Chapter 3

Lecture : Exercises & Correction

Prepared by:

- Dr. Abbas Rammal
- Dr. Rabih Assaf

EX 10.

Convert the octal expansion of each of these integers to a binary expansion.

a) $(572)_8$

b) $(1604)_8$

c) $(423)_8$

d) $(2417)_8$

EX 11.

Show that if $a^m + 1$ is composite if a and m are integers greater than 1 and m is odd. [*Hint:* Show that $x + 1$ is a factor of the polynomial $x^m + 1$ if m is odd.]

Solution Exercise 10

SOLUTION

(a) The octal expansion has base $b = 8$.

$$\begin{aligned}(572)_8 &= 5 \cdot 8^2 + 7 \cdot 8^1 + 2 \cdot 2^0 \\ &= 320 + 56 + 2 \\ &= 378\end{aligned}$$

You obtain the binary expansion of the decimal expansion of an integer by consecutively dividing the integer by 2 until you obtain 0.

$$378 = 2 \cdot 189 + 0$$

$$189 = 2 \cdot 94 + 1$$

$$94 = 2 \cdot 47 + 0$$

$$47 = 2 \cdot 23 + 1$$

$$23 = 2 \cdot 11 + 1$$

$$11 = 2 \cdot 5 + 1$$

$$5 = 2 \cdot 2 + 1$$

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

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

The successive remainders of each division represents the binary expansion from right to left.

$$(1\ 0111\ 1010)_2$$

(b) The octal expansion has base $b = 8$.

$$\begin{aligned}(1604)_8 &= 1 \cdot 8^3 + 6 \cdot 8^2 + 0 \cdot 8^1 + 4 \cdot 2^0 \\ &= 512 + 384 + 4 \\ &= 900\end{aligned}$$

You obtain the binary expansion of the decimal expansion of an integer by consecutively dividing the integer by 2 until you obtain 0.

$$900 = 2 \cdot 450 + 0$$
$$450 = 2 \cdot 225 + 0$$
$$225 = 2 \cdot 112 + 1$$
$$112 = 2 \cdot 56 + 0$$
$$56 = 2 \cdot 28 + 0$$
$$28 = 2 \cdot 14 + 0$$
$$14 = 2 \cdot 7 + 0$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

The successive remainders of each division represents the binary expansion from right to left.

$$(11\ 1000\ 0100)_2$$

Solution Exercise 11

DEFINITIONS

An integer p larger than x is called **prime** if the only positive factors of p are 1 and p.
An integer that is not prime is called **composite**.

Given: a and m are integers greater than 1 and m is odd

To proof: $a^m + 1$ is composite

PROOF
We add terms to $a^m + 1$ whose total is 0 (and thus does not affect $a^m + 1$ overall), then we regroup the terms using the distributive property.

$$\begin{aligned} a^m + 1 &= a^m + (a^{m-1} - a^{m-1}) + (a^{m-2} - a^{m-2}) + ... + (a^2 - a^2) + (a^1 - a^1) + 1 \\ &= (a^m + a^{m-1}) - (a^{m-1} + a^{m-2}) + (a^{m-2} + a^{m-3}) + ... - (a^2 + a^1) + (a^1 + 1) \\ &= a^{m-1}(a+1) - a^{m-2}(a+1) + a^{m-3}(a+1) + ... - a(a+1) + (a+1) \\ &= (a+1)(a^{m-1} - a^{m-2} + a^{m-3} + ... - a + 1) \end{aligned}$$

We then note that $(a + 1)$ is a factor of $a^m + 1$, while $(a + 1)$ is not 1 nor $a^m + 1$, thus $a^m + 1$ is not prime and thus $a^m + 1$ is composite.

Note: If m is odd, then you would obtain $(-a^1 + 1)$ instead of $(a^1 + 1)$ in the second step, which is not divisible by $(a + 1)$.
□

EX 12.

Show that if $2^n - 1$ is prime, then n is prime. [*Hint:* Use the identity $2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$.]

EX 13.

We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.

a) Show that 6 and 28 are perfect.

b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

Solution Exercise 12

Given: $2^n - 1$ is prime

To proof: n is a prime

PROOF BY CONTRADICTION

Let us assume that n is not prime, then there exist two integers a and b greater than 1 such that:

$$n = ab$$

For the number $2^n - 1$, we then obtain:

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1^b \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + ... + 2^a + 1) \end{aligned}$$

We then note that $(2^a - 1)$ is a factor of $2^n - 1$ and $(2^a - 1)$ is greater than 1 and $(2^a - 1)$ is not the integer $2^n - 1$ itself, thus we have then shown that $2^n - 1$ is not prime.

Since $2^n - 1$ is known to be prime, we have obtained a contradiction and thus n has to be prime.

□

Solution Exercise 13

DEFINITIONS

A positive integer is **perfect** if the sum of all positive divisors other than itself is equal to the positive integer.

$$\sum_{k=0}^{n-1} a^k = \frac{a^n - 1}{a - 1}$$

SOLUTION

(a) Let us determine all divisors of each number.

$$\text{Divisors of } 6 = 1, 2, 3, 6$$
$$\text{Divisors of } 28 = 1, 2, 4, 7, 14, 28$$

Let us determine the sum of all positive divisors other than the integer itself:

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$

We then note that 6 and 28 are both perfect.

