Advances in Pure Mathematics, 2016, 6, 493-497
Published Online June 2016 in SciRes. http://www.scirp.org/journal/apm
http://dx.doi.org/10.4236/apm.2016.67035

Scientific Research Publishing

Some New Results about Trigonometry in Finite Fields

Amiri Naser*, Hasani Fysal

Department of Mathematics, Payame Noor University, Tehran, Iran
Email: *n_amiri@pnu.ac.ir, f_hasani@pnu.ac.ir

Received 26 December 2015; accepted 11 June 2016; published 14 June 2016

Abstract

In this paper, we study about trigonometry in finite field, we know that $\sqrt{2}\in\mathbb{F}_p$, the field with p elements, where p is a prime number if and only if $p = 8k + 1$ or $p = 8k - 1$. Let F and K be two fields, we say that F is an extension of K, if $K \subseteq F$ or there exists a monomorphism $f: K \to F$. Recall that $F[x]=\left\{a_0+a_1x+a_2x^2+\cdots+a_nx^n \middle| a_i\in F, n\geq 0\right\}$, $F[x]$ is the ring of polynomial over F. If $K \leq^e F$ (means that F is an extension of K), an element $u \in F$ is algebraic over K if there exists $f(x)\in K[x]$ such that $f(u) = 0$ (see [1]-[4]). The algebraic closure of K in F is $\bar{K}$, which is the set of all algebraic elements in F over K.

Keywords

Trigonometry, Finite Field, Primitive, Root of Unity

1. Introduction

In this paper, we study about trigonometry in finite field, we know that $\sqrt{2}\in\mathbb{F}_p$, the field with p elements, where p is a prime number if and only if $p = 8k + 1$ or $p = 8k - 1$. More generally, what can be said about $\sqrt{p_1+\sqrt{p_2+\cdots+\sqrt{p_n}}}$ in $\mathbb{F}_p$ where $p_1, p_2, \cdots, p_n$ are prime numbers. To attempt to answer the question, for which p, $\sqrt{2+\sqrt{p}}\in\mathbb{F}_p$, we are naturally led to use the formula, $\cos^2\theta=\frac{1+\cos 2\theta}{2}$. Indeed, if $\theta=\frac{\pi}{8}$, we have $\cos^2\frac{\pi}{8}=\frac{2+\sqrt{2}}{4}$ and so $\cos\frac{\pi}{8}=\frac{\sqrt{2+\sqrt{2}}}{2}$, we can choose θ, a suitable 16*th* root of unity, such that

*Corresponding author.

How to cite this paper: Naser, A. and Fysal, H. (2016) Some New Results about Trigonometry in Finite Fields. *Advances in Pure Mathematics*, **6**, 493-497. http://dx.doi.org/10.4236/apm.2016.67035

$\frac{\theta+\theta^{-1}}{2}=\frac{\sqrt{2+\sqrt{2}}}{2}$. The crucial observation is that this formula makes sense any algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ if $p\neq 2$.

Let F and K be two fields, we say that F is an extension of K if $K\subseteq F$ or there exists a monomorphism $f:K\to F$. Recall that $F[x]=\left\{a_0+a_1x+a_2x^2+\cdots+a_nx^n \middle| a_i\in F, n\geq 0\right\}$, $F[x]$ is the ring of polynomial over F. If $K\leq^e F$ (means that F is an extension of K), an element $u\in F$ is algebraic over K if there exists $f(x)\in K[x]$ such that $f(u)=0$. The algebraic closure of K in F is $\bar{K}$, which is the set of all algebraic elements in F over K.

Definition. Let p be a prime number, $p\neq 2$ and let k be an integer such that $p\nmid k$. Then we can define the set $\cos[k]=\left\{c(\theta)=\frac{\theta+\theta^{-1}}{2} \middle| \theta \text{ is a primitive kth root of unity}\right\}$.

Note that symbol "|" is divisor or divides such that $a|b$ means a divides b and $a\nmid b$ means a does not divide b.

