阶&原根

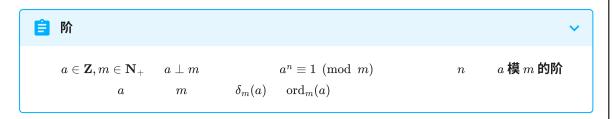
前置知识: 费马小定理、欧拉定理、拉格朗日定理

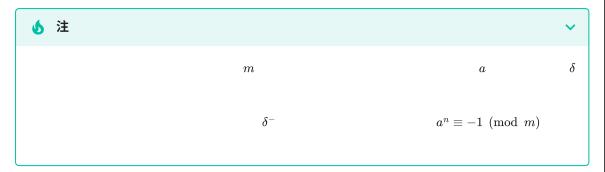
阶和原根,是理解模 m 既约剩余系 \mathbf{Z}_m^* 乘法结构的重要工具.基于此,可以定义 离散对数 等概念.更为一般的讨论可以参见抽象代数部分 群论 和 环论 等页面相关章节.

阶

本节中,总是假设模数 $m \in \mathbb{N}_+$ 和底数 $a \in \mathbb{Z}$ 互素,即 (a, m) = 1,也记作 $a \perp m$.

对于 $n \in \mathbb{Z}$,幂次 $a^n \mod m$ 呈现一种循环结构. 这个循环节的最小长度,就是 $a \notin m$ 的阶. 阶就定义为幂 $a^n \mod m$ 第一次回到起点 $a^0 \mod m = 1$ 时的指数:





幂的循环结构

利用阶,可以刻画幂的循环结构. 对于幂 $a^n \mod m$,可以将指数 n 对阶 $\delta_m(a)$ 做带余除法:

$$n=\delta_m(a)q+r,\ 0\leq r<\delta_m(a).$$

进而,利用幂的运算律,就得到

$$a^n = a^{\delta_m(a)q+r} = (a^{\delta_m(a)})^q \cdot a^r \equiv a^r \pmod m.$$

这说明,对于任意指数的幂,可以将它平移到第一个非负的循环节.由此,可以得到一系列关于 阶的性质.



 $a \in {f Z}, m \in {f N}_+ \hspace{0.5cm} a \perp m$

 $a^0 (=1), a, a^2, \cdots, a^{\delta_m(a)-1}$ m

☑ 证明

$$0 \leq i < j < \delta_m(a) \qquad a^i \equiv a^j \pmod m \qquad \qquad a^{j-i} \equiv 1 \pmod m$$

 $0 < j-i < \delta_m(a)$

✓ 性质 2

 $a,n\in {f Z}, m\in {f N}_+ \hspace{0.5cm} a\perp m$

 $a^n \equiv 1 \pmod{m}$

 $\delta_m(a)\mid n$

╱ 证明

 $a^n \equiv a^{n mod \delta_m(a)} \pmod m \qquad \qquad 0 \le r < \delta_m(a)$

$$a^r \equiv 1 \pmod m$$
 $r = 0$ $a^n \equiv 1 \pmod m$ $n \mod \delta_m(a) = 0$ $\delta_m(a) \mid a$

欧拉定理 中,同余关系 $a^{\varphi(m)}\equiv 1\pmod m$ 对于所有 $a\perp m$ 都成立.结合性质 2,这说明对于所有 $a\perp m$,都有 $\delta_m(a)\mid \varphi(m)$.换句话说, $\varphi(m)$ 是所有 $a\perp m$ 的阶的一个公倍数.对于一个正整数 m,所有 $a\perp m$ 的阶 $\delta_m(a)$ 的最小公倍数,记作 $\lambda(m)$,就是 m 的 Carmichael 函数.后文会详细讨论它的性质.

和其他的循环结构类似,可以根据 a 的阶计算 a^k 的阶.

