《离散数学二》第二次作业

1. 求线性同余式3x ≡ 7 (mod 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 (mod 10), 即 3 (mod 10)的逆. [提示：当gcd(a,n)=1, 则aφ(n)-1 \*a ≡ 1 mod n] **（20分）**

**参考答案：**用扩展欧几里得方法，3-1 (mod 10)=7，则 x ≡ 9 (mod 10);

另外3-1 (mod 10)= 3φ(10)-1=33 (mod 10)=7。

1. (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 mod 17=9, 3-1 mod 17=6, 4-1 mod 17=13, 5-1 mod 17=7, 8-1 mod 17=15, 10-1 mod 17=12, 11-1 mod 17=14。

(2) 先计算16-1 mod 17=-1，再在16! (mod 17)=-1 (mod 17)两端同时乘上16-1 mod 17，即-1，可得15！(mod 17)=1 (mod 17)

1. 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∤a，我们证明 p|b; 由p∤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∤b则 p|a的证明思路类似。P不是质数的例子：12|(4\*6)，但12∤4且12∤6。

1. 用中国剩余定理求解下列方程组，写出具体求解过程：

x ≡ 1 (mod 2), x ≡ 2 (mod 3), x ≡ 3 (mod 5), and x ≡ 4 (mod 11). (**20**分)

参考答案：x≡323 (mod 330)

1. 如a和b为互质的正整数，证明aφ(b) +bφ(a) ≡1 (mod ab). **（20分）**

**参考答案：**

证明：根据欧拉定理，aφ(b) ≡1 (mod b)，且bφ(a) ≡1 (mod a)，即

aφ(b) -1为b的倍数，bφ(a) -1为a的倍数，那么(aφ(b) -1)\*( bφ(a) -1)为ab的倍数；上式展开为 aφ(b) \*bφ(a) -(aφ(b)+ bφ(a) -1)为ab的倍数；

因为φ(b)和φ(a)均为大于或等于1的正整数，可知aφ(b) \*bφ(a) 为ab的倍数，推出aφ(b)+ bφ(a) -1也为ab的倍数，得证。