Bull. Korean Math. Soc.
Vol. 20, No. 2. 1983

REMARKS ON FINITE FIELDS

SHIN WON KANG

It is the purpose of this paper to give some remarks on finite fields. We shall show that the little theorem of Fermat, Euler's criterion for quadratic residue mod p, and other few theorems in the number theory can be derived from the theorems in theory of finite field $K=GF(p)$, where p is a prime. The forms of some irreducible ploynomials over $K=GF(p)$ will be given explicitly.

For every prime p and positive integer n, there is exactly one finite field $F=GF(p^n)$ (up to isomorphism) of order p^n. The Frobenius mapping $\varphi : F \to F$ such that $\varphi(x)=x^p$ is a K-automorphism of F and the Galois group $\mathrm{Aut}_K F$ is cyclic of degree n, generated by φ ([3], [5]).

LEMMA 1. *Let q be a prime. Then there are exactly $(p^q-p)/q$ distinct monic irreducible polynomials of degree q over $K=GF(p)$.*

Proof. Let $F=GF(p^q)$. Since $[F : K]=q$, the only non-trivial proper subfield of F is $K=GF(p)$. Each of $|F-K|=(p^q-p)$ elements of F satisfies some monic irreducible polynomial of degree q over K, but the q elements of them are conjugate each other and they are the roots of same monic irreducible polynomial of degree q over K.

COROLLARY. *If p, q are primes, then $p^q-p \equiv 0 \pmod q$. Moreover, if $(p, q)=1$ then $p^{q-1} \equiv 1 \pmod q$.*

LEMMA 2. *Let q be a prime and n an arbitrary positive integer. Then there are exactly $(p^{q^n}-p^{q^{n-1}})/q^n$ distinct monic irreducible polynomials of degree q^n over $K=GF(p)$.*

Proof. Let $E=GF(p^{q^n})$. Then $[E : K]=q^n$ and E contains the finite field $E_1=GF(p^{q^{n-1}})$ as the largest subfield, which contains the subfields of E of order $q, q^2, \cdots\cdots q^{n-2}$. Each of $|E-E_1|=(p^{q^n}-p^{q^{n-1}})$ elements of E satisfies some monic irreducible polynomial of degree q^n over K, but the q^n elements of them are conjugate each other, so the Lemma is true.

COROLLARY. *If p, q are primes and n is arbitrary positive integer, then $p^{q^n}-p^{q^{n-1}} \equiv 0 \pmod{q^n}$.*
Moreover, if $(p, q)=1$ then $p^{q^n}-q^{n-1} \equiv 1 \pmod{q^n}$.

THEOREM 1. *Let a be an arbitrary integer and p a prime not dividing a, Then $a^{p^n}-p^{n-1} \equiv 1 \pmod{p^n}$ for every positive integer n.*

Proof. Suppose that a can be factored into the product of primes. Without loss of generality, we may assume $a=qr$, where q, r are primes. By Lemma 2, we have

$q^{p^n} \equiv q^{p^{n-1}} \pmod{p^n}$ and $r^{p^n} \equiv r^{p^{n-1}} \pmod{p^n}$, so we have $q^{p^n} \cdot r^{p^n} = a^{p^n} \equiv q^{p^{n-1}} \cdot r^{p^{n-1}} \pmod{p^n}$ or $a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}$.

DEFINITION. Let f be any monic irreducible polynomial of degree n over $K = CF(p)$ and

$$K_f = K[x]/(f) = \{a_1 t^{n-1} + \cdots\cdots + a_{n-1} t + a_n \mid a_i \in K,\ f(t) = 0\}.$$

Then t is called the generating element of K_f.
If $\alpha \in K_f$ and $|\alpha| = p^n - 1$, then α is said a primitive element of K_f.
If the generating element t of K_f is primitive, then f is called a primitive polynomial of degree n over K.

LEMMA 3. *If ϕ denotes Euler ϕ-function, then there are $\phi(p^n - 1)/n$ primitive polynomials of degree n over K.*

Proof. See [1].

If f, g are monic irreducible polynomials of degree n over K, then there are n isomorphisms from K_f onto K_g. Let α be an arbitrary element of K_f and $\varphi^i(\alpha)$, $i = 1, 2, \ldots\ldots, n$ be mutually different in K_f. Then there exists uniquely determined monic irreducible polynomial h of degree n over K which is satisfied by $\varphi^i(\alpha)$, $i = 1, \ldots, n$. If s is the generating element of K_h, then α and s have same order and $\alpha \mapsto s$ induces an K-isomorphism ϕ from K_f onto K_h such that $\phi(\alpha) = s$. ([4]).

