一、（10 分）求解同余方程$x^2 \equiv 2(mod\ 311)$

答案：$\pm 66(mod\ 311)$

二、（10 分）给出模 19 的全部二次剩余，并用欧拉判别法判断 17 是否是 37 的二次剩余.

答案：1, 4, 5, 6, 7, 9, 11, 16, 17。 17 不是 37 的二次剩余。

三、（10 分）判断方程$x^2 \equiv 438\ (mod\ 593)$有多少解. 其中 593 为素数.

答案：无解

四、（10 分）用**雅可比符号**的计算方法求解勒让德符号$\left(\frac{1189}{1847}\right)$，其中 1847 是素数，1189 是合数.

答案：1

五、（10 分）求 50 的最小正原根，并用它构建出 50 的全部原根和 50 的一个既约剩余系.

答案：50 的最小原根是 3; 50 的全部原根$\{3^1, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}\}$; 50 的既约剩余系$\{3^1, 3^2, \dots, 3^{20}\}$

六、（10 分）下面的字符串是用维吉尼亚密码加密得到的密文：CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVX. 假定已破解出密钥为 JANET，计算上述密文在该密钥长度下的重合指标，并解密上述密文中带下划线部分的内容.

答案：重合指标: 0.0833(1/12), 0.0833(1/12), 0.1111(1/9), 0.0556(1/18), 0.0556(1/18);

明文: the almond tree

七、（12 分）设p是奇素数，$p \nmid n$，$\left(\frac{n}{p}\right) = 1$. 当$p \equiv 5(mod\ 8)$时，证明：

(1) 若$n^{\frac{p-1}{4}} \equiv 1(mod\ p)$，则$x^2 \equiv n(mod\ p)$的解为$x \equiv \pm n^{\frac{p+3}{8}}(mod\ p)$.

(2) 若$n^{\frac{p-1}{4}} \equiv -1(mod\ p)$，则$x^2 \equiv n(mod\ p)$的解为$x \equiv \pm\left(\frac{p-1}{2}\right)! \cdot n^{\frac{p+3}{8}}(mod\ p)$

答案：参看课件，定理 4.3.1(2)

八、（13 分）在 RSA 密码体制中，取$n = 41 \times 67$，在$\{11, 17, 25\}$这三个数中选出一个满足要求的加密指数b，求出解密指数a，并对密文$y = 23$进行解密

答案：$b = 17, a = 1553$; 明文: $23^{1553}\ mod\ 2747 = 2204$

九、（15 分）在 Fiat-Shamir 协议中，设$n = 3953 = 59 \times 67$，Alice 想向 Bob 证实她拥有秘密信息:$v_1 = 1001, v_2 = 21, v_3 = 3097, v_4 = 877$.

(1) Alice 公开信息s_1, s_2, s_3, s_4，其中$s_1 = 959, s_2 = 1730, s_3 = 2895$，求$s_4$.

(2) 假设 Alice 选取的随机数$r = 313$, Bob 选取$\{1,2,3,4\}$中的子集$S = \{1,3,4\}$，求 Alice 发送给 Bob 的y的值.

(3) 给出 Bob 验证需要的计算.

答案：(1) $s_4 = 2667$

(2) $y = 3632$

(3) 验证$y^2 \cdot \prod_{i \in \{1,3,4\}} s_i \equiv 3097 \equiv x\ (mod\ 3953)$