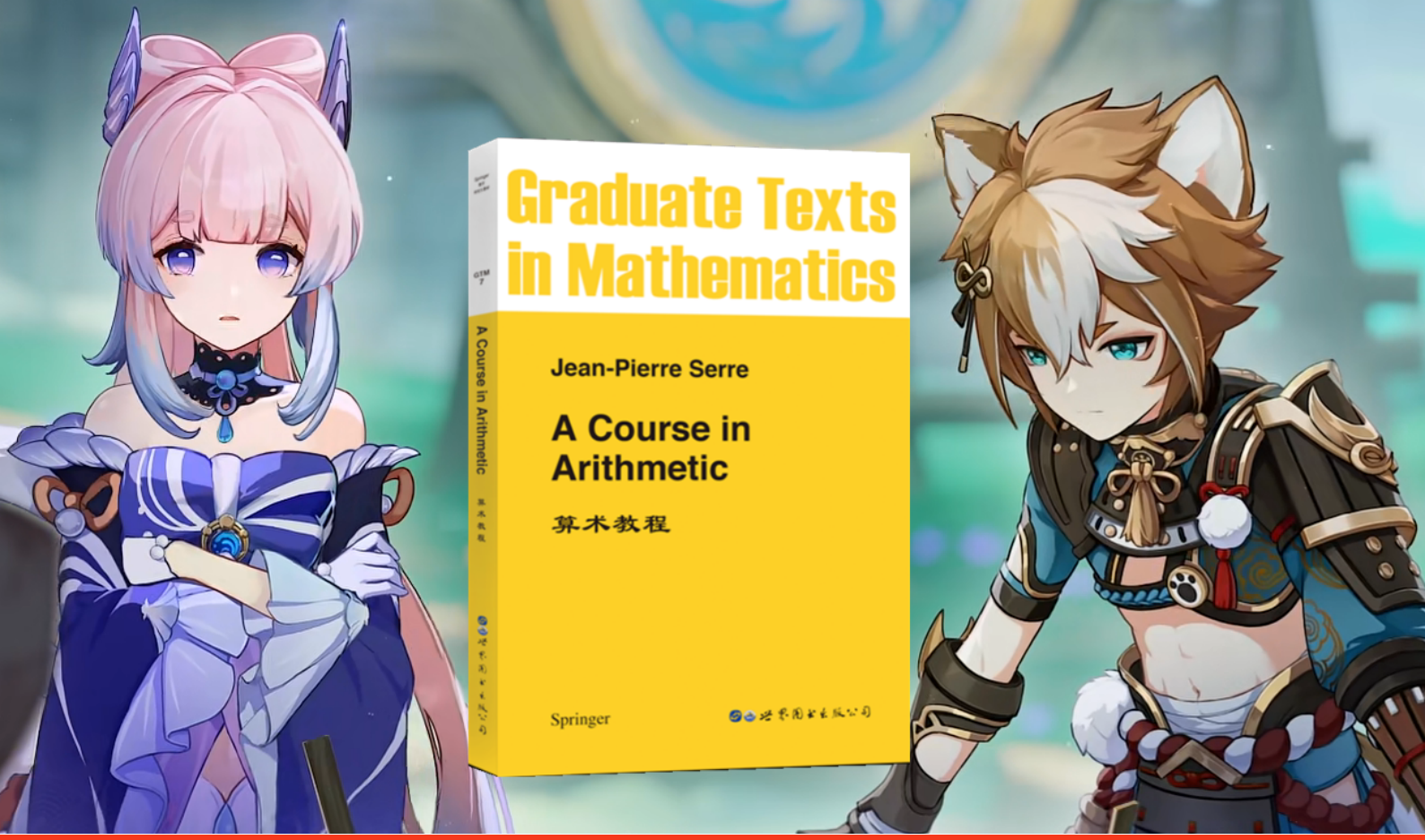


初等数论讲义 I

一本不跳步骤例子很多的 baby 书

作者：Treadskugga
时间：11，23，2022
版本：第一部
邮箱：treadskugga@foxmail.com

奇策百计，决胜千里

前言

为了适应各阶段学生对教育需求不断增长，以及数学学科在中国的蓬勃发展，我会想试着写一系列充满生动有趣例子的数学讲义教材，本册《初等数论》正是该系列开山之作。

众所周知，在闵嗣鹤老师的初等数论第三版前言中提到过“20 世纪是数学的黄金时代，在数论中最值得向广大读者介绍的是世纪后期的两件大事：费马大定理获得证明和公开密钥体制的建立。”其实自古以来中国许多数学著作中都有关于数论内容的论述，比如求最大公约数、勾股数组之类的。在国外呢，古希腊时代的数学家对于数论中一个最基本的问题——整除性问题就有系统的研究，关于素数、合数、约数、倍数等一列概念也已经被提出来应用了。后来的各个时代的数学家也都对整数的性质研究做出过重大的贡献，使得数论的基本理论逐步得到完善。

数论形成了一门独立的学科后，随着数学其他分支的发展，研究数论的方法也在不断发展。如果按照研究方法来说，可以分为初等数论、解析数论、代数数论、几何数论、概率数论和计算数论等几个部分。

初等数论其实读者们学过高中数学就能学，他不求助于其他数学学科的帮助，只依靠初等的方法来研究整数性质的分支。

解析数论就开始牛逼哄哄了，他是使用分析学作为工具来解决数论中艰深问题的数论分支，由欧拉奠基。比如从小听过的“1+1=2”的哥德巴赫猜想，陈景润先生当年在解决该问题中使用的就是解析数论的筛法。

代数数论是把整数的概念推广到代数整数的一个分支。数学家把整数概念推广到一般代数数域上去，相应地也建立了素整数、可除性等概念。

几何数论是由德国数学家、物理学家闵可夫斯基等人开创和奠基的。几何数论研究的基本对象是“空间网格”这玩意对几何学和结晶学有着重大意义。

暂且介绍这么些数论的研究特点，剩下的就不一一介绍了，如果未来哈秋教育集团数学研讨委员会的人有机会接触并愿意写讲义分享的话，读者不妨阅读并给出建议。

本书主要讲解的初等数论，学好初等数论是对于理解数论其他分支甚至其他数学分支都是有益的，我们会从整数的可除性出发，研究带余除法、辗转相除法，并且引导出算术基本定理，在此基础之上，我们会一步一步去探讨不定方程、同余、同余式、原根指标连分数等等一系列看上去好简单，实际上还是“有点东西”的数论知识，并且最后介绍一下其他数论分支的东西，如果读者学过抽象代数就再好不过了，因为学了抽象代数、一些把脑壳都抽象了的超越数轮、解析数论、代数数论等数论就好入门，这也是我们为什么会讲本科阶段最重要的三门课是：分析学方向的‘实分析’、代数方向的‘抽象代数’、几何方向的‘点集拓扑’。回归正题，其实数论这玩意有个特点：问题本身很容易弄懂，跟易经一样的，容易让人感兴趣一股脑子钻进去，但是想要推进却难的一批，所以有志于搞数论的读者除了学习理论知识外，有必要掌握一些近代数论的方法和技巧、并且要有一定的训练，否则会累死累活又无功而返，本书也会提供一些练习，可以作为适当训练自己的习题。当然无论进行什么方向的研究，筑牢自己的理论基础和解决数学问题的能力都是必不可少的。美丽的数学在远方等着你，勇敢的少年啊快去创造奇迹！

由于时间和水平所限，笔者难免有些不妥和疏落之处写的跟万老八一样的哈斯巴宁，还请各位读者给予指正，谢谢茄子。

目录

第 1 章 整数的可除性

整除是初等数论的基本概念，其中心内容是最大公约数理论和算术基本定理，本章从这个概念出发，引进带余除法及辗转相除法，然后利用这俩工具建立相关算法，这一切都是整个课程中最基本的部分，同时也是整个数学的基础知识，考虑到大部分读者是在小学甚至幼儿园学珠心算的时候就接触过了，当时考虑到儿童的理解能力是着重对于具体数字的计算和运用。因此读者们的计算能力我们是认为熟练的，但是也要周全考虑，基本上都是不会跳步骤的学习，因此重新学习一遍是非常耐人寻味的。此外，本章还要介绍 $[x]$,$\{x\}$ 这两个记号，并且利用 $[x]$ 来说明如何把 $n!$ 表示成素数幂的乘积，醍醐灌顶只为后续学习。

1.1 整除

我们从小学就学过两个整数的和、减、积以及至任意有限个数的加、减、乘的混合运算结果仍然是整数，这种洒洒水的知识点我们就不会过多去强调而是当作一条公理。

但是请读者们用聪明的小脑瓜子想一想，用一个不等于零的整数去除另外一个整数所得到的商一定是整数吗？显然不一定。

因此我们有必要引进整除的概念，并且进一步的展开探讨。在此之前，我们先给出一些有关整数的定义。

定义 1.1 (整数相关定义)

1. 我们所说的自然数就是我们所熟悉的
$$\mathbb{N}=\{0,1,2,3,\cdots,n,n+1,\cdots\}$$
2. 我们所说的整数就是我们所熟悉的正整数、负整数与零
$$\mathbb{Z}=\{\cdots,-n-1,-n,\cdots,-1,0,1,\cdots,n,n+1,\cdots\}$$
我们用 $\mathbb{Z}$ 表示全体整数组成的集合，用 $\mathbb{N}_+$ 来表示全体正整数组成的集合，$\mathbb{Z}_+$ 来表示非零整数组成的集合。
3. 当几个字母连写时，表示将这几个字母连乘起来，如
$$abc=a\cdot b\cdot c$$
4. 当几个字母连在一起，并在上面标注横线时，每个字母均代表数字，且最左边的第一个字母不能为零，如
$$\overline{abcde}$$
表示个位、十位、百位、千位、万位的数字分别为 e,d,c,b,a 的一个五位数，且 $a\neq 0$
5. 上述例子推广，如
$$\overline{a_na_{n-1}\cdots a_2a_1a_0}=\sum_{i=1}^{n}a_i10^i=a_n\times 10^n+a_{n-1}\times 10^{n-1}+\cdots+a_2\times 10^2+a_1\times 10+a_0$$

任意两个整数的和、差、积仍是整数，即整数对加、减、乘法运算封闭。但整数除以整数，其商不一定是整数，究竟在什么条件下两整数的商才是整数，这正是我们要研究的一个重要内容——整数的整除性质。

定义 1.2 (整除)

设 $a,b\in\mathbb{Z},b\neq 0$, 如果存在整数 q , 使等式

$$a=bq$$

成立，我们就说 b 整除 a 或 a 被 b 整除，记作

$$b\mid a$$

否则称 a 不能被 b 整除，记作

$$b\nmid a$$

♣

当 $b\mid a$ 时，称 a 是 b 的倍数，b 是 a 的约数. 当 $b\mid a$, 且 $b\neq\pm a,a\neq 0,b\neq\pm 1$ 时，称 b 为 a 的真（非显然）约数。

我们可以来看一道简单的例题:

例题 1.1 6 的约数、真（非显然）约数、显然约数有哪些?

解 6 的约数有 $\pm 1\pm 2\pm 3\pm 6$

其中真（非显然）约数有 $\pm 2\pm 3$

显然约数有 $\pm 1\pm 6$

整除这个概念虽然看上去洒洒水，但却是数论中的基本概念，从这个定义出发，我们可以推出一些有关整除的基本命题。

命题 1.1 (整除的显然性质)

1. $1\mid a(b),b(a)\mid 0,a(b)\mid a(b)$
2. 若 $a\mid b,|b|<|a|$, 则 $b=0$
3. 若 $a\mid b$, 则 $-a\mid b,a\mid -b,-a\mid -b,|a|\mid|b|$; 反之亦然。
4. 若 $m\neq 0$，则 $a\mid b$ 的充分必要条件是 $ma\mid mb$
5. 若 $a\mid b$，$b\mid a$，则 $a=\pm b$
6. 若 $a,b\in\mathbb{N}_+$，$a\mid b$，则 $a\leq b$
7. 若 a 是 b 的真约数，则 $1<|a|<|b|$

♠

以上几道整除的性质都是非常显然的，这里的证明作为练习交给感兴趣的读者练练手，接下来我们来学习几个看似很简单，其实重要单的小定理叭!

引理 1.1. 整除的传递性

$$c\mid b,b\mid a\Rightarrow c\mid a$$

❀

证明 其实不难发现，这句话想表达的意思是若 b 是 c 的倍数，a 是 b 的倍数，则 a 是 c 的倍数。

由定义 1.2，可知道存在两个整数 a_1，b_1，使得

$$a=a_1b,b=b_1c$$

成立，因此

$$a=(a_1b_1)c$$

但是 a_1b_1 是一个整数，故 $c\mid a$

此即得证。

引理 1.2. 倍数连加可整除性

若 $a_1,a_2,\cdots,a_n$ 都是 m 的倍数，$q_1,q_2,\cdots q_n$ 是任意 n 个整数，则 $q_1a_1+q_2a_2+\cdots+q_na_n$ 是 m 的倍数。❀

这个性质证明作为习题供读者练习。

从这里，我们就能够将整除的情形进行了初步的讨论，但是在米娜桑小学二年级的时候就学过了余数，就是未必能整除的一般情形下，那我们该如何表示呐？我就有了接下来这个基本且十分重要的定理。

定理 1.1 (带余除法)

若 a,b 是任意两个整数，其中 $b>0$，则存在两个整数 q 和 r，使得

$$a=bq+r \quad 0\leq r<b$$

成立，而且 q 和 r 是唯一的。 ♡

证明 先作整数序列

$$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots$$

则 a 必在上述序列的某两项之间，即存在一个整数 q 使得

$$qb\leq a<(q+1)b$$

成立。令 $a-qb=r$，则 $a=bq+r$, 而 $0\leq r<b$，即存在整数 q 和 r，使得定理成立。

再证明唯一性：设 q_1,r_1 是满足式子的两个整数，则

$$a=bq_1+r_1 \quad 0\leq r_1<b$$

$$bq_1+r_1=bq+r$$

$$b(q-q_1)=r_1-1$$

$$b\,|q-q_1|=|r_1-r|$$

由于 r 和 r_1 都是小于 b 的正数，所以上式右边是小于 b 的。如果 $q\neq q_1$ 则上式子左边 $\geq b$，显然是不可能的呀，所以捏，$q=q_1$,$r=r_1$

此即得证。

笔记

1. 每两个整数之间都有带余除法
2. 余数具有唯一性
3. 整除是带余除法的特殊形式（推广）
4. 余数必须为正数

整数中有许多的性质，都可以由带余除法引导出来的，我们可以说初等数论就是建立在带余除法性质上的。

定义 1.3

带余除法定理中，q 叫做 a 被 b 除所得到的不完全商，r 叫做 a 被 b 除所得到的余数。 ♣

为了更好的了解这个例子，我们举例说明一下：设 $b=15$，则当 $a=255$ 时，

$$a=17b+0,r=0<15,q=17$$

当 $a=417$ 时，

$$a=27b+12,0<r=12<15,q=27$$

当 $a=-81$ 时，

$$a=-6b+9,0<r=9,q=-6$$

在学完带余除法后，我们赶快来证明两道有意思的小结论练练手来结束整除这一小节吧！

命题 1.2

若 $n \in \mathbb{Z}, k \in \mathbb{N}_+$，则

$$\frac{n(n-1)\cdots(n-k+1)}{k!}$$

的值是整数。

证明 当 $n=0$ 时，$n(n-1)\cdots(n-k+1)=0$，$k! \mid 0$ 结论成立。

当 $n>0$ 时候，如果 $n \geq k$，则

$$\frac{n(n-1)\cdots(n-k+1)}{k!} = C_n^k$$

组合数一定是整数，结论成立。

当 $0<n<k$ 时，在 $n, n-1, \cdots, n-k+1$ 这 k 个数中一定有一个数是 0，即

$$n(n-1)\cdots(n-k+1)=0 \quad k! \mid 0$$

结论成立。

当 $n<0$ 时，令 $n=-n', -n'>0$, 则

$$\begin{aligned}&\frac{n(n-1)\cdots(n-k+1)}{k!}\\ =&\frac{-n'(-n'-1)\cdots(-n'-k+1)}{k!}\\ =&(-1)^k\frac{n'(n'+1)\cdots(n'+k-1)}{k!}\end{aligned}$$

又因为

$$n'+k-1 \geq k$$

所以

$$\frac{n'(n'+1)\cdots(n'+k-1)}{k!} = C_{n'+k-1}^k$$

又因为 $C_{n'+k-1}^k$ 是组合数，所以 $(-1)^k C_{n'+k-1}^k$ 是整数。

此即得证。

笔记 k 个连续整数的积一定能被 $k!$ 整除。

命题 1.3

如果存在 $a, b \in \mathbb{Z}$，且 $a \neq b$，当 $n \in \mathbb{N}_+$ 时

$$(a-b) \mid (a^n - b^n)$$

证明 如果 $b=0$, 那么 $a \neq b$，则 $b \neq 0$，$a \mid a^n$, 故结论成立（同样 $a=0$ 结论仍然成立）。

我们要讨论的是 $a, b \neq 0$ 的情况，我们可以先构造下列等比数列：

$$b^{n-1} + ab^{n-2} + \cdots + a^{n-2}b + a^{n-1} = \frac{a^n - b^n}{a-b}$$

即

$$a^n - b^n = (a-b)(b^{n-1} + ab^{n-2} + \cdots + a^{n-2}b + a^{n-1})$$

又因为 $a-b \neq 0$，$a^{n-1} + \cdots + b^{n-1}$ 是整数，所以

$$(a-b) \mid (a^n - b^n)$$

此即得证。

1.2 奇数与偶数以及数位整除特征

在大家小时候，第一次数学发现就是和老师一起做数学游戏让孩子们学习理解奇偶数和了解个位、十位、百位 $\cdots$ 等数位，既培养了孩子的数感，又能发现生活中存在的奇偶数现象，那作为初等数论的第二次数学启蒙，在了解带余除法后顺带让曾经为孩子的读者们再进一步从数论的角度了解一些奇偶数及数位规律，还是有必要的。

定义 1.4 (奇数与偶数)

如果 $2 \mid a$，则称 a 为偶数，常用 $2k(k \in \mathbb{Z})$ 表示，大于零的偶数也叫双数。

如果 $2 \nmid a$，则称 a 为偶数，常用 $2k+1/2k-1(k \in \mathbb{Z})$ 表示，大于零的奇数也叫单数。

♣

那么我们在定义奇数和偶数之后，进一步地学习一下有关奇数和偶数的性质。

命题 1.4 (奇数与偶数的性质)

1. 任意几个偶数的和还是偶数。
2. 任意一个整数与偶数的积是偶数，特别地，n 个偶数积是 2^n 的倍数 $(n \in \mathbb{N}_+)$。
3. 双数个奇数的和是偶数，单数个奇数的和是奇数，任意 n 个奇数的积还是奇数。
4. 奇数与偶数的和是奇数。
5. 任一奇数与任意偶数不相等。

♠

以上的几条性质都可以通过奇数与偶数的定义和相关运算得到证明。

在进一步了解奇数与偶数之后，我们要接着学习数位的整除特征，至于什么是数位，可以看前面的定义 1.1 的第四条。

对于数位整除特征，可能很多人从小学就发现了，比如说 3 能整除的数字就是所有数位加在一起能被 3 整除之类的，我们接下来就严格定义一下，数 b 整除数 a 的特征就是指 $b \mid a$ 的充分必要条件。

定理 1.2

若 $A=\sum_{i=0}^{n} a_i 10^i$，则

1. 2(或 5) 整除 A 的特征是 2 (或 5) 整除 a_0
2. 4(或 25) 整除 A 的特征是 4(或 25) 整除 $\overline{a_1 a_0}$
3. 8(或 125) 整除 A 的特征是 8(或 125) 整除 $\overline{a_2 a_1 a_0}$