THEOREM 2. *Suppose that an odd prime p can be written in the form $p = mn + 1$, where m, n are positive integers, and a is a primitive root of p. Then $x^n - a$ is irreducible over $K = GF(p)$, and so is $x^m - a$.*

Proof. If t satisfies $f = x^n - a$, then $t^n = a$ and $t^p = a^m t$, $t^{p^i} \equiv a^{im} \cdot t \pmod{p}$ for $i = 1, 2, \ldots n$. Since a is a primitive root of p, $|a| = p - 1 = mn$ in K, so we have $t^{p^{n-1}} \equiv 1 \pmod{p}$ and $t^{p^i} \neq t^{p^j} \pmod{p}$ if $i \neq j$, for all $1 \leqslant i,\ j \leqslant n-1$ and $t,\ t^p, \ldots, t^{p^{(n-1)}}$ are roots of $f = x^n - a$.

COROLLAY. *Let a be a primitive root of an odd prime p. Then $x^2 - a$ is irreducible over K, and so is $x^{p-1} - a$.*

Proof. Every odd prime p can be written in the form $p = 2k - 1$ or $p = 1 \cdot (p-1) + 1$.

LEMMA 4. *Let p be an odd prime. There are $(p-1)/2$ monic irreducible polynomials of degree 2 over $K = GF(p)$ of the form $x^2 - a$.*

Proof. Let r be a primitive root of $p = 2k + 1$. Then by the corollary of theorem 2, $f = x^2 - r$ is irreducible over K. The generating element t of K_f is conjugate to $\varphi(t) = t^p = r^k t$ in K_f and we must have $t + r^k t \equiv 0 \pmod{p}$. So $r^k \equiv -1 \pmod{p}$ and any element of K_f of the form $\alpha t, \alpha \in K$, is conjugate to $\varphi(\alpha t) = \alpha r^k\ t \equiv -\alpha t \pmod{p}$ in K_f. Now αt and $-\alpha t$ satisfy the uniquely determined monic irreducible polynomial h of degree 2 over K and if s is the generating element of K_h, then $\alpha t \mapsto s$ induces a K-isomorphism ϕ such that $\phi(\alpha t) = s$. Therefore, $s^2 = \phi(\alpha^2 t^2) = \alpha^2 r$ and s is the generating element of $h = x^2 - \alpha^2 r$. There are $(p-1)$ elements of the form αt,

$\alpha \in K$, in K_f, and the two elements of them are conjugate each other and determine one monic irreducible polynomial over K of the form $x^2-\beta$, $\beta \in K$. On the other hand, if $\xi t+\eta \in K_f$ and $\varphi(\xi t+\eta)$ satisfies a monic irreducible polynomial of degree 2 over K of the form x^2-a, then $\eta=0$.

COROLLARY. *For an odd prime p, if a is a primitive root of p, then* $\left(\frac{a}{p}\right)=-1$, *where* $\left(\frac{a}{p}\right)$ *is the Legendre symbol.*

Proof. If a is a primitive root of p, then by Lemma 4, $f=x^2-a$ is irreducible over $K=GF(p)$. So there exist no element $\alpha \in K$ such that $\alpha^2 \equiv a \pmod{p}$ and a is a non-quadratic residue mod p and $\left(\frac{a}{p}\right)=-1$.

COROLLARY. *If p is an odd prime, then* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$,

Proof. If $\left(\frac{a}{p}\right)=-1$, then x^2-a is irreducible over K, so by Lemma 4, for any primitive root r of p there exist an element $\alpha \in K$ *such that* $a \equiv \alpha^2 r \pmod{p}$, then $a^{\frac{p-1}{2}} \equiv (\alpha^2 r)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Conversely, if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, then for a root t of $f=x^2-a$, $t^p=a^{\frac{p-1}{2}}t \equiv -t \pmod{p}$ and $t \not\equiv tp \pmod{p}$, so f is irreducible over K, and $\left(\frac{a}{p}\right)=-1$. On the other hand, if $\left(\frac{a}{p}\right)=1$ then x^2-a is reducible over K, so there exist an element α of K such that $\alpha^2 \equiv a \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \alpha^{p-1} \equiv 1 \pmod{p}$. Conversely, if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then $f=x^2-a$ is reducible over K and $\left(\frac{a}{p}\right)=1$.

