

微博上的数学漫游 (连载三)

歌之忆 <http://weibo.com/wildmath>

当一部数学史摆在我们面前的时候，我们总会津津乐道于那些创造了伟大的数学理论或者证明了著名的数学猜想的数学家们。可是，真切的数学却同这个世界经历着同样的历程——战争与和平、繁华与凋零。我们不该忘却那些隐秘的数学英雄，他们以数学为武器来捍卫着我们安宁的生活，他们以卓绝的才华印证了数学在华美的外衣下，蕴含的是能将智慧发挥到极致的伟大力量。正是这强悍的力量，在守卫着我们的世界，构建着我们的心灵。

波兰三杰



波兰的密码三杰：雷耶夫斯基（1905-1980，右）、罗佐基（1909-1942，中）和佐加尔斯基（1907-1978，左）

■ 今年是计算机科学伟大的先驱者阿兰·图灵诞辰一百周年，在无数有关图灵的故事中，流传甚广而且特具魅力的就是他破译德国英格玛（Enigma）密码系统的传奇。可波兰数学家和密码学家雷耶夫斯基（Marian Rejewski）、罗佐基（Jerzy Różycki）和佐加尔斯基（Henryk Zygalski）对破译英格玛所做出的居功至伟的贡献，却并不广为人知。

围绕密码的传奇故事可谓汗牛充栋。古罗马的凯撒征战高卢（今法国）时，就用加密的方式向其副帅、政治家西塞罗的弟弟传递情报。凯撒的加密不过是把字母替换成字母表中后移三位的字母。如果借英语想象一下，埃及艳后收到凯撒的一行字“chdxwb”，她将会心一笑：夸我是美人儿（beauty）！

向美人儿表白心迹自然无需加密，可国与国



电影《凯撒与克利奥佩拉》剧照

之间，难免许多秘密。一战结束后，德国的保密通信成为各国的研究热门，不过大多无功而返。法国间谍还算不错，搞到了商用英格玛加密机，多少了解到一点加密原理。可是破译密码还需要找到密钥。估算一下可能的密钥数量，1 万亿，这可是个天文数字。

擅长解读爱情密码的法国人，在英格玛面前却一筹莫展，只好把这台加密机送给波兰。这是三十年代初的事情，当时全世界恐怕都没有想到，波兰人早在二十年代就探索用数学来解读密码。就在这台英格玛面前，波兰数学家雷耶夫斯基开启了波兰数学的另一段传奇。不过，这台好戏需要对手的配合。

对手戏的好看，在于双方旗鼓相当。德国人向来以严谨著称。二战时，盟军派出许多间谍去打探德国到底有多少坦克，而统计学家发现德国人严谨得过了头，居然给其出厂的坦克连续编号，于是要求盟军：别只顾清点战场上干掉了多少辆，把干下来的最大编号告诉我们！由此直接估算出了坦克总量。

德国人在使用貌似天衣无缝的英格玛加密机时，照样秉承了德国无与伦比的严谨，也同样严谨得过了头。德国人为了防止通信中的错误或干扰，每发送一条信息时，都在前端把三个字母的密钥重复发送两次。看似很保险的这一细微的步骤，却被曾在德国哥廷根学过保险精算的雷耶夫斯基抓住了漏洞。



波兰华沙博物馆的英格玛加密机

雷耶夫斯基从截获的德国密文中，判读出德国人把三字母密钥连发了两次，这个发现非同小可。更令人叫绝的是，他针对这种密钥重复，运用排列群来分析英格玛机的加密过程。由此，他把密钥搜索范围从原先的 1 万亿降低到了 10 万。德国人重复了密钥的三个字母，送给了波兰数学家一份真正的厚礼。

二战之前，英格玛让英法情报机构摇头叹息，因为谁都无法从 1 亿亿个候选中及时找到密钥。英格玛却让波兰情报机构大放异彩，因为他们只需在 10 万个候选中去找密钥。虽然德国每天都改变密钥，但只要截获到 80 条信息，就能确定密钥的位置，再用两小时即可破解。这就是波兰数学家创造的奇迹。



