Extended Euclidean algorithm (XGCD)

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Euclidean algorithm and gcd

- The Euclidean algorithm computes the gcd of two numbers

$$d = \gcd(m, n)$$

  in time polynomial in $\log_2(\max\{m, n\})$.
- This is much faster than factoring m and n.
- Each step computes the quotient and remainder of two integers, starting with $m = q_1 \cdot n + r_1$, followed by $n = q_2 r_1 + r_2$, $r_1 = q_3 r_2 + r_3, r_2 = q_4 r_3 + r_4, \ldots$.
  The algorithm stops when $r_i = 0$ and outputs $d = r_{i-1}$ as the gcd.

Euclidean algorithm and gcd

- The Euclidean algorithm computes the gcd of two numbers

$$d = \gcd(m, n)$$

  in time polynomial in $\log_2(\max\{m, n\})$.
- This is much faster than factoring m and n.
- Each step computes the quotient and remainder of two integers, starting with $m = q_1 \cdot n + r_1$, followed by $n = q_2 r_1 + r_2$, $r_1 = q_3 r_2 + r_3, r_2 = q_4 r_3 + r_4, \ldots$.
  The algorithm stops when $r_i = 0$ and outputs $d = r_{i-1}$ as the gcd.
- The extended Euclidean algorithm (XGCD) computes integers a, b with

$$d = \gcd(m, n) = am + bn,$$

  and $|a| < n$, $|b| < m$.

Euclidean algorithm and gcd

- The Euclidean algorithm computes the gcd of two numbers

$$d = \gcd(m, n)$$

in time polynomial in $\log_2(\max\{m, n\})$.
- This is much faster than factoring m and n.
- Each step computes the quotient and remainder of two integers, starting with $m = q_1 \cdot n + r_1$, followed by $n = q_2 r_1 + r_2$, $r_1 = q_3 r_2 + r_3, r_2 = q_4 r_3 + r_4, \dots$.
The algorithm stops when $r_i = 0$ and outputs $d = r_{i-1}$ as the gcd.
- The extended Euclidean algorithm (XGCD) computes integers a, b with

$$d = \gcd(m, n) = am + bn,$$

and $|a| < n$, $|b| < m$.
- Can compute a, b by reversing steps above, starting with

$$r_{i-1} = r_{i-3} - q_{i-1} r_{i-2} = r_{i-3} - q_{i-1}(r_{i-4} - q_{i-2} r_{i-3}) = \cdots = am + bn$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\, w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$\begin{array}{llll} [\ 312, & 1, & 0] & \\ [\ 213, & 0, & 1] & q = 1 \end{array}$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] &
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{rrrl}
[\ 312, & 1, & 0] & \\
[\ 213, & 0, & 1] & q = 1 \\
[\ 99, & 1, & -1] & q = 2 \\
[\ 15, & -2, & 3] &
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6 \\
[& 9, & 13, & -19] &
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   - 3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   - 3.2 $v \leftarrow w$
   - 3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6 \\
[& 9, & 13, & -19] & q = 1
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   - 3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   - 3.2 $v \leftarrow w$
   - 3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

[312,	1,	0]	
[213,	0,	1]	$q = 1$
[99,	1,	−1]	$q = 2$
[15,	−2,	3]	$q = 6$
[9,	13,	−19]	$q = 1$
[6,	−15,	22]	

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   - 3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   - 3.2 $v \leftarrow w$
   - 3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6 \\
[& 9, & 13, & -19] & q = 1 \\
[& 6, & -15, & 22] & q = 1
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

$$
\begin{array}{lrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6 \\
[& 9, & 13, & -19] & q = 1 \\
[& 6, & -15, & 22] & q = 1 \\
[& 3, & 28, & -41] &
\end{array}
$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

[312,	1,	0]	
[213,	0,	1]	$q = 1$
[99,	1,	-1]	$q = 2$
[15,	-2,	3]	$q = 6$
[9,	13,	-19]	$q = 1$
[6,	-15,	22]	$q = 1$
[3,	28,	-41]	$q = 2$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   3.2 $v \leftarrow w$
   3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

