Highest Common Factor

Greatest Common Divisor

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 2/2
Recorded: 8th October 2013

The multiplicative inverse

$$ax + ny = 1$$

Factorisation

- Factorising is to write an integer as a product

$$n = a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

- where all the a_i are integers
- Each factor a_i divides n
  - we write $a_i \mid n$
- Factors are also known as divisors

HØGSKOLEN I ÅLESUND
Aalesund University College

The non-invertible elements

- If a and n have a common factor greater than 1,
  - then there is no solution for

$$ax + ny = 1$$

- I.e. if a and n have a common factor > 1,
  - then a is not invertible

HØGSKOLEN I ÅLESUND
Aalesund University College

Zero divisors

Which are the zero divisors in $\mathbb{Z}_n$?

- For example, in $\mathbb{Z}_{26}$.
  - 2 and 13 are zero divisors because $2 \cdot 13 = 26 \equiv 0$
  - Multiples of 2: $2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24$
  - Multiples of 13? Well the next one is $26 \equiv 0$.
- The factorisation of n is the key.
  - $26 = 2 \cdot 13$
- 2 and 13 are the prime factors
  - their multiples are the zero divisors

HØGSKOLEN I ÅLESUND
Aalesund University College

Highest Common Factor

- American: greatest common divisor

Definition

The highest common factor of two integers a and b is the largest number q such that $q \mid a$ and $q \mid b$. We write $\mathrm{hcf}(a, b) = q$ or $\gcd(a, b) = q$.

- If there is a solution for

$$ax + ny = 1$$

- then $\mathrm{hcf}(a, n) = 1$
- Is the converse true?

HØGSKOLEN I ÅLESUND
Aalesund University College

Exercise

Find

1. $\text{hcf}(6, 4)$
2. $\text{hcf}(7, 3)$
3. $\text{hcf}(18, 12)$
4. $\text{hcf}(19, 8)$