离散数学第六次作业

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。

a) 若 $a \mid c$, $b \mid c$, 则 $ab \mid c$

b) 若 $a \mid c$, $b \mid d$, 则 $ab \mid cd$

c) 若 $ab \mid c$, 则 $a \mid c$

d) 若 $a \mid bc$, 则 $a \mid b$ 或 $a \mid c$

答案：

a) 假。

b) 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 $ab|cd$。

c) 真。证明：存在整数 k 使得 $c = k(ab) = (kb)a$，得证 $a|c$。

d) 假。

Problem 2

证明：任何 3 个连续整数的乘积可以被 6 整除。
证明：
任意两个连续整数中必有一个能被 2 整数（为偶数），任意三个连续整数中必有一个能被 3 整除，所以三个连续整数的乘积能同时被 2 和 3 整除，因此能被 6 整除。

Problem 3

计算：

a) 23300 mod 11

b) 2^{3300} mod 31

c) 3^{516} mod 7

答案：

a) 2。$23300 = 233 * 10 * 10 = (21 * 11 + 2) * 10 * 10 \equiv 2 * (-1) * (-1) \equiv 2(mod 11)$

b) 1。$2^{23300} \equiv 2^{5*4660} \equiv 32^{4660} \equiv 1^{4660} \equiv 1(mod 31)$

c) 1。$3^6 \equiv 1(mod 7), 3^{516} \equiv 3^{6*86} \equiv 1(mod 7)$

Problem 4

证明：如果 a 和 b 为正整数，则 $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$。
证明：
分情况讨论：
(1) 当 $a < b$ 时，$a \bmod b = a$，$2^a - 1 < 2^b - 1$，$(2^a - 1) \bmod (2^b - 1) = 2^a - 1 = 2^{a \bmod b} - 1$；
(2) 当 $a \geq b$ 时，设 $a \bmod b = r$，即 $a = nb + r$，$0 \leq r < b$，再对 r 进行讨论：
(i) 当 $r = 0$ 时，$a = nb$，此时有 $(2^a - 1) \bmod (2^b - 1) = (2^{nb} - 1) \bmod (2^b - 1) = 0$（由 $x^n - 1 = (x - 1)(x^0 + x^1 + \ldots + x^{n-1})$ 易得），此时 $a \bmod b = 0$，$2^{a \bmod b} - 1 = 0$；
(ii) 当 $0 < r < b$ 时，

$$
\begin{aligned}
(2^a - 1) \bmod (2^b - 1) &= (2^{nb+r} - 1) \bmod (2^b - 1) \\
&= (2^{nb} \cdot 2^r - 2^r + 2^r - 1) \bmod (2^b - 1) \\
&= ((2^{nb} - 1) \cdot 2^r + (2^r - 1)) \bmod (2^b - 1) \\
&= (2^r - 1) \bmod (2^b - 1) \\
&= 2^{a \bmod b} - 1
\end{aligned}
$$

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 6

证明：对于任意的整数 n

a) $6 \mid n(n+1)(n+2)$

b) $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ 是整数.

证明：
a) $6|n(n+1)(n+2) \Leftrightarrow 2|n(n+1)(n+2) \wedge 3|n(n+1)(n+2)$，而 n 与 $n+1$ 中必有一个被 2 整除，故 $2|n(n+1)(n+2)$。
再设 $n = 3k + i, i = 0, 1, 2.$ 若 $i = 0$，则 $3|n$；若 $i = 1$，则 $3|n+2$；若 $i = 2$，则 $3|n+1$. 总有 $3|n(n+1)(n+2)$。
证毕。
b) 要证 $15|3n^5 + 5n^3 + 7n$ ，只需证 $3|5n^3 + 7n$ 且 $5|3n^5 + 7n$
证 $3|5n^3 + 7n$。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，$3|0$，结论成立。
假设当 $n = k(k \geq 0)$ 时结论成立,

