**Lab\_1 Questions**

**Question 1.** First it will generate an integer between 0 and function parameter n randomly, this integer is the candidate, then it will set the last bit of candidate true, and that means if it is an even number, it will add 1 and become an odd number. Then determine if it is a prime number, if it is, the function will return candidate

**Question 2.** In IDEA

So if we are talking about perfectly safety, I think iteration is better than Miller-Robain, even though the odds of failure is very very small, it still can not guarantee that it is a prime number. However, in the real application, the complexity of the iteration is huge, which requires a lot of computing power. In general, miller-robain is a better choice.

**Question 3.** First, we define tow variables s and d, and they come from rewrite candidate, it may a function, I don’t know the specific method, then it is a five times iteration, then define a variable basis equal to a random number, which generate from 2 to candidate, and define a mutable variable x equal to mod\_exp function, this function implement a kind of calculation of ‘basis’ ‘d’ ‘candidate’,

If x equal to 1 certain unit or candidate minus 1, continue to iterate, if iterate five times x satisfy the condition, the function will return true. If x doesn’t meet the condition, set another iteration, iterate s minus 1\_usize minus one times, x equal to mod\_exp(x,2,candidate), if x equal to 1\_usize, return false, if x equal to candidate minus 1\_usize, break the iteration and return false. If x doesn’t match these conditions, it will return to the upper iteration

**Question 4.** Galss-pumpkin