Problem 1

$$\begin{aligned}9876^{3456789}(9^{99})^{5555}-6789^{3414259} &\equiv 6^{3456789}\times(81^{49}\times 9)^{5555}-(-1)^{3414259}\\ &\equiv 36^{1728394}\times 6\times((-3)^{49}\times 9)^{5555}+1\\ &\equiv (-6)^{1728394}\times 6\times(-3^{51})^{5555}+1\\ &\equiv -36^{864197}\times 6\times(27^{17})^{5555}+1\\ &\equiv -(-6)^{864197}\times 6\times((-1)^{17})^{5555}+1\\ &\equiv -6^{864198}+1 \mod 14\end{aligned}$$

注意到

$$\begin{aligned}-6^{864198}+1 &\equiv -(-1)^{864198}+1\\ &\equiv -1+1\\ &\equiv 0 \mod 7\end{aligned}$$

以及$-6^{864198}+1$是奇数，所以

$$\begin{aligned}9876^{3456789}(9^{99})^{5555}-6789^{3414259} &= 7\times(2k+1)\\ k &\in \mathbb{Z}\end{aligned}$$

因此

$$9876^{3456789}(9^{99})^{5555}-6789^{3414259}\equiv 7 \mod 14$$

Problem 2

(a)按提示定义e_a, e_b，令

$$x = me_a + ne_b$$

那么

$$\begin{aligned}e_a &\equiv 1 \mod b\\ e_b &\equiv 1 \mod a\\ x \equiv ne_b &\equiv n \mod a\\ x \equiv me_a &\equiv m \mod b\end{aligned}$$

(b)因为a, b互质，所以存在整数s, t，使得

$$as + bt = 1$$

因此

$$x = xas + xbt$$

因为

$$x \equiv 0 \mod a$$
$$x \equiv 0 \mod b$$

所以

$$ab|xas, ab|xbt$$
$$ab|xas + xbt = x$$
$$x \equiv 0 \mod ab$$

(c)由条件可得

$$x - x' \equiv 0 \mod a$$
$$x - x' \equiv 0 \mod b$$

由(b)可得

$$x - x' \equiv 0 \mod ab$$

所以

$$x \equiv x' \mod ab$$

(d)由(a)可得存在性得证，如果存在x'，使得

$$x' \equiv m \mod a$$
$$x' \equiv n \mod b$$

结合

$$x \equiv m \mod a$$
$$x \equiv n \mod b$$

可得

$$x \equiv x' \mod a$$
$$x \equiv x' \mod b$$

由(c)可得

$$x \equiv x' \mod ab$$

(e)首先证明(b)的逆命题，如果

$$x \equiv 0 \mod ab$$

那么

$$ab|x$$

那么显然有

$$a|x, b|x$$

所以

$$x \equiv 0 \mod a$$
$$x \equiv 0 \mod b$$

因此(b)的逆命题成立。现在考虑(c)的逆命题，如果

$$x \equiv x' \mod ab$$

那么

$$x - x' \equiv 0 \mod ab$$

由之前的讨论可得

$$x - x' \equiv 0 \mod a$$
$$x - x' \equiv 0 \mod b$$

所以

$$x \equiv x' \mod a$$
$$x \equiv x' \mod b$$

所以逆命题成立。

Problem 3

(a)Base cases:

如果$q = x$，那么

$$q(j) = j, q(k) = k$$

因为

$$j \equiv k \mod n$$

所以

$$q(j) \equiv q(k) \mod n$$

如果$q = m$，那么

$$q(j) = q(k) = m$$

所以

$$q(j) \equiv q(k) \mod n$$

Constructor cases：

$\forall r, s \in P$，由归纳假设可知，我们有

$$j \equiv k \mod n \Rightarrow s(j) \equiv s(k) \mod n, t(j) \equiv t(k) \mod n$$

所以

$$s(j)+t(j) \equiv s(k)+t(k) \mod n$$
$$s(j)t(j) \equiv s(k)t(k) \mod n$$

因此Constructor cases结论成立。

(b)$\forall n \in \mathbb{N}, k, v \in \mathbb{Z}$，我们有

$$(k+v)^n \equiv k^n \mod v$$

所以对于任意多项式q，正整数m，我们有

$$q(k) \equiv q(k+mv) \mod v$$

特别的，我们取$v=q(k)$，所以

$$q(k) \equiv q(k+mq(k)) \equiv 0 \mod q(k)$$

因此$q(k+mq(k))$都是$q(k)$的倍数。