CS 280 Fall '03, Homework 5

October 30, 2003

Due in class Wednesday, November 5.

1. (a) Evaluate $7^{1001} \bmod 11$.
   (b) Calculate $\varphi(120)$ and $\varphi(384)$.
   (c) Show that $(n^{13} - n)$ is divisible by 2, 3, 5, 7 and 13 $\forall n \in \mathbb{Z}$.
   (d) Show that if $n \geq 2$ and p is a prime such that $p|n$ but $p^2 \not| n$ then $p^{\varphi(n)+1} \equiv p \bmod n$. Can you find and prove a generalisation of this?
   (e) Explain carefully what happens if in the RSA cryptosystem we were to allow larger block sizes (relative to the two primes used) so that some of the blocks could fail to be relative prime to $n = pq$. (Illustrate with a specific example under encoding and decoding.)

2. In the following, translate messages into numbers base 26 so that, for example, "hi" would become $h.26^1 + i.26^\circ = 7.26 + 8.1 = 190$.
   (a) Suppose Xak sends a message to Yoshi using RSA with $p = 17$, $q = 43$. Assuming that Xak has written the message as a long string of characters and then encoded it by encrypting successive pairs of letters (translated as indicated above) via public key $e = 29$ and public modulus $n = 731$, decode 290 369 203 405 033 511 584 612 213.
   (b) Now Zoltan sends a message to Yoshi using $p = 113$, $q = 157$ and $e = 12707$. Using three-letter blocks, encrypt "This is mad".
   (c) With the same p, q, and e as in part (b), and assuming each block of five digits represents a block of three letters, decrypt 13681 16451 02046 03519 15362 06610.

3. Suppose that Eve knows Bob's public RSA modulus $m = pq$ and also has come by $n = (p-1)(q-1)$. Then it is possible for her to obtain p and q by the following means.
   (a) Show that $p + q = m - n + 1$.
   (b) By using the fact that $q = m/p$, show that p satisfies the quadratic equation $p^2 + (n - m - 1)p + m = 0$.
   (c) Deduce that p and q are
   $$p = \frac{(m - n + 1) + \sqrt{(m - n + 1)^2 - 4m}}{2}$$
   $$q = \frac{(m - n + 1) - \sqrt{(m - n + 1)^2 - 4m}}{2}.$$
   (d) If $pq = 5336063$ and $(p-1)(q-1) = 5331408$, find the prime factors p and q.

4. One instance in which an implementation of RSA may be subverted is when there is a **common modulus protocol failure**. Suppose that Anna and Zena have the same RSA modulus m and different public encryption exponents e_a and e_z, which are relatively prime. If Matt sends a message x (that is relatively prime to m) to both Anna and Zena encrypted with their respective exponents and Evelyn intercepts both of these ciphertexts, then she can obtain the plaintext without knowing a factorization of m or either decryption exponent!
   (a) By using the fact that $x^{se_a + te_z} \equiv (x^{e_a})^s (x^{e_z})^t \pmod m$ for any choice of s and t, show how this can be done.
   (b) If $m = 4171$, $e_a = 47$, and $e_z = 101$, find the numerical plaintext from which the ciphertexts 2467 and 2664 were computed.

5. Recall that in an earlier homework we defined an action of a group G on a set A to be a collection of functions $\varphi_g \ \forall g \in G$ where $\varphi_g : A \to A$ is notated $\varphi_g(a) = g_\bullet a \ \forall a \in A$, and $g_\bullet a$ is given some precise meaning. Now let G be a group under multiplication and define an action of G (as a group) on G (as a set) by $g_\bullet a := gag^{-1}$ (this action is called conjugation by g).

   (a) Show that ($a \sim b$ iff $\exists g \in G$ with $g_\bullet a = b$) is an equivalence relation on G (as a set).

   (b) For a given $x \in G$, and defining $N(x) := \{g \in G \mid gxg^{-1} = x\}$, show that $N(x)$ is a subgroup of G.

   (c) Defining $Z(G) := \{g \in G \mid gyg^{-1} = y \ \forall y \in G\}$, show that $Z(G)$ is a subgroup of G.

   (d) If G is finite, and $[g_1], \ldots, [g_r]$ are the distinct equivalence classes of G under $\sim$ of part (a) which don't lie in $Z(G)$, show that

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : N(g_i)|$$

   where $|G : N(g_i)|$ denotes the number of equivalence classes of G under $\approx$ where $u \approx v$ iff $v^{-1}u \in N(g_i)$.

6. Construct an algorithm to find the maximal spanning tree of a weighted graph Γ and prove that it's correct.

7. Question 8, page 212 of text.

8. Question 6, page 281 of text.

9. Question 24, page 285 of text.

10. *This question was 5(iii) on HW4.* Solve for x: $3x = 1 \bmod 5$ with $2x = 6 \bmod 8$.

11. *This question was 6 on HW4.* A hoard of gold pieces "comes into the possession of" a band of 15 pirates. When they come to divide up the coins, they find that three are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns, there remain only 7 pirates capable of making an effective claim on the hoard. When however the hoard is divided between these seven it is found that two pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the four pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces that could have been in the hoard? (from Humphreys and Prest, "Numbers, groups and codes", CUP 1989)