Chapter 31: Euclidean Algorithm

- Euclidean Algorithm
- Extended Euclidean Algorithm
- Solving $ax \mod n = 1$
- Solving $ax \mod n = b$
Overview

• Solving modular equations arises in cryptography
• Euclidean Algorithm
• From Euclid to solving $ax \mod n = 1$
• From $ax \mod n = 1$ to solving $ax \mod n = b$
Euclidean Algorithm

- Given positive integers $a$ and $b$, find their greatest common divisor

- Idea
  - if $x$ is the greatest common divisor of $a$ and $b$, then $x$ divides $r = a - b$
  - reduces problem to finding largest $x$ that divides $r$ and $b$
  - iterate
Example 1

- Take $a = 15$, $b = 12$
  
  \[
  \begin{array}{cccc}
  a & b & q & r \\
  15 & 12 & 1 & 3 \\
  12 & 3 & 4 & 0 \\
  \end{array}
  \]

  \[
  \begin{align*}
  q &= 15 / 12 = 1 \\
  r &= 15 - 1 \times 12 \\
  q &= 12 / 3 = 4 \\
  r &= 12 - 4 \times 3 \\
  \end{align*}
  \]

- so $gcd(15, 12) = 3$
  - The $b$ for which $r$ is 0
Example 2

- Take $a = 35731, b = 25689$

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$b$</td>
<td>$q$</td>
<td>$r$</td>
</tr>
<tr>
<td>35731</td>
<td>24689</td>
<td>1</td>
<td>11042</td>
</tr>
<tr>
<td>24689</td>
<td>11042</td>
<td>2</td>
<td>2,605</td>
</tr>
<tr>
<td>11042</td>
<td>2605</td>
<td>4</td>
<td>622</td>
</tr>
<tr>
<td>2605</td>
<td>622</td>
<td>4</td>
<td>117</td>
</tr>
<tr>
<td>622</td>
<td>117</td>
<td>5</td>
<td>37</td>
</tr>
<tr>
<td>117</td>
<td>37</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>37</td>
<td>6</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

$q = \frac{35731}{24689} = 1$
$r = 35731 - 1 \times 24689$

$q = \frac{24689}{11042} = 2$
$r = 24689 - 2 \times 11042$

$q = \frac{11042}{2605} = 4$
$r = 11042 - 4 \times 2605$

$q = \frac{2605}{622} = 4; r = 2605 - 4 \times 622$

$q = \frac{622}{117} = 5; r = 622 - 5 \times 117$

$q = \frac{117}{37} = 3; r = 117 - 3 \times 37$

$q = \frac{37}{6} = 6; r = 37 - 6 \times 6$

$q = \frac{6}{1} = 6; r = 6 - 6 \times 1$
/* find gcd of a and b */
rprev := r := 1;
while r <> 0 do begin
    rprev := r;
    r := a mod b;
    write 'a = ', a, 'b =', b, 'q = ', a div b,
        'r = ', r, endline;
    a := b;
    b := r;
end;
gcd := rprev;
Extended Euclidean Algorithm

- Find two integers $x$ and $y$ such that
  \[ xa + yb = 1 \]
Example 1

• Find $x$ and $y$ such that $51x + 100y = 1$

<table>
<thead>
<tr>
<th>$u$</th>
<th>$x$</th>
<th>$y$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>1</td>
<td>0</td>
<td>100/51 = 1</td>
</tr>
<tr>
<td>49</td>
<td>-1</td>
<td>1</td>
<td>51/49 = 1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>-1</td>
<td>49/2 = 24</td>
</tr>
<tr>
<td>1</td>
<td>-49</td>
<td>25</td>
<td>2/1 = 2</td>
</tr>
<tr>
<td>0</td>
<td>100</td>
<td>-51</td>
<td></td>
</tr>
</tbody>
</table>

• $u = 51 - 1 \times 49; x = 0 - 1 \times 1; y = 1 - 1 \times 0$
• $u = 51 - 1 \times 49; x = 1 - 1 \times (-1); y = 0 - 1 \times 1$
• $u = 49 - 24 \times 2; x = -1 - 24 \times 2; y = 1 - 24 \times (-1)$

• So, $51 \times (-49) + 100 \times 25 = 1$
  – This is $-2499 + 2500 = 1$
Example 2

