Class129: Finite Fields

Virendra Sule

The group of units $\mathbb{F}_q^*$

The set of nonzero elements of $\mathbb{F}_q$ forms a group denoted $\mathbb{F}_q^*$. Clealry $|\mathbb{F}_q^*| = q - 1$. Hence for any element a in $\mathbb{F}_q^*$

$$\operatorname{ord} a | (q-1)$$

Question. Does an element a exist in $\mathbb{F}_q$ of order d if $d|(q-1)$? This is a fundamental structure theorem about finite fields. It turns out that for every divisor d of $(q-1)$ there is an element of $\operatorname{ord} d$. This is because $\mathbb{F}_q^*$ is a cyclic group and can be generated by single elements called *primitive* elements. Hence elements of order $(q-1)$ exist called primitive elements.

Order of a power

Question. Consider a in $\mathbb{F}_q^*$ of order d. For $1 \leq e \leq d$ what is the order of a^e? Take $1 < e < d$.

- The set $\{1, a, a^2, \ldots, a^{(d-1)}\}$ is a cyclic group of d distinct elements. Hence $\operatorname{ord} a^e | d$. Let $r = \operatorname{ord} a^e$. Then r is smallest such that $a^{er} = 1$. Hence $er \geq d$ as all powers upto $d - 1$ are distinct.
- If $er = qd + r_0$, then $0 \leq r_0 < d$. Hence $a^{qd+r_0} = 1$ implies $r_0 = 0$.
- Let $d = gd_1$, $e = ge_1$ where $g = \gcd(e, d)$. Hence $er = gd_1e_1r_1$ where r_1 is smallest. Hence $r_1 = 1$. This proves

$$r = \operatorname{ord} a^e = d_1 = \frac{d}{\gcd(e, d)}$$

- Let $d|(q-1)$ and let there exist an element a of order d. Hence the number $\psi(d)$ of elements of order d is assumed positive, $\psi(d) > 0$.
- $\{1, a, a^2, \ldots, a^{(d-1)}\}$ are all distinct elements and each satisfies the equation $X^d - 1 = 0$. But this equation has at most d roots. Hence this set is the set of all roots of this equation and all are powers of a.
- By the previous formula, $\operatorname{ord}(a^e) = d/\gcd(e, d)$. Hence any of these elements have order d iff $\gcd(e, d) = 1$. Hence $\psi(d) = \phi(d)$.

- But for each distinct divisor of d of $(q-1)$ the sum of all elements of order d must be equal to all elements of $\mathbb{F}_q^*$,

$$\begin{aligned} (q-1) &= \textstyle\sum_{d|(q-1)} \psi(d) \\ &= \textstyle\sum_{d|(q-1)} \phi(d) \end{aligned}$$

Hence if for some d, $\psi(d) = 0$ then the $(q-1)$ is strictly less than the RHS which shows

$$(q-1) < \sum_{d|(q-1)} \phi(d)$$

This violates the identity for the function ϕ discussed previously

$$\sum_{d|n} \phi(d) = n$$

Structure of $\mathbb{F}_q^*$ cont...

- Hence it follows that $\psi(d) > 0$ for any divisor d of $(q-1)$. In particular for $d = (q-1)$. Hence primitive elements exist in $\mathbb{F}_q^*$.
- $\mathbb{F}_q^*$ is the cyclic group C_{q-1} .
- For every divisor d of $(q-1)$ there is an element in $\mathbb{F}_q^*$ of order d and a subgroup C_d. This shows that even if all subfields $\mathbb{F}_{\tilde{q}}$ of $\mathbb{F}_q$ have cyclic groups of units $\mathbb{F}_{\tilde{q}}^* \subset \mathbb{F}_q^*$ there are cyclic groups which are not unit groups of subfields.
- As an example consider $\mathbb{F}_{2^6}$. The subfields of $\mathbb{F}_{2^6}$ are $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$ their unit groups are C_4, C_8. Since $|\mathbb{F}_{2^6}^*| = 2^6 - 1 = 63 = 3^2 * 7$. There is cyclic group C_9 which is not a group of a finite field.

- Polynomial representation. If $\mathbb{F}_{p^m}$ is obtained as $\mathbb{F}_p[X]/f(X)$ by the *generating polynomial* $f(X)$, which is irreducible and θ denotes its root. Then

$$\mathbb{F}_{p^m} = \{\sum_{i=1}^{m} a_i\theta^i, a_i \in \mathbb{F}_p\}$$

This is called polynomial representation of $\mathbb{F}_{p^m}$ in the basis $\{1, \theta, \ldots, \theta^{(m-1)}\}$.

- Order computation. Let n denote the order of the group G which in this case is $\mathbb{F}_q*$ and the order of G is $n = (q-1)$. Let

$$n = \prod_{i=1}^{i=m} p_i^{m_i}$$

be the prime factorization of n.

- If a is an arbitrary element, then

$$\text{ord } a = \text{smallest } k_i \text{ such that } a^{\prod_{i=1}^{m} p^{k_i}} = 1$$

  Hence order of an element can be searched by raising a to the powers $\prod p_i^{k_i}$ successively.

- Example. Find order of 3 in $\mathbb{F}_{37}$. $n = 36 = 2^2 * 3^2$. Compute

$$3 \neq 1, 3^{2^2} \neq 1 \mod 37, 3^{2^2*3} = 10 \mod 37, 3^{2^2*3^2} = 1 \mod 37$$

- In extension field $\mathbb{F}_{p^m}$, a is given as a polynomial in θ a root of the generating polynomial. Compute the prime factorization of $n = p^m - 1$ and use above procedure. (Note: the problem of computing order of a in a group G without knowing prime factorization of the order of G is a hard problem).

Exponentiation in a group

- If $a \in G$ is given and an exponent $x < \operatorname{ord} G$ is given. The problem of computing a^x in G is called an exponentiation problem.
- For example find θ^{60} in $\mathbb{F}_{2^6}$ with generating polynomial $X^6 + X + 1$.
- Expand in binary

  $$60 = 1.2^5 + 1.2^4 + 1.2^3 + 1.2^2$$

  Then
  $$\theta^{60} = (\theta^{2^5})(\theta^{2^4})(\theta^{2^3})(\theta^{2^2})$$

  Hence by repeated squaring of θ the large power can be computed efficiently.
- Exponentiation is a polynomial time problem in length of the exponent.

Complete the previous example. It requires computation of powers upto 2^5. Each of these are further computed by binary expansion of the power and using previous computations.

- $\theta^{2^3} = \theta^6\theta^2 = (\theta+1)\theta^2 = \theta^3 + \theta^2$
- $\theta^{2^4} = \theta^{(8+8)} = (\theta^{2^3})^2 = (\theta^3)^2 + \theta^4 = (\theta+1) + \theta^4$
- $$\begin{aligned} \theta^{2^5} &= \theta^{(16+16)} \\ &= (\theta^{16})^2 \\ &= (\theta^4+\theta+1)^2 \\ &= \theta^8+\theta^2+1 \\ &= (\theta+1)\theta^2+\theta^2+1 \\ &= (\theta^2)(\theta)+1 = \theta^3+1 \end{aligned}$$
- Compute product of all powers required for θ^{60}