Cryptography and Security 2017

Exercise Sheet 2

Exercise 1 Coprime (SAGE)

Write your own function *mycoprime(N)* that returns all numbers $x < N$ coprime to a number N. Compute *mycoprime(100)*.

Exercise 2 Goldbach Conjecture (SAGE)

1. Write a function that checks the following conjecture. If N is even and $N > 2$, then N can be written as the sum of two primes. Verify the conjecture for the first 1000 even integers.
2. Write a function that returns for a given number N all such pairs of primes without any duplicate. Try it for 100.

Exercise 3 Multiplicative Group (SAGE)

Given N, write a function that

- Creates the ring $\mathbb{Z}/N\mathbb{Z}$.
- Prints whether the group of units is cyclic or not.
- Prints generators for the group of units.
- Using these generators, creates a list containing all the elements in the group $(\mathbb{Z}/N\mathbb{Z})^*$ and prints it.
- Tests Lagrange's theorem for a random element of this group.

  (Hint: it may be better to look for sage functions for the second and third bullets.)

Exercise 4 Perfect Power (SAGE)

Write a function that, given a number n, returns (x, b), with $x, b \in \mathbb{Z}$ and $b > 1$ such that $x^b = n$ if such a pair exists. If no such pair exists, return false.

Test your function with $589700950065322297792301221688 23$, 123^{1237} and with 456456456.