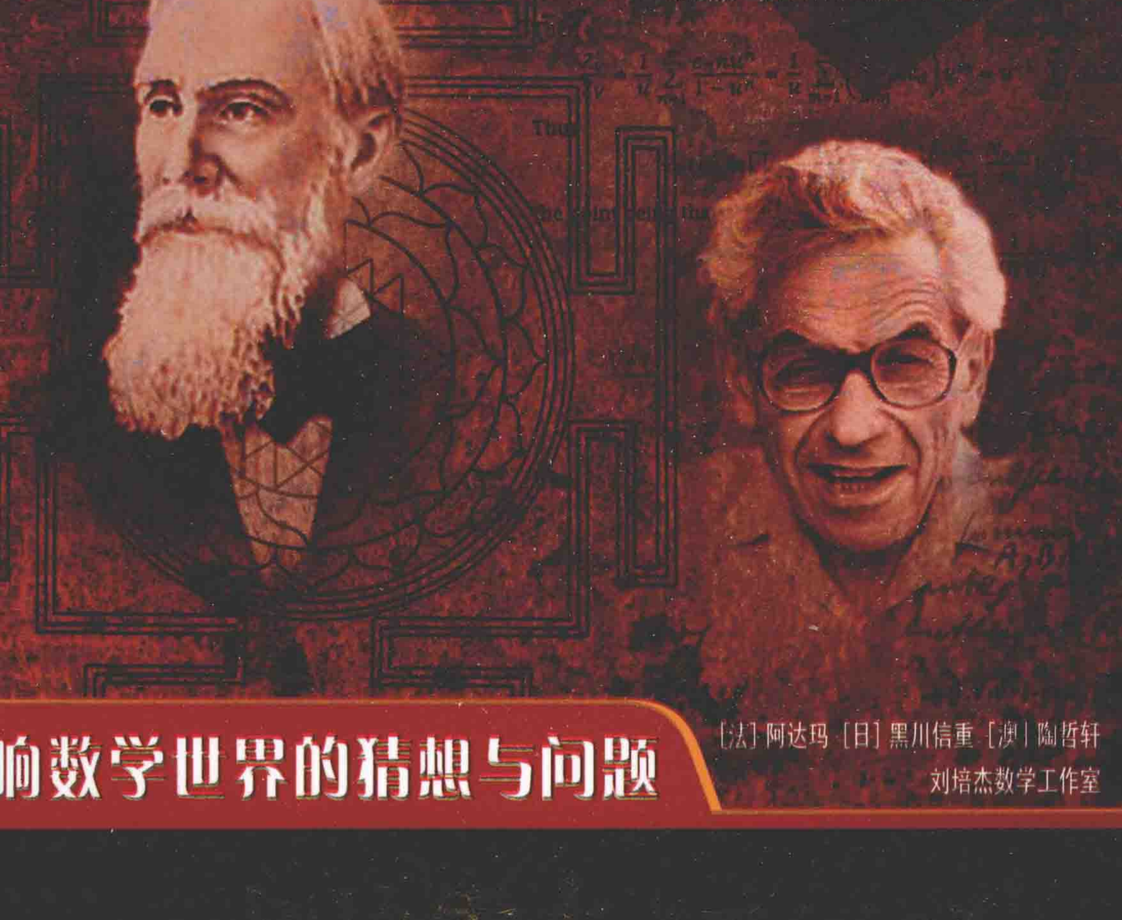
国家出版基金资助项目

国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

切比雪夫——彼得堡数学学派奠基人，机械大师，专攻经典问题，善用初等工具获高深结果。

爱尔特希——多产数学家，沃尔夫奖得主，无固定职位，世界各地游荡，与多人合作遍解数学难题。



影响数学世界的猜想与问题

[法] 阿达玛 [日] 黑川信重 [澳] 陶哲轩
刘培杰数学工作室

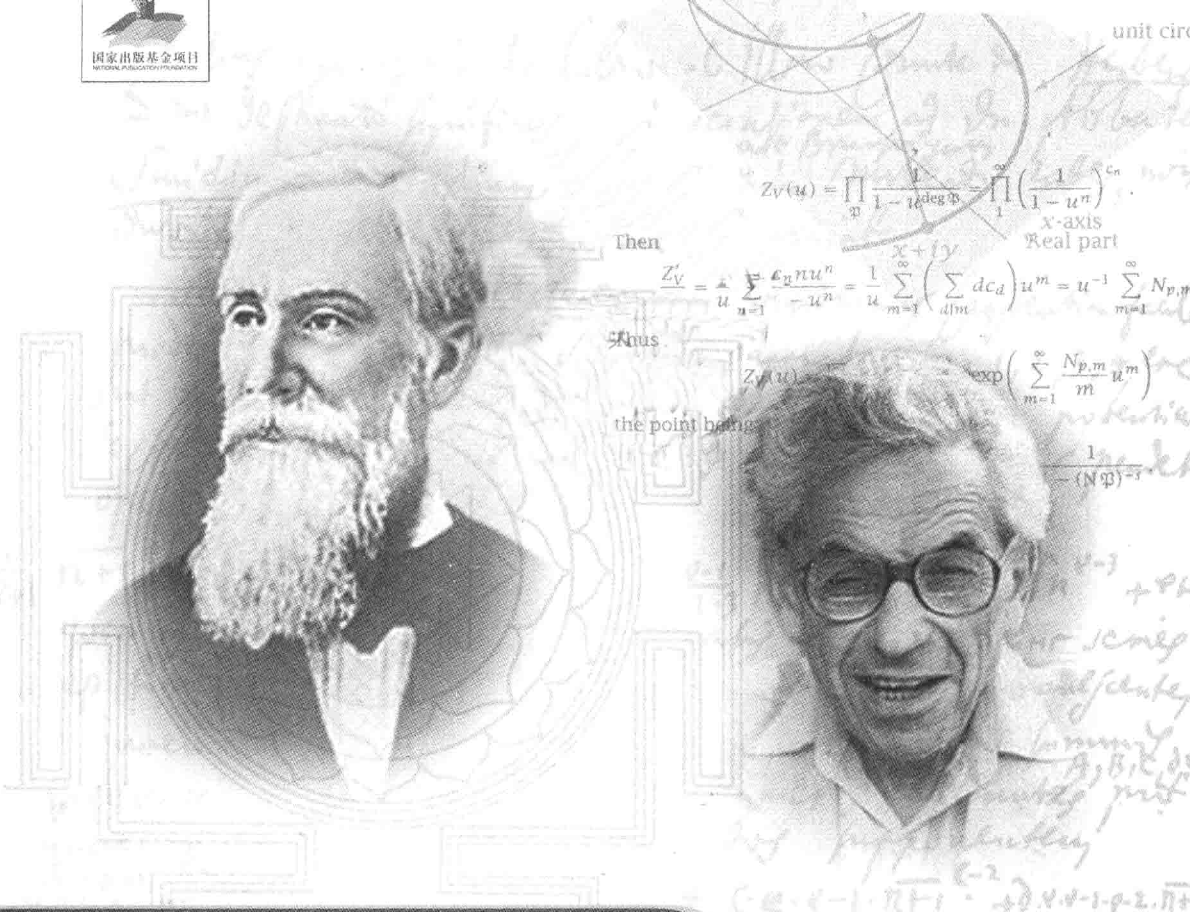
从切比雪夫到爱尔特希（下）
——素数定理的历史

From Chebyshev to Erdös (II)
——The History of The Prime Number Theorem

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

国家出版基金资助项目

国家出版基金项目 NATIONAL PUBLICATION FOUNDATION



影响数学世界的猜想与问题

[法] 阿达玛 [日] 黑川信重 [澳] 陶哲轩 著

刘培杰数学工作室 译

从切比雪夫到爱尔特希（下）

——素数定理的历史

From Chebyshev to Erdös (II)

—The History of The Prime Number Theorem

哈爾濱工業大學出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书包括素数的进展简介、素数无限性六证、素数中的长等差数列、素数定理的初等证明、素数定理等十三章。通过学习本书,对于了解素数定理相关各方面知识间的相互联系,提高观察问题、分析问题和解决问题的能力,以至对素数定理作进一步的研究,是很有裨益的。

