I. Short answer 1-12. Do not give proofs (3pts each).

1. Compute the following:

   28 div 3 = 9   28 mod 3 = 1

   −17 div 6 = −3   −17 mod 6 = 1

Division Algorithm

$28 = 9 \cdot 3 + 1$

$-17 = -3 \cdot 6 + 1$

$(-17 = -2 \cdot 6 - 5$, but $-5 < 0)$

2. What condition on positive integers a and b must hold for them to be *relatively prime*?

   $\gcd(a,b) = 1$

3. Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is one-to-one but not onto.

   $f(x) = e^x$

4. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3$, and $g : \mathbb{R} \to \mathbb{R}^+$ by $g(x) = 2^x$. Evaluate the following:

   $(g \circ f)(-1) =$ $1/2$

   $(g \circ f)^{-1}(16) =$ $\sqrt[3]{4}$

$(g \circ f)(-1) = g(f(-1)) = g((-1)^3)$
$= g(-1) = 2^{-1} = 1/2$

$(g \circ f)^{-1}(16) = (f^{-1} \circ g^{-1})(16) = f^{-1}(g^{-1}(16)) = f^{-1}(\log_2 16)$
$= f^{-1}(4) = \sqrt[3]{4}$

5. The first and second terms of an arithmetic progression are $a_1 = 5.5$ and $a_2 = 8$. What is a_4?

   $a_4 =$ 13

   $a_1 = 5.5 \quad a_2 = 8 \quad a_3 = 10.5 \quad a_4 = 13$

6. Assume for two positive integers a and b that $a \cdot b = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2$ and $\gcd(a, b) = 2^2 \cdot 3 \cdot 7$. What is $\mathrm{lcm}(a, b)$?

   $2^2 \cdot 3^2 \cdot 5 \cdot 7$

7. Compute the following:

   $\gcd(0, 4) =$ 4 $\gcd(-12, -50) =$ 2

   $12 = 2^2 \cdot 3 \quad 50 = 2 \cdot 5^2$

21

8. Order the following expressions in terms of **increasing** growth rate: n^2, $n!$, $n\log_2 n$, 2^n, $\log_2 n$

$\log_2 n$ $n\log_2 n$ n^2 2^n $n!$

9. In the best big-oh notation, how many multiplications are needed for Horner's method to evaluate a polynomial of degree n at a constant c?

$O(n)$

Horner's method
procedure $Horner(c, a_0, a_1, \ldots, a_n$: real numbers)
$y := a_n$
for $i := 1$ **to** n
$y := y * c + a_{n-i}$

10. Name an algorithm we studied for which the best-case time complexity is different than the worst-case time complexity (in terms of the representative operation we discussed).

linear search
(also binary search)

11. Circle the prime numbers and only the prime numbers in this list:

73, 92, 93, 109, 127, 133 $2,3,5,7 \nmid 73$ $2|92$ $3|93$

$2,3,5,7 \nmid 109$ $2,3,5,7,11 \nmid 127$ $7|133$

12. A 2 cent and a 5 cent stamp are available (without limit) to make postage. What is the smallest amount of postage N in cents such that every $N, N+1, N+2, N+3, \ldots$ can be composed of 2 cent and 5 cent stamps?

$N =$ 4

1 no
2 yes
3 no
4 yes
5 yes
$6 = 4+2$
$7 = 5+2$
8
⋮

II. Computation Problems 13-16 (10pts each). For full credit, show work to clearly justifying your answer.

13. Use the Euclidean Algorithm to express $\gcd(222, 180)$ as $r \cdot 222 + s \cdot 180$ for some $r, s \in \mathbb{Z}$.