图灵雕像

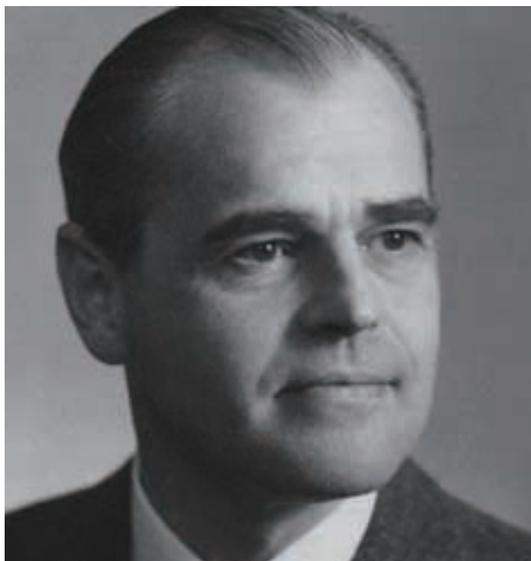


雷耶夫斯基雕像

今天人们习惯于把破译英格玛的功劳记在图灵身上，但那样一个横空出世的图灵反而是没有质感的。图灵破译英格玛的成就是在 40 年代，而在这之前的 1932-1938 年，波兰率先破译英格玛，令他国望尘莫及。甚至有数学家评价：雷耶夫斯基解密英格玛所创造的，是一条赢得第二次世界大战的数学定理。

二战后返回波兰的雷耶夫斯基，遭到安全机构反复调查。守口如瓶的他艰难地以记账员的身份生活着，直至退休多年才向世人告白真相。波兰三杰，从此成为波兰民族的骄傲。然而，波兰数学家创造的奇迹，却并非二战中的唯一。二战结束半个世纪后，又一位成就斐然的数学家以绝世高手的形象走出密码战的历史尘封。

玻尔林 *Beurling*



瑞典数学家玻尔林（1905-1986）

■ 德国在二战的战略通信中使用的是比 Enigma 远为复杂的 G-Schreiber 密码。但依旧是栽倒了，栽倒在更厉害的数学家手下。解码的巨牛甚至连样机都没见过，全靠手工演算两个星期，直接将密码攻克！后来，他到美国普林斯顿高等研究所，继承了爱因斯坦的办公室。此人就是瑞典数学天才玻尔林（Arne Beurling）。

破译德军战略通信密码的玻尔林，极富原创思想。虽破译密码只是其专业外的客串，但希特勒进攻苏联的巴巴罗萨行动就此被瑞典破译。多年来，人们百思不得其解：“只靠笔和纸在两个星期破解 G-Schreiber 密码，您到底怎么玩的？”他对此避而不答，却反问：哪有魔术师会揭秘自己玩的魔术？



美国数学家道格拉斯 (1897-1965)

不知道玻尔林猎杀的鳄鱼是否吃掉了一枚菲尔兹奖章，不过玻尔林倒没有因为这事和阿尔福斯闹过不愉快。两位杰出的数学家岂止是惺惺相惜，他们常聚在一块儿痛饮美酒，甚至跑到阿尔福斯家里一醉方休。末了，玻尔林和阿尔福斯再加上阿尔福斯太太，三个人一齐和衣醉卧在同一张床上！

假如时光能穿越，放在今天这样一个物欲横流的社会，那个曾经醉心于捕猎鳄鱼、二战时玩残了德军战略情报的瑞典天才玻尔林，会不会依然不去计较落在芬兰同行阿尔福斯手里的菲尔兹奖？虽然 1936 年在挪威奥斯陆颁发的第一届菲尔兹奖，名头远非今天这般如日中天，却也吸引了无数眼球。

与阿尔福斯同时获菲尔兹奖的是美国数学家道格拉斯 (Jesse Douglas)。然而此君无法出席会议，只得请维纳 (Norbert Wiener) 登场帮忙。求名心切的维纳毫不推辞、光鲜登场，对着记者一顿神侃。啥也没整明白的挪威记者，无比兴奋地拍了一通新闻照片，却没去理会个中曲直。最终报纸上名为道格拉斯的获奖者，却是维纳的尊容！