[312,	1,	0]	
[213,	0,	1]	$q = 1$
[99,	1,	-1]	$q = 2$
[15,	-2,	3]	$q = 6$
[9,	13,	-19]	$q = 1$
[6,	-15,	22]	$q = 1$
[3,	28,	-41]	$q = 2$
[0,	,	]	

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   - 3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   - 3.2 $v \leftarrow w$
   - 3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

Input 312, 213

[312,	1,	0]	
[213,	0,	1]	$q = 1$
[99,	1,	-1]	$q = 2$
[15,	-2,	3]	$q = 6$
[9,	13,	-19]	$q = 1$
[6,	-15,	22]	$q = 1$
[3,	28,	-41]	$q = 2$
[0,	,	]	

$d = 3, a = 28, b = -41$
indeed

$$28 \cdot 312 - 41 \cdot 213 = 3.$$

Extended Euclidean algorithm

Input $m, n \in \mathbb{N}$
Output $d \in \mathbb{N}, a, b \in \mathbb{Z}$ with $d = am + bn$

1. $v \leftarrow [m, 1, 0]$
2. $w \leftarrow [n, 0, 1]$
3. while $w[0] \neq 0$
   - 3.1 $x \leftarrow v - (v[0] \text{ div } w[0])\ w$
   - 3.2 $v \leftarrow w$
   - 3.3 $w \leftarrow x$
4. $d \leftarrow v[0]$, $a \leftarrow v[1]$, $b \leftarrow v[2]$
5. return d, a, b

At every step, $v[0] = v[1]m + v[2]n$.

Input 312, 213

$$
\begin{array}{rrrrl}
[& 312, & 1, & 0] & \\
[& 213, & 0, & 1] & q = 1 \\
[& 99, & 1, & -1] & q = 2 \\
[& 15, & -2, & 3] & q = 6 \\
[& 9, & 13, & -19] & q = 1 \\
[& 6, & -15, & 22] & q = 1 \\
[& 3, & 28, & -41] & q = 2 \\
[& 0, & , &] &
\end{array}
$$

$d = 3, a = 28, b = -41$
indeed

$$28 \cdot 312 - 41 \cdot 213 = 3.$$

XGCD for inversion

- On input m, n, XGCD computes d, a, b with

$$d = am + bn.$$

- An integer m is invertible modulo n if it is co-prime to n, i.e., if $\gcd(m, n) = 1$.
- XGCD is an efficient way to compute modular inverses:

$$1 = am + bn \quad \Rightarrow$$

XGCD for inversion

- On input m, n, XGCD computes d, a, b with
$$d = am + bn.$$
- An integer m is invertible modulo n if it is co-prime to n, i.e., if $\gcd(m, n) = 1$.
- XGCD is an efficient way to compute modular inverses:
$$1 = am + bn \quad \Rightarrow \quad 1 \equiv am \bmod n.$$

Thus
$$m^{-1} \equiv a \bmod n.$$

XGCD for inversion

- On input m, n, XGCD computes d, a, b with

$$d = am + bn.$$

- An integer m is invertible modulo n if it is co-prime to n, i.e., if $\gcd(m, n) = 1$.
- XGCD is an efficient way to compute modular inverses:

$$1 = am + bn \quad \Rightarrow \quad 1 \equiv am \bmod n.$$

  Thus

$$m^{-1} \equiv a \bmod n.$$

- Of course, this only works if m is invertible modulo n.

XGCD for inversion

- On input m, n, XGCD computes d, a, b with
$$d = am + bn.$$
- An integer m is invertible modulo n if it is co-prime to n, i.e., if $\gcd(m, n) = 1$.
- XGCD is an efficient way to compute modular inverses:
$$1 = am + bn \quad \Rightarrow \quad 1 \equiv am \bmod n.$$
Thus
$$m^{-1} \equiv a \bmod n.$$
- Of course, this only works if m is invertible modulo n.
In the example
$$28 \cdot 312 - 41 \cdot 213 = 3.$$
Thus 312 and 213 are not co prime.