Remark. 1) Recall that θ is a primitive kth root of unity if $\theta^k=1$ but $\theta^n\neq 1$, for all $1\leq n\leq k-1$ (see [2] [4]). The two make the assumption $p\nmid k$ because if $p|k$, then there are no primitive kth root of unity in $\overline{\mathbb{F}_p}$.

2) We can define $\sin[k]=\left\{s(\theta)=\frac{\theta-\theta^{-1}}{2i} \middle| \theta \text{ is the kth root of unity}\right\}$, in this set, i is a fixed square root of -1. We know that $s(\theta)\in\mathbb{F}_{p^n}$. In particular, we have $c(\theta)^2+s(\theta)^2=1$ and $\theta=c(\theta)+is(\theta)$.

Theorem 1. If K is a field with 9 elements and if $\mathbb{F}$ is a finite extension of K, then the mapping $\lambda:\mathbb{F}\to\mathbb{F}$ defined by $\lambda(x)=x^9$ is an automorphism of $\mathbb{F}$ which fixes exactly the elements of K.

Proof. It is obviously that λ is onto and one to one (see [5] [6]).

Theorem 2. Let θ be a primitive kth root of unity. Then $\theta+\theta^{-1}\in\mathbb{F}_p$ if and only if $p\equiv\pm 1(\mathrm{mod}\, k)$.

Proof: Assume $\theta+\theta^{-1}\in\mathbb{F}_p$. If $\theta\in\mathbb{F}_p$, then $p\equiv 1(\mathrm{mod}\, k)$. Since the order of the multiplicative group of $\mathbb{F}_p$ is $p-1$. If $\theta\notin\mathbb{F}_p$, then the irreducible polynomial of θ over $\mathbb{F}_p$ is $(x-\theta)(x-\theta^{-1})$. Hence $\theta^p=\theta^{-1}$ and so $p\equiv -1(\mathrm{mod}\, k)$.

Conversely, let $p\equiv\pm 1(\mathrm{mod}\, k)$. If $p\equiv 1(\mathrm{mod}\, k)$ then, since the multiplicative group of $\mathbb{F}_p$ is cyclic of order $p-1$, $\mathbb{F}_p$ contains a primitive kth root of unity. Therefore $\mathbb{F}_p$ contains all primitive kth root of unity and so $\theta\in\mathbb{F}_p$. Hence $\theta+\theta^{-1}\in\mathbb{F}_p$. If $p\equiv -1(\mathrm{mod}\, k)$ then $\theta^p=\theta^{-1}$ hence $(\theta+\theta^{-1})^p=\theta+\theta^{-1}$, so $\theta+\theta^{-1}\in\mathbb{F}_p$.

Corollary 3. If $p\neq 2$ and θ is a primitive kth root of unity, then $c(\theta)\in\mathbb{F}_p$ if and only if $p\equiv\pm 1(\mathrm{mod}\, k)$.

Remark. We observe that since membership of $c(\theta)$ in $\mathbb{F}_p$ depends only on p and k, we have that either $\cos[k]\subset\mathbb{F}_p$ or $\cos[k]\cap\mathbb{F}_p=\varnothing$.

Lemma 4. Let θ be a primitive kth root of unity in $\bar{Q}$, the algebraic closure of the rationales Q. Let $R=Z[\theta]$, the subring of $\bar{Q}$ generated by the integers Z and θ, and let P be a prime ideal of R containing of $R_{\underline{P}}$, where $(p, k) = 1$, where $(,)$ denotes the highest common factor. Let S be the valuation ring of $Q(\theta)$ containing the ring $A=\left\{xy^{-1} \middle| x,y\in R, y\notin P\right\}$, and let M be the maximal ideal of S. Then $\bar{\theta}=\theta+M$ is a primitive kth root of unity in the field of $\frac{S}{M}$.

Proof. The formal derivative kx^{k-1} of x^k-1 is relatively prime to x^k-1 and so x^k-1 has no repeated roots in $\frac{S}{M}$. On the other hand, $x^k-1=\prod_{i=0}^{k-1}(x-\theta^i)$ and so, over $\frac{S}{M}$: $x^k-1=\prod_{i=0}^{k-1}(x-\theta^i)$. It follows that $\bar{\theta}$ is a primitive root of unity in $\frac{S}{M}$.

