同余

2023 年 5 月 1 日

目录

1 同余

之前学习长除法的时候，我们的关注点是商q，而余数r不怎么关心，现在我们转过头来，我们将对给定的整数b是否是整数a的倍数感兴趣，但是对b是哪个整数的倍数不怎么感兴趣，我们从现在开始将强调余数。

如果$a, b \in Z$都是偶数，或者奇数，我们说它们同奇偶性，即：a,b同奇偶性当且仅当$a-b$是偶数，当a, b是偶数的时候，断言显然是正确的，令$a = 2n, b = 2m$。那么$2n - 2m = 2(n-m)$是个偶数。但当a, b是奇数时，我们令$a = 2n+1, b = 2m+1$则有$a - b = 2(m-n)$是偶数，反之，若$a-b$是偶数，那么a, b不可能一个是奇数一个是偶数。简单验证有$a - b = 2k$，令$a = 2n+1, b = 2m$和集合$C = \{2k|k \in Z\}$那么$2n + 1 - 2m \notin C$不是一个偶数。所以是不成立的。

1.1 定义：同余

给定整数$m \geq 0$，若对整数a, b有$m|(a-b)$，则称a, b模m同余，我们记为

$$a \equiv b(\mod m)\text{或者 } a \equiv b \mod m$$

通常我们假定$m \geq 2$，因为$m = 0, m = 1$的情况我们不是很感兴趣。若$a, b \in Z$则$a \equiv b(\mod 0)$当且仅当$0|(a-b)$当$a = b$的时候成立。所以模0的同余是等式。对于a, b，$1|(a-b)$永远成立。所以同余式$a \equiv b(\mod 1)$恒成立。

我们一般把$modulo$(模)缩写成 mod ，这个词的拉丁词根意思是“一个度量标准”，所以模在建筑学的应用就是提供一个标准。使得每个东西都是标准的m倍。

设a, b是正整数，则$a \equiv b(\mod 10)$当且仅当存在相同的末尾数字（即10和$100, 120, 130$诸如此类），一般的，$a \equiv b(\mod 10^n)$当且仅当有相同的末尾n个数字，例如$526 \equiv 1926(\mod 100)$。

我们来看一个例子：伦敦时间比芝加哥时间迟6个小时，若芝加哥时间是早上$10:00$，那么对应的伦敦时间是多少？我们知道伦敦时间 = 芝加哥时间和伦敦时间相差12小时，为此我们的关注点就是几点和芝加哥时间相差12点。然后12被自己整除，其中时钟以12为一个周期，实际上就是一个

关于模12同余的问题。那么我们有

$$10 + 6 = 16 \equiv 4 \pmod{12}$$

为此伦敦时间是下午4点。

我们给出一些和同余有着非常类似的性质。

1.2 命题

1. $a \equiv a \pmod{m}$
2. 若$a \equiv b \pmod{m}$，那么$b \equiv a \pmod{m}$
3. 若$a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$，则$a \equiv c \pmod{m}$

其中1是**自反性**，2是**对称性**，3是**对称性**

证明：$m|(a-a) = 0$所以$a \equiv a \pmod{m}$，若$m|(a-b)$，那么$m|-(a-b) = b-a$，所以$b \equiv a \pmod{m}$，对于第三个，若$m|(a-b)$和$m|(b-c)$，那么$m|(a-b)+(a-b) = a-c$，为此$a \equiv c \pmod{m}$

1.3 命题

1. 若$a = qm + r$则$a \equiv r \pmod{m}$
2. 若$0 \leq r' < r < m$，则$r \not\equiv r' \pmod{m}$
3. $a \equiv b \pmod{m}$当且仅当a, b被m除后的余数相同

证明：对于1有$a - r = qm$表明$m|(a-r)$为此a, r同余。

对于2，若有$r \equiv r' \pmod{m}$，则$m|(r-r')$，有$r - r' \geq m$，但根据定理内容有$r - r' \leq r < m$矛盾。

