组合数学第十一讲

授课时间: 2018年12月3日　授课教师: 孙晓明　记录人: 王靓璞　黄上京　方敏学

1　伯兰特-切比雪夫定理（Bertrand-Chebyshev Theorem）

定理 1. $\forall n \in \mathbb{N}$，$\exists$素数p，使得$p \in (n, 2n]$。

证明　我们将所有素数组成的集合记为P。对于一个素数p，首先定义函数

$$f_p(n) = \sum_{k \geq 1} [\frac{n}{p^k}],$$

此函数亦表示n的阶乘里能够整除p的最大阶数。

考虑组合数

$$\binom{2n}{n} = \frac{(2n)!}{n!n!}.$$

另一方面，

$$\binom{2n}{n} = \prod_{p \leq 2n, p \in P} p^{f_p(2n)-2f_p(n)}.$$

现在利用反证法证明定理。假如$(n, 2n]$之间不存在素数，则有

$$\binom{2n}{n} = \prod_{p \leq 2n, p \in P} p^{f_p(2n)-2f_p(n)} = \prod_{p \leq n, p \in P} p^{f_p(2n)-2f_p(n)}$$

$$= \prod_{p \leq \frac{2}{3}n, p \in P} p^{f_p(2n)-2f_p(n)} \prod_{\frac{2}{3}n < p \leq n, p \in P} p^{f_p(2n)-2f_p(n)} = AB,$$

其中

$$A = \prod_{p \leq \frac{2}{3}n, p \in P} p^{f_p(2n)-2f_p(n)},\ B = \prod_{\frac{2}{3}n < p \leq n, p \in P} p^{f_p(2n)-2f_p(n)}.$$

先估计B的值。假设$n \geq 5$，当$p > \frac{2}{3}n$时，

$$f_p(2n) = \sum_{k \geq 1} [\frac{2n}{p^k}] < [\frac{2n}{\frac{2}{3}n}] + [\frac{2n}{\frac{4}{9}n^2}] + \cdots = 3,$$

$$f_p(n) = \sum_{k \geq 1} [\frac{n}{p^k}] \geq [\frac{n}{n}] + [\frac{n}{n^2}] + \cdots = 1.$$

所以，

$$0 \leq f_p(2n) - 2f_p(n) \leq 2 - 2 = 0.$$

故有，

$$B = \prod_{\frac{2}{3}n < p \leq n, p \in P} p^{f_p(2n)-2f_p(n)} = 1.$$

进而

$$\binom{2n}{n} = AB = A = \prod_{p \leq \frac{2}{3}n, p \in P} p^{f_p(2n)-2f_p(n)}.$$

接着把A分成两部分，写成：

$$A=\prod_{p\le\sqrt{2n},p\in P}p^{f_p(2n)-2f_p(n)}\prod_{\sqrt{2n}<p\le\frac{2}{3}n,p\in P}p^{f_p(2n)-2f_p(n)}=CD,$$

其中

$$C=\prod_{p\le\sqrt{2n},p\in P}p^{f_p(2n)-2f_p(n)},\ D=\prod_{\sqrt{2n}<p\le\frac{2}{3}n,p\in P}p^{f_p(2n)-2f_p(n)}.$$

先估计C的值。当$p\le\sqrt{2n}$时，考虑$f_p(2n)-2f_p(n)$：

$$f_p(2n)-2f_p(n)=\sum_{k\ge1}[\frac{2n}{p^k}]-2\sum_{k\ge1}[\frac{n}{p^k}]=\sum_{k\ge1}([\frac{2n}{p^k}]-2[\frac{n}{p^k}]).$$

因为对于$x=[x]+\{x\}$，我们有

$$[2x]=[2[x]+2\{x\}]=2[x]+[2\{x\}]\le2[x]+1,$$

所以

$$\sum_{k\ge1}([\frac{2n}{p^k}]-2[\frac{n}{p^k}])=\sum_{k\ge1}([2\frac{n}{p^k}]-2[p^k])\le\sum_{k\ge1}^{\log_p 2n}1=[\log_p 2n].$$

