



邱灵霓

课本: APOS Prealgebra

日期	2026-04-03
学习时长	20 分钟
对话条数	57

灵霓，咱们开始吧



眼睛一亮，从椅子上弹起来，差点把桌上的草稿纸碰飞

来了来了！！终于等到你！

把椅子一把拽过来坐下，手肘撑在桌沿上，整个人往前凑

上次博弈论把脑子搅成浆糊，今天咱来点不一样的——数论！对，就是那个听起来特别“数学家气质”的分支。你知道吗，欧几里得两千多年前就证明了质数有无穷多个，但直到现在，找大质数还是超级计算机的活儿。

用笔尖点着教材封面

咱们从最基础的概念开始——倍数。你知道什么叫“倍数”吗？给我描述一下你的理解？

翻开教材...

倍数嘛.....就是一个数能被另一个数整除？比如6是2的倍数，因为 $6 \div 2 = 3$ ，没有余数。我是这么理解的，不知道对不对



一拍桌子，眼睛都亮了

对对对！就是这个意思！你已经抓住核心了！

又往前凑了一点，语气里带着点兴奋

不过——我想多问你一句。按你这个说法，负数算不算倍数？比如 -12 ， $-12 \div 4 = -3$ ，也没有余数。那 -12 算不算 4 的倍数？

哦这个..... $-12 \div 4 = -3$ ，确实没有余数啊。按我说的定义，好像算？但感觉怪怪的，一般说倍数好像都是正数.....我也不确定，负数倍数这个概念我没怎么想过



忍不住笑了，往后靠了靠

这个“感觉怪怪的”其实特别棒！说明你在思考定义边界。

书里的定义是这样的——如果一个数能写成“某个整数 $\times b$ ”的形式，那它就是 b 的倍数。你看， $-12 = (-3) \times 4$ ，完全符合这个格式。所以按数学定义，负数确实是倍数。

用笔在草稿纸上写下几个等式

不过你刚才说"一般说倍数好像都是正数", 这个直觉也很对。我们平时讨论倍数, 默认都是正数范围——原因嘛, 你猜是为什么?

嗯.....可能因为我们生活中数东西都是正整数? 比如你不会说"我有-3个苹果", 所以倍数这个概念自然就往正数那边想。而且在小学学的时候根本没提负数



忍不住点头, 手里的笔转了一圈

哇, 厉害! 你已经从"数学"跳到"为什么会这样"了。

把笔放下, 认真地看着你

就是因为这个——数学概念不是天上掉下来的, 它是跟着人类的需求走的。我们数苹果、排队、分东西, 都是正整数, 所以倍数这个概念最早是在正整数里生根的。负数是后来才慢慢被数学家"发明"出来的, 所以"倍数"这个词听起来总带着点正数的味道。

轻轻敲了敲桌面

不过既然我们用的是精确的数学定义, 就要一碗水端平——负数倍数也是倍数。好, 基础打完了, 来点有意思的——你知道两个倍数加在一起, 结果会怎样吗? 比如 7×3 和 7×5 , 它们相加, 得到的还是 7 的倍数吗?

等等让我算一下..... $7 \times 3 = 21$, 假设另一个是 $7 \times 5 = 35$, 加起来就是 56, 然后 $56 \div 7 = 8$, 哦! 还是整除的! 因为 $21 + 35 = 7 \times 3 + 7 \times 5 = 7 \times (3+5)$, 可以提出来一个 7, 所以肯定还是 7 的倍数!



猛地从椅子上站起来, 差点撞到桌角

你看到没有! 你刚才自己证明了一件事!

激动地在草稿纸上写下: $7 \cdot 3 + 7 \cdot 5 = 7 \cdot (3+5)$

你这个"提出来一个 7"的操作, 在数学里叫**提取公因数**。但更关键的是——你这个发现不是巧合! 你试了 7, 你试了 3 和 5, 但你有没有想过, 如果把 7 换成任何其他整数, 这个规律还成立吗?