✓ 性质 3

 $k,a\in {f Z}, m\in {f N}_+ \ \ \ \ a\perp m$

$$\delta_m(a^k) = rac{\delta_m(a)}{(\delta_m(a),k)}.$$

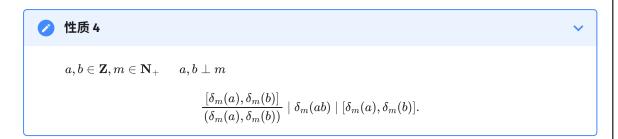
逆 证明
$$(a^k)^n = a^{kn} \equiv 1 \pmod m \qquad \qquad \delta_m(a) \mid kn$$

$$\frac{\delta_m(a)}{(\delta_m(a),k)} \mid n.$$

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a),k)}.$$

乘积的阶

设 a,b 是与 m 互素的不同整数.如果已知阶 $\delta_m(a)$ 和 $\delta_m(b)$,那么,同样可以获得一些关于它们乘积 ab 的阶 $\delta_m(ab)$ 的信息.





 $[\delta_m(a),\delta_m(b)] \qquad \delta_m(a) \qquad \delta_m(b)$

$$(ab)^{|\delta_m(a),\delta_m(b)|}=a^{|\delta_m(a),\delta_m(b)|}b^{|\delta_m(a),\delta_m(b)|}\equiv 1\pmod m.$$

$$\delta_m(ab) \mid [\delta_m(a), \delta_m(b)].$$

$$1\equiv (ab)^{\delta_m(ab)\delta_m(b)}\equiv a^{\delta_m(ab)\delta_m(b)}\pmod{m},$$

$$\delta_m(a) \mid \delta_m(ab)\delta_m(b) \qquad \qquad (\delta_m(a), \delta_m(b))$$

$$\frac{\delta_m(a)}{(\delta_m(a),\delta_m(b))}\mid \delta_m(ab)\frac{\delta_m(b)}{(\delta_m(a),\delta_m(b))}.$$

$$rac{\delta_m(a)}{(\delta_m(a),\delta_m(b))}\mid \delta_m(ab).$$

$$rac{\delta_m(b)}{(\delta_m(a),\delta_m(b))}\mid \delta_m(ab).$$

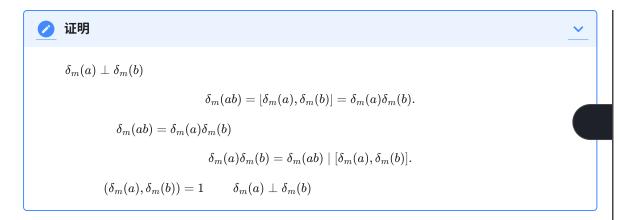
$$rac{[\delta_m(a),\delta_m(b)]}{(\delta_m(a),\delta_m(b))} = rac{\delta_m(a)\delta_m(b)}{(\delta_m(a),\delta_m(b))^2} \mid \delta_m(ab).$$

对于 a 和 b 的阶互素的情形,这一结论有着更为简单的形式.

🖊 性质 4'

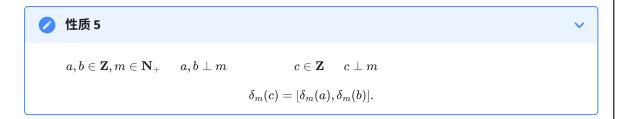
 $a,b\in {f Z}, m\in {f N}_+ \qquad a,b\perp m$

$$\delta_m(ab) = \delta_m(a)\delta_m(b) \iff \delta_m(a) \perp \delta_m(b).$$



一般情形中,性质 4 得到的界已经是紧的. 乘积的阶取得下界的情形很容易构造: 例如 (a,b,m)=(3,5,7) 时, $\delta_m(a)=\delta_m(b)=6$,但是它们的乘积的阶 $\delta_m(ab)=1$.

尽管一般情形中,乘积 ab 的阶未必是它们的阶的最小公倍数,但是总能找到一个元素使得它的阶等于这个最小公倍数.