出了风头的维纳，内心很是烦恼。维纳一生多次在优先权上与其他名流纠缠不清。他曾要求把巴拿赫空间命名为“巴拿赫 - 维纳空间”，无奈无人理睬。人性的弱点，早被莎士比亚一眼看穿。看看《亨利四世》就明白：惟友谊能超越荣誉，成就人生。而阿尔福斯和玻尔林，拥有了几乎完美的真正友谊。

也许玻尔林对自己破译 G-Schreiber 密码还有许多意犹未尽的思考。此君总是在深思熟虑之后才发表自己的作品。有次听 Peter Duren 做报告，玻尔林当即告知：数年前他就得到了同样结论，只不过没去发表。Duren 迎头痛击，申明自己要去发表。于是上演了一出玻尔林四处追打 Duren 的喜剧！

追猎可是玻尔林擅长的。在此君做博士论文的 1929 年，就已经证明了复分析中著名的 Denjoy 猜想。证明刚一完毕，玻尔林便拉着他老爹跑到巴拿马去捕猎鳄鱼。鳄鱼倒是逮到了，可这次度假却让他错失了一份巨大的荣耀——芬兰数学家阿尔福斯 (Lars Ahlfors) 率先发表了证明，并借此拿下 1936 年菲尔兹奖。

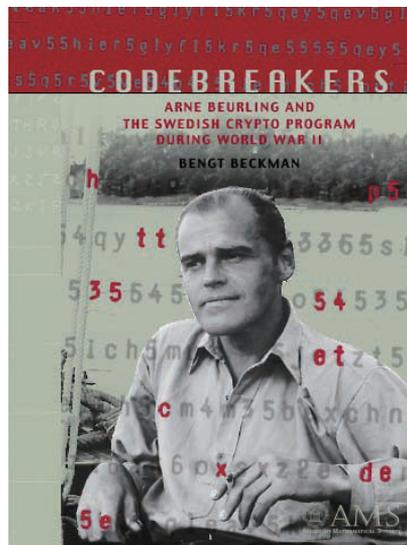


美国数学家维纳 (1894-1964)

来自斯堪的纳维亚半岛的两位数学高手阿尔福斯和玻尔林，自年轻时代就结下了深厚的情谊。二战降临，阿尔福斯一路辗转逃到美国，最终任教于哈佛。而玻尔林则为防备德国立下汗马功劳。战后，阿尔福斯念念不忘玻尔林，终将他请到哈佛一起工作了两年。阿尔福斯说，那是他生命中最美好的时光。

那段诗意的时光，让两位学者收获了丰硕成果。阿尔福斯的家就在哈佛广场附近。俩人把酒言欢至深夜，玻尔林就干脆挤到阿尔福斯两口子的床上。更多时候，俩人讨论至清晨。旭日东升之际，玻尔林满嘴酒气，跌跌撞撞回自己的寓所。街上巡视的警察向这位怪人打招呼：先生，早上好！晚安！

有人说，数学家的性格与他们从事的领域相关。做几何的大多优雅，搞分析的却容易暴躁。此话放到玻尔林身上，绝对吻合。此君习惯在课堂破口大骂那些思路一团糟的学生，甚至还和同事大打出手。某天忽然可怜兮兮跑去问学生：我脾气真有那么糟吗？学生安慰道：好多啦！您现在对咱就像天使一样温柔！



瑞典的民族英雄、密码战历史上最神秘的高手、50年代坐镇普林斯顿高等研究所的杰出数学家玻尔林



爱因斯坦逝世当日的办公室照片，此办公室后来由玻尔林使用

定全部细节之后才肯发表论文。如今他的大量遗作，成了令人垂涎的丰硕宝藏。世上惟有这等才华与自省，才配继承普林斯顿高等研究所爱因斯坦的办公室吧？

这个在祖国需要的时候，区区一周多就被译德军战略密码、使祖国免遭战火侵袭的玻尔林，不仅混合了率性果敢与精致优美，还时时玩出孩子般的恶作剧。寒冬雪夜，他曾当着阿尔福斯的面揉起一团雪球，把路灯砸灭，然后拉着一众人马笑着逃之夭夭。惟有被自由与激情抚养大的理性，才能迎来创造。