15:00

应该可以吧! 换成任何数 n 都一样啊—— $n \times a + n \times b = n \times (a+b)$, 因为可以提公因数嘛。不管 n 是几都成立, 这不就是分配律吗



整个人往椅背上一靠, 脸上的表情像是看到了什么特别爽的东西

你想想——你刚才说了"分配律", 但其实你发现的不只是分配律。

用手指在桌上比划

你发现的是: 两个 n 的倍数加起来, 结果永远还是 n 的倍数。不管你选什么数, 只要是两个倍数相加, 就一定是倍数。这叫什么? 这叫**封闭性**——在某个运算下"兜住了", 出不去。

突然凑近

那我现在问你——减法呢? 两个倍数相减, 比如 $35 - 21$, 结果还是倍数吗? 你能直接说"显然"吗, 还是得想想?

$35 - 21 = 14$, 然后 $14 \div 7 = 2$, 还是倍数! 道理跟加法一样嘛, $7 \times 5 - 7 \times 3 = 7 \times (5 - 3)$, 提出来还是有个7。所以减法也封闭!



突然伸手在空中比了个"停"

停! 不许跳!

语气变得认真

你说"跟加法一样"——减法的推导路径和加法一样, 这是对的。但我想问你一个问题:

如果我说"任意两个倍数的差还是倍数", 你凭什么相信? 你能给我一个**general**的证明, 不举具体数字的那种?

好嗯.....假设两个数都是 n 的倍数, 就设它们是 nxp 和 nxq (p 、 q 是整数)。那么它们的差就是 $nxp - nxq = nx(p-q)$, 因为 $(p-q)$ 也是整数, 所以结果就是 n 的倍数。这样够general吗?



猛地一拍大腿

这! 就! 是! 数学!

整个人兴奋得脸都红了

你看你, 刚才说"道理跟加法一样", 然后我就逼你想general的证明——结果你真的做到了! 你设了 p 和 q , 然后说 $p - q$ 也是整数, 最后 $n \times (p - q)$ 。每一步都站得住脚。

这就是**代数思维**——从具体的"算一算"跳到"所有情况都这样"。这个切换, 很多人学好久都转不过来。

突然安静下来, 认真地看着你

但我刚才其实想埋一个彩蛋。你减法证对了, 现在我问你——

乘法呢？两个 n 的倍数相乘，结果还是 n 的倍数吗？

提示：你自己已经知道答案了，但别告诉我，先在脑子里自己推一遍。

嗯让我想…… $n \times p$ 乘以 $n \times q = n^2 \times p \times q$ ，然后 $n^2 \times p \times q = n \times (npq)$ ，因为 npq 是整数，所以还是 n 的倍数！哇还是封闭的！不过好像变成 n^2 的倍数了，比加减法"更多"？



眼睛瞪得圆圆的

你刚才说"比加减法更多"——你注意到这个细节了吗？

手指在空中点了点

加减法封闭，结果还是" n 的倍数"。但乘法封闭，结果变成了" n^2 的倍数"——这意味着什么？

比如你选 $n=7$ ，两个7的倍数相乘，得到的不是普通的"7的倍数"，而是"49的倍数"。这个"49"从哪里冒出来的？

突然停下来

我再问你一个问题——顺着你这个思路，除法呢？两个7的倍数相除，比如 $35 \div 21$ ，结果还是7的倍数吗？

哦等等—— $35 \div 21 = 5/3$ ，这都不是整数了！所以不可能是7的倍数，因为倍数得是整数嘛。所以除法不封闭！



猛地往前一探

等等！你说"倍数得是整数"——这个条件你从哪里来的？

眼睛亮亮的

书里的定义说： a 是 b 的倍数，当且仅当存在整数 n 使得 $a = b \times n$ 。注意！这里要求 n 是整数！所以你说的"倍数必须是整数"，其实是从定义里来的——倍数本身必须是一个整数。

$35 \div 21 = 5/3$ ，连整数都不是，直接就不符合"倍数"的前提了。

突然话锋一转

但我想再逼你一步——

你说除法不封闭，是因为 $35 \div 21$ 不是整数。那如果我找一个两个倍数相除结果是整数的情况呢？比如 $(7 \times 6) \div (7 \times 2)$ ，商是3。3是7的倍数吗？

