Euclid's Algorithm

Highest Common Factor

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 2/4
Recorded: October 8, 2013

The Highest Common Factor

Definition

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

Exercise

Give an algorithm to calculate $\mathrm{hcf}(a, n)$ *given arbitrary natural numbers* a *and* n*.*

Euclid's Theorem

- We want to find $\mathrm{hcf}(a, n)$ (assume $a \geq n$)
- Recall $a = nq_1 + r_1$
- Write $h = \mathrm{hcf}(a, n)$
- $h \mid a \wedge h \mid n \Rightarrow h \mid r_1$
- Conversely $c \mid n \wedge c \mid r_1 \Rightarrow c \mid a$
- Let's find $n = r_1 q_2 + r_2$

Euclid's Theorem

- We want to find $\mathrm{hcf}(a, n)$ (assume $a \geq n$)
- Recall $a = nq_1 + r_1$
- Write $h = \mathrm{hcf}(a, n)$
- $h \mid a \wedge h \mid n \Rightarrow h \mid r_1$
- Conversely $c \mid n \wedge c \mid r_1 \Rightarrow c \mid a$
- Let's find $n = r_1 q_2 + r_2$

$\rightarrow \mathrm{hcf}(n, r_1)$

Numerical Example

$$\text{hcf}(951, 213)$$

$951 = 213 \cdot 4 + 99$

$213 = 99 \cdot 2 + 15$

$99 = 15 \cdot 6 + 9$

$15 = 9 \cdot 1 + 6$

$9 = 6 \cdot 1 + 3$

$6 = \boxed{3} \cdot 2 + 0$

$213 \cdot 4 = 852$

$99 \cdot 2 = 198$

$15 \cdot 6 = 90$

The process

HCF(a, n) a ≥ n

$$a = nq_1 + r_1 \quad (1)$$
$$n = r_1 q_2 + r_2 \quad (2)$$
$$r_1 = r_2 q_3 + r_3 \quad (3)$$
$$r_2 = r_3 q_4 + r_4 \quad (4)$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n \quad (5)$$
$$r_{n-1} = r_n q_{n+1} + 0 \quad (6)$$

Closure

- Euclid's algorithm finds $\mathrm{hcf}(a, b)$ given a and b

Exercise

Review the slides and write pseudo-code for Euclid's algorithm.