第 5 章　素数分布的初等结果

素数性质的研究不仅是数论中最为重要的内容在和之一，而且在公钥密码学中也占有很重要得地位. 前几章我们已经对素数的某些性质进行了探讨，这一章我们仍然讨论素数的其它性质及素数在整数中的分布问题-即素数定理，将介绍算术数列中素数分布的一个主要结果—即算术序列中的素数定理. 这一章的内容及结果在密码学中有非常广泛的应用，如整数的素分解是许多公钥密码算法安全的理论依据. 素数定理、算术序列中的素数定理分别说明了整数中、算术序列中素数分布的平均概率，为概率算法寻找素数提供理论依据.

§1　素数的基本性质与分布的主要结果介绍

本节我们简要介绍一下有关素数性质的几个结论以及素数分布的两个重要结果-素数定理与算术序列中的素数定理，对于前面已经介绍过的有关素数的性质和定理，在此仅给出简单回顾.

性质 1 （算术基本定理）对于任一大于 1 的整数 n，有以下的素分解

$$n = p_1^{a_1} \cdots p_r^{a_r} .$$

其中 $p_1, \cdots, p_r$ 是不同的素因子，如果不考虑素因子的顺序，这种分解是唯一的.

性质 1 说明了整数与素数之间的一种关系，实际上就是整数能表示成素数的乘积的形式，大整数的素分解是一个困难问题，在公钥密码学中，大量的密码算法就是建立在整数分解问题的基础之上.　另外关于算术基本定理的描述，还有一个分析等价形式，即

定理 1　　算术基本定理等价于

$$\prod_p (1-\frac{1}{p^s})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s>1. \tag{1}$$

这就是著名的 Euler 恒等式.

关于素数分布，我们已经在 1 章 1 节证明了素数有无穷多个，即

性质 2　素数有无穷多个，　即

$$\lim_{x\to\infty} \pi(x) = \infty$$

其中 $\pi(x)$ 表示不超过 x 的素数的个数.

关于 $\pi(x)$ 的主项估计已经有了精确的结果，这就是著名的素数定理，也称为不带余项估计的素数定理.

定理 2　（素数定理）

$$\pi(x)\sim\frac{x}{\ln x},\ x\to\infty. \qquad (2)$$

关于素数定理，早在 1800 年 Legendre 已经提出一个精确的估计：

$$\pi(x)\sim\frac{x}{\ln x-1.08366},\ x\to\infty.$$

另外，容易证明 $\int_2^x\frac{du}{\ln u}\sim\frac{x}{\ln x}$．记 $\mathrm{Li}\,x=\int_2^x\frac{du}{\ln u}$，素数定理经常也描述成

$$\pi(x)\sim\mathrm{Li}\,x,\qquad x\to\infty,$$

这就是 Gauss 给出的积分形式的猜测．

然而他们的猜测直到 1896 年才用高深的复变函数理论被证明．而对于这个结果的初等证明，却直到 1949 年才由 A.Selberg 和 P.Erdös 各自独立地给出．Selberg 为此获得了斐尔兹奖．本章第 3 节给出的是Ч е б ы ш е в 不等式的证明．

令 $R(x)=\pi(x)-Lix$，素数定理实际上等价于 $R(x)=o(\frac{x}{\ln x})$．对 $R(x)$ 的作出更精确的估计，称为带余项的素数定理．关于带余项的素数定理的估计属于解析数论中非常重要也是非常有趣的内容，并且已经有许多结果，这些结果的证明已经属于解析数论较深奥的内容，有兴趣的读者可参考[《素数定理的初等证明》潘承洞 潘承彪，上海科学技术出版社]．这里仅给出 1981 年 Balog 证明的一个结果．

定理 3 （Balog）$\pi(x)=Lix+O(x(\ln x)^{-\frac{5}{4}}(\ln\ln x))$．

最后，我们简单描述算术数列中的素数分布问题．在密码学中，经常需要选取大素数，这些素数一般通常具有某些特殊的形式．其中最为常见的是需要选取 $p-1$ 的分解因子是已知的素数．这种情况下的素数，常常需要从算术序列中选取．先给出下面的算术数列

$$b,b+a,b+2a,\cdots,b+ka,\cdots \qquad (3)$$

其中 $a\geq 3$，$1\leq b<a$，$(a,b)=1$．

我们已经知道自然数中有无穷多个素数，那么上面的算术数列中是否也有无穷多素数呢？Euler 曾宣布过当 $b=1$ 时算术数列（1）中有无穷多个素数，后来 A．M．Legendre 明确地提出它有无穷多个素数，但都没给出证明．虽然对特殊的 a 和 b，已证明了很多这样的结果，但一般结论是否成立，则是一个十分困难的猜想．Dirichlet 于 1837 年证明了这一猜想对 a 是素数时成立，继而利用他证明的二次型类数公式推出对一般的 a 猜想也成立，在这里就不给出证明，有兴趣的读者可以参阅相关资料．

