Problem 1 Factoring with Pollard’s $p−1$ Method  
5 Points
Apply Pollard’s $p$-1 algorithm to the problem of factoring 319 and 341. Explain why a naïve application of the algorithm fails, when trying to factor 341.

Problem 2 Factoring with ECM  
3+3 Points
Let $p$ be a prime number such that $p \equiv 3 \pmod{4}$ and $k$ an integer not divisible by $p$. Let $E_k$ be the curve over $\text{GF}(p)$ given by $y^2=x^3-kx$.

(a) Show that $-1$ is not a square mod $p$ and conclude that $E_k$ has exactly $p+1$ points.

(b) Explain why using the curve $E_k$ in ECM with different values for $k$ is not a good idea for factoring an integer $n$.

Problem 3 Factoring with Dixon’s Random Square Method  
4 Points
Use Dixon’s random square method to find a factor of $n:=2041$. As factor base you can use $B:=\{-1, 2, 3, 5, 7\}$.

Hint: As random values $x$, choosing $x \in \{43, 44, 45, 46\}$ could be helpful.

Problem 4 Interpolation  
2+3 Points
(a) Prove or disprove: For any non-empty list of pairwise different integers $[u_1,…,u_n]$ and any list of integers $[v_1,…,v_n]$ there exists a unique univariate polynomial $f$ of degree less than $n$ with integer coefficients such that $f(u_i)=v_i$ for all $i=1, \ldots, n$.

(b) Let GF$(4)$ be a field with four elements and $\alpha \in \text{GF}(4)$ such that $\alpha^2+\alpha+1=0$. Using Lagrange interpolation, find a polynomial $p \in \text{GF}(4)[x]$ of minimal possible degree such that all of the following hold: $p(0)=1$, $p(1)=\alpha^2$, $p(\alpha^2)=0$.

Good luck & please have fun and feel free to ask questions!!