Euclid's Division Theorem

The proof

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 2/3
Recorded: 8th October 2013

The foundation of modular arithmetics

Theorem (Euclid's Division Theorem)

Let n be a positive integer. Then for every integer m, there exist unique integers q and r so that $m = nq + r$ and $0 \leq r < n$.

Theorem (Restricted version)

Let n be a positive integer. Then for every non-negative integer m, there exist unique integers q and r so that $m = nq + r$ and $0 \leq r < n$.

Proof by Contradiction

$$\forall m, \exists (q, r), m = nq + r \wedge 0 \leq r < n$$

- We will use a proof by contradiction
- Interested in the smallest counter-example
    - which we explored introducing mathematical induction

Proving Euclid

Proving Euclid

Continued

Exercise

Prove that Euclid's Division Theorem is also valid for negative numbers m.

Hint. Note that if $m < 0$, then $-m > 0$ and the restricted version can be applied to $m' = -m$ to get numbers q' and r' to solve $m' = nq' + r'$. Note that q may be negative, while r cannot, so $q = -q'$ and $r = -r'$ is not quite the solution. Can you add/subtract a little bit to these numbers to get $0 \leq r < n$ and satisfy Euclid's theorem?