一道 CGMO 试题的加强与命题背景

赖力

(复旦大学, 200433)

2020 年中国女子数学奥林匹克 (CGMO) 于 8 月上旬在江西省鹰潭市第一中学成功举办. 试题中第一天第四题由我提供:

问题 1 设 p, q 是两个不同的素数, $p > q$. 证明: $p! - 1$ 与 $q! - 1$ 的最大公约数不超过 $p^{\frac{p}{3}}$.

问题 1 的解答可参考文 [1], 这里不再重复. 本文的目的有两重, 一是给出问题 1 的加强版本与证明; 二是介绍问题 1 的命题来源.

1. 问题的加强

本文中我们使用记号 $\gcd(x, y)$ 与 $\mathrm{LCM}[x, y]$ 分别表示两个整数 x, y 的最大公约数与最小公倍数. 我们用 $\exp(x)$ 表示指数函数 e^x. 对一个素数 p, 记号 $v_p(m)$ 表示正整数 m 含 p 的幂次, 即满足 $p^k \mid m$ 的最大的非负整数 k.

如果使用一些关于素数分布的结论, 则问题 1 中对于 p, q 是素数的这一要求可以去掉. 事实上, 下面我们首先将利用 Bertrand 假定 (对于任何正整数 $m \geqslant 2$, 区间 $\left(\frac{m}{2}, m\right]$ 中均存在素数) 和足够简单的工具来证明如下命题:

命题 1 对任意的 $\varepsilon > 0$, 存在仅依赖于 ε 的常数 C_ε, 使得对于任何两个不同的正整数 a, b, 其中 $a > b > 1$, 如果 $a > C_\varepsilon$, 则 $\gcd(a! - 1, b! - 1) \leqslant a^{\varepsilon a}$.

其次, 我们将使用复杂一些的办法来证明一个更强的命题:

命题 2 存在一个绝对常数 $C > 0$, 使得对于任何两个不同的正整数 a, b, 其中 $a > b > 1$, 我们有 $\gcd(a! - 1, b! - 1) \leqslant \exp(Ca\sqrt{\ln a})$.

除了需要引用 Bertrand 假定和素数定理, 我们证明命题 1 和命题 2 使用到

修订日期: 2020-09-16.

的知识均不超出高中数学竞赛的范围.

以上两个命题 (以及问题 1) 的证明的关键点是如下的观察: 对于任意两个正整数 u, v, 我们有

$$\gcd(a!-1,b!-1)\mid\frac{a!^u-b!^v}{\gcd(a!^u,b!^v)}.$$

这是因为, 记 $D=\gcd(a!-1,b!-1)$, 由 $a!\equiv b!\equiv 1 \pmod D$ 可得到 $a!^u-b!^v\equiv 0 \pmod D$, 即 $D\mid a!^u-b!^v$, 再注意到 D 与 $a!$, $b!$ 均互素, 从而 $D\mid\frac{a!^u-b!^v}{\gcd(a!^u,b!^v)}$. 接下来我们的思路是选取合适的 u, v 使得 $\frac{a!^u-b!^v}{\gcd(a!^u,b!^v)}$ 是一个非零的整数且绝对值尽可能小, 这样我们可以通过 $D\leqslant\frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)}$ 来得到 D 的上界估计.

我们先排除掉 $a!^u-b!^v=0$ 的可能. 下面引理 1 的这个简洁证明是重庆南开中学的周哲欧同学告诉我的:

引理 1 设 a, b, u, v 是正整数, $a>b$. 则 $a!^u-b!^v\neq 0$.

证明 设 p 是不超过 a 的最大的素数. 根据 Bertrand 假定, 我们有

$$\frac{a}{2}<p\leqslant a.$$

如果 $p>b$, 那么 p 整除 $a!$ 但不整除 $b!$, 从而 $a!^u-b!^v\neq 0$. 如果 $p\leqslant b$, 则因为 $\frac{b}{2}<\frac{a}{2}<p\leqslant b<a$, 我们有 $v_p(a!)=v_p(b!)=1$. 假设 $a!^u=b!^v$, 比较两端含 p 的幂次推出 $u=v$, 于是 $a!=b!$, $a=b$, 矛盾. 所以总有 $a!^u-b!^v\neq 0$. 得证. □

下面的引理 2 给出 $\gcd(a!^u,b!^v)$ 的一个下界估计, 它已满足证明命题 1 的需要. 稍后我们将使用更多的工具证明引理 2 的一个加强版本 (见引理 6) 来证明命题 2.