素数分布问题一直是数论研究的中心课题之一，前面我们详细讲过素数定理的初等证明，知道不超过 x 的素数个数 $\pi(x)$ 的主项估计．而对于算术数列

$$\{ak+b \mid a \geq 3, 1 \leq b < a, (a,b)=1\}$$

是否也可以估计不超过 x 的素数的个数．回答是肯定的，只是证明过程已经不是初等数论所能证明的．需要用到解析数论中高深的知识，有兴趣的同学可以查看相关文献．

本节仅给出算术序列素数分布的一个结果．

定义 $\pi(x;a,b)$ 表示数列

$$\{ak+b \mid a \geq 3, 1 \leq b < a, (a,b)=1\}$$

中不超过 x 的素数个数，即

$$\pi(x;a,b)=\{p \mid p \text{ 为素数且 } p \equiv b(\bmod a),\ p < x\}.$$

关于 $\pi(x;a,b)$ 的估计有下列结果．

定理 4 若 $(a,b)=1$，则

$$\pi(x;a,b)=\frac{1}{\phi(a)}Lix+O(xe^{-c\sqrt{\log x}}),$$

其中 $a \leq (\log x)^A$， $A>0$ 是常数， $c>0$ 是与 A 有关的常数， $\phi(a)$ 是 Euler 函数．特别地，

$$\pi(x)=Lix+O(x^{-c\sqrt{\log x}}).$$

由定理 4 与 $\pi(x) \sim \frac{x}{\ln x}$ 知算术序列 $\{ak+b \mid k=0,1,2,...,\}$ 中的素数分布的平均概率为 $\frac{1}{\varphi(a)\ln x}$．这个概率为概率多项式时间内寻找这种形式 $p \equiv b(\bmod a)$ 的素数提供理论根据．

§2 Euler 恒等式的证明

上节已经给出算术基本定理的分析等价形式—Euler 恒等式．本节我们将给出 Euler 恒等式的理论证明．首先需要证明两个相关的引理．

引理 1 当实数 $s>1$ 时，无穷乘积

$$\prod_p (1-\frac{1}{p^s})^{-1} \qquad (4)$$

收敛且大于 1，这里的连乘号表示对所有素数求积．

证明　由对数的性质可得

$$0<\frac{1}{p^s}<\ln(1-\frac{1}{p^s})^{-1}=\ln(1+\frac{1}{p^s-1})<\frac{1}{p^s-1},\ s>0.\qquad(5)$$

因而有

$$\sum_p\frac{1}{p^s}<\sum_p\ln(1-\frac{1}{p^s})^{-1}<\sum_p\frac{1}{p^s-1}$$

$$<2\sum_p\frac{1}{p^s}<2\sum_{n=1}^{\infty}\frac{1}{n^s},\ s>1.$$

这里求和号$\sum_p$表示对全体素数p求和．由于当$s>1$时级数$\sum_{n=1}^{\infty}n^{-s}$收敛，所以正项级数

$$\sum_p\ln(1-\frac{1}{p^s})^{-1},$$

当$s>1$时也收敛，由此就推出无穷乘积（1）收敛，它的值大于1是显然的，证毕．

若算术基本定理在没有被证明的情况下，假定任意整数n表示成下列形式的个数为$c(n)$

$n=p_1^{a_1}\cdots p_r^{a_r}$，$p_1,\cdots,p_r$是不同的素因子，且不考虑素因子的顺序，则下列结论成立．

引理 2

$$\prod_p(1-\frac{1}{p^s})^{-1}=\sum_{n-1}^{\infty}\frac{c(n)}{n^s}.\qquad(6)$$

证明 当实数$s>1$时，

$$(1-\frac{1}{p^s})^{-1}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots,$$

