Informal Notes on Mathematics

2022.10.31

一、整除的基本性质

1. b能整除a，$b|a$；…不能，$b\nmid a$

2. 性质：(1) $1|a$；$b|0$；$a|a$ 自反性

(2) 如果 $b|a$，那么 $\pm b|\pm a$

(3) $a|b$，$b|c \Rightarrow a|c$ 传递性

(4) $a|b$，$a|c$，$\Rightarrow a|bx+cy$

(5) $a|b \Rightarrow ac|bc$

(6) 若 $a|b$，则必有 $b=0$ 或 $|b|\geq|a|$

3. 带余除法定理：$a,b\in Z$，$b>0$，那么 $\exists!\, q,r\in Z$，$a=bq+r$，其中 $0\leq r<b$

4. 最小公倍数：$[a,b]$，最大公因数：(a,b)

有 $[a,b]\cdot(a,b)=ab$

性质：(1) $(a,1)=1$，$(a,0)=|a|$，$(a,a)=|a|$

(2) $(a,b)=(b,a)=(\pm a,\pm b)=(|a|,|b|)$

(3) $(a,b)=(a-b,b)$

(3)的证明：设 $(a,b)=k$

$\therefore k|a$，$k|b$ $\therefore k|a-b$

$\therefore k$ 为 b，$a-b$ 的公约数

若 k 不是最大的，设 $k_1>k$，满足 $k_1|b$，$k_1|a-b$

$\therefore k_1|(a-b)+b$，$\therefore k_1|a$

$\therefore k_1=(a,b)$，与 $k=(a,b)$ 矛盾

$\therefore (a,b)=(a-b,b)$

(3)推论：$(a,b)=(a-qb,b)$

5. 裴蜀定理

$a,b\in Z$，不全为0，那么 $\exists\, s,t\in Z$，使得 $as+bt=(a,b)$

（数学归纳法：关于 n 的命题 $P(n)$，

第一归纳法：i $P(1)=1$，ii $P(k)=1\Rightarrow P(k+1)=1$，则P对于 $\forall n$ 为真

第二归纳法：i $P(1)=1$ ii 对于 $n\leq k$，$P(n)=1\Rightarrow P(k+1)=1$，则P对于 $\forall n$ 为真）

