ASSIGNMENT 6 - MATH235, FALL 2009

Submit by 16:00, Monday, October 19

1. Calculate the following:
   (1) $(2^{19808} + 6)^{-1} + 1 \pmod{11}$.
   (2) $12, 12^2, 12^4, 12^8, 12^{16}, 12^{25}$ all modulo 29.

2. Use the Euclidean algorithm to find the gcd of the following pairs of polynomials and express it as a combination of the two polynomials.
   (1) $x^4 - x^3 - x^2 + 1$ and $x^3 - 1$ in $\mathbb{Q}[x]$.
   (2) $x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.
   (3) $x^4 + 3x^3 + 2x + 4$ and $x^2 - 1$ in $\mathbb{Z}/5\mathbb{Z}[x]$.
   (4) $4x^4 + 2x^3 + 3x^2 + 4x + 5$ and $3x^3 + 5x^2 + 6x$ in $\mathbb{Z}/7\mathbb{Z}[x]$.
   (5) $x^3 - ix^2 + 4x - 4i$ and $x^2 + 1$ in $\mathbb{C}[x]$.
   (6) $x^4 + x + 1$ and $x^2 + x + 1$ in $\mathbb{Z}/2\mathbb{Z}[x]$.

3. Diffie-Hellman's key exchange protocol.

The Diffie-Hellman key exchange protocol is a method to allow two parties, A and B, to share a secret while communicating "in the open". It was a revolutionary idea at the time. Here is how it's done. A third party, trusted by A and B chooses a large prime number p and a non-zero element $g \in \mathbb{Z}/p\mathbb{Z}$ such that $\{g, g^2, \dots, g^{p-1}\}$ are precisely all the non-zero congruence classes modulo p. The data p and g are then published for anyone to use.

A chooses a number a and B chooses a number b. A sends to B the element g^a modulo p and B sends to A the element g^b modulo p. The communication is done over an open channel. Then A calculates $(g^b)^a$ – the a-th power of the number A got from B, and B calculates $(g^a)^b$ – the b-th power of the element he got from A. Now both know $g^{ab} = (g^a)^b = (g^b)^a$. This is their shared secret. The assumption is that it is not feasible to an eavesdropper to calculate g^{ab} from the data g^a, g^b.

Answer the following questions.
   (1) What is it exactly that we need to know about integers modulo p to be sure that A and B indeed arrive at the same congruence class modulo p?
   (2) It is a fact that a g as above exists. Explain why we do not want to choose g such that $g^2 = 1$, or $g^3 = 1$, for example.
   (3) Let $p = 13$. Find all the elements g mod 13 that have the property that $\{g, g^2, \dots, g^{12}\}$ are precisely all the non-zero congruence classes modulo 13. (Labor reduction hint: if you

have calculated $\{g, g^2, \ldots, g^{12}\}$ note that you can easily determine the list $\{h, h^2, \ldots, h^{12}\}$ for any h of the form g^i.)

(4) Suppose one had a method to determine a knowing g^a and g (i.e., one could solve the "discrete log problem"). Explain how one would then break the security of Diffie-Hellman.

(5) Suppose that three parties A, B, C, wanted to share a secret. Propose a method to do that.