对任给的正整数N，取正整数k，$2^{k-1}\le N<2^k$，我们有

$$\sum_{n=1}^{N}\frac{c(n)}{n^s}\le\prod_{p\le N}(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots+\frac{1}{p^{ks}}),\ s>1.\qquad(7)$$

当$s>1$时由引理 1 知上式的无穷乘积收敛，所以由上式知式（6）右边的正项级数收敛，且有

$$\sum_{n=1}^{\infty}\frac{c(n)}{n^s}\le\prod_p(1-\frac{1}{p^s})^{-1}.\qquad(8)$$

反过来，对任给的正整数 M 及 h，取 $N_1=\prod_{p\le M}p^h$， 由算术基本定理知

$$\prod_{p\le M}(1+\frac{1}{p^s}+\cdots+\frac{1}{p^{hs}})\le\sum_{n=1}^{N_1}\frac{c(n)}{n^s}，\ s>1.$$

令 $h\to+\infty$， $M\to+\infty$ 由上式得

$$\prod_{p\le M}(1-\frac{1}{p^s})^{-1}\le\sum_{n=1}^{\infty}\frac{c(n)}{n^s}，\ s>1.$$

由此及式（7）就证明了引理 2.

定理 1 的证明　算术基本定理成立，则 $c(n)=1$，从而式(1)成立. 反过来，若（1）成立，则由引理 2 知

$$\sum_{n=1}^{\infty}\frac{c(n)-1}{n^s}=0，\ s>1.$$

由于对所有的 n 都有 $c(n)-1\ge 0$，由此及上式就推出 $c(n)=1$，从而算术基本定理成立.

3　素数定理的初等证明

在证明素数定理之前，先定义一个数论函数，即 Möbius 函数 $\mu(n)$

$$\mu(n)=\begin{cases}1, & n=1,\\ (-1)^s, & n=p_1p_2\cdots p_s, p_1<\cdots<p_s,\\ 0, & 其他.\end{cases}$$

关于 $\mu(n)$，有以下重要性质.

引理 1

$$\sum_{d|(n,P_s)}\mu(d)=\begin{cases}1, & (n,P_s)=1,\\ 0, & (n,P_s)>1,\end{cases}\quad P_s=p_1p_2\cdots p_s \qquad (1)$$

引理 2　设 $x>0$，$p_1,p_2,\cdots,p_s$ 为前 s 个素数，$\Phi(x,s)$ 表示不超过 x 且不被 $p_i(1\le i\le s)$ 所整除的自然数的个数， $P_s=p_1p_2\cdots p_s$. 则

$$\Phi(x,s)=\sum_{d|P_s}\mu(d)\left[\frac{x}{d}\right]. \tag{2}$$

证明 由式（1）知

$$\Phi(x,s)=\sum_{n\le x}\sum_{d|(n,P_s)}\mu(d)$$

$$=\sum_{d|P_s}\mu(d)\sum_{\substack{n\le x\\ d|n}}1=\sum_{d|P_s}\mu(d)\left[\frac{x}{d}\right].$$

证毕.

引理 3 设 s 为自然数，$x>s$，则

$$\pi(x)<x\prod_{i=1}^{s}(1-\frac{1}{p_i})+2^{s+1}, \tag{3}$$

这里 $p_1,p_2,\cdots,p_s$ 为前 s 个素数.

证明 因为大于 p_s 而又不超过 x 的素数不能被前 s 个素数整除，所以

$$\pi(x)\le s+\Phi(x,s)\,.$$

由引理 2 得

$$\pi(x)\le s+\sum_{d|P_s}\mu(d)\left[\frac{x}{d}\right]$$

$$=s+(x-\sum_{i=1}\left[\frac{x}{p_i}\right]+\sum_{1\le i\le j\le s}\left[\frac{x}{p_ip_j}\right]+\cdots+(-1)^s\left[\frac{x}{p_1p_2\cdots p_s}\right]$$

$$<s+x(1-\sum_{i=1}^{s}\frac{1}{p_i}+\cdots(-1)^s\frac{1}{p_1p_2\cdots p_s})+(\sum_{i=1}^{s}1+\sum_{1\le i\le j\le s}1+\cdots+1)$$

$$<s+x\prod_{i=1}^{s}(1-\frac{1}{p_i})+(1+\binom{s}{1}+\binom{s}{2}+\cdots+1)$$

$$=x\prod_{i=1}^{s}(1-\frac{1}{p_i})+s+(1+1)^s\,.$$

由此立即推出式（3）. 证毕.

