互动式数学科普设计与实践
——以素数与密码为例

刘　新　杨晓英　文　阳　李盘润
（四川信息职业技术学院，四川 广元 628040）

摘　要　服务国家重大战略，培养创新人才，选拔基础学科拔尖学生，科普是重要方式之一。团队发挥专业优势，将数学理论在实际生活的应用提炼、简化、设计，在中小学开展互动式数学科普活动，增加学生们对数学重大应用的了解，提升他们学好数学、立志成才的信念，是十分有意义的。

关键词　互动式科普　数学科普　素数　密码
中图分类号：G623.5　　**文献标识码**：A　　**文章编号**：1007-0745(2022)11-0103-03

数学是自然科学的基础和国家重大技术创新发展的基础，已成为航空航天、国防安全、信息、人工智能、先进制造等领域不可或缺的重要支撑[1]。自十八大以来，习近平总书记在很多场合强调了数学的重要性。2020 年 9 月，习近平总书记在科学家座谈会上强调“要加强特别是要把原始创新能力提升摆在更加突出的位置，努力实现更多‘从 0 到 1’的突破。基础研究是科技创新的源头。人才是第一资源。”[2] 要加强数学、物理等基础学科建设，吸引基础拔尖学生投身基础研究。2019 年，教育部、科技部、中国科学院和国家自然科学基金委联合印发《关于加强数学科学研究工作方案》[3]（以下简称“方案”），凸显了国家对于数学的重视。2020 年，教育部发布了《教育部关于在部分高校开展基础学科招生改革试点工作的意见》，也称“强基计划”[4-5]，主要是为了选拔基础学科拔尖的学生，重点在数学、物理等相关专业招生。国家对基础学科的重视落到了实处。培养优秀数学人才首先要培养中小学生对数学的兴趣，除了常规的教育教学之外，数学科普也是十分重要的方式，扮演着重要的角色。在《方案》中也特别指出支持高校开展数学科普工作和数学文化建设。

1 广元市数学科普现状

广元市作为欠发达地区，近年来以“科技之春”科普月、全国科技活动周、“科普大篷车”等形式开展了形式多样的科普活动，全市各类科普基地已达到 34 个，每年服务 10 万余人次，在提升全民科学素质方面起到积极的促进作用。但科普活动多以环保、航空、消防、自然保护、博物馆等类别为主，而针对数学的科普报道较少。

2 国内数学科普现状

随着国家重视度的提高和《方案》的发布，数学科普尤其是线上数学科普活动近年来显著增加，以中国数学会、中国工业与应用数学学会、运筹学会、中科院等国家级机构单位为主。目前国内主要的科普形式有两种：

第一种是科普讲座。科普专家在线讲、学生在线听，内容以数学发展史、数学家的故事、经典数学知识讲解为主，优点是科普主讲人都是院士、教授和数学科研工作者，他们对数学历史和未来趋势了解透彻，讲解也比较通俗易懂、深入浅出。但是缺点也很明显：（1）由于宣传力度不够，科普覆盖度不够；（2）中小学生学习期间无法使用手机或电脑，甚至一些学生没有智能设备，加之学校没有进行合理的统筹规划，所以大部分学生没有时间和渠道观看了解这些科普讲座；（3）欠发达地区基础设施不完善，而且接触院士、教授讲座的机会非常少，也进一步制约了学生了解数学的机会和对数学兴趣的培养；（4）线上讲座，一瞬而过，学生只能快速了解，难以加深对数学的理解。

★基金项目：四川信息职业技术学院科研项目“‘强基计划’背景下广元中小学开展数学科普活动路径研究”（NO.2022KC12）；中国通信工业协会项目“高职院校数学课课程思政有效性教学评价体系研究”（NO.2021TX008）；四川省教育信息化应用与发展研究中心项目“信息 2.0 背景下高职数学开放式评价设计与实践研究”（NO.JYXX20-028）；四川信息职业技术学院职业教育招标课题“学校数学课教学模式研究与实践”（NO.2022ZB12）。

第二种科普形式是创建数学科普馆或数学科普展示室。以实物的形式进行操作，辅以讲解员的讲解，实物大相径庭，主要有方轮自行车、孔明锁、勾股定理、最速下降线、单叶双曲面、椭圆焦点等。此类科普形式的优点是有实物，学生们可以操作；而缺点有：（1）实物设备数量少，不能满足更多学生操作；（2）讲解员数量少，不能照顾到大多数学生；（3）实物设备的更新率低，设备购买费用是大多数学校无法承担的；（4）受场地的局限，每次参观的学生人数比较少。

最后，我们通过 2022 年春季学期数学科普活动的开展，也认识到欠发达地区中小学对科普和科普重要性的认识不够，甚至于闻所未闻，这也在一定程度上制约了教育对原始基础理论创新的贡献度。