本书可供大学数学专业的师生,数学工作者及数学爱好者参考。

图书在版编目(CIP)数据

从切比雪夫到爱尔特希. 下,素数定理的历史/(法)阿达玛,(日)黑川信重,(澳)陶哲轩著;刘培杰数学工作室译. ——哈尔滨:哈尔滨工业大学出版社,2014.3

(影响数学世界的猜想与问题)

ISBN 978-7-5603-3919-1

Ⅰ.①从…　Ⅱ.①阿…②黑…③陶…④刘…　Ⅲ.①素数-定理证明　Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2013)第 006535 号

策划编辑　刘培杰　张永芹
责任编辑　张永芹　杨万鑫
出版发行　哈尔滨工业大学出版社
社　　址　哈尔滨市南岗区复华四道街 10 号　邮编 150006
传　　真　0451-86414749
网　　址　http://hitpress.hit.edu.cn
印　　刷　黑龙江省地质测绘印制中心印刷厂
开　　本　787mm×1092mm　1/16　印张 24.5　字数 466 千字
版　　次　2014 年 3 月第 1 版　2014 年 3 月第 1 次印刷
书　　号　ISBN 978-7-5603-3919-1
定　　价　98.00 元

◎目录

素数的进展简介①

第一章

§1 素 数

素数 2,3,5,7,11,13,17,…,就是对自然数 1,2,3,4,5,6,7,… 进行因子分解的时候,最后不能再分解的那些自然数(但是,1 不称为素数). 这就像分解宇宙的物质,终于找到原子和质子一样.

人们对素数的研究是从 2 500 年前古希腊时代开始的,其中以毕达哥拉斯(以毕达哥拉斯定理,即三平方定理而著名)为中心人物. 据说他认为宇宙万物(树、马及人类等)都是由素数产生的,而素数有无限个则确已证明了(用反证法证明. 假设只有有限个素数 $p_1,p_2,p_3,\cdots,p_n$ 存在,那么对于自然数 $p_1\cdot p_2\cdot\cdots\cdot p_n+1$,不论用哪个素数都除不尽它 —— 这是因为用 $p_1,p_2,\cdots,p_n$ 中的任一个来除它都余 1,与假设是矛盾的).

从那时开始的数学(数论)之梦就是写出无一遗漏地记载所有素数的"全素数表". 这个梦想什么时候才能实现呢? 比如,在杂志《数学 セシナー》的 2096 年 1 月号上,完成"全素数表"连载,这种无法实现的事情能发生吗? 如果能,那么不论是利用时间机器(time machine)还是其他什么,也绝对希望把那张表弄到手. 如果时间机器赶不及,那么只好寄希望于预订从现在起 100 年的《数学 セシナー》.

① 素数 いろいろ/素数定理 100 年. 译自:数学 セシナー,Vol. 34,No. 12,1995,42 - 46.

“全素数表”对现在的地球数学来说是个梦,也许外星人能带来. 对素数附上颜色,“全素数表”就是一个形如图1.1并涂有不同色彩的“素数圆板”,从整体上看,不是闪烁着美丽的光辉吗?

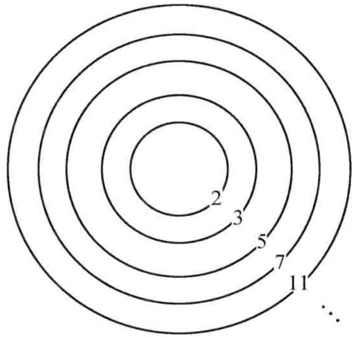


图1.1

§2 素数定理

虽然我们现在还见不到“全素数表”,但关于素数是怎样分布的问题,从素数定理能大概知道. 即使说素数的分布也还是含糊不清,我们现在仍可以先看个数为止的素数究竟有多少个.

比如,10以下的素数有2,3,5,7共4个(图1.2).