引理 4

$$\prod_p (1-\frac{1}{p}) = 0 \qquad (4)$$

证明 设 N 为充分大的自然数，则显然有

$$\prod_p (1-\frac{1}{p})^{-1} > \prod_{p\le N} (1-\frac{1}{p})^{-1} = \prod_{p\le N} (\sum_{r=0}^{\infty} \frac{1}{p^r}) > \sum_{n=1}^{N} \frac{1}{n}.$$

由

$$\lim_{N\to\infty} \sum_{n\le N} \frac{1}{n} = \infty,$$

即可推出

$$\prod_p (1-\frac{1}{p}) = 0.$$

证毕

现在我们可以证明（3）式了.

定理 1 $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x} = 0$

证明 由引理 3 知

$$\pi(x) < x\prod_{i=1}^{s} (1-\frac{1}{p_i}) + 2^{s+1},$$

取 $s+1 = \left[\dfrac{\ln x}{2\ln 2}\right]$，则

$$0 < \frac{\pi(x)}{x} < \prod_{i=1}^{\left[\frac{\ln x}{2\ln 2}\right]-1} (1-\frac{1}{p_i}) + \frac{2^{\frac{\ln x}{2\ln 2}}}{x}.$$

上式右边在 $x\to\infty$ 时趋于零，所以

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0.$$

亦即 $\pi(x) = o(x)$，$x\to\infty$. 证毕.

定理 1 说明了素数在自然数中的“密度”很小（概率是 0）.

下面，我们要对素数分布函数 $\pi(x)$ 给出比较好的上下界估计，即 Чебышев 不等式.

定理 2 设 $x \ge 2$, 则

$$(\frac{\ln 2}{3})\frac{x}{\ln x}<\pi(x)<(6\ln 2)\frac{x}{\ln x} \tag{5}$$

及

$$(\frac{1}{6\ln 2})n\ln n<p_n<(\frac{8}{\ln 2})n\ln n,\quad n\geq 2 \tag{6}$$

p_n表示第n个素数.

证明 先来证明式（5）. 设m是正整数，$M=\frac{(2m)!}{(m!)^2}$. 由第一章例题知，M 不仅是正整数，而且

$$\ln M=\ln(2m)!-2\ln m!$$

$$=\sum_{p\leq m}\{a(p,2m)-2a(p,m)\}\ln p$$

$$=\sum_{m<p\leq 2m}a(p,2m)\ln p, \tag{7}$$

这里

$$\mathrm{a}(p,n)=\sum_{j=1}^{\infty}[\frac{n}{p^j}]. \tag{8}$$

显见，

$$a(p,2m)=1,\ m<p\leq 2m. \tag{9}$$

当$p\leq m$时，由$0\leq[2y]-2[y]\leq 1$及式（7）得

$$0\leq a(p,2m)-2a(p,m)=\sum_{j=1}^{\infty}\{[\frac{2m}{p^j}]-2[\frac{m}{p^j}]\}$$

$$\leq\sum_{j}1=\left[\frac{\ln(2m)}{\ln p}\right]. \tag{10}$$

这样由式（7），（9）及（10）得到

$$\sum_{m<p\leq 2m}\ln p\leq\ln m\leq\sum_{p\leq 2m}[\frac{\ln(2m)}{\ln p}]\ln p. \tag{11}$$

因而有

$$\{\pi(2m)-\pi(m)\}\ln m \le \ln M \le \pi(2m)\ln(2m)\,. \tag{12}$$

另一方面，我们直接来估计 M 的上、下界．我们有

$$M=\frac{2m}{m}\cdot\frac{2m-1}{m-1}\cdots\frac{m+1}{1}\ge 2^m\,, \tag{13}$$

$$M=\frac{(2m)!}{(m!)^2}<(1+1)^{2m}=2^{2m}\,. \tag{14}$$

由以上三式即得

$$\pi(2m)\ln(2m)\ge m\ln 2 \tag{15}$$

$$\{\pi(2m)-\pi(m)\}\ln m<2m\ln 2 \tag{16}$$

当 $x\ge 6$ 时，取 $m=\left[\frac{x}{2}\right]>2$，这时显然有 $2m\le x<3m$．因而有式（5）的左半不等式.

