Discrete Mathematics 2015
(Home work 4)

November 09, 2015

- Due on Wednesday, November 18, before 10 a.m. (You can submit in class)
- Late home works will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.
- Collaboration is discouraged, but not prohibited. It is recommended that you try to solve the problems on your own. You can discuss the questions with your colleagues but you should not copy solutions. Always write down your own answers. If copying is detected that may immediately lead to a grade less than 7. (**This would be followed strictly**)
- Credits would be given to partial solutions also.
- The answers should be typed or written clearly and a hard copy is to be submitted.

Playing With Numbers: [$5 \times 10 = 50$ **points**]

1. Prove or disprove the following. (Note that to disprove it is enough to give a counterexample)
   (a) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $a + c \equiv b + d \bmod n$ and $ac \equiv bd \bmod n$.
   (b) If $ab \equiv ac \bmod n$ then $b \equiv c \bmod n$
   (c) If H and K are subgoups of G then $H \cap G$ is also a subgroup of G.
2. If $\gcd(m, n) = 1$, given a and b, prove that there exists an x such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

3. Let n be a positive composite integer. Show that there exist a prime p dividing n such that $p \leq \sqrt{n}$.

4. Find $d = \gcd(1024, 888)$ and find $x, y \in \mathbb{Z}$ such that $d = 1024x + 888y$.

5. If F_n be the n-th Fibonacci number, show that for any $n \geq 1$, $\gcd(F_{n+1}, F_n) = 1$.

6. What is $2^{2^{2009}} (\text{mod} 3)$?

7. Is the difference of $5^{30,000}$ and $6^{123,456}$ a multiple of 31?

8. Calculate $2^{125} (\text{mod} 127)$.

9. Let G be a group and A, B subgroups of G. If $x, y \in G$, define $x \sim y$ if $y = axb$ for some $a \in A$ and $b \in B$. Prove that the relation $\sim$ is an equivalence relation. What is the equivalence class of an $x \in G$.

10. The center Z of a group G is defined as

$$Z = \{z \in G : zx = xz \text{ for all } x \in G\}.$$

Prove that Z is a subgroup of G.

Algorithms with numbers [$15 \times 5 = 75$ **points**]

11. Show that the following rule is true

$$\gcd(a, b) = \begin{cases} 2\gcd(\frac{a}{2}, \frac{b}{2}) & \text{if } a, b \text{ are even} \\ \gcd(a, \frac{b}{2}) & \text{if } a \text{ is odd and } b \text{ is even} \\ \gcd(\frac{a-b}{2}, b) & \text{if } a, b \text{ are odd} \end{cases}$$

Using the above rule give an efficient algorithm to compute $\gcd(a, b)$. Discuss the complexity of your algorithm.

12. In this exercise we shall learn to compute square roots in $\mathbb{Z}_p^*$ where p is a prime, such that $p \equiv 3 \pmod 4$. We say that $x \in \mathbb{Z}_p^*$ has square root, if there exist a $y \in \mathbb{Z}_p^*$ such that $x \equiv y^2 \pmod p$, and y is called the square root of x.

    (a) Find the elements in $\mathbb{Z}_7^*$ which has a square root. What are their square roots?

    (b) Show that $\frac{p+1}{4}$ is an integer.

    (c) If $a \in \mathbb{Z}_p^*$ and a has a square root. Then show that $a^{\frac{p+1}{4}}$ is a square root of a.

    (d) Suppose p is a prime such that $p \equiv 3 \pmod 4$. Write an algorithm which takes as input an $a \in \mathbb{Z}_p^*$ and returns the two square roots of a if the square roots exists, otherwise returns "no square roots exist". What is the running time of your algorithm.

13. Assuming that you know $\phi(N)$ for a given modulus N, devise an algorithm to compute $a^{-1} \pmod{N}$ using the modular exponentiation algorithm. State the running time of your algorithm.

14. Give a polynomial time algorithm for computing $a^{(b^c)} \pmod{p}$ given a, b, c and a prime p.

15. (a) Suppose we have available a black box $\mathcal{B}(.)$, which when given as input an n bit integer a returns a^2 in $O(n)$ time. Use this black-box $\mathcal{B}(.)$ to multiply two n bit numbers a and b in $O(n)$ time.

    (b) Prof. Calculus claims that there is an algorithm for squaring integers which is asymptotically faster than multiplying two integers. Argue that this claim of Prof. Calculus is false.