CS 402 Cryptography

Problem Sheet 7

(1) Let $n = 2701$. Use the B-numbers 52^2, 53^2 mod n for a suitable factor base B to factorise 2701. What are the vectors ε corresponding to 52 and 53?

(2) Let $n = 4633$. Use 68, 152 and 153 with a suitable factor base B to factorise 4633. What are the corresponding vectors ε?

(3) Use Pollard's method with $k = 840$ and $a = 2$ to try to factorise 53467. Then try with $a = 3$.

(4) Explain why Pollard's method is unlikely to find the prime factorisation 383×1283 of 491389. What is the moral of this example with regard to RSA?

(5) What is an *elliptic curve* over a field of characteristic different from 2 or 3? Describe, using a suitable picture, how to add two points on an elliptic curve over $\mathbb{R}$, to obtain a uniquely defined third point on the curve.

(6) Verify that $y^2 = x^3 - x$ determines an elliptic curve over $\mathbb{R}$. Sketch a graph of the curve, and from this sketch determine the sum of the points $(-1, 0)$ and $(1, 0)$ on the curve.

(7) Verify that $y^2 = x^3 - 225x$ is an elliptic curve over $\mathbb{R}$, and that $P = (-9, 36)$, $Q = (15, 0)$ are points on the curve. Find $P + Q$, $P - Q$, and $2P$. What is nQ, where n is a positive integer? Is there a graphical interpretation in this last case?

In the next few problems, recall what is meant by the order of a finite group, and the order of an element of a (not necessarily finite) group.

(8) Give an example of an elliptic curve over $\mathbb{R}$ which has exactly two points of order 2, and another example which has exactly four points of order 2.

(9) Let P be a point on an elliptic curve over $\mathbb{R}$. Give a geometric condition that is equivalent to P being a point of order (a) 2, (b) 3, (c) 4.

(10) Let p be a prime, $p \equiv 3 \bmod 4$. Consider the elliptic curve E over $\mathbb{Z}_p$ determined by $y^2 = x^3 - x$. Prove that the group of points on E has order exactly $p + 1$.