当 $m=2^k$ 时，由式（16）可得

$$k\left\{\pi(2^{k+1})-\pi(2^k)\right\}<2^{k+1}\,.$$

由此及 $\pi(2^{k+1})\le 2^k\ (k\ge 0)$ 可推出

$$(k+1)\pi(2^{k+1})-k\pi(2^k)<3\times 2^k\,.$$

对上式从 $k=0$ 到 $l-1$ 求和，得到

$$l\pi(2^l)<3\times 2^l\,.$$

对任意 $x\ge 2$，必有唯一的整数 $h\ge 1$，使得 $2^{h-1}<x\le 2^h$，因而有

$$\pi(x)\le\pi(2^k)<3\times\frac{2^k}{k}<(6\ln 2)\frac{x}{\ln x}\,.$$

这就证明了式（5）的右半不等式.

在上式中取 $x=p_n$，利用 $p_n>n$ 就得到

$$p_n>(\frac{1}{6\ln 2})n\ln\ p_n>(\frac{1}{6\ln 2})n\ln n\,.$$

这就证明了式（6）的左半不等式．设 $n>1$，在式（11）中取 $2m=p_n+1$，得到

$$n\ln(p_n+1)\geq\frac{(p_n+1)}{2}\ln 2\,.$$

进而有

$$\ln(p_n+1)\leq\ln(2n/\ln 2)+\ln\ln(p_n+1)\,. \tag{17}$$

当$s>-1$时，

$$\frac{s}{1+s}\leq\ln(1+s)=\int_0^s\frac{dt}{1+t}\leq s\,. \tag{18}$$

取$s=y/2-1$，由右半不等式即得

$$\ln y\leq\frac{y}{2}-(1-\ln 2)<\frac{y}{2},\qquad y>0\,.$$

取$y=\ln(p_n+1)$, 由上式及式（13）得

$$\ln(p_n+1)\leq 2\ln(\frac{2n}{\ln 2})<4\ln n\,,\qquad n\geq 3\,.$$

由此及式（17）的前一式，就推出当$n\geq 3$时式（6）的右半不等式成立，当$n<3$时直接验证式（6）的右半不等式成立，证毕.

由定理 1 立即可得到有关素数平均分布的一些估计，为此需要下面的引理.

引理 2　设$y\geq 2$, 我们有

$$\ln\ln([y]+1)-\ln\ln 2<\sum_{2\leq k\leq y}\frac{1}{k\ln k}<\ln\ln[y]+\frac{1}{2\ln 2}-\ln\ln 2 \tag{19}$$

及

$$[y](\ln[y]-1)+1<\sum_{1\leq k\leq y}\ln k$$

$$<([y]+1)\{\ln([y]+1)-1\}+2-2\ln 2 \tag{20}$$

证明 我们有

$$\int_k^{k+1}\frac{dt}{t\ln t}<\frac{1}{k\ln k}<\int_{k-1}^{k}\frac{dt}{t\ln t},\qquad k\geq 3\,.$$

因此，

$$\sum_{2\leq k\leq y}\frac{1}{k\ln k}<\frac{1}{2\ln 2}+\int_2^{[y]}\frac{dt}{t\ln t}$$

$$=\ln\ln[y]+\frac{1}{\ln 2}-\ln\ln 2$$

$$\sum_{2\le k\le y}\frac{1}{k\ln k}>\int_2^{[y]+1}\frac{dt}{t\ln t}=\ln\ln([y]+1)-\ln\ln 2\,.$$

由以上两式即得式（19）. 类似地，由

$$\int_{k-1}^{k}\ln t dt<\ln k<\int_k^{k+1}\ln t dt$$

可得

$$\sum_{1\le k\le y}\ln k<\int_2^{[y]+1}\ln t dt=t\ln t\Big|_2^{[y]+1}-\int_2^{[y]+1}dt$$

$$=([y]+1)\ln([y]+1)-([y]+1)+2-2\ln 2$$

和

$$\sum_{1\le k\le y}\ln k>\int_1^{[y]}\ln t dt=[y]\ln[y]-[y]+1\,.$$

这就证明了式（20）.

