

1. Fill in the blank in the statements below:

(a) A function  $f: A \rightarrow B$  is one-to-one if and only if  $\forall x, y \in \text{dom}(f) (f(x) = f(y) \rightarrow x = y)$   
(or, equiv'ly:  $\forall x, y \in \text{dom}(f) (x \neq y \rightarrow f(x) \neq f(y))$ )

(b) A function  $f: A \rightarrow B$  is onto if and only if  $\forall y \in \text{codom}(f) \exists x \in \text{dom}(f) : y = f(x)$   
(equiv'ly:  $\text{range}(f) = \text{codomain}(f)$ )

(c) A function  $f: A \rightarrow B$  is bijective if and only if  $\text{is one-to-one and onto}$   
(i.e., injective and surjective)

(c) A sequence is a function w/ domain  $\{0, 1, 2, \dots\}$  (or  $\{1, 2, \dots\}$ )

(d) For a function  $f: A \rightarrow B$  and  $Y$  a subset of  $B$ , the preimage of  $Y$  through  $f$  is  $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$

(e) A function  $f(x)$  is big-O of  $g(x)$  if and only if  $\exists M$  and  $k$  so that  
 $|f(x)| \leq M|g(x)|, \forall x > k$

(e) A function  $f(x)$  is of the order of function  $g(x)$  if and only if  $f(x)$  is  $O(g(x))$  and  $f(x)$  is  $\Omega(g(x))$

(f) An integer  $a$  divides integer  $b$  if and only if  $\exists k \in \mathbb{Z} : b = a \cdot k$

(g) Integers  $a$  and  $b$  are congruent mod  $m$  if and only if  $m \mid a - b$   
(or, equiv'ly,  $a$  and  $b$  have the same remainder when div. by  $m$ )

(h) If  $\gcd(a, b) = 1$  then we say that  $a$  and  $b$  are relatively prime.

2. Prove that  $f: \mathbb{Z} \rightarrow \mathbb{Z}; f(n) = 2n + 3$  is one-to-one but not onto.

a)  $f(n) = f(m) \Rightarrow 2n + 3 = 2m + 3 \Rightarrow 2n = 2m \Rightarrow n = m$   $\checkmark$  ( $\Rightarrow f = 1-1$ )

b) no even number  $k$  is an  $f(n)$ : since  $f(n) = 2n + 3 = 2n + 2 + 1$   $\checkmark$   
 $= 2(n+1) + 1 = \text{odd}$

3. Prove that  $f: \mathbb{Z} \rightarrow \mathbb{Z}; g(n) = \left\lceil \frac{n-1}{2} \right\rceil$  is not one-to-one but it is onto.

( $\Rightarrow f$  not onto)

a)  $g(1) = \left\lceil \frac{1-1}{2} \right\rceil = \left\lceil 0 \right\rceil = 0$ ,  $g(0) = \left\lceil \frac{0-1}{2} \right\rceil = \left\lceil -0.5 \right\rceil = 0$

so  $g(1) = g(0)$ , but  $1 \neq 0 \Rightarrow f \neq 1-1$

b) for any  $m \in \mathbb{Z}$ , let  $n = 2m + 1 \in \mathbb{Z}$ ; then since  $m \in \mathbb{Z}$   
 $f(n) = \left\lceil \frac{2m+1-1}{2} \right\rceil = \left\lceil \frac{2m}{2} \right\rceil = \left\lceil m \right\rceil = m \Rightarrow f = \text{onto}$

4. Let  $S = \mathbb{R} - \{0\}$ . Prove that the function  $f: S \rightarrow S; f(x) = \frac{1}{x}$  is one-to-one and onto.

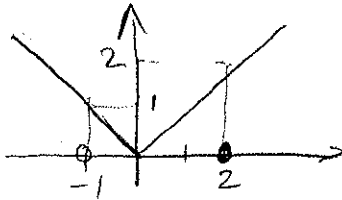
a)  $f(x) = f(y) \Rightarrow \frac{1}{x} = \frac{1}{y} \Rightarrow x = y \Rightarrow f = 1-1$

b) for  $y \in S$  (i.e.  $y \neq 0$ )  $\Rightarrow$  let  $x = \frac{1}{y} \in S \Rightarrow$   
 $f(x) = f(\frac{1}{y}) = \frac{1}{(\frac{1}{y})} = y \Rightarrow f = \text{onto}$

