初等数论及其应用

课程介绍

连宙辉
北大计算机所

关于计算机所

王选老师（1937.2-2006.2）：曾任北大计算机所所长，汉字激光照排系统之父，两院院士，2001年获国家最高科学技术奖

北京大学计算机科学技术研究所是北京大学的二级科研教学机构，是计算机应用技术国家重点学科主要建设单位，建有硕士、博士培养点及博士后流动站。

http://www.icst.pku.edu.cn/

联系老师

- **连宙辉** （博士，副教授）
  - Email：lianzhouhui@pku.edu.cn
  - 座机：82529245
  - 手机：13426244398
  - QQ：94141135
  - 办公室：北大计算机所大楼4层南面

☺插个广告☺

- 招收硕士研究生，招募实习生

http://www.icst.pku.edu.cn/cscl

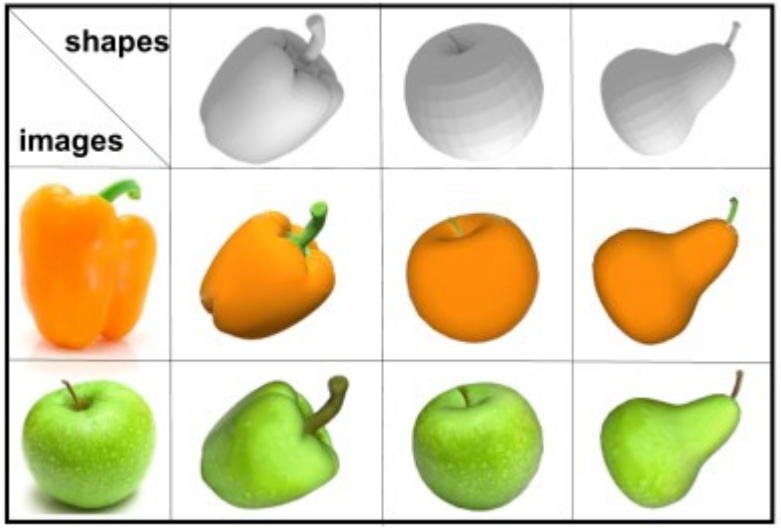
☺插个广告☺

- **招收硕士研究生，招募实习生**

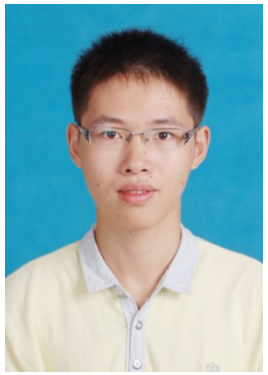
http://www.icst.pku.edu.cn/zlian/

☺插个广告☺

- 做什么？
  - ✓ “教”计算机识字、写字、设计字
  - ✓ 三维数据分析、检索和建模



认识助教



- 夏泽青：
  - Email：zeqing.xia@pku.edu.cn
  - 电话：156-5070-3612
- 王逸之：
  - Email：wangyizhi@pku.edu.cn
  - 电话：131-2033-8379
- 王文光：
  - Email：Wangwenguang_PKU@163.com
  - 电话：188-1069-3632
- 孙笑：
  - Email：xsun@pku.edu.cn
  - 电话：155-0117-9599

