最大公因数的一些性质.

Lemma：对$\forall\, a,b\in\mathbb{Z}$，$\forall n\in\mathbb{Z}_{\geq 1}$，有：$\gcd(a^n,b^n)=(\gcd(a,b))^n$

Proof：当a,b全为0时，$a=0$且$b=0$ $\therefore a^n=0$且$b^n=0$

$\therefore \gcd(a^n,b^n)=\gcd(0,0)=0$，$\gcd(a,b)=\gcd(0,0)=0$

$\therefore (\gcd(a,b))^n=0^n=0$. $\therefore$结论成立.

当a,b不全为0时，a^n与b^n不全为0. $\therefore \gcd(a,b)\in\mathbb{Z}_{\geq 1}$，$\gcd(a^n,b^n)\in\mathbb{Z}_{\geq 1}$.

$\therefore \gcd(a,b)\mid a$ 且 $\gcd(a,b)\mid b$ $\therefore \frac{a}{\gcd(a,b)}\in\mathbb{Z}$，$\frac{b}{\gcd(a,b)}\in\mathbb{Z}$

$\therefore \left(\frac{a}{\gcd(a,b)}\right)^n\in\mathbb{Z}$，$\left(\frac{b}{\gcd(a,b)}\right)^n\in\mathbb{Z}$ $\therefore \frac{a^n}{(\gcd(a,b))^n}\in\mathbb{Z}$，$\frac{b^n}{(\gcd(a,b))^n}\in\mathbb{Z}$

$\because a,b\in\mathbb{Z}$，$a,b$不全为0

$$\therefore \gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

$$\because \frac{a}{\gcd(a,b)}\in\mathbb{Z},\ \frac{b}{\gcd(a,b)}\in\mathbb{Z},\ \frac{b}{\gcd(a,b)}\in\mathbb{Z},\ \gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

$$\therefore \gcd\left(\frac{a}{\gcd(a,b)},\left(\frac{b}{\gcd(a,b)}\right)^2\right)=\gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

$$\because \frac{a}{\gcd(a,b)}\in\mathbb{Z},\ \left(\frac{b}{\gcd(a,b)}\right)^2\in\mathbb{Z},\ \frac{b}{\gcd(a,b)}\in\mathbb{Z},\ \gcd\left(\frac{a}{\gcd(a,b)},\left(\frac{b}{\gcd(a,b)}\right)^2\right)=1$$

$$\therefore \gcd\left(\frac{a}{\gcd(a,b)},\left(\frac{b}{\gcd(a,b)}\right)^3\right)=\gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

$$\because \frac{a}{\gcd(a,b)}\in\mathbb{Z},\ \left(\frac{b}{\gcd(a,b)}\right)^3\in\mathbb{Z},\ \frac{b}{\gcd(a,b)}\in\mathbb{Z},\ \gcd\left(\frac{a}{\gcd(a,b)},\left(\frac{b}{\gcd(a,b)}\right)^3\right)=1$$

$$\therefore \gcd\left(\frac{a}{\gcd(a,b)},\left(\frac{b}{\gcd(a,b)}\right)^4\right)=\gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

……

$\because \frac{a}{\gcd(a,b)} \in \mathbb{Z}$, $\left(\frac{b}{\gcd(a,b)}\right)^{n-1} \in \mathbb{Z}$, $\frac{b}{\gcd(a,b)} \in \mathbb{Z}$, $\gcd\left(\frac{a}{\gcd(a,b)}, \left(\frac{b}{\gcd(a,b)}\right)^{n-1}\right) = 1$

$$\therefore \gcd\left(\frac{a}{\gcd(a,b)}, \left(\frac{b}{\gcd(a,b)}\right)^{n}\right) = \gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

$$\therefore \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \frac{a}{\gcd(a,b)}\right) = 1$$

$\because \left(\frac{b}{\gcd(a,b)}\right)^{n} \in \mathbb{Z}$, $\frac{a}{\gcd(a,b)} \in \mathbb{Z}$, $\frac{a}{\gcd(a,b)} \in \mathbb{Z}$, $\gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \frac{a}{\gcd(a,b)}\right) = 1$

$$\therefore \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{2}\right) = \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \frac{a}{\gcd(a,b)}\right) = 1$$