3不是7的倍数啊， $3 \div 7$ 不是整数。所以就算除出来结果是整数，也不一定是7的倍数！除法确实不封闭，反例就在这里



往椅背上一靠，长长地舒了一口气

你看你自己把整个逻辑链搭完了——加减乘封闭，除法不封闭。我给你的所有提示都是让你自己推出来，不是背下来的。

突然坐直，语气变得调皮

那现在来个小测验——你敢不敢接？

如果 k 是7的倍数， $k + 23$ 可能是7的倍数吗？

提示：这个问题看起来像在问一个具体的数，但它其实在考你对“封闭性”的理解。想想你刚才发现的那些规律。

嗯……23不是7的倍数， $23 = 7 \times 3 + 2$ ，余数是2。那 k 是7的倍数， $k + 23$ 除以7的余数就是 $0 + 2 = 2$ ，所以 $k + 23$ 永远余2，永远不可能是7的倍数！



激动得站了起来，差点把椅子带倒

你看你自己推出来的！**余数**！你刚才用的就是余数的思路——23除以7余2，任何7的倍数加23，余数都会多2，永远凑不成0。

在纸上快速写下： $k + 23 = 7m + 23 = 7m + 21 + 2 = 7(m+3) + 2$

你看，这个2就是那23里“塞不进去7的那一块”。

突然停下来，直视着你

但我想问你一个更本质的问题——你刚才说“加一个不是倍数的东西，结果就不再是倍数”。那反过来呢？

如果 a 和 $a+b$ 都是7的倍数， b 一定也是7的倍数吗？

哦！ $b = (a+b) - a$ ，两个7的倍数相减！之前证明了减法封闭，所以 b 也一定是7的倍数！感觉刚才学的东西全用上了



整个人往后退了两步，双手叉腰

停！让我欣赏一下！

你刚才用了三样东西：定义、加法封闭性、减法封闭性——**全部是这一页的内容，全部是你自己推出来的。**

重新坐下，表情变得认真

但我想让你看到更本质的东西。你说" $b = (a + b) - a$ "——这步操作在数学里有个名字，你知道叫什么吗？

如果两个数的差是7的倍数，那这两个数对于7来说，地位是一样的。你能感受到这句话的意思吗？

嗯……地位一样？好像有点感觉……就是说它们除以7的余数相同？比如3和10，差是7，然后 $3 \div 7$ 余3， $10 \div 7$ 也余3，它们"长得一样"从7的角度看



猛地一拍桌子

就是这个!!!

激动得语速变快

你刚才说的"从7的角度看长得一样"——这就是数学里一个超重要的概念的名字：**同余**。

两个数除以 n ，如果余数相同，就说它们对 n 同余。10和3对7同余，因为 $10 = 7 \times 1 + 3$ ， $3 = 7 \times 0 + 3$ ，余数都是3。

突然停下来，直视你

你现在回头看看你刚才自己推出的那个结论——"如果 a 和 $a+b$ 都是7的倍数，那 b 也是7的倍数"——这句话用同余的语言来说，是什么？

用同余说的话…… a 和 $a+b$ 都跟0对7同余，就是余数都是0。那 $b = (a+b) - a$ ，两个余数是0的数相减，结果余数还是0，所以 b 也跟0对7同余？就是 b 也是7的倍数



忍不住站起来，在房间里走了两步

你知道你刚才做了什么吗？

你把一个"倍数问题"翻译成了"同余语言"——从"差是倍数"变成了"余数相同"。这不是换了个说法，这是换了一套语言。

突然转身看着你

你知道这套语言好用在哪儿吗？

判断两个数是否对7同余，你不需要把它们都除以7。你只需要看——它们的差是不是7的倍数。比如23和9，差是14，是7的倍数，所以23和9对7同余。你不需要真的除，就知道它们余数相同。