微信群

2018年春初等数论班级群

该二维码7天内(3月5日前)有效，重新进入将更新

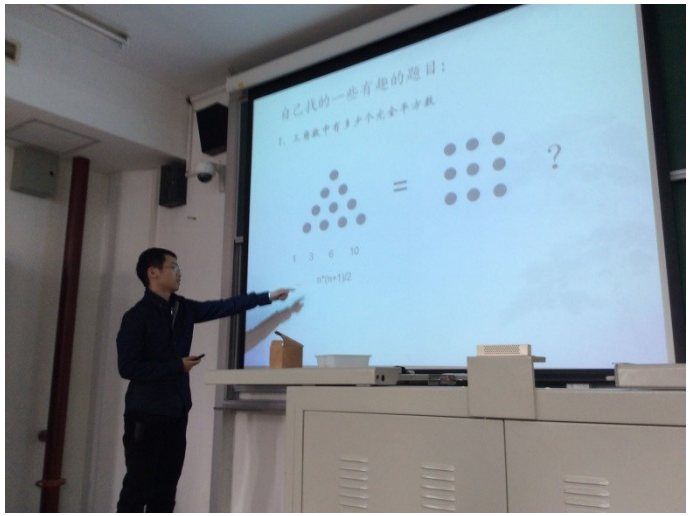
教学网

- http://course.pku.edu.cn/
- 下载课件、提交作业、网上答疑、课程讨论。
- **第一次作业**：上传照片，做自我介绍，并简要说明选这门课的原因、目的、知识基础等。

个人备用课程网站：
http://www.icst.pku.edu.cn/zlian/course/ENT/

关于这门课程

- 2014年北京大学第十四届青年教师教学基本功比赛理工组一等奖
- 2015年北京市第九届青年教师教学基本功比赛理工组三等奖
- 2015年第二届全国高校微课教学比赛北京市三等奖



互动问题1

互动问题1

- **哥德巴赫猜想**“1+1”到底代表什么？我国著名数学家**陈景润**证明的“1+2”又是什么意思?
- 命题“每一个充分大的偶数都能表示为一个不超过a个素数的乘积与另一个不超过b个素数的乘积之和”记作“a+b”。哥德巴赫猜想“1+1”，也就是说“**任一充分大的偶数都可表示成两个素数之和**”。
- 1966年陈景润证明了“1+2”成立，即“每一充分大的偶数都能表示为一个素数与一个不超过两个素数的乘积之和”。

互动问题1

大偶数表为一个素数及一个不超过二个素数的乘积之和

陈 景 润
(中国科学院数学研究所)

摘 要

本文的目的在于用筛法证明了：每一充分大的偶数是一个素数及一个不超过两个素数乘积之和.

关于孪生素数问题亦得到类似的结果.

一、引 言

把命题"每一个充分大的偶数都能表示为一个素数及一个不超过 a 个素数的乘积之和"简记为 $(1, a)$.

不少数学工作者改进了筛法及素数分布的某些结果，并用以改善 $(1, a)$. 现在我们将 $(1, a)$ 发展历史简述如下：

$(1, c)$——Renyi[1]，

$(1, 5)$——潘承洞[2]、Барбан[3]，

$(1, 4)$——王元[4]、潘承洞[5]、Барбан[6]，

$(1, 3)$——Бухштаб[7]、Виноградов[8]、Bombieri[9]，

在文献[10]中我们给出了 $(1, 2)$ 的证明提要.

互动问题1

- 在1742年给欧拉的信中哥德巴赫提出了以下猜想：**任一大于2的整数都可写成三个质数之和**。但是哥德巴赫自己无法证明它，于是就写信请教赫赫有名的大数学家欧拉帮忙证明，但是一直到死，欧拉也无法证明。
- 今日常见的猜想陈述为欧拉的版本，即**任一大于2的偶数都可写成两个素数之和**，亦称为“强哥德巴赫猜想”或“关于偶数的哥德巴赫猜想”。

互动问题1

- 1742年6月30日欧拉给哥德巴赫的回信：“正如在你给我的来信中所观察到的那样，每个偶数看来是两个素数之和，还蕴藏着每个数如果是两个素数之和，则它可以是任意多个素数之和，个数由你而定。如果给定一个偶数n，则它是两个素数之和，对n-2也是如此，则n是三到四个素数之和。如果n是奇数，则它一定是三个素数之和，因为n-1是两个素数之和。所以，n是一个任意多个素数之和。虽然我现在还不能证明，**但我肯定每个偶数是两个素数之和**。……”。

互动问题2

Tom Zhang

Lecturer

yitangz@unh.edu
(603) 862-4407

Tom Zhang

Professor

Analytic Number Theory

yitangz@unh.edu
(603) 862-4407

张益唐，华人数学家。1978年考入北京大学数学系，1982年本科毕业；1985年获北大硕士学位；1992年毕业于美国普渡大学，获博士学位；2014年前，在美国新罕布什尔大学任教，职称为讲师 (Lecturer)。2014年，他获得数学领域最高奖项之一的美国数学学会柯尔数论奖；2014年2月13日获2014年瑞典皇家科学院罗夫·肖克奖中的数学奖项；2014年9月16日，获得麦克阿瑟天才奖；2016年10月获“求是杰出科学家奖”。

