第二周作业讲解与拓展

助教 邓博文

中国科学技术大学, 少年班学院

2025 年 9 月 27 日

目录

目录

作业 1

问题

若 $n \in \mathbb{N}^*$, 证明 $(n!+1,(n+1)!+1)=1$.

作业 1

问题

若 $n \in \mathbb{N}^*$, 证明 $(n! + 1, (n+1)! + 1) = 1$.

证明.

$(n! + 1, (n+1)! + 1) = (n! + 1, (n+1)! + 1 - (n+1)(n! + 1)) = (n! + 1, -n) = 1$ $\square$

目录

作业 2

问题

用 Euclid 算法求 963 和 657 的最大公约数, 并求方程

$$963x + 657y = (963, 657)$$

的一组特解和所有整数解.

特解.

$$963 - 657 = 306$$

$$657 - 2 \times 306 = 45$$

$$7 \times 45 - 306 = 9$$

$$45 = 5 \times 9$$

故 $(963, 657) = 9$.

特解.

$$963 - 657 = 306$$

$$657 - 2 \times 306 = 45$$

$$7 \times 45 - 306 = 9$$

$$45 = 5 \times 9$$

故 $(963, 657) = 9$.

$$\begin{aligned} 9 &= 7 \times 45 - 306 = 7 \times (657 - 2 \times 306) - 306 \\ &= 7 \times 657 - 15 \times 306 = 7 \times 657 - 15 \times (963 - 657) \\ &= 22 \times 657 - 15 \times 963 \end{aligned}$$

特解 $x_0 = -15,\ y_0 = 22$. □

通解.

原方程

$$963x + 657y = (963, 657) = 9$$

$$107x + 73y = 1$$

特解 $x_0 = -15$, $y_0 = 22$. 代入原方程

$$107(x - x_0) = 73(y_0 - y)$$

故 $73 \mid x - x_0$, $107 \mid y_0 - y$. 设 $x - x_0 = 73k$, $y_0 - y = 107k$, $k \in \mathbb{Z}$. 通解

$$\begin{cases} x = x_0 + 73k = -15 + 73k \\ y = y_0 - 107k = 22 - 107k \end{cases}$$

□

目录

作业 3

问题

设 $a, b \in \mathbb{N}^*$, 且 $(a, b) = 1$. 证明当 $n > ab - a - b$ 时, 方程

$$ax + by = n$$

存在非负整数解. 但当 $n = ab - a - b$ 时, 方程无非负整数解.

作业 3

问题

设 $a, b \in \mathbb{N}^*$, 且 $(a, b) = 1$. 证明当 $n > ab - a - b$ 时, 方程

$$ax + by = n$$

存在非负整数解. 但当 $n = ab - a - b$ 时, 方程无非负整数解.

$$ax + by = n \iff a(x+1) + b(y+1) = n + a + b$$

作业 3

问题

设 $a, b \in \mathbb{N}^*$, 且 $(a, b) = 1$. 证明当 $n > ab - a - b$ 时, 方程

$$ax + by = n$$

存在非负整数解. 但当 $n = ab - a - b$ 时, 方程无非负整数解.

$$ax + by = n \Longleftrightarrow a(x+1) + b(y+1) = n + a + b$$

等价问题

设 $a, b \in \mathbb{N}^*$, 且 $(a, b) = 1$. 证明当 $n > ab$ 时, 方程

$$ax + by = n$$

存在正整数解. 但当 $n = ab$ 时, 方程无正整数解.

证明.

Euclid 算法 (Bézout 定理) 表明存在整数 x', y' 使得

$$ax' + by' = 1$$

故 $a(nx') + b(ny') = n$, $ax + by = n$ 存在整数解 x_0, y_0. 通解

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak \end{cases}$$

其中 $k \in \mathbb{Z}$.

证明.

Euclid 算法 (Bézout 定理) 表明存在整数 x', y' 使得

$$ax' + by' = 1$$

故 $a(nx') + b(ny') = n$, $ax + by = n$ 存在整数解 x_0, y_0. 通解

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak \end{cases}$$

其中 $k \in \mathbb{Z}$.
当 $n = ab$ 时, 通解

$$\begin{cases} x = bk \\ y = a(1-k) \end{cases}$$

无正整数解. □

证明.

当 $n > ab$ 时, 通解

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak \end{cases}$$

取整数 k 使得 $1 \leq x \leq b$.

$$by = n - ax \geq n - ab > 0$$

故 $y > 0$. 此即为一组正整数解. $\square$

目录

作业 4

问题

若整数 $n > 2$, 证明 n 到 $n!$ 之间至少有一个素数. 由此证明素数有无穷多.