Let us consider an irreducible polynomial $f=x^2-x-a$ over $K=GF(p)$, p any prime. The generating element t of K_f satisfies $t^2=t+a$. Straight forward calculation shows that $t^n=S_{n-1}t+T_{n-1}$, where $S_1=1$, $T_1=a$ and $S_r=S_{r-1}+T_{r-1}$, $T_r=aS_{r-1}$ $(r=2, 3, \ldots, n)$ or more explicitly

we have $S_r=\binom{r}{0}+\binom{r-1}{1}a+\ldots+\binom{m}{m}a^m$ for $r=2m$,

$$S_r=\binom{r}{0}+\binom{r-1}{1}a+\ldots+\binom{m+1}{m}a^m \quad \text{for } r=2m+1$$

where $\binom{n}{r}=\frac{n!}{r!(n-r)!}$

DEFINITION. For every positive integer n

$$\binom{n}{0}+\binom{n-1}{1}x+\ldots+\binom{m}{m}x^m \quad \text{if } n=2m,$$

$$\binom{n}{0}+\binom{n-1}{1}x+\ldots+\binom{m+1}{m}x^m \quad \text{if } n=2m+1$$

is called Shinwon polynomial of order n and is denoted by $S_n(x)$.

LEMMA 5. *If $f=x^2-x-a$ is irreducible over $K=GF(p)$, p is a prime, then for any positive integer n,*

$$S_n(a)\equiv S_{n+p^2-1}(a) \pmod{p}$$

Proof. Let $f=x^2-x-a$ be irreducible over $K=GF(p)$. The generating element t of K_f satisfies $t^{p^2-1}=1$. $t^n=t^{n+p^2-1}$

LEMMA 6. *For every prime p, $S_p(x)$ splits over $K=GF(p)$.*

Proof. $S_2(x)=1+x\equiv 0 \pmod 2$ has a solution $x=1$ in $K=GF(2)$. For every odd prime p, $S_p(x)$ is a polynomial of degree $(p-1)/2$ over $K=GF(p)$, and there are $(p-1)/2$ elements r in K such that $\left(\frac{r}{p}\right)=-1$, So by the corollary of Lemma 4 there are $(p-1)/2$ monic irreducible polynomials of degree 2 over K of the form $f=x^2-r$. The generating element t of K_f satisfies $t^2=r$ and an element $\alpha=t+b\in Kf$ must satisfy the irreducible polynomial $g=x^2-2bx+b^2-r$. We may choose $b=2^{-1}$ in K, so the generating element s of K_g satisfies $g=x^2-x-a$, where $a=r-b^2=r-(2^{-1})^2$, and we have $s^2=s+a$. Now $\varphi(s)=s^p=[S_{p-1}(a)]s+aS_{p-2}(a)$ is also a root of g, and the theorems in theory of equations show that $s+s^p=[1+S_{p-1}(a)]s+aS_{p-2}(a)\equiv 1 \pmod p$.

Hence
$$1+S_{p-1}(a)\equiv 0 \pmod p,$$
$$aS_{p-2}(a)\equiv 1 \pmod p$$

So $S_p(a)=S_{p-1}(a)+aS_{p-2}(a)\equiv 0 \pmod p$. If $r_1\neq r_2$ in K, then $a_1=r_1-b^2\neq r_2-b^2=a_2 \pmod p$ and the Lemma is evident.

COROLLARY. *For every odd prime p and positive integer n, the congruence $S_{n(p+1)-1}(x)\equiv 0 \pmod p$ has $(p-1)/2$ solusions in $GF(p)$.*

Proof. In Lemma 6, we have $(p-1)/2$ elements a of $K=GF(p)$ such that $s^{p+1}\equiv -a \pmod p$, so $s^{n(p+1)}\equiv(-a)^n \pmod p$.

DEFINITION. For every positive integer n the polynomial $x^{2n}-x^n-a$ over $K=GF(p)$, p is a prime, is called n-step polynomial of x^2-x-a over K. If f is any monic irreducible polynomiol of degree n over $K=GF(p)$, and t is the generating element of K_f, then the order of t is called the order of f and is denoted by $|f|$. The smallest positive integer r such that $t^r=\alpha$, for some $\alpha\in K$, is called Shinwon number of f and is denoted by $S(f)$.

LEMMA 7. *$S(f)$ divides $|f|$.*

Proof. It follows from the above definition.