证明：$\because (a,b)=(b,a)=(|a|,|b|)$ $\therefore$ 不妨设 $a\geq b\geq 0$，不全为0

对 $a+b$ 进行第二归纳法

(i) $a+b=1$ 时，$a=1$，$b=0$ $\therefore (a,b)=1=a\cdot1+b\cdot0$，成立

(ii) 若对于 $a+b\leq k$，命题成立，考虑 $a+b=k+1$

① $b=0$，$a=k+1$，$(a,b)=k+1=a\cdot1+b\cdot0$，成立

② $b\neq0$ $\therefore b\geq1$ $\therefore 1\leq a\leq k$

$(a,b)=(a-b,b)=(a-b)s_1+bt_1$

$=as_1+b(t_1-s_1)$，成立

$\therefore$ 成立。

6. 高级性质

(1) $(a,b)=1$，且 $a|bc$， 则 $a|c$

证明：$\because (a,b)=1$

$\therefore \exists s,t\in Z$， $as+bt=1$

$\therefore asc+btc=c$，即 $sc\cdot a+tc\cdot b=c$

又$\because a|a$， $a|bc$

$\therefore a|asc+btc$，即 $a|c$

(2) $a|c$，$b|c$，且 $(a,b)=1$，则 $ab|c$

证明：$\because (a,b)=1$

$\therefore \exists s,t\in Z$， $as+bt=1$

$\therefore asc+btc=c$，即 $s\cdot ac+t\cdot bc=c$

$\because a|c$ $\therefore ab|bc$ $\because b|c$ $\therefore ab|ac$

$\therefore ab|c$

(3) $(a^m-1, a^n-1)=a^{(m,n)}-1$

证明：对 $m+n$ 进行归纳，不妨设 $m\geq n\geq 0$ 且不全为0

(i) $m+n=1$ $\therefore m=1, n=0$

$\therefore (a^m-1, a^n-1)=(a-1, 0)=0=a^0-1$ 成立

(ii) 设 $m+n\leq k$ 时，成立，下面证明由此可得 $m+n=k+1$ 时成立

① $n=0$ $\therefore m=k+1$

$\therefore$ 同(i)可证

② $n\geq 1$ $\therefore m\leq k$

$(a^m-1, a^n-1)=(a^m-a^n, a^n-1)=(a^n(a^{m-n}-1), a^n-1)$

$\because (a^n, a^n-1)=1$ $\therefore (a^m-a^n, a^n-1)=(a^{m-n}-1, a^n-1)$

$\because (m-n)+n=m\leq k$ $\therefore$ 由假设得，$(a^{m-n}-1, a^n-1)=a^{(m-n,n)}-1=a^{(n,n)}-1$

$\therefore (a^m-1, a^n-1)=a^{(m,n)}-1$

$n\in N^*$， $x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1})$

n为奇数， $x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+\cdots-xy^{n-2}+y^{n-1})$

第一课时 整除的基本性质

整除理论是初等数论的基础，它是对在小学就学过的关于整数的算术，主要是涉及除法运算的内容，作抽象的、系统的总结，在讨论中不能涉及分数. 这看起来似乎很简单，但是它的内涵是十分重要和深刻的.

一、知识梳理

1. 设$a,b\in Z$，如果存在$q\in Z$，使得$a=bq$，那么称b整除a，记为$b\mid a$. 否则，若q不存在，那么称b不整除a，记作$b\nmid a$.

2.（带余除法定理）设$a,b\in Z$，且$b>0$，那么存在唯一的$q,r\in Z$，使得$a=bq+r$，其中$0\le r<b$.

3. 最大公因数与最小公倍数：

（1）设a_1,a_2是两个不全为零的整数，如果$d\mid a_1$且$d\mid a_2$，那么d就称为a_1和a_2的公约数，我们把a_1和a_2的公约数中的最大的称为a_1和a_2的最大公约数，记做(a_1,a_2). 若$(a_1,a_2)=1$，则称a_1和a_2是既约的，或是互素的.

(2) 设a_1,a_2是两个均不为零的整数，如果$a_1\mid l$，且$a_2\mid l$，那么l就称为a_1和a_2的公倍数，我们把a_1和a_2的公倍数中的最小的称为a_1和a_2的最小公倍数，记做$[a_1,a_2]$.

4.（裴蜀定理）设$a,b\in Z$，且不全为0，那么存在$s,t\in Z$，使得$as+bt=(a,b)$.

二、经典例题

例1　已知$x,y\in Z$，且$3\mid 4x-y$，求证：$9\mid 4x^2+7xy+7y^2$.

