CS 70 Discrete Mathematics for CS
Fall 2004 Rao

HW 3

Due Thursday, September 24 at 3:29PM (in-class)

1. **(5 pts.) Staples.**
   Staple your paper.

2. **(25 pts.) Modulo arithmetic**
   Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

   (a) $7x \equiv 1 \pmod{15}$.

   (b) $10x + 20 \equiv 11 \pmod{23}$.

   (c) $5x + 15 \equiv 4 \pmod{20}$.

   (d) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

3. **(20 pts.) Carmichael numbers**

   (a) Given that a and d are relatively prime, show that $ab = cd$ implies that d divides b.

   (b) Prove that if $a = b \bmod m_1$ and $a = b \bmod m_2$, $a = b \bmod m_1 m_2$ provided that $\gcd(m_1, m_2) = 1$.

   (c) (The remark on the footnote.) A carmichael number c can be written as a product of *distinct* primes $p_1 p_2 \cdots p_k$, where $p_i - 1$ divides $c - 1$, for all i.
   Show that if c is a Carmichael number and a is relatively prime to c, then $a^{c-1} = 1 \bmod c$.
   (Hint: Use Fermat's little theorem to reason about $a^{p_i - 1} \bmod p_i$. Now, what is $a^{c-1} \bmod p_i$?)

4. **(25 pts.) Modular inverse**
   Prove that the equation $ax \equiv ay \bmod n$ implies $x \equiv y \bmod n$ whenever $\gcd(a, n) = 1$. Show that the condition $\gcd(a, n) = 1$ is necessary by supplying a counterexample with $\gcd(a, n) > 1$.

5. **(10 pts.) RSA**
   Let p and q be primes and let $N = pq$. Show how to determine p and q given N and $(p-1)(q-1)$. (In other words, given the public key (N, e), N the RSA modulus and e the encryption exponent, and the value $\varphi(N) = (p-1)(q-1)$, it is possible to compute p and q by simple (polynomial time) algebraic operations. This shows that determining $\varphi(N)$ is "as hard as factoring.")

6. **(15 pts.) Signatures**

   (a) What happens if you sign an encrypted message which was encrypted using your public key?

   (b) Indeed, it is not safe to sign any random message given to you. Suppose someone gets a message $x' = x^e$ sent to you. He can pick another random message y, encrypt it using your public key e, and get y^e. Explain how the hacker can recover x if he can ask you to sign $y^e x'$.