September 25. 31 20 24 37 41 57 60 4.2 1 27 31 64
32 3 12 67 68
H2 41 10 39

3.1 algorithms

20. Describe an algorithm for finding both the largest and smallest integers in a finite sequence.

procedure maxMin ($a_1, a_2, \ldots a_n$: integers)
    max := a_1
    min := a_1
    for i := 2 to n
        if max < a_i then max := a_i
        if min > a_i then min := a_i
    return max, min

24. Describe an algorithm that determines whether a function from a finite set to another finite set is one-to-one.

procedure one-to-one (f: function A to B,
    where A = {a1,...an}, B = {b1,..., bm},
    and a_1.. an b1..bm are int.

for i := 1 to n
    mark(ai) := 0
for i := 1 to m
    preimage(bi) := 0
for j := 1 to n
    preimage(f(aj)) := preimage(f(aj)) + 1
    if preimage (f(aj)) > 1 then
        return false
return true

37. use Bubble Sort for 3, 1, 5, 7, 4, showing list obtained in every step.

Starting 3 1 5 7 4   1 3 5 4 7   1 3 swap 3 5, 5 7 no 7 4 swap
1st pass 1 3 5 4 7   * go down list look at each
2-4 pass 1 3 4 5 7

41. use insertion sort for 3 1 5 7 4
3 1 5 7 4 Starting (trivial)
1 3 5 7 4 Step 1
1 3 5 7 4 Step 2
1 3 5 7 4 Step 3
1 3 4 5 7 Step 4

3.1 60 4.1 10 39
3.2 8 12 67 68 4.2 12 27 31 64

3 Sep. 25

3.1 algorithms

57. use cashiers algorithm to make change for: 25¢ 10¢ 5¢ 1¢
a) 51 cents $51 - 25 - 25 - 1$: 2 quarter 1 pennie
b) 69 cents $69: -25 - 25 - 10 - 5 - 1(4)x$: 2 quarter 1 dime 1 nickel 4 penny
c) 76 cents $76: -25(3) - 1$: 3 quarter 1 penny
d) 60 cents $60: -25(2) - 10$: 2 quarters 1 dime

60. Show that if there were coins worth 12¢, then cashiers wouldn't work
15 coins, → {25, 12, 10, 5, 1} → 12¢ (3) 1¢ = 4 coins
15 coins → {25, 10, 5, 1} → 10¢ 5¢ = 15¢

~~3.2~~ 3.2 Growth Functions

8. Find the least integer n such that $f(x)$ is $O(x^n)$ for each of

a) $f(x) = 2x^2 + x^3 \log x$ pick $x^3 \log x$ check $n=3$
if $f(x) = O(x^3)$ then $x^3 \log x \le Cx^3$ $x \to \infty$, $\log x \le C$ Not true

check $n = 4$ for $x \ge 1$, $\log x \le x$ $= x \ge 1$
$f(x) = 2x^2 + x^3 \log x \le 2x^2 + x^4 \le 2x^4 + x^4 = 3x^4$
$\frac{2}{x^2} + \frac{\log x}{x}$ approaches '0' as $x \to \infty$
$\boxed{n = 4}$

b) $f(x) = 3x^5 + (\log x)^4$ $3x^5$
$|f(x)| \le C|x^n|$ where $x > k$ pick $n = 5$
b/c $\log x$ $\log \uparrow x$ exponent
for $x \ge 1$ $\log x \le x$
$(\log x)^4 \le x^4 \le x^5$ since $(x \ge 1)$
$\boxed{n = 5}$
for $x \ge 1$
$f(x) = 3x^5 + (\log x)^4 \le 3x^5 + x^5 = 4x^5$

c) $f(x) = (x^4 + x^2 + 1) / (x^4 + 1)$ x^4 pick $\frac{x^4}{x^4} = 0$
b/c numerator & denominator x^4 $x \to \infty$ $f(x)$ is bounded
$\boxed{n = 0}$

d) $f(x) = (x^3 + 5 \log x) / (x^4 + 1)$ $\boxed{n = 0}$
$\to \frac{x^3}{x^4} \to \frac{1}{x}$