互动问题2

- **孪生素数猜想**是什么？2013年这位轰动全球的传奇校友**张益唐**做了什么工作？
- 命题“**存在无穷多对素数p和p+2**”
- 2013年张益唐在《数学年刊》（Annals of Mathematics）上发表的这篇题为《素数间的有界距离》的文章，证明了**存在无数多个素数对（p, q），其中每一对中的素数之差，即p和q的距离，不超过七千万**。七千万听起来是个巨大的数字，但在数学上只是一个常数而已。虽然它和孪生素数猜想的距离为2的结果还有十万八千里，但用张益唐的方法把七千万缩短到几百以内也是指日可待的事情。

互动问题2

Bounded gaps between primes

Yitang Zhang

Abstract

It is proved that

$$\liminf_{n\to\infty}(p_{n+1}-p_n)<7\times 10^7,$$

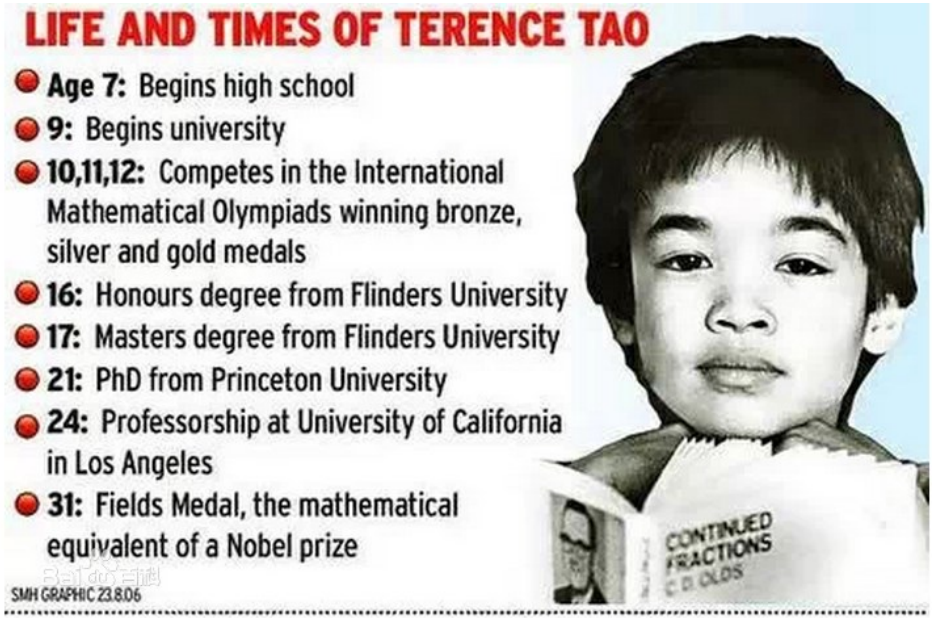
where p_n is the n-th prime.

Our method is a refinement of the recent work of Goldston, Pintz and Yildirim on the small gaps between consecutive primes. A major ingredient of the proof is a stronger version of the Bombieri-Vinogradov theorem that is applicable when the moduli are free from large prime divisors only (see Theorem 2 below), but it is adequate for our purpose.

互动问题2

- 在张益唐的文章被公布于众后，短短的一个月以内，七千万就被菲尔茨奖获得者**陶哲轩**发起的网上讨论班项目(Polymath-8)缩小到六万多，现在已经缩减到246

6: With a generalization of Elliott-Halberstam conjecture



互动问题2

- 在张益唐的文章被公布于众后，短短的一个月以内，七千万就被菲尔茨奖获得者**陶哲轩**发起的网上讨论班项目(Polymath-8)缩小到六万多，1年后已经缩减到246

