Math 1580 Final Exam 2011

Instructions:

- The exam is due in 303 Kassar by 5pm on Tuesday, December 13. Slide it under the door if Professor Kottke is not in. (The Kassar building closes at 5pm, so don't be late!)
- There are 7 problems of equal point value.
- You may use the textbook as well as a computer algebra system such as Wolfram alpha, but no other resources, either online or offline.
- Besides the use of a computer algebra system, you may not write computer code to solve the problems.
- You must complete the final on your own – no collaboration is allowed.
- Please sign the statement below and return this cover sheet with your completed exam.

By signing my name below, I affirm that all my answers to this exam are my own, that I did not discuss the contents of the exam with anyone, and that I have consulted only the resources permitted above during the time in which I completed this exam. I understand that doing otherwise constitutes a violation of Brown University's Academic Code.

Name: ____

Signature: ____

Problem 1. Alice and Bob are exchanging messages using ElGamal with the prime $p = 439$ and the base $g = 15$, which is a primitive root. Alice's public key is $g^a = 19$ and Bob sends her the encrypted message

$$c = (g^b, g^{ab}m) = (238, 159).$$

You are Eve. Find m by a method of your choice, showing your intermediate steps.

Problem 2. Find a quadratic polynomial $q(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with coefficients satisfying $-52 < a, b, c < 52$, whose roots mod p are

$$\begin{aligned} &\{0, -1\} \quad \text{for } p = 3, \\ &\{2, -2\} \quad \text{for } p = 5, \text{ and} \\ &\{1, -2\} \quad \text{for } p = 7. \end{aligned}$$

(In other words, for each set $\{\alpha_1, \alpha_2\}$ we have $q(\alpha_i) = 0 \pmod{p}$ for $i = 1, 2$.)

Problem 3. Consider the elliptic curve

$$E : y^2 = x^3 + 1$$

over a field $\mathbb{F}_p$, and suppose $\mathbb{F}_p$ contains an element ω such that $\omega^3 = 1$. Define a map ϕ by

$$\phi(x, y) = (\omega x, y), \qquad \phi(\mathcal{O}) = \mathcal{O}.$$

(a) Suppose $P \in E(\mathbb{F}_p)$. Show that $\phi(P) \in E(\mathbb{F}_p)$.

(b) Show that ϕ respects the addition law over E, in other words

$$\phi(P_1 \oplus P_2) = \phi(P_1) \oplus \phi(P_2)$$

for all $P_1, P_2 \in E(\mathbb{F}_p)$.

Problem 4. Describe a Pollard ρ algorithm which solves the ECDLP (Elliptic Curve Discrete Logarithm Problem) $nP = Q$ in an elliptic curve $E(\mathbb{F}_p)$. You may assume the order N of P in $E(\mathbb{F}_p)$ is known.

Problem 5. Find a good rational approximation $a/b \approx x$ for the number

$$x = 0.6923$$

where "good" means that a and b have small integer coefficients, (i.e. much smaller than 6923 and 10000). To find your answer, set up an integer lattice problem that simultaneously minimizes a, b, and the quantity $10000(a-bx)$ (Hint: you should have a 2-dimensional lattice in $\mathbb{Z}^3$), and then solve this problem.

Problem 6. Let R_q denote the convolution polynomial ring

$$R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N - 1)$$

where q is prime. For any $\alpha \in \mathbb{Z}/q\mathbb{Z}$ we can define an *evaluation map*

$$\mathrm{ev}_\alpha : R_q \longrightarrow \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{f}(x) \longmapsto \mathrm{ev}_\alpha\big(\mathbf{f}(x)\big) = \mathbf{f}(\alpha)$$

which just evaluates the polynomial at $x = \alpha$. Find a relation between N and q so that this evaluation map respects both addition and multiplication for all α, in other words so that

$$\begin{aligned} \mathrm{ev}_\alpha\big(\mathbf{f}(x) + \mathbf{g}(x)\big) &= (\mathbf{f} + \mathbf{g})\,(\alpha) = \mathbf{f}(\alpha) + \mathbf{g}(\alpha) \in \mathbb{Z}/q\mathbb{Z}, \text{ and} \\ \mathrm{ev}_\alpha\big(\mathbf{f}(x) \star \mathbf{g}(x)\big) &= (\mathbf{f} \star \mathbf{g})\,(\alpha) = \mathbf{f}(\alpha)\mathbf{g}(\alpha) \in \mathbb{Z}/q\mathbb{Z}. \end{aligned}$$

Problem 7. Alice and Bob are exchanging messages using NTRU with $p = 3$.

(a) Suppose Bob foolishly uses the same ephermal key $\mathbf{r}(x)$ to encrypt two different messages $\mathbf{m}_1(x)$ and $\mathbf{m}_2(x)$. Explain how Eve can use the two ciphertexts $\mathbf{e}_1(x)$ and $\mathbf{e}_2(x)$ to determine approximately 2/9 of the coefficients of $\mathbf{m}_1(x)$. For example, the ciphertexts

$$\begin{aligned} \mathbf{e}_1(x) &= 32 + 21x - 9x^2 - 20x^3 - 29x^4 - 29x^5 - 19x^6 + 38x^7 \\ \mathbf{e}_2(x) &= 33 + 21x - 7x^2 - 19x^3 - 31x^4 - 27x^5 - 19x^6 + 38x^7 \end{aligned}$$

were encrypted using the same ephermal key. Which coefficients of $\mathbf{m}_1(x)$ can Eve determine?

(b) Show that in general if Eve knows t of the coefficients of $\mathbf{m}(x)$, she can set up a CVP of dimension $2N - t$ to find $\mathbf{m}(x)$. (See exercise 6.32 in the book for more clues on how to formulate NTRU decryption as a Closest Vector Problem.)