Cryptography
CS 555

Topic 6: Number Theory Basics
Outline and Readings

• Outline
  – Divisibility, Prime and composite numbers, The Fundamental theorem of arithmetic, Greatest Common Divisor, Modular operation, Congruence relation
  – The Extended Euclidian Algorithm
  – Solving Linear Congruence

• Readings:
  • Katz and Lindell: 7.1.1, 7.1.2
Definition
Given integers $a$ and $b$, with $a \neq 0$, $a$ divides $b$ (denoted $a|b$) if $\exists$ integer $k$, s.t. $b = ak$.
$a$ is called a divisor of $b$, and $b$ a multiple of $a$.

Proposition:
(1) If $a \neq 0$, then $a|0$ and $a|a$. Also, $1|b$ for every $b$
(2) If $a|b$ and $b|c$, then $a|c$.
(3) If $a|b$ and $a|c$, then $a|(sb + tc)$ for all integers $s$ and $t$. 
Divisibility (cont.)

**Theorem (Division algorithm)**
Given integers $a$, $b$ such that $a>0$, $a<b$ then there exist two unique integers $q$ and $r$, $0 \leq r < a$ s.t. $b = aq + r$.

**Proof:**
Uniqueness of $q$ and $r$:
assume $\exists q'$ and $r'$ s.t $b = aq' + r'$, $0 \leq r' < a$, $q'$ integer then $aq + r = aq' + r'$ $\Rightarrow$ $a(q-q')=r'-r$ $\Rightarrow$ $q-q' = (r'-r)/a$ as $0 \leq r,r' < a$ $\Rightarrow$ $-a < (r'-r) < a$ $\Rightarrow$ $-1 < (r'-r)/a < 1$
So $-1 < q-q' < 1$, but $q-q'$ is integer, therefore $q = q'$ and $r = r'$
Definition
An integer $n > 1$ is called a **prime number** if its positive divisors are 1 and $n$.

Definition
Any integer number $n > 1$ that is not prime, is called a **composite number**.

Example
Prime numbers: 2, 3, 5, 7, 11, 13, 17 …
Composite numbers: 4, 6, 25, 900, 17778, …
Decomposition in Product of Primes

**Theorem (Fundamental Theorem of Arithmetic)**
Any integer number \( n > 1 \) can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

\[
n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}
\]

**Example:** \( 84 = 2^2 \cdot 3 \cdot 7 \)
Classroom Discussion Question
(Not a Quiz)

• Are the total number of prime numbers finite or infinite?
Greatest Common Divisor (GCD)

**Definition**
Given integers $a > 0$ and $b > 0$, we define $\text{gcd}(a, b) = c$, the greatest common divisor (GCD), as the greatest number that divides both $a$ and $b$.

**Example**
$\text{gcd}(256, 100) = 4$

**Definition**
Two integers $a > 0$ and $b > 0$ are relatively prime if $\text{gcd}(a, b) = 1$.

**Example**
25 and 128 are relatively prime.
GCD as a Linear Combination

**Theorem**
Given integers $a, b > 0$ and $a > b$, then $d = \gcd(a, b)$ is the least positive integer that can be represented as $ax + by$, $x, y$ integer numbers.

**Proof:** Let $t$ be the smallest positive integer s.t. $t = ax + by$. We have $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \mid t$, so $d \leq t$.
We now show $t \leq d$.
First $t \mid a$; otherwise, $a = tu + r$, $0 < r < t$; $r = a - ut = a - u(ax + by) = a(1-ux) + b(-uy)$, so we found another linear combination and $r < t$. Contradiction.
Similarly $t \mid b$, so $t$ is a common divisor of $a$ and $b$, thus $t \leq \gcd(a, b) = d$. So $t = d$.

**Example**

$\gcd(100, 36) = 4 = 4 \times 100 - 11 \times 36 = 400 - 396$
**Theorem**
Given integers $a$, $b$, $m > 1$. If $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m) = 1$

Proof idea:
$ax + ym = 1 = bz + tm$
Find $u$ and $v$ such that $(ab)u + mv = 1$
GCD and Division

**Theorem**
Given integers $a > 0$, $b$, $q$, $r$, such that $b = aq + r$, then $\text{gcd}(b, a) = \text{gcd}(a, r)$.

**Proof:**
Let $\text{gcd}(b, a) = d$ and $\text{gcd}(a, r) = e$, this means $d \mid b$ and $d \mid a$, so $d \mid b - aq$, so $d \mid r$

Since $\text{gcd}(a, r) = e$, we obtain $d \leq e$.

