Chap 1. 初等数论

§1.1 整除性和唯一因子分解

一. 整除性

def 1.1 设 $a,b\in\mathbb{Z}$, $a\neq 0$, 若 $\exists c\in\mathbb{Z}$, 使得 $b=ac$, 则称 a 整除 b, 记作 $a|b$, 并称 a 为 b 的一个因子（或约数）而 b 叫做 a 的倍数。
否则称 a 不整除 b, 表示成 $a\nmid b$.

Lemma 1.2. (1) 若 $a|b$, $b|c$, 则 $a|c$

(2) $a|b$ 且 $b|a$ $\Longleftrightarrow$ $a=\pm b$

(3) 若 $a|b$, $a|c$, 则对 $\forall x,y\in\mathbb{Z}$, 有 $a|bx+cy$

def 1.3 对实数 α, $[\alpha]$ 表示不超过 α 的最大整数, 叫做 α 的整数部分.
而 $\alpha-[\alpha]$ 叫做 α 的分数部分, 表示成 $\{\alpha\}$

因而, $\forall\alpha\in\mathbb{R}$, α 可唯一表示成: $\alpha=[\alpha]+\{\alpha\}$, $[\alpha]\in\mathbb{Z}$, $0\leq\{\alpha\}<1$

Thm 1.4 (带余除法) 设 $a,b\in\mathbb{Z}$, $b\geq 1$, 则存在唯一确定的 $q,r\in\mathbb{Z}$,
使得: $a=qb+r$, $0\leq r<b$

事实上, $q=[\frac{a}{b}]$

Lemma 1.5 设 S 是一个非空集合, 并满足以下两个条件:

(A) 若 $a,b\in S$, 则 $a\pm b\in S$

(B) 若 $a\in S$, 则对每个 $x\in\mathbb{Z}$, 均有 $ax\in S$

则存在唯一的整数 $d\geq 0$, 使得 S 是由 d 的所有倍数构成的, 即
$$S=d\mathbb{Z}=\{dy \mid y\in\mathbb{Z}\}$$

证明：(1) 若 $S=\{0\}$，则取 $d=0$ 即可

(2) 若 S 包含非零整数 a，则由条件 (A) 可知：$0=a-a\in S$

又 $-a=0-a\in S$，故 S 中必包含正整数 (a or $-a$)

令 d 是 S 中的最小正整数，下证 $S=d\mathbb{Z}$

由条件 (B) 可知：$\forall x\in\mathbb{Z}$，有 $dx\in S$　　$\therefore d\mathbb{Z}\subseteq S$

另一方面，对 $\forall a\in S$，由带余除法：$\exists\, q, r\in\mathbb{Z}$，使 $a=dq+r$，

$0\le r<d$

又 $a, d\in S$，由条件 (A)，$r=a-dq\in S$，但 $0\le r<d$

又 d 为 S中 最小正整数，　$\therefore r=0$

即 $a=qd\in d\mathbb{Z}$　　$\therefore S\subseteq d\mathbb{Z}$

从而 $S=d\mathbb{Z}$，且 d 为 S 中最小正整数，从而唯一。 #

定义 1.6　设 p 是大于 1 的整数，如果 p 的正因子只有 1 和 p，则称 p 是素数（也叫质数）。

定理 1.7　（欧几里得）素数有无穷多个。

证：（反证法）（有可能是历史上第一次使用反证法）

首先，素数是存在的。

进而，假设只有有限个素数 $p_1, p_2, \cdots, p_s$　$(s\ge 1)$

则对 $n=p_1p_2\cdots p_s+1\ge 2$，必有素因子 p

但 $p_i\nmid n$　$(i=1,\cdots,s)$　　则 p 为不同于 $p_1,\cdots,p_s$ 的素数

矛盾，故假设不成立。

$\therefore$ 素数有无穷多个。 #

二. 最大公因子和最小公倍数

概念：设 $a_1, a_2, \cdots, a_n$ $(n\geq 2)$ 是不全为零的整数.

① 则它们的公因子（公约数）只有有限个，其最大公因子记为 $(a_1, a_2, \cdots, a_n)$

若 $(a_1, a_2, \cdots, a_n)=1$，称这组数是互素的.

