离散数学（2023）作业 06

周帛岑
221900309

2023 年 3 月 26 日

1 Problem 1

证：

a)：假，令 a = b = 3，c = 6

ab = 9，9 并不能整除 6。

b)：真：

证：不妨令 a | c = p，b | d = q。p，q 均为正整数，则 cd /ab = (c / a) · (d / b) = p · q，为整数

c): 真：

证：不妨设 ab | c = d，即 c/ab = d，c = a · b · d，故 c/a = b · d，为整数

d): 真：不妨假设，bc/a = d，d 为正整数。

考察 b/a，假设 b/a 不为整数，结果为 e，e · c 显然不为整数。故此时 c/a 一定为整数，即 a|c。

考察 c/a，假设 c/a 不为整数，结果为 f，f · b 显然不为整数。故此时 b/a 一定为整数，即 a|b。

综上，有 a|c 或 a|b

订正：d) 有误，应该为假

例子：b = 6 ，c = 14，a = 21 .bc 此时为 84，满足 a|bc, 但并没有 a|b 或 a|c

2 Problem 2

证：设这三个数为 a,b,c(并未代表大小顺序)。由抽屉原理，这三个数中一定存在一个数为 3 的倍数，不妨令这个数为 a，且 a=3m。

由于奇数与奇数，偶数与偶数均不会相邻，故三个数中至少有一个偶数。

假设 3m 为偶数，此时 m = 2n，a = 6m，此时 abc = 6mbc，能被 6 整除。

假设 3m 为奇数，此时一定在三个整数中存在一个偶数，不妨令 b = 2n，此时 abc = 6mnc，能被 6 整除

3 Problem 3

解：

a)：

由 233（mod 11）· 100（mod 11）= 2 · 1 = 2 且 233 · 100 = 23300，得原式 = 2

b):

由 $2^5(mod31) = 1$, $(2^5)^{660} = 2^{3300}$, 得原式 $= 1^{660} = 1$

c)：

由 $3^6(mod7) = 1$, $(3^6)^{86} = 3^{516}$, 得原式 $= 1^{86} = 1$

原式 $= (3^2(mod7))^{258}$

4 Problem 4

证：

订正：当时未能想出证明方法：

证：我们使 a = mb+n(m,n∈ℕ(即 m 可以取 0) 且 1≤n≤(b-1)) , 此时 $2^a - 1 = 2^{mb+n} - 1 = 2^n(2^{mb} - 1) + 2^n - 1$

又 $2^b \equiv 1(\text{mod } (2^b - 1))$, 故 $2^{mb} \equiv 1(\text{mod } (2^b - 1))$

故 $(2^b - 1)|2^{mb} - 1$

故 $(2^a - 1)mod(2^b - 1) = 2^n - 1$

注意到 a mod b = n, 故 $2^a - 1mod(2^b - 1) = 2^{amodb} - 1$

5 Problem 5

证：

不妨假设 n 不为素数。且 $n = a \cdot b$, 其中 a,b 均为大于一的整数。$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots\ldots + (2^a) + 1)$ $2^a - 1$ $a > 1$, $2^a - 1 > 1$, $2^n - 1$ n

订正：使用 latex 时出现了格式问题，语言有些不严谨的地方，进行了修改：

证：

不妨假设 $2^n - 1$ 为素数且此时 n 不为素数。且 $n = a \cdot b$, 其中 a,b 均为大于一的整数。$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots\ldots + (2^a) + 1)$，又此时 $2^a - 1$ 中，a>1, 故 $2^a - 1 > 1$, 故 $2^a - 1 > 1$ 为 $2^n - 1$ 的一个不为 1 且不为其本身的因子，则此时 $2^n - 1$ 也不为素数，与假设产生矛盾，故假设不成立，$2^n - 1$ 为素数时，n 为素数

6 Problem 6

a): 证：

由抽屉原理，这三个数中一定有一个数为 3 的倍数，

且奇数与奇数，偶数与偶数均不相邻，故三个数中至少有一个偶数

不妨令三的倍数对应数为 a，且 a = 3m

假设 a 为偶数，此时 m = 2q，则 6|a，再乘上其余两个整数，结果也为整数，故此时可以被 6 整除

假设 a 为奇数，此时三个数中存在一个数 b = 2p，则 ab = 6pm 可以被 6 整除，再乘上剩余的一个整数，结果依旧为整数，故此时可以被 6 整除。

综上，6|(n)(n+1)(n+2)

b): 证：

原式通分，有原式等于 $\frac{3n^5+5n^3+7n}{15}$

考察 $3\mathrm{n}^5 + 5n^3 + 7n$

原式 $= \mathrm{n}(3\mathrm{n}^4 - 10n^2 + 7 + 15n^2) = n((3n^2 - 7)(n^2 - 1) + 15n^2) = (3n^2 - 7)(n - 1)n(n + 1) + 15n^3$

考察 $(3\mathrm{n}^2 - 7)(n - 1)n(n + 1)$

由 a),(n-1)n(n+1) 为 3 的倍数，下面考虑 (n-1)n(n+1) 是否为 5 的倍数

不妨假设三个数均不为 5 的倍数，此时 n 为 5k+2 或 5k+3，其中 k 为正整数

此时 $3\mathrm{n}^2 - 7 = 75k^2 + 60k + 5$ $75k^2 + 90k + 20 = 5(15k^2 + 12k + 1)$ $5(15k^2 + 16k + 4)$ 5

