Number-Theoretic Algorithms

B.H.M.

@ CSE_SSIT
Elementary number-theoretic notions

set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of integers

set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of natural numbers.

**Divisibility and divisors**

The notation $d \mid a$ (read “$d$ divides $a$”) means that $a = kd$ for some integer $k$.

Divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

Prime and composite numbers

The division theorem, remainders, and modular equivalence

Theorem 31.1 (Division theorem)
For any integer \( a \) and any positive integer \( n \), there exist unique integers \( q \) and \( r \) such that \( 0 \leq r < n \) and \( a = qn + r \).

The value \( q = \lfloor a/n \rfloor \) is the quotient of the division. The value \( r = a \mod n \) is the remainder (or residue) of the division. We have that \( n \mid a \) if and only if \( a \mod n = 0 \).

We can partition the integers into \( n \) equivalence classes according to their remainders modulo \( n \). The equivalence class modulo \( n \) containing an integer \( a \) is

\[
[a]_n = \{ a + kn : k \in \mathbb{Z} \}.
\]

For example, \([3]_7 = \{ \ldots, -11, -4, 3, 10, 17, \ldots \}\);

\( a \in [b]_n \) is the same as writing \( a \equiv b \pmod{n} \).
Common divisors and greatest common divisors

If $d$ is a divisor of $a$ and $d$ is also a divisor of $b$, then $d$ is a common divisor of $a$ and $b$. For example, the divisors of 30 are 1, 2, 3, 5, 6, 10, 15, and 30, and so the common divisors of 24 and 30 are 1, 2, 3, and 6. Note that 1 is a common divisor of any two integers.

An important property of common divisors is that

$$d \mid a \text{ and } d \mid b \implies d \mid (a + b) \text{ and } d \mid (a - b).$$

(31.3)

More generally, we have that

$$d \mid a \text{ and } d \mid b \implies d \mid (ax + by)$$

(31.4)

The greatest common divisor of two integers $a$ and $b$, not both zero, is the largest of the common divisors of $a$ and $b$; we denote it by $\gcd(a, b)$. For example,

$$\gcd(24, 30) = 6, \gcd(5, 7) = 1, \text{ and } \gcd(0, 9) = 9.$$
Theorem 31.2
If $a$ and $b$ are any integers, not both zero, then $\gcd(a, b)$ is the smallest positive element of the set $\{ax + by : x, y \in \mathbb{Z}\}$ of linear combinations of $a$ and $b$.

Proof  Let $s$ be the smallest positive such linear combination of $a$ and $b$, and let $s = ax + by$ for some $x, y \in \mathbb{Z}$. Let $q = [a/s]$. Equation (3.8) then implies

$$\begin{align*}
    a \mod s &= a - qs \\
    &= a - q(ax + by) \\
    &= a(1 - qx) + b(-qy),
\end{align*}$$

Corollary 31.3
For any integers $a$ and $b$, if $d \mid a$ and $d \mid b$, then $d \mid \gcd(a, b)$.

Corollary 31.4
For all integers $a$ and $b$ and any nonnegative integer $n$,

$$\gcd(an, bn) = n \gcd(a, b).$$

Corollary 31.5
For all positive integers $n, a,$ and $b$, if $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$. 
Relatively prime integers

Two integers $a$ and $b$ are \textit{relatively prime} if their only common divisor is 1, that is, if $\gcd(a, b) = 1$. For example, 8 and 15 are relatively prime, since the divisors of 8 are 1, 2, 4, and 8, and the divisors of 15 are 1, 3, 5, and 15.

\textbf{Theorem 31.6}

For any integers $a$, $b$, and $p$, if both $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$, then $\gcd(ab, p) = 1$.

\textbf{Proof} \quad$\text{It follows from Theorem 31.2 that there exist integers } x, y, x', \text{ and } y' \text{ such that}\$

\begin{align*}
ax + py &= 1, \\
bx' + py' &= 1.
\end{align*}

Multiplying these equations and rearranging, we have

\begin{align*}
ab(xx') + p(ybx' + y'ax + pyy') &= 1.
\end{align*}

Since 1 is thus a positive linear combination of $ab$ and $p$, an appeal to Theorem 31.2 completes the proof.
Greatest common divisor

Euclid(a, b)
1 if b = 0
2 then return a
3 else return Euclid(b, a mod b)

Euclid(30, 21) = Euclid(21, 9)
    = Euclid(9, 3)
    = Euclid(3, 0)
    = 3

The running time of Euclid's algorithm

We analyze the worst-case running time of EUCLID as a function of the size of \( a \) and \( b \). Assume with no loss of generality that \( a > b \geq 0 \).