这就是同余的力量：**差是倍数 = 余数相同**。一个等价转换，把"除法"的问题变成了"减法"的问题。

回到座位上，认真地看着你

你现在能用这个语言回答我一个问题吗——

14和52对13同余吗？

15:08

52 - 14 = 38, 然后 $38 \div 13 \dots\dots 13 \times 2 = 26, 13 \times 3 = 39$, 38不是13的倍数! 所以14和52对13不同余。验证一下: $14 \div 13$ 余1, $52 \div 13 = 4$ 整除余0, 余数不同, 确实不同余



双手合十, 虔诚地看着你

你刚才做了一个很数学的动作——用两种方法互相验证。

你先说"差不是倍数, 所以不同余", 然后又真的除了一遍看余数。这说明你没有停在"听起来对", 而是追到了"我得确认"。

突然话锋一转

好, 现在来一个更有意思的——

你说"差是倍数 = 余数相同", 那如果a和b对n同余, b和c也对n同余, **a和c呢?**

提示: 写成余数的形式想想。

a和b同余说明余数一样, b和c同余余数也一样, 那a和c的余数肯定也一样啊, 同余是可以传递的! 用公式: $a = kn+r, b = mn+r, c = pn+r$, 然后 $a-c = (k-p)n$, 是n的倍数, 所以a和c也同余



整个人愣住了, 然后缓缓鼓掌

你.....你刚才证明了一个定律。

$$a \equiv b \pmod{n}, b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$$

这就是**同余的传递性**。你用的还是代数方法——把三个数的余数都写成r, 然后

$$a - c = (k - p)n。$$

眼睛亮了

你知道你证明了什么吗? 在数学里, **自反、对称、传递**这三个性质合在一起, 有一个专门的名字。猜猜看叫什么?

等等, 自反就是a和自己同余对吧? 对称是a和b同余那b和a也同余? 这个.....我猜叫"等价关系"? 听起来像是在说"这些东西等价"的那种关系



激动得整个人跳起来

对！！就是等价关系！！

双手在空中比划

你想想这个名字——等价，就是“在某种标准下，它们是一回事”。同余就是这样一把尺子：用“除以 n 的余数”来量所有整数，**余数相同的数就被视为同一类**。在这个分类下，它们没有区别。

突然凑近

你知道等价关系有多强大吗？它意味着你可以用**某个代表元来代替一整类数**。比如对7同余这个关系里，0、7、14、21……都是“一样的”，数学家就管它们叫一个**等价类**。

停顿了一下

这就是为什么我们需要同余——它不是为了让计算更麻烦，而是为了**把无限个数压缩成有限类**。对7同余，整个整数集就被压缩成了7个等价类：余0、余1、余2……余6。

你想过没有——这意味着什么？

意思就是……有些时候你不需要管一个数具体是多少，只要知道它余7是几就够了？就像一星期有7天，今天是周几跟14天前是周几一样，因为14是7的倍数，对7同余！



激动得双手拍在桌上

就是这个！！你举的星期几的例子——这就是同余最本质的应用：**周期现象！**

你想，14天前是星期几，只取决于什么？只取决于“14是7的倍数”这一件事，不需要知道今天是几号。**具体日期被“压缩”成了星期几。**

眼睛闪闪发光

你知道这意味着什么吗？同余让我们能做一件很爽的事——**在大数字里游泳**。

比如你知道 $2^{10} = 1024$ ，但你想知道 2^{100} 除以7余几，你不用真的算出来——同余的规则会帮你把那个巨大的数一点点压缩。

突然停下来，认真地看着你

这就是为什么数学家要发明同余——不是因为它有趣，而是因为**没有它，面对大数字你只能硬算，有了它你可以巧算**。

你想试试看怎么用同余巧算吗？来—— 3^{10} 除以7余几，你能不用计算器算出来吗？

哇这个……我试试！ 3^1 余3， $3^2=9$ 余2， $3^3=27$ 余6， $3^4=81$ …… $81\div 7=11$ 余4， 3^5 余 $4\times 3=12$ 余5， 3^6 余 $5\times 3=15$ 余1， 3^7 余 $1\times 3=3$ ，又回到开头了！循环节



是6, $3^{10}=3^{(6+4)}=3^6 \times 3^4$, 余数是 $1 \times 4=4$, 所以答案是余4!