引理 2 设 a, b, u, v 是正整数, 则 $\gcd(a!^u,b!^v)\geqslant\frac{\min\{ua,vb\}!}{u^{ua}v^{vb}}$.

证明 记 $A=\frac{(ua)!}{a!^u}$, $B=\frac{(vb)!}{b!^v}$. 回忆, 作为二项式定理的推广, 我们有

$$(x_1+x_2+\cdots+x_n)^m=\sum_{\substack{m_1+m_2+\cdots+m_n=m\\ m_1,m_2,\cdots,m_n\geqslant 0}}\frac{m!}{m_1!m_2!\cdots m_n!}x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n},$$

取 $m=ua$, $n=u$, $x_1=x_2=\cdots=x_n=1$ 我们得到

$$A\leqslant(\underbrace{1+1+\cdots+1}_{u\text{ 个}})^{ua}=u^{ua}.$$

同理, $B\leqslant v^{vb}$.

由于 $\gcd(a!^u,b!^v)=\frac{\gcd(a!^uAB,b!^vAB)}{AB}$, 而根据 A, B 的定义, $a!^uAB$, $b!^vAB$ 分别是 $(ua)!$, $(vb)!$ 的倍数, 从而

$$\gcd(a!^u,b!^v)\geqslant\frac{\min\{ua,vb\}!}{AB}\geqslant\frac{\min\{ua,vb\}!}{u^{ua}v^{vb}}.$$

引理 2 得证. $\square$

我们还需要对阶乘的大小的估计. 著名的 Stirling 公式告诉我们当 $m \to +\infty$ 时 $m! \sim \sqrt{2\pi m}\left(\frac{m}{e}\right)^m$ (这里记号 $f(m) \sim g(m)$ 表示 $\lim_{m\to+\infty}\frac{f(m)}{g(m)} = 1$). 我们并不需要如此精确的估计, 下面的引理 3 已足够实用:

引理 3 对任意正整数 m, 不等式 $m! \geqslant \left(\frac{m}{e}\right)^m$ 成立.

证明 我们对 m 归纳. $m = 1$ 时显然. 假设已知 $m! \geqslant \left(\frac{m}{e}\right)^m$, 那么

$$(m+1)! = (m+1)\cdot m! \geqslant (m+1)\cdot\left(\frac{m}{e}\right)^m,$$

故为证 $(m+1)! \geqslant \left(\frac{m+1}{e}\right)^{m+1}$, 只用证 $e \geqslant \left(1+\frac{1}{m}\right)^m$, 而这是熟知的(数列 $\left(1+\frac{1}{m}\right)^m$ 关于 m 单调递增, 极限为 e). 引理 3 得证. $\square$

下面的引理 4 是基本的抽屉原理方法:

引理 4 设 a, b 是正整数, $a > b$. 则对任何实数 $U \geqslant 1$, 存在一组整数 $(u,v) \neq (0,0)$, 满足 $|u|,|v| \leqslant U$ 并且

$$|ua - vb| \leqslant \frac{2a}{U}.$$

证明 考虑以下 $([U]+1)^2$ 个数: $ia + jb\ (0 \leqslant i, j \leqslant [U])$, 它们均属于区间 $[0, 2[U]a]$. 由抽屉原理, 存在两组指标 $(i_1, j_1) \neq (i_2, j_2)$ 使得

$$|(i_1a + j_1b) - (i_2a + j_2b)| \leqslant \frac{2[U]a}{([U]+1)^2 - 1} \leqslant \frac{2a}{U}.$$

取 $u = i_1 - i_2$, $v = j_2 - j_1$, 则 $(u,v) \neq (0,0)$, $|u|,|v| \leqslant U$, 且 $|ua - vb| \leqslant \frac{2a}{U}$. 我们完成了引理 4 的证明. $\square$

现在我们可以证明命题 1 了.