(b) Given: $2^p - 1$ is prime

To proof: $2^{p-1}(2^p - 1)$ is a perfect number

PROOF
Determine all divisors of $2^{p-1}(2^p - 1)$ (using that $(2^p - 1)$ is prime and thus cannot be factorized):

$$1, 2, 2^2, ..., 2^{p-1}, (2^p - 1), 2(2^p - 1), 2^2(2^p - 1), ..., 2^{p-2}(2^p - 1), 2^{p-1}(2^p - 1)$$

Note: The last divisor is the number $2^{p-1}(2^p - 1)$ itself.

Let us determine the sum of all positive divisors other than the integer itself:

$$\begin{aligned}
&1 + 2 + 2^2 + ... + 2^{p-1} + (2^p - 1) + 2(2^p - 1) + 2^2(2^p - 1) + ... + 2^{p-2}(2^p - 1) \\
&= 1(1 + 2^p - 1) + 2(1 + 2^p - 1) + 2^2(1 + 2^p - 1) + ... + 2^{p-2}(1 + 2^p - 1) + 2^{p-1} \\
&= 1(2^p) + 2(2^p) + 2^2(2^p) + ... + 2^{p-2}(2^p) + 2^{p-1} \\
&= 2^p(1 + 2 + 2^2 + ... + 2^{p-2}) + 2^{p-1} \\
&= 2^p \left(\sum_{i=0}^{p-2} 2^i\right) + 2^{p-1} \\
&= 2^p \left(\frac{2^{p-1} - 1}{2 - 1}\right) + 2^{p-1} \\
&= 2^p \left(2^{p-1} - 1\right) + 2^{p-1} \\
&= 2^p \cdot 2^{p-1} - 2^p + 2^{p-1} \\
&= 2^p \cdot 2^{p-1} - 2 \cdot 2^{p-1} + 1 \cdot 2^{p-1} \\
&= (2^p - 2 + 1)2^{p-1} \\
&= (2^p - 1)2^{p-1} \\
&= 2^{p-1}(2^p - 1)
\end{aligned}$$

By the definition of a perfect number, we have then shown that $2^{p-1}(2^p - 1)$ is a perfect number.
$\square$

EX 14.

Show that if a and b are positive integers, then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$. [*Hint:* Use the prime factorizations of a and b and the formulae for $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of these factorizations.]

EX 15.

Use the Euclidean algorithm to find

a) gcd(1, 5).
b) gcd(100, 101).
c) gcd(123, 277).
d) gcd(1529, 14039).
e) gcd(1529, 14038).
f) gcd(11111, 111111).

Solution Exercise 14

Given: a and b are positive integers

To proof: $ab = gcd(ab) \cdot lcm(a, b)$

PROOF

Let $p_1, p_2, ..., p_k$ be the primes in the prime factorization in either a or b. Then the prime factorization of a and b is of the form:

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_k^{b_k}$$

The prime factorizations of the numbers have been given. The prime factorization of the **greatest common divisor** then contains all common primes in the prime factorizations of a and b, where its power is the minimum of the powers of the prime in the prime factorization of a and b.

$$gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot ... \cdot p_k^{\min(a_k, b_k)}$$

The prime factorizations of the numbers have been given. The prime factorization of the **least common multiple** then contains all primes in the prime factorizations of a and b, where its power is the maximum of the powers of the prime in the prime factorization of a and b.

$$lcm(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot ... \cdot p_k^{\max(a_k,b_k)}$$

Let us determine the product of the greatest common divisor and least common multiple (use the fact that if $\min(a_i, b_i) = a_i$ then $\max(a_i, b_i) = b_i$ and if $\min(a_i, b_i) = b_i$ then $\max(a_i, b_i) = a_i$):

$$\begin{aligned}
gcd(ab) \cdot lcm(a,b) &= \left(p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot ... \cdot p_k^{\min(a_k,b_k)}\right) \\
&\cdot \left(p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot ... \cdot p_k^{\max(a_k,b_k)}\right) \\
&= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \\
&\cdot ... \cdot p_k^{\min(a_k,b_k)+\max(a_k,b_k)} \\
&= p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdot ... \cdot p_k^{a_k+b_k} \\
&= (p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}) \cdot (p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_k^{b_k}) \\
&= a \cdot b
\end{aligned}$$

□

Solution Exercise 15

(a) gcd(1,5) = 1

(b) gcd(100,101)

101 = 100 * 1 + 1
100 = 1 * 100

Hence, the last nonzero remainder is 1 :
gcd(100,101) = 1

(c) gcd(123,277)

277 = 123 * 2 + 31
123 = 31 * 3 + 30
31 = 30 * 1 + 1
30 = 1 * 30

Hence, the last nonzero remainder is 1 :
gcd(123,277) = 1

(d) gcd(1529,14039)

14039 = 1529 * 9 + 278
1529 = 278 * 5 + 139
278 = 139 * 2

Hence, the last nonzero remainder is 139 :
gcd(1529,14039) = 139

(e) gcd(1529, 14038)

14038 = 1529 * 9 + 277
1529 = 277 * 5 + 144
277 = 144 * 1 + 133
144 = 133 * 1 + 11
133 = 11 * 12 + 1
12 = 1 * 12

Hence, the last nonzero remainder is 1 :
gcd(1529,14038) = 1

(f) gcd(11111, 111111)

$$111111 = 11111 * 10 + 1$$
$$11111 = 1 * 11111$$

Hence, the last nonzero remainder is 1 :

gcd(11111,111111) = 1