🖊 证明

$$\delta_m(a) = \prod\limits_p \; p^{lpha_p}, \; \delta_m(b) = \prod\limits_p \; p^{eta_p}.$$

 α_p β_p

$$A = \{p : \alpha_p \ge \beta_p\}, \ B = \{p : \alpha_p < \beta_p\}.$$

$$\gamma_A = \prod_{p \in A} p^{lpha_p}, \; \gamma_B = \prod_{p \in B} p^{lpha_p}, \; \eta_A = \prod_{p \in A} p^{eta_p}, \; \eta_B = \prod_{p \in B} p^{eta_p},$$

$$\delta_m(a) = \gamma_A \gamma_B ~~ \delta_m(b) = \eta_A \eta_B$$

$$egin{align} \delta_m(a^{\gamma_B}) &= rac{\delta_m(a)}{(\delta_m(a),\gamma_B)} = rac{\delta_m(a)}{\gamma_B} = \gamma_A, \ \delta_m(b^{\eta_A}) &= rac{\delta_m(b)}{(\delta_m(b),\eta_A)} = rac{\delta_m(b)}{\eta_A} = \eta_B. \end{align}$$

 $\gamma_A \perp \eta_B$

$$\delta_m(a^{\gamma_B}b^{\eta_A}) = \gamma_A\eta_B = \mathop{\sqcap}\limits_p \; p^{\max\{lpha_p,eta_p\}} = [\delta_m(a),\delta_m(b)].$$

$$c=a^{\gamma_B}b^{\eta_A} \qquad \qquad [\delta_m(a),\delta_m(b)]$$

这一结论常用于构造出指定阶的元素.

原根

原根是一些特殊元素——它的阶就等于所有模m既约剩余系的个数.



📋 原根

$$m\in {f N}_+$$
 $g\in {f Z}$ $g\perp m$ $\delta_m(g)=|{f Z}_m^*|=arphi(m)$ g 模 m 的原根 au

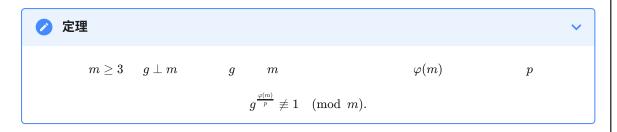
并非所有正整数 m 都存在模 m 的原根. 由上文的性质 1, 如果模 m 的原根 g 存在,那么, $g,g^2,\cdots,g^{arphi(m)}$ 所在的同余类互不相同,构成模 m 既约剩余系.特别地,对于素数 p,余数 $g^i \mod p$ 对于 $i = 1, 2, \dots, p-1$ 两两不同.

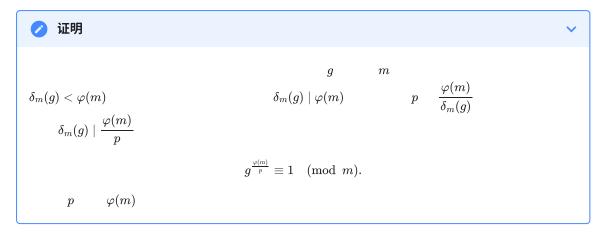


模为 1 时,模 1 整数乘法群就是 $\{0\}$. 这显然是循环群,所以原根就是 0.

原根判定定理

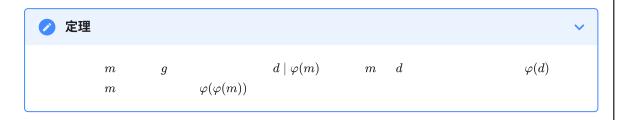
如果已知模数 $\varphi(m)$ 的全体素因子,那么很容易判断模 m 的原根是否存在.

