The multiplicative group modulo p: a primer for dummies

Giuseppe Bianchi

What is a group?

- **$(G, \circ)$**
  - G = set of elements (group members)
  - $\circ$ = operation (group operation)
- **4 properties:**
  - **Closure**: for any g_1, g_2:
    $g_x = g_1 \circ g_2$ must be a group member
  - **Identity**: there is a group member I such that
    $g \circ I = I \circ g = g$
  - **Inverse**: for any g, there is g^{-1} such that
    $g \circ g^{-1} = I$
  - **Associativity**: for any g_1, g_2, g_3:
    $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$
- **If also commutative → Abelian Group**

The Zp* group

- ➔ **multiplicative group modulo prime p**
  - ⇨ Set of p-1 elements {1,2,…, p-1} → **finite group**
  - ⇨ Multiplicative = we only care about multiplications mod p!!
    - →Forget the sum, here (otherwise you would have a field $\mathcal{F}$p)

- ➔ **Group properties:**
  - ⇨ Closure: obvious
  - ⇨ Identity: obvious
  - ⇨ Associativity: obvious
  - ⇨ Commutativity → Abelian group → also obvious
  - ⇨ **What about inverse???**
    - →If mod N, then x has inverse if and only if gcd(x,N)=1
    - →If N=p=prime, then all elements have inverse!
      - » Note that 0 is not an element of the group!

Example: Z_{11}^*

- ➔**Elements: {1,2,3,4,5,6,7,8,9,10}**
- ➔**Inverses:**
  - ⇨1→1
  - ⇨2→6 6→2
  - ⇨3→4 4→3
  - ⇨5→9 9→5
  - ⇨7→8 8→7
  - ⇨10→10 (analogous to -1)
- ➔**How to compute inverses for large groups?**
  - ⇨Extended euclidean algorithm

Back to multiplicative groups: exponentiation

- ➔ $x^k = x \circ x \circ x \circ \ldots \circ x$ (k times)
- ➔ **Generator of group of order m**
  - ⇨ exists g such that $\{g^0, g^1, \ldots g^{m-1}\}$ = all m group members
- ➔ **Prime-order group:**
  - ⇨ If m is prime, any member is generator
    - → Except the identity
- ➔ **Is Zp* a prime order group? NO!!**
  - ⇨ $|Zp^*| = p-1$ CANNOT be prime
    - → p is prime → p-1 is even

Example: Z_{11}^*

- **Elements: {1,2,3,4,5,6,7,8,9,10}**
- **Generators? $\{g^1, g^2, g^3, \dots, g^{10}\}$=?**
  - g=2 → {2,4,8,5,10,9,7,3,6,1} OK, generator
  - g=3 → {3,9,5,4,1,3,9,5,4,1} NO! Subgroup order 5
  - g=4 → {4,5,9,3,1,4,5,9,3,1} NO! Subgroup order 5
  - g=5 → {5,3,4,9,1,5,3,4,9,1} NO! Subgroup order 5
  - g=6 → {6,3,7,9,10,5,8,4,2,1} OK, generator
  - g=7 → {7,5,2,3,10,4,6,9,8,1} OK, generator
  - g=8 → {8,9,6,4,10,3,2,5,7,1} OK, generator
  - g=9 → {9,4,3,5,1,9,4,3,5,1} NO! Subgroup order 5
  - g=10→ {10,1,10,1,10,1,10,1,10,1} NO! Subgroup order 2
- **Take home:**
  - either g is a generator
  - Or generates a SUBGROUP → order = factor of |G|
  - **And Zp* as well as all subgroups are cyclic!**

Strong primes

- **Prime p such that**
  p = 2q +1
  being q also prime!

- **Order of Zp*: p-1**
  p-1 = 2q

- **Hence, any member x (except 1 and p-1) either**
  1. Generates the whole group, or
  2. Generates subgroup of prime order q
- **Both large if p and q large!**
  - Note the difference when Zp* uses «just» a large prime p: p-1 can factor down in small numbers!

Quadratic residue subgroup

- ➔ $x \in Z_p^*$ **is a quadratic residue if it admits square root in** Z_p^*
  - ⇨ i.e., there exists a such that $a^2 \bmod p = x$

- ➔ **QR form subgroup of order** $\frac{p-1}{2}$
  - ⇨ 2➔1 mapping: $\begin{matrix} x \searrow \\ p\text{-}x \nearrow \end{matrix} x^2$ Indeed, $(p-x)^2 \bmod p = p^2 - 2px + x^2 \bmod p = x^2$

- ➔ **QR test: legendre symbol**
  - ⇨ $a \in QR$ if $a^{\frac{p-1}{2}} \bmod p = 1$ (otherwise -1)

- ➔ **Example for** Z_{11}^*: $QR_{11} = \{1, 3, 4, 5, 9\}$
  - ⇨ If p strong prime, QR_p has prime order q!