$\because \cancel{\gcd}\ \left(\frac{b}{\gcd(a,b)}\right)^{n} \in \mathbb{Z}$, $\left(\frac{a}{\gcd(a,b)}\right)^{2} \in \mathbb{Z}$, $\frac{a}{\gcd(a,b)} \in \mathbb{Z}$, $\gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{2}\right) = 1$

$$\therefore \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{3}\right) = \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \frac{a}{\gcd(a,b)}\right) = 1$$

$\because \left(\frac{b}{\gcd(a,b)}\right)^{n} \in \mathbb{Z}$, $\left(\frac{a}{\gcd(a,b)}\right)^{3} \in \mathbb{Z}$, $\frac{a}{\gcd(a,b)} \in \mathbb{Z}$, $\gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{3}\right) = 1$

$$\therefore \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{4}\right) = \gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \frac{a}{\gcd(a,b)}\right) = 1$$

将上述过程继续下去，可得：

$\gcd\left(\left(\frac{b}{\gcd(a,b)}\right)^{n}, \left(\frac{a}{\gcd(a,b)}\right)^{n}\right) = 1$ $\quad\therefore \gcd\left(\left(\frac{a}{\gcd(a,b)}\right)^{n}, \left(\frac{b}{\gcd(a,b)}\right)^{n}\right) = 1$

$$\therefore \gcd\left(\frac{a^n}{(\gcd(a,b))^n}, \frac{b^n}{(\gcd(a,b))^n}\right) = 1$$

$\because \gcd(a,b) \in \mathbb{Z}_{\geq 1}$ $\quad\therefore (\gcd(a,b))^n \in \mathbb{Z}_{\geq 1}$ $\quad\because \left(\frac{a}{\gcd(a,b)}\right)^{n} \in \mathbb{Z}$, $\left(\frac{b}{\gcd(a,b)}\right)^{n} \in \mathbb{Z}$

$$\therefore (\gcd(a,b))^n \cdot \gcd\left(\left(\frac{a}{\gcd(a,b)}\right)^{n}, \left(\frac{b}{\gcd(a,b)}\right)^{n}\right) = \gcd\left((\gcd(a,b))^n \cdot \left(\frac{a}{\gcd(a,b)}\right)^{n}, (\gcd(a,b))^n \cdot \left(\frac{b}{\gcd(a,b)}\right)^{n}\right)$$

$$\therefore (\gcd(a,b))^n \cdot \gcd\left(\frac{a^n}{(\gcd(a,b))^n}, \frac{b^n}{(\gcd(a,b))^n}\right) = \gcd\left((\gcd(a,b))^n \cdot \frac{a^n}{(\gcd(a,b))^n}, (\gcd(a,b))^n \cdot \frac{b^n}{(\gcd(a,b))^n}\right)$$

$$\therefore (\gcd(a,b))^n \cdot 1 = \gcd(a^n, b^n)$$

$$\therefore \gcd(a^n, b^n) = (\gcd(a,b))^n \qquad \square$$

Lemma: $a, b \in \mathbb{Z}$, $\gcd(a,b)=1$, 则有: 对 $\forall\, n, m \in \mathbb{Z}_{\geq 1}$, 有: $\gcd(a^n, b^m) = 1$

Proof: $\because a, b, b \in \mathbb{Z}$, $\gcd(a,b)=1$ $\quad \therefore \gcd(a, b^2) = \gcd(a,b) = 1$

$\because a, b^2, b \in \mathbb{Z}$, $\gcd(a, b^2) = 1$ $\quad \therefore \gcd(a, b^3) = \gcd(a,b) = 1$

$\because a, b^3, b \in \mathbb{Z}$, $\gcd(a, b^3) = 1$ $\quad \therefore \gcd(a, b^4) = \gcd(a,b) = 1$

将上述过程继续下去, 可得: $\gcd(a, b^m) = 1$ $\quad \therefore \gcd(b^m, a) = 1$

$\because b^m, a, a \in \mathbb{Z}$, $\gcd(b^m, a) = 1$ $\quad \therefore \gcd(b^m, a^2) = \gcd(b^m, a) = 1$

$\because b^m, a^2, a \in \mathbb{Z}$, $\gcd(b^m, a^2) = 1$ $\quad \therefore \gcd(b^m, a^3) = \gcd(b^m, a) = 1$