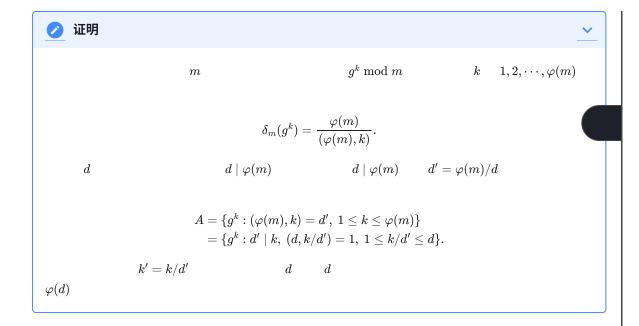




原根个数

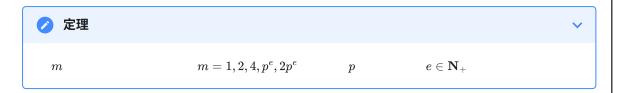
原根如果存在,也未必唯一.一般地,对于模m 既约剩余系中所有元素可能的阶和某个阶的元素数量,有如下结论:





原根存在定理

本节将建立如下原根存在定理:



为说明这一结论,需要分别讨论如下四种情形:

- 1. m = 1, 2, 4,原根分别是 g = 0, 1, 3,显然存在.
- 2. $m = p^e$ 是奇素数的幂,其中,p 为奇素数, $e \in \mathbf{N}_+$.



d

第一步
$$d \mid (p-1)$$
 $x^d \equiv 1 \pmod{p}$ d

$$x^d \equiv 1 \pmod{p}$$

$$p-1=kd$$

$$f(x) = x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1.$$

$$(x^d-1)f(x)=x^{p-1}-1\equiv 0\pmod p\qquad p-1$$

$$x^d-1$$
 $f(x)$

$$d(k-1) \hspace{1cm} d+d(k-1)=p-1 \hspace{1cm} d$$

$$x^d \equiv 1 \pmod p$$

第二步
$$d \mid (p-1) \quad d \qquad \qquad \varphi(d)$$

$$arphi(m)$$
 1 1 $d \mid (p-1)$ $x^d \equiv 1 \pmod m$

$$\delta_p(x) \mid d$$
 d

$$N(d) = d - \sum_{e \mid d, \, e
eq d} N(e) = d - \sum_{e \mid d, \, e
eq d} arphi(e) = arphi(d).$$

$$d \mid (p-1)$$
 $arphi(d) \quad d$

$$d=p-1 \qquad \qquad arphi(p-1) \qquad (p-1)$$

✓ 引理 2

 $p \quad e \in \mathbf{N}_+ \qquad p^e$

第一步
$$p$$
 g $g^{p-1} \not\equiv 1 \pmod{p^2}$

$$(g+p)^{p-1} \equiv inom{p-1}{0} g^{p-1} + inom{p-1}{1} g^{p-2} p \ = g^{p-1} + g^{p-2} p (p-1) \ \equiv 1 - p g^{p-2}
ot \equiv 1 \pmod{p^2}.$$

第二步
$$g \qquad \qquad e \geq 1 \qquad \qquad g^{\varphi(p^e)} \not\equiv 1 \pmod{p^{e+1}}$$

$$g^{arphi(p^e)}=1+\lambda p^e$$

$$\lambda \perp p \qquad \qquad arphi(p^{e+1}) = p arphi(p^e)$$

$$g^{arphi(p^{e+1})} = \left(\ g^{arphi(p^e)}
ight)^{\ p} = (1+\lambda p^e)^p \equiv 1+\lambda p^{e+1} \pmod{p^{e+2}}.$$

$$\lambda \perp p \qquad \quad g^{arphi(p^{e+1})}
ot \equiv 1 \pmod{p^{e+2}}$$

第三步
$$g$$
 $e\geq 1$ p^e

$$g$$
 $e=1$ e $e+1$ δ $e = 1 \pmod{n^e+1}$ $\delta = 1 \pmod{n^e}$

$$egin{aligned} g & e = 1 & e & e + 1 \ \delta_{p^{e+1}}(g) & \delta & g^{\delta} \equiv 1 \pmod{p^{e+1}} & g^{\delta} \equiv 1 \pmod{p^e} \ \delta_{p^e}(g) = arphi(p^e) & arphi(p^e) \mid \delta \ \delta \mid arphi(p^{e+1}) & arphi(p^{e+1}) = p arphi(p^e) & \delta = arphi(p^e) & \delta = arphi(p^e) \ g^{arphi(p^e)}
otin 1 \pmod{p^{e+1}} & \delta = arphi(p^e) & \delta = arphi(p^e) \ \delta = arphi(p^e) & \delta = arphi(p^e) \end{aligned}$$