- 张益唐起到的作用就是把**大海捞针**的力气活缩短到在水塘里捞针，而他给出的方法还可以把**水塘捞针**轻松变为游泳池里捞针。也许最后变成在**碗里捞针**还需要一些再创新的工作。但给出了这一伟大框架已经是让全世界数学家瞠目结舌的壮举了。甚至有人认为其对学界的影响将超过陈景润的“1+2”证明。

何谓数论

- **数论**是研究数的规律，特别是整数性质的数学分支。
- **初等数论**主要是用**整数的四则运算方法研究整数性质**的数论分支，它是数学中最古老的分支之一。
- 德国数学家高斯（Gauss）说过：“**数学是科学的女王，而数论则是数学的女王**。”数论之所以具有难以抗拒的魅力，其重要原因是它的问题浅显易懂但特别迷人。另外，它并不需要过多预备知识，初学者即可登堂入室，理解它的许多重要内容。

数论与ACM竞赛

- ACM国际大学生程序设计竞赛（英语：ACM International Collegiate Programming Contest, ICPC）是由美国计算机协会（ACM）主办的，一项旨在展示大学生创新能力、团队精神和在压力下编写程序、分析和解决问题能力的年度竞赛。经过30多年的发展，ACM国际大学生程序设计竞赛已经发展成为最具影响力的大学生计算机竞赛。赛事目前由IBM公司赞助。

数论与ACM竞赛

- ACM-ICPC以团队的形式代表各学校参赛，每队由3名队员组成。
- 比赛期间，每队使用1台电脑需要在5个小时内使用C、C++或Java中的一种编写程序解决7到10个问题。程序完成之后提交裁判运行，运行的结果会判定为"AC(正确)/WA（错误）/TLE（超时）/MLE（超出内存限制）/RE（运行错误）/PE（格式错误）"中的一种并及时通知参赛队。每队在正确完成一题后，组织者将在其位置上升起一只代表该题颜色的气球。

数论与ACM竞赛


+0:02:36
+0:02:36


acm International Collegiate Programming Contest
IBM
event sponsor


2013 ACM-ICPC World Finals, St. Petersburg, Russia

数论与ACM竞赛

- 参加ACM竞赛需要预备的数学知识：初等数论、组合数学等。初等数论是其中最重要的数学基础之一。希望大家平时能够动手编程序来实现初等数论里的一些经典算法。

ACM-ICPC
2018全球总决赛在北大举办！

数论的趣闻

- 费马（Fermat）是17世纪初期法国的一位重要数学家和物理学家。他在阅读古希腊数学家丢番图的《算术》一书时，在书旁的空白处写下了这样的批注：“$x^n + y^n = z^n$ 没有解（实质是指当n>2时非零整数解不存在）。对此，我确信已发现了一个绝妙的证明，可惜空白的地方太小，写不下”。

数论的趣闻

- 由于费马大定理的名声，在纽约的地铁车站出现了乱涂在墙上的话：“$x^n + y^n = z^n$ 没有解，对此我已经发现了一种真正美妙的证明，可惜我现在没时间写出来，因为我的火车正在开来。”
- 当然，这种话到1994年就不会有人再写了，因为在这一年，费马大定理终于被证明了。证明它的人-英国数学家怀尔斯（Wiles），也因此赢得了菲尔兹奖（数学界的最高奖）、沃尔夫奖等。正因为怀尔斯的证明相当复杂而且利用了很多现代数学的方法，根本不可能写在书的空白之处，更让人怀疑，费马是在故弄玄虚而已。

初等数论的应用

- 近几十年来，初等数论在物理学、化学、计算机科学、密码学、编码理论、电气工程等领域得到了广泛而深入的应用。

- 美国华盛顿大学布兰克（Blank）教授说：“现今如果你教一门数论课程，计算机专业的学生很可能比数学专业的学生更感兴趣。许多人较少关心能被表示为两个平方和的整数，但更关心Alice如何与Bob进行保密通信。”

