Bull. Korean Math. Soc. **22** (1985), No. 1, pp. 37-41

REMARKS ON FINITE FIELDS II

SHINWON KANG

For every positive integer n, the polynomial

$$S_n(x)=\begin{cases}\binom{n}{0}+\binom{n-1}{1}x+\cdots+\binom{m}{m}x^m, & \text{if } n=2m,\\ \binom{n}{0}+\binom{n-1}{1}x+\cdots+\binom{m+1}{m}x^m, & \text{if } n=2m+1\end{cases}$$

is called Shinwon polynomial of order n. For every odd prime p, the polynomial $S_p(x)$ splits over $K=GF(p)$ and has distinct $(p-1)/2$ roots in K (See [1]).

In this paper, a number of essential properties of $S_n(x)$ are proved and some number theoretical corollaries are obtained. The polynomial $f(x)=x^{p-1}-1$ is of degree $p-1$ over $K=GF(p)$ and, by the Fermat's theorem, has the distinct $p-1$ roots in $K=GF(p)$. So we have the following lemma.

LEMMA 1. *For every prime p,*

$$x^{p-1}-1\equiv 0 \pmod{S_p(x)}.$$

LEMMA 2. $S_n(x)=S_{n-1}(x)+xS_{n-2}(x),\quad n>2.$

Proof. It follows from the property of the binomial coefficients:

$$\binom{n-r}{r}=\binom{n-r-1}{r}+\binom{n-r-1}{r-1}.$$

THEOREM 1. *For all integers $n>r>1$*

$$S_n(x)=S_r(x)S_{n-r}(x)+xS_{r-1}(x)S_{n-r-1}(x).$$

Proof. We will prove this theorem by induction on $r\geq 2$. From the above lemma, we have

$$\begin{aligned}S_n(x)&=S_{n-1}(x)+xS_{n-2}(x)\\&=S_{n-2}(x)+xS_{n-3}(x)+xS_{n-2}(x)\\&=(1+x)S_{n-2}(x)+xS_{n-3}(x)\\&=S_2(x)S_{n-2}(x)+xS_1(x)S_{n-3}(x).\end{aligned}$$

So the theorem is true for $r=2$. Suppose that the theorem is true for all integers less than r. Then

$$\begin{aligned} S_n(x) &= S_{r-1}(x)S_{n-r+1}(x) + xS_{r-2}(x)S_{n-r}(x) \\ &= S_{r-1}(x)[S_{n-r}(x) + xS_{n-r-1}(x)] + xS_{r-2}(x)S_{n-r}(x) \\ &= [S_{r-1}(x) + xS_{r-2}(x)]S_{n-r}(x) + xS_{r-1}(x)S_{n-r-1}(x) \\ &= S_r(x)S_{n-r}(x) + xS_{r-1}(x)S_{n-r-1}(x). \end{aligned}$$

So the theorem is true for al integers $r \geq 2$.

THEOREM 2. *For all positive integers n and r,*

$$S_{n(r+1)-1}(x) \equiv 0 \ (mod\ S_r(x)).$$

Proof. We will prove the theorem by induction on n. If $n=1$, then

$$S_{n(r+1)-1}(x) = S_r(x).$$

If $n=2$, then it follows from Theorem 1 that

$$\begin{aligned} S_{2(r+1)-1}(x) &= S_{2r+1}(x) \\ &= S_r(x)S_{r+1}(x) + xS_{r-1}(x)S_r(x) \\ &\equiv 0 \ (mod\ S_r(x)). \end{aligned}$$

Suppose that the theorem is true for all integers less than n. Then

$$\begin{aligned} &S_{n(r+1)-1}(x) \\ &= S_r(x)S_{n(r+1)-1-r}(x, + xS_{r-1}(x)S_{n(r+1)-1-r-1}(x) \\ &= S_r(x)S_{nr+n-1-r}(x) + xS_{r-1}(x)S_{nr+n-1-r-1}(x) \\ &= S_r(x)S_{(n-1)r+n-1}(x) + xS_{r-1}(x)S_{(n-1)r+(n-1)-1}(x) \\ &= S_r(x)S_{(n-1)(r+1)}(x) + xS_{r-1}(x)S_{(n-1)(r+1)-1}(x) \\ &\equiv 0 \ (\mathrm{mod}\ S_r(x)). \end{aligned}$$

So the theorem is true for all integers n.

COROLLARY. *For every odd prime p and positive integer n, the polynomial $S_{n(p+1)-1}(x)$ over $K=GF(p)$ has at least $(p-1)/2$ solutions in K.*

Proof. From Theorem 2, we have $S_{n(p+1)-1}(x) \equiv 0$ (mod$S_p(x)$). Since the polynomial $S_p(x)$ has distinct $(p-1)/2$ roots in $K=GF(p)$, the corollary is valid.

THEOREM 3. *For every odd prime p, we have*

$$S_{p-1}(x) \equiv (1+4x)^{(p-1)/2} \ (mod\ p).$$

Proof. We can easily check the fact that

$$\binom{(p-1)/2}{r} 4^r \equiv \binom{p-r-1}{r} \ (\mathrm{mod}\ p),$$

from which the theorem follows.

THEOREM 4. *For every odd prime p, we have*

$$S_p(x) \equiv [S_{p-1}(x)+1](p+1)/2$$
$$\equiv [xS_{p-2}(x)-1](p-1) \quad (mod\ p).$$

Proof. It follows from the following properties:

$$2\binom{p-r}{r} \equiv \binom{p-r-1}{r} \quad (\text{mod } p)$$
$$\binom{p-r}{r} \equiv (p-1)\binom{p-r-1}{r-1} \quad (\text{mod } p)$$

where $1 \le r \le (p-1)/2$.