注: n 到 $n!$ 之间指 $(n, n!)$.

作业 4

问题

若整数 $n > 2$, 证明 n 到 $n!$ 之间至少有一个素数. 由此证明素数有无穷多.

注: n 到 $n!$ 之间指 $(n, n!)$.

证明.

若 n 到 $n!$ 之间存在素数, 则素数有无穷多.
否则设最大的素数为 p, 由 p 到 $p!$ 之间存在素数矛盾. $\square$

下证 n 到 $n!$ 之间存在素数. 我们给出三种方法.

方法 1

证明.

取 $n!-1$ 的素因子 p, $(p,n!)=1$.

p 与 $\leq n$ 的所有素数互质, 故 $p>n$. $\square$

方法 2

弱哥德巴赫猜想 (Harald Andrés Helfgott, 2013)

任一大于 5 的奇数都可以表示为三个素数之和.

方法 2

弱哥德巴赫猜想 (Harald Andrés Helfgott, 2013)

任一大于 5 的奇数都可以表示为三个素数之和.

证明.

$n=3$ 的情况是平凡的. $n\geq 4$ 时, $n!-1$ 为大于 5 的奇数, 由定理

$$n!-1=p+q+r$$

其中 p, q, r 为素数. 其中必有素数 $\geq \frac{n!-1}{3}>n$. □

方法 3

Bertrand-Chebyshev 定理

若整数 $n > 1$, 存在素数 p 满足 $n < p \leq 2n$.

方法 3

Bertrand-Chebyshev 定理

若整数 $n > 1$, 存在素数 p 满足 $n < p \leq 2n$.

定理证明思路.

反证法. 假设定理不成立, 估计 $\binom{2n}{n}$ 的上下界, 得出矛盾. $\square$

方法 3

Bertrand-Chebyshev 定理

若整数 $n > 1$, 存在素数 p 满足 $n < p \leq 2n$.

定理证明思路.

反证法. 假设定理不成立, 估计 $\binom{2n}{n}$ 的上下界, 得出矛盾. $\square$

证明.

$n > 2$ 时, $n! \geq 2n$. 由定理得证. $\square$

下界

对正整数 n,

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

定理证明

下界

对正整数 n,
$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

证明.

对 $1 \leq k \leq 2n$, $\binom{2n}{n} \geq \binom{2n}{k}$, 取等当且仅当 $k = n$. 故
$$2n\binom{2n}{n} \geq \sum_{k=1}^{2n} \binom{2n}{k} + 1 = 4^n$$
$\square$

定理证明

引理 1

对正整数 k,

$$\prod_{k+1<p\leq 2k+1} p < 4^k$$

其中 p 为素数.

引理 1

证明.

注意到

$$\prod_{k+1<p\leq 2k+1} p \mid \binom{2k+1}{k+1}$$

又

$$2\binom{2k+1}{k+1} = \binom{2k+1}{k} + \binom{2k+1}{k+1} < \sum_{i=0}^{2k+1} \binom{2k+1}{i} = 2^{2k+1} = 2\cdot 4^k$$

故

$$\prod_{k+1<p\leq 2k+1} p \leq \binom{2k+1}{k+1} \leq \prod_{k+1<p\leq 2k+1} p < 4^k$$

□

引理 2

对正整数 n,

$$\prod_{p\leq n} p < 4^n$$

其中 p 为素数.

引理 2

证明.

数学归纳法. $n=2$ 时成立.
对 $n\geq 3$, 若命题对 $<n$ 的情形成立, 下证 n 的情形.
若 n 为偶数, 则

$$\prod_{p\leq n} p=\prod_{p\leq n-1} p<4^{n-1}<4^n$$

若 n 为奇数, 设 $n=2k+1$, $k\in\mathbb{N}^*$. 由归纳假设和引理 1

$$\prod_{p\leq n} p=\prod_{p\leq k+1} p\cdot\prod_{k+1<p\leq 2k+1} p<4^{k+1}\cdot 4^k=4^n$$

□

定理证明

引理 3

对质数 p 和正整数 n, 设 $s_p = v_p(\binom{2n}{n})$. 我们有

$$p^{s_p} \leq 2n$$

故对 $p > \sqrt{2n}$, $s_p \leq 1$.
此外, 当 $n \geq 3$ 时, 对 $2n/3 < p \leq 2n$, $s_p = 0$.

