Exercise Notes - Basic Number Theory

Lecture By Danny Bickson - 1.12.03
Based on huji lecture notes from 2001 of security course by
Prof. Dahlia Malkhi and Dr. Shlomo Kipnis

In this lecture, we review some of the basics of number theory that will be used in the following lectures.

Definitions

Additive Group

Consider the following Set: $Z_p = \{0,1,2, \dots , p-1\}$ with the operation 'addition mod p' (to be denoted by +). The set Z_p with the + operation is an **Additive Group** because it has the following properties:

- It is **closed** – for every ***a*** and ***b*** in Z_p, ***a+b*** is also a member of that set.
  Formally: $\forall (a \in Z_p), \forall (b \in Z_p) : (a+b) \in Z_p$.
- It has a "**Zero**" element – there is an element ***z*** in Z_p, that for each member ***a*** in Z_p, performing the operation + on those 2 numbers will result in ***a***.
  Formally: $\exists (z \in Z_p): \forall (a \in Z_p)\ a+z = a$.
- Every element has an **opposite** element – for every element ***a*** in Z_p, there exists an element ***b*** in Z_p, so that ***a+b=0***.
  Formally: $\forall (a \in Z_p) : \exists (b \in Z_p) : a+b = 0$.
- **Associativity** – for every 3 elements in Zp, no matter in which order the + operation is performed, it always yields the same result.
  Formally: $\forall (a \in Z_p), \forall (b \in Z_p), \forall (c \in Z_p) : (a+b)+c = a+(b+c)$.

Multiplicative Group

Let us look at the set $Zp^* = \{1,2,3,\dots, p-1\}$ with the operation 'multiplication mod p' (to be denoted by *). Similarly, this set is called a **Multiplicative Group** if it has the following properties:

- It is **closed** – for every ***a*** and ***b*** in Z_p, **(a*b)** is also a member of that set.
  Formally: $\forall (a \in Z_p), \forall (b \in Z_p) : (a*b) \in Z_p$.
- It has a "**Unity**" element – there is an element ***u*** in Z_p, that for each member ***a*** in Z_p, performing the operation * on those 2 numbers will result in ***a***.
  Formally: $\exists (u \in Z_p)\ \forall (a \in Z_p) : a*u = a$.
- Every element has an **inverse** element (denoted as a^{-1}) – for every element ***a*** in Z_p, there exists an element ***b*** in Z_p, so that **a*b =1**.
  Formally: $\forall (a \in Z_p)\ \exists (b \in Z_p) : a*b = 1$.
- **Associativity** – for every 3 elements in Z_p, no matter in which order the * operation is performed, it always yields the same result.
  Formally: $\forall (a \in Z_p), \forall (b \in Z_p), \forall (c \in Z_p) : (a*b)*c = a*(b*c)$.

Field

A set is a **Field** if it is both an Additive Group and a Multiplicative Group, and it has the following properties:

- **Commutativity** – $\forall$ ($a \in Z_p$) $\forall$($b \in Z_p$) : a+b = b+a and a*b = b*a
- **Distributivity** – $\forall$ ($a \in Z_p$) , $\forall$($b \in Z_p$),$\forall$ ($c \in Z_p$) : a*(b+c) = a*b + a*c)

An example of a Field is the set of integers modulo a **prime p**: the group (Z_p, +,*,0,1) where $Z_p = \{0,1,2, \dots , p-1\}$.

Properties

If p is prime, then the set $Z_p^* = \{1, 2, \dots, p-1\}$ with the operation multiplication modulo p defined on it, has the following properties:

Zp* is Cyclic

Zp* is Cyclic, meaning it has a **generator.** A generator is an element g of Z_p^* so that every element ***i*** of Z_p^*, is the result of raising ***g*** to the ***j***-th power, where $1 \le j \le p-1$. Formally: $Z_p^* = \{g^i : i = 1, 2, \dots , p-1\} = \{g^1, g^2, g^3, \dots, g^{p-1}\}$.

A cyclic group may have more than one generator.

Let us consider the following example:
For $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ the element 3 is a generator, since:

$3^1 = 3 \pmod 7$ $\quad$ $3^4 = 4 \pmod 7$
$3^2 = 2 \pmod 7$ $\quad$ $3^5 = 5 \pmod 7$
$3^3 = 6 \pmod 7$ $\quad$ $3^6 = 1 \pmod 7$

Fermat's Little Theorem

If ***p*** is prime, then for each element ***a*** in the set Z_p^* : $a^{p-1} = 1 \pmod p$.

Let us prove this theorem: ***p*** is prime, and therefore ***a*** and ***p*** are relatively prime (The term 'relatively prime' means that they do not share any common factor other than 1.) In this case, ***a*** has an inverse, and therefore: $a*b = a*c \pmod p$ implies $b = c \pmod p$.

Since ***a*** and ***p*** are relatively prime, there is no ***k*** in Z_p^* for which $a*k=p \pmod p$. This is why the following multiples $a \pmod p$, $2a \pmod p$, …, $(p-1)a \pmod p$ give all the residues ***1, 2, …, p-1*** permuted:

$$a * 2a * \dots * (p-1)a = 1 * 2 * \dots * (p-1) \pmod p \quad \Rightarrow$$

$$a^{p-1} * [1 * 2 * \dots * (p-1)] = [1 * 2 * \dots * (p-1)] \bmod p$$

Since Z_p^* is a multiplicative group, we can remove $[1*2* \dots * (p-1)]$ from both sides of the equation to obtain: $a^{p-1} = 1 \pmod p$

From this theorem, we can easily deduce that:

1. $a^p = a \pmod p$ because $a \cdot a^{p-1} = a \cdot 1 = a$
2. $a^{-1} = a^{p-2} \pmod p$ because $a \cdot a^{p-2} = a^{p-1} = 1$

The second deduction gives us a way to calculate the inverse of an element (a^{-1} is the inverse of ***a***) in $O(\log p)$ steps, in comparison to a search that takes $O(p)$ steps. This is possible because a^{p-2} can be calculated in $O(\log p)$ steps.

Properties regarding order(a)

The **order of *a*,** denoted as ***order (a)***, is the smallest ***b*** that satisfies the equation $a^b = 1$.
For example: ***order (1) = 1***.

1. For every ***a*** in Z_p*, ***order (a)*** is a divisor of ***p-1*** (***order (a)*** divides ***p-1***).
   Formally: $\forall a \in Z^*_p$: ***order (a) | p-1***.
2. An element ***a*** of Z_p* is square (meaning there exists such a ***b*** in Z_p* so that $a = b^2$)
   if and only if $a^{(p-1)/2} = 1 \pmod{p}$.
   Formally: $\exists(b \in Zp)$, $a = b^2 \Leftrightarrow a^{(p-1)/2} = 1 \pmod{p}$.
3. The equation $g^x \equiv g^y \pmod{p}$ is true if and only if $x = y \pmod{(p-1)}$. Where g is a generator.
   Formally: $g^x \equiv g^y \pmod{p} \Leftrightarrow x = y \pmod{(p-1)}$.
   In the general case: $a^x \equiv a^y \pmod{p} \Leftrightarrow x = y \pmod{order(a)}$.