♡

以上这三个定理想必大家都是一眼瞪、立即推的，如果你感兴趣，可以自己证明一下。那么我们着重讲解以下两个常用的定理。

定理 1.3

若 $A=\sum_{i=0}^{n} a_i 10^i$，则 3(或 9) 整除 A 的特征是 3(或 9) 整除 $\sum_{i=0}^{n} a_i$

♡

证明

$$\begin{aligned}A=&\sum_{i=0}^{n}a_i10^i\\=&a_n10^n+a_{n-1}10^{n-1}+\cdots+a_210^2+a_110+a_0\\=&a_n\times(\underbrace{99\cdots99}_{n个9}+1)+a_{n-1}\times(\underbrace{99\cdots99}_{n-1个9}+1)+\cdots\\&+a_2\times(99+1)+a_1\times(9+1)+a_0\\=&9\times(\underbrace{11\cdots11}_{n个1}a_n+\underbrace{11\cdots11}_{n-1个1}a_{n-1}+\cdots+11a_2+a_1)+\sum_{i=0}^{n}a_i\end{aligned}$$

充分性此即得证，必要性略。

定理 1.4

11 | A 的特征是 A 的奇数位数字和偶数位数字和的差能被 11 整除。 ♡

证明 设 $A=\sum_{i=0}^{n}a_i10^i$

$$\begin{aligned}A=&a_0+a_1\times10+a_2\times10^2+a_3\times10^3+\cdots+a_n\times10^n\\=&a_0+a_1\times(11-1)+a_2\times(11-1)^2+a_3\times(11-1)^3+\cdots+a_n\times(11-1)^n\\=&a_0+11a_1-a_1+11\times(11-2)a_2+a_2+11\times(11^2-3\times11+3)a_3-a_3\\&+\cdots+11a_n\times(11^{n-1}-C_n^1\times11^{n-2}+\cdots+C_n^{n-1}(-1)^{n-1})+(-1)^na_n\\=&11\times[a_1+(11-2)a_2+(11^2-3\times11+3)a_3+\cdots+(11^{n-1}-C_n^1\times11^{n-2}+\\&\cdots+(-1)^{n-1}C_n^{n-1})a_0]+(a_0-a_1+a_2-a_3+\cdots+(-1)^na_n)\end{aligned}$$

充分性证明：

$$\begin{aligned}&11\mid11\times[a_1+(11-1)a_2+\cdots+(11^{n-1}+\cdots+(-1)^{n-1}C_n^{n-1})a_0]\\&11\mid(a_0-a_1+a_2-a_3+\cdots+(-1)^na_n)\\&11\mid A\end{aligned}$$

必要性证明：

$$\begin{aligned}&11\mid11\times[a_1+\cdots(11^{n-1}+\cdots+(-1)^{n-1}C_n^{n-1})a_n]\\&11\mid A\\&11\mid(a_0-a_1+a_2-a_3+\cdots+(-1)^na_n)\end{aligned}$$

此即得证。

1.3 素数与合数

第一节我们已经提到了：用不等于零的整数去除整数未必能整除。我们在小学学习的时候已经知道这一个事实啦。当时为了解决余数的问题，我们引进了分数进一步的学习数的理论。但是对其中重要的概念——最大公因数和最小公倍数，缺没有进行系统的讨论，但是为了研究最大公因数和最小公倍数，我们又必须要了解素数与合数，并且更深一步的从初等数论角度出发再一次剖析他，为此我们单独拿出一节细致地讲解素数与合数相关的性质与定理，为的是更进一步探讨初等数论。

在正整数里，1 的正因数就只有它本身，因此在整数中 1 占有特殊的地位。任一个大于 1 的整数都至少有 2 个正因数，即 1 和它本身，我们把这些数再加以分类，就得到了下面的定义

定义 1.5

一个大于 1 的整数，如果它的正因数只有 1 和它本身，就叫做素数；否则就叫做合数。 ♣

素数在研究整数的过程中占有一个非常非常重要的地位，这里给大家一个悬念，重要的内容我们放到本章的第六小节。在此之前，我们先证明一些作为铺垫的小定理，比如

定理 1.5

设 a 是任一大于 1 的整数，则 a 的除 1 外最小正因数 q 是一素数，并且当 a 是合数时，$q \leq \sqrt{a}$ ♡

证明 假设 q 不是素数，由定义，q 除 1 及本身外还有一正因数 q_1，因而 $1 < q_1 < q$。但 $q \mid a$，所以 $q_1 \mid a$，这与 q 是 a 的除 1 外的最小正因数矛盾，故 q 是素数。

当 a 是合数时，则 $a = a_1 q$，且 $a_1 > 1$，否则 a 是素数。由于 q 是 a 的除 1 外的最小正因数，所以 $q \leq a_1$，$q^2 \leq q a_1 = a$，故 $q \leq \sqrt{a}$

此即得证。

定理 1.6

设 p 是任一大于 1 的整数，如果所有不大于 $\sqrt{p}$ 的素数都不能整除 p，则 p 是素数。 ♡

证明 先证大于 1 且不大于 $\sqrt{p}$ 的所有整数都不能整除 p，则 p 是素数。

如果 p 是合数，一定有 b，$c \in \mathbb{Z}$，b，$c > 1$，b，$c < p$，使得 $p = bc$，由于大于 1 而不大于 $\sqrt{p}$ 的所有整数都不能整除 p，所以 $b > \sqrt{p}$，$c > \sqrt{p}$，则 $p = bc > \sqrt{p} \cdot \sqrt{p} = p$，矛盾。

故 p 是质数。

再用大于 1 且不大于 $\sqrt{p}$ 的质数试除即可

因为大于 1 且不大于 $\sqrt{p}$ 的合数一定被某一个小于 $\sqrt{p}$ 的质数整除。

此即得证。

定理 1.6 给出了一种寻找素数的有效方法，例如，为了求出不超过 100(或任给的正整数 n) 的所有素数，只要把 1 及不超过 100(或 n) 的合数全都删去即可。我们可以用这种方法来求出不超过 100 的素数。具体做法见下表

推论 1.1. 厄拉多赛 (Eratosthenes) 筛法

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

❀

例题 1.2 判断 359 是否是素数

解 因为 $18 < \sqrt{359} < 19$，不大于 $\sqrt{359}$ 的所有素数依次为 2，3，5，7，11，13，17。经过试除上述 7 个素数均不能整除 359。故 359 是素数。

这种方法我们也叫做试除法，关于试除法还有着许多其他的例子，这里就不一一例举了。

1.4 最大公因数与 Eucild 辗转相除法

有了素数与合数的定义，再加上带余除法的帮助，我们就可以着手研究整数的最大公因数的存在问题及其实际求法，在研究过程中，我们要用到由带余除法导出的基本而重要的 Eucild 辗转相除法，为此我们先引进一些相关的定义，来回顾一下小学学的知识有哪些有趣的深入探究。

定义 1.6

设 $a_1, a_2, \cdots, a_n$ 是 $n(n \geq 2)$ 个不全为零的整数。若整数 d 是它们之中每一个的因数，那么 d 就叫做 $a_1, a_2, \cdots, a_n$ 的一个公因数。

整数 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个叫做最大公因数，记作 $gcd(a_1, a_2, \cdots, a_n)$

若 $gcd(a_1, a_2, \cdots, a_n) = 1$，我们说 $a_1, a_2, \cdots, a_n$ 互素，若 $a_1, a_2, \cdots, a_n$ 中每两个整数互素，我们就说它们两两互素。

由上述定义我们可以立即得到下面两个结论

推论 1.2

1. 若 $b \neq 0$，则 $gcd(0, b) = |b|$
2. $gcd(a_1, a_2, \cdots, a_n) = gcd(|a_1|, |a_2|, \cdots, |a_n|)$

由于有上面两个结论，今后我们只讨论正整数的公约数问题。

命题 1.5

若 $a = bq + c(a, b \in \mathbb{Z})$，则 $gcd(a, b) = gcd(b, c)$

证明 设 $d \mid a$，$d \mid b$，则 $d \mid bq$，因为 $c = a - bq$，所以 $d \mid c$，故 $gcd(a, b) = gcd(b, c)$

此即得证。

接下来是重头戏了，我们要知道如何求两个正整数的最大因数，借此推出最大公因数的性质，还是解一次不定方程的基本工具。

定理 1.7 (Eucild 辗转相除法)

设 a, b 是任意两个正整数，且 $b \nmid a$，由带余除法，我们可以有下列等式：

$$
\begin{aligned}
a &= bq_1 + r_1 \quad 0 < r_1 < b \\
b &= r_1 q_1 + r_2 \quad 0 < r_2 < r_1 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + r_{n+1} \quad r_{n+1} = 0
\end{aligned}
$$

注 这是因为每进行一次带余除法，余数至少减 1，所以经有限次带余除法，总会得到一个余数是零的等式，一定存在一个大于零的整数 n，使得 $r_{n+1} = 0$

推论 1.3

1. 若 a, b 是任意两个整数，则 $gcd(a, b)$ 就是 Eucild 辗转相除法中最后一个不等于零的余数，即 $(a, b) = r_n$
2. a, b 的公因数与 $gcd(a, b)$ 的因数相同

这两个推论的证明交给读者。

我们在使用 Eucild 辗转相除法的同时可以得到余数 r_n 和 a、b 满足的关系式:

推论 1.4

$$Q_i a - P_i b = (-1)^{i-1} r_i$$

而 P_i，Q_i 由下面递推式确定:

$$\begin{cases} P_i = q_i P_{i-1} + P_{i-2} \\ \qquad\qquad\qquad\qquad (i = 2, \cdots, k) \\ Q_i = q_i Q_{i-1} + Q_{i-2} \end{cases}$$

这里 $P_0 = 1, P_1 = q_1, Q_0 = 0$，$Q_1 = 1$

证明 当 $i = 2$ 时，由 Eucild 辗转相除过程可得

$$\begin{aligned} -r_2 =& r_1 q_2 - b \\ =& (a - bq_1)q_2 - b \\ =& aq_2 - (q_1 q_2 + 1)b \\ P_2 =& q_1 q_2 + 1 = q_2 P_1 + P_0 \\ Q_2 =& q_2 = q_2 Q_1 + Q_0 \end{aligned}$$

故关系式成立，即 $i = 2$ 时结论成立。

假设该关系式对不大于 $k'(k' \geq 2)$ 的正整数成立，则

$$\begin{aligned} (-1)^{k'} r_{k'+1} =& (-1)^{k'} (r_{k'-1} - r_{k'} q_{k'+1}) \\ =& (Q_{k'-1} a - P_{k'-1} b) + (Q_{k'} - P_{k'} b) q_{k'+1} \\ =& (q_{k'+1} Q_{k'} + Q_{k'-1}) a - (q_{k'+1} P_{k'} + P_{k'-1}) b \\ =& Q_{k'+1} a - P_{k'+1} b \end{aligned}$$

故该关系式对于一切 $k' \leq k$ 的正整数成立。

此即得证。

推论 1.5

若 $a, b \in \mathbb{N}_+$，则一定存在整数 s，t，使得 $as + bt = gcd(a, b)$，同理，对 $a_1, a_2, \cdots, a_k \in \mathbb{N}_+$，一定存在整数 $m_1, m_2, \cdots, m_k$ 使得

$$\sum_{i=1}^{k} a_i m_i = gcd\left(a_1, a_2, \cdots, a_k\right)$$

例题 1.3 用辗转相除法求 $gcd(198, 252)$

解

$$\begin{aligned} 252 &= 198 \times 1 + 54 \\ 198 &= 54 \times 3 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 \end{aligned}$$

所以 $gcd(252, 198) = gcd(3, 18) = 18$

我们接下来再来证明俩最大公因数之间的性质

定理 1.8

设 a,b 是任意两个不全为零的整数，

1. 若 m 是任一正整数，则
$$gcd(am,bm)=gcd(a,b)m$$
2. 若 δ 是 a,b 的任一公因数，则 $gcd\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{gcd(a,b)}{|\delta|}$，特别 $gcd\left(\frac{a}{gcd(a,b)},\frac{b}{gcd(a,b)}\right)=1$

♡

证明留给读者作为练习

1.5 最小公倍数和整除的进一步性质

在上一个小节里我们已经探讨了 Eucild 辗转相除法在研究最大公因数的过程中的重要性，我们要在研究 Euclid 辗转相除法中 r_n 与 a,b 的关系，探讨最小公倍数的一些问题和了解更多的整除重要性质。

我们先继续来发现一些得以应用的定理

定理 1.9

若 a,b,c 是三个整数，且 $gcd(a,c)=1$，则

1. ab，c 与 b,c 有相同的公因数
2. $gcd(ab,c)=gcd(b,c)$

上面假定了 b,c 至少有一个不为零

♡

证明

1. 可知，存在两个整数 s,t 满足等式
$$as+ct=1$$
两边乘以 b，即得
$$(ab)s+c(bt)=b$$
设 d 是 ab 与 c 的任一公因数，且 $d\mid b$，因而 d 是 b,c 的一个公因数。反之 b,c 的任一公因数显然是 ab,c 的一个公因数。
2. 因为 b,c 不全为零，故 $gcd(b,c)$ 是存在的，因而 $gcd(ab,c)$ 存在，且
$$gcd(ab,c)=gcd(b,c)$$

此即得证。

定理 1.10

设 $a_1,a_2,\cdots,a_n$ 及 $b_1,b_2,\cdots,b_m$ 是任意两组整数。若前一组中任一整数与后一组任一整数互素，则 $a_1a_2\cdots a_n$ 与 $b_1b_2\cdots b_m$ 互素。

♡

证明 我们知道
$$gcd(a_1a_2\cdots a_n,b_j)=gcd(a_2a_3\cdots a_n,b_j)=\cdots=gcd(a_n,b_j)=1\quad j=1,2,\cdots m$$
又
$$gcd(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=gcd(a_1a_2\cdots,b_2b_3\cdots b_m)=\cdots=gcd(a_1a_2\cdots a_n,b_m)=1$$
此即得证。

下面我们要用上述得到的定理和之前学过的一定理与推论来研究公倍数和最小公倍数。

定义 1.7

设 $a_1, a_2, \cdots, a_n$ 是 $n(n \geq 2)$ 个不全为零的整数。若整数 d 是这 n 个数的倍数，那么 d 就叫做这 n 个数的一个公倍数。

整数 $a_1, a_2, \cdots, a_n$ 的公倍数中最小的一个叫做最小公倍数，记作 $lcm(a_1, a_2, \cdots, a_n)$

由于任何正数都不是 0 的倍数，故讨论整数的最小公倍数时，一概假定这些整数都不是零。

定理 1.11

$$lcm(a_1, a_2, \cdots, a_n) = lcm(|a_1|, |a_2|, \cdots, |a_n|)$$

和最大公因数的情形一样，我们来研究一下两个整数的最小公倍数。

定理 1.12

设 a, b 是任意两个正整数，则

1. a, b 是的所有公倍数就是 $lcm(a, b)$ 的所有倍数
2. a, b 的最小公倍数等于以它们的最大公因数除它们的乘积所得的商，即 $lcm(a, b) = \dfrac{ab}{gcd(a, b)}$. 特别的，若 $gcd(a, b) = 1$，则 $lcm(a, b) = ab$

定理 1.11 和定理 1.12 的证明就交给读者了。

1.6 算术基本定理与除数函数

在前面，我们通过整除发现在整数里，1 的正因数只有它本身，在这个特殊地位外的所有整数都至少拥有两个正因数，因此我们定义了素数与合数，接下来我们要讲的便是初等数论中应用最广发、最重要和最基本的定理–算术基本定理。

我们在学过最大公因数和最小公倍数之后，结合素数可以得到一个小结论

命题 1.6

若 p 是一素数，a 是任一整数，则

1. $p \mid a$ 或者 $gcd(a, p) = 1$
2. 若将 a 视作 a_i（其中 $i = 1, 2, \cdots, a_n$）。若 $p \mid \prod_{i=1}^{n} a_i$，则 $p \mid a_1, p \mid a_2, \cdots, p \mid a_n$ 中至少有一个成立。

既然上式成立，那么我们可以大胆猜测一下是否可以将所有正整数都分解，表达成一种形式，这样方便我们可以进一步谈讨整数呐，答案是肯定的。因为我们有

引理 1.3

设 a 是大于 1 的整数，则必有 $a = \prod_{i=1}^{n} p_i$（p_i 是素数），且在不计次序的意义下，$a = \prod_{i=1}^{n} p_i$ 这一表达方式是唯一的。

证明 设 a 是大于 1 的素数，则必有 $a = \prod_{i=1}^{n} p_i$，显然成立。

若 a 是合数，可知 a 必有素数约数 p_1，使 $a = p_1 a_1$，$1 < a_1 < a$

若 a_1 是素数，定理成立。若 a_1 是合数，同理 a_1 有素数约数 p_2，使得 $a_1 = p_2 a_2$，$1 < a_2 < a_1$，故 $a = p_1 p_2 a_2$，$1 < a_2 < a_1 < a$

这样继续下去，可以得到一递减的正整数数列：$a > a_1 > a_2 > \cdots > 1$

上述数列显然只能有有限项，故最后一定出现一个素数 a_{n-1}，使得 $a_{n-2} = p_{n-1}a_{n-1}$，令 $a_{n-1} = p_n$，则有 $a = \prod_{i=1}^{n} p_i$，故存在性得证。

设除了表达式 $a = \prod_{i=1}^{n} p_i$ 成立，还有表达式 $a = \prod_{i=1}^{m} q_i$ 成立（q_i 也全是素数），则

$$\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$$

由此可推出 $p_1 \mid \prod_{i=1}^{m} q_i$，故可知 p_1 必整除某一个 $q_t (1 \le t \le m)$，不妨设 $p_1 \mid q_1$，但是 p_1, q_1 都是素数，所以 $p_1 = q_1$，消去 p_1, q_2，则表达式可以变为

$$\prod_{i=2}^{n} p_i = \prod_{i=2}^{m} q_i$$

同理，$p_2 = q_2$，上述表达式又可以写成

$$\prod_{i=3}^{n} p_i = \prod_{i=3}^{m} q_i$$

如此进行下去，直到表达式有一边的乘积的因数全部约去只剩下 1 为止，这时表达式的另一边乘积的因数也应全部约去，否则，不妨设表达式右边乘积的因数已全部约去，而左边乘积的因数未被全部约去，即 $n > m$，于是有 $p_{m+1}p_{m+2}\cdots p_n = 1$，又因为 $p_{m+1}, p_{m+2}, \cdots, p_n$ 全是素数，所以 $p_{m+1}p_{m+2}\cdots p_n = 1$ 显然不可能，这说明了表达式两边是某些同样的素数之乘积，且同一个素数在式子两边出现的次数也是一样的，故不计次序，表达式 $a = \prod_{i=1}^{n} p_i$ 是唯一的。

此即得证。

我们把 $a = \prod_{i=1}^{n} p_i$ 中相同的质数合并一下，就得到了

定理 1.13 (算术基本定理)

$$a = \prod_{i=1}^{n} p_i = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$$

♡

这便是初等数论中最重要最基本的定理了，我们也可以叫他唯一分解定理，我们用这个定理把一个合数写成素因数连乘积的形式，称为分解素因数，则 $\prod_{i=1}^{n} {p_i}^{a_i}$ 被成为标准分解式。

例题 1.4 求 9828 的标准分解式

解

$$\begin{aligned} 9828 &= 9 \times 1092 \\ &= 3^2 \times 3 \times 364 \\ &= 3^3 \times 4 \times 91 \\ &= 2^2 \times 3^3 \times 7 \times 13 \end{aligned}$$

