Problem 1

取k为满足2^k≤n的最大整数, N为1, 2, … ,n的最小公倍数, 则N = 2^k·m, m为奇数.

有X = (1 + 1/2 + … + 1/n) × N = N + N/2 + … + N/n为整数.

若1 + 1/2 + … + 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 + … + 1/n不是整数.

Problem 2

a) 23300 mod 11 = 2

b) 2^3300 mod 31 = 32^660 mod 31 = ((32 mod 31) ^660) mod 31 = 1 mod 31 = 1

c) 3^516 mod 7 = 9^258 mod 7 = 2^258 mod 7 = 8^86 mod 7 = 1^86 mod 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) + … + x + 1)

1<a<n则x – 1 = 2^a – 1 > 1, 1<b<n则x^(b-1) + … + 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 | n(n+1)(n+2); n是奇数, n+1是偶数, 2 | n(n+1)(n+2). n mod 3 = 0, 1或2.

1° n mod 3 = 0, 3 | n, 3 | 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 | n+2, 3 | 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 | n+1, 3 | n(n+1)(n+2)

综上, 2 | n(n+1)(n+2), 3 | n(n+1)(n+2), 6 | n(n+1)(n+2)

b) 原式= (3 n^5 + 5 n^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 | n; 若n mod 5 = 1, 5 | n-1; 若n mod 5 = 2, 取n = 5a+2

n^2+1 = 25a^2+20a+5, 5 | n^2+1, 若n mod 5 = 3, 取n = 5a+3,

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

2° 若n mod 3 = 0, 3 | n, 若n mod 3 = 1, 3 | n-1; 若n mod 3 = 2, 3 | n+1.

综上, n^5 – n | 5, n^3 – 1 | 3, 原式是整数.

Problem 5

a) d | m, a≡b(mod m), 取整数n使m = nd, 取x = a mod m = b mod m,

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

且满足0≤x<m. pn, qn仍为整数, a mod d = x, b mod d = x, a≡b(mod d).

b) a≡b(mod m), 取x = a mod m = b mod m, 存在整数p, q使a = pm + x, b = qm + x.

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

da mod m = dx, db mod m = dx, da≡db(mod dm).

da≡db(mod dm), 取x = da mod dm = db mod dm, 存在整数p, q使da = d(pm) + x,

db = d(qm) + x, 0≤x≤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 mod m = b mod m = y, a≡b(mod m).

c) a≡b(mod m), 取x = a mod m = b mod m, 存在整数p, q使a = pm + x, b = qm + x.

ca = (cp)m + cx, cb = (cq)m + cx, ca mod m = cb mod m = cx mod m, ca≡cb(mod m).

ca≡cb(mod m), 取x = ca mod m = cb mod 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 div c, s = q div c,

y = (p mod c) m + x, z = (q mod 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 | c则p mod c | c, p mod c = 0, 同理q mod c = 0, y = z = x,

a mod m = b mod m = x/c, a≡b(mod m)

2° 若x mod c ≠ 0, ((p mod c)m mod c) + x mod c = ((q mod c)m mod c) + x mod c = c,

(p mod c)m≡(q mod c)m(mod c), ((p mod c)m – (q mod c)m) | c.

则a = rm + y/c, b = sm + z/c, a mod m = y/c mod m, b mod m = z/c mod m

(y/c – z/c)/m = ((p mod c) – (q mod c))/c, 是整数, y/c≡z/c(mod m), a≡b(mod 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≡1(mod 2), 若n不是3的倍数, n^2≡1(mod 3),

若n不是7的倍数, n^6≡1(mod 7), 则n^7 – n = n (n^6 – 1), 7 | (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 | (n – 1), (n + 1) (n – 1) = (n^2 – 1), 3 | (n^2 – 1).

7 | (n^7 – n), 2 | (n^7 – n), 3 | (n^7 – n), 则2×3×7 = 42 | (n^7 – n).

Problem 7

p^4≡1(mod 5), p^2≡1(mod 3), p≡1(mod 2)

p^4 – 1 = (p^2 + 1) (p^2 – 1) = (p + 1) (p – 1) (p^2 + 1).

5 | (p^4 – 1), 3 | (p^2 – 1), 2 | (p – 1).

又p≥7, p^4 – 1 ≥ 7^4 – 1 = 2400 > 240.

令p = 2k + 1, k为正整数且k≥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 | (p^4 – 1). 3×5×16 = 240 | (p^4 – 1).

Problem 8

m和n互素, 由欧拉定理可知m^ϕ(n)≡1(mod n), n^ϕ(m)≡0(mod n).

mϕ(n) + nϕ(m) ≡ 1(mod n). 同理nϕ(m)≡1(mod m), mϕ(n)≡0(mod m),

mϕ(n) + nϕ(m) ≡ 1(mod m). 又m和n互素, 则mϕ(n) + nϕ(m) ≡ 1(mod mn).