② 它们有正的公倍数，存在最小的正的公倍数，记为 $[a_1, a_2, \cdots, a_n]$，称为最小公倍数.

性质：

Lemma 1.8　设 a 和 b 是不全为零的整数，则

(1) $(a,b)=(b,a)$.　$(a,b)=(|a|,b)$

(2) 当 $a\neq 0$ 时，$(a,a)=|a|$

(3) 对 $\forall k\in\mathbb{Z}$，$(a,b)=(a, b+ak)$

由(3)可以得到求最大公因子的辗转相除法.

Thm 1.9　设 $a_1, a_2, \cdots, a_n$ 是不全为零的整数，$d=(a_1, a_2, \cdots, a_n)$，则对任意整数 l，不定方程 $a_1x_1+a_2x_2+\cdots+a_nx_n=l$ (*) 有整数解当且仅当 $d\,|\,l$.

证：令 $S=\{a_1x_1+a_2x_2+\cdots+a_nx_n \mid x_i\in\mathbb{Z}, i=1,2,\cdots,n\}$

则 S 为使 (*) 有整数解的所有整数 l 组成的集合.

$S\neq\varnothing$ 且 S 包含正整数（若 $a_i\neq 0$，则 a_i 及 $-a_i$ 都属于 S，即 $|a_i|\in S$）

$\therefore S$ 满足 Lemma 1.5 的条件. 故 $\exists k\in\mathbb{Z}$，且 $k>0$，使得 $S=k\mathbb{Z}$

$\because d=(a_1, a_2, \cdots, a_n)$　$\therefore d\,|\,a_1x_1+\cdots+a_nx_n$

又 $k\in k\mathbb{Z}=S$.　$\therefore d\,|\,k$

若$d\leq k$，$\because a_1,\cdots,a_n\in S$　$\therefore k|a_i$　$i=1,2,\cdots,n$

$\therefore k\leq d$

$\therefore k=d$.　从而$S=d\mathbb{Z}$　即$d|l$　#

性质：

Lemma 1.10　设$a_1,a_2,\cdots,a_n$是不全为零的整数.

(1) $a_1,a_2,\cdots,a_n$的每个公因子都是它们最大公因子的因子.

(2) 若$a_1\neq 0$，则$(a_1,a_2,\cdots,a_n)=((a_1,a_2),a_3,\cdots,a_n)$

(3) 对于$m\in\mathbb{Z}^+$，$m(a_1,a_2,\cdots,a_n)=(ma_1,ma_2,\cdots,ma_n)$

(4) 若$(a_1,a_2,\cdots,a_n)=d$，则$(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d})=1$

(5) 对于$m\in\mathbb{Z}$，若$(a_i,m)=1$.$(i=1,\cdots,n)$，则$(a_1a_2\cdots a_n,m)=1$

(6) 若$a.b.c\in\mathbb{Z}$，$c\neq 0$，$c|ab$，$(c,b)=1$，则$c|a$.

特别地，对素数p，若$p|ab$，则$p|a$或$p|b$.

证：(1) 记$d=(a_1,a_2,\cdots,a_n)$.则由Thm 1.9可知：

$\exists x_1,x_2,\cdots,x_n\in\mathbb{Z}$，使得$d=a_1x_1+a_2x_2+\cdots+a_nx_n$

若d'是$a_1,a_2,\cdots,a_n$的公因子.则$d'|a_1x_1+\cdots+a_nx_n$

即$d'|d$

(2) 设$d=(a_1,a_2,\cdots,a_n)$.　$d'=((a_1,a_2),a_3,\cdots,a_n)$

则d'是$a_1,a_2,\cdots,a_n$的公因子　由(1)，有　$d'|d$

又d是$a_1,\cdots,a_n$的公因子，$\therefore d|(a_1,a_2)$

$\therefore d$是$(a_1,a_2),a_3,\cdots,a_n$的公因子，由(1)，有$d|d'$

综上，$d=d'$

(3) 记 $d=(a_1,a_2,\cdots,a_n)$. $e=(ma_1,ma_2,\cdots,ma_n)$

则 md 是 ma_i 的公因子. $\therefore md\mid e$

另一方面, 由Thm 1.9. $\exists x_1,x_2,\cdots,x_n\in\mathbb{Z}$. 使得 $a_1x_1+\cdots+a_nx_n=d$