5. If  $f(x) = |x|$  is the absolute value function defined on the real numbers, find

(a) the image of  $(-1, 2]$

$$f((-1, 2]) = [0, 2]$$

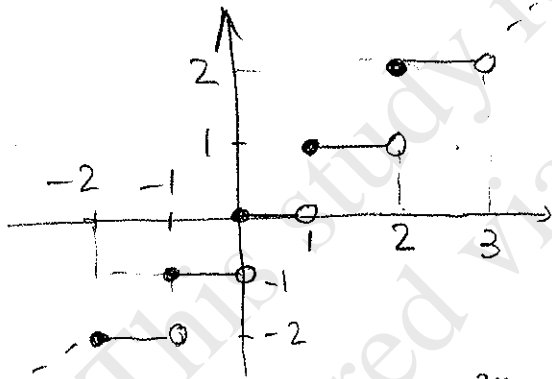


(b) the preimage of  $(0, 2]$ .

$$f^{-1}((0, 2]) = [-2, 0) \cup (0, 2]$$

6. Repeat problem 5 for  $f(x) = \lfloor x \rfloor$  the floor function defined on  $\mathbb{R}$ .

$$f(x) = \lfloor x \rfloor$$



a)  $f((-1, 2]) = \{-1, 0, 1, 2\}$

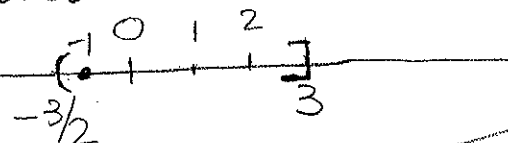
b)  $f^{-1}((0, 2]) = [1, 3)$

only integers here are 1 and 2

7. Repeat problem 5 for  $g(x) = \lceil \frac{3x}{2} \rceil$ .

a)  $g((-1, 2]) = \{ \lceil \frac{3x}{2} \rceil \mid -1 < x \leq 2 \} = \{-2, -1, 0, 1, 2, 3\}$

if  $-1 < x \leq 2$ , then  
 $-3 < 3x \leq 6$ , and so  
 $-\frac{3}{2} < \frac{3x}{2} \leq 3$



8. Evaluate the sum and simplify as much as possible. Show all your work. Calculator answers will not be accepted.

$$\sum_{n=100}^{200} \frac{5^{2n+3}}{3^{2n+1}} = \sum_{n=100}^{200} \frac{5^3 \cdot 5^{2n}}{3 \cdot 3^{2n}} = \sum_{n=100}^{200} \frac{125}{3} \left(\frac{5}{3}\right)^{2n} = \sum_{n=100}^{200} \frac{125}{3} \left(\frac{25}{9}\right)^n$$

= sum of consecutive terms of a geometric sequence:

1<sup>st</sup> term =  $\frac{125}{3} \left(\frac{25}{9}\right)^{100}$ ; ratio =  $\frac{25}{9}$ , # of terms =  $(200-100)+1=101$

9. Prove that for any positive integer  $n$ ,  $\sum_{k=1}^n (6k-1) = 3n^2 + 2n$ .

$$\sum_{k=1}^n (6k-1) = \sum_{k=1}^n 6k - \sum_{k=1}^n 1 = 6 \sum_{k=1}^n k - \sum_{k=1}^n 1 =$$

$$3 \cdot 6 \cdot \frac{n(n+1)}{2} - 1 \cdot n = 3n(n+1) - n = 3n^2 + 3n - n = 3n^2 + 2n \quad \checkmark \text{ done!}$$

10. Let  $a_n = 2^n + 5 \cdot 3^n$  for nonnegative integers  $n$ . Find  $a_0, a_1, a_2$  and  $a_3$ .

$$a_0 = 2^0 + 5 \cdot 3^0 = 1 + 5 \cdot 1 = 6$$

$$a_1 = 2 + 5 \cdot 3 = 2 + 15 = 17$$

$$a_2 = 2^2 + 5 \cdot 3^2 = 4 + 45 = 49$$

$$a_3 = 2^3 + 5 \cdot 3^3 = 8 + 5 \cdot 27 = 8 + 135 = 143$$

11. Consider the sequence  $\{a_n\}_n$  defined recursively by

$$a_1 = 3, \text{ and } a_{n+1} = 3a_n - 5 \text{ for } n \geq 1.$$

Find the values of  $a_2, a_3$  and  $a_4$ .