命题 1 的证明 记 $D = \gcd(a!-1, b!-1)$. 取 $U = \max\{\frac{4}{\varepsilon}, 1\}$. 由引理 4, 存在一组整数 $(u,v) \neq (0,0)$, 满足 $|u|,|v| \leqslant U$, 且 $|ua - vb| \leqslant \frac{2a}{U}$. 如果 $uv \leqslant 0$, 则

$$b = \min\{a,b\} \leqslant |ua - vb| \leqslant \frac{2a}{U},$$

于是从 $D \mid (b!-1)$ 推出

$$D \leqslant b! - 1 \leqslant a^b \leqslant a^{\frac{2a}{U}} \leqslant a^{\frac{\varepsilon a}{2}},$$

已得证. 下面设 $uv > 0$, 如有必要, 将 (u,v) 换成 $(-u,-v)$, 我们可不妨设 u, v 均为正整数.

根据引理 1 以及引理 1 之前的讨论, 我们知道 D 整除 $\frac{|a!^u - b!^v|}{\gcd(a!^u, b!^v)}$, 并且

$\frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)} \neq 0$, 从而 $D \leqslant \frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)}$. 由显然的不等式

$$|a!^u - b!^v| \leqslant \max\{a!^u, b!^v\} \leqslant a^{\max\{ua,vb\}}$$

以及引理 2 和引理 3, 我们推出

$$\begin{aligned} D &\leqslant \frac{|a!^u - b!^v|}{\gcd(a!^u, b!^v)} \\ &\leqslant \frac{a^{\max\{ua,vb\}}U^{2Ua}}{\min\{ua, vb\}!} \qquad \text{(引理 2)} \\ &\leqslant \frac{a^{\max\{ua,vb\}}U^{2Ua}e^{Ua}}{\min\{ua, vb\}^{\min\{ua,vb\}}} \qquad \text{(引理 3)} \\ &= a^{|ua-vb|}\left(\frac{a}{\min\{ua, vb\}}\right)^{\min\{ua,vb\}} (e^U U^{2U})^a. \end{aligned}$$

简单的求导分析可知函数 $x \mapsto \left(\frac{a}{x}\right)^x$ $(x > 0)$ 在 $x = \frac{a}{e}$ 时取最大值 $e^{\frac{a}{e}}$. 由于 $|ua - vb| \leqslant \frac{2a}{U}$, 我们得到

$$D \leqslant a^{\frac{2a}{U}} \left(e^{U+\frac{1}{e}}U^{2U}\right)^a.$$

回忆 $U = \max\{\frac{4}{\varepsilon}, 1\}$, 记 $C_\varepsilon = \left(e^{U+\frac{1}{e}}U^{2U}\right)^{\frac{2}{\varepsilon}}$, 这是一个仅依赖于 ε 的常数. 当 $a \geqslant C_\varepsilon$ 时, 我们有 $D \leqslant a^{\frac{\varepsilon a}{2}} \cdot a^{\frac{\varepsilon a}{2}}$, 这便完成了命题 1 的证明. □

2. 命题 2 的证明

为方便, 我们将使用 Landau 的 O 与 o 符号: 对于两个函数 $f(x)$, $g(x)$, 我们用 $f(x) = O(g(x))$ 表示存在一个常数 $C > 0$ 使得 $|f(x)| \leqslant Cg(x)$ 在定义域上恒成立; 我们用 $f(x) = o(g(x))$ 表示 $\lim \frac{f(x)}{g(x)} = 0$, 其中极限需另外说明, 例如我们用"当 $x \to +\infty$ 时 $x^2 = o(e^x)$" 表示 $\lim\limits_{x\to+\infty} \frac{x^2}{e^x} = 0$. 当我们使用记号 p 时将默认 p 是素数, 例如 $\sum\limits_{p\leqslant a} p$ 表示所有不超过 a 的素数的和.

