

## 《离散数学二》第二次作业

1. 求线性同余式  $3x \equiv 7 \pmod{10}$  的解, 要求利用扩展欧几里得方法求解  $3^{-1} \pmod{10}$ , 即  $3 \pmod{10}$  的逆. (20 分)

2、完成以下内容 (30 分)

a) 用欧几里得算法反向处理的方法以及扩展欧几里得算法把  $\gcd(100001, 1001)$  表示成 100001 和 1001 的线性组合 (20 分)。

b) 利用费马小定理求  $23^{1002} \bmod 41$  (10 分)。

3、证明当素数  $p \mid (a*b)$ , 则  $p \mid a$  或  $p \mid b$ , 其中  $a, b$  为整数, 请写出具体证明过程; 请写出一个当  $p$  不是素数时, 上述结论不成立的例子 (10 分)

4、用中国剩余定理求解下列方程组, 写出具体求解过程 (20 分)

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 4 \pmod{11}$$

5、 $N=55, k=37, t=54$  (20 分)

(1)  $k$  作为公钥, 求密文  $t$  对应的明文.

(2)  $k$  作为私钥, 求明文  $t$  对应的密文.