$$\delta = arphi(p^{e+1})$$
 $g \quad p^{e+1}$ $e \geq 1$

 $3. m = 2p^e$,其中,p 为奇素数, $e \in \mathbb{N}_+$.

○ 引理 3

$$p \hspace{0.5cm} e \in {f N}_{+} \hspace{0.5cm} 2p^{e}$$

🖊 证明

$$\delta_{p^e}(g) = arphi(p^e) \mid \delta \qquad \qquad arphi(2p^e) = arphi(p^e)$$

$$\delta = \delta_{2p^e}(g) = arphi(p^e) \qquad \qquad \delta \qquad \ \, 2p^e$$

4. $m \neq 1, 2, 4, p^e, 2p^e$,其中,p 为奇素数, $e \in \mathbf{N}_+$.

引理 4 $m \neq 1,2,4 \qquad \qquad p \qquad \qquad e \qquad m = p^e \quad m = 2p^e \qquad \qquad m$

综合以上四个引理,我们便给出了一个数存在原根的充要条件.

最小原根的范围估计

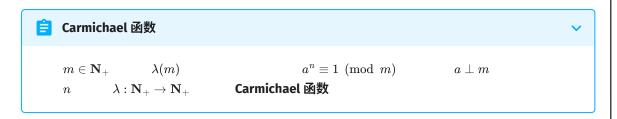
王元¹和 Burgess²证明了素数 p 的最小原根 $g_p=O\left(p^{0.25+\epsilon}\right)$,其中 $\epsilon>0$.Cohen, Odoni, and Stothers³和 Elliott and Murata⁴分别证明了该估计对于模数 p^2 和 $2p^2$ 也成立,其中,p 是奇素数.由于对于 e>2,模 p^2 (或 $2p^2$)的原根也是模 p^e (或 $2p^e$)的原根,所以,最小原根的上界 $O\left(p^{0.25+\epsilon}\right)$ 对于所有情形都成立.

Fridlander⁵和 Salié⁶证明了素数 p 的最小原根 $g_p = \Omega(\log p)$.

这保证了暴力找一个数的最小原根时,复杂度可以接受.

Carmichael 函数

相对于模m元素的阶这一局部概念,Carmichael 函数是一个全局概念.它是所有与m互素的整数的幂次的最小公共循环节.



根据性质 2,能够使得 $a^n \equiv 1 \pmod{m}$ 对于所有 $a \perp m$ 都成立,意味着 $\delta_m(a) \mid n$ 对于所有 $a \perp m$ 都成立.也就是说,符合这一条件的正整数 n,一定是全体 $\delta_m(a)$ 的公倍数.因此,最小的这样的 n 就是它们的最小公倍数:

$$\lambda(m) = \operatorname{lcm}\{\delta_m(a) : a \perp m\}.$$

这也常用作 Carmichael 函数的等价定义.

反复应用性质 5 可知,一定存在某个元素 $a\perp m$ 使得 $\delta_m(a)=\lambda(m)$. 因此,上式也可以写作

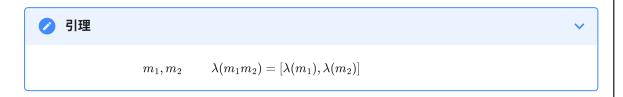
$$\lambda(m) = \max\{\delta_m(a) : a \perp m\}.$$