The overall running time of EUCLID is proportional to the number of recursive calls it makes. Our analysis makes use of the Fibonacci numbers \( F_k \)
**Lemma:** If \( a > b \geq 1 \) and the invocation EUCLID\((a, b)\) performs \( k \geq 1 \) calls then \( a \geq F_{k+2} \) and \( b \geq F_{k+1} \)

**Proof:** (By induction)

**Basis:** Let \( k=1 \), we know \( a > b \geq 1 \)

\[ \Rightarrow b \geq F_2 = 1 \text{ (here } k+1=2) \]

Since \( a > b \Rightarrow a \geq 2 \Rightarrow a \geq F_3 \text{ (here } k+2=3) \)

**Inductive Hypothesis:** Assume the result holds for \# of invocations \( \leq k - 1 \)

**Inductive proof:** Let EUCLID \((a, b)\) makes \( k \) invocations

\[ \Rightarrow \text{EUCLID} \ (b, a \mod b) \text{ makes } (k-1) \text{ invocation} \]

We have

From our inductive hypothesis:

\[ b \geq F_{(k-1)+2}, a \mod b \geq F_{(k-1)+1} \]

Therefore \( b \geq F_{k+1}, a \mod b \geq F_k \)

\[ b + (a \mod b) = b + (a - \lfloor a/b \rfloor b) \]

\[ \leq a \]

\[ a \geq b + (a \mod b) \]

\[ \geq F_{k+1} + F_k \]

\[ = F_{k+2} \]
EXTENDED-EUCLID Algorithm

Goal: Given 2 integers $a$ and $b$ compute integers $x$ and $y$ such that $gcd(a, b) = ax + by$.

EXTENDED-EUCLID $(a, b)$

1. if $b = 0$
2. then return $(a, 1, 0)$
3. $(d', x', y') \leftarrow$ EXTENDED-EUCLID $(b, a \mod b)$
4. $(d, x, y) \leftarrow (d', y', x' - \left[ \frac{a}{b} \right] y')$
5. return $(d, x, y)$

For $a=99$ and $b=78$ the following table illustrates the values of variables $d$, $x$, $y$ at different levels of recursion for the algorithm EXTENDED-EUCLID(99, 78). We can easily verify that $gcd(99, 78) = 3 = -11(99) + 14(78)$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$\left[ \frac{a}{b} \right]$</th>
<th>$d$</th>
<th>$x$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>78</td>
<td>1</td>
<td>3</td>
<td>-11</td>
<td>14</td>
</tr>
<tr>
<td>78</td>
<td>21</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>-11</td>
</tr>
<tr>
<td>21</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>--</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
The correctness of the algorithm is established from the following inductive argument.

**Basis:** Let \( d \) denote \( \gcd(a, b) \). When EUCLID terminates \( b = 0 \) and \( d = a \Rightarrow x = 1, \ y = 0 \). Thus the arguments returned by EXTENDED-EUCLID is correct.

**Inductive Hypothesis:** Assume the values \( d', x', y' \) returned by EXTENDED-EUCLID\((b, a \mod b)\) is correct.

**Induction Step:** We have to show EXTENDED-EUCLID\((a, b)\) correctly computes \( d, x, y \).

\[
d' = x'b + y' (a \mod b) = x'b + y' (a - \left\lfloor \frac{a}{b} \right\rfloor b) = y'a + (x' - \left\lfloor \frac{a}{b} \right\rfloor y')b = d
\]

\[
\Rightarrow x = y' \text{ and } y = x' - \left\lfloor \frac{a}{b} \right\rfloor y'.
\]
Modular Arithmetic

Integers modulo $n$

- Let $n \geq 2$ be an integer.

- Def: $a$ is congruent to $b$ modulo $n$, written $a \equiv b \mod n$, if $n \mid (a - b)$, i.e., $a$ and $b$ have the same remainder when divided by $n$.

- Note: $a \equiv b \mod n$ and $a = b \mod n$ are different.

- Def: $[a]_n = \{\text{all integers congruent to } a \text{ modulo } n\}$.

- $[a]_n$ is called a residue class modulo $n$, and $a$ is a representative of that class.
• There are exactly $n$ residue classes modulo $n$:
  $[0], [1], [2], \ldots, [n-1]$.

• Note: "congruence mod $n$" is an equivalence relation, whose equivalence classes are the residue classes.

• If $x \in [a]$, $y \in [b]$, then $x + y \in [a + b]$ and $x \cdot y \in [a \cdot b]$.

• Define addition and multiplication for residue classes:

  $[a] +_n [b] = [a + b]$

  $[a] \cdot_n [b] = [a \cdot b]$. 
Group

A group \((S, \oplus)\) is a set \(S\) together with a binary operation \(\oplus\) defined on \(S\) for which the following properties hold.