初等数论的应用

- **带余除法**：$35 = 2 \times 17 + 1$（即35/2的商为17，而余数为1，以后会证明商和余数是唯一的）

- 带余除法的应用：整数的二进制表示，以35为例

$$35 = 2 \times 17 + 1 \text{(低位)}$$
$$17 = 2 \times 8 + 1$$
$$8 = 2 \times 4 + 0$$
$$4 = 2 \times 2 + 0$$
$$2 = 2 \times 1 + 0$$
$$1 = 2 \times 0 + 1 \text{(高位)}$$

按从低位到高位顺序，依次取出上述除法中的余数，得到$(35)_{10} = (100011)_2$

初等数论的应用

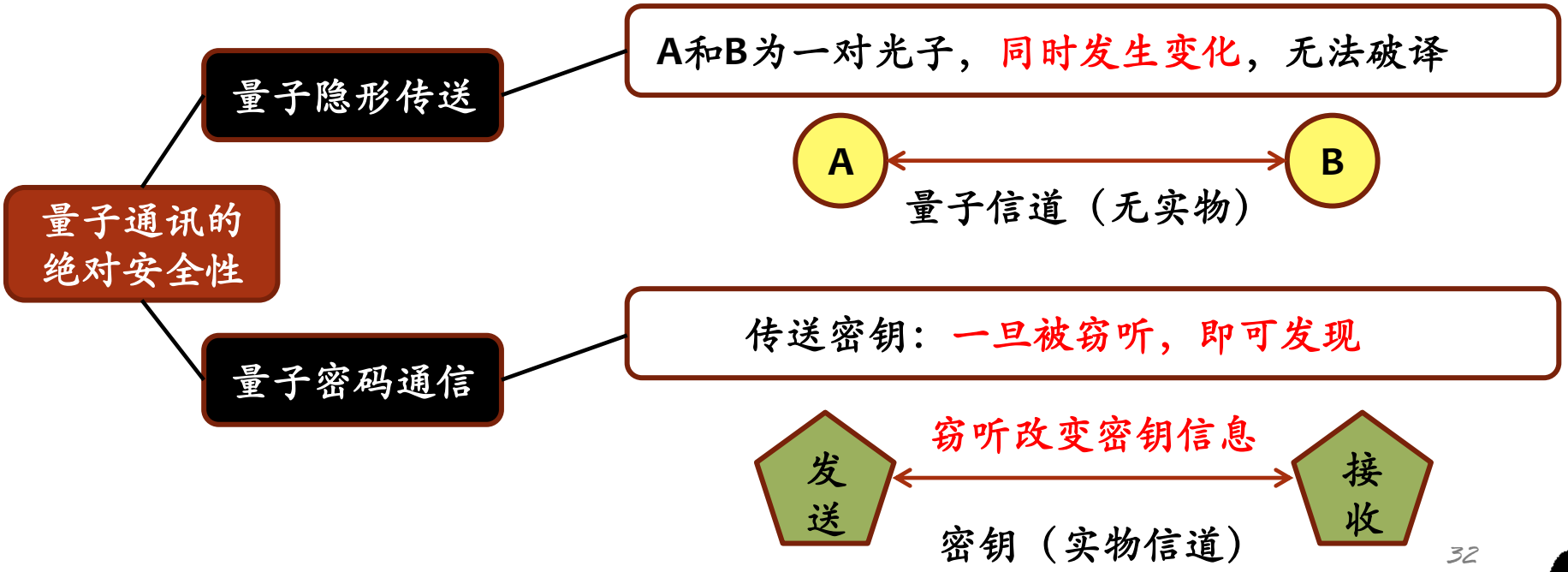
- **同余**的概念：$2=0\times3+2$，$5=1\times3+2$，则称5与2（模3）同余
- 同余可以有如下很多的应用：
  - 简单密码机制：将26个英文字母对应到数字1-26，通过移位和同余操作加密一段文字。
  - 简单信息校验：传递长度为n的二进制信息$x_1\ldots x_n$，增加一个校验位x_{n+1}，可以设置校验位（0或1）来保证这n+1位信息之和能被2整除。这样接收信息时可利用这个性质来检查信息传递是否出错。
  - 万年历
  - ……