同理用短除法也可以写出来。

我们在知道了算术基本定理，我们就可以知道中学教科书中求最大公因数和最小公倍数的根据

推论 1.6

设 a,b 是任意两个正整数，且

$$a = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$$

$$b = {p_1}^{\beta_1}{p_2}^{\beta_2}\cdots{p_k}^{\beta_k}$$

则

$$gcd(a,b) = {p_1}^{\gamma_1}{p_2}^{\gamma_2}\cdots{p_k}^{\gamma_k} \quad lcm(a,b) = {p_1}^{\delta_1}{p_2}^{\delta_2}\cdots{p_k}^{\delta_k}$$

其中，$\gamma_i = min(\alpha_i,\beta_i), \delta_i = max(\alpha_i,\beta_i)$

我们在掌握了算术基本定理后，还有一个除数函数我们没有了解，接下来我们就要通过除数函数来了解一下自然数的正约数的个位及所有正约数的和。

定义 1.8

$\tau(a)$ 表示自然数 a 所有正约数的个数（通常也被称为除数函数）
$\sigma(a)$ 表示自然数 a 的所有正约数的和（通常也被称为除数和函数）
$\sigma_1(a)$ 表示自然数 a 的一切正约数的乘积（通常也被称为除数积函数）

例题 1.5 $\tau(2)=2,\tau(4)=3,\sigma(2)=1+2=3,\sigma(4)=1+2+4=7$

定理 1.14

若 $a=\prod_{i=1}^{n}{p_i}^{a_i}$，则

$$\tau(a)=\prod_{i=1}^{n}(a_i+1)$$

这个定理可以让我们便捷的算出一个自然数的正约数个数，并且这个定理告诉我们，一个大于 1 的正整数的正约数的个数等于它的标准分解式中每个素因数的指数加 1 的连乘积。具体证明过程交给有兴趣的读者。

例题 1.6 $\tau(180)=?$

解

$$180 = 2^2\times 3^2\times 5$$

所以

$$\tau(180)=(2+1)(2+1)(1+1)=18$$

定理 1.15

若 $a=\prod_{i=1}^{n}{p_i}^{a_i}$，则

$$\sigma(a)=\prod_{i=1}^{n}\frac{{p_i}^{a_i+1}-1}{p_i-1}$$

同理，这个定理可以让我们便捷的算出一个自然数的正约数的和。

定理 1.16

若 $a=\prod_{i=1}^{n}{p_i}^{a_i}$，则

$$\sigma_1(a)=\sqrt{a^{\tau(a)}}$$

同理，这个定理可以让我们便捷的算出一个自然数的正约数的积。

推论 1.7

若 $gcd(a,b)=1$，则 $\tau(ab)=\tau(a)\tau(b)$

若 $gcd(a,b)=1$，则 $\sigma(ab)=\sigma(a)\sigma(b)$

至此，我们就基本上对除数函数有个基本的认识了，有兴趣的读者可以将本节的定理都证明一遍。

1.7 高斯函数在数论中的运用

高斯函数在大家学习高数或者数分的时候便接触过了，不管大家有没有印象我们都要再提一遍，因为高斯函数是可以很方便我们求出 $n!$ 的标准分解式的，我们上一节课讨论了把任意一个正整数分解成标准分解式的问题，这节课我们就从高斯函数出发来讨论 $n!$ 的标准分解式。

定义 1.9 (高斯函数)

函数 $[x]$ 和 $\{x\}$ 是对于一切实数都有定义的函数，函数 $[x]$ 的值等于不大于 x 的最大整数，也就是 x 的整数部分。函数 $\{x\}$ 表示的是 $x-[x]$，也就是 x 的小数部分。

例题 1.7 $[\pi]=3,[e]=2,\left\{-\frac{3}{5}\right\}=\frac{2}{5},\left\{\sqrt{2}\right\}=0.414\cdots$

我们由定义，可以得到一些简单的性质

命题 1.7

1. $x=[x]+\{x\}$
2. $[x]\le x<[x]+1, x-1<[x]\le x, 0\le\{x\}<1$
3. $[n+x]=n+[x]$,n 是整数
4. $[x]+[y]\le[x+y],\{x\}+\{y\}\le\{x+y\}$
5. $[-x]=\begin{cases}-[x]-1 & x\notin\mathbb{Z}\\ -[x] & x\in\mathbb{Z}\end{cases}\quad \{x\}=\begin{cases}1-\{x\} & x\notin\mathbb{Z}\\ -\{x\}=0 & x\in\mathbb{Z}\end{cases}$
6. 若 a,b 是两个整数，$b>0$，则
$$a=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\},\quad 0\le b\left\{\frac{a}{b}\right\}\le b-1$$
7. 若 a,b 是任意两个正整数，则不大于 a 而为 b 的倍数的正整数个数是 $\left[\frac{a}{b}\right]$
8. 对任意非零整数 n 有
$$\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right]$$

我们了解了这些性质后，接下来就要用这些性质去研究他的用法了。首先映入眼帘的就是

定理 1.17

若 $x\in\mathbb{R}^+,n\in\mathbb{N}_+$，则 1 到 x 的整数中，n 的倍数有 $\left[\frac{x}{n}\right]$ 个

证明 由于 $\left[\frac{x}{n}\right]\le\frac{x}{n}<\left[\frac{x}{n}\right]+1,\quad n\in\mathbb{N}_+$

所以 $n\left[\frac{x}{n}\right]\le x<n\left(\left[\frac{x}{n}\right]+1\right)$

于是从 1 到 x 的整数中，能被 n 整除的数只有 $n,2n,\cdots,\left[\frac{x}{n}\right]n$，总共有 $\left[\frac{x}{n}\right]$ 个

此即得证。

由这个定理，我们还可以得到一个推论

推论 1.8

若 $a,b,n\in\mathbb{N}_+$，则

$$\left[\frac{n}{ab}\right]=\left[\frac{\left[\frac{n}{a}\right]}{b}\right]$$

定理 1.18

在 $n!$ 的标准分解式中，素因数 $p(p\le n)$ 的指数为

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]$$

注 若 $p^s>n$，则 $\left[\frac{n}{p^s}\right]=0$，故上式只有有限项不为零，因而有意义。

证明 设想把 $2,3,\cdots,n$ 都分解成标准分解式，则由算术基本定理，h 就是这 $n-1$ 个分解式中 p 的指数之和，设其中 p 的指数是 r 的有 n_r 个 $(n\ge 1)$，则

$$\begin{aligned}h=&n_1+2n_2+3n_3+\cdots\\=&n_1+n_2+n_3+\cdots+\\&n_2+n_3+\cdots+\\&n_3+\cdots+\\&\cdots\\=&N_1+N_2+N_3+\cdots\end{aligned}$$

其中 $N_r=n_r+n_{r+1}+\cdots$ 恰好是 $2,3,\cdots,n$ 这 $n-1$ 个数中能被 p^r 除尽的个数，但是因为命题 1.7 中的第六条，$N_r=\left[\frac{n}{p_r}\right]$，故

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]$$

此即得证。

推论 1.9

$$n!=\prod_{p\le n}p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$$

注 其中 $\prod_{p\le n}$ 表示展布在不超过 n 的一切素数上的积式。

推论 1.10. 贾宪数

$$\frac{n!}{k!(n-k)!}\text{是整数}(0<k<n)$$

注 设 k,n 是正整数，且 $0<k\le n$，则上述贾宪数是从 n 个元素的集合中取 k 个元素的组合数，所以它是整数，并不需要单独证明。而且有一个很类似的命题我们之前学过，是命题 1.2，读者可以将这俩放在一起看看。

我们来看两道例题

例题 1.8 试求 $8!$ 标准分解式中素因子 $2,3,5$ 的指数。

解

$$\begin{aligned} 8! &= 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8 \\ &= 2^1\times 3^1\times 2^2\times 5^1\times 3^1\times 7^1\times 2^3 \\ &= 2^7\times 3^2\times 5\times 7 \end{aligned}$$

所以 $h_2=7, h_3=2, h_5=1$

例题 1.9 计算 10! 的标准分解式

解

$$h_2=\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right]+\left[\frac{10}{2^4}\right]=5+2+1+0=8$$
$$h_3=\left[\frac{10}{3}\right]+\left[\frac{10}{3^2}\right]+\left[\frac{10}{3^3}\right]=3+1+0=4$$
$$h_5=\left[\frac{10}{5}\right]+\left[\frac{10}{5^2}\right]=2+0=2$$
$$h_7=\left[\frac{10}{7}\right]+\left[\frac{10}{7^2}\right]=1+0=1$$

所以 10! 的标准分解式为 $2^8\times 3^4\times 5^2\times 7$

定理 1.19 (Hermite 恒等式)

$$[x]+\left[x+\frac{1}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]$$

♡

这个有趣的恒等式交给感兴趣的读者证明。

第 2 章 同余

在第一章节，我们详细地讲解了整除的性质，这一章我们便要把带余除法中的余数拿出来单独讨论，试想一下我们日常生活中常常用到的数字不一定都是整数，比如我问你答，现在是几点钟？这就是拿 24 去除某个宗的时数所得到的余数，余数的概念给生活带来了许多便利，也极大地丰富了数学内容，我们本章要从同余的概念出发，讲解剩余系和建立一系列 Euler 函数相关的定理，并且最后在各种循环数，尤其是循环小数上进行应用。

2.1 同余的基本性质

我们从具体例子出发，比如今天星期一，再过 24 天或 31 天都是疯狂星期四，也就是从某日开始计算的总天数除以 7 他的余数都是 3，这样我们就诞生了一个数学中同余的概念。

定义 2.1 (同余)

给定一个整数 m，把它叫做模，如果用 m 去除任意两个整数 a 和 b 所得的余数相同，我们就说 a,b 对模 m 同余，记作 $a\equiv b\,(mod\,m)$。如果余数不同，我们就说 a,b 对模 m 不同余，记作 $a\not\equiv b\,(mod\,m)$。

由这个定义，我们可以立刻得到三个性质

命题 2.1

1. $a\equiv a\,(mod\,m)$
2. 若 $a\equiv b\,(mod\,m)$，则 $b\equiv a\,(mod\,m)$
3. 若 $a\equiv b\,(mod\,m)$，$b\equiv c\,(mod\,m)$，则 $a\equiv c\,(mod\,m)$

换句话说，什么叫同余呢，我们用整除的方式可以得到

定理 2.1

整数 a,b 对模 m 同余的充分必要条件是 $m\mid(a-b)$，即 $a=b+mt$，t 是整数。

证明 由带余除法，可设

$$a=mq_1+r_1,\quad 0\le r_1<m$$

$$b=mq_2+r_2,\quad 0\le r_2<m$$

若 $a\equiv b(mod\,m)$，则 $r_1=r_2$，因此，$a-b=m(q_1-q_2)$，即 $m\mid(a-b)$

若 $m\mid(a-b)$，则 $m\mid[m(q_1-q_2)+(r_1-r_2)]$，但 $|r_1-r_2|<m$，所以 $r_1-r_2=0$，$r_1=r_2$，即 $a\equiv b(mod\,m)$

此即得证。

定理 2.1 其实就是在告诉我们同余这个概念也可以定义为：$m\mid(a-b)$，则 a,b 对模 m 同余。由该定理和及整除的性质可以很容易得到下列几个类似的性质：

命题 2.2

1. 若 $a_1\equiv b_1(mod\,m),a_2\equiv b_2(mod\,m)$，则 $a_1+a_2\equiv b_1+b_2(mod\,m)$
2. 若 $a+b=\equiv c(mod\,m)$，则 $a\equiv c-b(mod\,m)$
3. 若 $a_1\equiv b_1(mod\,m),a_2\equiv b_2(mod\,m)$，则 $a_1a_2\equiv b_1b_2(mod\,m)$
4. 若 $a\equiv b(mod\,m)$，则 $a^n\equiv b^n(mod\,m)$
5. 若 $A_{\alpha_1\alpha_2\cdots\alpha_k}\equiv B_{\alpha_1\alpha_2\cdots\alpha_k}(mod\,m),x_i\equiv y_i(mod\,m),i=1,2,\cdots,k$

则

$$\sum_{\alpha_1\alpha_2\cdots\alpha_k} A_{\alpha_1\alpha_2\cdots\alpha_k}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_k^{\alpha_k} \equiv \sum_{\alpha_1\alpha_2\cdots\alpha_k} B_{\alpha_1\alpha_2\cdots\alpha_k}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_k^{\alpha_k}(mod\, m)$$

特别地，若 $a_i \equiv b_i(modm), i = 0, 1, \cdots, n$ 则

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0(mod\, m)$$

6. 若 $a \equiv b(mod\, m)$，且 $a = a_1d, b = b_1d, gcd(d, m) = 1$，则 $a_1 \equiv b_1(modm)$
7. 若 $a \equiv b(mod\, m), k > 0$，则 $ak \equiv bk(modmk)$
8. 若 $a \equiv b(mod\, m)$，d 是 a, b 及 m 的任一正公因数，则 $\frac{a}{d} \equiv \frac{b}{d}\left(mod\frac{m}{d}\right)$
9. 若 $a \equiv b(mod\, m_i), i = 1, 2, \cdots, k$，则 $a \equiv b(mod\, lcm(m_1, m_2, \cdots, m_k))$
10. 若 $a \equiv b(mod\, m), d \mid m, d > 0$，则 $a \equiv b(mod\, d)$
11. 若 $a \equiv b(mod\, m)$，则 $gcd(a, m) = (b, m)$，因而若 d 能整除 m 及 a, b 二数之一，则 d 必能整除 a, b 中的另一个。

以上这几条同余的性质都是很简单的，但是同样也非常重要，如何灵活运用是关键。接下来，我们给出所列性质在算术里的两个重要应用。

一、检查因数的一些方法。

引理 2.1

一整数能被 3（或 9）整除的充分必要的条件是它的十进位数码的和能被 3（或 9）整除。

证明 我们只需要讨论任一正整数 a，我们把 a 写成十进位的方式，即

$$a = a_n10^n + a_{n-1}10^{n-1} + \cdots + a_0, \quad 0 \le a_i < 10$$

因为 $10 \equiv 1(mod\, 3)$，由命题 2.2 中的 5 点可以得到

$$a \equiv a_n + a_{n-1} + \cdots + a_0(mod\, 3)$$

由命题 2.2 中的 11 点可以得出 $3 \mid a$ 当且仅当 $3 \mid \sum_{i=0}^{n} a_i$，同样可得 $9 \mid a$ 当且仅当 $9 \mid \sum_{i=0}^{n} a_i$

此即得证。

例题 2.1 $a = 5874192$ 能否被 $3, 9$ 整除

解 若 $a = 5874192$，则 $\sum_{i=0}^{n} a_i = 5 + 8 + 7 = 4 + 1 + 9 + 2 = 36$，故 a 能被 $3, 9$ 整除。

引理 2.2

设正整数

$$a = a_n1000^n + a_{n-1}1000^{n-1} + \cdots + a_0 \quad 0 \le a_i < 1000$$

则 7（或 11，或 13) 整除 a 的充分必要条件是 7（或 11，或 13) 整除

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = \sum_{i=0}^{n}(-1)^i a_i$$

证明 因为 1000 与 -1 对模 7（或 11，或 13）同余，故可知 a 与 $\sum_{i=0}^{n}(-1)^i a_i$ 对 7（或 11，或 13）同余。由性质可知 7（或 11，或 13）整除 a 当且仅当 7（或 11，或 13）整除 $\sum_{i=0}^{n}(-1)^i a_i$

此即得证。

例题 2.2 $a=637693$ 能否被 $7,11,13$ 整除

解 若 $a=637693$，则 $a=637\cdot 1000+693$ $\sum_{i=0}^{n}(-1)^i a_i=693-637=56$，能被 7 整除而不能被 11 与 13 整除，故由引理可得 7 是 a 的因数，但 $11,13$ 不是 a 的因数。

二、弃九法（演算整数计算结果的方法）

我们在讲弃九法前，先来看一个引理

引理 2.3

设 $\overline{abcde}$ 那么

1. 若 $b=d=9$，则 $\overline{abcde}\equiv a+c+e(mod\,9)$
2. 若 $b+d=9$，则 $\overline{abcde}\equiv a+c+e(mod\,9)$

特别地，若第 1 点与第 2 点的条件满足，则 $9\mid\overline{abcde}$ 当且仅当 $9\mid(a+c+e)$

例题 2.3 计算 $a=28997,b=39459,c=114514,d=1145236415$ 被 9 除得的余数

解

1. 我们先看第一个，28997 如果用带余除法去除，那真是比狗还累，有什么用啊？非常难求。不如我们这个杀招，先划掉 9，那就是 28997。我们不难发现，$2+7=9$ 又可以划掉了，所以 28997，只剩下了 8，故 $a\equiv 8(mod\,9)$
2. 同上，$b=39459$，所以 $b\equiv 3(mod\,9)$
3. 同上，$c=114514$，且 $1+1+1+4=7$，故 $c\equiv 7(mod\,9)$
4. 同上，$d=1145236415$，且 $1+1+2+1=5$，所以 $d\equiv 5(mod\,9)$

总之，我们只要划掉所有的 9 和一些加起来是 9 的数，剩下的加起来就是被 9 除得的余数了。有了这个引理作为准备工作，我们可以开始讲解一下弃九法。

定理 2.2 (弃九法)

设某人计算 $a\cdot b=P$，且

$$a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0,\quad 0\le a_i<10$$

$$b+b_m10^{\cdot}+b_{m-1}10^{m-1}+\cdots+b_0,\quad 0\le b_j<10$$

$$P=c_l10^l+c_{l-1}10^{l-1}+\cdots+c_0,\quad 0\le c_k<10$$

则如果

$$\left(\sum_{i=0}^{n}a_i\right)\left(\sum_{j=0}^{m}b_j\right)\not\equiv\sum_{k=0}^{l}c_k(mod\,9)$$

那么所求得的结果是错误的。

例题 2.4 $a=28997,b=39459$，有人计算 $a\cdot b=P=1145236415$，请用弃九法验证此结果是否正确。

解 之前算过了，$a\equiv 8(mod\,9)$，$b\equiv 3(mod\,9)$，所以我们可以得出 $ab\equiv 24(mod\,9)$，$24\equiv 6(mod\,9)$，所以 $ab\equiv 6(mod9)$.

