T-79.5501 Cryptology
Additional material
September 27, 2005

1 Structure of Finite Fields

This section contains complementary material to Section 5.2.3 of the text-book. It is not entirely self-contained but must be studied in companion with the text-book. For the used notation we refer to the text-book. We also use the same numbering of the theorems whenever applicable. The new theorems and fact are marked by an asterisk (*). We start by sketching a proof of Theorem 5.4.
For a finite multiplicative group G, define the *order* of an element $g \in G$ to be the smallest positive integer m such that $g^m = 1$. Similarily, in an additive group G, the *order* of the element $g \in G$ is the smallest positive integer m such that $mg = 0$, where 0 is the neutral element of addition. An example of a finite additive group is a group formed by the points on an elliptic curve to be discussed later. For simplicity, we shall use the multiplicative notation in the rest of this section.

Theorem 5.4. (Lagrange) Suppose $(G, \cdot)$ is a multiplicative group of order n, and $g \in G$. Then the order of g divides n.

Proof. Denote by r the order of g, and consider the subset of G formed by the r distinct powers of g. We denote it by H. Thus $H = \{1, g, g^2, \dots, g^{r-1}\}$. It is straightforward to verify that H is a subgroup of G. Then we can define a relation in G by setting

$$f' \sim f \Leftrightarrow f' \in fH = \{f, fg, \dots, fg^{r-1}\}.$$

This relation is reflexive, symmetric, and transitive, hence it is an equivalence relation, and therefore, divides the elements of G into disjoint equivalence classes which can be given as follows fH, $f \in G$. Clearly, $|fH| = r$, for all $f \in G$. Consequently, r divides the number $|G|$ of all elements in G.

$\square$

Corollary 5.5 If $b \in \mathbb{Z}_n{}^*$ then $b^{\phi(n)} \equiv 1 (\mathrm{mod} n)$.

Proof. Recall that

$$\mathbb{Z}_n{}^* = \{a \in \mathbb{Z}_n \,|\, gcd(a, n) = 1\}$$

is a multiplicative group. The Euler ϕ-function is defined as

$$\phi(n) = |\{x \in \mathbb{Z} \,|\, 0 < x < n,\ \gcd(x, n) = 1\}|,$$

for a positive integer n. Thus $|\mathbb{Z}_n{}^*| = \phi(n)$. Let $b \in \mathbb{Z}_n{}^*$. By Theorem 5.4 the order r of b divides $\phi(n)$. Since $b^r \equiv 1 (\mathrm{mod} n)$, the claim follows.

$\square$

Corollary*. (Euler's theorem.) Let $\mathbb{F}$ be a finite field, which has q elements, and let $b \in \mathbb{F}^*$. Then the order of b divides $q-1$ and $b^{q-1} = 1$.

Proof. $(\mathbb{F}^*, \cdot)$ is a multiplicative group with $q-1$ elements.

$\square$

Corollary 5.6 (Fermat) Suppose p is prime and $b \in \mathbb{Z}_p$. Then $b^p \equiv b(\mathrm{mod} p)$.

Proof. $\mathbb{Z}_p$ is a finite field with p elements. For $b = 0$, the congruence holds. If $b \neq 0$, then $b \in {\mathbb{Z}_p}^*$, and the claim follows from Euler's theorem.

$\square$

Proposition 1* Suppose G is a finite group, and $b \in G$. Then the order of b divides every integer such that $b^r = 1$.

Proof. Let d be the order of b. Hence $d \leq r$. If r is divided by d, let t be the remainder, that is, we have the equality $r = d \times s + t$, withe some s, where $0 \leq t < d$. Then

$$1 = b^r = b^{ds+t} = (b^d)^s b^t = b^t.$$

Since t is strictly less than d, this is possible only if $t = 0$.

$\square$

Proposition 2* Suppose G is a finite group and $b \in G$ has order equal to r. Let k be a positive integer, and consider an element $a = b^k \in G$. Then the order of $a = b^k$ is equal to

$$\frac{r}{\gcd(k, r)}.$$

Proof. Since

$$(b^k)^{\frac{r}{\gcd(k,r)}} = (b^r)^{\frac{k}{\gcd(k,r)}} = 1,$$

it follows from Proposition 1 that the order of $a = b^k$ divides the integer $\frac{r}{\gcd(k,r)}$. To prove the converse, denote the order of a by t. Then

$$1 = (b^k)^t = b^{k \times t}$$

hence r divides $k \times t$. Then it must be that $\frac{r}{\gcd(k,r)}$ divides t, which is the order of $a = b^k$.

$\square$

For positive integers k, n, we denote $k|n$ if k divides n.

Proposition 3* For any positive integer n,

$$\sum_{k|n} \phi(k) = n,$$

where ϕ is the Euler phi-function.