初等数论的应用

- **算术基本定理**表明，每个大于1 的整数均可以表示为素数之积
- 用**素性测试**的方法可以判断给定的数是否是合数，进而可以求得很大的素数p和q，如果将p和q的乘积pq作为给定的数a，我们将很难将a分解为素数之积，这个奇特的事实是用数论知识建立安全密码的关键所在。

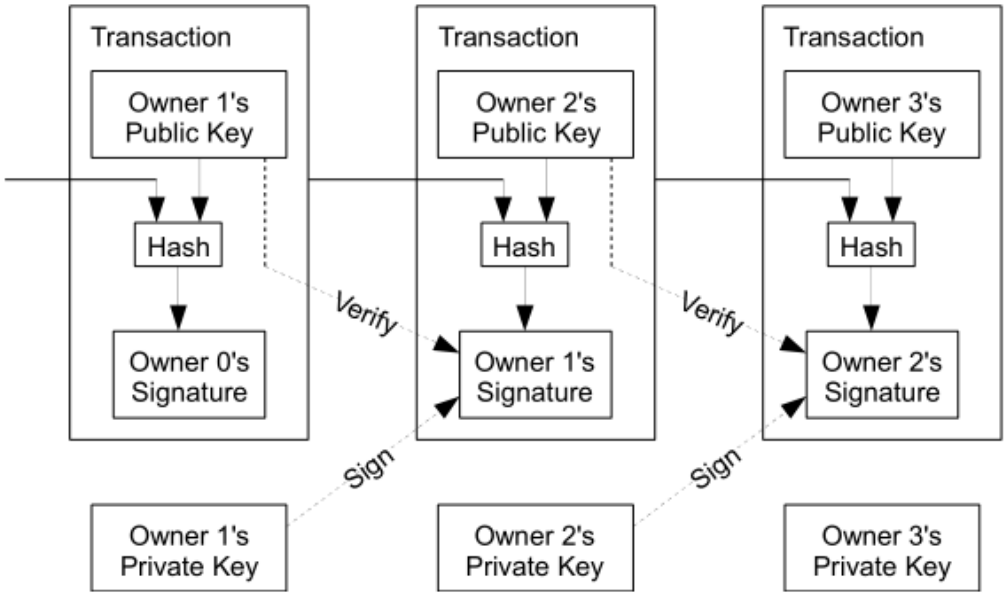
初等数论的应用

- **量子通讯：** 量子通讯（Quantum Communication）是指利用量子效应加密并进行信息传输的一种通讯方式。量子通讯具有高效率和绝对安全等特点，并因此成为国际上量子物理和信息科学的研究热点。



初等数论的应用

- **比特币（区块链）：** 比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。



初等数论的应用

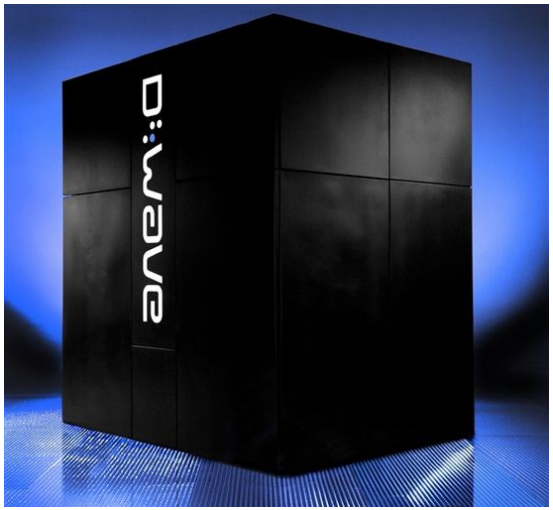
- **比特币（区块链）：** 矿工们利用其计算能力，使用**SHA-256哈希函数**为每个区块计算一个随机数，这个过程所得到的结果非常容易被验证，但是很难被找到。而**不对称密码术**则用于授权比特币区块链上的交易，整个链上的每个用户都会被分配一个公钥和一个私钥，这就是**公钥密码系统**，公钥密码系统使用一对密钥来加密信息：可以广泛共享的公钥和只有密钥所有者才知道的私钥。任何人都可以使用预期的接收者公钥加密消息，但只有接收者才能使用他的私钥解密消息。

