Mathematics and Cryptography

Part 7

Jean-Sébastien Coron

Université du Luxembourg

October 26, 2009

Algorithmic number theory

- Goal: modular computation with large integers.
  - Addition, multiplication, inversion modulo n.
- Euclidean division:
  - Given a, b, find q, r such that

$$a = b \cdot q + r$$

where a, b are big integers.

Substraction

- Computing $c = a - b$ with $a, b > 0$
  - Let $a = (a_{k-1} \dots a_0)$ and $b = (b_{\ell-1} \dots b_0)$ with $k \geq \ell \geq 1$.
    Let $c = (c_k c_{k-1} \dots c_0)$
    $carry \leftarrow 0$
    for $i = 0$ to $\ell - 1$ do
      $tmp \leftarrow a_i - b_i + carry$
      $carry \leftarrow tmp/B$; $c_i \leftarrow tmp \mod B$
    for $i = \ell$ to $k - 1$ do
      $tmp \leftarrow a_i + carry$
      $carry \leftarrow tmp/B$; $c_i \leftarrow tmp \mod B$
    $c_k \leftarrow carry$
  - If $a \geq b$ then $c_k = 0$, otherwise $c_k = -1$.
  - If $c_k = -1$, compute $c' = b - a$ and let $c := -c'$.

Division with remainder

- Let $a = (a_{k-1} \dots a_0)_B$ and $b = (b_{\ell-1} \dots b_0)_B$ with $a > b > 0$ and $b_{\ell-1} \neq 0$.
  - Compute q and r such that $a = b \cdot q + r$ and $0 \leq r < b$.
  - $q = (q_{m-1} \dots q_0)_B$, with $m := k - \ell + 1$.
- Algorithm overview:

$r \leftarrow a$
for $i = m - 1$ downto 0 do
  $q_i \leftarrow r / (B^i b)$
  $r \leftarrow r - B^i \cdot q_i \cdot b$
output r

Division with remainder

- For all i, $0 \leq r < B^i \cdot b$ after step i
  - Therefore, $0 \leq r < b$ eventually.
- How to compute $q_i = r/(B^i \cdot b)$
  - Test all possible values of $0 \leq q_i < B$
  - Not efficient, except if B is small (*e.g.* $B = 10$).
  - Possible to do much better

Division with remainder

- Complete algorithm (for small B)

$r \leftarrow a$
for $i = m - 1$ downto 0 do
  $q_i \leftarrow 0$
  while $r >= 0$
    $r \leftarrow r - B^i \cdot b$
    $q_i \leftarrow q_i + 1$
  $q_i \leftarrow q_i - 1$
  $r \leftarrow r + B^i \cdot b$
output r

Computing in $\mathbb{Z}_n$

- Computing $c = a + b$ in $\mathbb{Z}_n$
  - Let $c \leftarrow a + b$ in $\mathbb{Z}$
  - Let $c \leftarrow c \mod n$.
  - Complexity: $\mathcal{O}(\log n)$
- Computing $c = a \cdot b$ in $\mathbb{Z}_n$
  - Let $c \leftarrow a + b$ in $\mathbb{Z}$
  - Let $c \leftarrow c \mod n$.
  - Complexity: $\mathcal{O}(\log^2 n)$.