Problem 1

取 k 为满足 $2^k \leqslant n$ 的最大整数, N 为 1, 2, ⋯ ,n 的最小公倍数，则 $N = 2^k \cdot m$, m 为奇数.

有 $X = (1 + 1/2 + \cdots + 1/n) \times N = N + N/2 + \cdots + N/n$ 为整数.

若 $1 + 1/2 + \cdots + 1/n$ 为整数, X 为偶数，又有项 $N/2^k = m$ 为奇数，其余项均为偶数,

则 X 为奇数，矛盾，则 $1 + 1/2 + \cdots + 1/n$ 不是整数.

Problem 2

a) 23300 mod 11 = 2

b) $2^{3300} \bmod 31 = 32^{660} \bmod 31 = ((32 \bmod 31)^{660}) \bmod 31 = 1 \bmod 31 = 1$

c) $3^{516} \bmod 7 = 9^{258} \bmod 7 = 2^{258} \bmod 7 = 8^{86} \bmod 7 = 1^{86} \bmod 7 = 1$

Problem 3

若 n 不是质数，存在正整数 a 和 b 满足 $1<a<n$, $1<b<n$, $n = ab$.

$2^n - 1 = 2^{(ab)} - 1 = (2^a)^b - 1$，令 $2^a = x$,

$2^n - 1 = x^b - 1 = (x - 1)(x^{(b-1)} + x^{(b-2)} + \cdots + x + 1)$

$1<a<n$ 则 $x - 1 = 2^a - 1 > 1$, $1<b<n$ 则 $x^{(b-1)} + \cdots + 1 > 1$.

$2^n - 1$ 可分解为两个大于 1 的正整数的积, $2^n - 1$ 不是素数，矛盾，则 n 必为素数.

Problem 4

a) n 是偶数, $2 \mid n(n+1)(n+2)$; n 是奇数, n+1 是偶数, $2 \mid n(n+1)(n+2)$. n mod 3 = 0, 1 或 2.

1° n mod 3 = 0, $3 \mid n$, $3 \mid n(n+1)(n+2)$;

2° n mod 3 = 1，存在整数 a 使 $n = 3a+1$, $n+2 = 3(a+1)$, $3 \mid n+2$, $3 \mid n(n+1)(n+2)$

3° n mod 3 = 2，存在整数 b 使 $n = 3b+2$, $n+1 = 3(b+1)$, $3 \mid n+1$, $3 \mid n(n+1)(n+2)$

综上, $2 \mid n(n+1)(n+2)$, $3 \mid n(n+1)(n+2)$, $6 \mid n(n+1)(n+2)$

b) 原式= $(3n^5 + 5n^3 + 7n)/15 = (3(n^5 - n) + 5(n^4 - n) + 15n)/15$

$= (n^5 - n)/5 + (n^3 - n)/3 + n$.

$n^5 - n = n(n-1)(n+1)(n^2+1)$, $n^4 - n = n(n-1)(n+1)$则

1° 若 n mod 5 = 0, $5 \mid n$; 若 n mod 5 = 1, $5 \mid n-1$; 若 n mod 5 = 2，取 $n = 5a+2$

$n^2+1 = 25a^2+20a+5$, $5 \mid n^2+1$，若 n mod 5 = 3，取 $n = 5a+3$,

$n^2+1 = 25a^2+30a+10$, $5 \mid n^2+1$，若 n mod 5 = 4, $5 \mid n+1$.

2° 若 n mod 3 = 0, $3 \mid n$，若 n mod 3 = 1, $3 \mid n-1$; 若 n mod 3 = 2, $3 \mid n+1$.

综上, $n^5 - n \mid 5$, $n^3 - 1 \mid 3$，原式是整数.

Problem 5

a) $d \mid m$, $a \equiv b \pmod m$，取整数 n 使 $m = nd$，取 $x = a \bmod m = b \bmod m$,

存在整数 p, q 使 $a = pm + x = (pn)d + x$, $b = qm + x = (qn)d + x$.

且满足 $0 \leqslant x < m$. pn, qn 仍为整数, $a \bmod d = x$, $b \bmod d = x$, $a \equiv b \pmod d$.

b) $a \equiv b \pmod m$，取 $x = a \bmod m = b \bmod m$，存在整数 p, q 使 $a = pm + x$, $b = qm + x$.

$da = p(dm) + dx$, $db = q(dm) + dx$, $0 \leqslant x < m$ 则 $0 \leqslant dx < dm$.

$da \bmod m = dx$, $db \bmod m = dx$, $da \equiv db \pmod{dm}$.