$222 = 1 \cdot 180 + 42$
$180 = 4 \cdot 42 + 12$
$42 = 3 \cdot 12 + \boxed{6}$
$12 = 2 \cdot 6 + 0$

$\gcd(222,180) = 6$
$6 = 42 - 3 \cdot 12$
$6 = 42 - 3(180 - 4 \cdot 42)$
$6 = 13 \cdot 42 - 3 \cdot 180$
$6 = 13(222 - 1 \cdot 180) - 3 \cdot 180$
$6 = 13 \cdot 222 - 16 \cdot 180$

$\boxed{r = 13}$ $\boxed{s = -16}$

14. Compute the sum $\sum_{i=0}^{10}(2 \cdot 3^{i+2} - 4 \cdot i)$ (an unsimplified answer is acceptable but must not contain ellipses $(\cdots)$ or i).

$$\sum_{i=0}^{10} (2 \cdot 3^2 \cdot 3^i - 4 \cdot i)$$

$$= 12 \sum_{i=0}^{10} 3^i - 4 \sum_{i=0}^{10} i$$

$$= \boxed{12 \frac{3^{11}-1}{3-1} - 4 \frac{(10)(11)}{2}}$$

15. Compute $(60032 \cdot 24005 + 90511 \cdot 3030)$ mod 3. Shortcuts are recommended, but must be clear from your work.

$= (60032 \bmod 3)(24005 \bmod 3) + (90511 \bmod 3)(3030 \bmod 3) \bmod 3$

$= 2 \cdot 2 + 1 \cdot 0 \bmod 3$

$= 4 \bmod 3$

$= \boxed{1}$

16. Let $f(x) = 5x^2 + 10\log_2 x$. Compute witnesses C and k that show $f(x)$ is $O(x^2)$. (Hint: $x > k \to |f(x)| \leq C|x^2|$.)

Pick $k=1$.

$5|x^2| \leq 5|x^2|$ for $x > 1$.

$10|\log_2 x| \leq 10|x^2|$ for $x > 1$.

with $C = 15$, $x > 1 \to$

$|5x^2 + 10\log_2 x| \leq 5|x^2| + 10|\log_2 x|$

$\leq 5|x^2| + 10|x^2|$

$= 15|x^2| = C|x^2|$.

$\boxed{k=1, C=15}$

III. Proofs 17-18 (12pts each). Partial credit for good proof structure.

17. Prove the following. Let m, n be positive integers greater than 1, and let a, b be integers. If $n|m$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

(Direct Proof)
Assume $n|m$ and $a \equiv b \pmod{m}$.
Since $n|m$, $n \cdot k = m$ for some $k \in \mathbb{Z}$.
Since $a \equiv b \pmod{m}$, $m | a-b$ by definition of congruence mod m.

Then $m \cdot d = a - b$ for some $d \in \mathbb{Z}$.
substituting for m,

$n k d = a - b$.

$k \cdot d$ is an integer since $k, d \in \mathbb{Z}$.
By definition of congruence mod m,
$a \equiv b \pmod{n}$. □

18. Prove by a careful induction argument that every positive integer can be written in the form $2^r \cdot m$, where r is an integer and m is an odd integer.

For all $k \in \mathbb{Z}^+$, define $P(k)$ to be the statement
$k = 2^r \cdot m$ for some $r \in \mathbb{Z}$ and odd $m \in \mathbb{Z}$.

Proof by strong induction

Base case $k=1$: $1 = 2^0 \cdot 1$, and $0 \in \mathbb{Z}$, $1 \in \mathbb{Z}$ is odd.

Inductive step: Let $k \in \mathbb{Z}^+$ and assume $P(1), \ldots, P(k)$ all are true.
Consider $k+1$.
Case 1: $k+1$ is odd.
Then $k+1 = 2^0(k+1)$, and $0 \in \mathbb{Z}$, $k+1 \in \mathbb{Z}$ is odd.

Case 2: $k+1$ is even.
By definition $k+1 = 2h$ for $h \in \mathbb{Z}$, and
$k+1 > 0 \rightarrow h > 0$, and $1 \le h \le k$.
Since $P(h)$ is true,
$h = 2^r \cdot m$, where $r \in \mathbb{Z}$ and $m \in \mathbb{Z}$ is odd.
Then $k+1 = 2h = 2^{r+1} \cdot m$, where $r+1 \in \mathbb{Z}$ and $m \in \mathbb{Z}$ is odd.
Therefore $P(k+1)$ is true.
By strong induction, $\forall n \in \mathbb{Z}^+$ $P(n)$ is true. □