我们又知道了 $ab\equiv 5(mod\,9)$ 这就说明 $ab\not\equiv p(mod\,9)$，利用弃九法说明，$a\cdot b\neq P$

2.2 剩余类与完全剩余系

我们在上一节讲述了同余的概念，有了这个概念后一个很自然的想法就是：如果将模 m 的余数相同的所有整数放在一起作成一个集合，能够得到怎样的结果呐？这样就产生了剩余类的概念。本节的目的就是讨论剩余

类和完全剩余系以及与剩余类有关的完全剩余系的性质。

我们先有如下定理

定理 2.3

若 m 是一个给定的正整数，则全部整数可以分成 m 个集合，记作 $K_0, K_1, \cdots, K_{m-1}$，其中 $K_r (r = 0, 1, \cdots, m-1)$ 是由一切形如 $qm + r (q = 0, \pm 1, \pm 2 \cdots)$ 的整数所组成的。这些集合具有以下性质：

1. 每一整数必包含在且仅在上述的一个集合里面。
2. 两个整数同在一个集合的充分必要条件是这两个整数对模 m 同余。

♡

证明

1. 设 a 是任一整数，由辗转相除法即得

$$a = a_1 m + r_a, \quad 0 \leq r_a < m$$

故 a 在 K_{r_a} 内。又由同一定理知道 r_a 是由 a 唯一确定的，因此 a 只能在 K_{r_a} 内。

2. 设 a, b 是两个整数，并且都在 K_r 内，则

$$a = q_1 m + r, \quad b = q_2 m + r$$

故 $a \equiv b (mod\, m)$，反之若 $a \equiv b (mod\, m)$，则由同余的定义即知 a, b 同在某一 K_r 内。

此即得证。

例题 2.5 计算 $m = 2, 3, 5$ 时，所对应的 K_r

解

1. 当 $m = 2$ 时

$$K_0 = \{\cdots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \cdots\}$$

$$K_1 = \{\cdots, -7, -5, -3, -1, 1, 3, 5, 7, \cdots\}$$

2. 当 $m = 3$ 时

$$K_0 = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$

$$K_1 = \{\cdots, -5, -2, 1, 4, 7, 10, \cdots\}$$

$$K_2 = \{\cdots, -4, -1, 2, 5, 8, 11, \cdots\}$$

3. 当 $m = 5$ 时

$$K_0 = \{\cdots, -10, -5, 0, 5, 10, \cdots\}$$

$$K_1 = \{\cdots, -9, -4, 1, 6, 11, \cdots\}$$

$$K_2 = \{\cdots, -8, -3, 2, 7, 12, \cdots\}$$

$$K_3 = \{\cdots, -7, -2, 3, 8, 13, \cdots\}$$

$$K_4 = \{\cdots, -6, -1, 4, 9, 14, \cdots\}$$

定义 2.2

定理 2.3 中的 $K_0, K_1, \cdots, K_{m-1}$ 叫做模 m 的剩余类，一个剩余类中任一数叫做它同类的数的剩余。若 $a_0, a_1, \cdots, a_{m-1}$ 是 m 个整数，并且其中任何两个数都不在同一个剩余类中，则 $a_0, a_1, \cdots, a_{m-1}$ 叫做模 m 的一个完全剩余系。

♣

推论 2.1

m 个整数作成模 m 的一个完全剩余系的充分必要条件是两两对模 m 不同余。

证明就交给有兴趣的读者了。

练习 2.1

由推论我们知道

$0,1,\cdots,m-1$

$0,m+1,\cdots,am+a,\cdots,(m-1)m+(m_1)$

$0,-m+1,\cdots,(-1)^a m+a,\cdots,(-1)^{m-1}$

都是模 m 的完全剩余系。

定义 2.3

$0,1,\cdots,m-1$ 这 m 个整数叫做模 m 的最小非负完全剩余系。

当 m 是偶数时，

$$-\frac{m}{2},\cdots,-1,0,1,\cdots,\frac{m}{2}-1$$

或

$$-\frac{m}{2}+1,\cdots,-1,0,1,\cdots,\frac{m}{2}$$

叫做模 m 的绝对最小完全剩余系。

当 m 是奇数时，

$$-\frac{m-1}{2},\cdots,-1,0,1,\cdots,\frac{m-1}{2}$$

叫做模 m 的绝对最小完全剩余系。

我们学了就立马运用，来看下方例题

例题 2.6 写出当 m 等于 5 和 7 以及 m 等于 6 和 8 时的绝对最小完全剩余系，并验证你的结果。

解 当 $m=5$ 时候，$\frac{5-1}{2}=2$，且 $-1=5\times(-1)+4,-2=5\times(-1)+3$

故模 $m=5$ 的绝对最小完全剩余系等于:$\underbrace{-2,-1,0,1,2}_{5个}$

当 $m=7$ 时候，$\frac{7-1}{2}=3$，且 $-1=7\times(-1)+6,-2=7\times(-1)+5,-3=7\times(-1)+4$

故 $m=7$ 的绝对最小完全剩余系等于:$\underbrace{-3,-2,-1,0,1,2,3}_{7个}$

同理，当 $m=6$ 时候，

模 $m=6$ 的绝对最小完全剩余系等于:$\underbrace{-3,-2,-1,0,1,2}_{6个}$ 或者 $\underbrace{-2,-1,0,1,2,3}_{6个}$

当 $m=8$ 时候，

模 $m=8$ 的绝对最小完全剩余系等于:$\underbrace{-4,-3,-2,-1,0,1,2,3}_{8个}$ 或者 $\underbrace{-3,-2,-1,0,1,2,3,4}_{8个}$

定理 2.4

设 $m\in\mathbb{Z}_+,gcd(a,b)=1,b\in\mathbb{Z}$，若 x 通过模 m 的一个完全剩余系，则 $ax+b$ 也通过模 m 的完全剩余系，也就是说，若 $a_0,a_1,\cdots,a_{m-1}$ 是模 m 的完全剩余系，则 $aa_0+b,aa_1+b,\cdots,aa_{m-1}+b$ 也是模 m 的完全剩余系。

证明 由推论 2.1，只要证明 $aa_0+b,aa_1+b,\cdots,aa_{m-1}+b$ 两两不同余就够了。利用反证法。

假定 $aa_i+b\equiv aa_j+b(mod\ m),i\neq j$ 由命题 2.2 中的第 1 小点可得出 $aa_i\equiv aa_j(mod\ m)$，再由命题 2.2 中的第 6 小点以及 $gcd(a,m)=1$ 即得 $a_i\equiv a_j(mod\ m)$。这与 $a_0,a_1,\cdots,a_{m-1}$ 是完全剩余系的假设矛盾，故定理获证。

此即得证。

例题 2.7 设 $m=5,a=4,b=3$

1. 证明 x：$1,3,5,7,9$ 是模 m 的一个完全剩余系。
2. 计算由 x 确定的模 m 的完全剩余系 $ax+b$

解

1. 证明：$1=5\times0+1,3=5\times0+3,5=5\times1+0,7=5\times1+2,9=5\times1+4$，且他们与 5 两两不同余，所以 $1,3,5,7,9$ 对模 m 构成一个完全剩余系。
2. $ax+b=4x+3,x_0=1$，故 $x_1=3,x_2=5,x_3=7,x_4=9$ 时，所对应的 $ax+b$ 是 $7,15,23,31,39$，他们除以 5 所得到的余数是 $2,0,3,1,4$，且与 5 两两不同余，所以也是对 5 构成的完全剩余系。

这样的话，我们就理解了这个定理确定一个模 m 用一个完全剩余系我们可以得到很多其他的完全剩余系。

定理 2.5

若 m,n 是互素的两个正整数，而 x_1,x_2 分别通过 m,n 的完全剩余系，则 mx_1+nx_2 通过 m,n 的完全剩余系。 ♡

证明 由假设知道 x_1,x_2 分别通过 m,n 个整数，因此 nx_1+mx_2 通过 mn 个整数。由定理 2.3 的推论，只需要证明这 mn 个整数对模 mn 两两不同余就够了。

假定

$$nx_1'+mx_2'\equiv nx_1''+mx_2''(mod\ mn)$$

其中 x_1',x_1'' 是 x_1 所通过的完全剩余系中的整数，而 x_2',x_2'' 是 x_2 所通过的完全剩余系中的整数，则由命题 2.2 中的第 11 小点可得

$$nx_1'\equiv nx_2''(mod\ m),mx_1'\equiv mx_2''(mod\ n)$$

又由命题 2.2 中的第 6 小点以及 $gcd(m,n)=1$ 即得到 $x_1'\equiv x_1''(mod\,m),x_2'\equiv x_2''(mod\,n)$，可以得到 $x_1'=x_1'',x_2'=x_2''$ 这表明如果 x_1',x_2' 与 x_1'',x_2'' 不完全相同。式子不成立，因此定理获证。

此即得证。

2.3 既约剩余系和 Euler 函数

在上一节中我们讨论了完全剩余系的基本性质，这一节我们继续讨论完全剩余系中的一些与模互素的整数，引进既约剩余系的概念。并且我们要引入一个数论中很重要的 Euler 函数来辅助我们更进一步地探讨同余。

定义 2.4 (Euler 函数)

设 $n\in\mathbb{Z}_+$，在 $0,1,2,\cdots,n-1$ 上与 n 互素的数的个数，称为 n 的 Euler 函数，记作 $\varphi(n)$ ♣

例题 2.8 计算 $\varphi(12)$

解 $gcd(0,12)\neq1,gcd(1,12)=1,gcd(2,12)\neq1,gcd(3,12)\neq1,gcd(4,12)\neq1,gcd(5,12)=1,gcd(6,12)\neq1,gcd(7,12)=1,gcd(8,12)\neq1,gcd(9,12)\neq1,gcd(10,12)\neq1,gcd(11,12)=1$，所以 $\varphi(12)=4$

其实不管你怎么算，最容易发现且读者可以自己证明的性质是：

命题 2.3

设 $n\in\mathbb{Z},gcd(1,n)=1,gcd(n-1,n)=1$ ♠

其实还有五个，但是编者懒得证明，读者感兴趣可以证明一下练练自己的数学证明能力：

命题 2.4

1. $\varphi(n)=1$，当且仅当 $n=1,2$
2. $\varphi(n)\geq 2$，当且仅当 $m\geq 3$
3. $\varphi(n)$ 不是单调函数。
4. 若 p 是素数，$\varphi(p)=p-1$
5. 若 p 是素数，$\varphi(p^n)=p^n-p^{n-1}$

♠

上面我们讲了一些 Euler 函数的定义与性质，接下来我们要引入一个重要的知识点了。

定义 2.5

如果一个模 m 的剩余类里面的数与 m 互素，就把它们叫做一个与模 m 互素的剩余类，我们有时候可以叫做完全剩余类。

在与模 m 的互素的全部剩余类中，从每一个类各任取一数所作成的数的集合，叫做模 m 的一个既约剩余系。

♣

例题 2.9 当 m 等于 6 或 7 时，找出

1. 模 m 的最小非负完全剩余系
2. 与模 m 互素的完全剩余类
3. 模 m 的一个既约剩余系

解 当 $m=6$ 时

1. 因为 $K_0=0,K_1=1,K_2=2,K_3=3,K_4=4,K_5=5$，所以模 6 的最小非负完全剩余系为 $0,1,2,3,4,5$
2. 不难发现，K_1 和 K_5 是和模 6 互素的完全剩余类。
3. 像 $1,5$ 可以作为一个模 6 的既约剩余系，$7,11$ 也可以作为一个模 6 的完全剩余系。

当 $m=7$ 时

1. 因为 $K_0=0,K_1=1,K_2=2,K_3=3,K_4=4,K_5=5,K_6=6$，所以模 7 的最小非负完全剩余系为 $0,1,2,3,4,5,6$
2. 不难发现，K_1 到 K_6 是都和模 7 互素的完全剩余类。
3. 像 $1,2,3,4,5,6$ 可以作为一个模 7 的既约剩余系，我们还可以改一下，从不同的剩余类中找其他与模 7 互素的全部剩余类构成一个既约剩余系，比如 $8,2,10,4,19,-1$

不难看出，对于一个确定的模 m，它的完全剩余系要比既约剩余系多，有时候只多一个，有时候又要多好多个，读者可以自己多试几次找找感觉。

既约剩余系有许多性质，这些性质可以单独作为一个十分有意思且重要的定理存在，大部分定理作为练习交给感兴趣且想加深证明能力的读者证明，我们先来看定理 1：

定理 2.6

1. 模 m 的剩余类与模 m 互素的充分必要条件是此类中有一数与 m 互素。
2. 与模 m 互素的剩余类个数是 $\varphi(m)$ 个。
3. 模 m 的每一既约剩余系是由与 m 互素的 $\varphi(m)$ 个对模 m 不同余的整数组成的。

♡

证明 通俗证明一下，我们设 $K_0,K_1,\cdots,K_{m-1}$ 是模 m 的全部剩余类。若 K_r 是一个与模 m 互素的剩余类，则 $gcd(r,m)=1$，反之若有 $k_r\in K_r,gcd(k_r,m)=1$，则由剩余系的定理和命题 2.2 中第 11 小点可以得到 K_r 中每一个整数都与 m 互素，因而 K_r 是与模 m 互素的剩余类。且 K_r 为与模 m 互素的剩余类当且仅当 $gcd(r,m)=1$，因此由 Euler 函数的定义及模 m 的既约剩余系的定义可以得到证明。

此即得证。

定理 2.7

若 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数。并且两两对模 m 不同余，则 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是模 m 的一个既约剩余系。 ♡

根据这个定理，我们又有推论：

推论 2.2

若 $gcd(a, m) = 1$，x 通过模 m 的既约剩余系，则 ax 通过模 m 的既约剩余系。 ✽

证明 ax 通过 $\varphi(m)$ 个整数，由于 $gcd(a, m) = 1$，$gcd(x, m) = 1$，故 $(ax, m) = 1$，若 $ax_1 \equiv ax_2 9 mod\, m)$，由命题 2.2 第 6 小点，$x_1 \equiv x_2 (mod\, m)$，这与原设矛盾，故推论获证。

此即得证。

推论 2.3

若 m, n 是两个互素的正整数，x, y 分别通过模 m, n 的既约剩余系，则 $nx + my$ 通过 mn 的既约剩余系。 ✽

推论 2.4

若 m, n 是两个互素的正整数，则 $\varphi(mn) = \varphi(m)\varphi(n)$ ✽

以上没有给出证明的推论，感兴趣的读者可以自己证明一遍，甚至都不用证明，可以在维基百科上找到很多数论中的定理证明，把证明的方法和思路学会就是自己的了，这也是学习数学的一种方法。

接下来我们给出计算 Euler 函数的公式

定理 2.8

设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

♡

证明 由推论 2.3 可以得到

$$\varphi(a) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$$

现在证 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$，由 $\varphi(a)$ 的定义知 $\varphi(p^\alpha)$ 等于 p^α 减去 $1, 2, \cdots, p^\alpha$ 中与 p^α 不互素的数的个数，亦即等于从 p^α 减去 $1, 2, \cdots, p^\alpha$ 中与 p 不互素的数的个数。由于 p 是素数，故 $\varphi(p^\alpha)$ 等于从 p^α 减去 $1, 2, \cdots, p^\alpha$ 中被 p 整除的数的个数。由第一章的性质可知 $1, 2, \cdots, p^\alpha$ 中被 p 整除的数的个数是 $\left[\frac{p^\alpha}{p}\right] = p^{\alpha-1}$，故

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

由上述即得

$$\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{a_2} - p_2^{a_2-1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

此即得证。

其实我们还能得到两个小结论

命题 2.5

1. $\varphi(n)=\dfrac{n}{2}$ 当且仅当 $n=2^r,(r\in\mathbb{Z}_+)$
2. $\varphi(n)=\dfrac{n}{3}$ 当且仅当 $n=2^r\cdot 3^s,(r,s\in\mathbb{Z}_+)$

我们已经了解了既约剩余系，接下来就是要应用既约剩余系的性质来证明数论中的两个著名定理。

定理 2.9 (Euler 定理)

设 m 是大于 1 的整数，$gcd(a,m)=1$，则

$$a^{\varphi(m)}\equiv 1(mod\ m)$$

证明 设 $r_1,r_2,\cdots,r_{\varphi(m)}$ 是模 m 的既约剩余系，则由推论 2.3，$ar_1,ar_2,\cdots,ar_{\varphi(m)}$ 是模 m 的既约剩余系，故

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)})\equiv r_1r_2\cdots r_{\varphi(m)}(mod\ m)$$

即

$$a^{\varphi(m)}(r_1r_2\cdots r_{\varphi(m)})\equiv r_1r_2\cdots r_{\varphi(m)}(mod\ m)$$

但 $gcd(r_1,m)=(r_2,m)=\cdots=(r_{\varphi(m)},m)=1$，因此 $(r_1r_2\cdots r_{\varphi(m)},m)=1$，又由命题 2.2 中的第 6 小点可得

$$a^{\varphi(m)}\equiv 1(mod\ m)$$

推论 2.5. Fermat 小定理

若 p 是素数，则

$$a^p\equiv a(mod\ p)$$

证明 若 $gcd(a,p)=1$，由同余的定理可得 $a^{p-1}\equiv 1(mmod\ p)$，因而 $a^p\equiv a(mod\ p)$ 若 $gcd(a,p)\neq 1$，则 $p\mid a$，故 $a^{\varphi(m)}\equiv a(mod\ p)$

注 Fermat 小定理确切地说是 $gcd(a,p)=1$ 的情况，Fermat 在 1640 年提出，但是给不出证明，直到 1736 年，Euler 才给出了证明，并且在 1760 年证明了 Euler 定理。

例题 2.10 设 p 不等于 3 和 7 的奇素数，证明 $p^6\equiv 1(mod\ 84)$

证明 进行算术基本定理分解 $84=2^2\times 3\times 7=4\times 3\times 7$，所以由命题 2.2 中第 9 小点，只需要证明：

$$p^6\equiv 1(mod\ 4)$$

$$p^6\equiv 1(mod\ 3)$$

$$p^6\equiv 1(mod\ 7)$$

同时成立。

由于 p 是不等于 3 和 7 的奇素数，所以

$$gcd(p,4)=1,gcd(p,3)=1,gcd(p,7)=1$$

由 Euler 定理可知 $p^2=p^{\varphi(4)}==\equiv 1(mod\ 4)$，所以 $p^6\equiv 1(mod\ 4)$

同理可得 $p^6\equiv 1(mod\ 3)$，$p^6\equiv 1(mod\ 7)$

此即得证。

其实我们不难发现，若 m 为大于 1 的整数，a 为任意与 m 互素的整数，则由 Euler 定理可知，总可以找到自然 $\varphi(m)$ 使得 $a^{\varphi(m)}\equiv 1(mod\ m)$

然而，$\varphi(m)$ 并不一定是使 $a^x\equiv 1(mod\ m)$ 成立的自然数 x 中最小的，比如当 $a=5,n=8$ 时，

$$5^2\equiv 1(mod\ 8),而\varphi(8)=4$$

定理 2.10

若 m 为大于 1 的整数，a 为整数且 $gcd(a,m)=1$，如果自然数 h 为满足

$$a^x \equiv 1(mod\ m)$$

的所有自然数 x 中最小的，则 $h \mid x$

♡

证明 由带余除法可知 $x=hq+r \quad 0 \le r \le h-1)$

又由 $a^x \equiv 1(mod\ m)$ 和 $a^h \equiv 1(mod\ m)$ 知：

$$a^x = a^{h\cdot q+r} = a^{h\cdot q} \times a^r = (a^h)^q \times a^r \equiv 1(mod\ m)$$

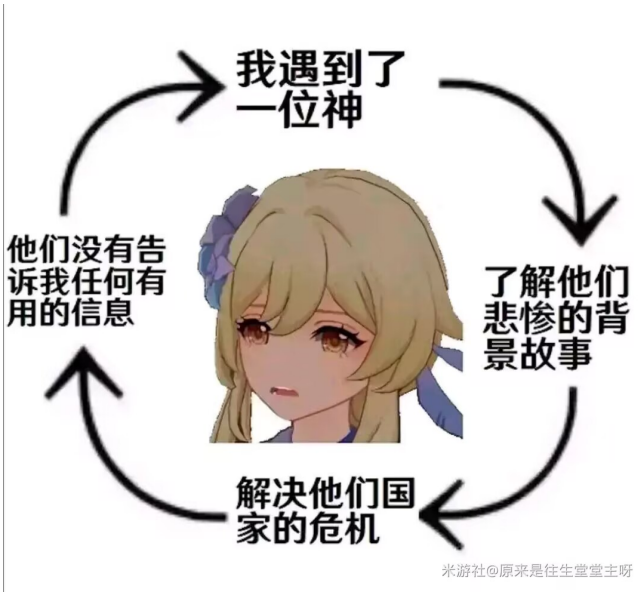
所以 $a^r \equiv 1(mod\ m)$，再由 h 的最小性可知：$r=0$，故 $h \mid x$

此即得证。

2.4 各种循环数

Euler 定理和 Fermat 小定理在数论上的地位非常重要，作为在数论上的一个应用，本节我们要来阐述它们在研究循环数还有分数和小数互化时的作用，最主要的研究就是循环小数了。

