CS207 (Discrete Structures)
Exercise problem set 11 – Modular arithmetic and number theory

November 3, 2015

---

1. Show that if $ac \equiv bc(\mod m)$ then $a \equiv b(\mod \frac{m}{d})$, where $d = gcd(m, c)$.

2. Use Fermat's little theorem to calculate the remainder when 3^{47} is divded by 23.

3. Let $gcd(m_1, m_2) = 1$.

   (a) Show that there is a solution x of the congruence equations:

   $$x \equiv a_1(\mod m_1), \quad x \equiv a_2(\mod m_2)$$

   Show that any two solutions are congruent modulo $m_1 \cdot m_2$.

   (b) Generalize the above statement to n simultaneous congruence equations and prove it. (This is called the *Chinese Remainder Theorem.*)

   (c) Use this to find the solutions to the system $x \equiv 1(\mod 4), x \equiv 2(\mod 5), x \equiv 3(\mod 7)$.

4. For a positive integer $N = pq$, recall that determining $\phi(N)$ is equivalent to factoring N. If one knows p, q, then one can efficiently compute $\phi(N)$. Conversely, if $\phi(N)$ and N are known, we can compute the primes p, q. Show that if $K = N + 1 - \phi(N)$ then the two prime factors p, q are

   $$(K \pm \sqrt{K^2 - 4N})/2$$

   and these are in fact integers.

5. Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The private key for Alice is 15 and for Bob is 10. We consider a commonly known prime 29.

   (a) Calculate the smallest primitive element for $p = 29$, i.e., smallest generator of the corresponding group.

(b) Obtain the common key by using the primitive element found above

6. Suppose that we use the RSA scheme with public key $(n = pq; e) = (55; 7)$.

   (a) Find the private key d.

   (b) If encrypted message seen by an interceptor in the channel is $C = 3$. What was the secret message M sent from Alice to Bob?

7. (Open ended questions).

   (a) In the crypto-systems designed in class, can Bob verify that the message indeed came from Alice? If not, how would you modify the key exchanges so that Alice can make some information public and Bob can verify that Alice sent the message.

   (b) A man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. Can you modify the cryptosystems discussed in class to avoid such attacks?