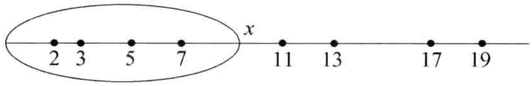


图1.2

我们数一下100以内的素数有:2,3,5,…,97,正好25个. 为了将这样的描述写成易懂的方式,我们将正数x以下的素数的个数记为$\pi(x)$(这里的π与圆周率无关,而是作为与素数prime的开头字母p相对应的希腊字的首字母而使用的符号). 这样,可以简单地写为

$$\pi(10)=4,\pi(100)=25$$

这时

$$\pi(x) \sim \frac{x}{\log x}, x\to+\infty$$

这里出现的 ~ 是几乎相等的意思,准确的意思是说:“用$\frac{x}{\log x}$去除$\pi(x)$所得的商(比),随x增大渐渐趋近于1.”用另一种记号来写就是

$$\lim_{x\to+\infty}\frac{\pi(x)}{\left(\dfrac{x}{\log x}\right)}=1$$

这就是在 1896 年就已经被证明了的素数定理，是由 J·阿达马(J. Hadamard) 和瓦莱普桑(Ch. de la Vallée-Poussin) 彼此独立证明的.

在这个素数定理的证明中,使用了欧拉发现的 ζ 函数

$$\zeta(s)=\frac{1}{\left(1-\dfrac{1}{2^s}\right)\times\left(1-\dfrac{1}{3^s}\right)\times\left(1-\dfrac{1}{5^s}\right)\times\left(1-\dfrac{1}{7^s}\right)\times\cdots}$$

分母是取遍所有素数的一种乘积. 把这个式子计算一下,得出

$$\begin{aligned}\zeta(s)&=\frac{1}{1-\dfrac{1}{2^s}}\times\frac{1}{1-\dfrac{1}{3^s}}\times\frac{1}{1-\dfrac{1}{5^s}}\times\frac{1}{1-\dfrac{1}{7^s}}\times\cdots=\\&\left(1+\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{8^s}+\cdots\right)\times\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\times\left(1+\frac{1}{5^s}+\cdots\right)\times\\&\left(1+\frac{1}{7^s}+\cdots\right)\times\cdots=\\&1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\frac{1}{7^s}+\frac{1}{8^s}+\frac{1}{9^s}+\frac{1}{10^s}+\cdots\end{aligned}$$

从以上可以看出,所说的 ζ 函数具有两种表示(关于所有素数的一种乘积以及关于全体自然数的一种和).

这是 ζ 函数最初被揭示的秘密. 如果使用这个关键点,立刻可以证明素数有无限个,不过这不是毕达哥拉斯当时的方法.

为此将 s 代换成 1 考虑 $\zeta(1)$ 即可

$$\frac{1}{1-\dfrac{1}{2}}\times\frac{1}{1-\dfrac{1}{3}}\times\frac{1}{1-\dfrac{1}{7}}\times\cdots=$$

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\cdots$$

因为知道其右边无穷大(如此加下去,没有尽头,不断增大),所以左边也无穷大,从

$$\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{3}+\frac{1}{4}}+\boxed{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}+$$

$$\boxed{\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}}+\cdots>$$

$$\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{4}+\frac{1}{4}}+\boxed{\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}}+$$

$$\boxed{\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}}+\cdots=$$

$$\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\cdots=+\infty\text{(无限大)}$$

而得知素数有无穷个(因为如果素数只有有限个,左边也就变为有限的了).

将这一朴素的想法稍加精细化,就可以证明素数定理.

这时必要的 ζ 性质是:即使变量 s 为复数,$\zeta(s)$ 仍有意义(称为解析开拓),特别是 s 的实部 $\mathrm{Re}(s)$ 若为 1 以上,则 $\zeta(s)$ 不为零.

素数定理的精密化出现各种各样的情况,但现状是,离开使用尚未解决的黎曼猜想"如果 $\mathrm{Re}(s)>\frac{1}{2}$,则 $\zeta(s)\neq 0$"得到的结论

$$\pi(x)=\int_2^x\frac{\mathrm{d}u}{\log u}+O(x^{\frac{1}{2}}\log x)$$

还相距甚远.这里,用积分(称为对数积分)代替$\frac{x}{\log x}$,正如高斯和黎曼都注意到了的,是因为在比较误差的时候,此时的近似要好得多.