$\therefore (ma_1)x_1+(ma_2)x_2+\cdots+(ma_n)x_n=md$

再由Thm 1.9. 可知 $e\mid md$

综上 $md=e$

(4) $\because (a_1,a_2,\cdots,a_n)=d$ $\therefore \frac{a_i}{d}\in\mathbb{Z}$. $i=1,2,\cdots,n$

由(3)可知: $d(\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d})=(a_1,a_2,\cdots,a_n)=d$

$\therefore (\frac{a_1}{d},\frac{a_2}{d},\cdots,\frac{a_n}{d})=1$

(5) 当 $n=2$ 时, 设 $a_1,a_2\in\mathbb{Z}$. 有 $(a_1,m)=1$, $(a_2,m)=1$

由Thm 1.9. $\exists x,y$ 和 x',y', 使得: $a_1x+my=1$, 和 $a_2x'+my'=1$

$\therefore 1=(a_1x+my)(a_2x'+my')=a_1a_2xx'+a_1xmy'+mya_2x'+m^2yy'$

$=a_1a_2(xx')+m(a_1xy'+a_2x'y+myy')$

其中 xx', $a_1xy'+a_2x'y+myy'\in\mathbb{Z}$

由Thm 1.9. $(a_1a_2,m)\mid 1$ 从而 $(a_1a_2,m)=1$

由数学归纳法可知: 若 $(a_i,m)=1$. 则 $(a_1a_2\cdots a_n,m)=1$

$$\left.\begin{matrix}(a_1,m)=1,\ (a_2,m)=1 \Longrightarrow (a_1a_2,m)=1 \\ (a_3,m)=1\end{matrix}\right\}\Rightarrow (a_1a_2a_3,m)=1 \Rightarrow \cdots\cdots$$

(6) $\because (c,b)=1$ $\therefore$ 由Thm 1.9. $\exists x,y\in\mathbb{Z}$. 使 $bx+cy=1$

又 $c\mid ab$ $\therefore c\mid (ab)x+a(cy)=a(bx+cy)=a$

特别地, 对素数 p. 若 $p\mid ab$. 但 $p\nmid a$. 则 $(p,a)=1$. $\therefore p\mid b$

类似, 若 $p\mid ab$ 但 $p\nmid b$. 则 $p\mid a$.

#

Lemma 1.11 设 $a_1, a_2, \cdots, a_n$ 均是非零整数.

(1) $a_1, \cdots, a_n$ 的每个公倍数都是它们最小公倍数的倍数;

(2) $[a_1, a_2, \cdots, a_n] = [[a_1, a_2], a_3, \cdots, a_n]$

(3) 对于 $m \in \mathbb{Z}^+$, $[ma_1, ma_2, \cdots, ma_n] = m[a_1, a_2, \cdots, a_n]$

(4) 设 $a, b \in \mathbb{Z}$, $ab \neq 0$. 则 $(a,b)[a,b] = |ab|$

(5) 若 $a_1, a_2, \cdots, a_n$ 两两互素, 则 $[a_1, a_2, \cdots, a_n] = |a_1 a_2 \cdots a_n|$

证: (1) 记 S 为 $a_1, a_2, \cdots, a_n$ 的所有公倍数组成的集合

则 $S \neq \phi$, 且 $[a_1, a_2, \cdots, a_n] \in S$

若 $a, b \in S$. 则 $a_i | a$ 且 $a_i | b$ $\quad \because a_i | (a \pm b)$ $\therefore a \pm b \in S$

若 $a \in S$. 则对 $\forall x \in S$. ax 是 $a_1, a_2, \cdots, a_n$ 的公倍数. 即 $ax \in S$

由Lemma 1.5. $\exists d \in \mathbb{Z}^+$ 使得 $S = d\mathbb{Z}$, d 为 S 中的最小正整数.

$\therefore d = [a_1, a_2, \cdots, a_n]$

若 m 为 $a_1, a_2, \cdots, a_n$ 的倍数. 则 $m \in S = d\mathbb{Z}$ $\quad \therefore d | m$.