对于3，若$a = qm + r$，$b = q'm + r'$，其中$0 \leq r < m$和$0 \leq r' < m$，那么$a - b = (q - q')m + (r - r')$，有

$$a - b \equiv r - r' \pmod{m}$$

所以，若$a \equiv b(\mod m)$，那么$a-b \equiv 0(\mod m)$，则$r-r' \equiv 0(\mod m)$有$r = r'$。反之，若$a \equiv b(\mod m)$，那么$a-b \equiv 0(\mod m)$所以$a \equiv b \mod m$

1.4 推论

给定$m \geq 2$，则每个整数a模m同余于$0, 1, \cdots, m-1$中的某一个。

证明：由除法算式可知，$a \equiv r(\mod m)$，其中$0 \leq r < m$，即r是$0, 1, \cdots, m-1$中的某个，若a与这列数中的两个整数同余，不妨设为r和r'，则$r \equiv r'(\mod m)$，这与命题1.3的2矛盾。所以a只能与这列数中的唯一一个同余。

1.5 命题

给定整数$m \geq 0$

1. 若$a_i \equiv a_i'(\mod m), i = 1, 2, 3, \cdots, n$，则

$$a_1 + \cdots + a_n \equiv a_1' + \cdots + a_n'(\mod m)$$

特别的，若$a \equiv a'(\mod m)$，$b \equiv b'(\mod m)$，则

$$a + b \equiv a' + b'(\mod m)$$

2. 若$a_i \equiv a_i'(\mod m), i = 1, 2, 3, \cdots, n$则

$$a_1 \cdots a_n \equiv a_1' \cdots a_n'(\mod m)$$

特别的，若$a \equiv a'(\mod m), b \equiv b'(\mod m)$，那么

$$ab \equiv a'b'(\mod m)$$

3. 若$a \equiv b(\mod m)$，且对所有的$n \geq 1$有$a^n \equiv b^n(\mod m)$

证明：对于1,我们对$n \geq 2$用归纳法，若$m|(a-a')$ $m|(b-b')$，则$m|[(a-a')+(b-b')] = (a+b)-(a'+b')$，因此$a+b \equiv a'+b'(\mod m)$

由归纳假设可得假设对于$0 \leq i \leq n-1$成立，有

$$m|(a_1+\cdots+a_{n-1})-(a'_1+\cdots+a'_{n-1})$$

。若$m|(a_n-a'_n)$ 那么

$$m|(a_1+\cdots+a_{n-1})-(a'_1+\cdots+a'_{n-1})+(a_n-a'_n)=(a_1+\cdots+a_n)-(a'_1+\cdots+a'_n)$$

证毕。

对于命题2，我们对$n \geq 2$使用归纳法，对基础步骤，若$m|(a-a'), m|(b-b')$我们要证明的就是$m|ab-a'b'$，那么

$$\begin{aligned} ab-a'b' =&(ab-a'b)+(a'b-a'b') \\ =&(a-a')b+a'(b-b') \end{aligned}$$

成立，所以$m|ab-a'b' \Rightarrow ab \equiv a'b' (\mod m)$

那么，对$0 \leq i \leq n-1$的每个a_i, a'_i假设成立，有

$$\begin{aligned} a_1\cdots a_{n-1}a_n-a'_1\cdots a'_{n-1}a'_n =&[(a_1\cdots a_n)-(a'_1a_2\cdots a_n)-\cdots-(a'_1a'_2\cdots a'_{n-1}a_n)] \\ &+[(a'_1a_2\cdots a_n)+\cdots+(a'_1a'_2\cdots a'_{n-1}a_n)-(a'_1a'_2\cdots a'_n)] \\ =&a_n(a_1\cdots a_{n-1}-a'_1\cdots a'_{n-1})-a_na_{n-1}(a_1\cdots a_{n-2}-a'_1\cdots a'_{n-2}) \\ &-\cdots-a_na_{n-1}\cdots a_2(a_1-a'_1) \end{aligned}$$

