立的素数 p 所占比例，等于 G 中恰有 k 个不动点的元素所占比例。根据伯恩赛德引理，传递作用的不动点平均数为 1，因此，$r_p(f)$ 在素数上的平均值也为 1。所需余项的渐近公式可由针对 $K/\mathbb{Q}$ 的切博塔廖夫密度定理的有效版本推出，见 [6, 定理 1.3]。

□

现在我们来证明定理 1。

定理 1 的证明。取一个较大的常数 A，再取一个更大的常数 B，并令

$$m = \frac{y}{B}(\ln y)^{\ell_f - 1} \left(\frac{(\ln \ln y)^2}{\ln \ln \ln y} \right)^{h_f} \left(\frac{\ln y \ln \ln \ln y}{(\ln \ln y)^2} \right)^{M(f)},$$

$$z_0 = (\ln y)^A, z_1 = \exp\left(\frac{\ln \ln \ln y \ln y}{A \ln \ln y} \right).$$

我们将分三步选择x_p。完成前两步后，我们计算未筛数 $i \leq m$的数量。更准确地说，若我们已经针对 p的某些取值选定了x_p，那么如果在已使用的素数中存在一个值 p，使得 i 满足

$$f(i) + x_p \equiv 0 \pmod{p}.$$

第一步，我们选择

$$x_p = 0 \text{ for } p \leq z_0 \text{ and for } z_1 < p < y/2.$$

现在，假设数 $i \leq m$ 在第一步之后尚未被筛。令 $k(x)$为 $f(x)$的一个一次因子。那么， $k(i)$没有素因子 $p \in [2, z_0] \cup (z_1, y/2)$。由于 $k(i) \ll m \ll y(\ln y)^{\ell_f + M_{(f)}}$，当 A 足够大时，我们可以得出结论： $|k(i)|$ 要么是素数，要么是 z_1–光滑数。当 A 足够大时， $\ll m$ 的 z_1–光滑数的数量可估计为

$$\Psi(O(m), z_1) \ll \frac{m}{(\ln y)^{\ell_f + M(f) + 2}} = o\left(\frac{y}{\ln y} \right).$$

第二步，对所有 $z_0 < p \leq z_1$，我们按如下方式选择x_p：根据 $M(f)$的定义，对于任意这样的 p，都存在一个非零的 $y_p \in \mathbb{F}_p \backslash \{0\}$，使得同余式 $f(i) \equiv y_p \pmod{p}$有 $M_p(f)$个解。我们设 $x_p \equiv -y_p \pmod{p}$。

接下来，我们将估计经过这两步后仍未被筛掉的 R 个 $i \leq m$ 的数量。我们的目标是证明以下不等式

$$R \leq \frac{y}{3 \ln y}$$

当 A 和 B 足够大时，对所有充分大的 y，该不等式都成立。对于 $p \le \sqrt{y}$，令 Ω_p^I 由所有满足以下条件的模 p 剩余类 t 组成：对 f的某个一次因子 $k(x)$，有 $k(t) \equiv 0 \pmod{p}$。接下来，如果$p \in [2, z_0] \cup (z_1, \sqrt{y})$，我们令

$$\Omega_p^{II} = \{t \quad \text{模 } p: \ \exists \ q(x) \text{ 是 } f(x) \text{ 的非线性不可约因子，且 } q(t) \equiv 0 \ (\text{模 } p)\} \qquad .$$

对于 $p \notin [2, z_0] \cup (z_1, \sqrt{y})$，我们定义 $\Omega_p^{II} = \emptyset$。最后，对于 $z_0 < p \le z_1$，我们令

$$\Omega_p^{III} = \{t \mod p : f(t) \equiv y_p \pmod{p}\}$$

对于 p 的其他取值，令 $\Omega_p^{III} = \emptyset$ 。设 $\Omega_p = \Omega_p^I \cup \Omega_p^{II} \cup \Omega_p^{III}$。我们声称，如果 $i \le m$ 经过两步后仍未筛出，那么要么 $i \ll \sqrt{y}$，要么 $k(i)$ 对某个 f 的一次因子 $k(x)$ 而是 z_1–光滑的（根据 A 的选取，此类 i 的数量为 $o(y/\ln y)$），或者对于任意 $p \le \sqrt{y}$，i 模 $p \notin \Omega_p$。事实上，假设对于某个 p，i 模 $p \in \Omega_p$。那么有三种可能情况。