初等数论中的一个熟知的结果是 $\sum\limits_{p\leqslant N} \frac{\ln p}{p} = \ln N + O(1)$. 其证明可以从 $N!$ 的素因子分解出发来得到(这通常被称作 Chebyshev 类型的估计). 限于我们的目的以及为了提高本节的自完备性, 我们下面给出 $\leqslant$ 这部分的证明:

引理 5 对任何正整数 $N \geqslant 2$, 我们有

$$\sum_{p\leqslant N} \frac{\ln p}{p} \leqslant \ln N + O(1).$$

证明 我们有 $\ln(N!) = \sum\limits_{p\leqslant N} v_p(N!) \ln p$. 熟知 $v_p(N!) = \sum\limits_{i=1}^{\infty} \left[\frac{N}{p^i}\right]$, 故

$$v_p(N!) \geqslant \frac{N}{p} - 1,$$

从而 $\sum\limits_{p\leqslant N}\left(\frac{N}{p}-1\right)\ln p\leqslant N\ln N$, 于是

$$\sum_{p\leqslant N}\frac{\ln p}{p}\leqslant \ln N+\frac{1}{N}\sum_{p\leqslant N}\ln p.$$

对任意正整数 m, 显然 $\prod\limits_{m<p\leqslant 2m}p\mid\binom{2m}{m}$, 故 $\sum\limits_{m<p\leqslant 2m}\ln p\leqslant(2\ln 2)m$. 在前式中取 m 为 2 的方幂并累加, 我们得到 $\sum\limits_{p\leqslant 2^{M+1}}\ln p\leqslant(4\ln 2)2^M$ 对任何正整数 M 成立. 取 $M=[\log_2 N]$ 推出 $\sum\limits_{p\leqslant N}\ln p\leqslant(4\ln 2)N$, 故

$$\sum_{p\leqslant N}\frac{\ln p}{p}\leqslant \ln N+4\ln 2,$$

引理 5 得证. □

推论 $\sum\limits_{p\leqslant N}\frac{\ln p}{p-1}\leqslant \ln N+O(1)$.

只需注意到 $\sum\limits_{p\leqslant N}\frac{\ln p}{p(p-1)}=O(1)$ 即可.

下面的引理 6 是引理 2 的改进:

引理 6 设 a, b, u, v 是正整数, $a>b$. 则当 $a\to+\infty$ 时我们有

$$\ln\left(\frac{a!^u}{\gcd(a!^u,b!^v)}\cdot\frac{b!^v}{\gcd(a!^u,b!^v)}\right)\leqslant|ua-vb|\,(\ln a+O(1))+(2+o(1))\max\{u,v\}a.$$

证明 熟知对任意正整数 m 和素数 p, 我们有 $v_p(m!)=\frac{m-S_p(m)}{p-1}$, 其中 $S_p(m)$ 表示 m 在 p 进制下的各位数字之和. 我们用 LHS 表示引理 6 中欲证不等式的左端, 则

$$\begin{aligned}\text{LHS}=\ln\left(\frac{\text{LCM}[a!^u,b!^v]}{\gcd(a!^u,b!^v)}\right)&=\sum_{p\leqslant a}|uv_p(a!)-vv_p(b!)|\ln p\\&=\sum_{p\leqslant a}\left|\frac{(ua-uS_p(a))-(vb-vS_p(b))}{p-1}\right|\ln p\\&\leqslant|ua-vb|\sum_{p\leqslant a}\frac{\ln p}{p-1}+\sum_{p\leqslant a}\frac{|uS_p(a)-vS_p(b)|}{p-1}\ln p.\end{aligned}$$

对于任何素数 $p\leqslant a$ 和正整数 $m\in\{a,b\}$, 由显然的不等式

$$S_p(m)\leqslant(p-1)(1+[\log_p m])\leqslant 2(p-1)\log_p a,$$

以及引理 5 的推论, 我们得到

$$\text{LHS}\leqslant|ua-vb|\,(\ln a+O(1))+2\max\{u,v\}\ln a\sum_{p\leqslant a}1,$$

再由素数定理知 $\sum\limits_{p\leqslant a}1=(1+o(1))\frac{a}{\ln a}$, 代入上式便完成了引理 6 的证明. □

下面我们证明命题 2.

