Project in 01427 – Advanced topics in cryptology F06

Let p be a prime chosen to just fit in a computer word (i.e. use the magma command

```
p=PreviousPrime(x);
```

to find a prime just below x) and so that an irreducible binomial of degree 5 exists over $\mathbb{F}_p$.

[Exercise 1] What is the condition on p to have an irreducible binomial of degree 5?

[Exercise 2] Give an irreducible binomial of degree 5 over $\mathbb{F}_p$ together with a proof that it is indeed irreducible. You may use MAGMA for the computations of GCDs and divisions but not simply as `IsIrreducible` (but please use this though to check your polynomial before starting on the proof).

[Exercise 3] Program the field operations `add, sub, mul, inv` (addition, subtraction, multiplication, inversion) for $\mathbb{F}_{p^5}$ in C or C++. Note that no long integer library is needed.

[Exercise 4] Do the same to implement field arithmetic in $\mathbb{F}_{p'^{11}}$, where p' is chosen such that the fields $\mathbb{F}_{p^5}$ and $\mathbb{F}_{p'^{11}}$ have about the same cardinality. Compare the speeds and explain the behavior.

[Exercise 5] Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_{p^5}$, i.e. $4A^3 + 27B^2 \neq 0$ and $A, B \in \mathbb{F}_{p^5}$.
Write a program that on input an integer m computes $[m]P$, where the E and the point $P \in E(\mathbb{F}_{p^5})$ may be hardcoded in the program (check, that P has sufficiently high order).

[Extra 6] Use other coordinate systems like projective or Jacobian coordinates and compare the speeds.

[Extra 7] Under which conditions is it possible to use Montgomery addition? How fast is an implementation using Montgomery coordinates on a suitable curve.

Just as a reminder, the MAGMA calculator is available at
`http://magma.maths.usyd.edu.au/calc/`