由引理 3 及（6）立即推出

定理 3　设 $x\ge 5$ 一定存在正常数 $c_1,c_2,\cdots,c_6$ 使得

$$c_1\ln\ln x<\sum_{p\le x}\frac{1}{p}<c_2\ln\ln x\,,\tag{21}$$

$$c_3x<\sum_{p\le x}\ln p<c_4x\,,\tag{22}$$

$$c_5\ln x<\sum_{p\le x}\frac{\ln p}{p}<c_6\ln x\,,\tag{23}$$

此外

$$\lim_{n\to\infty}(\ln p_n)/(\ln n)=1\,.\tag{24}$$

证明　式（24）由式（6）立即推出。由式（6）容易推出

$$a_1\ln n<\ln p_n<a_2\ln n\,,\qquad n\ge 2\tag{25}$$

$$a_3\ln\ln n<\ln\ln p_n<a_4\ln\ln n\,,\qquad n\ge 25\tag{26}$$

其中，a_1,a_2,a_3,a_4 是和 n 无关的正常数。下面来证式(21)——(23). 不妨设 $x\ge 100$. 令 $p_m\le x<p_{m+1}$，于是 $m\ge 25$。先来证式（21）. 由式（6）知，存在正常数 a_5， a_6 使得

$$a_5\sum_{k=2}^{m}\frac{1}{k\ln k}<\sum_{p\le x}\frac{1}{p}=\sum_{k=1}^{m}\frac{1}{p_k}<a_6\sum_{k=2}^{m}\frac{1}{k\ln k}+\frac{1}{2},$$

进而由式（19），$m\ge 25$推出存在正常数a_7，a_8使得

$$a_7\ln\ln(m+1)<\sum_{p\le x}\frac{1}{p_k}<a_8\ln\ln m.$$

进而由式（26）及$m\ge 25$知，

$$\ln\ln m<a_3^{-1}\ln\ln p_m\le a_3^{-1}\ln\ln x,$$

$$\ln\ln(m+1)>a_4^{-1}\ln\ln p_{m+1}>\ln\ln x,$$

由以上三式就推出式（21）.

下面来证式（22）. 由式（25）得

$$a_1\sum_{k=2}^{m}\ln k<\sum_{p\le x}\ln p=\sum_{k=1}^{m}\ln p_m<a_2\sum_{k=2}^{m}\ln k+\ln 2.$$

利用式（20）及$m\ge 25$，就推出存在正常数a_9，a_{10}使得

$$a_9(m+1)\ln(m+1)<\sum_{p\le x}\ln p<a_{10}m\ln m,$$

进而由式（20）及$m\ge 25$推出

$$m\ln m<(6\ln 2)p_m\le(6\ln 2)x$$

及

$$(m+1)\ln(m+1)>(\ln 2/8)p_{m+1}>(\ln 2/8)x,$$

由以上三式就推出式（22）.

最后来证式（13）. 由式（6）及（25）知，存在正常数a_{11},a_{12}使得

$$\frac{a_{11}}{n}<\frac{(\ln p_n)}{p_n}<\frac{a_{12}}{n},\quad n\ge 1.$$

因此

$$a_{11}\sum_{k=1}^{m}\frac{1}{k}<\sum_{p\le x}\frac{\ln p}{p}=\sum_{k=1}^{m}\frac{\ln p_k}{p_k}<a_{12}\sum_{k=1}^{m}\frac{1}{k}.$$

由此及

$$\ln(m+1)=\int_1^{m+1}t^{-1}dt<\sum_{k=1}^{m}\frac{1}{k}<1+\int_1^{m}t^{-1}dt=1+\ln m\ .$$

得到

$$a_{11}\ln(m+1)<\sum_{p\le x}(\ln p)/\,p<2a_{12}\ln m\ .$$

由式（25）可得

$$\ln m<a_1^{-1}\ln p_m<a_1^{-1}\ln x\ ,$$

$$\ln(m+1)>a_2^{-1}\ln p_{m+1}>a_2^{-1}\ln x\ .$$

由以上三式就推出式（13）. 证毕.

§4 素数定理的等价命题

为了证明素数定理，Чебышев引进了两个重要函数来代替$\pi(x)$,它们是

$$\theta(x)=\sum_{p\le x}\ln p \tag{1}$$

和

$$\psi(x)=\sum_{n\le x}\Lambda(n) \tag{2}$$

其中$\Lambda(n)$是定义为

$$\Lambda(n)=\begin{cases}\ln p, & n=p^{\alpha},\ p\text{是素数},\alpha\ge 1,\\ 0, & \text{其他}.\end{cases} \tag{3}$$

通常称$\Lambda(n)$为Mangoldt函数. 这两个函数讨论起来要比$\pi(x)$方便的多. 我们先来证明一个定理说明三个函数的关系.

