Chapter 5: Introduction to Number Theory Correction of Exercises

I. Divisors:

Exercise 1 : Find the greatest common divisor of each pair of integers :

- a) 0, 17
 - A divisor of zero would be any integer n such that another unique integer m can be found with nm = 0. For example, n can be 1 or 17.
 - The positive divisors of 17 are 1, 17.

$$gcd(0, 17) = 17$$

- b) 110, 273
 - The positive divisors of 110 are 1, 2, 5, 10, 11, 22, 55, 110
 - The positive divisors of 273 are 1, 3, 7, 13, 21, 39, 91, 273

$$gcd(110, 273) = 1$$

- c) 20, 40
 - The positive divisors of 20 are 1, 2, 4, 5, 10, 20.
 - The positive divisors of 40 are 1, 2, 4, 5, 8, 10, 20, 40

$$gcd(20, 40) = 20$$

d)
$$3^2 \times 7^3 \times 11$$
, $3^2 \times 7^3 \times 11$

A divisor of $3^2 \times 7^3 \times 11$ would be any integer n such that another unique integer m can be found with nm = $3^2 \times 7^3 \times 11$.

$$gcd(3^2 \times 7^3 \times 11, 3^2 \times 7^3 \times 11) = 3^2 \times 7^3 \times 11$$

Exercise 2: Find the least common multiple of each pair of integers:

- a) 5, 25
 - The prime factorization of $5 = 1 \times 5$.
 - The prime factorization of $25 = 5 \times 5$.

$$lcm(5, 25) = 1 \times 5 \times 5 = 25$$

b) 60, 90

• The prime factorization of $60 = 2^2 \times 3 \times 5$

• The prime factorization of $90 = 2 \times 3^2 \times 5$

$$lcm(60, 90) = 2^2 \times 3^2 \times 5 = 180$$

c) 20, 40

• The prime factorization of $20 = 2^2 \times 5$

• The prime factorization of $40 = 2 \times 2^2 \times 5$

$$lcm(20, 40) = 2^2 \times 2 \times 5 = 40$$

Exercise 3: Let m, n and d be integers. Show that if d | m, then d | mn.

Since d divides m, there exists q such that m = dq. Multiplying by n gives mn = d(qn).

Therefore, d divides mn (with quotient qn).

Exercise 4 : Let a, b and c be integers. Show that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Since a divides b, there exists q1 such that b = aq1. Since b divides c, there exists q2 such that c = bq2. Now

$$c = bq2 = (aq1) q2 = a (q1q2)$$

II. Representation of integers and some algorithms for integer arithmetic:

Exercise 1 : Express each binary number in decimal.

a)
$$1001$$

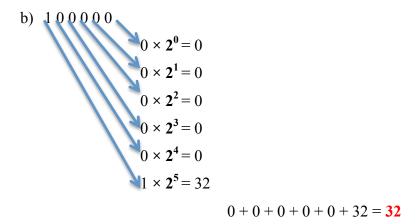
$$1 \times 2^{0} = 1$$

$$0 \times 2^{1} = 0$$

$$0 \times 2^{2} = 0$$

$$1 \times 2^{3} = 8$$

$$1+0+0+8=9$$



Exercise 2 : Express each decimal number in binary.

a) 43

The computation shows that the successive divisions by 2 with the remainders recorded at the right

2) 43	quotient = 21	remainder $= 1$	1's bit
2) 21	quotient = 10	remainder = 1	2's bit
2) 10	quotient = 5	remainder $= 0$	4's bit
2) 5	quotient = 2	remainder = 1	8's bit
2) 2	quotient = 1	remainder = 0	16's bit
2) 1	quotient = 0	remainder = 1	32's bit
0			

Binary number = 101011

b) 400

The computation shows that the successive divisions by 2 with the remainders recorded at the right

2) 254	quotient = 127	remainder $= 0$	1's bit
2) 127	quotient = 63	remainder = 1	2's bit
2) 63	quotient = 31	remainder = 1	4's bit
2) 31	quotient = 15	remainder = 1	8's bit
2) 15	quotient = 7	remainder = 1	16's bit
2) 7	quotient = 3	remainder $= 1$	32's bit

0

Binary number = 111111110

Exercise 3: Add the binary numbers.

The binary number added = 11000

The binary number added = 1001000

Exercise 4: Express each hexadecimal number in decimal

a)
$$3A$$

 $3A = 3 * 16^1 + 10 * 16^0 = 58$

$$A03 = 10 * 16^{2} + 0 * 16^{1} + 3 * 16^{0} = 10 * 256 + 3 = 2560 + 3 = 2563$$

III. The Euclidean algorithm:

Exercise 1 : Use the Euclidean algorithm to find the greatest common divisor of each pair of integers.

Exercise 2:

Let consider $\{f_n\}$ a Fibonacci sequence. Show by the mathematical induction that

$$gcd(f_n, f_{n+1}) = 1, \quad n \ge 1.$$

The Fibonacci sequence begins 1, 1, 2, 3, 5, 8, 13, ...

In mathematical terms, the sequence F_n of Fibonacci numbers is defined by the recursive relation $\mathbf{f_n} = \mathbf{f_{n-1}} + \mathbf{f_{n-2}}$

We prove the statement by induction on n.

- 1) Basic step: (n = 1) $gcd(f_1, f_2) = gcd(1, 1) = 1$
- 2) Inductive step: Suppose that the statement is true. We must prove that the statement is true with n+1.

$$gcd(f_{n+1}, f_{n+2}) = gcd(f_{n+1}, f_n + f_{n+1}) = gcd(f_{n+1}, f_n) = 1$$

According to the Fibonacci property: $f_{n+2} = f_n + f_{n+1}$

We can conclude that the statement is true.