Remark. For the basic properties of valuation rings, the reader can consult. In particular, it is worth recalling that each valuation ring is integrally closed in its quotient field K, and so, if $k^2-a=0$, $k\in K$, then $k\in A$ (see [7]-[9]). Moreover, each valuation ring is a local ring which means that for each $a\in A/M$, $a-1\in A/M$ as well. Expression obtained for the real and imaginary parts of the roots of unity over complex number is meaningful in A/M.

2. Some Properties

Corollary 5. Let $(q, 10) = 1$. Then $\sqrt{2+\sqrt{2+\cdots+\sqrt{2+\frac{\sqrt{5}-1}{2}}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1 \left(mod\, 2^n \cdot 5\right)$ were n is the number of 2's occurring under the root signs (excluding the 2 in the denominator!).

Proof. Define $r_1 = \frac{\sqrt{5}-1}{2}$, $a_1 = \frac{\sqrt{10+2\sqrt{5}}}{2}$, and for each $n \geq 2$: $r_n = \sqrt{2+a_{n-1}}$, $a_n = \sqrt{2-a_{n-1}}$. Let $b_{n=\frac{r_n}{2}}$, $d_{n=\frac{a_n}{2}}$. Now $b_1 + id_1$ is a primitive 5*th* root of unity viewed as an element of the complex number. Thus $b_1 + id_1$ is a 5*th* primitive root of unity in $\overline{\mathbb{F}_p}$ provided $p \neq 5$. Moreover, it is easy to check that $\left(b_n + id_n\right)^2 = b_{n-1} \pm id_{n-1}$ and so $\theta = b_n + id_n$ is a primitive $2^{n-1} \cdot 5$ root of 1.

Remark. If in corollary 5 we take $n = 0$, $q = p$, we obtain a special case of the quadratic reciprocity law, namely: $\frac{\sqrt{5}-1}{2} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1 \left(mod 5\right)$ or $\sqrt{5} \in \mathbb{F}_p \Leftrightarrow p \equiv \pm 1 \left(mod 5\right)$.

Corollary 6. Assume $(2, q) = 1$. Then $\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1 \left(mod\, 2^{n+2}\right)$ where n is the number of 2's occurring under root signs.

Proof. Let $a_1 = 0$, $b_1 = 2$ and for each $n \geq 2$ Let $a_n = \sqrt{2+b_{n-1}}$, $b_n = \sqrt{2-a_{n-1}}$ where at each stage we make a specific choice of square root.

As before letting $r_{n=\frac{a_n}{2}}, t_{n=\frac{b_n}{2}}$ and we have $r_n + it_n$ is a primitive 2^{n+2} root of unity.

Corollary 7. Let $(6, q) = 1$. Then $\sqrt{2+\sqrt{2+\cdots+\sqrt{3}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1 \left(mod\, 2^{n+2} \cdot 3\right)$, where n is the number of 2's under the square root signs.

Proof. Let $a_1 = \sqrt{3}, b_1 = 2$ and for each $n \geq 2$ Let $a_n = \sqrt{2+b_{n-1}}, b_n = \sqrt{2-a_{n-1}}$. Then with the same notation as above we have $r_n + it_n$ is a primitive $2^{n+2} \cdot 3$ root of unity.

Remark. If $n = 0$ and $q = p$ above we have $\sqrt{3} \in \mathbb{F}_p \Leftrightarrow p \equiv \pm 1 \left(mod 12\right)$ which is again a particular case of the quadratic reciprocity Law.

Corollary 8. Let $(q, 34) = 1$. Then

$$a = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{2} + \sqrt{17+3\sqrt{17}-\sqrt{34-\sqrt{17}}-2\sqrt{34+2\sqrt{17}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1 \left(mod 17\right).$$

The Formula in corollary 8 is quite complicated and one is naturally interested to know whether already some subformula of this formula is an element of $\mathbb{F}_q$. Suppose that $q \equiv \pm 1 \left(mod 17\right)$, then $\sqrt{17} \in \mathbb{F}_q$.