因此，

$$C\le\prod_{p\le\sqrt{2n},p\in P}p^{[\log_p(2n)]}\le\prod_{p\le\sqrt{2n},p\in P}(2n)\le(2n)^{\sqrt{2n}}.$$

易知当$n\ge8192$时，

$$C\le(2n)^{\sqrt{2n}}=2^{\sqrt{2n}\log_2(2n)}<\frac{2^{\frac{1}{3}n}}{2n+1}.$$

最后来估计D。当$\sqrt{2n}<p\le\frac{2}{3}n$时，

$$f_p(2n)-2f_p(n)=[\frac{2n}{p}]+[\frac{2n}{p^2}]+\cdots-(2[\frac{n}{p}]+2[\frac{n}{p^2}]+\cdots)=[\frac{2n}{p}]-2[\frac{n}{p}]\le1,$$

所以，

$$D\le\prod_{\sqrt{2n}<p\le\frac{2}{3}n,p\in P}p\le\prod_{p\le\frac{2}{3}n,p\in P}p.$$

现在估计$\prod_{p\le\frac{2}{3}n,p\in P}p$的值。令

$$T_m=\prod_{p\le m,p\in P}p,$$

则

$$T_m=(\prod_{\frac{m}{2}<p\le m,p\in P}p)(\prod_{p\le\frac{m}{2},p\in P}p)\le T_{\frac{m}{2}}\binom{m}{\frac{m}{2}}\le T_{\frac{m}{2}}2^m\le T^{\frac{m}{4}}2^{\frac{m}{2}}2^m\le\cdots\le2^{2m},$$

所以，

$$\prod_{p\le\frac{2}{3}n,p\in P}p=T_{\frac{2}{3}n}\le2^{\frac{4}{3}n}.$$

由此得到：

$$\binom{2n}{n}=CD\le\frac{2^{\frac{1}{3}n}}{2n+1}\cdot2^{\frac{4}{3}n}=\frac{2^{\frac{5}{3}n}}{2n+1},$$

而另一方面，

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1},$$

矛盾。所以假设不成立。

所以对足够大的n ($n \geq 8192$)，$\exists p$是素数，使得$p \in (n, 2n]$。对于$n < 8192$的n，经过检验：

- $n = 1$, 取素数2;
- $n = 2$, 取素数3;
- $n \in [3, 4]$, 取素数5;
- $n \in [5, 6]$, 取素数7;
- $n \in [7, 12]$, 取素数13;
- $n \in [13, 22]$, 取素数23;
- $n \in [23, 42]$, 取素数43;
- $n \in [43, 82]$, 取素数83;
- $n \in [83, 162]$, 取素数163;
- $n \in [163, 316]$, 取素数317;
- $n \in [317, 630]$, 取素数631;
- $n \in [631, 1258]$, 取素数1259;
- $n \in [1259, 2502]$, 取素数2503;
- $n \in [2503, 5002]$, 取素数5003;
- $n \in [5003, 8191]$, 取素数8209;

亦满足题目要求。故定理成立。 □

2 素数定理（Prime Number Theorem）

定义函数

$$\pi(n) := |\{p | p \leq n, p \in P\}|$$

定理 2 (素数定理). *存在*$c_1, c_2 > 0$，*使得*$c_1 \frac{n}{\log_2 n} \leq \pi(n) \leq c_2 \frac{n}{\log_2 n}$，*即*$\pi(n) = \Theta(\frac{n}{\log_2 n})$.

证明 由伯兰特-切比雪夫定理的证明过程可知

$$\prod_{n < p \leq 2n, p \in P} p^{f_p(2n) - 2f_p(n)} \geq \frac{\frac{2^{2n}}{2n+1}}{\frac{2^{\frac{5}{3}n}}{2n+1}} = 2^{\frac{1}{3}n}.$$

当$n < p \le 2n$时

$$\begin{aligned} f_p(2n) - 2f_p(n) &= \left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \cdots - 2\left[\frac{n}{p}\right] - 2\left[\frac{2n}{p}\right] - \cdots \\ &= \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \le 1. \end{aligned}$$