综上，原命题得证

订正：b) 最后步骤中 latex 格式出现错误：

b): 证：

前略

此时 $3n^2 - 7 = 75k^2 + 60k + 5$ 或 $75k^2 + 90k + 20$

即 $3n^2 - 7 = 5(15k^2 + 12k + 1)$ 或 $5(15k^2 + 16k + 4)$　均为 5 的倍数

综上，原命题得证

7 Problem 7

a): 证：

不妨设 b mod m = n，即 b = km+n，同理，a = pm+n，又 d|m, 不妨令 m/d = l，即 m = d · l，即 b = k(d · l)+n = kl · d+n，a = p(d · l)+n = pl · d+n, 故有 a≡b(mod d)

b):

证：

1.a≡b(mod m) 时，不妨设 b mod m = n，即 b = km+n，同理，a = pm+n

db = dkm+dn = k · dm+dn,da = dpm+dn = p · dm+dn, 则 da mod dm = dn mod dm 且 db mod dm = dn mod dm, 即 da mod dm = db mod dm，有 da≡db(mod dm)

2.da≡db(mod dm) 时，不妨设 db mod dm = n，即 db = kdm+n，同理，da = pdm+n, 由 da，db 均为 d 的倍数，故 n 也为 d 的倍数，

b = km+n/d, a = pm+n/d，有 a≡b(mod m)

c):

证：

1.a≡b(mod m) 时，不妨设 b mod m = n，即 b = km+n，同理，a = pm+n

cb = ckm+cn = kc · m+cn,ca = cpm+cn = pc · m+cn, 则 ca mod m = cn mod m 且 cb mod cm = cn mod cm，此时有 ca≡cb(mod m)

2.ca≡cb(mod m) 时，不妨设 cb mod m = n，即 cb = km+n，同理，ca = pm+n

8 Problem 8

证：当 n 为 7 的倍数时 n$^7 - n = n(n^6-1) = n(n^3+1)(n^3-1) = n(n+1)(n-1)(n^2-n+1)(n^2+n+1)$ n 7 $n-1$ 6 42

当 n 不为 7 时，由费马小定理可知，n$^7 = 7k+m, n = 7l+m$

n$^7 - n = n(n+1)(n-1)(n^2-n+1)(n^2+n+1) = 7(k-l)$ 7

又由 problem6 a) 可知，n(n+1)(n-1) 为 6 的倍数，故 n$^7 - n$1 7 6 42

订正：使用 latex 时格式出现问题

证：当 n 为 7 的倍数时 $n^7 - n = n(n^6-1) = n(n^3+1)(n^3-1) = n(n+1)(n-1)(n^2-n+1)(n^2+n+1)$ 此时 n 为 7 的倍数，n-1 为 6 的倍数，可以被 42 整除

当 n 不为 7 的倍数时，由费马小定理可知，$n^7 = 7k+m, n = 7l+m$

$n^7 - n = n(n+1)(n-1)(n^2-n+1)(n^2+n+1) = 7(k-l)$ 为 7 的倍数

又由 problem6 a) 可知，n(n+1)(n-1) 为 6 的倍数，故 $n^7 - n$ 既为 7 的倍数也为 6 的倍数，能被 42 整除

综上，命题得证

9 Problem 9

证：由 p$^4 = (p-1)(p+1)(p^2+1)$

且 p 为素数, 且 p≥7, 故 (p-1), (p+1), (p^2+1) $p-1$ $p+1$ p^4 $2 \cdot 2 \cdot 4 = 16$ $p^2 = 1(mod3)p^4 = 1(mod5)$, $p^2-1|3, p^4-1|5,$ 3 5

综上，原式可以被 $16 \cdot 3 \cdot 5 = 240$ 整除

命题得证。

订正：latex 格式出现了问题：

证：由 p$^4 = (p-1)(p+1)(p^2+1)$

且 p 为素数，且 $p \geq 7$, 故 (p-1)，(p+1)，(p$^2+1$) 均为偶数，且 p-1 与 p+1 为相邻偶数，即 p^4 可以被 $2 \cdot 2 \cdot 4 = 16$ 整除。

由费马小定理可知，$p^2 = 1(mod3), p^4 = 1(mod5)$, $p^2-1|3, p^4-1|5$, 即原式可以被 3，5 整除。

综上，原式可以被 $16 \cdot 3 \cdot 5 = 240$ 整除

命题得证。

10 Problem 10

证:

由欧拉定理可知: $\mathrm{n}^{\varphi(m)} - 1 = km, m^{\varphi(n)} - 1 = ln$

两式相乘有 $(\mathrm{n}^{\varphi(m)} - 1)(m^{\varphi(n)} - 1) = klmn$

左侧 $= \mathrm{n}^{\varphi(m)} m^{\varphi(n)} - n^{\varphi(m)} - m^{\varphi(n)} + 1$

又 $\mathrm{n}^{\varphi(m)} m^{\varphi(n)} | mn$, 且$(n^{\varphi(m)} - 1)(m^{\varphi(n)} - 1) | mn$, 故$(-n^{\varphi(m)} - m^{\varphi(n)} + 1) | mn$

即 $\mathrm{n}^{\varphi(m)} + m^{\varphi(n)} = 1 (mod \quad mn)$