情形 1：$k(i)$ 可被 p 整除，其中 p 是 f 的某个一次因子 $k(x)$。在这种情况下，要么 $k(i) = \pm p$ 且 $i \ll \sqrt{y}$，要么 $|k(i)|$ 不是素数，因此 $k(i)$ 必须是 z_1–光滑的，否则 i 必须在第一步之后进行筛选。

情形 2：$p \in [2, z_0] \cup (z_1, \sqrt{y})$，并且对于 $f(x)$ 的某个不可约非一次因子 $q(x)$，有$q(i) \equiv 0 \pmod{p}$。于是 $f(i)$ 也可被 p 整除，因此 p 必须在第一步之后进行筛选。情形 3：$z_0 < p \le z_1$ 且 $f(i) \equiv y_p$。于是 i 在第二步之后进行筛选。

由此我们得出

$$R \le S(m, \Omega) + O(\sqrt{y} + \Psi(O(m), z_1)) = S(m, \Omega) + o(y/\ln y)$$

根据我们对 A 的选择。现在我们将应用推论 1 来估计 $S(m,\Omega)$。设 $g(p) = |\Omega_p|$。若对于某个 $p \le \sqrt{y}$，有 $g(p) = p$，那么显然 $S(m,\Omega) = 0$。否则注意到，Ω_p 的三个部分都至多包含 $d = \deg f$ 个元素，因此推论适用于 $\kappa = 3d$，从而得到

$$S(m, \Omega) \ll m \prod_{p \le \sqrt{y}} \left(1 - \frac{g(p)}{p}\right) \ll m \exp\left(-\sum_{p \le \sqrt{y}} \frac{g(p)}{p}\right).$$

现在，设 $k_1(x) \ldots, k_{\ell_f}(x)$ 和 $q_1(x) \ldots, q_{h_f}(x)$ 分别为 $f(x)$ 的所有一次和非线性不可约因子。任意两个固定的不可约多项式在充分大的素数模下都没有公共根。因此，存在一个常数 p_0，使得对于 $p > p_0$，集合 Ω_p^I、Ω_p^{II} 和 Ω_p^{III} 两两不相交。此外，只要取 p_0 足够大，就可以保证对于所有 $p > p_0$ 都有 $|\Omega_p^I| = \ell_f$，并且对于 $p \in (p_0, z_0] \cup (z_1, \sqrt{y})$ 有 $|\Omega_p^{II}| = r_p(q_1) + \ldots + r_p(q_{h_f})$。另外，根据定义，对于所有 $z_0 < p \le z_1$，都有 $|\Omega_p^{III}| = M_p(f)$。因此，

$$\sum_{p \le \sqrt{y}} \frac{g(p)}{p} = \sum_{p_0 < p \le \sqrt{y}} \frac{\ell_f}{p} + \sum_{h \le h_f} \sum_{p \in (p_0, z_0] \cup (z_1, \sqrt{y})} \frac{r_p(q_h)}{p} + \sum_{z_0 < p \le z_1} \frac{M_p(f)}{p}.$$

根据默滕斯定理，第一个求和式为

$$\sum_{p_0 < p \le \sqrt{y}} \frac{\ell_f}{p} = \ell_f \ln\ln y + O(1).$$

引理 2 给出，对每个 $h \le h_f$

$$\sum_{p\in(p_0,z_0]\cup(z_1,\sqrt{y})} \frac{r_p(q_h)}{p} = \ln\ln y - \ln\ln z_1 + \ln\ln z_0 + O(1).$$

最后，根据 $M(f)$ 的定义，第三个和可以计算为

$$\sum_{z_0<p\le z_1} \frac{M_p(f)}{p} = M(f)(\ln\ln z_1 - \ln\ln z_0) + O(1).$$

将上述所有结果代入我们的估计，得到

$$S(m,\Omega) \ll m(\ln y)^{-\ell_f} \left(\frac{\ln z_1}{\ln y \ln z_0}\right)^{h_f} \left(\frac{\ln z_0}{\ln z_1}\right)^{M(f)} =$$

$$= m(\ln y)^{-\ell_f} \left(\frac{\ln\ln\ln y}{A^2(\ln\ln y)^2}\right)^{h_f} \left(\frac{A^2(\ln\ln y)^2}{\ln y \ln\ln\ln y}\right)^{M(f)} = \frac{A^{2M(f)-2h_f} y}{B\ln y}.$$