另外,记号 $O(x^{\frac{1}{2}}\log x)$ 意味着:误差 $\left|\pi(x)-\int_2^x\frac{\mathrm{d}u}{\log u}\right|$ 的大小在 $x^{\frac{1}{2}}\log x$ 的某常数倍以下,还知道不能根据比$\frac{1}{2}$小的数 a,而取误差估计为 $O(x^a)$ 的形式.在此种意义上,如果证明了黎曼猜想,素数定理的精密化也就迎来了大体的完成.

但遗憾的是,至今为止,连误差取为 $O(x^{1-\frac{1}{100\,000\,000}})$ 的形式也没有完成(不论$\frac{1}{100\,000\,000}$取怎样小的正数).

黎曼猜想是 ζ 函数的美的象征,是生存的原动力所在.从"全素数表"看,黎曼猜想也许非常简单易懂.

§3　各种素数的分布

关于素数全体的分布情况的研究,目前只到素数定理.详细看一下素数的形式和特性将是怎样的呢?请看下面的三个例子

$p=4n+1$(n 是正整数)的形式,例如

$$p=5,13,17,\cdots \tag{1}$$

$p=n^4+1$ 的形式,例如

$$p=2,17,257,\cdots \tag{2}$$

$p=2^n-1$(梅森素数)的形式,例如

$$p=3,7,31,\cdots \tag{3}$$

稍微计算一下即可看出,无论哪种形式,其中的素数都很多.

我们知道,对应式(1)的素数个数是无限的,已于1837年由狄利克雷(Dirichlet)证明了.但对应式(2),(3),素数有无限个的问题,至今为止尚未证明.

这时,还要考虑与原素数定理相似之处,只要研究公式

$\pi(x,4n+1)=$(x以下的素数p中,满足$4n+1$条件的素数的个数)

$\pi(x,n^4+1)=$(x以下的素数p中,满足n^4+1条件的素数的个数)

$\pi(x,2^n-1)=$(x以下的素数p中,满足2^n-1条件的素数的个数)

将狄利克雷的结果稍加严密化即为

$$\pi(x,4n+1)\sim\frac{1}{2}\cdot\frac{x}{\log x},x\to+\infty$$

也就是说,x以下的素数($\pi(x)$个)中,按概率有一半是用4除余1的素数,因此其余一半是用4除余3的素数(但是2是例外的)

$$\pi(x,4n+3)\sim\frac{1}{2}\cdot\frac{x}{\log x},x\to+\infty$$

狄利克雷将素数融于形形色色的ζ函数中,再从中抽出个性,从而导出这样的结果(对$p=an+b$的形式时也是如此).

再有,对(2),(3)从概率上考虑,可得出下面的猜想

$$\pi(x,n^4+1)\sim(2.678\,9\cdots)\cdot\frac{x^{\frac{1}{4}}}{\log x},x\to+\infty \tag{2'}$$

$$\pi(x,2^n-1)\sim(2.569\,5\cdots)\cdot\log\log x,x\to+\infty \tag{3'}$$

其中,直到x相当大的时候,研究(2′)都很符合猜想.关于式(3′),虽例子不多(现在知道的有$3,7,31,\cdots,2^{859\,433}-1$共33),但可以认为基本符合猜想.证明式(2′),(3′)的论据不足.素数分布的密度,按(1′),(2′),(3′)的顺序,逐渐变得稀少,随着素数分布密度的变稀,边计算边证明就更困难了.

今后,按公式的形式,将式(1′)称为一次型,式(2′)称为多项式型,式(3′)称为指数型.比如,$p=an+b$称一次型,$p=an^2+bn+c$称多项式型.在式(1′)的情况下,由狄利克雷的结果证明了素数定理,其他的情况则仅被认为是猜想.

猜想的(2′)例子

$$\begin{cases}\pi(x,n^2+1)\sim(1.372\,8\cdots)\cdot\dfrac{x^{\frac{1}{2}}}{\log x},x\to+\infty\\[2ex]\pi(x,n^2+n+41)\sim(6.639\,5\cdots)\cdot\dfrac{x^{\frac{1}{2}}}{\log x},x\to+\infty\end{cases}$$

另外,式(2′)和(3′)也有变形版本存在,下面看几种变形.

(2′)的变形1:孪生素数.