由于m整除任意的$a_1\cdots a_i-a'_1\cdots a'_i$，$i=0,2,3,\cdots,n-1$。所以等式成立。
证毕。

对于命题3，令所有i都有$a_i=a$和$b_i=b$，利用命题2可知
$m|(a_1a_2\cdots a_n-a'_1a'_2\cdots a'_n)$，又因为$a_i=a, b_i=b$带入有命题3证毕。

1.5.1 例子

1. 若$a \in Z$，那么$a^2 \equiv 0,1,4 (\mod 8)$

   若a是整数，那么$a \equiv r (\mod 8)$，其中$0 \leq r \leq 7$，当我们利用命题1.5的3时可知，$a^2 \equiv r^2 (\mod 8)$，为此，该例子说明了一个事情，对于一个完全平方数被8整除后的余数只能是$0,1,4$三种

2. 对于$n=1\,003\,456\,789$不是一个完全平方数。

   因为$1000=8\cdot 125$，那么$1000 \equiv 0 (\mod 0)$，那么

$$1\,003\,456\,789=1003\,456\cdot 1000+789 \equiv 789 (\mod 8)$$

所以余数不是$0,1,4$不是一个完全平方数。

3. 对于m,n是整数，那么不存在形如3^m+3^m+1的完全平方数。

   利用刚才的例2，我们来看看模8的余数，由于$3^2=9\equiv 1(\mod 8)$，若$m=2k$，那么$3^m=3^{2k}=9^k\equiv 1(\mod 8)$，若$m=2k+1$，则$3^m=3^{2k+1}=9^k\cdot 3\equiv 3(\mod 8)$所以

$$3^m \equiv \begin{cases} 1(\mod 8) & m=2k \\ 3(\mod 8) & m=2k+1 \end{cases}$$

   所以该式子被8整除后可能会有如下几种可能

$$\begin{aligned} 3+1+1 &\equiv 5(\mod 8) \\ 3+3+1 &\equiv 7(\mod 8) \\ 1+1+1 &\equiv 3(\mod 8) \\ 1+3+1 &\equiv 5(\mod 8) \end{aligned}$$

   所以没有余数是$0,1,4$的情况，为此每个关于等式的数都不可能是完全平方数。

1.6 命题

存在无穷多个素数p满足$p\equiv 2(\mod 3)$

证明：我们利用素数是无穷多个的证明方法，我们假设只有有限个素数模3同余2，设为$p_1\cdots p_s$，那么考虑

$$m=1+p_1^2\cdots p_s^2$$

由题设有$p_i\equiv 2(\mod 3)$有$p_i^2\equiv 4\equiv 1(\mod 3)$，因为余数中还含有一个3，我们不妨把3提出来，这样子余数就是1了，那么$p_1^2\cdots p_i^2\equiv 1(\mod 3)$，那么$m\equiv 1+1=2(\mod 3)$，但对所有的$i$存在$m>p_i$，$m$不是素数，所以并不是$p_i$中的某个，而$p_i$甚至都不整除$m$。另一个方面，若我们定义$Q_i=p_1^2\cdots p_{i-1}^2p_ip_{i+1}^2\cdots p_s^2$，再做$m/Q_i$可知$m/Q_i=p_iQ_i+1$，这表明$m$被 p_i除后余数为1，我们设m的一个素分解式为$m=q_1\cdots q_t$，对每个j都有$q_j\equiv 1($

$\bmod 3)$或者$q_j \equiv 0(\mod 3)$这与我们上面得到的结论矛盾，所以存在无穷多个素数使得$p \equiv 2(\mod 3)$

1.7 命题

若p是素数，a, b是整数，则

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

我们由二项式定理可知

$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \binom{p}{r} a^{p-r} b^r$$

利用之前一个关于二项式的命题：若p是素数，则$p|\binom{p}{j}$，$0 < j < p$，那么$\binom{p}{r} \equiv 0(\mod p)$, $0 < r < p$，所以$(a+b)^p \equiv a^p + b^p(\mod p)$