由于隐含常数不依赖于 A 和 B，我们可以取足够大的 B，从而得到

$$S(m,\Omega) \le \frac{y}{4\ln y},$$

因此

$$R \le S(m,\Omega) + o(y/\ln y) \le \frac{y}{3\ln y}.$$

由于在第三步中我们有 $\pi(y) - \pi(y/2) = \dfrac{y}{(2+o(1))\ln y}$ 个素数位于左侧，因此可以一次筛去剩余数字中的一个，以确保每个数字 $i \le m$ 都在这三步中被筛去。证明完毕。

□

3 $M(f)$ 的计算

在本节中，我们证明关于 $M(f)$ 的值的定理 2。量 $M(f)$ 是 p 的素数值上 $M_p(f)$ 的对数平均值。数 $M_p(f)$ 定义为：对于固定的非零 $y \in \mathbb{F}_p$，$f(x) = y$ with $x \in \mathbb{F}_p$ 的解的最大个数。我们将证明 $M(f)$ 总是存在且为有理数，并将其计算归结为群作用。

在引言中，我们将 $f(x)$ 与若干伽罗瓦群联系起来，这些群自然地作用在集合 X 上，该集合包含方程 $f(x) - y$ 的所有根，其中 y 是一个形式变量。具体而言，G_f 是 $f(x) - y$ 在 $\mathbb{Q}(y)$ 上的伽罗瓦群，而 G_f^+ 是同一多项式在 $K(y)$ 上的伽罗瓦群。容易看出，G_f^+ 是 G_f 的正规子群。事实上，显然 K 是 $\mathbb{Q}$ 的有限正规扩张。若 G_f^0 是其伽罗瓦群，则存在一个自然的满同态 $\pi : G_f \to G_f^0$。更确切地说，$f(x) - y$ 在 $\mathbb{Q}(y)$ 上的分裂域的每个自同构都会将常数映到常数。当且仅当所有常数元素都保持不变时，这样的自同构才是 $K(y)$ 上的自同构，因此 $G_f^+ = \ker\pi$ 是一个正规子群。

伯奇和斯温纳顿-戴尔 [7] 能够将关于$f(x) = y$ 的解的数量问题归结为某些其他伽罗瓦群。

引理 3. 设 G_p^+为 $f(x) - y$ 在 $\overline{\mathbb{F}}_p(y)$ 上的伽罗瓦群， G_p 为同一多项式在 $\mathbb{F}_p(y)$ 上的伽罗瓦群。对于 $n \leq d = \deg f$，设 m_n 为 G_p^+作用于 $f(x) = y$的互异根组成的有序 n-元组时的 G_p-不变轨道数。那么，对于 $m_n = 0$，方程组 $f(x_1) = f(x_2) = \ldots = f(x_n)$ 在 $\mathbb{F}_p$中当 $x_i \neq x_j$时无解；而对于 $i \neq j$，解的数量为

$$m_n p + O(\sqrt{p}).$$

为方便起见，我们来表述切博塔廖夫密度定理。首先，定义弗罗贝尼乌斯元素。

定义。设 $K/\mathbb{Q}$ 是一个有限伽罗瓦扩张， $\mathcal{O}_K$ 是其整数环， G_K 是其伽罗瓦群。假设 p 是一个未分歧有理素数，且 $\mathfrak{p} \subset \mathcal{O}_K$ 是位于 p之上的一个素理想。 $\mathfrak{p}$ 的弗罗贝尼乌斯元素是满足下式的元素 $\sigma_\mathfrak{p} \in G_K$

$$\sigma_\mathfrak{p} x \equiv x^p \pmod{\mathfrak{p}}$$

对所有 $x \in \mathcal{O}_K$均成立。

对于位于固定素数 p 之上的不同素理想 $\mathfrak{p}$，弗罗贝尼乌斯元素彼此共轭，因此我们可以在共轭意义下定义弗罗贝尼乌斯元素 σ_p。

切博塔廖夫密度定理表述如下

引理 4。设 $K/\mathbb{Q}$ 是一个伽罗瓦群为 G_K的有限伽罗瓦扩张。假设 $C \subset G_K$是一个共轭类，且 $\pi(x; K, C)$ 表示满足弗罗贝尼乌斯元素 σ_p 属于 C的素数 $p \leq x$ 的数量。那么对于某个 $c_K > 0$，有