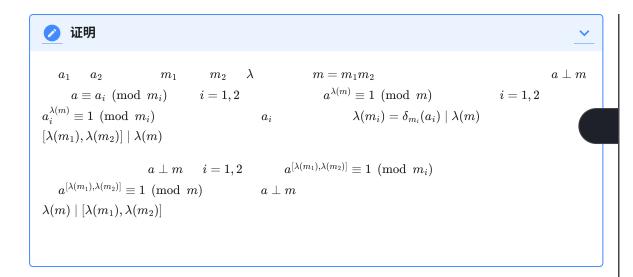
取得这一最值的元素 $a\perp m$ 也称为模 m 的 λ -原根. 它对于所有模数 m 都存在.

递推公式

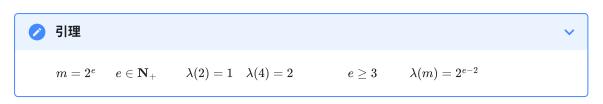
Carmichael 函数是一个数论函数.本节讨论它的一个递推公式,并由此给出原根存在定理的另一个证明.

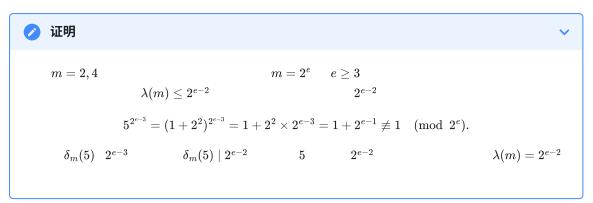
虽然不是积性函数,但是计算 Carmichael 函数时,同样可以对互素的因子分别处理.



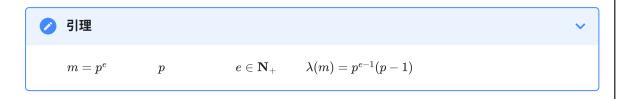


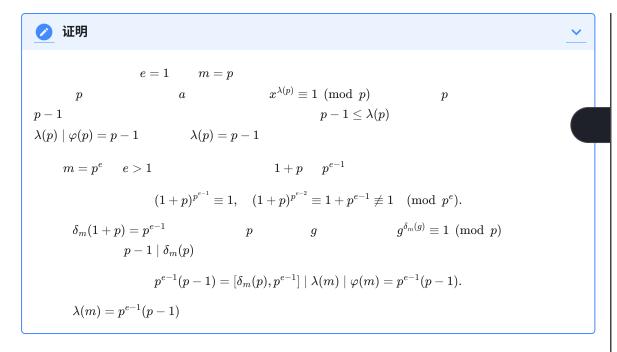
因此,接下来只要计算 Carmichael 函数在素数幂处的取值. 首先,处理 2 的幂次的情形.



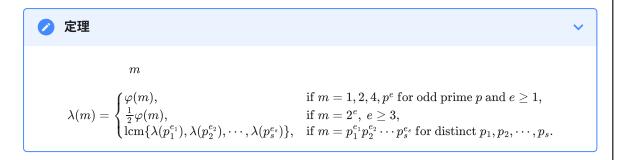


然后,处理奇素数幂的情形.

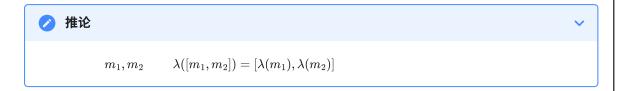




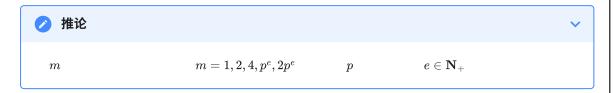
将本节的结果简单归纳,就得到 Carmichael 函数的递推公式:



利用该递推公式可以加强前文的结果:



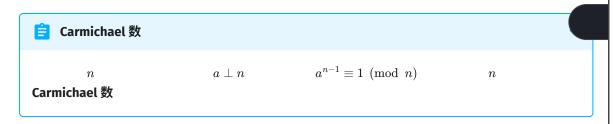
比较原根和 Carmichael 函数的定义可知,模 m 的原根存在,当且仅当 $\lambda(m)=\varphi(m)$.从 Carmichael 函数的递推公式中,容易归纳出如下结果:



由于本节对于递推公式的证明并没有用到原根存在定理,因此,这就构成了对该定理的又一个证明.