$e \mid a$ and $e \mid r$, so $e \mid aq + r$, so $e \mid b$, Since $\text{gcd}(b, a) = d$, we obtain $e \leq d$.

Therefore $d = e$
Finding GCD

**Using the Theorem:** Given integers $a > 0$, $b$, $q$, $r$, such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

**Euclidian Algorithm**

Find $\gcd(b, a)$

```plaintext
while $a \neq 0$ do
    $r \leftarrow b \mod a$
    $b \leftarrow a$
    $a \leftarrow r$

return $b$
```
Euclidian Algorithm Example

Find $\gcd(143, 110)$

$143 = 1 \times 110 + 33$

$110 = 3 \times 33 + 11$

$33 = 3 \times 11 + 0$

$\gcd (143, 110) = 11$
Modulo Operation

Definition:

\[ a \mod n = r \iff \exists q \text{ s.t. } a = q \times n + r \]

where \(0 \leq r \leq n - 1\)

Example:

7 mod 3 = 1
-7 mod 3 = 2
Congruence Relation

**Definition:** Let $a$, $b$, $n$ be integers with $n > 0$, we say that \(a \equiv b \pmod{n}\),

if $a - b$ is a multiple of $n$.

**Properties:** \(a \equiv b \pmod{n}\)

- if and only if \(n | (a - b)\)
- if and only if \(n | (b - a)\)
- if and only if \(a = b + k \cdot n\) for some integer $k$
- if and only if \(b = a + k \cdot n\) for some integer $k$

**E.g.,** \(32 \equiv 7 \pmod{5}\), \(-12 \equiv 37 \pmod{7}\), \(17 \equiv 17 \pmod{13}\)
Properties of the Congruence Relation

**Proposition:** Let a, b, c, n be integers with n > 0

1. \( a \equiv 0 \pmod{n} \) if and only if \( n \mid a \)
2. \( a \equiv a \pmod{n} \)
3. \( a \equiv b \pmod{n} \) if and only if \( b \equiv a \pmod{n} \)
4. if \( a \equiv b \) and \( b \equiv c \pmod{n} \), then \( a \equiv c \pmod{n} \)

**Corollary:** Congruence modulo n is an equivalence relation.

Every integer is congruent to exactly one number in \( \{0, 1, 2, \ldots, n-1\} \) modulo n.
Equivalence Relation

**Definition**
A binary relation $R$ over a set $Y$ is a subset of $Y \times Y$. We denote a relation $(a,b) \in R$ as $aRb$.

• example of relations over integers?

**Definition**
A relation is an equivalence relation on a set $Y$, if $R$ is

- **Reflexive**: $aRa$ for all $a \in R$
- **Symmetric**: for all $a, b \in R$, $aRb \Rightarrow bRa$
- **Transitive**: for all $a, b, c \in R$, $aRb$ and $bRc \Rightarrow aRc$

**Example**
"=" is an equivalence relation on the set of integers
More Properties of the Congruence Relation

**Proposition:** Let $a$, $b$, $c$, $n$ be integers with $n > 0$

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

- $a + c \equiv b + d \pmod{n}$,
- $a - c \equiv b - d \pmod{n}$,
- $a \cdot c \equiv b \cdot d \pmod{n}$

E.g., $5 \equiv 12 \pmod{7}$ and $3 \equiv -4 \pmod{7}$, then, ...
Multiplicative Inverse

**Definition**: Given integers $n>0$, $a$, $b$, we say that $b$ is a **multiplicative inverse of $a$ modulo $n$** if $ab \equiv 1 \pmod{n}$.

**Proposition**: Given integers $n>0$ and $a$, then $a$ has a multiplicative inverse modulo $n$ if and only if $a$ and $n$ are relatively prime.
Towards Extended Euclidian Algorithm

- **Theorem:** Given integers $a, b > 0$, then $d = \text{gcd}(a,b)$ is the least positive integer that can be represented as $ax + by$, $x, y$ integer numbers.