定理证明

引理 3

对质数 p 和正整数 n, 设 $s_p = v_p(\binom{2n}{n})$. 我们有

$$p^{s_p} \le 2n$$

故对 $p > \sqrt{2n}$, $s_p \le 1$.
此外, 当 $n \ge 3$ 时, 对 $2n/3 < p \le 2n$, $s_p = 0$.

Legendre 公式

对质数 p 和正整数 n, $v_p(n!) = \sum_{i \ge 1} \lfloor \frac{n!}{p^i} \rfloor$

引理 3

证明.

注意到 $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, 由 Legendre 公式

$$s_p = \sum_{i\geq 1}(\lfloor\frac{2n}{p^i}\rfloor - 2\lfloor\frac{n}{p^i}\rfloor)$$

当 $x > 0$ 时 $\lfloor 2x\rfloor - 2\lfloor x\rfloor \leq 1$.
故 $s_p \leq \log_p(2n)$, $p^{s_p} \leq 2n$. 对 $p > \sqrt{2n}$, $s_p \leq 1$.
对 $2n/3 < p \leq 2n$, $p > 2n/3 \geq 2$, 故 $p^2 > 2n$. 因此

$$s_p = \lfloor\frac{2n}{p}\rfloor - 2\lfloor\frac{n}{p}\rfloor = 0$$

□

定理证明

上界

对正整数 $n \geq 128$, 若 n 到 $2n$ 之间没有素数,

$$\binom{2n}{n} < (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}$$

定理证明

上界

对正整数 $n \geq 128$, 若 n 到 $2n$ 之间没有素数,

$$\binom{2n}{n} < (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}$$

证明.

对 $n \geq 128$, $\sqrt{2n} \geq 16$, $\pi(\sqrt{2n}) < \sqrt{2n}/2 - 1$. 由引理 2 和引理 3,

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{s_p} = \prod_{p \leq 2n/3} p^{s_p} < \prod_{p \leq \sqrt{2n}} p^{s_p} \cdot \prod_{p \leq 2n/3} p$$

$$\leq 2n^{\pi(\sqrt{2n})} \cdot 4^{2n/3} < (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}$$

$\square$

定理证明

反证.

若存在正整数 $n \geq 128$, 使得 n 到 $2n$ 之间没有素数, 我们有

$$(2n)^{-1}4^n \leq \binom{2n}{n} < (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}$$

整理得

$$4^{2n/3} < 2n^{\sqrt{2n}}$$

设 $x = \sqrt{2n} \geq 16$, 对上式取对数

$$x \ln 2 - 3 \ln x < 0$$

其在 $x \geq 16$ 时不成立, 矛盾. 故定理对 $n \geq 128$ 成立. $\square$

目录

作业 5

问题

1. 设 m 为正整数, 证明: 若 2^m+1 为素数，则 m 为 2 的方幂.
2. 对 $n \geq 0$, 记 $F_n = 2^{2^n}+1$, 这称为**费马数**. 证明: 若 $m > n$, 则
$$F_n \mid (F_m - 2).$$
3. 证明: 若 $m \neq n$, 则 $(F_m, F_n) = 1$. 由此证明素数有无穷多个.

证明.

1. 若 m 有奇素因子 p, 设 $m = pk$, $x = 2^k \geq 2$. 则
$$2^m + 1 = 2^{pk} + 1 = x^p + 1 = (x+1)(x^{p-1} - x^{p-2} + x^{p-3} + \cdots + 1)$$
不为素数, 矛盾. 故 m 为 2 的方幂.
2. 我们给出更一般的公式
$$\begin{aligned} F_m - 2 = 2^{2^m} - 1 &= (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1) = F_{m-1}(F_{m-1} - 2) \\ &= F_{m-1}F_{m-2}(F_{m-2} - 2) = \cdots = F_{m-1}F_{m-2}\cdots F_0(F_0 - 2) \\ &= F_{m-1}F_{m-2}\cdots F_0 \end{aligned}$$
3. 不妨 $m > n$, 则 $(F_m, F_n) = (2, F_n) = 1$. 取 p_n 为 F_n 的任一素因子, 则当 $m \neq n$ 时 $p_n \neq p_m$. 因此 $\{p_n\}_{n=0}^{\infty}$ 为无限素数列.

□

费马数中的素数称为**费马素数**. 例如

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

都是素数. 1640 年, 费马提出了如下猜想

猜想 (Fermat, 1640)

所有的费马数 F_n 都是素数.