说到循环，读者可能会想到好多东西，比如有学计算机的读者会想循环是程序设计语言中反复执行某些代码的一种计算机处理过程，常见的有按照次数循环和按照条件循环。比如一些喜欢玩原神的玩家们可能会发现这 9+ 剧情也是个循环。



循环不循环的都不说了，我们先来看看一个通过 Fermat 小定理推出的小结论：

命题 2.6

设 $a,m \in \mathbb{Z}_+$，则 a^{m+4},a^m 的个位数字相同。

(即正整数的正整数次幂的个位数字是以 4 为周期循环变化的)

♠

证明

1. 当 $m=1$ 时，$a^{m+4}=a^5 \cdot a^m = a$，则可知这两个数 a^{m+4},a 的个位数字相同。
2. 当 $m>1$ 时，$a^{m+4}-a^m = a^{m-1}(a^5-a)$，且 $a^5 \equiv a^m(mod\ 10) \Leftrightarrow 10 \mid a^{m-1}(a^5-a) = a^{m+1}-a^m$

故 $a^{m+4} \equiv a^m(mod\ 10) \Rightarrow a^{m+4},a^m$ 的个位数字相同。

我们可以说，这就是一种循环，其实关于这种指数的循环我们有许多结论，我们就不一一证明而是直接列出来：

命题 2.7

1. 个位数是 $0,1,5,6$ 的任何正整数幂，其个位数字仍是 $0,1,5,6$
2. 2^n 的个位数字以 $2,4,8,6$ 为一个周期循环变化。
3. 3^n 的个位数字以 $3,9,7,1$ 为一个周期循环变化。
4. 4^n 的个位数字以 $4,6,4,6$ 为一个周期的循环变化。
5. 7^n 的个位数字以 $7,9,3,1$ 为一个周期的循环变化。
6. 8^n 的个位数字以 $8,4,2,6$ 为一个周期的循环变化。
7. 9^n 的个位数字以 $9,1,9,1$ 为一个周期的循环变化。

例题 2.11 求下列各数的个位数字。

1. $2^{100}+3^{101}+4^{102}$
2. $2022^{2020^{2021}}$
3. $1^5+2^5+\cdots+2021^5+2022^5$

解 我们要合理运用命题 2.62.7 给出的结论

1. $100=4\times25+0,101=4\times25+1,102=4\times25+2$，所以在 25 个周期的循环变化后，它们的个位数分别所对应的数字是 $6,3,6$，也就是说 $2^{100}\equiv6(mod\ 10),3^{101}\equiv3(mod\ 10),4^{102}\equiv6(mod\ 10)$，所以
$$2^{100}\equiv6(mod\ 10)+3^{101}\equiv3(mod\ 10)+4^{102}\equiv6(mod\ 10)\equiv6+3+6=15(mod\ 10)\equiv5(mod\ 10)$$
所以 $2^{100}+3^{101}+4^{102}$ 的个位数字是 5
2. 显然，2020^{2021} 是 4 的倍数，我们知道多位数字的指数幂的个位数是多少，我们只关系个位数，2022 的个位数是 2，又因为指数幂是 4 的倍数，所以 $2022^{2020^{2021}}\equiv6(mod\ 10)$
所以 $2022^{2020^{2021}}$ 的个位数是 6
3. 其实咋一看感觉很复杂，其实命题 2.6 里都有结论了，根据这个结论我们知道
$$1^5\equiv1(mod\ 10),2^5\equiv2(mod\ 10),3^5\equiv3(mod\ 10),\cdots,2022^5\equiv2022(mod\ 10)$$
所以用求和公式算一算 $S_{2022}=\dfrac{2022+1}{2}\times2022=2023\times1011$ 算到这里就可以了，个位数相乘是 3，所以 $1^5+2^5+\cdots+2021^5+2022^5\equiv3(mod\ 10)$
即 $1^5+2^5+\cdots+2021^5+2022^5$ 的个位数是 3

这种奥赛里出现的循环题，就是和 Euler 和 Fermat 定理相关的，多琢磨琢磨其实不会很难的。

接下来就是我们重点探寻的小学就学过的分数和循环小数了，我们先不讨论有哪些，先来看几道例题:

例题 2.12 指出下列小数哪些是纯循环小数、混循环小数，并且指出它们的循环节和循环节长度。

1. $0.3163116311163111116\cdots$
2. $0.31636363\cdots$
3. $0.333\cdots$
4. $0.8916438916438916438\cdots$
5. $0.23565787878\cdots$
6. 0.114514114514

解 我们什么方法还没学过，就用小学生都会的找规律瞪眼法来解。

1. 一下 116, 一下 1116，一下 11116，虽然规律找出来了，但是你一定能发现这既不是纯循环小数也不是混循环小数，这是个无限不循环小数。
2. 很明显是 $0.31\dot{6}\dot{3}$，那么 63 是循环节，循环节长度是 2
3. 很明显是 $0.\dot{3}$，那么 3 是循环节，循环节长度是 1
4. 读者们数一数也不难发现是 $0.8\dot{9}1643\dot{}$，那么 896143 是循环节，循环长度是 6

5. 很明显是 $0.236578\dot{9}$，那么 78 是循环节，循环节长度是 2
6. 看到这个你们喜欢的数字，是不是想说循环节是 114514，循环节长度是 6？如果你这么想那笔者只能说一句："6"。请看清楚数字后面没有省略号，所以这是个有限小数。

关于讨论小数，我们要先去讨论分数，这两者是密不可分的关系。

引理 2.4. 有理数表示方法

任何一个有理数 $\frac{a}{b}(b>0,a,b\in\mathbb{Z})$ 都可以表示成

$$\frac{a}{b}=\left[\frac{a}{b}\right]+\left\{\frac{a}{b}\right\},\text{其中}0\leq\left\{\frac{a}{b}\right\}<1$$

因此，我们只要讨论区间 $(0,1)$ 上的分数和小数的互化问题，显然 $(0,1)$ 中的有理数可以表示成 $\frac{a}{b}(a,b\in\mathbb{Z},0<a<b,gcd(a,b)=1)$ 的形式。

定义 2.6 (小数)

1. 如果在小数 $0.a_1a_2\cdots a_n(a_i=0,1,2,\cdots,9\text{中的某一个数字})$ 中，$a_n\neq 0$，则称此小数为 n 位有限小数。
2. 对于一个无限小数 $0.a_1a_2\cdots a_n\cdots(a_i=0,1,2,\cdots 9\text{中的某一个数字，并且从任意一位以后不全为}0)$，能找到两个整数 $s\geq 0,t>0$ 使得

$$a_{s+i}=a_{s+kt+i},\quad i=1,2,\cdots,t;k=0,1,2\cdots$$

我们就称它为循环小数，并且简单地把它记作为 $0.a_1a_2\cdots a_s\dot{a_{s+1}}\cdots\dot{a_{s+t}}$

如果上述的 s,t 不存在，则我们称之为无限不循环小数。

对于循环小数而言

(a). 如果 t 是满足循环小数性质的最小数，则我们称 $a_{s+1}a_{s+2}\cdots a_{s+t}$ 为此循环小数的循环节，t 称为循环节长度。

(b). 若最小的 $s=0$，则我们称此循环节为纯循环小数，否则为混循环小数。

注 对于循环小数而言，具有上述性质的 s 和 t 不止一个，比如循环小数 $0.301\dot{4}\dot{5}$ 中，可以有 $s=3,t=2$，还可以有 $s=4,t=4$

例题 2.13 将下列分数化为小数，并指出哪些是有限小数，哪些是纯循环小数，哪些是混循环小数。

$$\frac{1}{2},\frac{1}{3},\frac{1}{4},\frac{1}{5},\frac{1}{6},\frac{1}{7},\frac{1}{8},\frac{1}{9}$$

解 我们用最简单的除法运算可以得到

1. 有限小数：$\frac{1}{2}=0.5,\frac{1}{4}=0.25,\frac{1}{5}=0.2,\frac{1}{8}=0.125$
2. 纯循环小数：$\frac{1}{3}=0.\dot{3},\frac{1}{7}=0.\dot{1}42857,\frac{1}{9}=0.\dot{1}$
3. 混循环小数：$\frac{1}{6}=0.1\dot{6}$

注 这些都可以当作结论记下来，在我们分数小数互化的时候非常有用，后续内容有涉及到这一部分的互化我们就不过多讲解而是默认大家都会了。

我们发现了在这几个纯循环小数中，分母与 10 的最大公因数都是 1，故我们可以引入一个重要的定理。

定理 2.11

有理数 $\frac{a}{b},0<a<b,gcd(a,b)=1$ 能表示成纯循环小数的充分必要条件是 $gcd(b,10)=1$。这时，$\frac{a}{b}$ 所化成的纯循环小数的循环节长度 t 是满足 $10^x\equiv 1(mod\ b)$ 的最小正整数。

证明 若 $gcd(10,b)=1$，则由 Euler 定理和和定理 2.10 知：存在最小的正整数 t，使

$$10^t\equiv 1(mod\ b)$$

所以，$10^t = kb+1$，因而 $\frac{10^t}{b} = k + \frac{1}{b}$，等式两边同时乘以 a 得 $\frac{10^t \cdot a}{b} = ka + \frac{a}{b}$，即 $(10^h - 1) \cdot \frac{a}{b} = ka$，令 $ka = q, 0 < q < 10^t - 1$，因此 $q = \overline{a_1 a_2 \cdots a_h}$（$a_i$ 为整数，$0 \le a_i \le 0, i = 1, 2, \cdots, t, a_1, a_2, \cdots, a_t$ 既不全为 0，亦不全为 9）从而

$$\begin{aligned}\frac{a}{b} &= \frac{1}{10^t} \cdot + \frac{1}{10^t} \cdot \frac{a}{b} \\ &= 0.a_1 a_2 \cdots a_t + \frac{1}{10^t} \cdot \frac{a}{b} \\ &= 0.1 a_1 a_2 \cdots a_t a_1 a_2 \cdots a_t + \frac{1}{10^{2t}} \cdot \frac{a}{b}\end{aligned}$$

重复上述运算，即得

$$\frac{a}{b} = 0.a_1 a_2 \cdots a_t a_1 a_2 \cdots a_t \cdots = 0.\dot{a_1} a_2 \cdots \dot{a_t}$$

由于 t 的最小性，所以 $\frac{a}{b}$ 化为纯循环小数时循环节的长度为 t

若 $\frac{a}{b} = 0.\dot{a_1} a_2 \cdots \dot{a_t}$，则

$$\begin{aligned}10^t \cdot \frac{a}{b} &= \overline{a_1 a_2 \cdots a_t} + 0.a_1 a_2 \cdots a_t a_1 a_2 \cdots a_t \cdots \\ &= \overline{a_1 a_2 \cdots a_t} + \frac{a}{b} \\ (10^t - 1) \cdot \frac{a}{b} &= \overline{a_1 a - 2 \cdots a_t}\end{aligned}$$

又因为 $gcd(a, b) = 1$，所以，$b \mid 10^t - 1$，即 $gcd(10, b) = 1$

此即得证。

例题 2.14 将下列混循环小数表示成分数

$$0.8\dot{3} \quad 0.4\dot{6} \quad 0.6\dot{3} \quad 0.32\dot{1}42857\dot{}$$

解

1. 令 $x = 0.8\dot{3} \Rightarrow 10x = 8.\dot{3} = 8 + \frac{1}{3} \Rightarrow 2x = \frac{5}{3} \Rightarrow x = \frac{5}{6}$
2. 令 $x = 0.4\dot{6} = 0.3 + 0.1\dot{6} = \frac{3}{10} + \frac{1}{6} \Rightarrow x = \frac{7}{15}$
3. 令 $x = 0.6\dot{3} \Rightarrow 10x = 6.\dot{3} = 6 + \frac{1}{3} \Rightarrow 10x = \frac{19}{3} \Rightarrow x = \frac{19}{30}$
4. 令 $x = 0.32\dot{1}42857\dot{} \Rightarrow 100x = 32 + 0.\dot{1}42857\dot{} = 32 + \frac{1}{7} \Rightarrow x = \frac{9}{28}$

我们可以看看这些混循环小数表示成的分数有什么特点，首先分数都是 $\frac{a}{b}$ 格式，其次 $0 < a < b, gcd(a, b) = 1$，读者们可能会想这是所有最简真分数的通常样子，可是大家关注一下每个分式的分母，$6 = 2^1 \times 3^1, 15 = 3^1 \times 5^1, 30 = 2^1 \times 3^1 \times 5^1, 28 = 2^2 \times 7^1$，其实混循环小数化为分数形式，它前面的不循环的个数问题，其实和分母化为标准分解式他 2 的指数和 5 的指数有关，我们可以把 b 写成 $b = 2^\alpha 5^\beta b_1$ 的形式。

对于第一题来说 α 是 1 β 是 0，第二题 α 是 1 β 是 1，第三题 α 是 1 β 是 1，第四题 α 是 2 β 是 0，所以它们循环节前面不循环的个数分别是 $1, 1, 1, 2$，这样的话读者是否能看到某些规律，这样一个分数化为混循环小数的定理就呼之欲出了。

定理 2.12

若 $\frac{a}{b}$ 是有理数，其中 $0 < a < b, gcd(a, b) = 1, b = 2^\alpha 5^\beta b_1, gcd(b_1, 10) = 1, b_1 \ne 1, \alpha\beta$ 不全为零，则 $\frac{a}{b}$ 可以表示为混循环小数，其中不循环的位数是 $\mu = max(\alpha, \beta)$ ♡

证明 需要就 $\beta \ge \alpha, \beta < \alpha$ 两种情形进行证明，因为证明方法相同，我们可以假设 $\mu = \beta \ge \alpha$，用 10^μ 乘 $\frac{a}{b}$ 得

$$10^\mu \cdot \frac{a}{b} = \frac{2^{\beta - \alpha}}{b_1} = M + \frac{a_1}{b_1}$$

其中 $0 < a_1 < b_1, 0 \le M < 10^\mu$ 且 $gcd(a_1, b_1) = gcd(2^{\mu-\alpha} a - M b_1, b_1) = gcd(2^{\mu-\alpha} a, b_1) = 1$，故根据定理 2.11 可以把 $\frac{a_1}{b_1}$ 化成纯循环小数：$\frac{a_1}{b_1} = 0.\dot{c_1} \dot{c_2} \cdots \dot{c_t}$

设 $M = m_1 10^{\mu-1} + m_2 10^{\mu-2} + \cdots + m_\mu (0 \le m_r \le 9)$，则

$$\frac{a}{b} = 0.m_1 m_2 \cdots m_\mu \dot{c_1}\dot{c_2}\cdots\dot{c_t}$$

我们还需要证明不循环位数不能小于 μ，假定 $\frac{a}{b}$ 又可以表示成

$$\frac{a}{b} = 0.m_1' m_2' \cdots m_v' \dot{c_1}'\dot{c_2}'\cdots\dot{c_s}', \quad v < \mu$$

则由定理 2.11 又有

$$10^v \frac{a}{b} - \left[10^v \frac{a}{b}\right] = \dot{c_1}'\dot{c_2}'\cdots\dot{c_s}' = \frac{a_1'}{b_1'}$$

其中 $gcd(b_1', 10) = 1$，故存在一整数 a' 使得

$$10^v \frac{a}{b} = \frac{a_1'}{b_1'} \quad 即 10^v a b_1' = a' b$$

上式右边可用 $5^\beta = 5^\mu$ 除尽，而左边 a 及 b_1' 都与 5 互素，故 $5^\mu \mid 10^v$，但是 $\mu > v$，显然不可能。

此即得证。

除此之外，还有个最简单的：

定理 2.13

有理数 $\frac{a}{b}(a, b \in \mathbb{Z}, 0 < a < b, gcd(a, b) = 1)$ 能化为有限小数的充分必要条件为：b 中不含有 2 和 5 外的素因数，并且当 $2^\alpha \cdot 5^\beta$ 时，$\frac{a}{b}$ 是一个 s 位有限小数，其中 $s = max(\alpha, \beta)$

♡

还有证明的必要吗？喜欢的读者可以证一下玩玩。

上述三个定理告诉我们有理数 $\frac{a}{b}$ 化为小数时可能出现的三种情况，虽然这三种情况彼此互相独立，但是在有理数和小数互化的过程中所采用的手法不能说十分相似，只能说完全一致的。而且前两个定理求循环节的长度也是十分相似。

由于循环节长度 t 为满足 $10^x \equiv 1 (mod\ b)$ 或者 $10^x \equiv 1 (mod\ b_1)$ 的最小正整数，因此，它只依赖于 b，换句话说，相同的 b 具有相同的循环节长度，而对不同的 a 来说，每个循环节的长度是否一样？它们之间有何关系？这就是所谓循环节构造的问题，我们来探讨一下。

设 $\frac{a}{b}$ 是有理数，其中 $0 < a < b, gcd(a, b) = 1, b = 2^\alpha 5^\beta b_1, gcd(b_1, 10) = 1, b_1 \ne 1, \alpha\beta$ 不全为零，则 $\frac{a}{b}$ 可以表示为混循环小数，其中不循环的位数是 $s = max(\alpha, \beta)$

$$\begin{aligned}\frac{a}{b} &= 0.a_1 a_2 \cdots a_s + \frac{1}{10^t} \cdot \frac{r_s}{b} \\ &= 0.a_1 a_2 \cdots a_s \dot{a_{s+1}} \cdots \dot{a_{s+h}} \\ &= 0.a_1 a_2 \cdots a_s + \frac{1}{10^s} \times 0.\dot{a_{s+1}} \cdots \dot{a_{s+h}}\end{aligned}$$

所以，$\frac{r_s}{b} = 0.\dot{a_{s+1}} \cdots \dot{a_{s+h}}$ 为一个与 $\frac{a}{b}$ 有相同的循环节的纯循环小数。可见由 $\frac{r_s}{b}$ 化成的既约分数的分母中一定只含有异于 2 和 5 的素因数，所以只需就分母与 10 互素的情况来讨论循环节的构造。

显然，形容 $\frac{a}{b}, 0 < a < b, gcd(a, b) = 1$ 的有理数共有 $\varphi(b)$ 个，它们的分子分别是模 b 的非负最小完全剩余系中的各个数。由前面的的讨论我们知道了，它们的循环节长度是一个 t，并且 $t \mid \varphi(b)$