设$\pi_2(x)$=(x以下的素数p中,$p+2$也是素数的素数个数),形成像(3,5),(5,7),(11,13)等形式的孪生素数.猜想为

$$\pi_2(x) \sim C \cdot \frac{x}{(\log x)^2}, x \to +\infty$$

这点,在其他的情况虽然也相同,但常数C可以准确地计算,现在的情况就是

$$C = 2 \times \left(1 - \frac{1}{(3-1)^2}\right) \times \left(1 - \frac{1}{(5-1)^2}\right) \times \left(1 - \frac{1}{(7-1)^2}\right) \times \cdots = 1.320\,3\cdots$$

其中无限积为与3以上的素数3,5,7,…有关的乘积.素数的倒数之和等于无穷大(这从$\zeta(1)=+\infty$可见),但是孪生素数的倒数之和是有限的,这已在1919年由布朗证明过.计算一下,$(\frac{1}{3}+\frac{1}{5})+(\frac{1}{5}+\frac{1}{7})+\cdots=1.902\,1\cdots$,我们知道孪生素数很少,但是并没有证明它们有无穷个(说少比证明无限个更容易).

(2′)的变形2:椭圆曲线及自守形式的情况.

关于椭圆曲线及自守形式,在这里由于篇幅的关系,不能作深入说明,但无论哪一个对费马猜想的解决都起了重要的作用.请参看加藤和也先生的《解决!费马的最后定理/现代数论的轨迹》(日本评论社,1995年).

设E为有理系数的椭圆曲线且不带虚数的乘法.

例1 如果用方程式$x^3-x^2=y^2-y$定义的曲线.这时若设$L(s,E)=\sum_{n=1}^{+\infty} a(n,E)n^{-s}$为其$\zeta$函数,则对(充分大的)素数$p$有

$$a(p,E) = 1 + p - \#\widetilde{E}(E_p)$$

成立.在这里

$$\#\widetilde{E}(E_p) = (\mathrm{mod}\ p \text{ 的解的个数}) + 1$$

(加1是由于$(-\infty,+\infty)$也看做是椭圆曲线上的点).此时,考虑:$\pi_E(x)$=(x以下的素数p中,满足$a(p,E)=0$的素数的个数)(这样的p称为超奇异的),猜想有下述结果成立

$$\pi_E(x) \sim \text{常数} \cdot \frac{x^{\frac{1}{2}}}{\log x}, x \to +\infty$$

(朗·托洛塔,1976年).从而应该与$\pi(x,n^2+1)$等有同样程度的分布.这里,应该注意之点是$\pi_E(x)$比$\pi(x,n^2+1)$等情况的研究更进一步,当$x\to+\infty$时,$\pi_E(x)\to+\infty$.亦即证明了满足$a(p,E)=0$的p有无限个(Erdös,1987)(例1),此时超奇异的p为:19,29,199,569,809,…(个位数为9).

椭圆曲线E的说法按照解决费马猜想的Wiles的定理,可以改为自守形式

$f=\sum_{n=1}^{+\infty}a(n,f)q^n$ 的说法(但是,现在"E 的导数不含平方因子"这条件是必要的). 在这里,$a(n,f)=a(n,E)$ 成立,ζ 函数同样

$$L(s,f)=\sum_{n=1}^{+\infty}a(n,f)n^{-s}=\sum_{n=1}^{+\infty}a(n,E)n^{-s}=L(s,E)$$

从而,若令

$$\pi_f(x)=(\text{在 } x \text{ 以下的素数 } p \text{ 中,满足 } a(p,f)=0 \text{ 的素数的个数})$$

则 $\pi_f(x)=\pi_E(x)$ 成立. 对 $\pi_E(x)$ 的说明可以解释为关于 $\pi_f(x)$ 的说明. 比如,与例 1 的 E 相对应的 f 为

$$f=q\prod_{n=1}^{+\infty}(1-q^n)^2(1-q^{11n})^2=q-2q^2-q^3+2q^4+q^5+\cdots$$

(请确认 q^{19} 及 q^{29} 的系数变为零). 我们把这样的说法推广到阿贝尔簇,代数簇,及多变量的自守形式,恐怕也很有意思.

(3′) 的变形:阿贝尔的问题(1828 年).