这一猜想对前 5 个费马数成立, 于是费马宣称他找到了表示素数的公式.

费马数

费马数中的素数称为**费马素数**. 例如

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

都是素数. 1640 年, 费马提出了如下猜想

猜想 (Fermat, 1640)

所有的费马数 F_n 都是素数.

这一猜想对前 5 个费马数成立, 于是费马宣称他找到了表示素数的公式. 然而, 欧拉在 1732 年否定了这一猜想, 他给出了 F_5 的分解式

证伪 (Euler, 1732)

$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$

事实上, 目前人们还未找到除前 5 个费马数以外的费马素数.

费马数的素因数

定理 (Euler)

F_n 的素因数 $p \equiv 1 \pmod{2^{n+1}}$.

费马数的素因数

定理 (Euler)

F_n 的素因数 $p \equiv 1 \pmod{2^{n+1}}$.

定义 (阶)

设 a, n 为互素的正整数.
a 模 n 的**阶** (order) 是指最小的正整数 k 满足 $a^k \equiv 1 \pmod{n}$.
阶的性质: 对正整数 l, 若 $a^l \equiv 1 \pmod{n}$, 则 $k \mid l$.

费马数的素因数

定理 (Euler)

F_n 的素因数 $p \equiv 1 \pmod{2^{n+1}}$.

定义 (阶)

设 a, n 为互素的正整数.
a 模 n 的**阶** (order) 是指最小的正整数 k 满足 $a^k \equiv 1 \pmod{n}$.
阶的性质: 对正整数 l, 若 $a^l \equiv 1 \pmod{n}$, 则 $k \mid l$.

证明.

$p \mid F_n = 2^{2^n} + 1 \Longrightarrow 2^{2^n} \equiv -1 \pmod{p}$, $2^{2^{n+1}} \equiv 1 \pmod{p}$
设 2 模 p 的阶为 d, 则 $d \nmid 2^n$, $d \mid 2^{n+1}$. 故 $d = 2^{n+1}$.
由费马小定理 $2^{p-1} \equiv 1 \pmod{p}$. 故 $2^{n+1} = d \mid p - 1$. □

费马数的素因数

定理 (Lucas)

对 $n \geq 2$, F_n 的素因数 $p \equiv 1 \pmod{2^{n+2}}$.

费马数的素因数

定理 (Lucas)

对 $n \geq 2$, F_n 的素因数 $p \equiv 1 \pmod{2^{n+2}}$.

公式

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

费马数的素因数

定理 (Lucas)

对 $n \geq 2$, F_n 的素因数 $p \equiv 1 \pmod{2^{n+2}}$.

公式

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

证明.

由 Euler 的结果 $p \equiv 1 \pmod{2^{n+1}}$, 故 $p \equiv 1 \pmod{8}$.
由公式 $\left(\frac{2}{p}\right) = 1$, 存在整数 x 使得 $x^2 \equiv 2 \pmod{p}$.
$x^{2^{n+1}} \equiv 2^{2^n} = F_n - 1 \equiv -1 \pmod{p}$, $x^{2^{n+2}} \equiv 1 \pmod{p}$.
设 x 模 p 的阶为 d, 则 $d \nmid 2^{n+1}$, $d \mid 2^{n+2}$. 故 $d = 2^{n+2}$.
由费马小定理 $x^{p-1} \equiv 1 \pmod{p}$. 故 $2^{n+2} = d \mid p-1$. □

目录

作业 6

问题

1. 设正整数 $m, n > 1$. 证明: 若 $m^n - 1$ 是素数, 则 $m = 2$ 且 n 是素数.
2. 设 p 是素数, 记 $M_p = 2^p - 1$, 这称为**梅森数**. 证明: 若 p, q 是不同的素数, 则
$$(M_p, M_q) = 1$$

证明.

1. $m^n - 1 = (m-1)(m^{n-1} + m^{n-2} + \cdots + 1)$. 故 $m-1=1$, $m=2$.
   若 $n = st$ 为合数, 其中正整数 $s, t > 1$.
   设 $k = 2^s > 2$, 则 $k^t - 1 = 2^{st} - 1 = 2^n - 1$ 是素数.
   由先前的结论 $k = 2$, 矛盾. 故 n 为素数.
2. 若 $(M_p, M_q) > 1$. 取其任一素因子 r, 则 $2^p, 2^q \equiv 1 \pmod{r}$.
   设 2 模 r 的阶为 d, 则 $d \mid p$, $d \mid q$, 只能 $d = 1$.
   故 $2 = 2^d \equiv 1 \pmod{r}$, 矛盾. 故 $(M_p, M_q) = 1$.

