UNIVERSITY OF ZAMBIA

SCHOOL OF NATURAL SCIENCES

CSC2901 – Discrete Structures

Tutorial Sheet III

1. Let $a \equiv b(mod\ n)$. Prove that $a^p \equiv b^p(mod\ n)$, using the principle of mathematical induction (PMI).
2. Evaluate
    a. $3^{76}(mod\ 31)$
    b. Inverse of $21(mod\ 37)$
3. Suppose p and q are non-identical primes such that $n = pq$. Prove that
    a. if $a \equiv b(mod\ p)$, and $a \equiv b(mod\ q)$, then $a \equiv b(mod\ n)$
4. Prove that
    a. $4^n \equiv 1(mod\ 3)$
    b. $n^5 \equiv n(mod\ 30)$
5. Find the greatest common divisor of 1729 and 15,210
6. Find the number s, if possible, such that
    a. $3s \equiv 1(mod\ 4)$
    b. $17s \equiv 1(mod\ 72)$
    c. $9s \equiv 6(mod\ 12)$
    d. $3s \equiv 5(mod\ 9)$
7. Perform encryption and decryption using the RSA algorithm, for the following:
    a. $p = 13;\ q = 31, e = 19;\ M = 2$
    b. $p = 11;\ q = 31, e = 7;\ M = 4$
    c. $p = 3;\ q = 17, e = 5;\ M = 5$
8. In a public-key system using RSA, you intercept the ciphertext C = 61 sent to a user whose public key is e = 11, n = 91. What is the plaintext M?
9. In an RSA system, the public key of Harry is as follows: e = 47, n = 4757. What is the private key of Harry?
10. Consider a Diffie-Hellman scheme with a common prime $q = 23$ and a primitive root $a = 5$.
    a. Alice has public key $Y_A = 10$, what is Alice's private key X_A?
    b. Bob has public key $Y_B = 8$, what is the shared secret key K?