Math 418/818
Take-Home Exam, Part 2

Due 18 December 2015

5. (a) By stating appropriate propositions from our textbook (give precise references), explain what we know about an odd number \( n > 1 \) if it passes the Miller-Rabin test \( k \) times. What do we know if it fails the test?

(b) Let \( n > 1 \) be an odd number, and let \( \mathcal{P}_n = \{ b (\text{mod } n) : b^{n-1} \equiv 1 \pmod{n} \} \) be the set of bases \( b \) for which \( n \) is a pseudoprime to the base \( b \). Prove that

\[
|\mathcal{P}_n| = \prod_{p|n} \gcd(p - 1, n - 1).
\]

[Note: You can use the result of Question 1(b)* of Assignment 4.]

(c) Deduce from the formula in part (b) that a composite odd number \( n \) is a Carmichael number if and only if \( n \) is square free and \( (p - 1) | (n - 1) \) for all primes \( p | n \).

6. (a) Write a MAPLE program \texttt{addpts}(pt1, pt2, a, p) which adds two points \( pt1 = [x_1, y_1] \) and \( pt2 = [x_2, y_2] \) on the elliptic curve \( E : y^2 = x^3 + ax + b \) over \( \mathbb{F}_p \). (Use the symbol \([\] \) (empty list) to denote the point \( P_\infty \) at infinity.) Write your addition program in such a way that it also works if one or both of the points are \( P_\infty \).

(b) Use your program to add the following pairs of points:

(i) the points \( P_1 = P_2 = (-2, 3) \) on the curve \( y^2 = x^3 + 17 \) over \( \mathbb{F}_{31} \);

(ii) the points \( P_1 = (-2, 3) \) and \( P_\infty \) on the curve of part (i);

(iii) the points \( P_1 = (8, 23) \) and \( P_2 = (2, 4) \) on \( y^2 = x^3 + 50x + 5 \) over \( \mathbb{F}_{97} \).

(c) Using your program in (a), write a program \texttt{ordpt}(pt, a, p) which computes the order of a point \( pt = [x, y] \) on the above curve.

(d) Use your program of part (c) to find the order of the following points:

(i) \( P_\infty \) and \( P_1 = (0, 1) \) on the elliptic curve \( E_1 : y^2 = x^3 + 4x + 1 \) over \( \mathbb{F}_p \) with \( p = 17 \);

(ii) \( P_2 = (1, 2) \) on the elliptic curve \( E_2 : y^2 = x^3 + 2x + 1 \) over \( \mathbb{F}_p \) with \( p = 997 \).

(e) Use the results of your calculations in (d) to determine the order and structure of the groups \( E_1(\mathbb{F}_{17}) \) and \( E_2(\mathbb{F}_{997}) \). (Justify your answer.)
7. For the elliptic curves $E_1, E_2, E_3,$ and $E_4$ defined below, determine the structure of the groups $E_k(\mathbb{F}_{13})$ by using the information given below together with a minimal amount of extra (hand) calculation. (Hint: Look at the 2-torsion and/or 3-torsion points of $E_k$.) Be sure to include enough calculation to justify your conclusions. (Do not refer to MAPLE computations; all calculations should be done by hand.)

(a) Let $E_1 : y^2 = x^3 + x + 2$ and $E_2 : y^2 = x^3 + 1$, and use the fact that $|E_1(\mathbb{F}_{13})| = |E_2(\mathbb{F}_{13})| = 12$.

(b) Let $E_3 : y^2 = x^3 + 3$ and $E_4 : y^2 = x^3 + 3x + 5$, and use the fact that $|E_3(\mathbb{F}_{13})| = |E_4(\mathbb{F}_{13})| = 9$.

8. Describe the elliptic curve analogue (ECDSA) of the Digital Signature Algorithm:

(a) Explain how to generate the ECDSA key and how to generate the signature.

(b) Explain how the receiver ($B$) verifies the sender’s ($A$) signature.

(c) Explain why the protocol works, i.e. why $B$ should expect that the two numbers are equal.

(d) Explain why $B$ should be satisfied that it was $A$ who sent the message (in the case that the two numbers agree). More precisely, give a careful analysis of why we expect that signature test should fail if a spy (Eve) alters the message.

Instructions for the take-home exam: See the instructions in part 1 of the exam.

Instructions for the MAPLE question #6: Hand in your computer output of this question. On the top, put your name(s) using MAPLE’s text feature. In addition, use MAPLE’s text feature to label your questions and to document/explain your MAPLE programs and output. See also the Maple instruction sheet.