Discrete Mathematics: Homework 6

(Deadline: 10:00am, April 17, 2020)

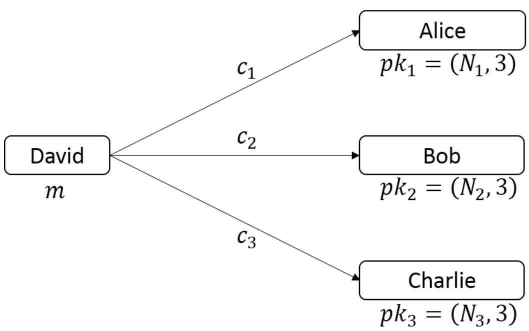
1. (20 points) Let p be an odd prime and let $\mathbb{Z}_p^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$.
   (1) Show that $([a]_p)^2 = [1]_p$ if and only if $[a]_p \in \{[1]_p, [p-1]_p\}$.
   (2) Show that $[1]_p \cdot [2]_p \cdots [p-1]_p = [-1]_p$ and thus conclude that $(p-1)! \equiv -1 (\text{mod } p)$.
   (**Hint**: Partition the elements of $\mathbb{Z}_p^*$ as $(p+1)/2$ subsets of the form $\{\alpha, \alpha^{-1}\}$)

2. (20 points) Let x, y, z be integers such that $x^2 + y^2 \equiv 3z^2 (\text{mod } 4)$. Show that x, y, z must be all even. Based on this result, show that the equation $x^2 + y^2 \equiv 3z^2$ has no other integer solutions except $(x, y, z) = (0, 0, 0)$.

3. (20 points) Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.
$$\begin{cases} x \equiv a_1 (\text{mod } 11); \\ x \equiv a_2 (\text{mod } 13); \\ x \equiv a_3 (\text{mod } 17); \\ x \equiv a_4 (\text{mod } 19). \end{cases}$$

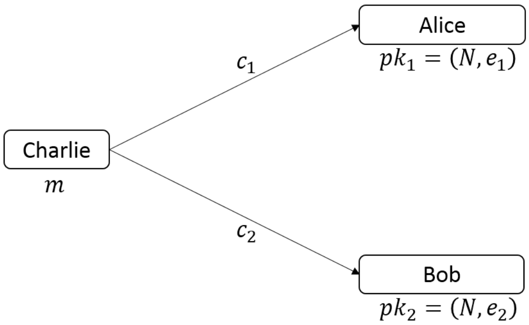
4. (20 points) A composite integer N that satisfies the congruence $b^{N-1} \equiv 1 (\text{mod } N)$ for all positive integers b with $\gcd(b, N) = 1$ is called a Carmichael number. Suppose that $N = p_1 p_2 p_3$ is an integer, where p_1, p_2, p_3 are primes such that $(p_i - 1) | (N - 1)$ for $i = 1, 2, 3$. Show that N is a Carmichael number. (**Hint**: See page 283 of the textbook for an example.)

5. (20 points) See the following figure. The RSA public keys of Alice, Bob and Charlie are $pk_1 = (N_1, 3), pk_2 = (N_2, 3)$ and $pk_3 = (N_3, 3)$, respectively. David wants to send a private message m to Alice, Bob and Charlie, where m is an integer and $0 < m < N_i$ for $i = 1, 2, 3$. In order to keep m secret from an eavesdropper Eve, David encrypts m as $c_1 = m^3 \text{ mod } N_1$, $c_2 = m^3 \text{ mod } N_2$ and $c_3 = m^3 \text{ mod } N_3$; and then sends c_1 to Alice, c_2 to Bob and c_3 to Charlie.



Suppose that N_1, N_2, N_3 are pairwise relatively prime. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.

6. (20 points) See the following figure. Alice and Bob trust each other very much. They set their RSA public keys as $pk_1 = (N, e_1)$ and $pk_2 = (N, e_2)$, respectively. Charlie wants to send a private message m to Alice and Bob, where $0 \leq m < N$ is an integer and $\gcd(m, N) = 1$. In order to keep m secret from an eavesdropper Eve, Charlie encrypts m as $c_1 = m^{e_1} \bmod N$ and $c_2 = m^{e_2} \bmod N$; and then sends c_1 to Alice and c_2 to Bob.



Suppose that $\gcd(e_1, e_2) = 1$. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.