□

证明.

1. $m^n - 1 = (m-1)(m^{n-1} + m^{n-2} + \cdots + 1)$. 故 $m-1=1$, $m=2$.
   若 $n = st$ 为合数, 其中正整数 $s, t > 1$.
   设 $k = 2^s > 2$, 则 $k^t - 1 = 2^{st} - 1 = 2^n - 1$ 是素数.
   由先前的结论 $k = 2$, 矛盾. 故 n 为素数.
2. 若 $(M_p, M_q) > 1$. 取其任一素因子 r, 则 $2^p, 2^q \equiv 1 \pmod r$.
   设 2 模 r 的阶为 d, 则 $d \mid p$, $d \mid q$, 只能 $d = 1$.
   故 $2 = 2^d \equiv 1 \pmod r$, 矛盾. 故 $(M_p, M_q) = 1$.

□

思考

第二问的证明中, p, q 的条件是否能加强?

拓展

问题

设 p, q 是正整数. 证明: 若 $(p, q) = 1$, 则

$$(M_p, M_q) = 1$$

拓展

问题

设 p, q 是正整数. 证明: 若 $(p, q) = 1$, 则

$$(M_p, M_q) = 1$$

证明.

若 $(M_p, M_q) > 1$. 取其任一素因子 r, 则 $2^p, 2^q \equiv 1 \pmod{r}$.
设 2 模 r 的阶为 d, 则 $d \mid p$, $d \mid q$, $d \mid (p, q) = 1$, $d = 1$.
故 $2 = 2^d \equiv 1 \pmod{r}$, 矛盾. 故 $(M_p, M_q) = 1$. □

拓展

问题

设 p, q 是正整数. 证明: 若 $(p,q)=1$, 则

$$(M_p, M_q) = 1$$

证明.

若 $(M_p, M_q) > 1$. 取其任一素因子 r, 则 $2^p, 2^q \equiv 1 \pmod{r}$.
设 2 模 r 的阶为 d, 则 $d \mid p$, $d \mid q$, $d \mid (p,q) = 1$, $d = 1$.
故 $2 = 2^d \equiv 1 \pmod{r}$, 矛盾. 故 $(M_p, M_q) = 1$. $\square$

思考

底数 2 能否替换为更一般的 $a > 1$? (p,q) 是否有更一般的表示?

拓展

问题

设 a, p, q 是正整数, $a > 1$. 证明: $(a^p - 1, a^q - 1) = a^{(p,q)} - 1$.

拓展

问题

设 a, p, q 是正整数, $a > 1$. 证明: $(a^p - 1, a^q - 1) = a^{(p,q)} - 1$.

证明.

不妨 $p \geq q$. 由 Euclid 算法

$$(a^p - 1, a^q - 1) = (a^p - 1 - a^{p-q}(a^q - 1), a^q - 1) = (a^{p-q} - 1, a^q - 1)$$

其指数变化为 Euclid 算法, 故结果为 $a^{(p,q)} - 1$. □

梅森素数

1644 年, 法国数学家梅森 (Mersenne) 研究过形如 $M_p = 2^p - 1$ 的素数, 后来人们将这样的素数称为**梅森素数**. 是否存在无穷多个梅森素数是一个悬而未决的问题. **互联网梅森素数大搜索** (Great Internet Mersenne Prime Search, GIMPS) 是互联网上志愿者通过使用闲置计算机资源 (CPU/GPU) 寻找梅森素数的一个分布式计算项目. 通过此项目, 人们在 2024 年 10 月 21 日找到了第 52 个已知的梅森素数

$$M_{136279841},$$

也是迄今为止最大的素数.

梅森素数的性质

记 $M_n = 2^n - 1$.

性质 1

若 M_n 为素数, 则 n 为素数.

梅森素数的性质

记 $M_n = 2^n - 1$.

性质 1

若 M_n 为素数, 则 n 为素数.

性质 2

若素数 $n \equiv 3 \pmod 4$, 则 $2n+1 \mid M_n \iff 2n+1$ 为素数.

梅森素数的性质

记 $M_n = 2^n - 1$.

性质 1

若 M_n 为素数, 则 n 为素数.