对于自然数 $a=2,3,\cdots$,考虑

$$\pi^a(x)=(\text{在 } x \text{ 以下的素数 } p \text{ 中,满足 } a^p\equiv a(\bmod p^2) \text{ 的素数的个数})=$$
$$(\text{在 } x \text{ 以下的素数 } p \text{ 中,满足 } a'(p)=0 \text{ 的素数的个数})$$

但是,a' 是"绝对微分"

$$a'(p)=\left[\frac{a^p-a}{p}(\bmod p)\right]$$

这时,可以猜想

$$\pi^a(x)\sim\log\log x,x\to+\infty$$

(这样的素数,在费马猜想的第一种情况下,也可以考虑作为维富利的条件). 关于这点,对不太大的 a,有计算的实例,比如,$a=2$ 时,$p=1\ 093$ 及 $3\ 511$(无论哪个都可以手算);$a=3$ 时,也可找到 $p=11$ 及 $1\ 006\ 003$($p=11$ 是雅可比(Jacobi)发现的)(关于"数的微分",请参看伊藤康隆先生的《Fermat 商和关于"数的微分"》,(《数理解析研究所讲录》. 1992(810):324-341).

另外,$2'(1\ 093)=0$,$2'(3\ 511)=0$ 等,微分变为 0,这样做下去,2 的图形允许变为如图 1.3 那样.

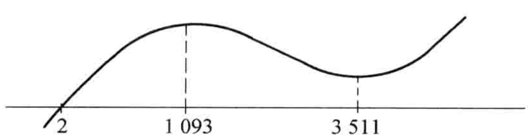


图 1.3

从在"一元域"F_1 上考虑数学这种绝对数学的观点出发,整数 0,±1,

±2,… 可以称为 F_1 系数的多项式. 这样,素数 2,3,5,7,… 也应该构成某种多项式,而且,毫无疑问,在黎曼猜想的证明等方面发挥巨大作用.(关于绝对数学请看:《绝对数学的探求:1 和 2 和 3》(Springer-Science. 1995,10(2):6-10)

关于定理的注记

这里出现的常数各个都具有数论的结构. 如果使用平方剩余记号 (p/q),则有如下的表示

$$2.6789\cdots=\prod_{p:\text{奇素数}}\left(1-\frac{\frac{-1}{p}+\frac{2}{p}+\frac{-2}{p}}{p-1}\right)$$

$$1.3728\cdots=\prod_{p:\text{奇素数}}\left(1-\frac{\frac{-1}{p}}{p-1}\right)$$

$$6.6395\cdots=2\times\prod_{p:\text{奇素数}}\left(1-\frac{\frac{-163}{p}}{p-1}\right)$$

在梅森素数的分布中出现的常数是

$$2.5695\cdots=\frac{\mathrm{e}^{r}}{\log 2}$$

其中

$$r=\lim_{n\to+\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)=0.577\cdots$$

是欧拉常数.

§4 素数的进化

到现在为止,我们见到了 2,3,5,7 等普通的素数,但是"素数"的概念在不断地进化着. 任何物体进行分解最后所得到的元素称为"素数".

众所周知,有两种考虑方法. 即从环(可以进行加减乘(除)的"数"的集合) R 中取出不能分解为积的"素数"全体 $P(R)$,以及从群(可以进行乘除的"数"的集合) G 中取出不是其他元素的乘积的"素数"全体 $P(G)$((详见:黑川写的《素数的一般化和 ζ 函数》数学セシナー. 1993(10):11)).

无论哪种情况都能构成 $\zeta(s)$,由此可以证明"素数定理",但是在后者的情况,已经知道的要精确得多,证明了黎曼猜想的类似结论,并且在与(2)非常相似的分布的情况,完成了素数定理的证明(胜田 - 砂田,菲利普斯 - 萨尔纳库,1987 年). 从几何的角度看,前者的情况"素数"是对"点"的,而后者的情况不同,被看做"直线"及"圆".(请看砂田利一先生的《素数和测地线和鼓声》(数

理科学. 1994,8:20-24）从而,为了在通常素数的情况下,也按照群 G 而解释为 $\zeta(s)=\zeta(s,G)$,像图 1.1 那样看素数全体,图 1.1 比图 1.2 要好.