以下设有理数 $\frac{a}{b}, 0 < a < b, gcd(a, b) = 1, gcd(10, b) = 1$，则由带余除法可知

$$10a = ba_1 + r_1 \quad 0 < r_1 \le b - 1 (0 \le a_1 \le 9)$$

$$10r_1 = ba_2 + r_2 \quad 0 < r_2 \le b - 1 (0 \le a_2 \le 9)$$

$$\cdots$$

$$10r_{t-1} = ba_t + r_t \quad 0 < r_t \le b - 1 (0 \le a_t \le 9)$$

$$\cdots$$

又由定理 2.13 知，$\frac{a}{b}$ 能化为纯循环小数，即

定理 2.14

如上述假设，

$$\frac{a}{b}=0.\dot{a_1}a_2\cdots\dot{a_t}$$

$$\frac{r_i}{b}=0.\dot{a_{i+1}}\cdots a_t a_1\cdots\dot{a_i}$$

♡

例题 2.15 将有理数 $\frac{a}{7}(0<a<7,gcd(a,7)=1)$ 化为纯循环小数，并说出它们的循环节的构造。

解 因为 $\varphi(7)=6$，而 6 的全部正约数 $1,2,3,6$，经计算知：此类有理数的循环节长度为 6，又由带余除法，有

$$10\times1=7\times1+3,10\times3=7\times4+2$$

$$10\times2=7\times2+6,10\times6=7\times8+4$$

$$10\times4=7\times5+5,10\times5=7\times7+1$$

所以，由定理 2.14，我们有

$$\frac{1}{7}=0.\dot{1}42857\dot{1},\frac{3}{7}=0.\dot{4}28571\dot{4}$$

$$\frac{2}{7}=0.\dot{2}85714\dot{2},\frac{6}{7}=0.\dot{8}5714|dot2$$

$$\frac{4}{7}=0.\dot{5}71428\dot{5},\frac{5}{7}=0.\dot{7}14285\dot{7}$$

它们的循环节分别由 $1,4,2,8,5,7$ 这 6 个数字顺序轮换而得。

其实我们仔细观察这个例题里的每个循环节，我们可以发现一个有趣的现象：若将有理数 $\frac{a}{7}$ 表示成 $\frac{a}{7}=0.q_1q_2q_3t_1t_2t_3$，则

$$q_i+t_i=9(i=1,2,3)$$

一般地，我们有

定理 2.15

1. 如定理 2.14 假设，如果有理数 $\frac{a}{b}$ 化成的循环小数的循环节长度为偶数，即 $t=2k$，且 $(10^k-1,b)=1$，若将 $\frac{a}{b}$ 表示为

   $$\frac{a}{b}=0.\dot{q_1}q_2\cdots q_kt_1t_2\cdots\dot{t_k}$$

   则

   $$q_i+t_i=9(i=1,2,3)$$

2. 如定理 2.14 假设，如果有理数 $\frac{a}{b}$ 化成的循环小数的循环节长度为 $t=\frac{\varphi(b)}{m}$，则形如 $\frac{a}{b}(0<a<b,gcd(a,b)=1)$ 的有理数共可分成 m 个组，每个组有 t 个数，在同一组中的数在化为纯循环小数后，其循环节由相同 t 个数字循环顺序轮换而得到。

♡

例题 2.16

1. 将有理数 $\frac{a}{11}(0<a<11,gcd(a,11)=1)$ 化为纯循环小数，并说出它们的循环节构造。
2. 将有理数 $\frac{a}{13}(0<a<11,gcd(a,13)=1)$ 化为纯循环小数，并说出它们的循环节构造。

解

1. 因为 $\varphi(11)=10$，而 10 的全部正因数为 $1,2,5,10$，所以经过计算得到 $t=2$（这里用到了定理 2.11 中

$10^2 \equiv 1(mod\ 11)$，之后不过多讲纯循环小数这个 t 怎么求了。）由带余除法可得：

$$10 \times 1 = 11 \times 0 + 10$$

所以，$\frac{1}{11} = 0.\dot{0}\dot{9}, \frac{10}{11} = 0.\dot{9}\dot{0}$

$$10 \times 2 = 11 \times 1 + 9, 所以, \frac{2}{11} = 0.\dot{1}\dot{8}, \frac{9}{11} = \dot{8}\dot{1}$$

$$10 \times 3 = 11 \times 2 + 8, 所以, \frac{3}{11} = 0.\dot{2}\dot{7}, \frac{8}{11} = \dot{7}\dot{2}$$

$$10 \times 4 = 11 \times 3 + 7, 所以, \frac{4}{11} = 0.\dot{3}\dot{6}, \frac{7}{11} = \dot{6}\dot{3}$$

$$10 \times 5 = 11 \times 4 + 6, 所以, \frac{5}{11} = 0.\dot{4}\dot{5}, \frac{6}{11} = \dot{5}\dot{4}$$

形如 $\frac{a}{11}(0 < a < 11, gcd(a, 11) = 1)$ 的有理数，共可以分成 5 个组，每个组有 2 个数，在同一组数在化为纯循环小数后，其循环节由相同的两个数字按顺序轮换得到。

2. 因为 $\varphi(13) = 12$，而 12 的全部正因数为 $1, 2, 3, 4, 6, 12$，经过计算可知 $t = 6$，因此形如 $\frac{a}{13}(0 < a < 11, gcd(a, 13) = 1)$ 的有理数共可分成 2 个组，每个组有 6 个数，由带余除法可知

$$10 \times 1 = 13 \times 0 + 10, 10 \times 10 = 13 \times 7 + 9$$

$$10 \times 9 = 13 \times 6 + 12, 10 \times 12 = 13 \times 9 + 3$$

$$10 \times 3 = 13 \times 2 + 4, 10 \times 4 = 13 \times 3 + 1$$

由此得第一组数字和它们化成的纯循环小数

$$\frac{1}{13} = 0.\dot{0}76923\dot{.}\frac{10}{13} = 0.\dot{7}69230\dot{,}\ \frac{9}{13} = 0.\dot{6}92307\dot{}$$
$$\frac{12}{13} = 0.\dot{9}23076\dot{.}\frac{3}{13} = 0.\dot{2}30769\dot{,}\ \frac{4}{13} = 0.\dot{3}07692\dot{}$$

其循环节由 $0, 7, 6, 9, 2, 3$ 六个数字按顺序轮换而成。

$$10 \times 2 = 13 \times 1 + 7, 10 \times 10 = 7 \times 5 + 5$$

$$10 \times 5 = 13 \times 3 + 11, 10 \times 12 = 11 \times 8 + 6$$

$$10 \times 6 = 13 \times 4 + 8, 10 \times 4 = 8 \times 6 + 2$$

由此得第二组数字和它们化成的纯循环小数

$$\frac{2}{13} = 0.\dot{1}53846\dot{,}\ \frac{7}{13} = 0.\dot{5}38461\dot{,}\ \frac{5}{13} = 0.\dot{3}84615\dot{}$$
$$\frac{11}{13} = 0.\dot{8}46153\dot{,}\ \frac{6}{13} = 0.\dot{4}61538\dot{,}\ \frac{8}{13} = 0.\dot{6}15384\dot{}$$

其循环节由 $1, 5, 3, 8, 4, 6$ 六个数字按顺序轮换而成。

定理的主要证明就交给感兴趣的读者自己去证明了，我虽然有个完美的证明方法，因为这里空隙太小，写不下了（Fermat 并感）。那么到此，我们的同余这一章就结束了。

第 3 章 同余式

不知道读者有没有看过 BiliBili 的一个 UP 主分析学玩家的视频：《孤勇者》大学数学版。里面有句歌词叫：分析、方程、这积分的学问，代数、数论、这抽象的理论，研究数学绝不是一帆风顺，永不放弃才是我们的特征。

这一句也鼓励各位读者学完了之前的知识，从这一章开始我们就要讨论更难一点的数论知识了。我们知道在如此抽象的代数学中，有一个主要问题就是解代数方程。不仅要求我们对代数方程何时有解、何时无解及其原因作出回答，而且还要在有解的情况下求出所有解的答案。我们刚刚学完同余，这一章就要来讨论同余式的解了。例如问，x 取何值，能使

$$x^5+x+1\equiv 0(mod\ 7)$$

成立？这就是解同余式的，也可以称为解同余方程的问题。当然聪明的读者都能看出答案是 $x\equiv 2(mod\ 7)$ 是一解。本章我们主要从同余式出发探讨一次同余式和一次同余方程组，然后进阶到高次同余式。我们还会特别介绍一些中国古代数学家在这方面的卓越成就，感受中国古代数学在人类历史上的熠熠生辉。

3.1 同余式基本概念与一次同余式

我们首先要讲的就是同余式的一些基本概念，我们选择从一些例子出发去探讨。

例题 3.1

下列各数哪些能使式子 $x^2+x\equiv 6(mod\ 7)$ 成立

A.4　B.2　C.7　D.3

解 先看 A 选项，带入 4 可得到 $16+4=20\equiv 6(mod\ 7)$，显然是成立的。再看 B 选项，带入 2 可得到 $4+2=6\equiv 6(mod\ 7)$，显然也是成立的。同样的方法，C 和 D 就不行了。所以答案是 A 和 B

例题 3.2

下列各数哪些能使式子 $2x\equiv 3(mod\ 5)$ 成立

A.4　B.8　C.9　D.24

解 笔者这里都不想写过程了，狠狠地把数字往里面带再利用同余的性质就知道答案了，显然是 ACD 正确，B 错误。我们要关注的地方是这些答案有什么共性，4 在模 5 里是 K_4，9 在模 5 里也是 K_4，24 在模 5 里还是 K_4。这就是一个大发现了。这样就为后面的定义做了铺垫。

定义 3.1 (同余式)

若用 $f(x)$ 表示成多项式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，其中 a_i 是整数；又设 m 是一个正整数，则

$$f(x)\equiv 0(mod\ m)$$

叫做模 m 的同余式，若 $a_n\not\equiv 0(mod\ m)$，则 n 叫做上述式子的次数。

其实根据同余式定义，我们也能根据前面学过的命题 2.2 中的第 5 小点得到如下命题

命题 3.1

若 $f(0)\equiv 0(mod\ m)$ 是一个模 m 的同余式，$a\in\mathbb{Z},K_a$ 为所在 a 的模 m 剩余类，则对任意 $b\in K_a$ 都有 $f(b)\equiv 0(modm)$

这也是我们有如下定义

定义 3.2

若 a 是使得同余式 $f(a)\equiv 0(mod\ m)$ 成立的一个整数，则称 a 所在的模 m 的剩余类 K_a 是同余式 $f(a)\equiv 0(mod\ m)$ 的一个解，记为 $x\equiv a(mod\ m)$

注 上述定义说明，把适合 $f(a)\equiv 0(mod\ m)$ 而对模 m 同余的一切整数，即模 m 的一个剩余类 K_a 作 $f(a)\equiv 0(mod\ m)$ 的一个解，而模 m 又只有 m 个，因此要求同余式 $f(a)\equiv 0(mod\ m)$ 的解只要逐个将 $0,1,2,\cdots,m-1$ 代入 $f(a)\equiv 0(mod\ m)$ 中验算，就可以得到所有解。然而当 m 很大，并且 $f(a)\equiv 0(mod\ m)$ 的次数 n 也很大时，计算量往往也很大。

例题 3.3

下列各数哪些能使式子 $x^2+x\equiv 6(mod\ 7)$ 成立?

A.4　B.2　C.7　D.3

解 其实你光带数字进去肯定能做出来 A 和 B 是对的，毕竟这是一道选择题，我们主要是再探讨一下和定义有关的性质。

$4\in K_4$ 满足 $x^2+x\equiv 6(mod\ 7)$，所以 K_4 是 $x^2+x\equiv 6(mod\ 7)$ 的解

$2\in K_2$ 满足 $x^2+x\equiv 6(mod\ 7)$，所以 K_2 是 $x^2+x\equiv 6(mod\ 7)$ 的解

$7\in K_0, 3\in K_3$ 不满足 $x^2+x\equiv 6(mod\ 7)$，所以 K_0,K_3 不是 $x^2+x\equiv 6(mod\ 7)$ 的解

$1\in K_1, 5\in K_5, 6\in K_6$ 不满足 $x^2+x\equiv 6(mod\ 7)$，所以 K_1,K_5,K_6 不是 $x^2+x\equiv 6(mod\ 7)$ 的解

所以这个 $x^2+x\equiv 6(mod\ 7)$ 只有两类解，就是 $m=7$ 的剩余类 K_2,K_4，我们可以写成 $x\equiv 2(mod\ 7), x\equiv 4(mod\ 7)$

所以验算法当然可以作为解同余式的一个方法，n 次同余式的解的个数可以大于 n 但是不能大于模 m，接下来我们讲一下有关一元一次同余式的求解问题。

定理 3.1 (一次同余式唯一解定理)

一次同余式 $ax\equiv b(mod\ m), a\not\equiv 0(mod\ m)$ 当 $gcd(a,m)=1$ 时有唯一解。 ♡

证明 因为整数集合 $\{1,2,\cdots,m\}$ 为模 m 的一个完全剩余系，又因为 $gcd(a,m)=1$，所以由推论 2.3 可知整数集合 $\{a,2a,\cdots,m\}$ 也为模 m 的一个完全剩余系，所以其中恰有一个整数 aj 适合

$$aj\equiv b(mod\ m)$$

所以

$$x\equiv j(mod\ m)$$

是同余式 $ax\equiv b(mod\ m)$ 的唯一解

但是定理 3.1 并没有告诉我们怎样来求这个唯一解，除非你把 $1,2,\cdots,m$ 带入同余式 $ax\equiv b(mod\ m)$ 一个一个验算，这不累的跟狗一样啊？这是我们不愿意看到的。那怎么办呐？我们有：

定理 3.2 (一次同余式唯一解求解公式)

若 $m\in\mathbb{Z}_+; a,b\in\mathbb{Z}, gcd(a,m)=1$，则 $ax\equiv b(mod\ m)$ 的唯一解是

$$x\equiv a^{\varphi(m)-1}b(mod\ m)$$

♡

证明 因为 $gcd(a,m)=1$，所以由 Euler 定理我们可以知道

$$a^{\varphi(m)}\equiv aa^{\varphi(m)-1}\equiv 1(mod\ m)$$

所以，由命题 2.2 的第 3 点可知

$$aa^{\varphi(m)-1}\cdot b\equiv b(mod\ m)$$

又由定理 3.1 可知 $x\equiv a^{\varphi(m)-1}\cdot b(mod\ m)$ 是 $ax\equiv b(mod\ m)$ 的唯一解。

显然，定理 3.2 给出了一次同余式唯一解的求解公式，这是一件非常好的事情。在了解了只有一个解的情况下，我们该给出有多个解的情形了。

定理 3.3 (一次同余式有 d 个解定理)

一次同余式 $ax \equiv b(mod\, m), a \not\equiv 0(mod\, m)$ 当 $gcd(a,m) = d$ 时，
有解的充分必要条件是 $d \mid b$，且当该一次同余式有解时，它有 d 类解。 ♡

证明 先证充分性，因为 $d \mid b$，又 $gcd(a,b) = d$, 所以 $(\frac{a}{d}, \frac{m}{d} = 1)$, 由定理 3.1 知，同余式基本概念与一次同余式

$$\frac{a}{d}x \equiv \frac{b}{d}(mod\, m)$$

恰有一解，设为 $x \equiv c(mod\, \frac{m}{d})$，即 $\frac{a}{d} \cdot c = \frac{b}{d}(mod\, \frac{m}{d})$

所以 $\frac{a}{d} \cdot c = \frac{m}{d} \cdot q + \frac{b}{d}(q \in \mathbb{Z})$，即 $ac = mq + b$，故 $ac \equiv b(mod\, m)$，所以同余式有唯一解 $x \equiv c(mod\, m)$。

再证必要性，如果同余方程有解，不妨设为 $x \equiv c(mod\, m)$ 所以 $ac \equiv b(mod\, m), ac = mq + b$ 又因为 $gcd(a,b) = d$，所以 $d \mid a, d \mid m$ 因而 $d \mid b$

由前面的讨论所知，所有形如

$$x = c + \frac{m}{d}t \quad t = 0, \pm 1, \pm 2, \cdots$$

的整数都满足同余式 $ax \equiv b(mod\, m)$，而这些整数对模 m 来说，可以写成

$$x \equiv c + \frac{m}{d}k(mod\, m) \quad k = 0, 1, \cdots, d-1$$

且整数 $c, c + \frac{m}{d}, \cdots, c + \frac{m}{d}(d-1)$ 对模 m 两两不同余，因此它们分别属模 m 的 d 的两个不同剩余类，所以同余式

$$ax \equiv b(mod\, m)$$

恰有 d 类解。

此即得证。

例题 3.4 求一次同余式 $4x \equiv 6(mod\, 10)$ 的所有解

解 $gcd(4,10) = 2, 2 \mid 6$，由定理知该同余式有 2 类解，

又因为 $a = 4 = 2 \times 2, \quad b = 6 = 2 \times 3, \quad m = 10 = 2 \times 5$, 所以可以考察 $2x \equiv 3(mod\, 5)$

又因为 $gcd(2,5) = 1$，用方程的思想去解，可以设 $s, t \in \mathbb{Z}$ 使得 $as + mt = 1$，很明显 $s = 3, t = -1$ 是一解，我们知道 x 是 $s \cdot b$ 所以该同余式唯一解是

$$x \equiv 9(mod\, 5)$$

但是这不是最简解，我们知道 9 模 5 余 4，所以最简解是 $x \equiv 4(mod\, 5)$

原同余式有两类解的，第一个就是 $x \equiv 4(mod\, 10)$，第二类解就是 $x \equiv 4 + 5(mod\, 10) \equiv 9(mod\, 10)$

但是一般来说，当 a 与 m 都很大的时候，用 Euler 方法来解一元一次同余式时候计算量也往往大的露卵，这就要求我们去寻找其他方式来破解难题。

下面笔者又在其他初等数论书上偷抄了三个比较杀火但是前面定理貌似讲过不太行、但是你实在不会算了就可以用来算的方法来介绍一下。

1. 同余倍数连加法与同余变形法

例：计算 $8x \equiv 9(mod\, 11)$ 与 $9x \equiv 6(mod\, 15)$

(1) 因为 $gcd(8,11) = 1$, 所以只有唯一解。由同余性质可知 $8x \equiv 9 + 11 \equiv 20(mod\, 11)$，又因为 $gcd(8,11) = 1$，所以

$2x \equiv 5(mod\, 11)$，由同余性质可知 $2x \equiv 5 + 11 \equiv 16(mod\, 11)$，又因为 $gcd(2,11) = 1$，所以 $x \equiv 8(mod\, 11)$

这里解释一下为什么叫同余倍速连加法，因为原同余式的解是唯一的，倍数可以一直加，$8x \equiv 9 + 11 + 11 + 11 + 11 + 11 \equiv 9 + 11 \times 5(mod\, 11) \Rightarrow x \equiv 8(mod\, 11)$

反正解是唯一的时候你想铁着头皮硬算，那么这种算法是可以的，只要一直加模 m 的倍数你总能算出来。

(2) 因为 $gcd(9,15) = 3, 3 \mid 6$，所以同余式恰有三类解。那我们先求同余式 $3x \equiv 2(mod\, 5)$，显然 $gcd(3,5) = 1$ 只有唯一解

显然有 $3x \equiv 2+5+5 \equiv 2+10 \equiv 12 \equiv (mod\ 5)$，所以原同余式的三个解为

$$x \equiv 4(mod\ 15) \quad x \equiv 9(mod\ 15) \quad x \equiv 14(mod\ 15)$$

这里解释一下为什么叫同余变形法，其实和同余倍数连加法一样的，只不过这里原同余式三个解，但是并不影响我们经过适当变形后求得其解。

2. 组合数法

定理 3.4 (组合数求同余式唯一解)

若 p 为素数，且 $a,b \in \mathbb{Z}, 0<a<p$，则

$$x \equiv b \times (-1)^{a-1} \times \frac{(p-1)(p-2)\cdots(p-a+1)}{a!}(mod\ p)$$

为同余方程 $ax \equiv b(mod\ p)$ 的唯一解 ♡

证明 由定理内容知，$gcd(a,p)=1$，故同余式有唯一解，我们将

$$x \equiv b \times (-1)^{a-1} \times \frac{(p-1)(p-2)\cdots(p-a+1)}{a!}(mod\ p)$$

代入到上述同余式中，并注意到 $C_p^a = \frac{p!}{a!(p-a)!}$，且

$$(p-1)(p-2)\cdots(p-a+1) \equiv (-1)^{a-1} \times (a-1)!(mod\ p)$$

此即得证。

例题 3.5 求同余式 $7x \equiv 8(mod\ 11)$ 的所有解。

解 我们一上来还是老样子，判别解的情况，$gcd(7,11)=1$，此同余式有唯一解。又因为 11 是素数，且 $0<7<11$，可用组合数法

$$x \equiv 8 \times (-1)^{7-1} \times \frac{10 \times 9 \times 8 \times 7 \times 6 \times 5}{7!}(mod\ 11)$$