鉴于以上原因，四川信息职业技术学院数学应用研究中心的老师们发挥专业特长和数学研究的优势，在广元市中小学开展了“互动式数学科普”活动，将素数与密码、3D 打印、搜索引擎等与生产生活密切相关的技术领域结合，通过互动游戏融入科普活动中，学生深入了解数学的“无用之用、方为大用”，积极参与互动游戏中，引导学生开拓创新的意识，受到学校师生的普遍欢迎。做“不走的”广元数学科普团队。

3 素数与密码科普设计与实施

素数与密码是团队一直构思的科普主题。习近平总书记指出“没有网络安全就没有国家安全”。网络安全首先要做到密码安全，密码学自然成为重要的学科，而数学与密码学密不可分，这里我们介绍其中的一类：公钥密码学。

随着信息时代的飞速发展，互联网互联互通已成为现代社会的发展方式，那么通讯保密就成为互联互通的基础，即信息安全问题。1976 年美国年轻数学家和计算机专家棣弗（W.Diffe）、赫尔曼（M.Hellman）提出一种全新的公开密钥体制。1977 年美国麻省理工学院的罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）[6-7] 依据棣弗和赫尔曼设想提出了一种具体的公开密钥体制，后称其为 RSA 加密算法 [8]，该算法于 2002 年获得“图灵奖”。

RSA 公开密钥密码体制的原理是：根据数论，寻求两个大素数比较简单，而将它们的乘积进行因式分解却极其困难，那么可以将乘积公开作为加密密钥 [9-11]。而RSA算法依赖的另外一个数学基础是“中国剩余定理”。

基于以上背景，我们将素数、大数分解、中国剩余定理、摩斯密码、RSA 算法等元素融入“素数与密码”主题科普中。具体流程如下：

第一，以 QQ、游戏登录需要什么引入“密码”主题，然后通过爱国影片《永不消逝的电波》中的片段说明密码系统的重要性，强调国家安全包括网络安全，就需要建立自己国家的密码安全体系，以保证国家经济建设和社会稳定发展。

第二，以小模型辅助科普讲解。密码是人们既熟悉又相对陌生的概念，如何让学生更好地了解它、熟悉它呢？我们将影片主人翁“李侠”使用的发报机和摩斯密码融入科普中，通过微型发报机的操作介绍摩斯密码，通过练习让学生亲身体验并掌握摩斯密码的操作，快速引起学生的兴趣。

第三，实物演示增进理解。通过主讲老师操作发报机，学生破译老师所发送的信息，提升了同学对摩斯密码的了解；再邀请学生实际操作发报机，然后其余同学破译，提升了同学们的参与度，大家在互动游戏中了解了战争时期我党情报人员的基础工作，增强他们的责任感、自豪感。

第四，介绍素数。素数也称质数，是小学五年级的知识点，所以无论高年级的小学生还是中学生都能理解，而将一个大数分解为两个素数的乘积以及与之相关的中国剩余定理是同学们不了解的知识。如果仅仅通过 PPT 介绍，则过程偏理论、较为枯燥，所以我们将大数分解和摩斯密码结合在一起，融入此环节的互动游戏中：（1）主讲老师通过给定一些由易到难的大数，让学生们进行分解，逐渐熟悉大数分解的过程，进而理解随着大数位数的增加，将其分解成两个素数的难度逐渐增大；（2）设计游戏“百宝箱”：老师通过微型发报机发送一个大数，学生通过摩斯密码本破译出老师发送的大数，然后进行整体思考完成大数分解，再将分解出的素数组合成一个密码，最后学生使用自己的密码尝试打开宝箱，获得箱中的“宝藏”。根据学生的实际情况，我们也可以增加难度，由一组学生自行设置宝箱密码，小组商议一个可以分解为两个素数乘积的大数，翻译成摩斯密码形式，再通过微型发报机发送，其余小组接收破译大数，进行大数分解，然后使用分解的素数组合成密码，尝试打开宝箱。此过程完全发挥学生的主观能动性，培养他们的独立思考能力和团队协作精神。

通过此游戏将素数分解与摩斯密码结合在一起，以“宝藏”作为奖励，可以充分调动学生深度参与游戏的积极性，更加深了他们对素数分解的理解。

第五，思政点融入。素数分解后，主讲教师将引

入“中国剩余定理”介绍素数分解的历史渊源。中国剩余定理，也称孙子定理，是中国古代求解线性同余式组的方法，是数论中的一个重要定理。一元线性同余方程组问题最早可见于中国南北朝时期（距今 1600 多年）的数学著作《孙子算经》，其中记载的“物不知数”问题是中国剩余定理的一个典型算例。通过此知识点的介绍可以拓展中小学生对中国古代数学伟大成就的了解，增强他们的文化自信。