Indeed set $\lambda = \theta + \theta^{16} + \theta^4 + \theta^{13} + \theta^9 + \theta^8 + \theta^{15} + \theta^2$ where θ is a primitive 17^{th} root of unity in $\overline{\mathbb{F}_q}$. Since $q \equiv \pm 1 \left(mod 17\right)$ we see $\lambda^q = \lambda$ and $\lambda \in \mathbb{F}_q$. On the other hand one checks easily that $\left(2\lambda + 1\right)^2 = 17$, hence $\sqrt{17} \in \mathbb{F}_q$. We climb that also $\lambda^2 + 4$ is a square in $\mathbb{F}_q$. To show this consider $\alpha = \theta + \theta^{16} + \theta^4 + \theta^{13}$ and $\beta = \theta^9 + \theta^8 + \theta^{15} + \theta^2$. Then $\alpha + \beta = \lambda$. Moreover we have $\alpha\beta = \sum_{i=1}^{16} \theta^i = -1$. Thus $\alpha - \alpha^{-1} = \lambda$. Since $q \equiv \pm 1 \left(mod 17\right)$ we see that both $\alpha, \beta \in \mathbb{F}_q$. Hence $\sqrt{\lambda^2 + 4} \in \mathbb{F}_q$ too. Since $\lambda = \frac{\sqrt{17}-1}{2}$ or $\lambda = \frac{-\left(\sqrt{17}+1\right)}{2}$ we see that $\sqrt{2\left(17-\sqrt{17}\right)} \in \mathbb{F}_q$ or $\sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$. Since $\sqrt{2\left(17-\sqrt{17}\right)} \cdot \sqrt{2\left(17+\sqrt{17}\right)} = \pm 8\sqrt{17} \in \mathbb{F}_q$. we see that both element $\sqrt{2\left(17-\sqrt{17}\right)}$ and $\sqrt{2\left(17+\sqrt{17}\right)}$ belong to $\mathbb{F}_q$. Combining corollary 8 with the considerations above, we obtain.

Corollary 9. Suppose that $(q, 34) = 1$, Then $\sqrt{34-2\sqrt{17}}$ and $\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$ both belong to $\mathbb{F}_q$ if $q \equiv \pm 1 \left(mod 17\right)$.

Remark ([10] [11])**.** One could use the formula given in the table at the end of this note to deduce corollary 9,

more easily. Indeed, for example, from c_1 and c_4 in $\mathbb{F}_q$ we deduce that $c_1 + c_4 = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{4} \in \mathbb{F}_q$, similarly $c_2 + c_8 = \frac{-1+\sqrt{17}-\sqrt{34-2\sqrt{17}}}{4} \in \mathbb{F}_q$. From this follows that $\sqrt{17}$ and $\sqrt{34-2\sqrt{17}} \in \mathbb{F}_q$.

Theorem 10. Suppose (34, q) = 1, Then $\sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$ if and only if $q \equiv \pm 1, \pm 4 \left(mod 17\right)$.

Proof. If $\lambda = \sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$ then also $\sqrt{17} \in \mathbb{F}_q$ and $q \equiv \pm 1, \pm 4, \pm 2, \pm 8 \left(mod 17\right)$. Indeed $\sqrt{17} \in \mathbb{F}_q$ if either $q = p^r$ and $\sqrt{17} \in \mathbb{F}_q$ or $q = p^r$ with r even. In the first case $p \equiv \pm 1, \pm 4, \pm 2, \pm 8 \left(mod 17\right)$ and therefore $p^r \equiv \pm 1, \pm 4, \pm 2, \pm 8 \left(mod 17\right)$, too. On the other hand p, when r is even, is congruent to one of the elements ±1, ±4, ±2, ±8. On the other hand, in the notation as above, we have $\alpha = \theta + \theta^{-1} + \theta^4 + \theta^{-4} \in \mathbb{F}_q$ if and only if $\sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$. If $q \equiv \pm 1$ or $q \equiv \pm 4$ we see that $\alpha^q = \alpha$ and $\alpha \in \mathbb{F}_q$. Hence $q \equiv \pm 1, \pm 4 \left(mod 17\right)$. So $\sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$.

