Exercise 4.1

1. Does 17 divide each of these numbers?

a) 68

68 = 17 * 4,

Yes, $17|68$.

9. What are the quotient and remainder when

a) 19 is divided by 7?

Quotient is 2, and remainder is 5.

29. Decide whether each of these integers is congruent to 5 modulo 17.

a) 80

Is $80 \equiv 5 \pmod{17}$?

80 = 17 * 4 + 12

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

Exercise 4.2

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

a) 231

231 – 128 = 103

103 – 64 = 39

39 – 32 = 7

7 – 4 = 3

3 – 2 = 1

1 – 1 = 0

$(231)_{10} = (1110\ 0111)_2$

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

binary expansion.

a) $(572)_8$

5 = 101

7 = 111

2 = 010

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

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

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

Sum:

```
     100 0111
     111 0111
_______________
    1011 1110
```

Product:

```
        100 0111
        111 0111
_________________
        100 0111
       1000 1110
     1 0001 1100
   100 0111 0000
  1000 1110 0000
1 0001 1100 0000
_________________
10 0001 0000 0001
```

Exercise 4.3

1. Determine whether each of these integers is prime.

a) 21

Since 21 = 1 * 21 or 3 * 7

∴ 21 is not prime.

5. Find the prime factorization of 10!.

10! = 1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10

10! = 2 * 3 * 2^2 * 5 * (2 * 3) * 7 * 2^3 * 3^2 * (2 * 5)

10! = $2^8 * 3^4 * 5^2 * 7$

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

b) 14, 15, 21

gcd(14, 15) = 1

gcd(14, 21) = 7

gcd(15, 21) = 1

∴ 14, 15, 21 are not pairwise relatively prime.

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

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

$\gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^{\min(0, 11)} * 3^{\min(7, 5)} * 5^{\min(3, 9)} * 7^{\min(3, 0)}$

$\gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^0 * 3^5 * 5^3 * 7^0$

$\gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 1 * 3^5 * 5^3 * 1$

$\gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 3^5 * 5^3$

∴ 30375 is the greatest common divisor.

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

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

$\text{lcm}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^{\max(0, 11)} * 3^{\max(7, 5)} * 5^{\max(3, 9)} * 7^{\max(3, 0)}$

$\text{lcm}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^{11} * 3^7 * 5^9 * 7^3$

∴ $2^{11} * 3^7 * 5^9 * 7^3$ is the least common multiple.

Exercise 4.6

5. Decrypt these messages encrypted using the shift cipher f (p) = (p + 10) mod 26.

a) CEBBOXNOB XYG

Since it is decryption, the operation goes backward.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

210   109876543

C = S

E = U

B = R

B = R

O = E

X = N

N = D

O = E

B = R

X = N

Y = O

G = W

∴ the decrypted message is SURRENDER NOW