$da \equiv db \pmod{dm}$，取 $x = da \bmod dm = db \bmod dm$，存在整数 p, q 使 $da = d(pm) + x$,

$db = d(qm) + x, 0 \leqslant x \leqslant m$，且 $x = d(a - pm) = d(b - qm)$为 d 的整数倍.
存在正整数 y 使 $x=dy$, $a = pm + y$, $b = qm + y$, $a \bmod m = b \bmod m = y$, $a \equiv b \pmod m$.

c) $a \equiv b \pmod m$，取 $x = a \bmod m = b \bmod m$，存在整数 p, q 使 $a = pm + x$, $b = qm + x$.
$ca = (cp)m + cx$, $cb = (cq)m + cx$, $ca \bmod m = cb \bmod m = cx \bmod m$, $ca \equiv cb \pmod m$.

$ca \equiv cb \pmod m$，取 $x = ca \bmod m = cb \bmod m$，存在 p, q 使 $ca = pm + x$, $cb = qm + x$.
$ca = pm + x$, $cb = qm + x$ 为 c 的整数倍，又 c 与 m 互素，存在整数 $r = p \operatorname{div} c$, $s = q \operatorname{div} c$,
$y = (p \bmod c)\, m + x$, $z = (q \bmod c)\, m + x$, $ca = rcm + y$, $cb = scm + z$,
其中 rcm, scm 为 c 的整数倍，则 y, z 为 c 的整数倍,
1° 若 $x \mid c$ 则 $p \bmod c \mid c$, $p \bmod c = 0$，同理 $q \bmod c = 0$, $y = z = x$,
  $a \bmod m = b \bmod m = x/c$, $a \equiv b \pmod m$
2° 若 $x \bmod c \neq 0$, $((p \bmod c)m \bmod c) + x \bmod c = ((q \bmod c)m \bmod c) + x \bmod c = c$,
  $(p \bmod c)m \equiv (q \bmod c)m \pmod c$, $((p \bmod c)m - (q \bmod c)m) \mid c$.
  则 $a = rm + y/c$, $b = sm + z/c$, $a \bmod m = y/c \bmod m$, $b \bmod m = z/c \bmod m$
  $(y/c - z/c)/m = ((p \bmod c) - (q \bmod c))/c$，是整数, $y/c \equiv z/c \pmod m$, $a \equiv b \pmod m$.

Problem 6
$7 - 1$ 为 6, 6 的正因数有 1, 2, 3, 6，分别+1 得 2, 3, 4, 7，其中 2, 3, 7 为质数,
若 n 不是 2 的倍数, $n \equiv 1 \pmod 2$，若 n 不是 3 的倍数, $n^2 \equiv 1 \pmod 3$,
若 n 不是 7 的倍数, $n^6 \equiv 1 \pmod 7$，则 $n^7 - n = n(n^6 - 1)$, $7 \mid (n^6 - 1)$,
$n^6 - 1 = (n^3 + 1)(n^3 - 1) = (n + 1)(n^2 - n + 1)(n - 1)(n^2 + n + 1)$.
$2 \mid (n - 1)$, $(n + 1)(n - 1) = (n^2 - 1)$, $3 \mid (n^2 - 1)$.
$7 \mid (n^7 - n)$, $2 \mid (n^7 - n)$, $3 \mid (n^7 - n)$，则 $2 \times 3 \times 7 = 42 \mid (n^7 - n)$.

Problem 7
$p^4 \equiv 1 \pmod 5$, $p^2 \equiv 1 \pmod 3$, $p \equiv 1 \pmod 2$
$p^4 - 1 = (p^2 + 1)(p^2 - 1) = (p + 1)(p - 1)(p^2 + 1)$.
$5 \mid (p^4 - 1)$, $3 \mid (p^2 - 1)$, $2 \mid (p - 1)$.
又 $p \geqslant 7$, $p^4 - 1 \geqslant 7^4 - 1 = 2400 > 240$.
令 $p = 2k + 1$, k 为正整数且 $k \geqslant 3$, $p^4 - 1 = 16k^4 + 32k^3 + 24k^2 + 8k$.
$P^4 - 1 = 8k(k + 1)(2k^2 + 2k + 1)$, k 与 k+1 必为一个奇数与一个偶数,
可见 $16 \mid (p^4 - 1)$. $3 \times 5 \times 16 = 240 \mid (p^4 - 1)$.

Problem 8
m 和 n 互素，由欧拉定理可知 $m^{\phi(n)} \equiv 1 \pmod n$, $n^{\phi(m)} \equiv 0 \pmod n$.
$m\phi(n) + n\phi(m) \equiv 1 \pmod n$. 同理 $n\phi(m) \equiv 1 \pmod m$, $m\phi(n) \equiv 0 \pmod m$,
$m\phi(n) + n\phi(m) \equiv 1 \pmod m$. 又 m 和 n 互素，则 $m\phi(n) + n\phi(m) \equiv 1 \pmod{mn}$.