组合数学第 11 讲

授课时间: 2024 年 11 月 11 日　授课教师: 孙晓明　记录人: 马振鑫

1　素数分布的阶

定理 1 (Chebyshev Theorem). 记 $\pi(n)$ 为 n 以内的素数个数, 则存在正常数 $0 < c_1 < c_2$ 使得

$$c_1 \frac{n}{\log_2 n} \le \pi(n) \le c_2 \frac{n}{\log_2 n}.$$

证明　对于 $\binom{2n}{n} = \frac{2n!}{n!n!}$，若存在大于 n 的素因子，它只在分子中出现一次, 故

$$\binom{2n}{n} = \prod_{p\le n, p\text{为素数}} p^{d_p(2n)-2d_p(n)} \prod_{n<p\le 2n, p\text{为素数}} p. \tag{1}$$

由上一讲对 Bertrand-Chebyshev 定理的证明知

$$\prod_{p\le n, p\text{为素数}} p^{d_p(2n)-2d_p(n)} \le 2^{\frac{4}{3}n + c\sqrt{2n}\ln 2 + c'\ln n}. \tag{2}$$

其中 c, c' 是与 n 无关的常数. 因为

$$\sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n},$$

且 $\binom{2n}{n}$ 为上式左侧求和式中的最大项，所以

$$\binom{2n}{n} > \frac{2^{2n}}{2n+1}. \tag{3}$$

联立 (1)(2)(3) 式可得

$$\prod_{n<p\le 2n, p\text{为素数}} p = \frac{\binom{2n}{n}}{\prod_{p\le n, p\text{为素数}} p^{d_p(2n)-2d_p(n)}} > \frac{\frac{2^{2n}}{2n+1}}{2^{\frac{4}{3}n + c\sqrt{2n}\ln 2 + c'\ln n}} > 2^{\frac{2}{3}n - c\sqrt{2n}\ln 2 - (c'-1/\ln 2 + 2)\ln n}.$$

又由于 $\prod_{n<p\le 2n, p\text{为素数}} p < (2n)^{\pi(2n)-\pi(n)}$，取对数得

$$\pi(2n) > \pi(2n) - \pi(n) > \frac{\frac{2}{3}n - c\sqrt{2n}\ln 2 - (c'-1/\ln 2+2)\ln n}{\log_2(2n)} \ge \frac{\tilde{c}n}{\log_2(2n)}.$$

即 $\pi(n) \ge \frac{\tilde{c}}{2}\frac{n}{\log_2 n}$.

另一方面，由上一讲引理 $\prod_{p\le n, p\text{为素数}} p \le 4^n$，有

$$4^n \ge \prod_{p\le n, p\text{为素数}} p \ge \prod_{\frac{n}{2}\le p\le n, p\text{为素数}} p \ge (\frac{n}{2})^{\pi(n)-\pi(\frac{n}{2})}.$$

取对数得

$$\pi(n) - \pi(\frac{n}{2}) \le \frac{2n}{\log_2 \frac{n}{2}}. \tag{4}$$

以下利用数学归纳法，证明 $\pi(n) \le 12\frac{n}{\log_2 n}$.

$n \le 8$ 时，通过计算发现命题成立.

假设 $n < k(k > 8)$ 时命题成立，则 $n = k$ 时，$\log_2 n > 3$，所以 $\log_2 n < \frac{3}{2}\log_2 \frac{n}{2}$

$$\pi(n) = \left(\pi(n) - \pi(\frac{n}{2})\right) + \pi(\frac{n}{2}) < \frac{2n}{\log_2 \frac{n}{2}} + \frac{6n}{\log_2 \frac{n}{2}} = \frac{8n}{\log_2 \frac{n}{2}} < \frac{12n}{\log_2 n}.$$

其中红色部分的估计由 (4) 式得到，蓝色部分的估计由归纳假设得到. 综合对 $\pi(n)$ 的上下界分析，我们得到

$$\frac{\tilde{c}}{2}\frac{n}{\log_2 n} \le \pi(n) \le 12\frac{n}{\log_2 n}.$$

□

2 特殊形式素数分布的讨论

定理 2. *存在无穷多个 $4k+3$ 型素数.*

证明 反证法，假设只有有限个 $4k+3$ 型素数，记为 $p_1 < p_2 < \ldots < p_s$，设 $M = 4p_1p_2\cdots p_s - 1$.

由于 M 是一个奇数且对于所有 i，有 $M \equiv -1 \pmod{p_i}$，因此 $2 \nmid M$，且 $p_i \nmid M$，因此 M 的素因子均为 $4k+1$ 型.