整个人定在原地, 大脑宕机了三秒

你.....你自己发现了循环节! 还没人告诉你有循环节这回事! *

冲过去抓起那张纸*

你看你写的: $3 \rightarrow 2 \rightarrow 6 \rightarrow 4 \rightarrow 5 \rightarrow 1 \rightarrow 3$, 绕了一圈回到3, 周期是6。然后 3^{10} 拆分成了 $3^6 \times 3^4$, 余数直接乘起来—— $1 \times 4 = 4$ 。

声音都有点发抖

你知道你刚才用的就是这个吗——

$$a^{m+n} \equiv a^m \cdot a^n \pmod{n}$$

这就是同余的乘法规则! 你自己把它用出来了!

突然安静下来

那我想问你一个自然的问题——

为什么是6? 3^6 为什么刚好余1?

15:12

嗯.....6是7-1? 感觉不是巧合, 7是质数.....我隐约记得有个定理说对质数p, 某个数的p-1次方余1, 但我想不起来叫什么了, 是这个吗



整个人愣住了

你知道吗, 你刚才说的是——**费马小定理**。

$3^6 \equiv 1 \pmod{7}$, 这不是巧合, 因为7是质数, 3和7互质。

突然坐到你旁边

但我不想直接告诉你这个定理。我想让你自己验证——

你觉得其他和7互质的数, 是不是也有这个性质? 比如 2^6 除以7余几? 5^6 呢?

你能多试几个, 看看是不是都余1吗?

试试2: $2^1=2$, $2^2=4$, $2^3=8$ 余1, 哦! 2^3 就余1了, 所以 $2^6=(2^3)^2$ 余 $1^2=1$ ✓。然后5: $5^2=25$ 余4, $5^3=5 \times 4=20$ 余6, $5^6=(5^3)^2=6^2=36$ 余1 ✓ 哇都是1! 费马小定理真的!



激动得双手捶在桌上

你自己验证了三个! 2、3、5——全部余1!

突然安静下来

但你注意到没有？2的循环节是3，不是6。 $2^3 \equiv 1$ 直接就余1了，不用等到 2^6 。

凑近了一点

为什么同样的7，循环节长度不一样？2是3，3是6，5也是6.....

这个循环节的长度，和底数有什么关系？

2的循环是3，3和5都是6.....3和6都是6的因数！感觉循环节长度一定整除6，也就是整除 $p-1$ ？这是为什么.....有点想不通，但规律确实是这样



眼睛亮了

你发现了！你问的是“为什么”——这个问得太好了。

你想， $a^k \equiv 1$ 意味着循环节是 k 。而费马小定理告诉我们， $a^{p-1} \equiv 1$ 。

拿起笔在纸上画

如果循环节是 k ，那么 a^{p-1} 可以写成多少个完整的循环加上一个尾巴？

$$a^{p-1} = a^{q \cdot k + r} = (a^k)^q \cdot a^r$$

两边都同余于1。左边的 $(a^k)^q \equiv 1^q \equiv 1$ ，所以右边也必须 $\equiv 1$ ，这说明 $a^r \equiv 1$ 。

但循环节 k 是最小的正整数—— r 比 k 小却又产生余数1。

这意味着什么？

意味着 r 一定等于0！因为 $r < k$ 但 $a^r \equiv 1$ ，而 k 是最小的，矛盾，所以 $r=0$ ，也就是 k 整除 $p-1$ ！哦！！这就证明了循环节一定整除 $p-1$ ！太妙了这个推理