$5(k+1)^3+7(k+1)=(5k^3+7k)+3(5k^2+5k+4)$
由归纳假设，$3|5k^3+7k$，故 $3|5(k+1)^3+7(k+1)$，即当 $n=(k+1)$ 时结论也成立。
类似可证 $5|3n^5+7n$。

Problem 7

证明:

a) 设 $d \geq 1$, $d \mid m$, 则 $a \equiv b(\mathrm{mod}\ m) \Rightarrow a \equiv b(\mathrm{mod}\ d)$.

b) 设 $d \geq 1$, 则 $a \equiv b(\mathrm{mod}\ m) \Leftrightarrow da \equiv db(\mathrm{mod}\ dm)$.

c) 设 c 与 m 互素, 则 $a \equiv b(\mathrm{mod}\ m) \Leftrightarrow ca \equiv cb(\mathrm{mod}\ m)$.

证明:
a) 设 $a \equiv b(mod\ \ m)$，有 $m|a-b$. 又已知 $d|m$，由性质“如果 $a|b$ 且 $b|c$，则 $a|c$”，得到 $d|a-b$，故有 $a \equiv b(mod\ \ d)$
b) 因为 $d \neq 0$，根据性质“设 $m \neq 0$，则 $a|b$ 当且仅当则 $ma|mb$”，
$m|a-b \leftrightarrow dm|d(a-b)$,
从而 $a \equiv b(mod\ \ m) \leftrightarrow da \equiv db(mod\ \ dm)$。
c) 由 $m|a-b \Rightarrow m|ca-cb$,
有 $a \equiv b(mod\ \ m) \Rightarrow ca \equiv cb(mod\ \ m)$。
反之，设定 $ca \equiv cb(mod\ \ m)$，有 $m|ca-cb$. 已知 c 与 m 互素，由“如果 $a|bc$ 且 a,b 互素，则 $a|c$”，必有 $m|a-b$，得证 $a \equiv b(mod\ \ m)$。

Problem 8

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。

证明:
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 $a^{p-1} \equiv 1 \pmod p$，取 $a=n$，$p=7$，若 n 是 7 的倍数 7 能整除 n^7-n 显然成立，若 n 不是 7 的倍数，则 $a^6 \equiv 1 \pmod 7$，即 $7|(n^6-1)$,7 能整除 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 能整除 n^7-n。
综上，42 能整除 n^7-n。

Problem 9

试证明: 若 $p \geq 7$ 为质数，则 $240 \mid (p^4-1)$。

证明:
因为 $p \geq 7$ 为质数，所以 p 为奇数。又因为 $p^4-1=(p-1)(p+1)(p^2+1)$，且 $p-1$ 与 $p+1$ 为相邻偶数，p^2+1 亦为偶数，故 $2\cdot 2\cdot 4 \mid (p-1)(p+1)(p^2+1)$。由费马小定理，$(3,p)=(5,p)=1$，所以 $3 \mid (p^2-1), 5 \mid (p^4-1)$，又因为 $2\cdot 2\cdot 4=16$ 与 $3,5$ 两两互质，所以 $16\cdot 3\cdot 5 \mid p^4-1$，即 $240 \mid (p^4-1)$。

Problem 10

证明：若 m 和 n 互素，则 $m^{\phi(n)}+n^{\phi(m)} \equiv 1(\mathrm{mod}\ mn)$.

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

Problem 5

记 $n=pq$(p 为 n 的一个质因子且 q 为正整数)，那么 $2^n-1=2^{pq}-1=(2^p-1)(2^{(q-1)p}+2^{(q-2)p}+\cdots+1)$ 为质数，由质数的性质可知，$2^p-1=1$ 或 $2^{(q-1)p}+2^{(q-2)p}+\cdots+1=1$，因为 $2^p-1=1$ 与 p 为质数矛盾，所以 $2^{(q-1)p}+2^{(q-2)p}+\cdots+1=1$，即 $q=1, 2^n-1=2^p-1$ 满足质数的性质，此时 $n=p$ 为质数，得证