《离散数学二》第二次作业

1. 求线性同余式 $3x \equiv 7 \pmod{10}$的解，要求分别利用扩展欧几里得方法 和 欧拉定理求解 $3^{-1} \pmod{10}$，即 $3 \pmod{10}$的逆. [提示：当 gcd(a,n)=1，则 $a^{\phi(n)-1} * a \equiv 1 \bmod n$] **（20 分）**

参考答案：用扩展欧几里得方法，$3^{-1} \pmod{10}=7$，则 $x \equiv 9 \pmod{10}$;

另外 $3^{-1} \pmod{10}= 3^{\phi(10)-1}=3^{3} \pmod{10}=7$。

2. (1)验证 16!（mod 17)=-1（mod 17)，请写出 1 到 16 中每个数 mod 17 的逆，从而辅助验证；(2)计算 15！（mod 17）**（30分）**：

参考答案：(1)参考 wilson 定理证明思路，除了 1 和 16 的模 17 逆分别为其自身，2 到 15 中每个数的逆均为其中一个数，两两配对，共 7 对， 其中 $2^{-1} \bmod 17=9$, $3^{-1} \bmod 17=6$, $4^{-1} \bmod 17=13$, $5^{-1} \bmod 17=7$, $8^{-1} \bmod 17=15$, $10^{-1} \bmod 17=12$, $11^{-1} \bmod 17=14$。

(2) 先计算 $16^{-1} \bmod 17=-1$，再在 16!（mod 17)=-1（mod 17)两端同时乘上 $16^{-1} \bmod 17$，即-1，可得 15！（mod 17)=1（mod 17)

3. 证明当质数 p|(a*b)，则 p|a 或 p|b，其中 a,b 为整数，请写出具体证明过程; 请写出一个当 p 不是质数时, 上述结论不成立的例子。**(10 分)**

参考答案：当 $p \nmid a$，我们证明 p|b；由 $p \nmid a$，可知 gcd(p,a)=1，则可直接推出 p|b （参考基本算术定理的唯一性证明中用到的引理）；当 $p \nmid b$ 则 p|a 的证明思路类似。P 不是质数的例子：12|(4*6)，但 $12 \nmid 4$ 且 $12 \nmid 6$。

4. 用中国剩余定理求解下列方程组，写出具体求解过程：

$x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$. (**20** 分)

参考答案：$x \equiv 323 \pmod{330}$

5. 如 a 和 b 为互质的正整数，证明 $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$. **(20分)**

参考答案:

证明：根据欧拉定理，$a^{\phi(b)} \equiv 1 \pmod b$，且 $b^{\phi(a)} \equiv 1 \pmod a$，即 $a^{\phi(b)}-1$ 为 b 的倍数，$b^{\phi(a)}-1$ 为 a 的倍数，那么$(a^{\phi(b)}-1)*(b^{\phi(a)}-1)$为 ab 的倍数；上式展开为 $a^{\phi(b)}*b^{\phi(a)}-(a^{\phi(b)}+b^{\phi(a)}-1)$为 ab 的倍数；

因为 $\phi(b)$和 $\phi(a)$均为大于或等于 1 的正整数，可知 $a^{\phi(b)}*b^{\phi(a)}$ 为 ab 的倍数，推出 $a^{\phi(b)}+b^{\phi(a)}-1$ 也为 ab 的倍数，得证。