命题 2 的证明 记 $D=\gcd(a!-1,b!-1)$. 在引理 4 中取 $U=\sqrt{\ln a}$, 则存在整数对 $(u,v)\neq(0,0)$, $|u|,|v|\leqslant U$ 使得 $|ua-vb|\leqslant\frac{2a}{U}$. 如果 $uv\leqslant 0$, 则

$$b=\min\{a,b\}\leqslant|ua-vb|\leqslant\frac{2a}{U},$$

于是从 $D\mid(b!-1)$ 推出

$$D\leqslant b!-1\leqslant a^b\leqslant a^{\frac{2a}{U}}=\exp\left(2a\sqrt{\ln a}\right).$$

以下我们考虑 $uv>0$ 的情况, 此时可不妨设 u, v 均是正整数.

根据引理 1 以及引理 1 之前的讨论, D 整除 $\frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)}\neq 0$. 于是

$$\begin{aligned}
D\leqslant\frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)}&\leqslant\max\left\{\frac{a!^u}{\gcd(a!^u,b!^v)},\frac{b!^u}{\gcd(a!^u,b!^v)}\right\}\\
&\leqslant\frac{a!^u}{\gcd(a!^u,b!^v)}\cdot\frac{b!^v}{\gcd(a!^u,b!^v)}\\
&\leqslant\exp\left(\frac{2a}{U}(\ln a+O(1))+(2+o(1))Ua\right)\quad(\text{引理 }6)\\
&=\exp\left((4+o(1))a\sqrt{\ln a}\right),\qquad(\text{因为 }U=\sqrt{\ln a})
\end{aligned}$$

这便完成了命题 2 的证明. □

若对引理 4 和引理 6 更仔细地分析, 我们可以改进估计

$$D\leqslant\exp\left((4+o(1))a\sqrt{\ln a}\right)$$

中的常数 4. 但若想进一步改进量级, 可能需要非平凡的新的想法. 回忆我们的出发点是 D 整除 $\frac{|a!^u-b!^v|}{\gcd(a!^u,b!^v)}$, 这还是以一种比较特殊的方式用到了 $D=\gcd(a!-1,b!-1)$ 的定义. 或许我们能有其它的出发点来得到更好的估计. 利用和命题 2 证明同样的想法(以及带误差项估计的素数定理), 我们可以证明一个更一般的结果, 以下只给出叙述而不加以证明了:

命题 3 *给定正整数 $k\geqslant 2$, 则存在一个仅依赖于 k 的常数 $C_k>0$, 使得对任何正整数 $a\geqslant k+1$, 对区间 $[2,a]$ 中任何 k 个两两不同的正整数 $a_1,a_2,\cdots,a_k$ 以及任意的 $\delta_i\in\{\pm1\}$ $(i=1,2,\cdots,k)$, 我们总有*

$$\gcd\left(a_1!+\delta_1,a_2!+\delta_2,\cdots,a_k!+\delta_k\right)\leqslant\exp\left(C_ka(\ln a)^{\frac{1}{k}}\right).$$

3. 问题的来源

$n!\pm1$ 型的正整数的素因子分布是一个有趣的问题. 下面我们用记号

$P(n!+1)$ 表示 $n!+1$ 的最大素因子.

对一个奇数 k, 若 p 是 $k!+1$ 的一个素因子, 则由 Wilson 定理可推出 p 也是 $(p-k-1)!+1$ 的素因子, 由此不难证明存在无穷多个正整数 n 使得 $P(n!+1)>2n$ (细节留给读者).

