Problem 1

根据提示，我们记录满足如下等式的系数u_x, v_x, u_y, v_y

$$
\begin{aligned}
u_x a + v_x b = x \\
u_y a + v_y b = y
\end{aligned}
$$

在初始状态，$(x, y) = (a, b)$，所以

$$
\begin{aligned}
u_x = 1, v_x = 0 \\
u_y = 0, v_y = 1
\end{aligned}
$$

假设第一种状态转移执行k步，使得$(\frac{x}{2^k}, \frac{y}{2^k})$中至少有一个为奇数，那么等式可以修改为

$$
\begin{aligned}
u'_x a + v'_x b = \frac{x}{2^k} \\
u'_y a + v'_y b = \frac{y}{2^k}
\end{aligned}
$$

对比

$$
\begin{aligned}
u_x a + v_x b = x \\
u_y a + v_y b = y
\end{aligned}
$$

可得对应更新公式为

$$
\begin{aligned}
u'_x = \frac{u_x}{2^k}, v'_x = \frac{v_x}{2^k} \\
u'_y = \frac{u_y}{2^k}, v'_y = \frac{v_y}{2^k}
\end{aligned}
$$

如果使用第二种状态转移，那么我们有

$$
u'_x a + v'_x b = \frac{x}{2}
$$

对比

$$
u_x a + v_x b = x
$$

可得更新公式为

$$
u'_x = \frac{u_x}{2}, v'_x = \frac{v_x}{2}
$$

同理如果使用第三种状态转移，那么我们有

$$
u'_v = \frac{u_v}{2}, v'_v = \frac{v_v}{2}
$$

如果使用第四种状态转移，那么我们有

$$u'_x a + v'_x b = x - y = (u_x - u_y)a + (v_x - v_y)b$$

所以更新公式为

$$\begin{aligned} u'_x &= u_x - u_y \\ v'_x &= v_x - v_y \end{aligned}$$

如果使用第五种状态转移，那么我们有

$$\begin{gathered} u'_x a + v'_x b = y - x = (u_y - u_x)a + (v_y - v_x)b \\ u'_y a + v'_y b = x = u_x a + v_x b \end{gathered}$$

所以更新公式为

$$\begin{gathered} u'_x = u_y - u_x, v'_x = v_y - v_x \\ u'_y = u_x, v'_y = v_x \end{gathered}$$

如果使用最后一种状态转移，注意此时有

$$u_x a + v_x b = x$$

注意我们知道此时的e，由之前的讨论可知

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

此时两边乘以e，即可得到

$$eu_x a + ev_x b = ex = \gcd(a, b)$$

所以最后的更新公式为

$$u'_x = eu_x, v'_x = ev_x$$

Problem 2

(a)self-inverse等价于

$$p | k^2 = (k-1)(k+1)$$

所以

$$p | k - 1 \text{或} \ p | k + 1$$

结合$0 < k < p$可得

$$\begin{gathered} k - 1 = 0 \text{或} \ k + 1 = p \\ k = 1 \text{或} \ k = p - 1 \end{gathered}$$

(b)对于$j = 1, \ldots, p-1$，因为p是质数，所以存在逆元，使得

$$j^{-1} . j \equiv 1 \mod p$$

对于$i, j \in \{1, \ldots, p-1\}$且$i \neq j$，我们必然有

$$i^{-1} \not\equiv j^{-1} \mod p$$

反证法，如果上述结论不成立，那么

$$1 \equiv i^{-1}i \equiv j^{-1}i \mod p$$
$$j \equiv jj^{-1}i \equiv i \mod p$$

这就与$i \neq j$矛盾，因此原结论成立。

该结论告诉我们，

$$\{1^{-1}, \ldots, (p-1)^{-1}\} = \mathbb{Z}_p$$

所以

$$1^{-1} \times \ldots \times (p-1)^{-1} \times 1 \times \ldots \times (p-1) \equiv 1 \equiv ((p-1)!)^2 \equiv p$$

假设

$$(p-1)! \equiv a \mod p$$

那么

$$a^2 \equiv 1 \mod p$$

由(a)可得，

$$a = 1\text{或}\, a = p - 1$$

注意到$p = 3$时，我们有

$$(p-1)! \equiv 2 \equiv -1 \mod p$$

所以我们必然有

$$a = p - 1$$

因此

$$(p-1)! \equiv p - 1 \equiv = -1 \mod p$$

Problem 3

(a)证明：首先证明f是单射，$\forall x, y \in [0, ab)$，如果

$$f(x) = (\text{rem}(x, a), \text{rem}(x, b)) = (\text{rem}(y, a), \text{rem}(y, b)) = f(y)$$

那么

$$\text{rem}(x, a) = \text{rem}(y, a)$$
$$\text{rem}(x, b) = \text{rem}(y, b)$$

因为a, b互质，所以由中国剩余定理可知，

$$x \equiv y \mod ab$$

由$x, y \in [0, ab)$，我们有

$$x = y$$

所以f是单射。

接着证明f是满射，由中国剩余定理可知，对于任意m, n，存在x，使得

$$\begin{aligned} x \equiv m \mod a \\ x \equiv n \mod b \end{aligned}$$

因此f是满射。

综上，f是双射。

(b)证明：单射的证明同(a)，所以只需要证明该映射为满射。

$\forall m \in \mathbb{Z}_a^*, n \in \mathbb{Z}_b^*$，由中国剩余定理可知存在$x$，使得

$$\begin{aligned} x \equiv m \mod a \\ x \equiv n \mod b \end{aligned}$$

接下来证明$x \in \mathbb{Z}_{ab}^*$，如果不然，那么

$$(ab, x) > 1$$

由a, b互质可得

$$(a, x) > 1 \text{或} (b, x) > 1$$

因为m, n显然不为0，所以这就与

$$\begin{aligned} x \equiv m \mod a \\ x \equiv n \mod b \end{aligned}$$

矛盾。因此$x \in \mathbb{Z}_{ab}^*$，这说明该映射是满射。

综上映射是双射。

(c)如果两个有限之间集合存在双射，那么这两个集合元素数量相同，所以

$$\phi(ab) = |\mathbb{Z}_{ab}^*| = |\mathbb{Z}_a^*|.|\mathbb{Z}_b^*| = \phi(a)\phi(b)$$

(d)设

$$n = \prod_{i=1}^{j} p_i^{m_i}$$

那么反复运用(c)可得

$$
\begin{aligned}
\phi(n) &= \phi(\prod_{i=1}^{j} p_i^{m_i}) \\
&= \prod_{i=1}^{j} \phi(p_i^{m_i}) \\
&= \prod_{i=1}^{j} (p_i^{m_i} - p_i^{m_i - 1}) \\
&= \prod_{i=1}^{j} p_i^{m_i} \prod_{i=1}^{j} (1 - \frac{1}{p_i}) \\
&= n \prod_{i=1}^{j} (1 - \frac{1}{p_i})
\end{aligned}
$$