即 m 为 $[a_1, a_2, \cdots, a_n]$ 的倍数

(2) 记 $d = [a_1, a_2, \cdots, a_n]$. $d' = [[a_1, a_2], a_3, \cdots, a_n]$

$\because d'$ 是 $a_1, a_2, \cdots, a_n$ 的倍数. 由(1) $d | d'$

又 d 是 $a_1, a_2, \cdots, a_n$ 的公倍数. $\therefore$ $[a_1, a_2] | d$

即 d 是 $[a_1, a_2], a_3, \cdots, a_n$ 的公倍数, 由(1). $d' | d$

综上, $d = d'$

(3) 记 $d = [a_1, a_2, \cdots, a_n]$, $e = [ma_1, ma_2, \cdots, ma_n]$

$\because a_i | d$ $\quad \therefore ma_i | md$ $\quad$ 由(1). $e | md$

另一方面．e 是 ma_i 的倍数．$\therefore \frac{e}{m}$ 是 a_i 的倍数．$(\frac{e}{m}\in\mathbb{Z})$

$\therefore d\mid\frac{e}{m}$ $\therefore md\mid e$

综上：$e=md$

(4) 不妨设 $a,b\in\mathbb{Z}^+$

① 若 $(a,b)=1$．

由最小公倍数的定义．$\exists x,y\in\mathbb{Z}$，使 $ax=[a,b]=by$

$\therefore b\mid ax$，又 $(a,b)=1$．由 Lemma 1.10，$b\mid x$ $\therefore ab\mid ax=[a,b]$

又 ab 是 $a.b$ 的倍数．$\therefore [a,b]\mid ab$

综上 $ab=[a,b]=[a,b]\cdot 1=[a,b](a,b)$

② 对于一般情形，记 $d=(a,b)$．$d\neq 1$．则由 Lemma 1.10 (4)．

有 $(\frac{a}{d},\frac{b}{d})=1$．

由①可知：$[\frac{a}{d},\frac{b}{d}]=\frac{a}{d}\cdot\frac{b}{d}=\frac{ab}{d^2}$

由③．$[a,b]=d[\frac{a}{d},\frac{b}{d}]=d\cdot\frac{ab}{d^2}=\frac{ab}{d}$

$\therefore ab=[a,b]d=(a,b)[a,b]$

(5) 当 $n=2$ 时，$(a_1,a_2)=1$．由(4)，有 $(a_1,a_2)[a_1,a_2]=|a_1a_2|$

$\therefore [a_1,a_2]=|a_1a_2|$

当 $n=3$ 时．$(a_1,a_3)=1$，$(a_2,a_3)=1$ 由 Lemma 1.10 (5)．

有 $(a_1a_2,a_3)=1$，从而

$[a_1,a_2,a_3]=[[a_1,a_2],a_3]=[|a_1a_2|,a_3]=|a_1a_2a_3|$

由数学归纳法可知：若 $(a_i,a_j)=1$．$1\leq i,j\leq n$ 且 $i\neq j$

则 $[a_1,a_2,\cdots,a_n]=|a_1a_2\cdots a_n|$

#

定理1.9 给出多元一次方程存在整数解的充要条件. 对于二元情形, 可以给出 $ax+by=n$ 的全部整数解的表达式。

不妨设 $a,b\in\mathbb{Z}^*$ （若 $a\neq 0$, $b=0$. 则 $ax=n$ 有整数解 $\Leftrightarrow a\mid n$ ）

令 $d=(a,b)$. 由Thm 1.3 可知: 当 $d\nmid n$ 时, $ax+by=n$ (*) 无整数解。而当 $d\mid n$ 时, 令 $a=a'd$, $b=b'd$, $n=n'd$, $a',b',n'\in\mathbb{Z}^*$ 且原方程(*)等价于 $a'x+b'y=n'$ 其中 $(a',b')=1$. 从而二元一次方程讨论整数解的情况归结为未知量的系数互素的情形.

Thm 1.12 设 a, b 为非零整数, 且 $(a,b)=1$. 则对 $\forall n\in\mathbb{Z}$. 方程 $ax+by=n$ 均有解.
并且若 $(x,y)=(x_0,y_0)$ 是方程的一组整数解. 则该方程的所有整数解为:

$$\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases} \quad t\in\mathbb{Z}$$

证: 由Thm 1.9. 可知. $ax+by=n$ 必有整数解 $(x,y)=(x_0,y_0)$.