12) Show $3x^4 + 1$ is $O(x^4/2)$ and $x^4/2$ is $O(3x^4 + 1)$
$|f(x)| \le C|g(x)|$ for all $x > k$

$3x^4 + 1 \le 4x^4 = C\frac{x^4}{2}$ $= x^4/2 \le C(3x^4 + 1)$
$= \frac{x^4}{2} / 3x^4 + 1 \le C$
$= \frac{x^4}{2} = O(3x^4 + 1)$
$3x^4 + 1 = O(x^4/2)$
$3x^4 + 1 = x^4/2$

3.2 67 68 4.1 10 39

Sup 25 4.2 1 27 31 64

~~67. Show that the deferred acceptance always terminates with stable assignment~~ ← Gale Shapley $X_1 \to Y_1$ $Y_1 \to X_1$

Stable = no blocking pairs

67. Suppose $f(x)$ is $o(g(x))$ Does it follow that $2^{f(x)}$ is $o(2^{g(x)})$

$f(x) = o(g(f(x)))$ little o notation

$\frac{2^{f(x)}}{2^{g(x)}} = f(x) - g(x) = 0$

pick $f(x) \frac{1}{x}$ $g(x) = \frac{1}{x^2}$ as $x \to \infty$ $\frac{1}{x^2} - \frac{1}{x} = 0 - 0 = 0$

$\boxed{\text{NO}}$ b/c $f(x) = o(g(x))$ means f grows slower ~~g(x)~~

68. Suppose $f(x)$ is $o(g(x))$. does it follow $\log|f(x)|$ is $o(\log|g(x)|)$

$\lim_{x \to \infty} \frac{\log|f(x)|}{\log|g(x)|} = 0$ Assume $f(x) = o(g(x))$

$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$

$\boxed{\text{NO}}$ b/c $f(x) = x$ & $g(x) = x^2$ $\to \frac{\log x}{2 \log x} = \frac{1}{2} \neq 0$

Supplements

25 arrange in order of big O, n^n, $(\log n)^2$, $n^{1.0001}$, $(1.001)^n$, $2^{\sqrt{\log_2 n}}$, $n(\log n)^{1001}$ | $O(1)$, $O(\log n)$, $O(n \log n)$, $O(n^2)$, $O(2^{n})$, $O(n!)$

1) $(\log n)^2$ 2) $2^{\sqrt{\log n}}$ 3) $n(\log n)^{1001}$ 4) $n^{1.0001}$ 5) 1.0001^n 6) n^n

4.1 Divisibility and Modular Arithmetic.

10. Prove that if a, b non zero integers, a divides b, and a+b is odd then a is odd

use k

a, b = non zero a|b a + b = odd

since a|b, ∃ K where b = aK

then a + b = a + aK = a(1 + K)

if a + b is odd & product a(1+K) odd

a must be odd.

42 1 27 31 69

$99 \bmod 32 = 3 \quad 3^2 = 9 \quad 9 \bmod 32 = 9$
$9^3 = 729 \quad 729 \bmod 15 = 9$

4.1

39. a) $(99^{2} \bmod 32)^3 \bmod 15$ ignore
$99 \bmod 32 = 3 \quad 3^3 \quad 27^2 \cancel{\bmod 15} \quad 729 \bmod 15 = \boxed{9}$

b) $(3^4 \bmod 17)^2 \bmod 11$
$81 \bmod 17 = 13^2 \cdot 13^2 = 169 = \boxed{4}$

c) $(19^3 \bmod 23)^2 \bmod 31$
$19^3 = 6859 \bmod 23 = 5 \to 5^2 = 25 \bmod 31 = \boxed{25}$

d) $(89^3 \bmod 79)^4 \bmod 26$
$89 \bmod 79 = 10 \quad 10^3 = (1000)^4 \cancel{\bmod 26}$
$1000 \bmod 79 = 52 \quad 52^4 \bmod 26 \quad 52 \bmod 26 = \boxed{0}$