$$\pi(x; G_K, C) = \frac{|C|}{|G_K|} li(x) + O(xe^{-c_K\sqrt{\ln x}}).$$

证明。参见 [6]。 □

现在我们来证明定理 2。

定理 2 的证明。在 [7] 中已证明，对于足够大的 p，群 G_p^+ 可以视为 $f(x) - y$ 关于 $\mathbb{C}(y)$ 的伽罗瓦群。容易看出，该群与G_f^+ 一致。接下来，大素数 p 在 K中不分歧，因此我们固定一个位于 p 上方、属于 $\mathcal{O}_K$ 的素理想 $\mathfrak{p}$，并考虑相应的弗罗贝尼乌斯元素 $\sigma_\mathfrak{p}$。$(\mathbb{F}_p)^f$ 的最大常数子域可以视为 $\mathcal{O}_K/\mathfrak{p}$。此外， G_p 通过弗罗贝尼乌斯自同构及其幂作用于常数。对于较大的 p，群 G_p 由 G_f^+ 和 $\sigma_\mathfrak{p}$ 的原像生成，即

$$G_p = \langle \pi_p^{-1}(\sigma_\mathfrak{p}), G_f^+ \rangle,$$

其中π_p 是 G_p–对常数的作用所对应的限制同态（其像是 $\mathcal{O}_K/\mathfrak{p}$ 在 $\mathbb{F}_p$上的伽罗瓦群），因此我们可以将 G_p视为 G_f的子群。设 $\pi_p^{-1}(\sigma_\mathfrak{p})$中的任意元素为 g。下面证明，在这种情况下，满足 $m_n > 0$ 的最大 n 等于 $\max_{h \in G_f^+} |X^{hg}|$。事实上，$G_f^+$ 是 G_p的正规子群，因此后者由 g 和G_f^+ 生成；所以，一个 G_f^+–轨道在 G_p–下不变，当且仅当它在 g下不变。这意味着，如果我们的轨道具有 $G_f^+(x_1, \ldots, x_n)$的形式，那么对任意 $h_1 \in G_f^+$，必存在 $h_2 \in G_f^+$ 使得

$$gh_2(x_1, \ldots, x_n) = h_1(x_1, \ldots, x_n).$$

子群 G_f^+ 是正规子群，因此存在 h_3 使得 $gh_2 = h_3g$。因此，我们的条件等价于：对任意 h_3，都可以找到 h_1，使得 $x_1,\dots,x_n$ 在 hg作用下不变，其中 $h = h_1^{-1}h_3$。这就证明了所需的恒等式。因此，当 p 充分大时，数 $M_p(f)$等于 $\max_{h\in G_f^+}|X^{hg}|$，其中 $g \in \pi_p^{-1}(\sigma_\mathfrak{p}) \subset \pi_p^{-1}(\sigma_p) =: C$，而$\sigma_p$ 是$\sigma_\mathfrak{p}$ 在 G_f^0中的共轭类。由于 G_f^+ 是正规子群，这个数不取决于 g 和 $\mathfrak{p}$的选取。切博塔廖夫密度定理表明

$$\sum_{p\le x} M_p(f) = \sum_{C, g_0\in C} \frac{|C|}{|G_f^0|} \max_{h\in G_f^+} |X^{h\pi_p^{-1}(g_0)}| li(x) + O(xe^{-c_K\sqrt{\ln x}}) =$$

$$li(x)\frac{1}{|G_f^0|}\sum_{g_0\in G_f^0} \max_{h\in G_f^+} |X^{h\pi_p^{-1}(g_0)}| + O(xe^{-c_K\sqrt{\ln x}}),$$

