2. PART II

Exercise 2.1. For each integer $10^{20} \leq n \leq 10^{20} + 100$, determine whether n can be written as the sum of two perfect square (i.e. there exist x, y such that $x^2 + y^2 = n$) and print the string $n = x^2 + y^2$. You can use the function `NormEquation(d,n)`. This function return a solution of the equation $x^2 + y^2 d = n$ if exists.

Exercise 2.2. Choose randomly a prime power $0 \leq q \leq 1000$. Check that $x^q - x = 0$ for any $x \in GF(q)$. (You can use the function `IsPrimePower(q)`.)

Exercise 2.3. Write a function `RandomPolynomialOfDegree(q,d)` that return a random polynomial of degree d over $GF(q)$. You need to define the univariate polynomial ring over $GF(q)$.

Exercise 2.4. Write a function `EuclideanAlgorithm(f,g)` that implements the Euclidean algorithm for polynomials.

Exercise 2.5. Write a function `Factorize(p)`, p prime, that returns the factorization of the polynomial $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$ as in *Exercise 6.4*.

Exercise 2.6. Write a function that, for a given polynomial $f(x, y) \in GF(q)[x, y]$, returns the $q \times q$ matrix whose i, j component if $f(i, j)$, where $i, j \in GF(q)$.

Exercise 2.7. Write a function that, for a set of vectors, return the cardinality of the biggest set of linearly independent vectors.

Exercise 2.8. Write a function `RotatePolynomial(f,k)` that, for a given polynomial $f(x) \in GF(q)[x]$ of degree d, return the polynomial $g(x) \in GF(q)[x]$ of degree d obtained by rotating the coefficient of $f(x)$ by k.