4.2 Integer representations and algorithms.

1. Convert the decimal expansion of each int to binary expansion.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32,768	65,536

a) 231
$- 128$ 7
103
64 6
39
-32 5
7
4 2 1 0
3

$\boxed{11100111}$

b) 4532
4096 12
436
256 8
180
128 7
52
32 5
20
16 4
4 2

$\boxed{1000110110100}$

c) 97644 why? !!
65536 16
32,108
16,384 14
15,724
8,192 13
7532
4096 12
3436
$-2,048$ 11
1,388
1,024 10
364
-256 8
108
-64 6
44

44
32 5
12 3 + 2

10111110100101100

31 69 3^{644} mod 645

gcd - greatest divisor $3^{2?}$ mod 645

22) Use Algorithm 5 to find 3^{2003} mod 99

procedure mod exp(b: integer, $n = (a_{k-1} \dots a_1 a_0)_2$, M: int)

x := 1

power := b mod M

for i := 0 to k − 1

if $a_i = 1$ then x := (x · power) mod M

power := (power · power) mod M

return x {x equals b^n mod M}

X = X · power

power = power² mod 99

2003/2 =	1001	r:1
1001/2 =	500	r:1
500/2:	250	r:0
250/2:	125	r:0
125/2:	62	r:1
62/2:	31	r:0
31/2:	15	r:1
15/2:	7	r:1
7/2:	3	r:1
3/2	1	r:1
1/2	0	r:1

1 1 1 1 1 0 1 0 0 1 1

a_{10} 9 8 7 6 5 4 3 2 1 a_0

j = a_0 … 10

"j" 3^{j+2}

$a_0 = 1$

② X := 1 power := 3 mod 99 = 3

i = 0 '1' x = (1 · 3) mod 99 = 3

power = 3^2 mod 99 = 9

i = 1 '1' x = (3 · 9) mod 99 = $\boxed{27}$

power 9^2 mod 99 = 81

i = 2 '0' x = skip b/c '0' power = 81^2 mod 99 = 27

i = 3 '0' x = skip power = 27^2 mod 99 = 36

i = 4 '1' x = (27 · 36) mod 99 = 81 power = 36^2 mod 99 = 9

i = 5 '0' x = skip power 9^2 mod 99 = 81

i = 6 '1' x = (81 · 81) mod 99 = $\boxed{27}$ power = 81^2 mod 99 = $\boxed{27}$

i	a_i	power before	x before	action	x after	power after
7	1	27	27	x power	36	36
8	1	36	36	=	9	9
9	1	9	9	=	81	81
10	1	81	81	=	$\boxed{27}$	27

final x = $\boxed{27}$

64

31. Show positive Integer is divisible by 3 if and only if the Sum of its decimal digits is divisible by 3

let $a = (a_{n-1} a_{n-2} \dots a_1 a_0)_{10}$ $a_j \in \{0, \dots, 9\}$ $S = \sum_{j=0}^{n-1} a_j$

$3 \mid a$ $3 \mid S$

1) write a in base 10 propositional form

$a = 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots 10^1 a_1 + 10^0 a_0$

2) use congruence modulo 3

$$10^j = 1^j = 1 \pmod 3$$

3) reduce each term modulo 3

$$10^j a_j \equiv 1 \cdot a_j = a_j \pmod 3$$

$$a = \sum_{j=0}^{n-1} 10^j a_j \equiv \sum_{j=0}^{n-1} a_j = S \pmod 3$$

4) congruence

$a \equiv S \pmod 3$ $3 \mid a - S \rightarrow 3 \mid a$ $3 \mid S$

64. Algorithm 5 Show $O((\log m)^2 \log n)$

let $L = \log m$

let K be the number of bits of n $K = \log n + 1$

the ~~loop~~ algorithm uses one loop $= \log n$

w/ two Mod Multiplication at most $- O(L^2)$

$O(K) \cdot O(L^2) = O(KL^2)$

So.. loop $\log n$ $\times$ 2 mods $(\log m)^2$

result

$$\boxed{O(KL^2) = O((\log m)^2 \log n)}$$

let $L = \log_2 m$ and $K = \log n + 1$, alg performs K iterations, each doing at most 2 modular multiplications $= O(L^2)$ thus total is $O(KL^2) = O((\log m)^2 \log n)$