LEMMA 8. *Let $f=x^2-x-a$ be irreducible over $K=GF(p)$, p be a prime. If $s=S(f)$, then $S_n(a)\equiv 0 \pmod p$ if and only if $n=rs-1$ for some positive integer r.*

Proof. Let t be a generating element of K_f, then $t^s\equiv\alpha \pmod p$ for some $\alpha\in K$. If $S_n(a)\equiv 0 \pmod p$, then $t^{n+1}=[S_n(a)]t+aS_{n-1}(a)\equiv aS_{n-1}(a)\in K \pmod p$, so $s|(n+1)$, and there exists a positive integer r such that $n+1=rs$. Conversely, if $n=rs-1$, then $t^{n+1}=t^{rs}\equiv(\alpha)^r\equiv[S_n(a)]t+aS_{n-1}(a) \pmod p$, so $S_n(a)\equiv 0 \pmod p$.

COROLLARY. *Let* $f=x^2-x-a$ *be irreducible over* $K=GF(p)$. *Then* $S_{|f|-1}(a)\equiv 0 \pmod p$ *and* $aS_{|f|-2}(a)\equiv 1 \pmod p$.

Proof. $t^{|f|}\equiv 1\equiv[S_{|f|-1}(a)]t+aS_{|f|-2}(a) \pmod p$.

THEOREM 3. *Let* $f=x^2-x-a$ *be an irreducible polynomial over* $K=GF(p)$, p *a prime. If* $n\cdot|f|\,|(p^{2n}-1)$ *and* $n\cdot|f|\nmid(p^i-1)$, $i=1,2,\ldots,2n-1$ *then the n-step polynomial of* f *is irreducible over* K.

Proof. Let t satisfy the polynomial $g=x^{2n}-x^n-a$, then $t^{2n}=t^n+a$ and $t^{nr}=[S_{r-1}(a)]t^n+aS_{r-2}(a)$, so $t^{n|f|}=[S_{|f|-1}(a)]t^n+aS_{|f|-2}(a)\equiv 1 \pmod p$ by the corollary of Lemma 8.

If $n|f|\,|(p^{2n}-1)$ then $t^{p^{2n-1}}\equiv 1 \pmod p$ and if $n|f|\,|(p^i-1)$ $i=1,\ldots,2n-1$, then $t^i\not\equiv t^j \pmod p$ if $i\neq j$, for all $1\leqslant i,j\leqslant 2n-1$. Clearly, $t, t^p, \ldots, t^{p^{2n-1}}$ are roots of g.

THEOREM 4. *If* $f=x^2-x-a$ *is irreducible over* $K=GF(p)$, p *is a prime, and* $S(f)=p+1$, *then* $g=x^{p+1}-x-a$ *is irreducible over* K.

Proof. Assume that g is not irreducible over K. Let t be an element which satisfies $x^{p+1}-x-a=0$ Then $t^{p+1}=t+a$, and straightforward calculation shows $t^{p^r+p^{r-1}+\cdots+p+1}=[S_r(a)]t+aS_{r-1}(a)$. Hence $t^{p^p+\cdots+p+1}\equiv -a \pmod p$, and so $t^{p^{p+1}-1}\equiv 1 \pmod p$ and t^{p^i} are roots of g for $i=0,1,\cdots,p$. Since $S(f)=p+1$, by Lemma 8, $S_i(a)\not\equiv 0 \pmod p$ for $i=1,2,\ldots p-1$, and if $t^{p^i}\equiv t \pmod p$ for some $1<i\leqslant p$ then $t^{p^{i-1}+\cdots+p+1}\equiv t\cdot t^{p^{i-1}+\cdots+p+1} \pmod p$

$\Leftrightarrow$ $[S_i(a)]t+aS_{i-1}(a)\equiv t[\{S_{i-1}(a)\}t+aS_{i-2}(a)] \pmod p$

$\Leftrightarrow$ $S_{i-1}(a)\equiv 0 \pmod p$, $aS_{i-2}(a)\equiv S_i(a) \pmod p$.

But, this contradicts to $S(f)=p+1$. Hence g is irreducible over K.

References

1. G. Birkhoff, and T. Bartee, *Modern applied algebra*, McGraw-Hill Book Co. 1970.
2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1965.
3. T. W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974.
4. S. W. Kang, *Irreducible polynomials over GF(p)*, to appear.
5. S. Lang, *Algebra*, Addison Wesley, Reading, Mass, 1965.
6. P. Samuel, *Algebraic theory of numbers*, Hermann, Paris, 1970.

Hanyang University
Seoul 133, Korea