1976 年, P. Erdös 和 C. L. Stewart [6] 证明了存在常数 $\varepsilon_0>0$, 使得有无穷多个正整数 n 满足 $P(n!+1)>(2+\varepsilon_0)n$. 2004 年, F. Luca 和 I. E. Shparlinski [2] 证明了对任何正实数 $\varepsilon>0$, 存在无穷多个正整数 n 满足 $P(n!+1)>(2.5-\varepsilon)n$. 同年, Stewart [3] 将常数 2.5 改进到 5.5. 另外我们需要提及, 在 2002 年, M. R. Murty 和 S. Wong [4] 证明了若 ABC 猜想成立, 则对任意的正整数 n, 当 $n\to+\infty$ 时有 $P(n!+1)\geqslant(1+o(1))n\ln n$.

Luca, Shparlinski 以及 Stewart 的证明是初等的, 其思路和 Chebyshev 尝试证明素数定理的经典思路一致. 我们将 Stewart (的一个弱化版本)的证明过程整理成下面的练习题, 供有兴趣的同学自行完成. 其中第 (3) 小问的证明方法和 2009 年集训队的一道试题的方法一致, 其证明源自于 1976 年 Stewart 的博士论文 [5]. 第 (6) 小问将使用素数定理以及它的一个推论, 同学们可以承认它们而不必证明.

练习题 [3] 本题的目标是证明如下结论: 给定 $\varepsilon>0$, 存在无穷多个正整数 n, 使得 $n!+1$ 有一个素因子 $>(2.5-\varepsilon)n$. 我们用反证法, 取定一个实数 $\gamma<2.5$ $(\gamma>1)$, 假设存在 n_0 使得当 $n\geqslant n_0$ 时 $n!+1$ 的所有素因子均 $\leqslant\gamma n$.

(1) 取充分大的正整数 N (N 大于一个仅依赖于 n_0 的常数), 记

$$Z=\prod_{n=n_0}^{N}(n!+1).$$

证明: $\ln Z\geqslant\frac{1}{2}N^2\ln N-100N^2$.

(2) 证明:

$$\ln Z\leqslant\sum_{p\leqslant\gamma N}\ln p\sum_{n\in I_p}v_p(n!+1),$$

其中区间 $I_p=[\frac{1}{\gamma}p,\min\{p,N\}]$.

(3) 暂时固定一个素数 $p\leqslant\gamma N$. 设

$$\{n\in I_p\mid n!+1\text{ 被 }p\text{ 整除}\}=\{n_1,n_2,\cdots,n_t\},$$

并不妨设

$$v_p(n_1!+1)\geqslant v_p(n_2!+1)\geqslant\cdots\geqslant v_p(n_t!+1).$$

证明:

$$t \leqslant 100N^{\frac{2}{3}}.$$

(提示: 和 2009 年中国集训队的一道测试题方法一致.)

(4) 对于 $2 \leqslant i \leqslant t$, 证明: $\gcd(n_1!+1, n_2!+1, \cdots, n_i!+1) \leqslant N^{\frac{|I_p|}{i-1}}$. 由此进一步证明: $v_p(n_i!+1)\ln p \leqslant \frac{|I_p|}{i-1}\ln N$.

(5) 证明: $\ln p \sum_{n\in I_p} v_p(n!+1) \leqslant \frac{2}{3}|I_p|\ln^2 N + 100N\ln N$. 并进一步证明:

$$\ln Z \leqslant \frac{2}{3}\ln^2 N \sum_{p\leqslant N} p - \frac{2}{3}\frac{1}{\gamma}\ln^2 N \sum_{p\leqslant \gamma N} p + \frac{2}{3}N\ln^2 N \sum_{N<p\leqslant \gamma N} 1 + 100N\ln N \sum_{p\leqslant \gamma N} 1.$$

(6) 素数定理给出当 $x\to+\infty$ 时 $\sum_{p\leqslant x} 1 = (1+o(1))\frac{x}{\ln x}$. 素数定理和 Abel 求和(分部积分)给出 $\sum_{p\leqslant x} p = (\frac{1}{2}+o(1))\frac{x^2}{\ln x}$. 利用这两个结论证明: 当 $N\to+\infty$ 时,

$$\ln Z \leqslant \frac{1}{3}(\gamma - 1 + o(1))N^2\ln N,$$

并完成本题的证明.