• Find $x$ and $y$ such that $24689x + 35731y = 1$

<table>
<thead>
<tr>
<th></th>
<th>$u$</th>
<th>$x$</th>
<th>$y$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>35731</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24689</td>
<td>1</td>
<td>0</td>
<td>35731/24689 = 1</td>
<td></td>
</tr>
<tr>
<td>11042</td>
<td>−1</td>
<td>1</td>
<td>24689/11042 = 2</td>
<td>$u = 35721−1×24689; x = 0−1×1; y = 1−1×0$</td>
</tr>
<tr>
<td>2605</td>
<td>3</td>
<td>−2</td>
<td>11042/2.605 = 4</td>
<td>$u = 24689−2×11042; x = 1−2×(−1); y = 0−2×1$</td>
</tr>
<tr>
<td>622</td>
<td>−13</td>
<td>9</td>
<td>2605/622 = 4</td>
<td>$u = 11042−4×2605; x = −1−4×3; y = 1−4×(−2)$</td>
</tr>
<tr>
<td>117</td>
<td>55</td>
<td>−38</td>
<td>622/117 = 5</td>
<td>$u = 2605−4×622; x = 3−4×(−13); y = −2−4×9$</td>
</tr>
<tr>
<td>37</td>
<td>−288</td>
<td>199</td>
<td>117/37 = 3</td>
<td>$u = 622−5×117; x = −13−5×55; y = 9−5×(−38)$</td>
</tr>
<tr>
<td>6</td>
<td>919</td>
<td>−635</td>
<td>37/6 = 6</td>
<td>$u = 117−3×37; x = 55−3×(−288); y = −38−3×199$</td>
</tr>
<tr>
<td>1</td>
<td>−5802</td>
<td>4,009</td>
<td>6/1=6</td>
<td>$u = 37−6×6; x = −288−6×919; y = 199−6×(−635)$</td>
</tr>
<tr>
<td>0</td>
<td>35731−24689</td>
<td></td>
<td>$u = 6−6×1; x = 919−6×(−5802)$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$y = −635−6×(4009)$</td>
<td></td>
</tr>
</tbody>
</table>

• So, $24689 \times (−5802) + 35731 \times 4009 = 1$
/* find $x$ and $y$ such that $ax + by = 1$, for given $a$ and $b$ */
uprev := a; u := b;
xprev := 0; x := 1; yprev := 1; y := 0;
write 'u = ', uprev, ' x = ', xprev, ' y = ', yprev, endline;
write 'u = ', u, ' x = ', x, ' y = ', y;
while u <> 0 do begin
  q := uprev div u;
  write 'q = ', q, endline;
  utmp := uprev – u * q; uprev := u; u := utmp;
  xtmp := xprev – x * q; xprev := x; x := xtmp;
  ytmp := yprev – y * q; yprev := y; y := ytmp;
  write 'u = ', u, ' x = ', x, ' y = ', y;
end;
write endline;
x := xprev; y := yprev;
Solving $ax \mod n = 1$

- If $ax \mod n = 1$ then choose $k$ such that $ax = 1 + kn$, or $ax - kn = 1$. If $b = -k$, then $ax + bn = 1$.
- Use extended Euclidean algorithm to solve for $a$
Example

• Solve for $x$: $51x \mod 100 = 1$
  – Recall (from earlier example)
    $51 \times (-49) + 100 \times 25 = 1$
    Then $x = -49 \mod 100 = 51$

• Solve for $x$: $24689 \mod 35731 = 1$
  – Recall (from earlier example)
    $24689 \times (-5802) + 35731 \times 4009 = 1$
    Then $x = -5802 \mod 35731 = 29929$
Solving $ax \mod n = b$

- A fundamental law of modular arithmetic:
  
  $xy \mod n = (x \mod n)(y \mod n) \mod n$

  so if $x$ solves $ax \mod n = 1$, then as

  $b(ax \mod n) = a(bx) \mod n = b$

  $bx$ solves $ax \mod n = b$
Example

• Solve for $x$: $51x \mod 100 = 10$
  – Recall (from earlier example) that if $51y \mod 100 = 1$, then $y = 51$.
    Then $x = 10 \times 51 \mod 100 = 510 \mod 100 = 10$

• Solve for $x$: $24689 \mod 35731 = 1753$
  – Recall (from earlier example) that if $24689y \mod 35731 = 1$, then $y = 29929$.
    Then $x = 1753 \times 29929 \mod 35731 = 12429$