1.8 费马定理

1. 若p是素数，那么对每个$a \in z$存在

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

2. 若p是素数，那么对每个$a \in Z$和每个整数$k \geq 1$ 有

$$a^{p^k} \equiv a(\mod p)$$

对1，我们假设$a \geq 0$，然后对a使用归纳法，当$a = 0$的时候是成立的，由命题1.7可知，$(1+a)^p \equiv 1 + a^p(\mod p)$

由归纳假设有$a^p \equiv a(\mod p)$，那么$(a+1)^p \equiv a^p + 1$，有$p|(a+1)^p - (a^p+1)$而由归纳假设，因为$a^p \equiv a(\mod p)$有$p|(a^p - a)$，那么$p \mid (1+a^p) - (a+1) = (a^p - a)$，所以$(a+1)^p \equiv a^p + 1 \equiv a + 1$证毕。

然后我们再考虑$-a$，其中$a \geq 0$，若$p = 2$，那么$-a \equiv a(\mod p) \Rightarrow 2|(-a-a) = -2a$成立。所以$(-a)^2 = a^2 \equiv a \equiv -a(\mod 2)$成立。因

为a^2若是奇数，那么加上a是偶数，奇数加奇数是偶数$2k+1+2x+1=2(x+k)+2$被2整除。对偶数的情况成立，为此该同余式子成立

对于第二个命题，只要对$k\geq 1$用归纳法。对于$k=1$的情况就是命题1成立。我们假设命题对a的时候成立，那么有$p|(a^{p^k}-a)$，因为

$$p|\binom{p}{r}$$
$$\Rightarrow p|\left(\binom{p}{r}\right)^k$$

那么

$$(a+1)^{p^k}\equiv a^{p^k}+1\equiv a+1$$

证毕。

1.9 推论

正整数n可以被3（或9）整除，当且仅当其（十进制）各位数字之和可以被3（或9）整除。

证明：若n的十进制形式为$d_k\cdots d_1d_0$，那么我们可以分解为

$$n=d_k10^k+\cdots+d_110+d_0$$

是平凡的。而$10\equiv 1(\mod 3)$，所以由命题1.5的3可知，对于每个i，存在$10^i\equiv 1^i=1(\mod 3)$，所以，若$3|n$，且每个10^i都存在余数1,这说明每个d_k都有$d_i10^i\equiv d_i(\mod 3)\Rightarrow 3|(d_i10^i-d_i)=d_i(10^i-1)$，为此，根据命题1.5的1，我们知道

$$n\equiv d_0+\cdots+d_k(\mod 3)$$

因此，若$3|n$，当且仅当$n\equiv 0(\mod 3)$，有$d_k+\cdots+d_1+d_0\equiv 0(\mod 3)$（由传递性得到）或者，设$r_k=d_0+\cdots+d_k$

$$3|n-0\text{和}3|n-r_k$$
$$=3|(n-0)-(n-r_k)=r_k-0$$

就有$r_k\equiv 0(\mod 3)$

为此，我们不妨把这种证法推广到关于9的结论。

1.9.1 例子：弃9法

在正整数n的十进制数字上定义两种运算

1. 除去所有的9或者任意一组总和为9的数字
2. 把所有的数字加起

这种通过重复$1,2$两种运算的方法叫弃9法。若n至少为2个数字，我们利用这种运算都可以用一个小于n的整数作为代替n进行计算，所以在运算后弃九法最终给出一个单个的数字，不妨设为$r(n)$，满足$0 \leq r(n) < 9$

例如：对于一个整数5261934我们改变为526134，现在进行第二个算法，因为$5+4=9$，那么在舍去就有$526134 \to 2613$，有$2613 \to 21$而$2+1=3$，为此我们得到了3。

推论1.9表明一个整数n的数字总和模9同余于n即$n \equiv d_0 + \cdots + d_n (\mod 9)$，利用推论1.9。对整数$n$使用法2并不能改变模9的余数。把$d_0+\cdots+d_k$写成一个整体即可。然后我们再用运算1去掉它们，剩下的整数是一个严格小于9的数$r(n)$，因为$r(n)$不是9的因子，这个时候$r(n) \equiv n (\mod 9)$是成立的。再利用推论1.4可知，$r(n)$是n中唯一模9的，这表明$r(n)$是n除9得到的余数。

