Problem 1

(a)记

$$a=30,b=22$$

利用欧几里得除法可得:

$$\begin{aligned}30&=1\times 22+8\Rightarrow 8=30-22=a-b\\22&=2\times 8+6\Rightarrow 6=22-2\times 8=b-2\times(a-b)=-2a+3b\\8&=1\times 6+2\Rightarrow 2=8-6=a-b-(-2a+3b)=3a-4b\\6&=3\times 2+0\end{aligned}$$

所以

$$\gcd(30,22)=2=3a-4b=3\times 30-4\times 22$$

(b)注意到

$$2=(3-22k)\times 30+(-4+30k)\times 22$$

取$k=1$可得

$$2=-19\times 30+26\times 22$$

所以

$$y'=26$$

Problem 2

(a)

$$\begin{aligned}\gcd(m,n)&=2^3 11^7 17^9\\\mathrm{lcm}(m,n)&=2^9 5^{24} 7^{22} 11^{211} 13^1 17^{12} 19^2\end{aligned}$$

不难验证有

$$\gcd(m,n).\,\mathrm{lcm}(m,n)=mn$$

(b)假设m,n的分解如下:

$$m=\prod_{i=1}^{d}p_i^{m_i}$$
$$n=\prod_{i=1}^{d}p_i^{n_i}$$

其中$n_i,m_i\ge 0,p_i$为质数，那么

$$
\gcd(m,n)=\prod_{i=1}^{d} p_i^{\min\{m_i,n_i\}}
$$

$$
\operatorname{lcm}(m,n)=\prod_{i=1}^{d} p_i^{\max\{m_i,n_i\}}
$$

Problem 3

(a)我们将证明

$$
e\times\gcd(x,y)=\gcd(a,b)
$$

如果该性质成立，那么因为结束时

$$
\gcd(x,y)=\gcd(1,0)=1
$$

所以

$$
e=\gcd(a,b)
$$

下面证明这点：

start state：

$$
e\times\gcd(x,y)=1\times\gcd(a,b)=\gcd(a,b)
$$

transitions：

(2)

$$
2e\times\gcd(\frac{x}{2},\frac{y}{2})=2e\times\frac{\gcd(x,y)}{2}=e\times\gcd(x,y)=\gcd(a,b)
$$

(3)(4)情形类似，只证明(3)

$$
e\times\gcd(\frac{x}{2},y)=e\times\gcd(x,y)=\gcd(a,b)
$$

(5)(6)情形类似，只证明(5)

$$
e\times\gcd(x-y,y)=e\times\gcd(x,y)=\gcd(a,b)
$$

(7)

$$
ex\times\gcd(1,0)=e\times\gcd(x,y)=\gcd(a,b)
$$

所以结论成立。

(b)如果(3)执行，那么y是奇数，所以(1)不会执行；(4)同理；如果其余步骤执行，那么x,y都是奇数，所以(1)不会执行。

(c)首先(2)最多执行的次数为

$$
\min\{\log a,\log b\}
$$

显然小于等于

$$\log a+\log b$$

由(b)可知，步骤(2)只可能在最开始的时候执行，所以后面只考虑步骤(3)(4)(5)(6)(7)

如果进入(5)，那么x,y是奇数，所以$x-y$是偶数，因此下一步必然进入(3)，执行(3)之后，状态变为

$$(\frac{x-y}{2},y)$$

同理(6)的下一步必然进入(4)，且状态变为

$$(\frac{y-x}{2},x)$$

因为

$$\frac{x-y}{2}<\frac{x}{2},\frac{y-x}{2}<\frac{y}{2}$$

所以每执行两步，最大元素必然减小一半，所以这部分最大迭代次数为

$$2(\log a+\log b)$$

步骤(7)只执行一次，因此总共迭代的次数最多为

$$1+3(\log a+\log b)$$

Problem 4

(a)由裴蜀定理可得，存在整数s,t，使得

$$\gcd(a,b)=sa+tb$$

$\forall a,b$的公约数c，我们有

$$c|a,c|b$$

所以

$$c|sa+tb=\gcd(a,b)$$

(b)因为

$$\gcd(a,b)=1$$

所以存在整数s,t，使得

$$sa+tb=1$$

乘以c可得

$$sac+tbc=c$$

因为$a|bc,a|a$，所以

$$a|sac+tbc=c$$

(c)如果$p|b$，那么结论得证；否则因为p是质数，那么必然有

$$\gcd(p,b)=1$$

利用(b)可得

$$p|c$$

所以结论成立。

(d)反证法，如果结论不成立，设

$$\gcd(a,b)=m_0$$

那么

$$m\neq m_0$$

事实上，我们还有

$$0<m<m_0$$

由m的定义以及裴蜀定理可得，存在整数s_1,t_1,s_2,t_2，使得

$$\begin{aligned}m&=s_1a+t_1b\\m_0&=s_2a+t_2b\end{aligned}$$

所以

$$0<m_0-m=(s_2-s_1)a+(t_2-t_1)b<m_0$$

这就与m的定义矛盾。