性质 2

若素数 $n \equiv 3 \pmod 4$, 则 $2n+1 \mid M_n \iff 2n+1$ 为素数.

推论

对素数 $n > 3$, 若 $n \equiv 3 \pmod 4$ 且 $2n+1$ 为素数, 则 M_n 不为素数.

梅森素数的性质

记 $M_n = 2^n - 1$.

性质 1

若 M_n 为素数, 则 n 为素数.

性质 2

若素数 $n \equiv 3 \pmod 4$, 则 $2n+1 \mid M_n \iff 2n+1$ 为素数.

推论

对素数 $n > 3$, 若 $n \equiv 3 \pmod 4$ 且 $2n+1$ 为素数, 则 M_n 不为素数.

例子

$n = 11,\ 2n+1 = 23,\ M_n = 2^{11} - 1 = 2047 = 23 \times 89.$

性质 2 的证明

证明 1.

若 $2n+1 \mid M_n$. 任取素数 $p \mid 2n+1$, 则 $p \mid M_n = 2^n - 1$, $2^n \equiv 1 \pmod p$.
设 2 模 p 的阶为 d, 则 $d \mid n$, 由 n 为素数只可能 $d = n$.
由费马小定理 $2^{p-1} \equiv 1 \pmod p$. 故 $n = d \mid p-1$, $p \geq n+1$,
$p = 2n+1$. □

性质 2 的证明

证明 1.

若 $2n+1 \mid M_n$. 任取素数 $p \mid 2n+1$, 则 $p \mid M_n = 2^n - 1$, $2^n \equiv 1 \pmod p$.
设 2 模 p 的阶为 d, 则 $d \mid n$, 由 n 为素数只可能 $d = n$.
由费马小定理 $2^{p-1} \equiv 1 \pmod p$. 故 $n = d \mid p-1$, $p \geq n+1$,
$p = 2n+1$. □

证明 2.

若 $2n+1$ 为素数, 记为 p. 由 $n \equiv 3 \pmod 4$, $p = 2n+1 \equiv 7 \pmod 8$.
由费马小定理 $2^{2n} \equiv 1 \pmod p$, $p \mid 2^{2n} - 1 = (2^n - 1)(2^n + 1)$.
若 $p \mid 2^n + 1$, 则 $2^n \equiv -1 \pmod p$, $(2^{\frac{n+1}{2}})^2 = 2^{n+1} \equiv -2 \pmod p$.
然而 $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = -1 \times 1 = -1$, 矛盾.
故 $p \mid 2^n - 1 = M_n$. □

梅森素数的判定

令梅森数 $M_p = 2^p - 1$ 作为检验对象.

Lucas-Lehmer Test

定义序列 $\{s_i\}_{i \geq 0}$:

$$s_0 = 4, \quad s_i = s_{i-1}^2 - 2(i \geq 1)$$

对奇素数 p, M_p 是梅森素数当且仅当

$$s_{p-2} \equiv 1 \pmod{M_p}$$

Lucas-Lehmer Test

Algorithm 1 Determine if M_p is a Mersenne Prime

Require: an odd prime p.

Ensure: **True** if M_p is a prime, **False** otherwise.

$M_p \leftarrow 2^p - 1$

$s \leftarrow 4$

for $i \leftarrow 1$ to $p - 2$ **do**

  $s \leftarrow (s^2 - 2) \bmod M_p$

end for

if $s \equiv 0 \pmod{M_p}$ **then**

  return True

else

  return False

end if

目标: 给定正整数 N, 找出所有满足 $n \leq N$ 的梅森素数 M_n, 并输出 n.

1. 编程语言: `Python` (无限整数精度)
2. 算法: 输出 2; 对所有 $3 \leq n \leq N$, 先判定其是否为素数, 若是, 再用 Lucas-Lehmer Test 判定 M_n 是否为梅森素数, 若是, 输出 n.
3. 时间复杂度: 约为 $O(N^{3.3})$
4. 效果: $N = 10000$ 耗时 442.00 秒.

程序优化

1. 编程语言：C
2. GMP 大整数运算库
3. n 的预处理：通过 Eratosthenes 筛法筛选素数，利用性质 2 排除
4. 模运算优化：$\bmod\ 2^n - 1$
5. 系统优化：提高进程优先级
6. 并行优化：OpenMP 多线程计算

效果

- $N = 10000$ 耗时 1.67 秒, 速度提升近 300 倍.
- 4 小时计算出所有满足 $n \leq 150000$ 的梅森素数 M_n, 即前 30 个梅森素数.