藉由上述分析，我们发现可以利用这个方法检验算数是否错误。我们利用弃九法检验等式$(12345+5261944)1776 = 9367119504$是否正确。我们的思路如下：利用弃九法检验是否同余，那么$r([12345+5261944] \times 1776)$，其中 $r(12345)=6$，$r(5261934)=3$而$r(1776) \to 1+7+7+6=21 \to 3 (\mod 9)$那么$r(1776)=3$ 则，$r[6+3] \times 3 = 0$，且$r(9367119504)=0$，两边的余数都是相同的，检验通过。但是，这个诀窍不能保证计算的正确性，我们颠倒两个数字得到n'，但是$r(n')=r(n)$。所以颠倒数字不能被弃九法检测。

1.10 推论

设p是素数，n是正整数，若$m \geq 0$，且$\sum(m)$是m的$p-$进位数之和，则

$$n^m \equiv n^{\Sigma(m)} (\mod p)$$

我们设$m = d_k p^k + \cdots + d_1 p + d_0$是$m$以$p$为底数的表达式，现在由费马定理的定理2可知，对所有的i都有$n^{p^i} \equiv n(\mod p)$，那么$n^{d_i p^i} = (n^{d_i})^{p^i} \equiv n^{d_i}(\mod p)$，所以

$$\begin{aligned} n^m =& n^{d_k p^k + \cdots + d_1 p + d_0} \\ =& n^{d_k p^k} n^{d_{k-1} p^{k-1}} \cdots n^{d_1 p} n^{d_0} \\ \equiv& n^{d_k} n^{d_{k-1}} \cdots n^{d_1} n^{d_0} (\mod p) \\ \equiv& n^{d_k + \cdots + d_1 + d_0} (\mod p) \\ \equiv& n^{\Sigma(m)} \end{aligned}$$

证毕。

例子　3^{12345}被7除后的余数是多少，首先我们需要算出12345的$7-$进位数。利用长除法有

$$\begin{aligned} 12345 =& 1763 \times 7 + 4 \\ 1763 =& 251 \times 7 + 6 \\ 251 =& 35 \times 7 + 6 \\ & 355 \times 7 + 0 \\ 5 =& 0 \times 7 + 5 \end{aligned}$$

那么12345在7进制下表达为50664，即$7-$进位数为50664，那么由推论1.10有$3^{12345} \equiv 3^{5+0+6+6+4} = 3^{21}(\mod 7)$那么由于$3^{21} \equiv 3^3 = 27 \equiv 6(\mod 7)$，这说明余数为6

1.11　定理

若$(a, m) = 1$，则对每个整数b，同余式

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

对x总是有解的，(实际上$x = sb,\ \ sa \equiv 1(\mod m)$)而且，任何两个解都对模$m$同余。

我们先考虑$(a, b) = 1$的情况，其他$(a, m) \neq 1$的情况在习题中会给出。

证明 由于$(a,m)=1$，所以存在整数s满足$as\equiv 1(\mod m)$，（利用$sa+tm=1\to as-1=tm$。所以$m|(as-1)$），于是$b=sab+tmb$，所以$asb\equiv b(\mod m)$，所以$x=sb$为其中一个解。

若y是另一个解，则$ax\equiv ay(\mod m)$，所以$m|(x-y)$，而$(a,m)=1$，所以m只能去整除$x-y$，那么他俩同余，有$x\equiv y(\mod m)$

1.12 推论

若p是素数且$p\nmid a$，则$ax\equiv b(\mod p)$总是有解。

证明 由于p是素数且$p\nmid a$，所以$(a,p)=1$，那么存在整数s满足$sa+tp=1$，有$sa\equiv 1(\mod p)$，于是$b=sab+tpb$得到$x=sb$是一个解。

例子 当$(a,m)=1$时，定理1.11是在说$ax\equiv b(\mod m)$的解正好是那些形如$sb+km$的整数$k\in Z$，其中有$sa\equiv 1(\mod m)$，所以利用欧几里得算法我们就可以找到这个s，但是当m非常小的时候，我们就通过依次检查$ra=2a,3a,\cdots,(m-1)a$来找这个数s。每一步都应该检验是否有$ra\equiv 1(\mod m)$