Proof. Let integer d be such that $d|n$, and denote

$$A_d = \{r \mid 1 \leq r \leq n,\, \gcd(r,n) = d\},$$

or what is the same,

$$A_d = \{r \mid r = \ell \times d,\, 1 \leq \ell \leq \frac{n}{d},\, \gcd(\ell, \frac{n}{d}) = 1\}.$$

Hence it follows that $|A_d| = \phi(\frac{n}{d})$. On the other hand, we have that $A_d \cap A_{d'} = \emptyset$, if $d \neq d'$. Also,

$$\bigcup_{d|n} A_d = \{r \mid 1 \leq r \leq n\}.$$

It follows that

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{\frac{n}{d}|n} \phi(\frac{n}{d}) = \sum_{k|n} \phi(k).$$

□

Proposition 4* Suppose that $\mathbb{F}$ is a finite field of q elements. Let d be a divisor of $q-1$. Then there are $\phi(d)$ elements in $\mathbb{F}$ with order equal to d.

Proof. Let $a \in \mathbb{F}^*$ such that the order of a is equal to d. Then $d|(q-1)$. Denote

$$B_d = \{x \in \mathbb{F}^* \mid \text{order of } x = d\}.$$

Then by Proposition 2, we have $\{a^k \mid \gcd(k,d)=1\} \subset B_d$.
On the other hand, $\{1, a, a^2, \ldots, a^{d-1}\} \subset \{x \in \mathbb{F}^* \mid x^d = 1\}$. Since the set on the left hand side has exactly d elements, and the set on the right hand side has at most d elements, it follows that these sets must be equal. Hence we have

$$B_d \subset \{x \in \mathbb{F}^* \mid x^d = 1\} = \{1, a, a^2, \ldots, a^{d-1}\}.$$

It follows that $B_d = \{a^k \mid \gcd(k,d)=1\}$ and that $|B_d| = \phi(d)$.
Suppose now that d is an arbitrary divisor of $q-1$. If $B_d = \emptyset$, then $|B_d| = 0$. If $B_d \neq \emptyset$, then we know from above that $|B_d| = \phi(d)$. It follows that

$$q-1 = |\mathbb{F}| = \sum_{d|(q-1)} |B_d| \leq \sum_{d|(q-1)} \phi(d).$$

But Proposition 3 states that

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

Consequently,

$$\sum_{d|(q-1)} \phi(d) = \sum_{d|(q-1)} |B_d| = q-1,$$

and this happens exactly if, $|B_d| = \phi(d)$, for all divisors d of $q-1$.

$\square$

Definition* A group G is cyclic, if there is $g \in G$ such that for all $h \in G$ there is an integer k such that $h = g^k$. Then we say that g is a generating element of G, or what is the same, G is generated by g.

Corollary* Suppose that $\mathbb{F}$ is a finite field. Then the multiplicative group $(\mathbb{F}^*, \cdot)$ is a cyclic group.

Proof. Denote $|\mathbb{F}| = q$. By Proposition 4 there are $\phi(q-1)$ elements of order $q-1$ in $\mathbb{F}^*$. Clearly, each such element is a generator of $\mathbb{F}^*$.

$\square$

Definition. Suppose that $\mathbb{F}$ is a finite field. An element in $\mathbb{F}^*$ with maximal order that is equal to $|\mathbb{F}| - 1 = |\mathbb{F}^*|$, is called a primitive element. A finite field $\mathbb{F}$ has $\phi(|\mathbb{F}| - 1)$ primitive elements.

Example. Consider the field $\mathbb{Z}_{19}$. Then the number 2 is primitive modulo 19, which we can verify, for example, as follows. The factorization of the integer 19 -1 = 18 is $18 = 2 \times 3 \times 3$. By exercise 5.4 of the textbook it suffices to check that that

$$2^9 = 512 \neq 1(\text{mod} 19) \text{ and } 2^6 = 64 \neq 1(\text{mod} 19).$$

Hence

$$\mathbb{Z}_{19}{}^* = \{2^k \bmod 19 \,|\, k = 0, 1, \ldots, 17\}.$$

Next we determine the syclic subgroups of $\mathbb{Z}_{19}{}^*$. The number of elements of a cyclic subgroup of $\mathbb{Z}_{19}{}^*$ must be a divisor of 18. By Euler's theorem, the following numbers are possible: 1, 2, 3, 6, 9 and 18. We denote by S_r the cyclic subgroup of r elements. Below, we list the exponents k such that $2^k \in S_r$, for all divisors r of 18.

r	k	S_r
18	$k = 0, 1 \ldots, 17$	1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10
9	k even	1, 4, 16, 7, 9, 17, 11, 6, 5
6	$\frac{18}{6}$ divides k	1, 8, 7, 18, 11, 12
3	$\frac{18}{3}$ divides k	1, 7, 11
2	9 divides k	1, 18
1	$k = 0$	1