1. **Closure:** For all \(a, b \in S\), we have \(a \oplus b \in S\).
2. **Identity:** There is an element \(e \in S\), called the identity of the group, such that \(e \oplus a = a \oplus e = a\), for all \(a \in S\).
3. **Associativity:** For all \(a, b, c \in S\), we have \((a \oplus b) \oplus c = a \oplus (b \oplus c)\).
4. **Inverses:** For each \(a \in S\), there exists a unique element \(b \in S\), called the inverse of \(a\), such that \(a \oplus b = b \oplus a = e\).

As an example, consider the familiar group \((\mathbb{Z}, +)\) of the integers \(\mathbb{Z}\) under the operation of addition: \(0\) is the identity, and the inverse of \(a\) is \(-a\).

**Abelian group:**

If a group \((S, \oplus)\) satisfies the **commutative law** \(a \oplus b = b \oplus a\), for all \(a, b \in S\), then it is an **abelian group**.
The groups defined by modular addition and multiplication

First we define the congruence notation $\equiv$ as follows:

If $a, b \in \mathbb{Z}$ then we say $a \equiv b$ modulo $n$ if $\exists p, q, r \in \mathbb{Z}$ such that $a = pn + r$ and $b = qn + r$.

We will denote $a \mod n$ as $[a]_n$.

We can form two finite abelian groups by using addition and multiplication modulo $n$, where $n$ is a positive integer. These groups are based on the equivalence classes of the integers modulo $n$.

If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$a + b \equiv a' + b' \pmod{n},$

$ab \equiv a'b' \pmod{n}$. 
Thus, we define addition and multiplication modulo $n$, denoted $+_n$ and $\cdot_n$, as follows:

$[a]_n +_n [b]_n = [a + b]_n$ (addition modulo $n$)

$[a]_n \cdot_n [b]_n = [a \cdot b]_n$ (multiplicative modulo $n$)

Using this definition of addition modulo $n$, we define the **additive group modulo $n$** as $(\mathbb{Z}_n, +_n)$. The size of the additive group modulo $n$ is $|\mathbb{Z}_n| = n$. Modular addition over the group $(\mathbb{Z}_6, +_6)$ is defined as follows:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

(a) The group $(\mathbb{Z}_6, +_6)$.

Closure: If $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_n$ then from the definition of addition modulo $n$ $a +_n b = [a + b]_n \in \mathbb{Z}_n$.

Identity: 0 is the identity element of $\mathbb{Z}_n$

Inverse: Inverse of $[a]_n$ is $[-a]_n \equiv [n-a]_n$
Using this definition of multiplication modulo $n$, we define the **multiplicative group modulo** $n$ as $(Z^*_n, \cdot_n)$ where $Z^*_n = \{ [a]_n \in Z_n | \gcd(a, n) = 1 \}$. For e.g. when $n = 15$,

$Z^*_15 = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Modular multiplication over the group $(Z^*_15, \cdot_{15})$ is defined as follows:

\[
\begin{array}{cccccccc}
  & 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\
1 & 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\
2 & 2 & 4 & 8 & 14 & 1 & 7 & 11 & 13 \\
4 & 4 & 8 & 1 & 13 & 2 & 14 & 7 & 11 \\
7 & 7 & 14 & 13 & 4 & 11 & 2 & 1 & 8 \\
8 & 8 & 1 & 2 & 11 & 4 & 13 & 14 & 7 \\
11 & 11 & 7 & 14 & 2 & 13 & 1 & 8 & 4 \\
13 & 13 & 11 & 7 & 1 & 14 & 8 & 4 & 2 \\
14 & 14 & 13 & 11 & 8 & 7 & 4 & 2 & 1 \\
\end{array}
\]

(b) The group $(Z^*_15, \cdot_{15})$.

**Identity:** $[1]_n$

**Inverse:** Since $\gcd(a, n) = 1$ for every $a \in Z^*_n$ from **Extended-Euclid** $(a, n)$ we obtain $x$ and $y$ such that $ax + ny = 1 \Rightarrow ax \equiv 1 \mod n \Rightarrow x$ is the inverse of $a$. 


Subgroups

- Let \((G, \cdot)\) be a group.
  - \((H, \cdot)\) is a subgroup of \(G\) if \((H, \cdot)\) is a group \(H \subseteq G\)
  - For example, \(H = (\{1,2,4\}, \times)\) is a subgroup of \(\mathbb{Z}_7^*\).

- Lagrange’s theorem:
  If \((G, \cdot)\) is finite and \((H, \cdot)\) is a subgroup of \((G, \cdot)\), then \(|H|\) divides \(|G|\)
  - In our example: \(3|6\).