经过整理得 $x \equiv 8 \times 30 \equiv 9(mod\ 11)$

最后，我们来介绍一种由我们中国古代数学家秦九韶得出的求解同余式 $ax \equiv b(mod\ m)$ 的方法。

3. 大衍求一术

大衍求一术是最早的完整记载见于宋代大数学家秦九韶所著的《数书九章》，秦九韶称为“求一术”，喜欢研究古代数学的读者可以看看李俨著《中算史论丛》第一集：大衍求一术的过去与将来。废话不多说，大衍求一术用现代数学语言表达就是

定理 3.5 (大衍求一术)

已知 $m,a \in \mathbb{Z}, gcd(a,m)=1, m>0$ 来求整数 k，使得

$$ak \equiv 1(mod\ m)$$

成立，显然 $x \equiv kb(mod\ m)$ 为唯一解。其具体步骤为：

1. 对 a,m 实施辗转相除法，即

$$a = mq_1 + r_1 \quad 0 < r_1 \leq m-1$$

$$m = r_1q_2 + r_2 \quad 0 < r_2 \leq r_1 - 1$$

$$\cdots$$

$$r_{n-2} = r_{n-1}q_n + r_n \quad 0 < r_n \leq r_{n-1} - 1$$

$$r_{n-1} = r_nq_{n+1}$$

因为 $gcd(a,m)=1$，所以 $r_n=1$，且由推论 1.4 知

$$Q_na - P_nm = (-1)^{n-1}r_n$$

于是可以发现，$a\left[(-1)^{n-1}Q_n\right]+m\left[(-1)^nP_n\right]=1$
所以 $a\left[(-1)^{n-1}Q_n\right]\equiv 1(mod\, m)$，其中 Q_n 可根据

$$Q_0=0 \quad Q_1=1 \quad Q_k=q_kQ_{k-1}+Q_{k-2}$$

求出

2. 继续求出 $x\equiv\left[(-1)^{n-1}Q_n\right]\times b(mod\, m)$ 的最简表达式。

♡

例题 3.6 求同余式 $59x\equiv 179(mod\, 312)$ 的所有解

解 因为 $gcd(59,312)=1$，所以该同余式有唯一解。由大衍求一术中的递推公式知

a	q_n	m
59	0	312
0	5	295
59	3	17
51	2	16
8	7	1
7		
1	$=r_5$	

n	1	2	3	4	5	
q_n	0	5	3	2	1	
Q_n	1	5	16	37	275	$=Q_5$

所以

$$x\equiv\left[(-1)^{5-1}\times 275\right]\times 179\equiv 241(mod\, 312)$$

以上我们就介绍了三个解法，在求解一元一次同余式的时候根据具体情况选用适当的方法就好了。

3.2 一次同余方程组与中国剩余定理

在上一节我们已经看到了一元一次同余式有解的条件，在有解的条件下有多少个解，求解的方法和解的公式等问题都已能够解答。在对方程问题的研讨中，如果对于方程有解的条件，在有解的条件下有多少个解、求解的方法和解的公式等问题就能够找到像对一元一次同余式这样完美的解答，我们的目的就算是达到了。回想小学，学完解一元方程，我们就要学二元一次方程组，所以我们从这里入手。

探讨一下从 k 个同余式组成的一元一次同余方程组：

$$\begin{cases} x\equiv b_1 \quad (mod\, m_1) \\ x\equiv b_2 \quad (mod\, m_2) \\ \cdots \\ x\equiv b_k \quad (mod\, m_k) \end{cases}$$

其中 $m_1,m_2,\cdots,m_k$ 为正整数，$b_1,b_2,\cdots,b_k$ 为整数的求解问题。

这样我们就可以给出一个定义

定义 3.3

在 k 个同余式组成的一元一次同余方程组中，设 $m=lcm(m_1,m_2,\cdots,m_k)$ 如果整数 c 满足该同余方程

组，则我们称

$$x \equiv c(mod\ m)$$

为该一元一次同余方程组的一个解。 ♣

显然例子里的 k 个同余式组成的一元一次同余方程组最多有 m 个解。

为了方便起见，以下我们称一元一次同余方程组为一次同余方程组，我们先来看看一些可以用来计算的性质。

例题 3.7 求证 $660x \equiv 1(mod\ 7)$ 与 $2x \equiv 1(mod\ 7)$ 同解。

证明 因为 $660 = 7 \times 94 + 2$，所以 $660 \equiv 2(mod\ 7)$，通过命题 2.2 的第 3 点我们知道了 $660x \equiv 2x(mod\ 7)$

1.

$$\left.\begin{aligned} 660x &\equiv 2x\ (mod\ 7) \\ 660x &\equiv 1\ (mod\ 7) \end{aligned}\right\} \xrightarrow{\text{命题 2.1 第 3 小点}} 2x \equiv 1\ (mod\ 7)$$

2.

$$\left.\begin{aligned} 660x &\equiv 2x\ (mod\ 7) \\ 2x &\equiv 1\ (mod\ 7) \end{aligned}\right\} \xrightarrow{\text{命题 2.1 第 3 小点}} 2x \equiv 660\ (mod\ 7)$$

由上述 1，2 可知，上述两同余式同解。

我们接着把例题 3.7 里的常数换成任意变量的形式，那我们便有了

命题 3.2

已知 $a = mq + r$，则同余式 $ax \equiv b(mod\ m)$ 与 $rx \equiv b(mod\ m)$ 同解。 ♠

证明 因为 $a = mq + r$，所以 $a \equiv r(mod\ m) \Rightarrow ax \equiv rx(mod\ m)$

1.

$$\left.\begin{aligned} ax &\equiv rx\ (mod\ m) \\ rx &\equiv b\ (mod\ m) \end{aligned}\right\} \xrightarrow{\text{命题 2.1 第 3 小点}} rx \equiv b\ (mod\ m)$$

2.

$$\left.\begin{aligned} ax &\equiv rx\ (mod\ m) \\ ax &\equiv b\ (mod\ m) \end{aligned}\right\} \xrightarrow{\text{命题 2.1 第 3 小点}} ax \equiv b\ (mod\ m)$$

由上述 1，2 可知，上述两同余式同解。

接着，我们要具体讨论一下一次同余方程组的解：

定理 3.6

一次同余方程组

$$\begin{cases} x \equiv b_1\ (mod\ m_1) \\ x \equiv b_2\ (mod\ m_2) \end{cases}$$

有解的充分必要条件为 $gcd(m_1, m_2) \mid gcd(b_1 - b_2)$，且在有解的条件下有唯一解。 ♡

证明交给感兴趣的读者。

注 当 $k > 3$ 时，对于一次同余方程组来说，可以先解得前面两个

$$x \equiv b_2'(mod\ [m_1, m_2])$$

再与 $x \equiv b_3(mod\ m_3)$ 联立解得 $x \equiv b_3'(mod\ [m_1, m_2, m_3])$

如此继续下去，最后可得唯一解

$$x \equiv b_k'(mod\ [m_1, m_2, \cdots, m_k])$$

如果中间有一步无解，则该一次同余方程组无解。

例题 3.8 解一次同余式方程组

$$\begin{cases} x \equiv 7\,(mod\,4) \\ x \equiv 10\,(mod\,8) \end{cases} \text{与} \begin{cases} x \equiv 5\,(mod\,14) \\ x \equiv 3\,(mod\,10) \end{cases}$$

解 我们一个一个看咯

1. 由于 $gcd(10,8)=2$，而 $2 \nmid 3(=7-4)$，所以由定理 3.6 知，一次同余方程组

$$\begin{cases} x \equiv 7\,(mod\,4) \\ x \equiv 10\,(mod\,8) \end{cases}$$

无解。

2. 由于 $gcd(14,10)=2$，而 $2 \mid 2(=5-3)$，所以由定理 3.6 知，一次同余方程组

$$\begin{cases} x \equiv 5\,(mod\,14) \\ x \equiv 3\,(mod\,10) \end{cases}$$

有唯一解，由 $x \equiv 5(mod\,14)$ 可得 $x=5+14y$ 带入到 $x \equiv 3(mod\,10)$ 里得到

$$5+14y \equiv 3(mod\,10) \Rightarrow 14y \equiv 8(mod\,10)$$

显然，一次同余式 $7y \equiv 2(mod\,5)$ 的唯一解为 $y \equiv 2(mod\,5)$，所以一次同余式 $14y \equiv 8(mod\,10)$ 的两个解为

$$y \equiv 2+\frac{m_2}{2}t \equiv 2+5(mod\,10), \quad (t=0,1)$$

所以，满足一次同余方程组的所有整数为

$$x=5+14(2+5t+10t')=5+28+5\times 14t+10\times 14t'$$

其中 $t=0,1$，$t'=0,\pm 1,\pm 2,\cdots$，所以，原一次同余方程组的唯一解为

$$x \equiv 33(mod\,77)$$

既然学了怎么解，我们更要学怎么来的对吧，话说呐，在我们中国古代有一本非常杀火的数学著作《孙子算经》。里面就提出过经典地解答解一次同余方程组的问题。其中一个非常有名的问题就是：

练习 3.1. 物不知其数

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?”“答曰二十三”

其实用现代数学的同余的符号，我们就可以把其编写为求解一次同余方程组：

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

《孙子算经》里所用的方法可以如下

除数	余数	最小公倍数	衍数	乘率	各总	答数	最小答数
3	2	$3\times 5\times 7=105$	5×7	2	$35\times 2\times 2$	$140+63+30=233$	$233-2\times 105=23$
5	3		7×3	1	$21\times 1\times 3$		
2	2		3×5	1	$15\times 1\times 2$		

把这个结果加以推广就是孙子定理了，在国外文献和教科书里均被称为“中国剩余定理（China Remainder Theorem）”我们用代数学把他推广成非常一般的形式便有了

定理 3.7 (中国剩余定理)

在一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

中

设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，$m = m_1 m_2 \cdots m_k = m_i M_i, i = 1, 2, \cdots, k$，则该一次同余方程组的解是

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k (mod\ m)$$

其中 $M_i' M_i \equiv 1 (mod\ m_i), i = 1, 2, \cdots, k$

♡

证明 由 $gcd(m_i, m_j) = 1, i \neq j$ 即得 $gcd(M_i, m_i) = 1$，故由同余式定理可知，即对每一 M_i，存在一 M_i' 使得

$$M_i' M_i \equiv 1 (mod\ m_i)$$

另一方面，$m = m_i M_i$，因此 $m_j \mid M_i, j \neq j$，故

$$\sum_{j=1}^{k} M_j' M_j b_j \equiv M_i' M_i b_i \equiv b_i (mod\ m_i)$$

即为该一次同余方程组的解。

若 x_1, x_2 是适合该一次同余方程组的的任意两个整数，则

$$x_1 \equiv x_2 (mod\ m_i), \quad i = 1, 2, \cdots, k$$

因而 $gcd(m_i, m_j) = 1$，于是 $x_1 \equiv x_2 (mod\ m)$，故适合该一次同余方程组的整数都属于模 m 的同一剩余类，因而该一次同余方程组的解只有

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k (mod\ m)$$

此即得证。

这个定理还提供了解一次同余方程组中（$gcd(m_i, m_j) = 1, i \neq j$ 的情形）的方法，现在我们也把它列表如下：

除数	余数	最小公倍数	衍数	乘率	各总	答数	最小答数
m_1	b_1	$m=m_1 m_2 \cdots m_k$	M_1	$M_1^{'}$	$M_1 M_1^{'} b_1$	$x \equiv \sum_{i=1}^{k} M_i M_i^{'} b_i \pmod{m}$	与x同余的模m的最小非负剩余系中的数
m_2	b_2		M_2	$M_2^{'}$	$M_2 M_2^{'} b_2$		
⋮	⋮		⋮	1	⋮		
m_k	b_k		M_k	$M_k^{'}$	$M_k M_k^{'} b_k$		

从上述的两个表可以看出，它们的算法是一致的。因此，我们完全可以说这个定理是孙子发明的。我们再聊一聊和这个孙子定理有关的小知识：

（1）首先，孙子算法卷下“今有佛书”一问，说明孙子算经的作者和孙子兵法的孙子是不同的人。

（2）秦九韶在《数书九章》中明确地系统地叙述了求解一次同余组的一般计算步骤。秦的方法，正是前述的剩余定理。我们知道，剩余定理把一般的一次同余问题归结为满足条件的一组数 K_i，的选定。秦九韶给这些数起名叫“乘率”，并且在《数书九章》卷一“大衍总术”中详载了计算乘率的方法——“大衍求一术”（定理 3.5）。两者解法很相似。

（3）南宋大数学家秦九韶则进一步开创了对一次同余式理论的研究工作，推广“物不知数”的问题。德国数学家高斯（K.F. Gauss. 公元 1777-1855 年）于公元 1801 年出版的《算术探究》中明确地写出了上述定理。公元 1852 年，英国基督教士伟烈亚士（Alexander Wylie 公元 1815-1887 年）将《孙子算经》“物不知数”问题的解法传到欧洲，公元 1874 年马蒂生（L.Mathiesen）指出孙子的解法符合高斯的定理，从而在西方的数学史里将这一个定理称为“中国的剩余定理”（Chinese remainder theorem）。

（4）这个孙子不是希腊神克洛诺斯的孙子——奎托斯（某宝鳖在这里发电）

（5）中国剩余定理表格中一些计算公式

推论 3.1

1. 衍数：$M_k = \dfrac{lcd(m_1, m_2, \cdots, m_k)}{m_k}$
2. 乘率：$M_k' = M_k \cdot b_k$
3. 各总：$M_k \cdot M_k' \cdot b_k$
4. 答数：$x \equiv \sum_{i=1}^{k} M_k\ M_k' b_k (mod\ m)$

掌握了公式，再利用表格法，可以轻而易举地解有关类似的一次同余方程组的题了。接下来的例题表格我就不画了。

例题 3.9 求一次同余方程组

$$\begin{cases} x \equiv b_1\ (mod\ 5) \\ x \equiv b_2\ (mod\ 6) \\ x \equiv b_3\ (mod\ 7) \\ x \equiv b_4\ (mod\ 11) \end{cases}$$

解 由于 $5, 6, 7, 11$ 两两互素，所以由中国剩余定理知此一次同余方程组有唯一解，此时

$m = 5\times6\times7\times11 = 2310, M_1 = 6\times7\times11 = 462, M_2 = 5\times7\times11 = 385, M_3 = 5\times6\times11 = 330, M_4 = 5\times6\times7 = 210$

又由 $M_i' M_i \equiv 1 (mod\ m_i), (1 \le i \le 4)$，可得

$$M_1' = 3, M_2' = 1, M_3' = 1, M_4' = 1$$

所以该一次同余方程组的唯一解为

$$x \equiv 3 \times 462b_1 + 385b_2 + 330b_3 + 210b_4 (mod\ 2310)$$

其实经过这些计算，我们知道中国剩余定理最重要的条件是 $m_1, m_2, \cdots, m_k$ 两两互素，当它们不是两两互素的适合就要想办法转化为两两互素。

最后我们给出一些更方便地解一次同余方程组的小技巧：

命题 3.3

1. 设 m 为正整数，且标准分解式为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，其中 $p_1 < p_2 < \cdots < p_s$，p_i 为素数 $(1 \le i \le s)$，则一次同余式

$$x \equiv a (mod\ m)$$

与一次同余方程组

$$\begin{cases} x \equiv a\ (mod\ p_1^{\alpha_1}) \\ x \equiv a\ (mod\ p_2^{\alpha_2}) \\ \cdots \\ x \equiv a\ (mod\ p_s^{\alpha_s}) \end{cases}$$

等价。

2. 设 p 为素数，且 $\alpha \ge \beta$，则该一次同余方程组

$$\begin{cases} x \equiv b_1\ (mod\ p^{\alpha}) \\ x \equiv b_2\ (mod\ p^{\beta}) \end{cases}$$

的解就是一次同余式 $x \equiv b_1 (mod\ p^{\alpha})$ 的解，即在有解的情况下它们等价。

我们来看本小节最后一道例题

例题 3.10 求一次同余方程组

$$\begin{cases} x \equiv 2\ (mod\ 35) \\ x \equiv 9\ (mod\ 14) \\ x \equiv 7\ (mod\ 20) \end{cases}$$

的所有解

解 显然，由于 $35, 14, 20$ 并不是两两互素，所以不能直接使用中国剩余定理。但是我们通过命题 3.3 的第一小点可以知道，此一次同余方程组与一次同余方程组

$$\begin{cases} x \equiv 2\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \\ x \equiv 9\ (mod\ 7) \\ x \equiv 9\ (mod\ 2) \\ x \equiv 7\ (mod\ 4) \\ x \equiv 7\ (mod\ 5) \end{cases}$$

等价，显然，去掉相同的一次同余式后，此一次同余方程组又与一次同余方程组

$$\begin{cases} x \equiv 2\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \\ x \equiv 9\ (mod\ 2) \\ x \equiv 7\ (mod\ 2^2) \end{cases}$$

等价，由于 $gcd(2^2,2)=2\mid(9-7)$，所以由命题 3.3 的第二小点可知此一次同余方程组又与一次同余方程组

$$\begin{cases} x\equiv 2\,(mod\ 5)\\ x\equiv 2\,(mod\ 7)\\ x\equiv 7\,(mod\ 4)\end{cases}$$

等价，此时我们注意到了 $5,7,4$ 两两互素，所以由中国剩余定理知，原一次同余方程组有唯一解。

因 $m=5\times 7\times 4=140, M_1=7\times 4=28, M_2=5\times 4=20, M_3=5\times 7=35$ 而由

$$M_i'M_i\equiv 1(mod\ m_i),(1\le i\le 3)$$

知 $M_1'=2, M_2'=6, M_3'=3$

$$x\equiv 2\times 28\times 2+6\times 20\times 2+3\times 35\times 7\equiv 1087\equiv 107(mod\ 140)$$

为原同余方程的唯一解。

显然，由上面的讨论，我们也看出了原一次同余方程组还与下列一次同余方程组等价

$$\begin{cases} x\equiv 2\,(mod\ 5)\\ x\equiv 2\,(mod\ 7)\\ x\equiv 3\,(mod\ 4)\end{cases}\quad\begin{cases} x\equiv 2\,(mod\ 35)\\ x\equiv 3\,(mod\ 4)\end{cases}\quad\begin{cases} x\equiv 2\,(mod\ 7)\\ x\equiv 7\,(mod\ 20)\end{cases}$$

所以在求解此类一次同余方程组时，应采取尽量减少一次同余方程组中一次同余式的个数，并使每个同余式的余数 b_i 的绝对值要小于 m_i，以达到简化运算的目的。如果我们用一次同余方程组

$$\begin{cases} x\equiv 2\,(mod\ 7)\\ x\equiv 7\,(mod\ 20)\end{cases}$$

求解一次同余方程组的时候运算量就要比用例题解答中的一次同余方程组运算小的多，这一点请读者们多多验算一下，这也是有说的道理的。

第 4 章 不定方程

终于来到了我们的最后一章，所谓的不定方程就是指未知数的个数多于方程的个数且未知数受到某种限制的方程；不定方程是数论中最古老的的一个分支，也是数论中一个十分重要的研究课题。中国古代对不定方程的研究很早，且研究内容也极为丰富，在世界数学史上占有不可忽视的地位，例如：《周髀算经》提到的商高定理“勾三股四弦五”，《九章算术》中的“五家共井”问题... 等等，堪称中外驰名，影响甚远。例如中国古代数学家张邱建曾经答了下面的题目：

“今有鸡翁一，直钱五，鸡母一，直钱三，鸡雏一，直钱一。凡百钱买鸡百只，问鸡翁、母、雏各几何?”