证明：$4x^2+7xy+7y^2$

$=(4x-y)(x+2y)+9y^2$

$\because x+2y=4x-y-3(x-y)$

$\therefore 3\mid x+2y$

$\therefore 9\mid(4x-y)(x+2y)$

$\therefore 9\mid 4x^2+7xy+7y^2$

例2　求最大的正整数n，使得$n+10\mid n^3+201$

解：$n^3+2016=(n+10)(n^2-10n+100)+1016$

$\because n+10\mid n^3+2016$

$\therefore n+10\mid 1016$

$\therefore n$最大为1006

可直接用 $n+10\mid n^3+10^3$

$\therefore n+10\mid 1016$

例 3　给定正整数 a,b，对任意的正整数 k，（$k\neq b$）都有 $(b-k)\mid(a-k^2)$，求证：$a=b^2$．

解：$\begin{cases}(b-k)\mid(b^2-k^2)\\(b-k)\mid(a-k^2)\end{cases}$

$\therefore (b-k)\mid(a-b^2)$

$\therefore a-b^2=0$

$\therefore a=b^2$

例 4　设 m,n 为正整数，$m>2$．证明：$(2^m-1)\nmid(2^n+1)$．

证明：当 $m>n$ 时，$2^m-1>2^n+1$，显然 $2^m-1\nmid 2^n+1$

当 $m\le n$ 时，$\because 2^m-1\mid 2^{mt}-1^t$，$t\geq 1$

假设 $2^m-1\mid 2^n+1$，则 $2^m-1\mid 2^{mt}+2^t$

$\therefore$ 上式对 $\forall t\geq 1$ 成立

$\therefore 2^m-1=1$ 或 $2^{mt}+2^t=0$，均舍

$\therefore (2^m-1)\nmid(2^n+1)$

$m=n$ 时，若 $2^m-1\mid 2^m+1$，

则 $2^m-1\mid 2$

又 $\because m>2$ $\therefore 2^m-1>3$

$\therefore$ 不成立

$m<n$ 时，设 $n=mq+r$

$\therefore 2^n+1=2^{mq}\cdot 2^r+1=(2^{mq}-1)\cdot 2^r+2^r+1$

$\therefore$ 由于已经证明的结论，$2^m-1\mid 2^{mq}-1$，

$2^m-1\nmid 2^r+1$　$\therefore 2^m-1\nmid 2^n+1$

综上，命题得证

例 5　计算：$(2^{200}-1,2^{88}-1)$．

解：$\because 2^{200}-1=(2^8)^{25}-1^{25}$，$2^{88}-1=(2^8)^{11}-1^{11}$

$\therefore 2^8-1\mid 2^{200}-1$，$2^8-1\mid 2^{200}-1$

$\because 8=(200,88)$

$\therefore 2^8-1=(2^{200}-1,2^{88}-1)$

$\therefore (2^{200}-1,2^{88}-1)=255$

运用结论 $(2^m-1,2^n-1)=2^{(m,n)}-1$

例 6　正整数 a,b,c,d 满足 $ab=cd$，求证：$a+b+c+d$ 不是质数．

证明：$a=\dfrac{cd}{b}$

$\therefore a+b+c+d$

$=\dfrac{cd}{b}+c+d+b$

$=\dfrac{(b+c)(b+d)}{b}$

假设 $\dfrac{(b+c)(b+d)}{b}=p$，$p\in P$

$\therefore p\mid(b+c)(b+d)$

$\therefore p\mid b+c$ 或 $p\mid b+d$

若 $p\mid b+c$，则 $b+c=0$（舍）

或 $p\le b+c$

$\therefore \dfrac{(b+c)(b+d)}{b}\le b+c$

$b+d\le b$

$d\le 0$

与 $d>0$ 矛盾 $\therefore p\nmid b+c$

同理 $p\nmid b+d$

$\therefore$ 假设不成立

$\therefore a+b+c+d$ 不是质数

证明：设 $(a,c)=m$

$\therefore m\mid a$，$m\mid c$

设 $a=mx$，$c=my$

$\therefore (x,y)=1$

$\therefore xb=yd$

$\therefore x\mid yd$　$\therefore x\mid d$

$\therefore$ 设 $d=nx$

$\therefore xb=nxy$

$ny=b$

$\therefore a+b+c+d=mx+ny+my+nx$

$=(m+n)(x+y)$

$\therefore a+b+c+d$ 不是质数

三、巩固练习

1. 设 a、b、c、d 为整数，$a-c\mid ab+cd$，则 $a-c\mid ad+bc$.

解 $\because (ab+cd)-(ad+bc)$

$= a(b-d)-c(b-d)$

$=(a-c)(b-d)$

$\therefore a-c\mid (ab+cd)-(ad+bc)$

又 $\because a-c\mid ab+cd$

$\therefore a-c\mid ad+bc$

2. 设 a、b 都是正整数，a^2+ab+1 被 b^2+ab+1 整除. 证明：$a=b$.

证明：$\because b^2+ab+1\mid a^2+ab+1$

$b^2+ab+1\mid b^2+ab+1$

$\therefore b^2+ab+1\mid a^2-b^2$

$\because b^2+ab+1=b(a+b)+1 \nmid a+b$ 应换成证明 $(b(a+b)+1,\ a+b)=1$

$\therefore b^2+ab+1\mid a-b$

$\because b^2+ab+1=b(a+b)+1>b(a+b)>a-b$

$\therefore a-b=0$，即 $a=b$

3. 证明：对任意整数 n，$n^6+2n^5-n^2-2n$ 能被 120 整除.