- How to find such $x$ and $y$?
The Extended Euclidian Algorithm

First computes

\[ b = q_1 a + r_1 \]
\[ a = q_2 r_1 + r_2 \]
\[ r_1 = q_3 r_2 + r_3 \]
\[ \vdots \]
\[ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \]
\[ r_{k-2} = q_k r_{k-1} \]

Then computes

\[ x_0 = 0 \]
\[ x_1 = 1 \]
\[ x_2 = -q_1 x_1 + x_0 \]
\[ \vdots \]
\[ x_k = -q_{k-1} x_{k-1} + x_{k-2} \]

And

\[ y_0 = 1 \]
\[ y_1 = 0 \]
\[ y_2 = -q_1 y_1 + y_0 \]
\[ \vdots \]
\[ y_k = -q_{k-1} y_{k-1} + y_{k-2} \]

And

We have \( ax_k + by_k = r_{k-1} = \gcd(a, b) \)
Extended Euclidian Algorithm

Extended_Euclidian (a,b)

\[ x=1; \ y=0; \ d=a; \ r=0; \ s=1; \ t=b; \]

while (t>0) {

\[ q = \lfloor \frac{d}{t} \rfloor; \]

\[ u=x-qr; \ v=y-qs; \ w=d-qt; \]

\[ x=r; \quad y=s; \quad d=t; \]

\[ r=u; \quad s=v; \quad t=w; \]

}

return (d, x, y)

end

Invariants:

\[ ax + by = d \]
\[ ar + bs = t \]
Another Way

Find gcd(143, 111)

\begin{align*}
143 &= 1 \times 111 + 32 \\
111 &= 3 \times 32 + 15 \\
32 &= 2 \times 15 + 2 \\
15 &= 7 \times 2 + 1 \\
\text{gcd (143, 111)} &= 1 \\
\end{align*}
Linear Equation Modulo $n$

If $\gcd(a, n) = 1$, the equation

$$ax \equiv 1 \mod n$$

has a unique solution, $0 < x < n$. This solution is often represented as $a^{-1} \mod n$.

**Proof:** if $ax_1 \equiv 1 \pmod{n}$ and $ax_2 \equiv 1 \pmod{n}$, then $a(x_1-x_2) \equiv 0 \pmod{n}$, then $n \mid a(x_1-x_2)$, then $n \mid (x_1-x_2)$, then $x_1-x_2=0$.

How to compute $a^{-1} \mod n$?
Examples

Example 1:
• Observe that $3 \cdot 5 \equiv 1 \pmod{7}$.
• Let us try to solve $3 \cdot x + 4 \equiv 3 \pmod{7}$.
• Subtracts 4 from both side, $3 \cdot x \equiv -1 \pmod{7}$.
• We know that $-1 \equiv 6 \pmod{7}$.
• Thus $3 \cdot x \equiv 6 \pmod{7}$.
• Multiply both side by 5, $3 \cdot 5 \cdot x \equiv 5 \cdot 6 \pmod{7}$.
• Thus, $x \equiv 1 \cdot x \equiv 3 \cdot 5 \cdot x \equiv 5 \cdot 6 \equiv 30 \equiv 2 \pmod{7}$.
• Thus, any $x$ that satisfies $3 \cdot x + 4 \equiv 3 \pmod{7}$ must satisfy $x \equiv 2 \pmod{7}$ and vice versa.

Question: To solve that $2x \equiv 2 \pmod{4}$.
Is the solution $x \equiv 1 \pmod{4}$?
Linear Equation Modulo (cont.)

To solve the equation

\[ ax \equiv b \mod n \]

When \( \gcd(a,n)=1 \), compute \( x = a^{-1} b \mod n \).

When \( \gcd(a,n) = d > 1 \), do the following

- If \( d \) does not divide \( b \), there is no solution.
- Assume \( d | b \). Solve the new congruence, get \( x_0 \)

\[ \left(\frac{a}{d}\right)x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \]

- The solutions of the original congruence are \( x_0, x_0+(n/d), x_0+2(n/d), \ldots, x_0+(d-1)(n/d) \pmod{n} \).
Solving Linear Congruences

Theorem:

• Let $a$, $n$, $z$, $z'$ be integers with $n>0$. If $\gcd(a,n)=1$, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n}$.

• More generally, if $d:=\gcd(a,n)$, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.

Example:

• $5 \cdot 2 \equiv 5 \cdot -4 \pmod{6}$
• $3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$
Coming Attractions …

- More on secure encryption
- Reading: Katz & Lindell: 3.4, 3.5, 3.6