$$a_2 = 3a_1 - 5 = 3 \cdot 3 - 5 = 9 - 5 = 4$$

$$a_3 = 3a_2 - 5 = 3 \cdot 4 - 5 = 12 - 5 = 7$$

$$a_4 = 3a_3 - 5 = 3 \cdot 7 - 5 = 21 - 5 = 16$$

Cont'd #8

$$\text{Sum} = \frac{125}{3} \left(\frac{25}{9}\right)^{100} \cdot \frac{\left(\frac{25}{9}\right)^{101} - 1}{\frac{25}{9} - 1}$$

you can leave it in this form (no meaningful simplification exists!)

12. For each of the given the functions find the best big-O estimate. Explain all your steps by referring to the theorems you are using.

a)  $f(x) = x^5 + x \log(x^7) + \frac{x^5 + 4x}{x^3 + 1000}$

$\boxed{O(x^5)}$

$\underbrace{x^5}_{O(x^5)} + \underbrace{7x \log(x)}_{\in O(x \log(x))} + \underbrace{\frac{x^5 + 4x}{x^3 + 1000}}_{\in O(x^2)}$

$\frac{x^5}{x^3} = x^2$

b)  $f(x) = (x^3 + \log(x))(\log(x) + 17)$

$\underbrace{(x^3 + \log(x))}_{\in O(x^3)} \underbrace{(\log(x) + 17)}_{\in O(\log(x))}$   
 $\in \boxed{O(x^3 \log(x))}$

$\in O(x^5)$  since

$x \log(x) \in O(x^5)$

$x^2 \in O(x^5)$

c)  $g(n) = (2^n + \log(n))(\log(n!) + n^2)$

$\underbrace{(2^n + \log(n))}_{\in O(2^n)} \underbrace{(\log(n!) + n^2)}_{\in \log(n!)}$   
 $\in \boxed{O(2^n \cdot \log(n!))}$

13. Write the following functions in order such that each of them is big-O of the next one; justify your answer:

$n \log(n^7)$ ,  $\frac{n^5 + 4n}{n^3 + 1000}$ ,  $\sqrt{n} \log(n)$ ,  $2^n$ ,  $\log(5^n)$ ,  $n^3 \log(n)$ ,  $\frac{n^3}{1000000}$ ,  $7000\sqrt{n}$   
 $7n \log(n) \sim n^2$ ,  $n \log(5) = \text{constant}$

$7000\sqrt{n}$ ,  $\sqrt{n} \log(n)$ ,  $\log(5^n)$ ,  $n \log(n^7)$ ,  $\frac{n^3}{1000000}$ ,  $n^3 \log(n)$ ,  $2^n$

14. Prove or disprove:

a) If  $a$  divides  $b$  then  $a$  divides  $b^2$ .

Proof  
 Assume  $a \mid b$ . Then, by definition, there is a  $k \in \mathbb{Z}$  so that  $b = ak$ . Then  $b^2 = a^2 k^2 = a \cdot (ak^2)$  and  $ak^2 \in \mathbb{Z}$ , hence  $a \mid b^2$ .  $\square$

b) If  $a$  divides  $b^2$  then  $a$  divides  $b$ .

FALSE

counterexample:  $9 \mid 36$ , but  $9 \nmid 6$

15. a) Convert  $(1011000010001)_2$  from binary to decimal.

$2^{12} + 2^{10} + 2^9 + 2^4 + 1 = 4096 + 1024 + 512 + 16 + 1 = \boxed{5649}$

b) Convert 3124 from decimal to binary.

$3124 = 2048 + 1024 + 32 + 16 + 4 =$

$= 2^{11} + 2^{10} + 2^5 + 2^4 + 2^2 = \boxed{(110000110100)_2}$

base 8      base 16

- c) Convert
- $100011111$
- from binary to octal and hexadecimal.

$$(1077)_8 = (22F)_{16}$$

- d) Calculate
- $100101 \cdot 1101$
- where both numbers are in binary representation form.

$$\begin{array}{r} 100101 \\ \times 1101 \\ \hline 100101 \\ 1001010 \\ 00000000 \\ 100101000 \\ \hline 111100001 \end{array} \rightarrow (11110000)_2$$

