4.1 Divisibility and Modular Arithmetic

Chapter 4.1 Question 1(a)

1. Does 17 divide each of these numbers?

a) 68

yes, since $68 = 17 \cdot 4$

$$\begin{array}{r} 4 \\ 17\overline{)68} \\ \underline{68} \\ 0 \end{array}$$

9. What are the quotient and remainder when

a) 19 is divided by 7?

$a = dq + r$, $0 \le r < d$

$q = \lfloor a/d \rfloor$

$$\begin{array}{r} 2 \\ 7\overline{)19} \\ \underline{14} \\ 5 \end{array}$$

2 -> quotient

5 -> remainder

$19 = 7 \cdot 2 + 5$

$q = 2$

$r = 5$

29. Decide whether each of these integers is congruent to 5 modulo 17. **a)** 80

a) $80 = 17 \cdot 4 + 12$

$\Rightarrow 80 \not\equiv 5 \pmod{17}$

4.2 Integer Representations and Algorithms

1. Convert the decimal expansion of each of these integers to a binary expansion.

a) 231

2 | 231   1 ← a_7
2 | 115   1 ← a_6
2 | 57   1 ← a_5
2 | 28   0 ← a_4
2 | 14   0 ← a_3
2 | 7   1 ← a_2
2 | 3   1 ← a_1
2 | 1   1 ← a_0
0

$a_0 = 1$
$a_1 = 1$
$a_2 = 1$
$a_3 = 0$
$a_4 = 0$
$a_5 = 1$
$a_6 = 1$
$a_7 = 1$

$$a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$$

$\Rightarrow (a_7a_6a_5a_4a_3a_2a_1a_0)_2$
$= (11100111)_2$

$\Rightarrow$ Check
$2^0 + 2^1 + 2^2 + 2^5 + 2^6 + 2^7 = 1 + 2 + 4 + 32 + 64 + 128$
$= 231$

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

a) $(572)_8$

$(5)_8 = (101)_2$

$(7)_8 = (111)_2$

$(2)_8 = (010)_2$

$(572)_8 = (1\ 0111\ 1010)_2$

21. Find the sum and the product of each of these pairs of numbers. Express your answers as a binary expansion.

a) $(100\ 0111)_2$, $(111\ 0111)_2$

$0+0=0$
$0+1=1+0=1$
$1+1=10$ "carry the 1 into the next column."

$0\cdot 0 = 0\cdot 1 = 1\cdot 0 = 0$
$1\cdot 1 = 1$

$(100\ 0111)_2 = 1\cdot 2^6 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 64 + 4 + 2 + 1 = 71$

$(111\ 0111)_2 = 1\cdot 2^6 + 1\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 64 + 32 + 16 + 4 + 2 + 1 = 119$

$100\ 0111 + 111\ 0111 = 1011\ 1110$ (decimal : $71 + 119 = 190$)

```
  100 0111
+ 111 0111
----------
 1011 1110
```

$100\ 0111 \cdot 111\ 0111 = 10\ 0001\ 0000\ 0001$ (decimal : $71 \cdot 119 = 8449$)

```
           100 0111
       x   111 0111
       ------------
           1000111
          1000111
         1000111
        00000000
       1000111
      1000111
     1000111
     ----------------
     100001000000001
```

4.3 Primes and Greatest Common Divisors

1. Determine whether each of these integers is prime.

a) 21

prime numbers are numbers that have only 2 factors: 1 & itself.

$21 = 3 \cdot 7$

So, 21 is not prime.

5. Find the prime factorization of 10!.

$$10! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$$
$$= 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5)$$
$$= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

17. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 11, 15, 19

$1 \underline{| \ 11 \quad 15 \quad 19}$

$\quad 11 \quad 15 \quad 19$

gcd (11, 15) = 1

gcd (11, 19) = 1

gcd (15, 19) = 1

The three numbers are pairwise relatively prime.

b) 14, 15, 21

gcd (15, 21) = 3 > 1

These 3 numbers are not pairwise relatively prime.

25. What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

1st number has no prime factors of 2, so the gcd has no 2's.

1st number has seven factors of 3, but the 2nd number only has five.

=> the gcd has five factors of 3.

gcd $(5^3, 5^9) = 5^3$

The gcd has a factor of 5^3.

$\Rightarrow$ The gcd is $3^5 \cdot 5^3$.

27. What is the least common multiple of each pair in Exercise 25?

25. What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

The first number has no prime factors of 2,
but 2nd number has 11 of 2.
=> the lcm has 11 factors of 2.

The first number has seven factors of 3 and the second number has five, the lcm has seven factors of 3.

Similarly, the lcm has a factor of 5^9.

Similarly, the lcm has a factor of 7^3.

=> the lcm is $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$

4.6 Cryptography

5. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \ \mathbf{mod}\ 26$.

a) CEBBOXNOB XYG

to undo the encryption.

=> the letter occurred ten places later in the alphabet.

we need to go backwards 10 places.

OR forward 16 places.

$\Longrightarrow$ SURRENDER NOW

2 A
1 B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
10 S
9 T
8 U
7 V
6 W
5 X
4 Y
3 Z

A	K
B	L
C	M
D	N
E	O
F	P
G	Q
H	R
I	S
J	T
K	U
L	V
M	W
N	X
O	Y
P	Z
Q	A
R	B
S	C
T	D
U	E
V	F
W	G
X	H
Y	I
Z	J