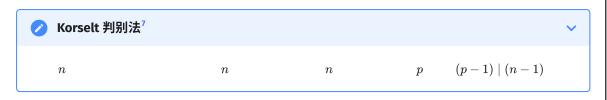
Carmichael 数

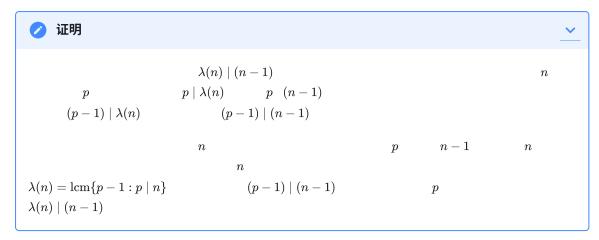
利用 Carmichael 函数,可以讨论 Carmichael 数(卡迈克尔数,OEIS:A002997)的性质与分布。 这是 Fermat 素性测试 一定无法正确排除的合数.



最小的 Carmichael 数是 $561 = 3 \times 11 \times 17$.

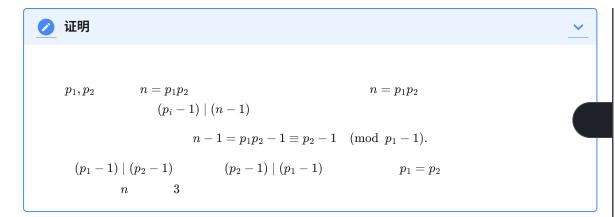
由 Carmichael 函数的定义可知,合数 n 是 Carmichael 数当且仅当 $\lambda(n) \mid n-1$,其中 $\lambda(n)$ 为 Carmichael 函数.进一步地,可以得到如下判断合数 n 是否为 Carmichael 数的方法:





从这一判别法出发,可以建立 Carmichael 数的一些简单性质:





利用解析数论还可以得到 Carmichael 数分布的一些性质.设 C(n) 为小于等于 n 的 Carmichael 数个数.Alford, Granville, and Pomerance 8 证明,对于充分大的 n,有 $C(n) > n^{2/7}$.由此,Carmichael 数有无限多个.在这之前,Erdős 9 已经证明, $C(n) < n \exp\left(-c\frac{\ln n \ln \ln \ln n}{\ln \ln n}\right)$,其中 c 为常数.因此,Carmichael 数的分布(相对于素数来说)十分稀疏.实际上,有 10 $C(10^9) = 646$, $C(10^{18}) = 1$ 401 644.

参考资料与注释

- Primitive root modulo n Wikipedia
- The order of a unit Course Notes
- The primitive root theorem Amin Witno's notes
- Carmichael function Wikipedia
- Carmichael's Lambda Function Brilliant Math & Science Wiki
- Carmichael number Wikipedia
- Carmichael Number Wolfram MathWorld

 $10^{20} \leftarrow$

▲ 本页面最近更新: 2025/8/30 15:23:07, 更新历史

▶ 发现错误?想一起完善? 在 GitHub 上编辑此页!

本页面贡献者: Peanut-Tang, EarlyOvO, Ir1d, StudyingFather, Tiphereth-A, Great-designer, MegaOwler, Xeonacid, 2008verser, Enter-tainer, bobhan1, c-forrest, CCXXXI, chuxin0816, CroMarmot, GavinZhengOI, GeorgePlover, hhc0001, huhaoo, Larry0716, Marcythm, opsiff, ouuan, PeterlitsZo, ShelpAm, tml104, wty-yy

ⓒ 本页面的全部内容在 CC BY-SA 4.0 和 SATA 协议之条款下提供,附加条款亦可能应用