考试范围

1、 整除、同余的基本性质

2、 欧几里得求最大公约数

3、 如何构造两个互素的整数

4、 逆元计算方法

5、 欧拉函数计算

6、 利用欧拉定理、费马定理求解

7、 RSA 加密解密过程及证明。

8、 中国剩余定理求解同余方程

9、 原根与指数的基本定理与性质

10、 判断平方剩余、高斯互反律

11、 素数确定性判别算法

12、 素数的概率判别算法

练习题

1、 正合数 n 的最小正因子 p，则 p 一定是素数，且 p≤$\sqrt{\mathbf{n}}$。

2、 厄尔托斯筛法寻找素数，200 内

3、 7 ｜ n， 5 ｜ n，则 35 ｜ n

4、 假设 n, a, b,是三个整数 c≠0，如果 c ｜ a*n，c ｜ b*n,如果（a , b）=1, 求证 c ｜ n。

5、 如果 a 是整数，则$\boldsymbol{a^3-a}$能够被 3 整除

6、 奇整数的平方具有形式 8k+1。

7、 a，b ，q，r 是整数，如果 a = q * b + r，证明（a，b）=（b，r）。

8、 假设 a，b 是两个非零正整数，证明（a , b）*[a , b] = a * b。

9、 运用广义欧几里得除法求整数 s，t 使得 s*167 + t*335 = （167，335）

10、 写出模 11 的简化剩余系，并列举每个简化剩余的阶（ord11）

11、 x= 2 mod 7， x = 3 mod 5 ，利用中国剩余定理求 x mod 35

12、 p，q 是两个不相等的大素数，n= p*q，选择整数 e 使得（e, φ(n)）=1，计算 d 使得 ed = 1 mod φ(n)，对于任意的整数 m∈[1,n-1]，证明 $\boldsymbol{m^{ed}}$=m mod n。

13、 求解同余方程：33x=22 mod 77

14、 计算 60mod 137 是否为平方剩余。

15、 p 是奇素数，证明在模 p 的简化剩余系中，平方剩余与平方非剩余的个数都是$\frac{\mathbf{p-1}}{\mathbf{2}}$个。

16、 Fermat 素数检测和 Miller-Rabin 素数检测过程