我们设 x, y, z 分别代表公鸡、母鸡、雏鸡的数目，就得到了下面的方程：

$$5x + 3y + \frac{1}{3}z = 100$$
$$x + y + z = 100$$

消去 z，即得：

$$7x + 4y = 100$$

我们要解决这个问题就是要求出上述方程的非负整数解。但是上述方程不过是二元一次不定方程的一个具体例子。在公元三世纪初，古希腊数学家丢番图（Diophantus）曾系统地研究了某些不定方程问题，因此不定方程也叫做丢番图方程。我们这一章的目的就是首先讨论二元一次不定方程有整数解的条件及其解法，进而讨论多元一次不定方程的解法，最后介绍几个高次不定方程。

4.1 二元一次不定方程

本节将讨论二元一次不定方程有整数解的条件，并且说明在有解的情况下，如何求出它的一切整数解。

定义 4.1 (不定方程)

形如

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$$

的方程，称为 $n(n \geq 2)$ 元一次不定方程，这里 $a_1, a_2, \cdots, a_n$ 和 N 是给定整数，并且 $a_1a_2 \cdots a_n \neq 0$ ♣

既然我们这一章是要研究二元一次不定方程，那么我们先来看一道例题。

例题 4.1 求不定方程 $3x + 5y = 45$ 的所有正整数解。

解 我们可以将式子改写成 $y = \dfrac{45 - 3x}{5}$，既然是正整数，只要保证 x, y 都是正整数就行，如果读者看到这里懂了，那么很显然把 1 到 14 都带入，即可得到当 $x = 5$ 时，$y = 6$，$x = 10$ 时，$y = 3$ 所以这个二元一次不定方程的两组正整数解就是

$$\begin{cases} x = 5 \\ y = 6 \end{cases} \quad \begin{cases} x = 10 \\ y = 13 \end{cases}$$

现在假设一个一元二次不定方程有一个整数解，说明如何借此表示出它的一切解。

定理 4.1

设二元一次不定方程

$$ax + by = c$$

(其中 $a, b, c \in \mathbb{Z}$ 且 $a, b \neq 0$) 有一整数解 $x = x_0, y = y_0$，则该一元二次不定方程的一切解可以表示成

$$x = x_0 - b_1t, \quad y = y_0 + a_1t$$

其中 $gcd(a,b)=d,\quad a=a_1d,b=b_1d,\quad t=0,\pm1,\pm2,\cdots$ ♡

我们现在来改写一下例题 4.1，并且用上述定理来试着解答。

例题 4.2 求不定方程 $3x+5y=45$ 的所有整数解。

解 我们之前就知道了，$x=5,y=6$ 是该二元一次不定方程的一个特解。而且 $gcd(3,5)=1$，则此方程的所有整数解可以写为：

$$\begin{cases} x=5-5t \\ y=6+3t \end{cases}$$

当 $t=0$ 时，$x=5,y=6$，当 $t=1$ 的时，$x=0,y=9$，当 $x=-1$ 时，$x=10,y=3$... 只要你愿意列下去就可以一直这样列下去，我们就不列了。

那么我们通过这道例题掌握了定理 4.1 的用法，确实非常方便，只要找到了一组二元一次不定方程的解，就可以得到所有解。但是这也隐含了一个麻烦，我们给出的 a 和 b 比较小，找特解比较容易，如果是二元一次不定方程的系数比较大，就不太好找了，因此我们接下来要集中精力花在找特解上。

定理 4.2

二元一次不定方程 $ax+by=c$ 有整数解的充分必要条件是 $gcd(a,b)\mid c$ ♡

我们一次性给定理 4.1 和 4.2 来个证明

证明

1. 既然 x_0,y_0 是该二元一次不定方程的一个特解，当满足 ax_0+by_0，因此

$$a(x_0-b_1t)+b(y_0+a_1t)=c+(ba_1-ab_1)t=c$$

这表明对任何任何整数 t，$x=x_0-b_1t,y=y_0+a_1t$ 都是该二元一次不定方程的解。

反之，设 x',y' 是该二元一次不定方程的任一解，则 $ax'+by'=c$，从此减去 $ax_0+by_0=c$，即得

$$a(x'-x_0)+b(y'-y_0)=0$$

由上式及 $a=a_1d,b=b_1d$ 得到

$$a_1(x'-x_0)=-b_1(y'-y_0)$$

又 $d=gcd(a,b)$，故 $gcd(a_1,b_1)=1$，可知有一整数 t，使得 $y'-y_0=a_1t$，即 $y'=y_0+a_1t$。将 y' 代入上式得 $x'=x_0-b_1t$ 因此 x',y' 只能表示成定理中所给出的形式，故可以表示为一切整数的解。

2. 若该二元一次不定方程有一整数解，设为 x_0,y_0，则 $ax_0+by_0=c$，但是 $gcd(a,b)\mid a$及b，因而 $\mid c$，故必要性获证。

反之，若 $gcd(a,b)\mid c$，则 $c=c_1gcd(a,b),c_1$ 是整数，可知存在两个整数 s,t 满足下列等式

$$as+bt=gcd(a,b)$$

令 $x_0=sc_1,y_0=tc_1$ 即得 $ax_0+by_0=c$，故该二元一次不定方程有整数解 x_0,y_0

此即得证。

我们根据上面两个定理来练一道比较综合的题目：

例题 4.3 $3x+5y=1306$ 有多少组正整数解

解 $gcd(3,5)=1\mid 1306$，所以该不定方程有正整数解。

$$3x=1306-5y\Rightarrow x=\frac{1306-5y}{3}=435+\frac{1}{3}-\frac{6y-y}{3}\Rightarrow x=435-2y+\frac{y+1}{3}$$

当 $y=-1$ 时，$x=437$，这是通解则该不定方程的一切解可以表示成

$$\begin{cases} x=437-5t \\ y=-1+3t \end{cases}\quad t\in\mathbb{Z}$$

又因为要求的是正整数解，所以 $x>0,y>0$，故

$$\begin{cases} x=437-5t \\ y=-1+3t \end{cases} \Rightarrow \frac{1}{3}<t<\frac{437}{5}=87\frac{2}{5}$$

因此 $t=1,2,\cdots,87$，所以我们将 t 值代入上式立刻可知 $3x+5y=1306$ 有 87 组正整数解。

笔记 我们可以通过以上的例题和定理总结出解二元一次不定方程 $ax+by=c$ 的整数解的步骤

1. $gcd(a,b)\mid c$ 是否成立？
2. 找 $ax+by=c$ 的特解 $\begin{cases} x=x_0 \\ y=y_0 \end{cases}$
3. 求出通解（一切解） $\begin{cases} x=x_0-b_1t \\ y=y_0+a_1t \end{cases}$

我们知道了，解二元一次不定方程的关键就是求特解。求特解的求法可根据不同情况决定。较简单的方程可用观察法直接求特解，较复杂的方程可以通过变量替换，使系数的绝对值逐步缩小，直到用观察法得到他的特解为止。但是这好累啊是不是，有的读者又要抱怨累的跟狗一样了。

你看，在有解的情况下我们要先证明方程

$$ax+by=gcd(a,b)$$

有解，因此我们要给出个特殊解的方法，应该从这个方程入手，首先上述方程的解与方程

$$\frac{a}{gcd(a,b)}x+\frac{b}{gcd(a,b)}y=1$$

的解完全相同，而在这个方程里，未知数 x,y 的系数是互素的，所以只要讨论求出形式如

$$ax+by=1,\quad gcd(a,b)=1$$

的方程的一个整数解就足够了。

综合一下上述我们给出的想法，便有了

命题 4.1

$gcd(a_1,b_1)=1$ 当且仅当方程 $a_1x+b_1y=1$ 有整数解

证明 显然，既然 $gcd(a_1,b_1)=1$，一定存在整数 s,t 使得 $a_1s+b_1t=1$，故得证。

我们再给出上述与原始二元一次不定方程的联系

推论 4.1

设 $a,b,c\in\mathbb{Z},a_1=\frac{a}{gcd(a,b)},b_1=\frac{b}{gcd(a,b)}$，则如果 $x_0=s,y_0=t$ 是方程 $a_1x+b_1y=1$ 的整数解，那么 $x_1=\frac{cs}{gcd(a,b)},y_1=\frac{ct}{gcd(a,b)}$ 是方程 $ax+by=c$ 的整数解。

其实我们也容易看出啊，由 $ax+by=1,gcd(a,b)=1$ 的一个特殊解。就可以得出 $|a|x+|b|y=1$ 的一个特殊解，反之亦然，因此为了简单起见，我们可以假定 $a>0,b>0$，应用辗转相除法，可以得到

命题 4.2

设 $gcd(a,b)=1$，则 $x_0=(-1)^{n-1}Q_n,y_0=(-1)^nP_n$ 是 $ax+by=1$ 的一个整数解，其中

$$P_0=1,P_1=q_1,P_k=q_kP_{k-1}+P_{k-2}$$

$$Q_0=1,Q_1=q_1,Q_k=q_kQ_{k-1}+Q_{k-2}$$

$$k=2,3,\cdots,n\quad q_k\text{为}a,b\text{做辗转相除法时的商的集合}$$

例题 4.4 求 $7x+4y=100$ 的一切整数解

解 先解 $7x+4y=1$，此处 $a=7,b=4,gcd(a,b)=1$

1. 我们要先求 $7x+4y=1$ 的特解

$$\begin{aligned} a=7&=\underbrace{4}_{b}\times\underbrace{1}_{q_1}+\underbrace{3}_{r_1}\\ b=4&=\underbrace{3}_{r_1}\times\underbrace{1}_{q_2}+\underbrace{1}_{r_2}\\ 3&=\underbrace{1}_{r_2}\times\underbrace{3}_{q_3}+\underbrace{0}_{r_3}\end{aligned}$$

且 $P_2=q_2P_1+P_0=1\times1=2,Q_2=q_2Q_1+Q_0=1\times1+0=1$

故 $\begin{cases} x_0=(-1)^{2-1}Q_2=(-1)\times1=(-1)\\ y_0=(-1)^2P_2=1\times2=2\end{cases}$ 是 $7x+4y=1$ 的一个整数解。

2. 由定理可知，特解为 $\begin{cases} x_0=\dfrac{cs}{gcd(a,b)}=\dfrac{100\times(-1)}{1}=-100\\ y_0=\dfrac{ct}{gcd(a,b)}=\dfrac{100\times2}{1}=200\end{cases}$

3. 通解为

$$\begin{cases} x=-100-4t\\ y=200+7t\end{cases}\quad t\in\mathbb{Z}$$

其实在中学里，我们还学过一种解二元一次不定方程的方法，我们可以抽象为

定理 4.3

设 $a,b,c\in\mathbb{Z},a>0,b>0,gcd(a,b)=1,a=bq_1+r_1,c=bq_2+r_2$，则 (x_0,y_0) 就是方程 $ax+by=c$ 的整数解，当且仅当 (x_0,y_0') 是方程 $r_1x+by=r_2$ 的整数解。这里 $y_0'=\dfrac{r_2-r_1x_0}{b}$ ♡

证明 显然，用 b 分别除 a,c 后再进行调整即得。

例题 4.5 求 $107x+37y=25$ 的一切整数解

解 由于 $gcd(107,37)=1\mid25$，故原方程有整数解。且 $y=\dfrac{25-107x}{37}=\dfrac{25-(37\times2+33)x}{37}=-2x+\dfrac{25-33x}{37}$

1. 设 $y'=\dfrac{25-33x}{37}\Rightarrow33x+37y=25$，记为 (1) 式。

$$x=\frac{25-37y'}{33}=\frac{25-(33\times1+4)y'}{33}=-y'+\frac{25-4y'}{33}$$

2. 设 $x'=\dfrac{25-4y'}{33}\Rightarrow33x'+4y'=25$，记为 (2) 式。

$$y'=\frac{25-33x}{4}=\frac{24+1-(4\times8)x'}{4}=6-8x'+\frac{1-x'}{4}$$

3. 设 $y''=\dfrac{1-x'}{4}\Rightarrow x'+4y''=1$，记为 (3) 式。

显然

$$\begin{cases} x'=1-4t\\ y''=t\end{cases}\quad t\in\mathbb{Z}$$

是 (3) 式通解。

$$y'=6-8(1-4t)+\frac{1-(1-4t)}{4}=6-8+32t+t=-2+33t$$

显然

$$\begin{cases} x'=1-4t\\ y'=-2+33t\end{cases}\quad t\in\mathbb{Z}$$

是 (2) 式通解。

$$x=-y'+\frac{25-4'}{33}=-(-2+33t)+\frac{25-4(-2+33t)}{33}=2-33t+1-4t=3-37t$$

显然

$$\begin{cases} x = 3 - 37t \\ y' = -2 + 33t \end{cases} \quad t \in \mathbb{Z}$$

是 (1) 式通解。

$y = -2x + \dfrac{25 - 33x}{37} = -2(3 - 37t) + \dfrac{25 - 33(3 - 37t)}{37} = -6 + 74t + (-2) + 33t = -8 + 107t$ 显然

$$\begin{cases} x = 3 - 37t \\ y = -8 + 107t \end{cases} \quad t \in \mathbb{Z}$$

是 $107x + 37y = 25$ 的通解。

4.2 多元一次不定方程

学会了二元，就来学学多元。

定义 4.2 (多元一次不定方程)

形如

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \quad n \geq 2$$

的方程，叫做多元一次不定方程，这里 $a_1, a_2, \cdots, a_n$ 和 N 是给定整数，并且 $a_1a_2 \cdots a_n \neq 0$ ♣

我们可以类似地把二元一次不定方程的例子推广到多元一次不定方程，那便有了

定理 4.4

$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$ 有解的充分必要条件是 $gcd(a_1, a_2, \cdots, a_n) \mid N$ ♡

证明 证明方法很显然，主要是给出一个求多元一次不定方程的方法，先顺次求出 $gcd(a_1, a_2) = d_2, gcd(d_2, a_3) = d_3, \cdots, gcd(d_{n-1}, a_n) = d_n$，若 $d_n \nmid N$，则无解，若 $d_n \mid N$，则作方程

$$a_1x_1 + a_2x_2 = d_2t_2$$

$$d_2t_2 + a_3x_3 = d_3t_3$$

$$\cdots$$

$$d_{n-2}t_{n-2} + a_{n-1}x_{n-1} = d_{n-1}t_{n-1}$$

$$d_{n-1}t_{n-1} + a_nx_n = N$$

首先求出最后一个方程的一切解，然后把 t_{n-1} 的每一个值代入倒数第二个方程求出它的一切解，这样反复下去就能得出式子的一切解。

例题 4.6 求 $9x + 24y - 5z = 1000$ 的一切解

解 不难发现 $gcd(9, 24) = 3, gcd(3, -5) = 1$，故原方程有解。考虑方程

$$9x + 24y = 3t \Rightarrow 3x + 8y = t$$

$$3t - 5z = 1000$$

由定理 4.4 给出的证明方法中的计算方法，我们可以得到

$$\begin{cases} x = 3t - 8u \\ y = -t + 3u \end{cases} \quad \begin{cases} t = 2000 + 5v \\ z = 1000 + 3v \end{cases}$$

其中 $u=0,\pm1,\pm2,\cdots,v=0,\pm1,\pm2\cdots$ 消去 t，得

$$x=6000+15v-8u$$
$$y=-2000-5v+3u$$
$$z=1000+3v$$

4.3 商高不定方程

终于来到了初等数论 I 的最后一小节，这一小节我们也要介绍研究一种特殊形式的二次不定方程，在我国古代数学书《周髀算经》中，已经载有“句广三，股修四，径隅五”（即“勾三，股四，弦五”的原始提法），这个三边是整数的直角三角形，因此已经知道了不定方程

$$x^2+y^2=z^2$$

的一组解，3，4，5. 当然这个大家都很熟悉啦，刘徽在《九章算术注》中又记载 $5^2+12^2=13^2, 8^2+15^2=17^2, 7^2+24^2=25^2, 20^2+21^2=29^2$，由此可知我国古代已经知道了 $x^2+y^2=z^2$ 的很多整数解。在古希腊，毕达哥拉斯（Pythagoras）也能找到该方程的许多整数解，因此在西方这些解也称为 Pythagoras 三元组。本节就不给出证明过程，简单的了解一下这类商高不定方程的一切解。

定义 4.3

能够作为直角三角形的三边边长的三个正整数，称为一组勾股数，也称为商高数和 Pythagoras 三元组。其中

$$x^2+y^2=z^2 \quad x,y,z\in\mathbb{Z}$$

称为商高不定方程

首先我们要做一些基础工作

引理 4.1

研究商高不定方程的整数解 (x_0,y_0,z_0) 的三个假定：

1. $x_0>0,y_0>0,z_0>0$
2. $gcd(x_0,y_0)=1$
3. x_0,y_0 一个是奇数，另一个是偶数。

证明过程请感兴趣的读者自己尝试一下。

引理 4.2

不定方程

$$uv=w^2,2>0,u>0,v>0,gcd(u,v)=1$$

的一切正整数解可以写成公式

$$u=a^2,v=b^2,w=ab,a>0,b>0,gcd(a,b)=1$$

同理，证明过程请感兴趣的读者自己尝试一下。

有了上面两个基础工作，我们便有了

定理 4.5

商高不定方程适合条件

$$x>0,y>0,z>0,gcd(a,b)=1,2\mid x$$

的一切正整数解可以用下列公式表示出来

$$x=2ab,y=a^2-b^2,z=a^2+b^2$$

其中，$a>b>0,gcd(a,b)=1,a,b$ 一奇一偶

♡

证明 显然，

$$x^2+y^2=4a^2b^2+(a^2-b^2)^2=(a^2+b^2)^2=z^2$$

$x>0,y>0,z>0,2\mid x,2\nmid y$，设 $d=gcd(x,y)$，则通过一系列公因数运算可得 $d=1$，同理，要证明其互素，也不是难事，感兴趣的读者可以自己尝试一下。

那么，我们就可以得到商高不定方程的一切解表达方式

定理 4.6 (商高不定方程的一切解)

单位圆周上的一切有理数点可以表示为

$$\left(\pm\frac{2ab}{a^2+b^2},\pm\frac{a^2-b^2}{a^2+b^2}\right)\text{及}\left(\pm\frac{a^2-b^2}{a^2+b^2},\pm\frac{2ab}{a^2+b^2}\right)$$

其中 a,b 不全为 0，$\pm$ 号可以任意取

商高不定方程的所有解为

$$(\pm2abt,\pm(a^2-b^2)t,\pm(a^2+b^2)t)\text{及}(\pm(a^2-b^2)t,\pm2abt,\pm(a^2+b^2)t)$$

♡

关于勾股数，很容易让我们联想到一个定理

定理 4.7 (Fermat 大定理)

当整数 $n>2$ 时，$x^n+y^n=z^n$ 无整数解

♡

证明 我确信已发现了一种美妙的证法，可惜这里空白的地方太小，写不下。

那么到此为止，我们初等数论 I 的内容就结束了。虽然于费马没有写下证明，而他的其它猜想对数学贡献良多，由此激发了许多数学家对这一猜想的兴趣。数学家们的有关工作丰富了数论的内容，涉及许多数学手段，推动了数论的发展。1986 年，英国数学家安德鲁 · 怀尔斯听到里贝特证明弗雷命题后，感到攻克费马大定理到了最后攻关阶段。1994 年 10 月 25 日 11 点 4 分 11 秒，怀尔斯通过他以前的学生、美国俄亥俄州立大学教授卡尔 · 鲁宾向世界数学界发送了费马大定理的完整证明邮件，包括一篇长文“模形椭圆曲线和费马大定理”，作者安德鲁 · 怀尔斯。另一篇短文“某些赫克代数的环理论性质”作者理查德 · 泰勒和安德鲁 · 怀尔斯。至此费马大定理得证。

关于数论还有许多知识等着我们探寻，我们初等数论 II 再见！

4.4 6 栋 111 备考专升本

定理 4.8 (好好复习)

$$\int_{\text{3 月 4 日}}^{\text{4 月 20 日}}f(x)\mathrm{d}x=\text{上岸}$$

♡