**Lab works 2022**

**L1. Congruence, Repeated squaring, Euler theorem**

1. Find the 3 last digits of 20182019
2. Find the remainder when 2018201920192018 is divided by 12345
3. Find the remainder when  is divided by 1001.

**L2. Square root of -1.**

Find the number m such that m2 + 1 is divisible by p for following p

1. p = 2029
2. p = 1003001

**L3. Euclidean Algorithm**

Find the GCD of following pairs of integers

1. 2021019 and 1431471
2. 1234567 and 234569
3. 1234567 and 56789

**L4. Extended Euclidean Algorithm**

a) Find x, y such that ax + by = (a, b) for a =123456789, b = 97654321

b) Find the modular inverse of 37 mod 2019

c) Find the modular inverse of 372 mod 20192.

**L5. Effective Fermat**

For following p, find integers a, b such that p = a2 + b2.

p = 2017 p = 1

46837 p = 252497801

**L6. Rational Reconstruction**

Recover following fractions from its decimal representation

(3/3, 4/4, 5/5 respectively)

0.372636, 0.373346671, 0.2173836482

**L7. Chinese Remaindering**

a) When divide number A by 54 the remainder is 363. The number A is divisible by 16. Find the last 4 digits of A.

b) Do chinese remaindering for 12345 🡪 6789, 56789 🡪 54292.

c) Do chinese remaidnering for 41 🡪 30, 152 🡪 87, 263 🡪 127.

**L8. Computing Jacobi symbol**

Find Jacobi notation (or Legendre notation): (1983 | 2017), (873 | 2019), (474993 | 1003001)

**L9. Discrete Logarithm**

Find x such that 37x ≡ 235 mod 2003

**L10. Computing Square root**

Find x such that x2 ≡ a mod n for

1. a = 448, n = 673
2. a = 448, n = 6732
3. a = 448, n = 20193