Stewart 原始的版本是 $5.5-\varepsilon$, 这个改进来自于他对 (4) 小问做出了更好的估计如下:

Stewart 的引理 ([3]的 Lemma 2) 设 n, t 是正整数, $t\geqslant 2$. 设 I 为区间 $[1,n]$ 的一个子区间, 其长度 $|I|=\ell$. 设 $a_1,a_2,\cdots,a_t$ 是区间 I 中的任意 t 个两两不同的正整数. 则

$$\gcd(a_1!+1,\cdots,a_t!+1) < n^{\frac{\ell}{t-1}}.$$

进一步, 存在常数 $c_1>0$, 若 $n>c_1$ 且 $t\geqslant 3$, 则

$$\gcd(a_1!+1,\cdots,a_t!+1) < e^n n^{\frac{2\ell}{(t-1)^2}}.$$

更进一步, 任给两个正实数 $\varepsilon,\delta>0$, 存在仅依赖于 ε,δ 的常数 c_2, 使得若 $n>c_2$, 若

$$3\leqslant t < n^{\frac{13}{18}-\delta},$$

以及

$$\ell > \frac{n}{\sqrt{\ln n}},$$

则

$$\gcd(a_1!+1,\cdots,a_t!+1)<\exp\left((1+\varepsilon)\ell\left(\frac{\ln t}{t}+\frac{\ln\left(\frac{en}{\ell}\right)}{t}+\frac{2\ln n\max\{1,\ln\ln t\}}{(t-1)^2}\right)\right).$$

Stewart 的核心观察是: 对于四个正整数 k_1,k_2,k_3,k_4, 若 $k_1-k_2\geqslant k_3-k_4>0$, 则 $\gcd(k_1!+1,\cdots,k_4!+1)$ 整除

$$\frac{1}{(k_3-k_4)!}\left(k_1(k_1-1)\cdots(k_2+1)-k_3(k_3-1)\cdots(k_4+1)\right).$$

利用这一观察, Stewart 用初等而技术性的方法在 $a_1,\cdots,a_t$ 中选出合适的 k_1, $\cdots$, k_4, 使得上式右端非零且绝对值尽量小来得到上面的引理.

如果我们能对(比如说) $t\geqslant\ln n$ 的情况改进 Stewart 的引理中对最大公约数的上界估计的量级, 那么我们有希望改进 Stewart 的结果. 为此, 我先尝试了 $t=2$ 的情况作为玩具模型, 得到了前面的命题 2 的结果. 其中 $\gcd(a!-1,b!-1)$ 整除 $\frac{a!^u-b!^v}{\gcd(a!^u,b!^v)}$ 这一关键想法是有趣的, 经过命题组的打磨, 最终将它加工成问题 1 作为一道CGMO试题. 遗憾的是, 这个想法无法改进 Stewart 的引理中 $t\geqslant\ln n$ 的情况, 试图改进 Stewart 的结果需要新的洞察.

参考文献

[1] 瞿振华, 第 19 届 CGMO 试题解答, 数学新星网, 教师专栏, 2020.

[2] F. Luca and I. E. Shparlinski, *Prime divisors of shifted factorials*, Bull. London Math. Soc. 37 (2005), no. 6, 809-817.

[3] C. L. Stewart, *On the greatest and least prime factors of* $n!+1$*, II*, Publ. Math. Debrecen 65 (2004), no. 3-4, 461-480.

[4] M. R. Murty and S. Wong, *The ABC conjecture and prime divisors of the Lucas and Lehmer sequences*, Number Theory for the Millenium, III, (Urbana, IL, 2000), A. K. Peters, Natick, MA, 2002, 43-54.

[5] C. L. Stewart, *On divisor properties of arithmetical sequences*, Ph.D. thesis, University of Cambridge, 1976.

[6] P. Erdös and C. L. Stewart, *On the greatest and least prime factors of* $n!+1$, J. London Math. Soc 13, no. (2) (1976), 513-519.