即 $ax_0+by_0=n$

则对任意整数解 (x,y). 有 $ax+by=n$

则 $0=(ax+by)-(ax_0+by_0) = a(x-x_0)+b(y-y_0)$

$\therefore a(x-x_0)=-b(y-y_0)$ $\quad\because (a,b)=1$. $\quad\therefore b\mid x-x_0$

$\therefore \exists t\in\mathbb{Z}$, 使得 $x-x_0=bt$. 即 $x=x_0+bt$

$\therefore -b(y-y_0)=abt$ $\quad\therefore y-y_0=-at$ $\quad\therefore y=y_0-at$

特解

$\therefore$ 整数解 (x,y) 的形式为 $\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases}$ $t\in\mathbb{Z}$

反过来, 易验证 $\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases}$, $t\in\mathbb{Z}$ 表示的 (x,y) 是原方程的整数解.

例1. 求 $60x-14y=18$ 的全部整数解.

解: $\because (60,-14)=2$, 而 $2\mid 18$ $\therefore$ 方程有整数解.

简化原方程: $30x-7y=9$,

求 $(30,7)$ 的辗转相除法:

$\because 30=4\times7+2$ $(2=30-4\times7)$ $\therefore (30,7)=(7,2)$

$\therefore 7=3\times2+1$ $(1=7-3\times2)$ $\therefore (7,2)=(2,1)=1$

反推: $1=(30,7)=1\times7-3\times2=1\times7-3\times(30-4\times7)$

$=-3\times30+13\times7=-3\times30+(-13)\times(-7)$

$\therefore (x,y)=(-3,-13)$ 是 $30x-7y=1$ 的一组整数解

$\therefore (x,y)=(-27,-117)$ 是 $30x-7y=9$ 的一组整数解

$\therefore$ 原方程的全部整数解为: $\begin{cases} x=-27-7s \\ y=-117-30s \end{cases}$ $s\in\mathbb{Z}$

即 $\begin{cases} x=-27+7t \\ y=-117+30t \end{cases}$ $t\in\mathbb{Z}$ (即 $t=-s$)

例2. 求 $18x+30y+45z=48$ 的全部整数解.

解: $\because (18,30,45)=3$, 而 $3\mid 48$. $\therefore$ 原方程有整数解.

简化原方程: $6x+10y+15z=16$ (1)

$\because (10,15)=5$, 从而 $\{10y+15z \mid y,z\in\mathbb{Z}\}=5\mathbb{Z}$ (由Thm1.9的证明)

$\therefore$ 方程(1) 等价于 $\begin{cases} 10y+15z=5w \\ 6x+5w=16 \end{cases}$ 即 $\begin{cases} 2y+3z=w & (2) \\ 6x+5w=16 & (3) \end{cases}$

方程 $2y+3z=1$ 有整数解 $(y,z)=(-1,1)$ (不唯一)

$\therefore$ 方程(2) 有整数解 $(y,z)=(-w,w)$

∴ 对 $\forall w\in\mathbb{Z}$，方程(2)的所有整数解为：$\begin{cases} y=-w+3t \\ z=w-2t \end{cases}$，$t\in\mathbb{Z}$ (4)

又方程(3)有整数解：$(x,w)=(1,2)$.

∴ 方程(3)的所有整数解为：$\begin{cases} x=1+5s \\ w=2-6s \end{cases}$. $s\in\mathbb{Z}$ (5)

将(5)代入(4)，得原方程的全部整数解为：

$$\begin{cases} x=1+5s \\ y=-2+6s+3t \\ z=2-6s-2t \end{cases},\quad t,s\in\mathbb{Z}$$

三. 唯一因子分解定理 —— 初等数论的基石

Thm 1.13 （Euclid） 每个大于1的整数均可分解为有限个素数的乘积，并且若不计素数因子在分解式中的次序，则这种分解式是唯一的.

证：(1) 存在性 （对 n 进行归纳）

$n=2$ 时 $n=1\times 2$ 命题正确

假设对 $2,3,\cdots,n-1$，命题均成立.