THEOREM 5. *Let p be an odd prime and $a \in K = GF(p)$. If $S_p(a)=0$, then $S_{p-1}(a)=-1$ and $aS_{p-2}(a)=1$ in K.*

Proof. From Therem 3, we have

$$S_p(x) = [S_{p-1}(x)+1](p+1)/2$$
$$\text{and } S_p(x) = [xS_{p-2}(x)-1](\mathrm{p}-1)$$

as a polynomial over K. So, if $S_p(a)=0$ then

$$0 = [S_{p-1}(a)+1](p+1)/2$$
$$\text{and } 0 = [aS_{p-2}(a)-1](p-1).$$

This completes the proof.

THEOREM 6. *For every odd prime p, $p \ge 5$, the polynomial $S_{p-2}(x)$ over $K = GF(p)$ splits.*

Proof. For all $a \in K = GF(p)$ such that $1+4a \ne 0$, we have

$$S_p(a) = [S_{p-1}(a)+1](p+1)/2$$
$$= [(1+4a)^{(p-1)/2}+1](p+1)/2.$$

But, $(1+4a)^{(_p-1)/2}=1$ or $(1+4a)^{(p-1)/2}=-1$. From these it follows that $S_p(a)=1$ or $S_p(a)=0$. On the other hand, from Theorem 4, we have

$$S_p(a) = [aS_{p-2}(a)-1](p-1),$$

so $S_p(a)+(p-1)=(p-1)aS_{p-2}(a)$.
Now, if $S_p(a)=1$ then

$$0 = (p-1)aS_{p-2}(a)$$

and this means $S_{p-2}(a)=0$. But there are $(p-3)/2$ distinct elements a such that $1+4a \ne 0$ in K, and $S_{p-2}(x)$ is a polynomial over K of degree $(p-3)/2$. This completes the proof.

COROLLARY 1. *If p is an odd prime with $p \equiv -1$ (mod 3), then*

$$\left(\frac{-3}{p}\right) = -1.$$

Proof. Since p is of the from $p=3n-1$ for some positive integer n,

$$S_p(x)=S_{3n-1}(x)\equiv 0 \pmod{S_2(x)}.$$

Since $S_p(x)=[S_{p-1}(x)+1](p+1)/2$
$$=[(1+4x)^{(p-1)/2}+1](p+1)/2$$

in $K=GF(p)$, $x=-1$satisfies $S_p(x)$. So we have $0=S_p(-1)$ in K, and $(-3)^{(p-1)/2}\equiv -1 \pmod p$.

COROLLARY 2. *If p is an odd prime with $p\equiv 1$ (mod 3), then*

$$\left(\frac{-3}{p}\right)=1.$$

Proof. Since p is of the form $p=3n+1$ for some positive integer n, $p-2$ is of the form $3n-1$. From

$$S_p(x)=S_{3m+1}(x)\equiv(p-1)\ [xS_{3n-1}(x)-1] \pmod p$$

and $S_{3n-1}(x)\equiv 0 \pmod{S_2(x)}$, we have

$$S_p(-1)=(p-1)(-1)=[(-3)^{(p-1)/2}+1](p+1)/2$$

in $K=GF(p)$. So $(-3)^{(p-1)/2}\equiv 1 \pmod p$.

COROLLARY 3. *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right)=\begin{cases}+1 & \text{if } p\equiv 1 \pmod 4\\ -1 & \text{if } p\equiv -1 \pmod 4).\end{cases}$$

Proof. If $p=4n-1$, then $S_p(x)\equiv S_{4n-1}(x)\equiv 0 \pmod{S_3(x)}$. Since $S_3(x)=1+2x$, we have $0=S_{4n-1}((p-1)/2)$ in $K=GF(p)$ and $(-1)^{(p-1)/2}\equiv -1 \pmod p$.
If $p=4n+1$, then

$$S_p(x)=S_{4n+1}(x)\equiv(p-1)[xS_{4n-1}(x)-1] \pmod p$$

and $S_{4n+1}((p-1)/2)=1$ in K and $(-1)^{(p-1)/2}\equiv 1 \pmod p$.

COROLLARY 4. *For every odd prime p, the polynomial x^2-x-a with $1+4a\neq 0$ is irreducible over $K=GF(p)$ if and only if $S_p(a)=0$.*

Proof. If x^2-x-a is irreducible over K then clearly $S_p(a)=0$ (See [1]). Conversely, assume that $S_p(a)=0$. Suppose that x^2-x-a is not irreducible over K. Then there exists an element $t\in K$ such that $t^2-t-a=0$. Then $t^2=t+a$, and the straight forward calculation shows that

$$t^p=S_{p-1}(a)t+aS_{p-2}(a), \text{ and}$$
$$t^{P+1}=S_p(a)t+aS_{p-1}(a).$$

Since $S_p(a)=0$, it follows from Theorem 5 that

$$t^p=-t+1,\quad t^{p+1}=-a.$$

Since $t^p=t$ we have $2t=1$ and $t^2=-a$. Hence it follows that $1+4a=0$. But this is a contradiction.

References

1. Shin Won Kang, *Remarks on finite fields*, Bull. Korean Math. Soc. **20** (1983) 81–85.
2. Shin Won Kang, *A note on finite fields*, to appear.

Hanyang University
Seoul 133, Korea