- e) Evaluate
- $310563_7 + 23104_7$
- without changing to base 10 first.

$$\begin{array}{r} 310563 \\ + 23104 \\ \hline 334000 \end{array} \rightarrow (334000)_7$$

16. a) Using the Euclidean algorithm, find
- $\gcd(1386, 490)$
- .

$$\begin{aligned} 1386 &= 490 \cdot 2 + 406 \\ 490 &= 406 \cdot 1 + 84 \\ 406 &= 84 \cdot 4 + 70 \\ 84 &= 70 \cdot 1 + 14 \\ 70 &= 14 \cdot 5 + 0 \end{aligned}$$

- b) Find
- $\text{lcm}(1386, 490)$
- .

$$\frac{1386 \cdot 490}{14} = 48510$$

17. a) Prove that for any positive integers
- $a$
- and
- $b$
- ,
- $\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$
- .

$$\begin{aligned} a &= p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} & k_i, l_i \geq 0, p_i = \text{primes} \\ b &= p_1^{l_1} p_2^{l_2} \dots p_m^{l_m} \\ \gcd(a, b) &= p_1^{\min(k_1, l_1)} p_2^{\min(k_2, l_2)} \dots p_m^{\min(k_m, l_m)} \\ \text{lcm}(a, b) &= p_1^{\max(k_1, l_1)} p_2^{\max(k_2, l_2)} \dots p_m^{\max(k_m, l_m)} \end{aligned}$$

multiply and use that  $\max(s, t) + \min(s, t) = s + t$

- b) If the product of two integers is
- $2^7 \cdot 3^8 \cdot 5^2 \cdot 7^2$
- and their greatest common divisor is
- $2^3 \cdot 3^4 \cdot 5$
- what is their least common multiple?

$$\frac{2^7 \cdot 3^8 \cdot 5^2 \cdot 7^2}{2^3 \cdot 3^4 \cdot 5} = \boxed{2^4 \cdot 3^4 \cdot 5 \cdot 7^2} = 79380 \text{ or } 79380$$

18. Evaluate the following quantities.

a)  $-45 \bmod 8 = \boxed{3}$   
 $-45 = 8 \cdot (-6) + 3$

b)  $33 \bmod 7 = \boxed{5}$   
 $33 = 7 \cdot 4 + 5$

c)  $45 \operatorname{div} 7 = \boxed{6}$   
 $45 = 7 \cdot 6 + 3$

d)  $((\underbrace{18 \bmod 14}_4) + (\underbrace{-35 \bmod 7}_0)) \bmod 8 = \boxed{4}$

e)  $6^{23456} \bmod 5 = \boxed{1}$   
 $6^{23456} = 6^{2 \cdot 11728} = (6^2)^{11728} = 36^{11728} \equiv 1^{11728} \pmod{5}$

f)  $4^{12345} \bmod 5 = \boxed{4}$   
 $4^{12345} = 4^{12344+1} = 4^{12344} \cdot 4 = 4^{2 \cdot 6172} \cdot 4 = (4^2)^{6172} \cdot 4 = 16^{6172} \cdot 4 \equiv 1^{6172} \cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod{5}$

g) Find two (integer) values for  $c$  such that  $11 \equiv c \pmod{5}$ .

$c = 11, c = 16$  (others:  $c = -6, c = -21$  etc)

19. Compute  $4^{1033} \bmod 9$  using fast modular exponentiation. Show and explain all your steps.

$4^{1033} \bmod 9 = \boxed{4}$   
 $1033 = 1024 + 8 + 1 = 2^{10} + 2^3 + 1$   
 $4^{1033} = 4^{2^{10}} \cdot 4^{2^3} \cdot 4 \equiv 4 \cdot 7 \cdot 4 = 112 \equiv 4 \pmod{9}$

Aside

$4^2 = 16 \equiv 7 \pmod{9}$   
 $4^{2^2} = (4^2)^2 = 49 \equiv 4 \pmod{9}$   
 $4^{2^3} = (4^{2^2})^2 = 16 \equiv 7 \pmod{9}$   
 $4^{2^4} = (4^{2^3})^2 = 49 \equiv 4 \pmod{9}$   
 $4^{2^5} = (4^{2^4})^2 = 16 \equiv 7 \pmod{9}$   
 $4^{2^6} = (4^{2^5})^2 = 49 \equiv 4 \pmod{9}$