

离散数学 (2023) 作业 06 - 自然数与数论初步

March 21, 2023

Problem 1

设 a, b, c, d 均为正整数, 下列命题是否为真? 若为真, 给出证明; 否则, 给出反例。

1. 若 $a \mid c, b \mid c$, 则 $ab \mid c$
2. 若 $a \mid c, b \mid d$, 则 $ab \mid cd$
3. 若 $ab \mid c$, 则 $a \mid c$
4. 若 $a \mid bc$, 则 $a \mid b$ 或 $a \mid c$

答案:

1. 假。反例: $a = 2, b = 2, c = 2$ 。
2. 真。证明: 由题设, 存在整数 k_1, k_2 使得 $c = k_1 a, d = k_2 b$, 从而有 $cd = k_1 k_2 ab$, 得证 $ab \mid cd$ 。
3. 真。证明: 存在整数 k 使得 $c = k(ab) = (kb)a$, 得证 $a \mid c$ 。
4. 假。反例: $a = 4, b = 2, c = 2$ 。

Problem 2

计算:

1. $23300 \bmod 11$
2. $2^{3300} \bmod 31$
3. $3^{516} \bmod 7$

答案:

1. 2. $23300 = 233 * 10 * 10 = (21 * 11 + 2) * 10 * 10 \equiv 2 * (-1) * (-1) \equiv 2 \pmod{11}$
2. 1. $2^{3300} \equiv 2^{5*660} \equiv 32^{660} \equiv 1^{660} \equiv 1 \pmod{31}$
3. 1. $3^6 \equiv 1 \pmod{7}, 3^{516} \equiv 3^{6*86} \equiv 1 \pmod{7}$

Problem 3

试证明: 对于任意的正整数 n , 都有 $n^2 \mid (n+1)^n - 1$ 。

答案: 基于 $(n+1)^n - 1$ 的二项展开, 易得:

$$(1+n)^n - 1 = \binom{n}{1}n + \binom{n}{2}n^2 + \dots + \binom{n}{n}n^n$$

右边第一项 $\binom{n}{1}n = n^2$, 第二项之后均包含大于等于 2 的 n 的指数幂, 显然有 $n^2 \mid (n+1)^n - 1$ 。

Problem 4

证明: 如果 a 和 b 为正整数, 则 $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$ 。

答案: 分情况讨论:

1. 当 $a < b$ 时, $(2^a - 1) \bmod (2^b - 1) = 2^a - 1 = 2^{a \bmod b} - 1$;
2. 当 $a \geq b$ 时, 设 $a \bmod b = r$, 即 $a = nb + r$, 此时

$$\begin{aligned}(2^a - 1) \bmod (2^b - 1) &= (2^{nb+r} - 1) \bmod (2^b - 1) \\&= (2^{nb} \cdot 2^r - 2^r + 2^r - 1) \bmod (2^b - 1) \\&= ((2^{nb} - 1) \cdot 2^r + (2^r - 1)) \bmod (2^b - 1) \\&= \left((2^b - 1)[(2^b)^0 + (2^b)^1 + \dots + (2^b)^{(n-1)}] \cdot 2^r + (2^r - 1) \right) \bmod (2^b - 1) \\&= (2^r - 1) \bmod (2^b - 1) \\&= 2^{a \bmod b} - 1\end{aligned}$$

综上, 对所有的情形, 都有 $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$ 成立。

Problem 5

证明: 如果 $2^n - 1$ 是质数, 则 n 也为质数。

答案: 假设 n 是合数, 则存在大于等于 2 的整数 x, y 满足 $n = xy$ 。此时:

$$2^n - 1 = 2^{xy} - 1 = (2^x)^y - 1 = (2^x - 1)(2^{y(x-1)} + 2^{y(x-2)} + \dots + 2^y + 1)$$

显然, $2^y - 1 \mid 2^n - 1$, 则 $2^n - 1$ 不是质数, 和题设矛盾, 所以 n 是质数得证。

Problem 6

证明: 对于任意的整数 n , $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ 是整数。

答案: 只要证 $15 \mid 3n^5 + 5n^3 + 7n$, 即证 $3 \mid 5n^3 + 7n$ 且 $5 \mid 3n^5 + 7n$ 。

1. 证 $3 \mid 5n^3 + 7n$: 因为 $5n^3 + 7n$ 是奇函数, 只需证对非负整数 n 成立。用归纳法:
 - 当 $n = 0$ 时, $3 \mid 0$, 结论成立。
 - 假设当 $n = k (k \geq 0)$ 时结论成立。当 $n = k + 1$ 时, $5(k+1)^3 + 7(k+1) = (5k^3 + 7k) + 3(5k^2 + 5k + 4)$ 。
 - 由归纳假设, $3 \mid 5k^3 + 7k$, 故 $3 \mid 5(k+1)^3 + 7(k+1)$, 即当 $n = k + 1$ 时结论也成立。
2. 类似可证 $5 \mid 3n^5 + 7n$ 。