定理1 设$x\ge 2$，那么存在正常数c，使得

$$(\ln x-c)\pi(x)<\theta(x)<(\ln x)\pi(x) \tag{4}$$

及

$$\theta(x)\le\psi(x)\le\theta(x)+x^{\frac{1}{2}}\ln x\ . \tag{5}$$

证明 先来证式（4）. 我们有

$$\theta(x)=\sum_{p\le x}\ln p=\sum_{k\le x}\ln k(\pi(k)-\pi(k-1))$$

$$=-\sum_{k=2}^{[x]-1}\pi(k)(\ln(k+1)-\ln k)+\pi([x])\ln[x]\,.$$

利用

$$\frac{s}{1+s}\le\ln(1+s)=\int_0^s\frac{dt}{1+t}\le s$$

的左边得

$$\frac{1}{y+1}<-\ln(1-\frac{1}{y+1})=\ln(1+\frac{1}{y})<\frac{1}{y}\,,\ y\ge1\,,\qquad(6)$$

由此得

$$\pi(x)\ln[x]-\sum_{k=2}^{[x]-1}\frac{1}{\ln k}<\theta(x)<\pi(x)\ln x-\sum_{k=2}^{[x]-1}\frac{1}{k+1}\,.$$

由Чебышев不等式得

$$\sum_{k=2}^{[x]-1}\frac{\pi(k)}{k}<a_1\sum_{k=2}^{[x]-1}\frac{1}{\ln k}<\frac{a_1}{\ln 2}+a_1\int_2^x\frac{dt}{\ln t}$$

$$=\frac{a_1}{\ln 2}+a_1\left\{\int_2^{\sqrt{x}}\frac{dt}{\ln t}+\int_{\sqrt{x}}^x\frac{dt}{\ln t}\right\}$$

$$<\frac{a_1}{\ln 2}+\frac{a_1}{\ln 2}\sqrt{x}+a_1\frac{x}{\ln x}$$

$$<a_2\pi(x)\,.$$

最后一步用到了$\sqrt{x}<\dfrac{x}{\ln x}$（为什么），这里$a_1$，$a_2$是正常数．此外

$$\ln[x]>\ln(x-1)=\ln x+\ln(1-\frac{1}{x})$$

$$>\ln x-\frac{1}{x-1}\,.$$

由以上三式即得式（4）.

下面来证式（5）．我们知道

$$\psi(x)=\sum_{n\le x}\Lambda(n)=\sum_{p^a\le x}\ln p\,,$$

右边是在对素变数p，以及整变数a满足条件$p^a\le x$的范围上求和．显见，对固定的p，a的

求和范围是$1 \le a \le \dfrac{\ln x}{\ln p}$，所以有（记$a_p = \dfrac{\ln x}{\ln p}$）.

$$\begin{aligned}\psi(x) &= \sum_{p \le x} \ln p + \sum_{\substack{p^a \le x \\ a \ge 2}} \ln p \\ &= \theta(x) + \sum_{p \le \sqrt{x}} \ln p \sum_{2 \le a \le a_p} 1 \\ &\le \theta(x) + \sum_{p \le \sqrt{x}} \ln p \cdot \frac{\ln x}{\ln p} \\ &\le \theta(x) + x^{\frac{1}{2}} \ln x .\end{aligned}$$

由此就推出式（5）. 证毕.

定理 1 表明了为什么引入$\theta(x)$和$\psi(x)$来代替$\pi(x)$研究素数的分布，总起来说，就是

定理 2　设$x \ge 2$，

（I）以下三个命题等价

1. 存在正常数d_1，d_2使得

$$d_1 x / \ln x < \pi(x) < d_2 x / \ln x .$$

2. 存在正常数d_3，d_4使得

$$d_3 x < \theta(x) < d_4 x .$$

3. 存在正常数d_5，d_6使得

$$d_5 x < \psi(x) < d_6 x .$$

（II）以下三个命题等价

4. $\lim\limits_{x \to \infty} \pi(x) \ln x / x = 1 .$

5. $\lim\limits_{x \to \infty} \theta(x) / x = 1 .$

6. $\lim\limits_{x \to \infty} \psi(x) / x = 1 .$