这样进化了的素数其自身就饶有兴味,无疑对原来素数的研究也会带来深入的思考.

素数今后将向何处去呢? 等待素数未来的将是什么呢? 毫无疑问,素数走到了终点一定也就是数学的目的地(到达数学也将完结的地方),人类的进化果真能够赶超素数 $\zeta(s)$ 的进化吗?

素数无限性六证

第二章

通常归功于Euclid的关于有无限多个素数的证明,也许是最古老的天书证明(Elements IX,20). 我们从它开始是最自然不过的.

§1 第1种证明(Euclid的证明)

对素数的任一有限集$\{p_1,\cdots,p_r\}$,考察数$n=p_1p_2\cdots p_r+1$. 此数n有素因子p,但p一定不是某个p_i,否则p将是n的因子和乘积$p_1p_2\cdots p_r$的因子,从而也是$n-p_1p_2\cdots p_r=1$的因子,这不可能. 所以有限集$\{p_1,\cdots,p_r\}$不能包含所有素数.

在接下去讨论之前,先规定一些记号. $\mathbf{N}=\{1,2,3,\cdots\}$是自然数集合,$\mathbf{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$是整数集合,而$P=\{2,3,5,7,\cdots\}$是素数集合.

下面我们将(从大量证明中)展示另外几种证明,希望读者像我们一样欣赏它们. 虽然几种证明的想法各不相同,但都有下述共同的基本思想:自然数集没有上界,而且每个自然数$n\geqslant 2$都有素因子. 这两个事实合起来迫使P成为无限集. 第2种证明来自Christian Goldbach(在1730年给Leonhard Euler的一封信),第3种证明似乎是民间流传的,第4种证明由Euler本人给出,第5种证明是Harry Fürstenberg提出的,而最后一种证明则归功于Paul Erdös.

§2 第2种证明

首先考察 Fermat 数① $F_n = 2^{2^n}+1(n=0,1,2,\cdots)$，我们将证明 Fermat 数两两互素，从而一定有无限多个素数. 为此，我们验证递推公式

$$\prod_{k=0}^{n-1} F_k = F_n - 2, n \geqslant 1$$

由此即可得断言. 事实上，若 m 是 F_k 和 $F_n(k<n)$ 的因子，则 m 整除 2，从而 $m=1$ 或 2. 但是 $m=2$ 是不可能的，因为 Fermat 数都是奇数.

现对 n 用归纳法证明此递推公式. $n=1$ 时，我们有 $F_0=3$ 和 $F_1-2=3$，根据归纳假设，可得

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = (F_n - 2)F_n =$$
$$(2^{2^n}-1)(2^{2^n}+1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

§3 第3种证明

设 P 有限，记其中最大素数为 p，我们证明所谓的 Mersenne 数 2^p-1 的每个素因子 q 都大于 p，从而证得结论. 设素数 q 整除 2^p-1，则 $2^p \equiv 1(\bmod q)$，因 p 是素数，可知域 $\mathbf{Z}_q$ 的乘法群 $\mathbf{Z}_q\setminus\{0\}$ 中元素 2 的阶是 p. 该群有 $q-1$ 个元素. 根据 Lagrange 定理②，我们知道每个元素的阶整除该群的元素个数，即我们有 $p \mid (q-1)$. 从而 $p<q$.

现在来看一个利用初等微积分的证明.

§4 第4种证明

设 $\pi(x):=\#\{p\leqslant x : p\in P\}$ 是小于或等于实数 x 的素数个数. 把 P 中素数按增序排列为 $P=\{p_1,p_2,p_3,\cdots\}$，现考察自然对数 $\log x$，其定义为 $\log x = \int_1^x \frac{1}{t}\mathrm{d}t$.

比较函数 $f(t)=\frac{1}{t}$ 及其上阶梯函数下方的面积（图 2.1），则对 $n\leqslant x<$

① 前几个 Fermat 数是 $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65\ 537, F_5=641\times 6\ 700\ 417$. ——原注

② Lagrange 定理：设 G 是有限（乘法）群，U 是 G 的子群，则 $|U|$ 整除 $|G|$. ——原注