Euclid's Algorithm

The Proof

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 3/1
Recorded: October 9, 2013

The process

$$a = nq_1 + r_1 \tag{1}$$
$$n = r_1 q_2 + r_2 \tag{2}$$
$$r_1 = r_2 q_3 + r_3 \tag{3}$$
$$r_2 = r_3 q_4 + r_4 \tag{4}$$
$$\vdots \tag{5}$$
$$r_{n-2} = r_{n-1} q_n + r_n \tag{6}$$
$$r_{n-1} = r_n q_{n+1} + 0 \tag{7}$$

Exercise

Prove that Euclid's algorithm is correct.

Recursive formulation

$$a \mod n \neq 0 \implies \mathrm{hcf}(a,n) = \mathrm{hcf}(n, a \mod n)$$

procedure $\mathrm{hcf}(a,n)$
  if $a < n$, return $\mathrm{hcf}(n,a)$
  else
    $r = a \mod n$
    if $r = 0$, return n
    else return $\mathrm{hcf}(n,r)$

Correctness

$$P(r) : \mathrm{hcf}(a, n) \text{ is correct when } r = a \mod n,$$

Base Case

$$P(r) : \mathrm{hcf}(a, n) \text{ is correct when } r = a \mod n,$$

- Is $P(0)$ true?
- We have $r = 0$ in the algorithm
  - $n \mid a$ and $n \mid n$
  - Clearly $m > n$ cannot divide n
  - Hence $\mathrm{hcf}(a, n) = n$
- The algoritm outputs n which is correct
- Thus $P(0)$ is true.

Inductive case

$$P(r) : \mathrm{hcf}(a, n) \text{ is correct when } r = a \mod n,$$

- For $r > 0$, the algorithm returns $\mathrm{hcf}(a, r)$
- Do we have $\mathrm{hcf}(a, n) = \mathrm{hcf}(n, r)$?
- We need to prove to claims
  1. $\mathrm{hcf}(a, n) \mid \mathrm{hcf}(n, r)$
  2. $\mathrm{hcf}(n, r) \mid \mathrm{hcf}(a, n)$

First case

- Claim: $\mathrm{hcf}(a, n) \mid \mathrm{hcf}(n, r)$
- We know that
  1. $\mathrm{hcf}(a, n) \mid a$
  2. $\mathrm{hcf}(a, n) \mid n$
- We have to prove $\mathrm{hcf}(a, n) \mid r$
- Recall $a = qn + r$
  1. Since $\mathrm{hcf}(a, n) \mid a$ and $\mathrm{hcf}(a, n) \mid n$
  2. we get $\mathrm{hcf}(a, n) \mid r$
- Hence the claim is proved.

Second case

- Claim: $\mathrm{hcf}(n, r) \mid \mathrm{hcf}(a, n)$
- We know that
  1. $\mathrm{hcf}(n, r) \mid n$
  2. $\mathrm{hcf}(n, r) \mid r$
- We have to prove $\mathrm{hcf}(n, r) \mid a$
- Recall $a = qn + r$
  1. Since $\mathrm{hcf}(n, r) \mid qn$ and $\mathrm{hcf}(n, r) \mid r$
  2. we get $\mathrm{hcf}(n, r) \mid a$
- Hence the claim is proved.

Second case

- Claim: $\mathrm{hcf}(n, r) \mid \mathrm{hcf}(a, n)$
- We know that
  1. $\mathrm{hcf}(n, r) \mid n$
  2. $\mathrm{hcf}(n, r) \mid r$
- We have to prove $\mathrm{hcf}(n, r) \mid a$
- Recall $a = qn + r$
  1. Since $\mathrm{hcf}(n, r) \mid qn$ and $\mathrm{hcf}(n, r) \mid r$
  2. we get $\mathrm{hcf}(n, r) \mid a$
- Hence the claim is proved.

Closure

- Euclid's algorithm uses the fact that
    - if $a \geq b$ and $a \mod b \neq 0$, then
    - $\mathrm{hcf}(b, b) = \mathrm{hcf}(a, a \mod b)$