在独具魅力的数学家身上，往往流传着许多传奇。体格强壮、性格刚毅的玻尔林，爱好航海、捕鱼，颇有北欧海盗的侠肝义胆。可这个外表粗犷的男子汉，写出来的论文却极其优美。他的学生卡尔松（Carleson）深情地说：正是瑞典幽深的森林、湖泊、山脉连同迷人的童话仙女，养育出了玻尔林的瑞典式数学。

生于1905年的玻尔林，20多岁便开启了将复分析、调和分析、位势理论融为一体的创造历程，才华如青年牛顿一样令人震撼。他性格既刚猛而又深沉内敛，总是在敲

阿尔福斯 Ahlfors



芬兰数学家阿尔福斯（1907-1996）

■ 阿尔福斯评价玻尔林成熟而自信、性格刚毅，他把自己归结成谦和好静的宅男，与玻尔林恰好南辕北辙。可这么个谦和好静的阿尔福斯，晚年退休仍喜好喝上几杯。某日腋下夹着一瓶酒，快进家门时，却见有人冲过来向他偷袭。二话不说，抡起瓶子砸过去。那可是一瓶上好的苏格兰威士忌啊！

退休在家尚能这么果敢地打斗，可见阿尔福斯绝非谦和好静那么简单。这位大数学家看到瑟斯顿以几何直觉研究拓扑取得巨大成功、斩下菲尔兹奖，便向美国国家自然科学基金会提交了研究申请书——与那些洋洋洒洒的申请书不同，他只写了一句话：我想研究瑟斯顿的理论。如此彪悍的学者！

阿尔福斯说玻尔林是其一生最好的朋友。他们联手为后人留下了玻尔林-阿尔福斯算子、玻尔林-阿尔福斯定理等传世篇章。玻尔林更是瑞典的民族英雄。但他究竟如何单枪匹马靠手工演算就破译了德军战略密码，却已随英雄的逝去，成为永久的谜团。也许只有上帝才懂得天才吧！

曾经有人罗列出了人类历史上十大最神秘的、被带进坟墓的未解之谜。玻尔林提前两周破译德国进攻苏联的计划，榜上有名。而名列榜首的，则是意大利传奇乐器制作大师斯特拉迪瓦里制作提琴的秘密。数学大师与乐器制作大师遗留下千古之谜，那是人类的无上荣光，那是人类心智与心灵的绝响。

大文豪雨果说：“人的智慧掌握着三把钥匙，一把开启数学，一把开启字母，一把开启音符，知识、思想、幻想就在其中。”我们该对每一位手握钥匙的精英致以深切的敬意，因为他们成功攀登了凡人难以企及的高峰，因为他们定义了我们所拥有的文明的高度。而数学，无疑是文明高度的一个标杆。

数学处在文明的中心地带，难免让数学家滋生了优越感。阿尔福斯听到有人把菲尔兹奖说成“数学里的诺贝尔奖”，便调侃到：诺贝尔奖本不该给数学，你没法仰望数不清的数学天才，从中找出最厉害的。设经济奖倒很容易，只要在烂木桶底上去刮一刮，把刮出来的渣子拿去，就是经济奖得主了！



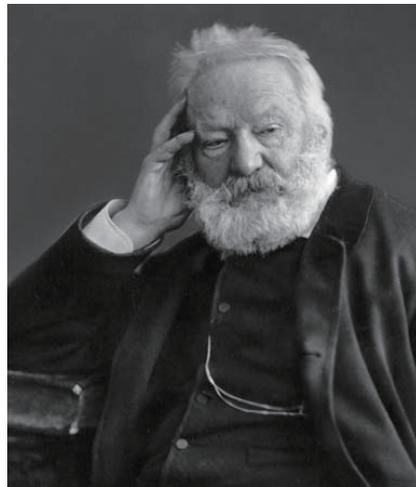
意大利小提琴制作大师斯特拉迪瓦里制作的小提琴，是价值连城的艺术瑰宝。

阿尔福斯如此对诺贝尔奖不敬，也不偶然。当时从芬兰出境，随身只许带 10 克朗现金。这位第一届菲尔兹奖得主，悄悄把菲尔兹奖章藏在身上带到瑞典，然后拿到典当铺换回现金！事后被瑞典的朋友们得知，花了一笔钱把奖章赎了回来。对自己的菲尔兹奖尚且如此，无怪乎对诺贝尔奖这般不敬。