$\because b^m, a^3, a \in \mathbb{Z}$, $\gcd(b^m, a^3) = 1$ $\quad \therefore \gcd(b^m, a^4) = \gcd(b^m, a) = 1$

将上述过程继续下去, 可得: $\gcd(b^m, a^n) = 1$

$\therefore \gcd(a^n, b^m) = 1 \qquad \square$

Lemma: $a, b \in \mathbb{Z}_{\geq 1}$, $\gcd(a,b) = 1$, $c \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$, $ab = c^n$, 则有:

$$a = (\gcd(a,c))^n, \quad b = (\gcd(b,c))^n$$

~~Proof: 当n=0时, 此时有: $c \in \mathbb{Z}$ 且 $c \neq 0$ $\because a, b \in \mathbb{Z}_{\geq 1}$ $\therefore ab \in \mathbb{Z}_{\geq 1}$~~

~~$\therefore c^n = ab \in \mathbb{Z}_{\geq 1}$ $\quad \therefore c \neq 0$ (假设 $c=0$, 则有: $ab = c^n = 0^n = 0$. 矛盾).~~

~~当n=0时,~~

Proof：假设 $c=0$．则有以下两种可能：

(i)．$n=0$．此时 $c^n=0^0$ 无意义．矛盾．

(ii) $n\in\mathbb{Z}_{\geqslant 1}$．此时 $c^n=0^n=0$． $\therefore ab=c^n=0$ $\therefore a=0$ 或 $b=0$．

$\because a\in\mathbb{Z}_{\geqslant 1}$ 且 $b\in\mathbb{Z}_{\geqslant 1}$ $\therefore$ 矛盾．

$\therefore c\neq 0$． $\therefore c\in\mathbb{Z}$ 且 $c\neq 0$．

分如下的情况讨论：

① $n=0$．此时 $c^n=c^0=1$． $\therefore ab=1$． $\because a\in\mathbb{Z}_{\geqslant 1}$ 且 $b\in\mathbb{Z}_{\geqslant 1}$

$\therefore a=1$ 且 $b=1$．

$\therefore (\gcd(a,c))^n=(\gcd(1,c))^0=1=a$．

$(\gcd(b,c))^n=(\gcd(1,c))^0=1=b$ $\therefore$ 结论成立．

② $n=1$．此时 $ab=c^1=c$ $\therefore c=ab=ba$， $a\in\mathbb{Z}_{\geqslant 1}$， $b\in\mathbb{Z}_{\geqslant 1}$

$\therefore a\mid c$ 且 $b\mid c$．

$\therefore \gcd(a,c)=a$， $\gcd(b,c)=b$

$\therefore a=\gcd(a,c)=(\gcd(a,c))^1$， $b=\gcd(b,c)=(\gcd(b,c))^1$．结论成立．

③ $n\geqslant 2$．此时 $n-1\geqslant 1$ $\therefore n-1\in\mathbb{Z}_{\geqslant 1}$

$\because a,b\in\mathbb{Z}_{\geqslant 1}$， $\gcd(a,b)=1$ $\therefore \gcd(a^{n-1},b)=1$， $\gcd(a^n,b)=1$

$\because a^n,b,a\in\mathbb{Z}$， $\gcd(a^n,b)=1$ $\therefore \gcd(a^n,ba)=\gcd(a^n,a)=\gcd(a,a^n)=a$

这里用到了a是正整数这条件

$\therefore a=\gcd(a^n,ba)=\gcd(a^n,ab)=\gcd(a^n,c^n)=(\gcd(a,c))^n$

$\because a,b\in\mathbb{Z}_{\geqslant 1}$， $\gcd(a,b)=1$ $\therefore \gcd(a,b^{n-1})=1$， $\gcd(a,b^n)=1$

$\therefore \gcd(b^n,a)=1$

$\because b^n,a,b\in\mathbb{Z}$， $\gcd(b^n,a)=1$ $\therefore \gcd(b^n,ab)=\gcd(b^n,b)=\gcd(b,b^n)=b$

这里用到b是正整数这个条件．

$\therefore b=\gcd(b^n,ab)=\gcd(b^n,c^n)=(\gcd(b,c))^n$． $\square$