整除相关性质:

$a|a$

$a|b \quad b|a \Rightarrow a=\pm b$

$a|b. \quad b|c \Rightarrow a|c$

$a|b. \Rightarrow a|bc$

$a|b, a|c \Rightarrow a|xb+yc$

$a.b>0. \ a|b \Rightarrow \begin{cases} b\geq a \\ b=a \text{或} \ b\geq 2a \end{cases}$

$\forall c\neq 0 \quad a|b \Leftrightarrow ac|bc$

最大公约数 $gcd(a,b)$ [可写作(a,b)]的相关性质.

1.裴蜀定理: $d=(a.b) \Rightarrow \exists \ s,t\in\mathbb{Z} \quad s.t \quad d=sa+tb$

证明见"上集"

注:此处 $s.t$ 不唯一, $d=sa+tb \rightarrow d=(s-b)a+(t+a)b$

加限制 $s\in\{0,1,\cdots,b-1\}$ 有: $d=(s-\frac{b}{d})a+(t+\frac{a}{d})b$ 很在此限制下有$\frac{b}{d}$个组合对

再加限制: $1\leq s<\frac{b}{d}$

注:下面这些看起来显然的,都需要证明!!! 以下主要用我们已有的裴蜀公式证明

2. $a,b,c\in\mathbb{Z}$, $m\in N^+$ 有 $(ma,mb)=m(a,b)$

特别的: $\begin{cases} (a.b)=d \Rightarrow (\frac{a}{d},\frac{b}{d})=1 \\ c|a, \ c|b \Rightarrow c|(a.b) \end{cases}$ $[(d\frac{a}{d},d\frac{b}{d})=d \Rightarrow (\frac{a}{d},\frac{b}{d})=1$

$(a.b)=d$ 则 $(c\cdot\frac{a}{c},c\cdot\frac{b}{c})=d \Rightarrow c\underbrace{(\frac{a}{c},\frac{b}{c})}_{\in N^+}=d\Rightarrow c|d$

证:由裴蜀 $(ma,mb)=\min\{sma+tmb\}$

$=\min\{m(sa+tb)\}$

其中, $m\in N^+$, $s,t\in\mathbb{Z}$

原式 $=m\cdot\min\{sa+tb\}$

$=m(a,b)$

3. $(a, c)=1, \ (b, c)=1 \Rightarrow (ab, c)=1$

证：由裴蜀：$\exists\ s, t, m, n$ s.t $\begin{cases} sa+tc=1 & ① \\ mb+nc=1 & ② \end{cases}$

①×②：$\underbrace{sm}_{x}ab + (\underbrace{tmb+sna+ntc}_{y})c = 1$

所 $\exists\ x, y \in \mathbb{Z}$, s.t $\ xab+yc=1 \Rightarrow (ab, c)=1$

4. $(a, b) = (a, b+ac)$

$A = \{xa+yb \mid x, y \in \mathbb{Z}\}$

$= \{a(x+yc)+yb \mid x, y \in \mathbb{Z}\}$

$= \{xa+y(b+ac) \mid x, y \in \mathbb{Z}\}$

$\therefore \min^{+}\{xa+yb\} = \min^{+}\{xa+y(b+ac)\} \Rightarrow (a, b) = (a, b+ac)$

5. $c \mid ab, \ (c, a)=1 \Rightarrow c \mid b$

$(c, a)=1 \Rightarrow \ \exists\ s, t$ s.t. $sc+ta=1$

$\Rightarrow scb+tab=b$

而 $c \mid ab \Rightarrow \exists k$ s.t $ab=kc \Rightarrow LHS=(sb+kt)c$ 有 $c \mid LHS=b$

6. $a \mid c, \ b \mid c, \ (a, b)=1 \Rightarrow ab \mid c$

$(a, b)=1 \Rightarrow sa+tb=1$

$a \mid c, \ b \mid c \Rightarrow \exists\ k, m \in \mathbb{Z}$ s.t $c=ka=mb$

有：$sac+tbc=c$

$\Rightarrow samb+tbka=c \qquad ab \mid (sm+tk)ab=c$

6'：更一般的：证 $a|c$，$b|c$，$(a,b)=d$，$\Rightarrow \frac{ab}{d} \mid c$

$(a,b)=d \Rightarrow \exists\ s,t$，$sa+tb=d$

$a|c$，$b|c \Rightarrow \exists\ k,m\in\mathbb{Z}$ s.t $c=ka=mb$

$sac+tbc=dc$

$\Rightarrow samb+tbka=(sm+tk)ab=dc \Rightarrow \frac{ab}{d} \mid c$.

则所有 $\frac{ab}{d}$ 可以整除 a,b 的公倍数，先有 $\frac{ab}{d} \mid \mathrm{lcm}(a,b)$.

$\frac{ab}{\gcd(a,b)} = \mathrm{lcm}(a,b)$

再证 $a \mid \frac{ab}{d}$，$b \mid \frac{ab}{d}$：$\exists\ x,y$ s.t $\begin{cases} a=xd \\ b=yd \end{cases}$

$\Rightarrow \frac{ab}{d} = xdy = ay = xb$. 则 $\frac{ab}{d}$ 是 a,b 的公倍数 $\Rightarrow \frac{ab}{d} \geq \mathrm{lcm}(a,b)$

7. 辗转相除法 $\Rightarrow (a,b)=(a,b+ka)$ $k\in\mathbb{Z}$，保证欧几里德算法是有效的

减 $-ka$ 可一直减小

a,b，$a\geq b>0$

$a=q_0b+r_0$ $\quad 0<r_0<b$ $\quad \rightarrow r_0 = a-q_0b$

$b=q_1r_0+r_1$ $\quad 0<r_1<r_0$ $\quad (r_0,b)=(a-q_0b,b)=(a,b)$ 其 gcd 是相同的.

$r_0=q_2r_1+r_2$ $\quad 0<r_2<r_1$

$\vdots$

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

$r_{n-1}=q_{n+1}r_n$ $\quad (a,b)=r_n$