其中，C在第一个求和中遍历 G_f^0的所有共轭类。接下来，$G_f^0 = G_f/G_f^+$和最大值$_h\,|X^{hg}|$ 仅取决于商群 G_f/G_f^+ 中 $g \in G_f$所属的共轭类。这意味着最后一个求和等于 $m(G_f, G_f^+; X)$。因此，

$$\sum_{p\le x} M_p(f) = m(G_f, G_f^+; X) li(x) + O(xe^{-c_K\sqrt{\ln x}})$$

通过分部求和，我们得到

$$\sum_{p\le x} \frac{M_p(f)}{p} = m(G_f, G_f^+; X)\ln\ln x + O(1),$$

由此证明得证。 □

注 2. 对于一些自然的例子，数值 $m(G, H; X)$结果为整数，至少在 H 是 G的正规子群，且 G 和 H 的作用都忠实且传递时如此。然而，也存在非整数性的例子：群 $G = S_4 \times \mathbb{Z}/2\mathbb{Z}$ 在含有 6 个元素的集合 X 上传递作用。取 $H = A_4$，我们得到 $m(G, H; X) = \frac{7}{2}$。这个例子由 Peter Kosenko 找到，他还为 $|X| = 8$、9 和 10 找到了一些非整数性的例子。顺便一提，$S_4 \times \mathbb{Z}/2\mathbb{Z}$ 是一般偶六次多项式的伽罗瓦群。遗憾的是，我们未能构造出次数为 6 且满足 $G_f = S_4 \times \mathbb{Z}/2\mathbb{Z}$ 和 $G_f^+ = A_4$的多项式 $f(x)$的例子。

既然现在我们有了计算 $M(f)$ 的工具，就来求 f_d 以及一个典型的 d 次多项式的 $M(f)$。如果 $G_f^+ \cong S_d$，我们就称次数为 d 的多项式为一般多项式。

定理 3. 设 d 为整数。

i) 我们有 $M(x^d) = \tau(d)$，其中 $\tau(d)$ 是因子函数。

ii) 对于任意次数为 d 的一般多项式 $f(x)$，我们有 $M(f) = d$。

证明。为证明第一部分，注意，对于 $f(x) = x^d$，我们有

$$M_p(f) = (p-1, d).$$

事实上，在这种情况下很容易看出，如果 $y \neq 0$ 和 $x^d = y$ 至少有一个解，那么解的数量等于 $\mathbb{F}_p$中的 d–次单位根的数量。接下来，利用恒等式

$$(d, p-1) = \sum_{d_1 | (d, p-1)} \varphi(d_1),$$

对于任意 $x \geq$，我们得到 2

$$\sum_{p \leq x} \frac{M_p(f_d)}{p} = \sum_{p \leq x} \frac{(d, p-1)}{p} =$$

$$= \sum_{p \leq x} \frac{\sum_{d_1 | (d, p-1)} \varphi(d_1)}{p} = \sum_{d_1 | d} \varphi(d_1) \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{d_1}}} \frac{1}{p}.$$

接下来，由等差数列素数定理可得

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{d_1}}} \frac{1}{p} = \frac{\ln \ln x}{\varphi(d_1)} + O(1).$$

将此恒等式代入上面的公式，我们得到所需的恒等式：因子$\varphi(d_1)$ 和 $\varphi^{-1}(d_1)$ 相互抵消，剩下求和式 $\sum_{d_1 | d} 1 \equiv \tau(d)$。此证明不依赖于定理 2，但可以很容易地改写为仿射群 Aff$(\mathbb{Z}/d\mathbb{Z})$ 在 $\mathbb{Z}/d\mathbb{Z}$ 上的自然作用的表述。事实上，在我们的情形下， $K = \mathbb{Q}(\zeta_d)$ 是分圆域。 $\mathbb{Q}_f$ 的每个自同构都将 ζ_d 映射到某个 $a \in (\mathbb{Z}/d\mathbb{Z})^*$ ，并将 y 映射到某个 $b \in \mathbb{Z}/d\mathbb{Z}$。映射 $(a, b) \mapsto ($ $x \mapsto ax + b)$ 是到 Aff$(\mathbb{Z}/d\mathbb{Z})$ 的同构 $G_f \cong$ 。由于 G_f^+ 固定 ζ_d，我们还看到 G_f^+ 对应于平移子群 $y \mapsto y + b$ ，并且与 $\mathbb{Z}/d\mathbb{Z}$ 同构。A

s f或一般的ic polynomial数，我们 have $G_f^+ \cong S_d$, hence $G_f = G_f^+$ and for all $g \in G_f$

$$\max_{h \in G_f^+} |X^{gh}| = |X^e| = d,$$

按需进行。 □

论文 [7] 还包含其他内容，其中提出了一些判据，用于判断 $f(x)$ 是否为一般多项式。特别地，作者证明，若 $f'(x)$ 有单根，且任意两个不同的根都满足 $f(\alpha) \neq f(\beta)$，则 $f(x)$ 是一般多项式。当然，这意味着任何非一般多项式的系数都必须满足某种多项式关系。进而可知，次数为 d 的大多数多项式都是一般多项式。