则对 n：① 若 n 为素数，则 $n=1\times n$ 命题成立

② 若 n 不是素数，则 $n=ab$，$a,b\in\mathbb{Z}$，且 $0<a,b<n-1$

由归纳假设可知，a,b 均为有限个素数的乘积

从而 $n=ab$ 也是有限个素数的乘积. 命题正确

综上，对任意大于1的整数，均可分解为有限个素数的乘积.

(2) 唯一性：

设 $n=p_1p_2\cdots p_s=q_1q_2\cdots q_r$，其中 $p_1,\cdots,p_s,q_1,\cdots,q_r$ 均为素数

则 $p_1|n=q_1q_2\cdots q_r$ $\therefore p_1$ 整除某个 q_i

从而 $p_2\cdots p_s=q_1\cdots q_{i-1}q_{i+1}\cdots q_r$

继续，则有 $s=r$，且 $\{q_1,q_2,\cdots,q_r\}$ 是 $\{p_1,p_2,\cdots,p_s\}$ 的一个置换

从而唯一性获证. #

由Thm 1.13. 每个 ≥ 2 的整数 n 均可表示成 $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ (*).

其中 p_i $(i=1,2,\cdots,s)$ 是不同的素数. 且 $e_i\geq 1$，该表达式叫做 n 的标准分解式。如果固定 $p_1,p_2,\cdots,p_s$ 的一种顺序，比如 $p_1<p_2<\cdots<p_s$，则分解式(*)是唯一的.

求两个非零整数 a 和 b 的最大公因子或最小公倍数，不妨假设

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\quad.\quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}\qquad (1)$$

其中 $p_1,p_2,\cdots,p_k$ 是不同的素数，此时 α_i. β_i 可以取 0.

Cor 1.14 设正整数 a 和 b 有形如(1)的分解式，则

(1) $a|b \iff \alpha_i\leq\beta_i\quad(1\leq i\leq k)$

(2) $(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$，其中 $\gamma_i=\min\{\alpha_i,\beta_i\}$

(3) $[a,b]=p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}$，其中 $\delta_i=\max\{\alpha_i,\beta_i\}$

证：(1) 若 $a|b$，则 $b=ac$，$c\in\mathbb{Z}^+$，且 $c=p_1^{\lambda_1}\cdots p_k^{\lambda_k}q_1^{\mu_1}\cdots q_s^{\mu_s}$.

其中 $p_1,\cdots,p_k,q_1,\cdots,q_s$ 是互不相同的素数，$\lambda_i,\mu_j\in\mathbb{Z}^+$

由 $b=ac$ 可知：

$$p_1^{\beta_1}\cdots p_k^{\beta_k}=p_1^{\alpha_1}\cdots p_k^{\alpha_k}p_1^{\lambda_1}\cdots p_k^{\lambda_k}q_1^{\mu_1}\cdots q_s^{\mu_s}$$

$$=p_1^{\alpha_1+\lambda_1}\cdots p_k^{\alpha_k+\lambda_k}q_1^{\mu_1}\cdots q_s^{\mu_s}$$

由唯一因子分解定理，可知：$\beta_i=\alpha_i+\lambda_i\geq\alpha_i \quad (1\leq i\leq k)$

反之，若 $\beta_i\geq\alpha_i$. $(1\leq i\leq k)$，则

$$\frac{b}{a}=p_1^{\beta_1-\alpha_1}\cdots p_k^{\beta_k-\alpha_k}\in\mathbb{Z} \qquad \therefore a|b$$

(2) 设正整数 d 是 a 和 b 的公因子，则 $d=p_1^{u_1}\cdots p_k^{u_k}$

d 为 a 和 b 的公因子 $\overset{(1)}{\iff}$ $u_i\leq\alpha_i$ 且 $u_i\leq\beta_i \quad (1\leq i\leq k)$

$\iff u_i\leq\min\{\alpha_i,\beta_i\}$

$\therefore d=p_1^{\nu_1}\cdots p_k^{\nu_k}$ 是 a,b 的最大公因子 $\iff \nu_i=\min\{\alpha_i,\beta_i\}$

(3) 类似(2)可以证明.