故

$$(2n)^{\pi(2n)-\pi(n)} = \prod_{n<p\le 2n, p\in P}(2n) \ge \prod_{n<p\le 2n, p\in P} p \ge \prod_{n<p\le 2n, p\in P} p^{f_p(2n)-2f_p(n)}.$$

因此

$$\pi(2n) - \pi(n) \ge \log_{2n} 2^{\frac{1}{3}n} = \frac{n}{3(\log_2 n + 1)} \ge \frac{n}{6\log_2 n},$$

$$\pi(2n) \ge \frac{n}{6\log_2 n} + \pi(n).$$

从而

$$\pi(n) \ge \frac{\frac{n}{2}}{6\log_2 \frac{n}{2}} + \pi(\frac{n}{2}) \ge c_1 \frac{n}{\log_2 n},$$

其中$c_1 > 0$为常数。

另一方面，由伯兰特-切比雪夫定理的证明过程可知

$$\prod_{p\le n, p\in P} p = T_n \le 2^{2n},$$

又有

$$(\frac{n}{2})^{\pi(n)-\pi(\frac{n}{2})} \le \prod_{\frac{n}{2}<p\le n, p\in P} p \le \prod_{p\le n, p\in P} p,$$

得

$$\pi(n) - \pi(\frac{n}{2}) \le \log_{\frac{n}{2}} 2^{2n} = \frac{2n}{\log_2 \frac{n}{2}} = 4\frac{\frac{n}{2}}{\log_2 \frac{n}{2}}.$$

解此递推式，可得

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

其中$c_2 > 0$为常数。

□

3 狄利克雷定理（Dirichlet's Theorem）

定理 3. 对于任意互素的正整数a和b，存在无穷多个自然数k，使得$ak + b$是素数。

这条定理即是著名的狄利克雷定理。下面我们证明这一定理的某些特殊情况。

命题4. 形如$4k - 1$的素数有无穷多个。

证明 利用反证法：假设形如$4k - 1$的素数只有有限多个，分别设为$p_1, p_2, \cdots, p_n$。令

$$N = 4p_1 p_2 \cdots p_n - 1$$

则N不是素数且N是奇数，并且$p_1, p_2, \cdots, p_n$显然不是N的因子，从而N有且只有$4l+1$型的素因子，而$4l+1$型的素因子相乘只能得到$4l+1$型的数，矛盾！ □

同样的方法，我们也可以证明存在无穷多个$6k-1$型素数。而对于$4k+1$型素数，这种方法并不奏效。为此，我们需要用到二次剩余这一概念并对证明过程稍作修改。

二次剩余 对于一个素数p,称自然数a是模p的二次剩余，当且仅当存在一个自然数b，使得

$$b^2 \equiv a \pmod p$$

例1

$$1^2 \equiv 1 \pmod 7$$

$$2^2 \equiv 4 \pmod 7$$

$$3^2 \equiv 2 \pmod 7$$

可知$1, 2, 4$是模7的二次剩余；同理可知$1, 3, 4, 5, 9$是模11的二次剩余，$1, 4$是模5的二次剩余。一般的，奇素数p有$\frac{p+1}{2}$个二次剩余。

引理5. *若素数$p = 4k-1$(k为正整数)，对于任意正整数a，$a^2 \not\equiv -1 \pmod p$。*

这个引理将在下节课被证明。

定理 6. *形如$4k+1$的素数有无穷多个。*

证明 利用反证法：假设形如$4k+1$的素数只有有限多个，分别设为$p_1, p_2, \cdots, p_n$。令

$$N = 4p_1^2 p_2^2 \cdots p_n^2 + 1$$

则N不是素数且N是奇数，并且$p_1, p_2, \cdots, p_n$显然不是N的因子，从而N有$4l-1$型的素因子q,从而有

$$N = 4p_1^2 p_2^2 \cdots p_n^2 + 1 \equiv 0 \pmod q,$$

则有

$$(2p_1 p_2 \cdots p_n)^2 \equiv -1 \pmod q,$$

这与引理5矛盾！ □