若对 M 做素因子分解，得到 $M = q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_t^{\alpha_t}$，其中的每个素因子均为 $4k+1$ 型的素数. 但是 $4k+1$ 型整数的乘积仍然是 $4k+1$ 型整数，而 $M \equiv 3 \pmod 4$，这说明 M 无法进行上述素因子分解，所以 M 一定有除 $p_1, p_2, \ldots, p_s$ 以外，更大的 $4k+3$ 型素因子，矛盾，因此命题得证. □

引理 3 (Fermat's little theorem)**.** *假设 a 是一个正整数，p 是一个素数，则有 $a^p \equiv a \pmod p$. 特别的，当 $p \nmid a$ 时，有 $a^{p-1} \equiv 1 \pmod p$.*

证明 见下一讲. □

引理 4. *若 p 是一个 $4k+3$ 型的素数，则不存在整数 x 使得 $x^2 \equiv -1 \pmod p$.*

证明 反证法，若存在 x 使得 $x^2 \equiv -1 \pmod p$，$p = 4k+3$，则 $p \nmid x$，故由 Fermat's little theorem，有

$$x^{p-1} \equiv 1 \pmod p;$$

另一方面，$x^{p-1} = x^{2(2k+1)} = (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod p$, 矛盾，故命题得证. □

定理 5. *存在无穷多个 $4k+1$ 型素数.*

证明 反证法，假设只有有限个 $4k+1$ 型素数，记为 $p_1 < p_2 < \cdots < p_s$，设 $M = 4{p_1}^2{p_2}^2\cdots{p_s}^2 + 1$.

同样由于 M 是一个奇数且对于所有 i，有 $M \equiv 1 \pmod{p_i}$，因此 $2 \nmid M$，且 $q_i \nmid M$. 因此 M 的素因子均为 $4k+3$ 型. 设 q 是 M 的一个 $4k+3$ 型素因子，则 $4p_1^2p_2^2\cdots p_s^2 = (2p_1p_2\cdots p_s)^2 \equiv -1 \pmod q$，这与上一个引理矛盾，所以 M 也没有 $4k+3$ 型素因子，进而 M 一定有除 $p_1, p_2, \ldots, p_s$ 以外，更大的 $4k+1$ 型素因子，矛盾，命题得证. □

3 二次剩余

定义 6. 对于素数 p 和整数 a，若存在整数 x 使得 $a \equiv x^2 \pmod p$, 则称 a 是模 p 的二次剩余.

定义 7 (Legendre 符号)**.** 对于任意一个素数 p，记

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a, \exists x, s.t\ a \equiv x^2 \pmod p; \\ 0 & p \mid a; \\ -1 & otherwise. \end{cases}$$

引理 8. 素数域 $\mathbb{Z}_p$ 上的多项式 $P(x)$ 的不同根的个数不超过 $\deg P$.

证明 见下一讲. $\square$

定理 9 (Euler 判别定理)**.** 若 p 为奇素数，且 $(a,p)=1$，则有

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

证明 由 Fermat's little theorem，

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p.$$

故 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ 和 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 有且只有一个成立，它满足勒让德符号的取值范围. 以下只需证明

$$(\frac{a}{p}) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

一方面，当 $\left(\frac{a}{p}\right) = 1$ 时, 由定义知, 存在 t 使得 $a \equiv t^2 \pmod p$，由 Fermat's little theorem，

$$a^{\frac{p-1}{2}} \equiv t^{p-1} \equiv 1 \pmod p.$$

所以 $(\frac{a}{p}) = 1 \implies a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

另一方面，当 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 时，考虑同余方程 $x^{\frac{p-1}{2}} \equiv 1 \pmod p$，由上一个引理，该方程的不同解的个数不超过 $\frac{p-1}{2}$ 个. 再由 Fermat's little theorem，$1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ 均为此方程的解. 且对于不同的 $m,n \le \frac{p-1}{2}$，$m^2 - n^2 = (m+n)(m-n)$，其中 $0 < m+n, m-n < p$，所以 $p \nmid (m^2 - n^2)$，即 $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ 在模 p 意义下为互不相同的解，它们总共是 $\frac{p-1}{2}$ 个数，所以此同余方程有且仅有这些解，这说明 a 一定是其中的某个解，记为 t^2，所以 $a \equiv t^2 \pmod p$，$a^{\frac{p-1}{2}} \equiv 1 \pmod p \implies (\frac{a}{p}) = 1$.

综合以上两方面讨论，我们得到

$$(\frac{a}{p}) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

$\square$

推论 10.

$$(\frac{2}{p}) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

证明

见下一讲. □

定理 11. *存在无穷多个 $8k+7$ 型素数.*

证明 反证法,若只有有限个 $8k+7$ 型素数,记为 $p_1 < p_2 < \cdots < p_s$. 设 $M = 8{p_1}^2{p_2}^2\cdots{p_s}^2-1$.

对于任意一个素数 q,若 $q \mid M$, 即 $q \mid (4p_1p_2\cdots p_s)^2-2$ 即 $\left(\frac{2}{q}\right)=1$,所以 q 只能为 $8k\pm1$ 型素数.

而由假设,对于 $8k+7$ 型素数 p_i,$M \equiv -1 \pmod{p_i}$,故 M 只能有 $8k+1$ 型素因子.

若对 M 做素因子分解,得到 $M = q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_t^{\alpha_t}$,其中的每个素因子均为 $8k+1$ 型的素数. 但是 $8k+1$ 型整数的乘积仍然是 $8k+1$ 型整数,而 $M \equiv 7 \pmod 8$,这说明 M 无法进行上述素因子分解,所以 M 一定有除 $p_1, p_2, \ldots, p_s$ 以外,更大的 $8k+7$ 型素因子,矛盾,因此命题得证. □

4 选做题

证明对于充分大的 n, 在 $(n, 2n)$ 存在 $4k+3$ 型素数。

这个结论还可以推广到那些类型的数上?