

Homework Assignment One due Monday, January 28 in class.

Total 50 points. Every homework assignment will be 50 points total. After dropping the worst score, there will be three scores left with a maximum total of 150 points for 30% of your course grade. Remember that homework must be on flat (not spiral) 8 1/2 by 11 inch paper and must be neat. Staple together multiple pages. Homework must be turned in in the first fifteen minutes of class on Monday, January 28, 2008.

- (10 points) For each of the following expressions, simplify the expression if possible and tell if it is $\Theta(n)$, $\Theta(n^2)$, $\Theta(n \log n)$, $\Theta(\log n)$ or $\Theta(2^n)$. Remember that \log means \log_2 . (Assume that $n > 1$ to use the definitions of O and Θ in the book.) You need not give a reason for your answer to this exercise other than your simplification of the expression.
 - $\log(2^n)$
 - $2^{\log n}$
 - $\log(2n)$
 - $\log(n^2)$
 - $\log(n^n)$
 - $2^{\log(n^2)}$
 - $2^{(\log n)+5}$
 - 2^{n+5}
 - $n^{\log 4}$
 - $(\log 4)^n$

- (10 points) Using the extended Euclidean Algorithm, find the inverse of 31 mod 100. (I.e, find x where $31x \equiv 1 \pmod{100}$.) Show work. No credit for answer alone.
- (10 points) Show that if both x and y are odd integers (not divisible by 2),

$$\gcd(x, y) = \gcd((x - y)/2, y)$$

Here is how to do it. First assume that there is a number d that divides both x and y . Show that d must divide $(x - y)/2$. Then assume there is a number g that divides $(x - y)/2$ and divides y . Show that g must divide x . (Hint 1: one way is easier than the other. Hint 2: "A divides B" means $B = KA$ for some integer K .)

4. (10 points)

- (a) If $a \equiv b \pmod{n}$, show that $ax \equiv bx \pmod{n}$ for any integer x , $1 \leq x \leq n-1$.
Use the definition: $a \equiv b \pmod{n}$ means $a - b$ is divisible by n , or $a - b = kn$ for some integer k .
- (b) Give a counterexample to show that it is not true that if $ax \equiv bx \pmod{n}$ and $1 \leq x \leq n-1$, then $a \equiv b \pmod{n}$.
- (c) Show that if $ax \equiv bx \pmod{p}$ and $1 \leq x \leq p-1$, then $a \equiv b \pmod{p}$ if p is a prime.

5. (10 points)

- (a) Find an integer x such that

$$2x \equiv 5 \pmod{9}$$

- (b) Find an integer $m > 2$ such that there is no integer x where

$$2x \equiv 5 \pmod{m}$$

- (c) Show that if p is a prime and $p > 2$,

$$2x \equiv 5 \pmod{p}$$

always has a (integer x) solution.