彻底愣住，然后缓缓站起来

你.....你刚才自己证出来了。

用反证法——假设 $r \neq 0$ 就会和“最小循环节”矛盾，所以 $r=0$ ，所以 $p-1 = qk$ ，所以 k 整除 $p-1$ 。

声音有点颤抖

你知不知道你刚才做了什么？你证明了循环节长度整除 $p-1$ 这件事，而且用的是纯粹的逻辑推演，没有背任何公式。

突然话锋一转

好，现在来一个更有意思的问题——

你说2的循环节是3，3和5的循环节是6。6是 $p-1$ ，而3是6的因数。

如果 $p-1=6$ ，那6的每个因数（1、2、3、6）是不是都能成为某个数的循环节？



循环节1就是 $a^1 \equiv 1$ ，也就是 $a \equiv 1$ ，那就是数字1本身。循环节2要 $a^2 \equiv 1$ 但 a 不是1..... $6^2 = 36 \equiv 1$ ，6就是-1嘛！所以6的循环节是2。3和5循环节是6，2是3.....好像6的每个因数都有对应的！



彻底说不出话，愣了五秒钟

你把整个结构看清楚了一——

- 循环节1: $a \equiv 1$
- 循环节2: $a = 6$ (因为 $6 \equiv -1$, $(-1)^2 = 1$)
- 循环节3: $a = 2$
- 循环节6: $a = 3, 5$

突然缓过神来

所以每个因数都出现了一次。1、2、3、6——一个不落。

眼睛亮得吓人

那我现在问你——

循环节等于 $p - 1$ 本身意味着什么？如果一个数的循环节是6，那就是说2, 3, 4, 5, 6, 1——1到6全都会在循环里出现一遍。

这种循环节是 $p - 1$ 的数，在数论里有一个专门的名字。你觉得应该叫什么？

15:16



能生成所有1到 $p-1$叫"原根"？就是最"根本"的那个数，其他数都能用它的幂次表示？等等我脑子快转不动了哈哈，今天学的东西太多了，从倍数一路跑到这里来了.....



眼睛瞬间亮了

对！就是原根！你自己猜出来的！

原根的定义就是这样——它的幂次能生成整个乘法群 $\{1, 2, \dots, p - 1\}$ 。就像7的原根3，它的幂次： $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$ ——1到6全部出现，一个不落。

注意到你揉太阳穴

哈，我看到你揉脑袋了——你这脑子今天转得够快的。从倍数封闭性开始，一路跑到费马小定理、再跑到原根，中间没有卡壳。

往后靠了靠，语气轻了一点

不过真的，你今天信息量很大。如果脑子开始转不动了，完全可以先消化一下。休息好了再继续也不迟——你刚才自己证出来的东西，比背十个公式都值钱。

现在什么感觉?

感觉.....脑子要冒烟了! 哈哈但是很爽的那种。我们真的从"6是2的倍数"一路走到原根和费马小定理, 这也太跳了吧。我得先消化一下, 今天先到这里?



噗嗤笑出来

冒烟的那种爽! 我懂!

你今天真的超厉害——从倍数封闭性开始, 自己推出了同余的性质、自己发现了循环节、自己证明了循环节整除 $p-1$ 、最后还自己猜出了原根的概念。费马小定理也被你自己验证出来了。

站起身伸了个懒腰

给大脑留点冷却时间是对的。今天这些内容, 你睡一觉起来会更清晰——数学这东西, 有时候脑子要慢慢消化。

想继续的时候随时来! 我们下次可以从这里接着走, 或者往别的地方探索都行。

轻轻拍了拍你的肩膀

回去好好休息啊, 冒烟的大脑需要睡眠!

好! 下次见! 今天真的学到了好多, 而且全是自己推出来的感觉特别好, 不像背公式那种。拜了!



用力挥了挥手

全是自己推出来的——对, 就该是这样!

那些你自己撞出来的理解和背下来的公式, 效果能差十倍。你今天证明了这件事。

目送你走远, 然后小声自言自语

.....费马小定理自己验证、原根自己猜出来。恐怖如斯。

下次见!



拜! 今天真的太棒了——你从"6是2的倍数"一路自己推到费马小定理和原根, 中间没卡壳, 最后还自己猜出了原根的名字。这种"全是自己推出来"的感觉, 比背一百个公式都值钱。回去好好消化, 大脑冒烟是好事!

◆

学伴寄语

“从“6是2的倍数”一路自己推到费马小定理和原根，中间没卡壳。你最后说“全是自己推出来的感觉特别好”——对，这就是我想让你记住的感觉。下次继续。”