Announcements

• HW8 due today
• HW9 up on course webpage. Due on Thursday, 4/23.
Agenda

• Last time:
  – Practical constructions of block ciphers (6.2)
    • Feistel, AES, DES
  – Please read (6.2.3) on your own on Differential and Linear Cryptanalysis

• This time:
  – Practical constructions of CRHF (6.3)
  – Number Theory (8.1)
Posted lecture notes include only the Number Theory material.
Modular Arithmetic

Definition of modulo:
We say that two integers $a, b$ are congruent modulo $p$ denoted by
$$a \equiv b \mod p$$
If
$$p \mid (a - b)$$
(i.e. $p$ divides $(a - b)$).
Modular Arithmetic

Examples: All of the following are true

\[ 2 \equiv 15 \mod 13 \]
\[ 28 \equiv 15 \mod 13 \]
\[ 41 \equiv 15 \mod 13 \]
\[ -11 \equiv 15 \mod 13 \]
Modular Arithmetic

Operation: addition mod p
Regular addition, take modulo p.

Example: $8 + 10 \mod 13 \equiv 18 \mod 13 \equiv 5 \mod 13$. 
Properties of Addition mod $p$

Consider the set $\mathbb{Z}_p$ of integers $\{0,1,...,p-1\}$ and the operation addition mod $p$.

• Closure: Adding two numbers in $\mathbb{Z}_p$ and taking mod $p$ yields a number in $\mathbb{Z}_p$.

• Identity: For every $a \in \mathbb{Z}_p$, $[0 + a] \mod p \equiv a \mod p$.

• Inverse: For every $a \in \mathbb{Z}_p$, there exists a $b \in \mathbb{Z}_p$ such that $a + b \equiv 0 \mod p$.
  – $b$ is simply the negation of $a$ ($b = -a$).
  – Note that using the property of inverse, we can do subtraction. We define $c - d \mod p$ to be equivalent to $c + (-d) \mod p$.

• Associativity: For every $a, b, c \in \mathbb{Z}_p$:
  $$(a + b) + c = a + (b + c) \mod p.$$  

$\mathbb{Z}_p$ is a group with respect to addition!
Definition of a Group

A group is a set $G$ along with a binary operation $\circ$ for which the following conditions hold:

- **Closure**: For all $g, h \in G$, $g \circ h \in G$.
- **Identity**: There exists an identity $e \in G$ such that for all $g \in G$, $e \circ g = g = g \circ e$.
- **Inverse**: For all $g \in G$ there exists an element $h \in G$ such that $g \circ h = e = h \circ g$. Such an $h$ is called an inverse of $g$.
- **Associativity**: For all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

When $G$ has a finite number of elements, we say $G$ is finite and let $|G|$ denote the order of the group.
Abelian Group

A group $G$ with operation $\circ$ is abelian if the following holds:

• Commutativity: For all $g, h \in G$, $g \circ h = h \circ g$.

We will always deal with finite, abelian groups.
Other groups over the integers

• We will be interested mainly in multiplicative groups over the integers, since there are computational problems believed to be hard over such groups.
  – Such hard problems are the basis of number-theoretic cryptography.

• Group operation is multiplication mod $p$, instead of addition mod $p$. 
Multiplication mod p

Example:
\[ 3 \cdot 8 \mod 13 \equiv 24 \mod 13 \equiv 11 \mod 13. \]
Multiplicative Groups

Is $\mathbb{Z}_p$ a group with respect to multiplication mod $p$?

• Closure—YES
• Identity—YES (1 instead of 0)
• Associativity—YES
• Inverse—NO
  
  – 0 has no inverse since there is no integer $a$ such that $0 \cdot a \equiv 1 \text{ mod } p$. 

For $p$ prime, define $\mathbb{Z}^*_p = \{1, \ldots, p - 1\}$ with operation multiplication mod $p$.

We will see that $\mathbb{Z}^*_p$ is indeed a multiplicative group!

To prove that $\mathbb{Z}^*_p$ is a multiplicative group, it is sufficient to prove that every element has a multiplicative inverse (since we have already argued that all other properties of a group are satisfied).

This is highly non-trivial, we will see how to prove it using the Euclidean Algorithm.
Inefficient method of finding inverses mod $p$

Example: Multiplicative inverse of $9 \mod 11$.

9 · 1 ≡ 9 $mod$ 11
9 · 2 ≡ 18 ≡ 7 $mod$ 11
9 · 3 ≡ 27 ≡ 5 $mod$ 11
9 · 4 ≡ 36 ≡ 3 $mod$ 11
9 · 5 ≡ 45 ≡ 1 $mod$ 11

What is the time complexity?
Brute force search. In the worst case must try all 10 numbers in $\mathbb{Z}^*_{11}$ to find the inverse.

This is exponential time! Why? Inputs to the algorithm are $(9,11)$. The length of the input is the length of the binary representation of $(9,11)$. This means that input size is approx. $\log_2 11$ while the runtime is approx. $2^{\log_2 11} = 11$. The runtime is exponential in the input length.

Fortunately, there is an efficient algorithm for computing inverses.
Euclidean Algorithm

Theorem: Let $a, p$ be positive integers. Then there exist integers $X, Y$ such that $Xa + Yb = \gcd(a, p)$.

Given $a, p$, the Euclidean algorithm can be used to compute $\gcd(a, p)$ in polynomial time. The extended Euclidean algorithm can be used to compute $X, Y$ in polynomial time.

***We will see the extended Euclidean algorithm next class***
Proving $\mathbb{Z}^*_p$ is a multiplicative group

In the following we prove that every element in $\mathbb{Z}^*_p$ has a multiplicative inverse when $p$ is prime. This is sufficient to prove that $\mathbb{Z}^*_p$ is a multiplicative group.

Proof. Let $a \in \mathbb{Z}^*_p$. Then $\gcd(a, p) = 1$, since $p$ is prime. By the Euclidean Algorithm, we can find integers $X, Y$ such that $aX + pY = \gcd(a, p) = 1$.

Rearranging terms, we get that $pY = (aX - 1)$ and so $p \mid (aX - 1)$. By definition of modulo, this implies that $aX \equiv 1 \mod p$.

By definition of inverse, this implies that $X$ is the multiplicative inverse of $a$.

Note: By above, the extended Euclidean algorithm gives us a way to compute the multiplicative inverse in polynomial time.