敢把菲尔兹奖章拿去换钱的阿尔福斯，只不过对诺贝尔奖说了点戏谑之词。而萨特却断然拒绝了诺贝尔文学奖：“一切来自官方的荣誉我都不接受，我只接受不受任何限制的自由。”当然，存在主义大师可没法拒绝美女萨冈的情书：“这个世纪疯狂，没人性，腐败。您却一直清醒，温柔，一尘不染。”

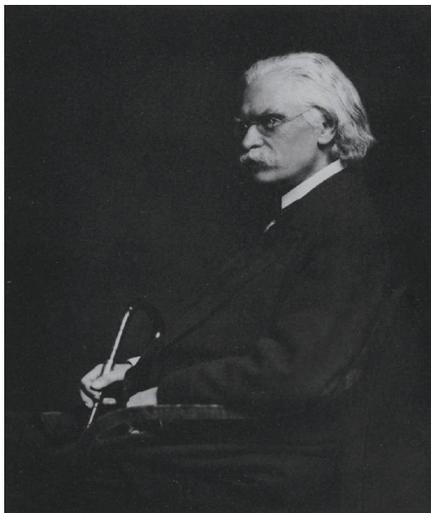
在理性的巅峰，有最卓绝而又骄傲的灵魂。俄罗斯大数学家柯尔莫哥洛夫拒绝了沃尔夫奖，佩雷尔曼不但拒绝了菲尔兹奖，继而拒绝了美国克雷研究所千禧年百万美元数学大奖。在至高无上的荣耀面前，那些泰然处之、平静自如的精英们，构筑起了人类心智最具魅力的绝美景观，高山仰止，景行行止。

在理性巅峰上的数学，历来是年轻智力的角斗场。阿尔福斯年仅 21 岁就斩下 Denjoy 猜想，它是青年学子孜孜以求的传奇，也是学术薪火代代相传的佳话。自瑞典数学之父米塔-莱夫勒执教当时属于沙俄的赫尔辛基大学始，芬兰一代接一代有了 Mellin、Lindelöf、Nevanlinna 及至阿尔福斯，学术传承延绵不绝。



法国文豪雨果（1802-1885）

米塔-莱夫勒 Mittag-Leffler



瑞典数学之父米塔-莱夫勒（1846-1927）

■ 斯堪的纳维亚半岛曾经有过挪威阿贝尔（Abel）的传奇，可惜天妒英才，27 岁就撒手人寰。北欧的数学童话，还得从那个传说中被诺贝尔妒恨的米塔-莱夫勒说起。此人早年成就平平，只是造化弄人，在完成学业后居然搞到一笔为期三年的奖学金，而使用这笔钱的唯一条件却是：离开瑞典闯天下，留学三年！

一心想学分析的米塔-莱夫勒踏上欧洲大陆，他首先跑到巴黎去跟随埃尔米特（Charles Hermite）。但埃尔米特却严肃地告诫这位同行：“你搞错了！你根本就不该追随我，你该去柏林，去听魏尔斯特拉斯（Karl Weierstrass）的课程——他是我们所有人的大师”！人们常说文人相轻，但在追随真理的数学家那里，如此开阔的胸襟，并非鲜见。

在埃尔米特看来，魏尔斯特拉斯才代表了数学中最高规格的逻辑标准。埃尔米特自知法国人天生富有艺术气质，常常以



法国数学家埃尔米特 (1822-1901)

直觉取胜，此乃做分析的大忌。而他的高足庞加莱 (Henri Poincaré) 就曾这么评价自己：你们居然还说他是逻辑学家！鬼才相信！事实恰好相反，我真搞不懂那些稀奇古怪的思路是怎么从他脑袋里面跑出来的！