例如，我们求

$$2x\equiv 9(\mod 13)$$

那么我们就考虑$2\cdot 2,3\cdot 2,\cdots(\mod 13)$，只需要计算下去就可以发现$7\times 2=14\equiv 1(\mod 13)$，那么$s=7$，利用之前的定理，一个解就是$x=sb=7\times 9=63$，下一步，如果有其他的解$y$，那么解关于$x\equiv y(\mod 13)$，为此，我们的目的就是找出$y$到底是啥，现在有$x=63,m=13$，那么$13|63-y\to 63-11=4\times 13$即$x\equiv 11(\mod 13)$，为此另一个解就是

$$x\equiv 11(\mod 13)$$

且解是$\cdots,-15,-2,11,24,\cdots$

又例如，求$51x\equiv 10(\mod 94)$的所有解

这里94非常大，我们不可能一个一个去求。为此，利用欧几里得算法。就有$1=-35\cdot 51+19\cdot 94$，那么一个解就是-35，算$-35\equiv y(\mod 94)$，则

$y=59$，这说明$s=59$是另一个解，为此x可以是$59\times 10=590$。那么如果同余$x\equiv y(\mod m)$，设$y=590, m=94$那么x可以表示为

$$x\equiv 590(\mod 94)$$

即形如$590+94k$的数

1.13 中国剩余定理

设整数m, m'互素，则两个同余方程

$$\begin{aligned} x\equiv & b(\mod m) \\ x\equiv & b'(\mod m') \end{aligned}$$

存在公共解，且任何两个解对模mm'同余

第一个方程的解具有形如$x=b+km,\ k\in Z$，我们只需要找到k使得$b+km\equiv b'(\mod m')$，即$km\equiv b'-b(\mod m')$，但是因为$(m,m')=1$，由定理1.11我们知道这个k是存在的。

若y是另一个公共解，则m, m'都整除$x-y$，现在给出另一个命题

命题： 若a, b都是素数且整除n，那么ab也整除n

证明：由题有$a|n$和$b|n$和$(a,b)=1$，那么设$ax=by=n$，其中因为$(a,b)=1$，那么由欧几里得引理可知，$b|x$或者$a|y$，不妨假设$y=at$，那么$n=by=bat$，即$ab|n$。

回到证明上来，由于m, m'都整除$x-y$，利用上述命题可知$mm'|x-y$，所以$x\equiv y(\mod mm')$

例子 求同余方程组

$$\begin{aligned} x&\equiv 7(\mod 8) \\ x&\equiv 11(\mod 15) \end{aligned}$$

的所有解。那么对于第一个方程，解的形式有$x=7+8k$，令

$$x=7+8k\equiv 11(\mod 15)$$

那么

$$7+8k-11=15$$
$$=8k-4=15$$
$$\rightarrow 8k\equiv 4(\mod 15)$$

利用定理1.1，那么由于$(8,15)=1$，就存在整数s满足$8s\equiv 1(\mod 15)$，有$s=2$，所以$16\equiv 1(\mod 15)$，所以就有

$$k\equiv 16k(\mod 15)$$

因为$16k\equiv 8(\mod 15)$由传递性可知$k\equiv 8(\mod 15)$ 那么$k=8$是一个解。且$x=7+8\cdot 8=71$也是问题的一个解。根据中国剩余定理，我们知道两个解是模mm'的，问题中的$m=8, m'=15$，那么就有$x-y=nmm', n\in Z$（由线性组合得到），那么$x-71=120n$即通解为$x=71+120n$

例2　解同余方程组

$$x\equiv 2(\mod 5)$$
$$x\equiv 5(\mod 13)$$

方程1具备解形式为$x=2+5k, k\in Z$带入2有

$$3(2+5k)\equiv 5(\mod 13)$$
$$15k+6\equiv 5(\mod 13)$$
$$\rightarrow 13|15k+1=13|2k+1\rightarrow 2k\equiv -1(\mod 13)$$