证明：$n^6+2n^5-n^2-2n$

$=\cancel{(n-1)\ (n^5)}\ n^6+2n^5-(n^2+2n)$

$=(n+2)(n^5-n)$

根据费马小定理，$p\mid n^p-n$

$\therefore 5\mid n^6+2n^5-n^2-2n$

$\because n^5-n=n(n^4-1)=(n^2+1)(n^3-n)$

$\therefore 3\mid n^6+2n^5-n^2-2n$

$\because n(n^2-1)=(n^2-n)(n+1)$

$\therefore 2\mid n^6+2n^5-n^2-2n$

连续n个整数一定能被n!整除.

$\because 120=3\times5\times8$

$\therefore$ 只需证 $8\mid n^6+2n^5-n^2-2n$

~~若n为偶数，~~

~~则 $n^6+2n^5-n^2-2n$~~

$\cancel{=(n+2)(n^2+1)(n^2-n)(n+1)}$

$\because n^6+2n^5-n^2-2n$

$=n(n-1)(n+1)(n+2)(n^2+1)$

$\because$ 其中 $n-1, n, n+1, n+2$ 为连续4个整数

$\therefore 8\mid n^6+2n^5-n^2-2n$

$\therefore 120\mid n^6+2n^5-n^2-2n$

$n^6+2n^5-n^2-2n$

$=n(n-1)(n+1)(n+2)(n^2+1)$

$=(n-1)n(n+1)(n+2)(n^2-4+5)$

$=(n-1)n(n+1)(n+2)(n-2)+5(n-1)n(n+1)(n+2)$

$\because (n-1)n(n+1)(n+2)$ 为连续4整数

$\therefore 24\mid n^6+2n^5-n^2-2n$

又 $\because 5\mid n^6+2n^5-n^2-2n$

$\therefore 120\mid n^6+2n^5-n^2-2n$

又 $\because (n-2)(n-1)\cdots(n+2)$ 为连续5整数

$\therefore 5\mid (n-2)\cdots(n+2)$

$\therefore 5\mid n^6+2n^5-n^2-2n$

4. 设 m、n 是正整数，m 是奇数，证明：$(2^m-1, 2^n+1)=1$.

法②：设 $(2^m-1, 2^n+1)=d$

$\therefore 2^m=da+1,\ 2^n=db-1$

$\therefore (da+1)^n=(db-1)^m$

$\therefore db^m-C_m^1 db^{m-1}+C_m^2 db^{m-2}+\cdots-1$

$=da^n+C_n^1 da^{n-1}+\cdots+1$

$\therefore dA-1=dB+1$

$\therefore d(A-B)=2$

$\therefore d\mid 2$ 又 $\because 2^m-1, 2^n+1$ 均为奇

$\therefore d\neq2$ $\therefore d=1$ $\therefore$ 得证

证明：设 $(2^m-1, 2^n+1)=k$

$\therefore k\mid 2^m-1,\quad k\mid 2^n+1$

又 $\because 2^n+1\mid 2^{nt}+1 \rightarrow 2^m-1\mid 2^{mt}-1$

$\therefore k\mid 2^{mt}+2^{nt},\ t\in N_+$

$\because m$ 为奇数 $\therefore k=1$ 或 $2^{mt}+2^{nt}=0$（舍）

$\therefore k=1$ $\therefore (2^m-1, 2^n+1)=1$

法①：证明：$\because m$ 为奇数 $\therefore (2^n)^m+1^m$ 可被 2^n+1 整除

$\therefore 2^n+1\mid 2^{mn}+1$ 又 $\because 2^m-1\mid 2^{mn}-1$

$\therefore (2^m-1, 2^n+1)\mid 2^{mn}+1$

$\because 2^m-1, 2^n+1$ 均为奇数

$\therefore 2\nmid (2^m-1, 2^n+1)$

$\therefore (2^m-1, 2^n+1)=1$

5. 设 a、m、n 都是正整数，$a>1$ 且 $a^m+1\mid a^n+1$. 证明: $m\mid n$.