综上, 对于任意的整数 n , $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ 是整数得证。

Problem 7

证明：对于任意的正整数 m 和 $a > 1$ ，都有 $\gcd\left(\frac{a^m-1}{a-1}, a-1\right) = \gcd(a-1, m)$ 。

答案： 令 $d = \gcd\left(\frac{a^m-1}{a-1}, a-1\right)$ 。注意到，

$$\frac{a^m-1}{a-1} = (a^{m-1}-1) + (a^{m-2}-1) + \dots + (a-1) + m$$

以及对于任意的自然数 k 都有 $a-1 \mid a^k-1$ ，可知 $d \mid m$ 。因此， d 是 $a-1$ 和 m 的一个公因数。

再证 $d = \gcd(a-1, m)$ ：假设 $a-1$ 和 m 有更大的公因数 $\delta > d$ ，由上式可得 $\delta \mid \frac{a^m-1}{a-1}$ ，那么 $\frac{a^m-1}{a-1}$ 和 $a-1$ 也有更大的公因数 $\delta > d$ ，与 $d = \gcd\left(\frac{a^m-1}{a-1}, a-1\right)$ 矛盾。因此，不存在公因数 $\delta > d$ ，故 $d = \gcd(a-1, m)$ ，原命题成立。

Problem 8

证明：

1. 设 $d \geq 1$, $d \mid m$, 则 $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$
2. 设 $d \geq 1$, 则 $a \equiv b \pmod{m} \Leftrightarrow da \equiv db \pmod{dm}$
3. 设 c 与 m 互质, 则 $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{m}$

答案：

1. 由 $a \equiv b \pmod{m}$ ，有 $m \mid a-b$ 。又已知 $d \mid m$ ，得到 $d \mid a-b$ ，故有 $a \equiv b \pmod{d}$ 。
2. 因为 $d \neq 0$ ，所以 $m \mid a-b \Leftrightarrow dm \mid d(a-b)$ ，从而 $a \equiv b \pmod{m} \Leftrightarrow da \equiv db \pmod{dm}$
3. 由 $m \mid a-b \Rightarrow m \mid ca-cb$ ，有 $a \equiv b \pmod{m} \Rightarrow ca \equiv cb \pmod{m}$ 。反之，设定 $ca \equiv cb \pmod{m}$ ，有 $m \mid c(a-b)$ 。已知 c 与 m 互质，则 $m \mid a-b$ ，得证 $ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}$ 。

Problem 9

借助于费马小定理证明如果 n 是一个正整数，则 42 能整除 $n^7 - n$ 。

答案： 只需证明 7 能整除 $n^7 - n$ 且 6 能整除 $n^7 - n$ 。

- 先证 7 能整除 $n^7 - n$ ：根据费马小定理，若 a 不是 p 的倍数，则 $a^p \equiv a \pmod{p}$ ，即 $a^{p-1} \equiv 1 \pmod{p}$ 。取 $a = n$, $p = 7$ ，若 n 是 7 的倍数， $7 \mid n^7 - n$ 显然成立；若 n 不是 7 的倍数，则 $a^6 \equiv 1 \pmod{7}$ ，即 $7 \mid (n^6 - 1)$, $7 \mid n^7 - n$ 也同样成立。
- 再证明 6 能整除 $n^7 - n$ ： $n^7 - n = n(n-1)(n^2+n+1)(n+1)(n^2-n+1)$ ， $(n-1)n(n+1)$ 必然被 2 和 3 整除，所以 $6 \mid n^7 - n$ 成立。

综上，42 能整除 $n^7 - n$ 。

Problem 10

证明：若 m 和 n 互质，则 $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$ 。

答案： 由欧拉定理， $m^{\phi(n)} \equiv 1 \pmod{n}$ ，即 $n \mid m^{\phi(n)} - 1$ 。同理 $m \mid n^{\phi(m)} - 1$ 。从而， $mn \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1)$ ，即 $mn \mid m^{\phi(n)}n^{\phi(m)} - (m^{\phi(n)} + n^{\phi(m)} - 1)$ 。而 $mn \mid m^{\phi(n)}n^{\phi(m)}$ ，故有 $mn \mid m^{\phi(n)} + n^{\phi(m)} - 1$ 。得证 $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$ 。