跟刚才一样，由于$7\times 2\equiv 1(\mod 13)$，这次我们乘7，有

$$k\equiv -7(\mod 13)$$

而$13|6+7$说明$k=6$是另一个解。就有

$$k\equiv 6(\mod 13)$$

则解具备形式$x\equiv 5k+2\equiv 5\cdot 6+2=32(\mod 65)$

对定理反例，如果我们没有假设m, m'互素，那么它可能不存在解，例如$m=m'>1$，则

$$x\equiv 0(\mod m)$$
$$x\equiv 1(\mod m)$$

是没有解的，由除法算式可得余数$r=r'$，也就不存在$0=1$这种奇怪的矛盾。

1.14 命题

设$d=(m,m')$，则系统

$$x \equiv b(\mod m)$$
$$x \equiv b'(\mod m')$$

有解当且仅当$b \equiv b'(\mod d)$

注：对于$b \equiv b'(\mod 1)$的情况永远成立。

证明 若$h \equiv b(\mod d)$，$h \equiv b'(\mod d)$，说明$m|(h-b)$和$m'|(h-b')$，由于d是m和m'的公因子，所以$d|(h-b)$和$d|(h-b')$这说明d整除h,b的线性组合，那么$(h-b)-(h-b')=b-b'$，所以$d|b-b'$，那么有$b \equiv b'(\mod d)$

反之，我们设$b \equiv b'(\mod d)$，那么存在整数k满足$b'=b+kd$，我们设$m=dc$和$m'=dc'$，现在给出一个命题来辅助证明。

命题 若$d=(a,b)$，证明a/d和b/d互素。

证明 不妨假设$a=dc$和$b=dc'$，那么$a/d=c$和$b/d=c'$，若$(a,b)\neq 1$，这说明c,c'都是可分解的，但根据欧几里得算法可知存在整数s,t使得$s(a/d)+t(b/d)=1$，这说明$(c,c')=1$互素，矛盾，为此a/d和b/d互素

回到证明上来，根据上述命题我们知道，$(c,c')=1$，所以就存在整数s,t使得$sc+tc'=1$，我们定义$h=b'sc+btc'$，那么

$$\begin{aligned} h =& b'sc+btc' \\ =&(b+kd)sc+btc' \\ =&bsc+kdsc+btc' \\ =&b(sc+tc')+kdsc \\ =&b+ksm \end{aligned}$$

我们就得到了$h \equiv b(\mod m)$，所以h是一个解，同样的，我们要得到关于模b'的解。

依然假设$b \equiv b'(\mod d)$，那么$b = b' - kd$，设$m = dc, m' = dc'$因为$(c, c') = 1$就存在整数s, t使得$sc + tc' = 1$，我们定义$h = bsc + b'tc'$

$$\begin{aligned} h =& bsc + b'tc' \\ =& (b' - kd)sc + b'tc' \\ =& b'sc - kdsc + b'tc' \\ =& b'(sc + tc') - kdsc \\ =& b' - ksm \end{aligned}$$

那么$h \equiv b'(\mod m)$，得到b, b'的同余式是同解。

例1，解线性系统

$$\begin{aligned} x \equiv 1(\mod 6) \\ x \equiv 4(\mod 15) \end{aligned}$$

这里，$m = 6, m' = 15, d = 3, c = 2, c' = 5, s = 3, t = -1$(由$1 \equiv 4(\mod 3)$)得到，利用命题1.14

$$\begin{aligned} h =& b'sc + btc' \\ =& 4 \times 3 \times 2 + 1 \times (-1) \times 5 \\ =& 19 \end{aligned}$$