*Theorem 31.14 (A nonempty closed subset of a finite group is a subgroup)*
If \((S, \oplus)\) is a finite group and \(S'\) is any nonempty subset of \(S\) such that \(a \oplus b \in S'\) for all \(a, b \in S'\), then \((S', \oplus)\) is a subgroup of \((S, \oplus)\).

For example, the set \(\{0, 2, 4, 6\}\) forms a subgroup of \(\mathbb{Z}_8\), since it is nonempty and closed under the operation \(\oplus\) (that is, it is closed under \(+_8\)).
Solving modular linear equations

Solve for the unknown $x$ in the following equation:

$$ax \equiv b \mod n$$

given $a$, $b$ and $n$.

Consider the subgroup of $(\mathbb{Z}_n, +)$, i.e., $\{ a^x : x > 0 \} = \{ ax \mod n : x > 0 \} = \langle a \rangle$. Thus the above equation has a solution if and only if $b \in \langle a \rangle$.

The following procedure computes all solutions of the modular linear equation $ax = b \mod n$.

**MODULAR-LINEAR-EQUATION-SOLVER** $(a, b, n)$

1. $(d, x', y') \leftarrow$ EXTENDED-EUCLID$(a, n)$
2. if $d | b$
3. then $x_0 \leftarrow x' \cdot (b / d) \mod n$
4. for $i = 0$ to $d - 1$
5. do print $(x_0 + i \cdot (n / d)) \mod n$
6. else print “No Solution.”
Solving modular linear equation

\[ 14x \equiv 30 \pmod{100} \]

\[ a=14, \ b=30, \ n=100 \]

Line 1: \((d,x,y) = (2, 7,1)\)

Line 2: \(2 \mid 30\) is true \(\rightarrow\) line 3-5 are executed.

Line 3: \(x_0 = (-7)(15) \pmod{100}\)

\[ = -105- (100 \times -2) \]
\[ = 95 \]

Line 5: \(x_1 = x_0 + i(n/d) \pmod{n}\)

\[ = 95 + 1(100/2) \pmod{100} \]
\[ = 95 + 50 \pmod{100} \]
\[ = 145 \pmod{100} \]
\[ = 145 - (100 \times 1) \]
\[ = 45 \]

answer = 95, 45

\[ 14 \times 95 - (100 \times 13) = 1330 - 1300 = 30 \]

\[ 14 \times 45 - (100 \times 6) = 630 - 600 = 30 \]
Exercise: Find all solutions to the equation $35 \times x \equiv 10 \pmod{50}$

Solution: Here $a = 35$, $b = 10$ and $n = 50$. We know $\gcd(35, 50) = 5$. Thus there are 5 solutions to the given equation.

Since $3 \times 35 + (-2) \times 50 = 5$ we have $x' = 3$. Thus $x_0 = x' \left( \frac{b}{d} \right) \mod n = 3 \times (10/5) \mod 50 = 6$. Other solutions are $x_i = x_0 + i \left( \frac{n}{d} \right)$ [i.e., $x_1 = 16$, $x_2 = 26$, $x_3 = 36$, $x_4 = 46$.]
Modular-Exponentiation\((a, b, n)\)

Solving: \[ a^b \mod n \]

Modular-Exponentiation\((a, b, n)\)
1 c \leftarrow 0
2 d \leftarrow 1
3 let \( \langle b_k, b_{k-1}, \ldots, b_0 \rangle \) be the binary of \( b \)
4 for \( i \leftarrow k \) downto 0
5 \hspace{1em} do c \leftarrow 2c
6 \hspace{1em} d \leftarrow (d \times d) \mod n
7 \hspace{1em} if b_i = 1
8 \hspace{2em} then c \leftarrow c+1
9 \hspace{2em} d \leftarrow (d \times a) \mod n
10 return d
Modular-Exponentiation \((a, b, n)\)

\[7^{560} \mod 561\]

<table>
<thead>
<tr>
<th>i</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>b_i</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>c</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>17</td>
<td>35</td>
<td>70</td>
<td>140</td>
<td>280</td>
<td>560</td>
</tr>
<tr>
<td>d</td>
<td>7</td>
<td>49</td>
<td>157</td>
<td>526</td>
<td>160</td>
<td>241</td>
<td>298</td>
<td>166</td>
<td>67</td>
<td>1</td>
</tr>
</tbody>
</table>

\[a^{2^c} \mod n = (a^c)^2 \mod n,\]

\[a^{2^c+1} \mod n = a.(a^c)^2 \mod n\]

\[C = (a.b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n\]