显然，我们对一般多项式证明 $M(f) = d$ 时，只用到了 $G_f = G_f^+$。显然，后一个条件实际上等价于 $M(f) = d$。由于 $G_f^0 = G_f / G_f^+$，它也等价于 $K = \mathbb{Q}$，即 $\mathbb{Q}_f$ 中的所有常数都是有理数。我们将这类多项式称为普通多项式。

目前，除了 Birch and Swinnerton-Dyer 提出的更狭义判据外，我们还不知道有什么简单方法可以检验给定的多项式是否为普通多项式。
我们称为一般的多项式，在 J.-P. Serre 关于伽罗瓦理论的书中被称为莫尔斯函数 [8, 第 4 节 4]。书中还提到，Hilbert 为所有这类多项式建立了一个同构$G_f \cong S_n$ 另见 [9]

与关于素数间隔的结果类似，我们的结果推出以下结论

推论 2. 对于任意 $f(x) \in \mathbb{Z}[x]$，存在一个常数 $c_f > 0$，使得对于所有 $X \geq e^{16}$，都存在一个正整数 $n \leq X$，满足对于所有 $1 \leq m \leq Y$，$\Omega(n + f(m)) > A(n)$，其中

$$Y = c_f \ln X (\ln \ln X)^{\ell_f - 1} \left(\frac{(\ln \ln \ln X)^2}{\ln \ln \ln \ln X} \right)^{h_f} \left(\frac{\ln \ln X \ln \ln \ln \ln X}{(\ln \ln \ln X)^2} \right)^{M(f)},$$

Ω 表示按重数计数的素因子个数，而 $A(n)$ 表示 $f(x) + n$ 的不可约因子个数。

还可以注意到，我们的证明可以推广到不一定属于 $\mathbb{Z}[x]$ 的整值多项式 $f(x)$。

4 致谢

我们感谢 Peter Kosenko 提供了一个关于 $m(G, H; X)$ 非整数性的抽象例子（见注 2），也感谢 MathOverflow 用户 Joachim K¨onig 提供了定理 2 证明的主要思路：https://mathoverflow.net/a/430001/101078。我们还感谢匿名审稿人指出了若干不准确之处，尤其是第 3 节中的问题，并提供了 Serre 和 Hilbert 的相关参考文献。

本工作在斯捷克洛夫国际数学中心完成，并得到俄罗斯联邦科学与高等教育部的资助（协议编号：075-15-2022-265）。第一作者得到国立高等经济大学基础研究计划的资助。

参考文献

[1] K. Ford、B. Green、S. Konyagin、J. Maynard、T. Tao，《素数间的长间隔》，美国数学会杂志，31:1（2018），65–105。[2] H. Iwaniec，《关于雅各布斯塔尔问题》，数学论证 11（1978），第 1 期，225–231。[3] R. A. Rankin，《相邻素数之差》，伦敦数学会杂志 13（1938），242-247。[4] R. Dietmann、C. Elsholtz、A. Kalmynin、S. Konyagin、J. Maynard，《二元二次型取值之间的更长间隔》，国际数学研究通知（2022）。[5] H. Halberstam、H. E. Richert，《筛法》，伦敦；纽约：学术出版社（1974）。[6] J.C. Lagarias 和 A.M. Odlyzko，《切博塔廖夫定理的有效版本》，《代数数域》：409–464，1977。[7] B.J. Birch、H.P.F. Swinnerton-Dyer，《关于乔拉问题的注记》，算术学报 5（1959），417-423。[8] J.-P. Serre，《伽罗瓦理论专题》（第 2 版）。A K Peters/CRC 出版社（ 2007 ）。[9] D. Hilbert，《关于具有整数系数的整有理函数的不可约性》，克雷勒杂志 110（1892），104-129