在主张直觉的数学家眼里，数学的真理是被发现的。而在主张逻辑的人那里，数学的真理是被发明的。直觉强大的埃尔米特一心向往逻辑，意味深长地说：“在数学面前，我们是仆人而非主人”。天生就是数学的主人的巴拿赫，居然被自己的老师史坦因豪斯批评道：巴拿赫，空间想象力还是差了

点！

巴黎有以直觉见长的埃尔米特，柏林有以逻辑见长的魏尔斯特拉斯。一心想研究解析函数的米塔-莱夫勒，最终听从了埃尔米特的建议，转赴柏林。这一步注定要在数学史上留名：它不仅点燃了瑞典与芬兰长盛不衰的数学火焰，它还引出了数学史上极有影响的一次交锋，一次直觉与逻辑之间的交锋。

直觉与逻辑之间这场精彩的缠斗，源自为瑞典国王奥斯卡二世而发起的一场竞赛。比赛内容是解释太阳系运动是否稳定。竞赛的三位裁判是擅长直觉的埃尔米特、以严格著称的魏尔斯特拉斯以及崇尚严格的米塔-莱夫勒。最终，埃尔米特的学生庞加莱获胜，获奖论文将在期刊 *Acta Mathematica* 公开。



德国数学家魏尔斯特拉斯 (1815-1897)

弗拉格门 Phragmén



瑞典数学家弗拉格门 (1863-1937)

除了认可庞加莱的论文具有非凡的创造性，擅长直觉的埃尔米特没有看出问题，以严格性著称的魏尔斯特拉斯没有看出问题，崇尚严格性的米塔-莱夫勒也没有看出问题。清样送到 *Acta Mathematica* 的编辑那里，只等排版印刷。然而，名叫弗拉格门 (Lars Phragmén) 的小编，却看出了一连串逻辑上无法回避的问题。

直觉与逻辑，既是永恒的对手，也是永恒的朋友。如果说直觉像是建筑设计师，那么逻辑就是结构工程师。曾经调侃过导师埃尔米特缺乏逻辑严密性的庞加莱，却忠实遗传了导师擅长直觉的特质。看似天衣无缝的论文，被弗拉格门指出无数破绽。甚至连已经排印好的修订版，依旧还是被抓住了漏洞。

不知米塔-莱夫勒是否是想讨好圣上，居然建议用数学论文竞赛来庆贺奥斯卡二世国王的60大寿。庞加莱从国王那里赢得了2500克朗的奖金，却被弗拉格门指出错误，排好论文的杂志只得撤回来。修订错误后，论文从原先的160页变成270页。庞加莱又只得乖乖地掏出了不止2500克朗用作排印费用。

从瑞典流到法国的2500克朗，在庞加莱的口袋捂热了一年，现在又转了回来。更悲催的是，这枚由瑞典国王颁发给庞加莱的奖章，多年之后，居然又在庞加莱孙子的家里被梁上君子盗走。想想看，法兰西真不愧是个数学大国，不仅夺走那么多菲尔兹奖，连小偷都知道与数学有关的宝物是无价的。

庞加莱不仅把赢来的奖金如数奉还，最终还弄丢了自己的奖章。但人类却千载难逢地收获了魅力无穷的崭新数学——混沌。瑞典，也在这场逻辑与直觉的较量中，发现了自己的数学天才弗拉格门。这个从读大学开始就接二连三发表论文的才俊，后来与芬兰数学家提出了极为深刻的Phragmén-Lindelöf原理。



瑞典奥斯卡二世国王



法国数学家庞加莱 (1854-1912)

此时从赫尔辛基来到斯德哥尔摩的米塔-莱夫勒，正在开辟瑞典数学之路。弗拉格门从大学期间就开始帮助打理他的数学期刊，直到成为编辑。就这样，历史上第一次，一位数学家因为审读论文清样而赢得了国际声望。弗拉格门的犀利眼光，让庞加莱认识到自己出了很大的错误。这是科学史上最宝贵的错误之一。这个错误，引出了混沌的概念。

作者简介：歌之忆（笔名），生于六十年代，数学博士，任电子信息专业教授十年有余。现阶段在网络数据分析与图像识别等领域主持技术研发。