  这样的非对称密码算法使用称为**椭圆曲线密码**来生成密钥，给定一个私钥，很容易推导出相应的公钥，但是，反过来计算困难。这就是现在比特币安全的原因。

  而量子计算机可能会对这两道安全防线产生巨大威胁，未来，量子计算机能很快破解哈希函数，从而垄断整个区块链，同时，更近的未来，在2027年，量子计算机的舒尔算法（Shor's algorithm）被预测能在十分钟（600秒）内破解密钥。

初等数论的应用

- **量子计算机：** 量子的重叠与牵连原理产生了巨大的计算能力。普通计算机中的2位寄存器在某一时间仅能存储4个二进制数（00、01、10、11）中的一个，而量子计算机中的2位量子位（qubit）寄存器可同时存储这四个数，因为每一个量子比特可表示两个值。如果有更多量子比特的话，计算能力就呈指数级提高。



2014年1月3日，美国国家安全局（NSA）正在研发一款用于破解加密技术的量子计算机，希望破解几乎所有类型的加密技术。投入巨资 投入4.8亿进行“渗透硬目标”

初等数论的应用

“2，不错啊，质数的第一个。”

其他用途？

初等数论的应用

毕竟李健,毕竟清华_娱乐八卦_天涯论坛

54条回复 - 发帖时间: 2015年1月31日

2015年1月31日 - 李健说:"2是质数里面最大的。" 学霸本色显露无疑哈。 科普下,质数又称素数... 顶楼住,超级喜欢李健,沉稳低调,但性格中有掩饰不住的傲气。他去参加我...

bbs.tianya.cn/post-fun... - 百度快照 - 2824条评价

真没想到李健对于2会说是质数中最小的,真不愧是理工男..._百度贴吧

17条回复 - 发帖时间: 2015年1月30日

真没想到李健对于2会说是质数中最小的,真不愧是理工男啊! 只看楼主 收藏 回复...质数是什么 梦中_失意 画心歌魂 9 清华的学霸呀,让我秒回高考时代..... ...

tieba.baidu.com/p/3558... V3 - 百度快照 - 评价

教学方法和目的

- 基于初等数论的特点，本门课程将采用经典理论与现代应用相结合的方式，系统地介绍初等数论的基本理论、方法和思想，及其在信息科学中的应用。**本课程的预备知识仅仅要求是中学数学即可**。

- **本课程教学目的如下**：通过深入浅出的讲授，使得信息科学专业的学生能够系统掌握和理解初等数论的基本概念与思维方法，为“密码学”和“信息安全”等课程的学习打下坚实基础。

主要的教学内容

- **整除性**：整除定义、最大公因数、最小公倍数、一次不定方程、算术基本定理、素数分布
- **同余**：同余定义、剩余系、欧拉函数、一次同余方程、中国剩余定理、素性测试
- **RSA密码体制**：RSA公钥密码体制、RSA的实现、RSA的安全性讨论
- **二次剩余**：勒让德符号、雅可比符号、二次同余方程、二次剩余的应用
- **原根及其应用**：整数的阶、原根、伪随机数、ElGammal密码体系、椭圆曲线密码

课时安排及上课地点

- 3学分，54课时

- 1-16周：

  每周周四7-9节（**二教319**）

  15: 10 pm – 18:00 pm

- 17-18周： 复习考试

  （期末考初定6月28日，周四下午）

作业及考试成绩

- **平时作业**：3次随堂测试，测试时答对的题得100%分数，课后答对的得60%分数
- **课堂表现**：课堂互动、讲演、考勤等
- **期末考试**：填空题，计算题，应用题，证明题
- **总成绩**：平时成绩*40%+期末成绩*60%

参考文献

- **主要教材**：初等数论及其在信息科学中的应用，朱萍著，清华大学出版社

参考文献

- **主要教材**：初等数论及其在信息科学中的应用，朱萍著，清华大学出版社
- **参考资料**：
  - 数论讲义，柯召、孙琦著，高等教育出版社
  - 初等数论及其应用（原书第5版），Kenneth H. Rosen著，夏鸿刚译，机械工业出版社