证明: $(a^m+1^m, a^n+1^n)=a^{(m,n)}+1^{(m,n)}$

并无此结论

∵ $a^m+1 \mid a^n+1$

∴ $a^m+1 \le a^{(m,n)}+1$

∴ $m \le (m,n)$

∵ $(m,n)\le m$

∴ $m=(m,n)$

∴ $m\mid n$

证明: ∵ $a^m+1\mid a^n+1$

∴ $a^m+1\le a^n+1$

∴ $m\le n$

不妨设 $n=mq+r$

∴ $a^m+1\mid a^{mq+r}+1$

∵ $a^m+1\mid a^n+1$

∴ $a^m+1\mid a^n-a^m$

$a^m+1\mid (a^{n-m}-1)a^m$

∴ $a^m+1\mid a^{n-m}-1$

同理 $a^m+1\mid a^{n-2m}-1$

$a^m+1\mid a^{n-3m}-1$

......

∴ $a^m+1\mid a^{n-qm}-1$

即 $a^m+1\mid a^r-1$

∵ $0\le r<m$

∴ $a^m+1>a^r-1$

∴ $a^r-1=0$, $r=0$

即 $m\mid n$

6. 是否存在两个不同的正整数 a,b，使得 $[a,a+7]=[b,b+7]$?

解: $(a,a+7)=(a+7,a)=(7,a)$

∴ $(a,a+7)=1$ 或 7

i $7\nmid a$, $7\nmid b$ 或 $7\mid a$, $7\mid b$

∴ $a(a+7)=b(b+7)$

∵ $(a,a+7)=(b,b+7)=1$或7, $a\ne b$

∴ $a=b+7$, $a+7=b$, 舍

ii $7\nmid a$, $7\mid b$

∴ $a(a+7)=\frac{b(b+7)}{7}$

∴ $b=\frac{1}{2}(\sqrt{7}\sqrt{4a^2+28a+7}-7)$

∵ b为整数

∴ $7\mid 4a^2+28a+7$

∴ $7\mid 4a^2$

又∵ $7\nmid a$

∴ $7\nmid 4a^2$, 矛盾

∴ 舍

iii $7\mid a$, $7\nmid b$

同(ii), 舍。

综上, 不存在

ii $7\nmid a$, $7\mid b$

∴ $7\mid b$, $7\mid b+7$

∴ $7\mid \frac{b(b+7)}{7}$

又∵ $(a+7)a=\frac{b(b+7)}{7}$

$7\nmid a(a+7)$

∴ $(a+7)a=\frac{b(b+7)}{7}$ 无整数解

∴ 不存在

7. 求所有的正整数 a、b、c $(a<b<c)$，使得其中任意两个数的和加 1 都能被第三个数整除.

解: $\begin{cases} a+b+1=k_1c \\ a+c+1=k_2b \\ b+c+1=k_3a \end{cases}$

又∵ $a<b<c$

∴ $a+b+1\le 2b<2c$

∴ $k_1=1$

∴ $1+a+(a+b+1)=k_2b$

∴ $2a+2=(k_2-1)b$

∵ $2a+2\le 2b$

∴ $k_2=2$或3

∴ i $k_2=2$

∴ $\begin{cases} a+c+1=2b \\ a+b+1=c \end{cases}$

∴ $b+c+1=2a+c+2=\cancel{5a+b}$

∴ $2a+c+2=k_3a$

∴ $a=\frac{6}{k_3-5}$为正整数

∴ $k_3=6,7,8,11$

∴ $(a,b,c)=(3,8,12),(2,6,9),(1,4,6),(6,14,21)$

ii $k_2=3$

∴ $\begin{cases} a+c+1=3b \\ a+b+1=c \end{cases}$

∴ $b+c=\frac{5}{3}a+\frac{2}{3}c+\frac{2}{3}$

$\ge \frac{7}{3}a+2$

又∵ $b+c=a+2b+1$

$\ge 3a+3$

∴ $k_3\ge 3$, $a=\frac{4}{k_3-3}$为正整数

∴ $k_3=4,5,7$

∴ $(a,b,c)=(4,5,10),(2,3,6),(1,2,4)$

综上, (a,b,c)为$(3,8,12),(2,6,9),(1,4,6),(4,5,10),(2,3,6),(1,2,4),(6,14,21)$