Section 5

Wednesday, July 10

CS 70: Discrete Mathematics and Probability Theory, Summer 2013

1. In the RSA encryption algorithm, let $p = 3$, $q = 11$, and $e = 7$.

   1a. What is the public key?

   1b. What is the private key?

   1c. Encrypt the message $x = 32$. (Hint: find a trick to make this calculation easy.)

   1d. Decrypt the message $y = 6$.

2. Use repeated squaring to compute 2^{21} mod 13.

3. Practice with Lagrange interpolation!

   3a. Find the coefficients of the polynomial of degree ≤ 2 that fits the points $(-1, 1)$, $(0, 1)$, $(1, 2)$ in the real numbers (i.e., familiar, non-modular arithmetic).

   3b. Find the coefficients of the polynomial of degree ≤ 2 that fits the points $(-1, 1)$, $(0, 1)$, $(1, 2)$ in $GF(3)$ (i.e., arithmetic modulo 3).

4. Consider two polynomials $p(x), q(x)$ whose product is zero: that is, $p(x) \cdot q(x) = 0$ for all x.

   4a. Show that if $p(x)$ and $q(x)$ are polynomials over the real numbers then in this case, either $p(x) = 0$ for all x or $q(x) = 0$ for all x (or both). (Hint: You may want to first prove this lemma, true in all fields: The set of roots of $p(x) \cdot q(x)$ is the union of the roots of $p(x)$ and $q(x)$.)

   4b. Show that, in contrast, over $GF(p)$ there exist such polynomials whose product is zero but which are both nonzero. (A polynomial $p(x)$ is nonzero if $p(x) \neq 0$ for some, but not necessarily all, x.) (Hint: Fermat's Little Theorem is useful here.)