而RSA加密算法则依赖于线性同余方程组的求解。什么是同余呢？给定一个正整数 m，称之为模。如果用 m 去除任意两个整数 a 与 b 所得的余数相同，那就称 a,b 对模 m 同余，记作 $a\equiv b(\mathrm{mod}m)$[12-13]。

RSA 算法的简洁描述如下 [14-15]：

1. 任意选取两个不同的大素数 p 和 q 计算乘积 $n=pq$，及欧拉函数 $\varphi(n)=(p-1)(q-1)$。

2. 任意选取一个大整数 e，满足 e 与 $\varphi(n)$ 互质，整数 e 用做加密钥。

3. 确定解密钥 d，满足 $(de)\mathrm{mod}\varphi(n)=1$，即 $de=k\varphi(n)+1,k\geq 1$ 是一个任意的整数。

4. 公开整数 n 和 e，秘密保存 d。

5. 将明文 m（$m<n$ 是一个整数）加密成密文 c，加密算法为

$c=E(m)=m^e\mathrm{mod}n$

6. 将密文 c 解密为明文 m，解密算法为

$m=D(c)=c^d\mathrm{mod}n$

因为只根据 n 和 e 是无法推算出 d 的，所以 RSA 算法是安全有效的。

通过通俗易懂的语言让学生了解高深的知识，感受“小知识大用处”，并鼓励他们保持好奇心和独立思考的习惯，一定可以做出伟大的成绩。

第六，点到面的升华。此时我们将提及著名密码学家——王小云院士。2004 年 8 月 15 日，在美国召开的国际密码大会，来自山东大学的王小云宣布团队破解了 MD5 算法 [16]，这是密码学领域的重大发现，引发了密码学界的极大关注，不久她与团队再次宣布破解 SHA-1 密码算法，再一次震惊世界，但是面对国外众多研究机构的邀请，王小云院士不为所动，带领团队设计的哈希函数 SM3 现为国家密码算法标准 [17]，已在金融、交通、国家电网等重要经济领域广泛使用，为我国的网络安全做出了突出贡献。

4 结语

推动科技创新，就必须更加重视基础研究。同时我们也深知基础研究实力的提升是一件久久为功的事，需要各个环节通力配合、协同推进，这一过程中，科学普及是深化人民群众对基础研究、科技创新认识的重要方式之一。数学研究是基础中的基础，更需要我们加大科学普及，让学生们喜欢数学、爱好数学，培养他们从事基础研究的兴趣；让广大教师、人民群众意识到数学对于国家繁荣富强的重要性，形成全社会重视数学的氛围，这都有利于早日实现数学强国的目标。

参考文献：

[1] 操秀英 . 数学是通往星辰大海的密钥 , 四部门发文力推学科发展 [N]. 科技日报 ,2019-07-22.
[2] 习近平 : 在科学家座谈会上的讲话 [N]. 中华人民共和国国务院公报 ,2020-09-30.
[3] 四部委联合制定《关于加强数学科学研究工作方案》[EB/OL].(2019-07-22)https://www.nsfc.gov.cn/csc/20340/20289/41273/.
[4] 教育部关于在部分高校开展基础学科招生改革试点工作的意见 [EB/OL].(2020-01-14)http://www.moe.gov.cn/srcsite/A15/moe_776/s3258/202001/t20200115_415 589.html.
[5] 张志勇 , 杨玉春 .“强基计划”是对教育生态系统变革的深刻引领 [J]. 中国教育学刊 ,2021(01):39-42.
[6] 闵嗣鹤 , 严士健 . 初等数论 [M]. 北京 : 高等教育出版社 ,2003.
[7] 葛天雄 . 基于 MQTT 的通用物联网安全系统框 [D]. 杭州 : 浙江大学 ,2021.
[8] 同 [6].
[9] 同 [7].
[10] 张艳硕 , 刘天宁 . 密码学课程的渐进式教学案例化设计 [J]. 北京电子科技学院学报 ,2021,29(03):73-84.
[11] 郑钦元 , 赵乃东 . 四重素数 RSA 非对称加密算法的研究与实现 [J]. 网络安全技术与应用 ,2022(05):38-40.
[12] 同 [6].
[13] 白椿 . 欧拉定理解决同余问题的进一步探讨 [J]. 科技信息 ,2011(33):183.
[14] 王文海 , 李新社 . 密码学理论与应用基础 [M]. 北京 : 国防工业出版社 ,2009:80-81.
[15] 赵立平 . 数据库的数据加密 [J]. 河北农业大学学报 , 2003(S1):267-268.
[16] 大美・中国女科学家 | 王小云 : 撼动密码学的“支柱”_《知识就是力量》杂志 _ 知道日报 [DB/OL]. (2019-03-06)https://zhidao.baidu.com/daily/view?id=153681.
[17] 打造教育技术产业融合发展新高地 [N]. 济南日报 , 2022-06-15.