2 习题

2.1 判断题

1 若a是一个整数，则$a^6 \equiv a(\mod 6)$

错，例如$2^6 - 6 = 58, 6 \nmid 58$所以是错的

2 若a是一个整数，则$a^4 \equiv a(\mod 4)$

我们依然考虑$a \geq 2$的情况，$2^4 - 2 = 14, 4 \nmid 14$所以也是错的。

3 存在整数n满足$n \equiv 1(\mod 100)$和$n \equiv 4(\mod 1000)$ 错

方程1具备解的形式如$n = 1 + 100k$，那么带入方程2有

$$\begin{aligned} 1 + 100k \equiv 4(\mod 1000) \\ 100k \equiv 3(\mod 1000) \end{aligned}$$

那么就有整数m使得解形式有$100k+1000m=3$，但左边整除100右边不整除，矛盾。所以题设是错的。

4 存在整数n满足$n\equiv 1(\mod 100)$和$n\equiv 4(\mod 1001)$

由中国剩余定理，因为$(100,1001)=1$互素，所以存在公共解。第一个方程具备解形式为$n=1+100k$，带入方程2有

$$1+100k\equiv 4(\mod 1001)$$
$$100k\equiv 3(\mod 1001)$$

由于$(100,1001)=1$，那么就存在整数s使得$100s\equiv 1(\mod 1001),s=-10$，那么$-1001|1001$，都乘$-10$，那么

$$-1000k\equiv -30(\mod 1001)$$
$$k\equiv -30(\mod 1001)$$

，所以一个解就是$x=1-3000=-2999$是一个解。且$-2999-4=-3003|1001$也是成立的。

2.2 计算

1

$$3x\equiv 2(\mod 5)$$

那么，因为$(3,5)=1$，则存在一个数s使得$3s\equiv 1(\mod 5)$，不难计算$s=2$，那么一个解就是$x=2\times 2=4$，下一步，由于$m=5,x=4$，那么存在

$$4\equiv y(\mod 5)$$

具备解形式$x=-(4+5k)$，通解为$x\equiv -4(\mod 5)$

2.3 证明

证明1： 设m是一个正整数，并设m'是由重排m的十进制数字得到的整数（例如$m=314\,159$, $m'=539114$），证明$m-m'$是9的倍数。

由推论1.9我们知道，若$9|m-m'$，那么$m-m'$的每个数字之和加起来能被9整除。我们使用弃九法，对$m-m'$的每个进位数加起来。并循环使用弃九法，这意味着

$$r(m-m')=r(m)-r(m')=0$$

因为弃九法加的是进制位，所以改变顺序不改变结果，则$r(m) = r'(m)$，所以$m - m'$使用弃九法之后得到的余数是0，这表示着$9|m - m'$，所以$m - m'$都是9的倍数。

证明2　给定正整数m，求出满足$0 < r < m$且使得$2r \equiv 0(\mod m)$的所有整数r。

由题设可知$(r, m) = r$是一定的。这意味着对于任意r，其两倍正好是m或者是m的倍数。所以对于m的倍数，只需要左边同乘倍数k，则解为$x = kr$由推论1.4可知每个数模m只能同余$0, 1, \cdots m - 1$中的某个可知，r只能是$0 \cdots, m - 1$中的某个数，所以解为$x = kr, k \in Z$

证明　证明满足$x^2 + y^2 + z^2 = 999$的整数x, y, z不存在。
利用例子1.5.1，若x是一个完全平方数，那么$x^2 \equiv 0, 1, 4 \mod 8$

这表明，若999可以表示成任意3个数的平方数，那么根据命题1.5的1有$x^2 + y^2 + z^2$同余$0, 1, 4$的各种线性组合。有那么一共有$3 \times \sum_{i=1}^{3} \binom{3}{i} = 15$种结果，即

$$000 = 0, 001 = 1, 004 = 4, 014 = 5, 041 = 5$$
$$100 = 1, 140 = 5, 104 = 5, 110 = 2, 111 = 3$$
$$400 = 4, 401 = 5, 440 = 8, 411 = 6, 444 = 12$$

这意味着

$$x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, 6, 8, 12(\mod 8)$$
$$=999 \equiv 0, 1, 2, 3, 4, 5, 6, 8, 12(\mod 8)$$

仔细验算一下发现关于减去每个同余数都不被8整除，所以999不可能表示为3个整数的平方和。