1. 用扩展欧几里得算法把 gcd(100001, 1001) 表示成 100001 和 1001 的线性组合。（10 分）

2. 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求解 3^{-1} (mod 10), 即 3 (mod 10)的逆. （20 分）

3. 证明当素数 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：

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

5. 利用费马小定理求23^{1002} **mod** 41. （10 分）

6. N=55, k=37, t=54（30 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.