We want to prove that $\sqrt{2\left(17+\sqrt{17}\right)} \in \mathbb{F}_q$ then $q \equiv \pm 1, \pm 4 \left(mod 17\right)$. It is enough to exclude possibilities $q \equiv \pm 2, \pm 8 \left(mod 17\right)$. Suppose that $q \equiv \pm 2, \pm 8 \left(mod 17\right)$, Then $\alpha = \alpha^q = \theta^8 + \theta^9 + \theta^2 + \theta^{15} = -\alpha^{-1}$. Thus

$$\theta = \alpha + \beta = \begin{cases} \frac{-1+\sqrt{17}}{2} \\ \frac{-\left(1+\sqrt{17}\right)}{2} \end{cases} \text{ iff } \begin{cases} \sqrt{17} = 1 \\ \sqrt{17} = -1 \end{cases} \text{ that this is contradiction.}$$

Corollary 11. Assume (34, q) = 1. If $q = p^r$, then $\sqrt{17+\sqrt{17}} \in \mathbb{F}_q$ if and only if $q \equiv \pm 1 \left(mod 8\right)$ and $q \equiv \pm 1, \pm 4 \left(mod 17\right)$ or $q \equiv \pm 3 \left(mod 8\right)$ and $q \equiv \pm 2, \pm 8 \left(mod 17\right)$.

Therefore the inclusion $\sqrt{17+\sqrt{17}} \in \mathbb{F}_q$ depends only on q(*mod* 136). we now focus attention on $s\left(\theta\right) = \frac{\theta - \theta^{-1}}{2i}$ where θ is a primitive kth root of unity in $\overline{\mathbb{F}_q}$. Note that if $p = 2$, $\frac{\theta - \theta^{-1}}{2i} = \frac{\theta + \theta^{-1}}{2}$ which has been dealt with is lemma 4 from now on we assume $2 \nmid q$.

Definition. Let $\sin\left[k\right] = \left\{ s\left(\theta\right) \middle| \theta \text{ is a primitive } k\text{th root of unity} \right\}$, we shall abbreviate $s(\theta)$ to s. The reader should beware that "*is*" is not necessarily the third person singular of the present tense of the verb to be!

Theorem 12. Let θ be a primitive kth root of unity. Then $s\left(\theta\right) \in \mathbb{F}_q$ iff one of the following holds :

(i) $q \equiv \pm 1 \left(mod \left[4, k\right]\right)$ where [,] denotes the least common multiple.

(ii) k has the form $8m + 4$ and $q \equiv 4m + 1 \left(mod\ k\right)$

(iii) k has the form $8m + 4$ and $q \equiv 4m + 3 \left(mod\ k\right)$

Proof. Assume $s = s\left(\theta\right) \in \mathbb{F}_q$. Then $q \equiv 1 \left(mod\, k\right)$ and set $c = c\left(\theta\right)$ so that $\theta = c + is$. For case (i), Let $\theta \in \mathbb{F}_q$. Then $q \equiv 1 \left(mod\, k\right)$ and by corollary 3: $c \in \mathbb{F}_q^*$. Therefore $is \in \mathbb{F}_q$ and so $\in \mathbb{F}_q$. Hence $q \equiv 1 \left(mod\, 4\right)$ and thus $q \equiv 1 \left(mod \left[4, k\right]\right)$.

Case (ii), Let $\theta \notin \mathbb{F}_q$ and $c \in \mathbb{F}_q$. Then $is \notin \mathbb{F}_q$ too, and thus $i \notin \mathbb{F}_q$. Therefore $q \equiv 1 \left(mod\, 4\right)$. On the other hand $q \not\equiv 1 \left(mod\ k\right)$ Since $\theta \notin \mathbb{F}_q$ and so $q \equiv -1 \left(mod\, k\right)$, with $c \in \mathbb{F}_q$, implies that $q \equiv -1 \left(mod \left[4, k\right]\right)$.

Case (iii), $\theta \notin \mathbb{F}_q$, $c \in \mathbb{F}_q$ and is belong to $\mathbb{F}_q$. In this case $i \in \mathbb{F}_q$ and so $q \equiv 1 \left(mod\, 4\right)$. Now $c^2 = 1 - s^2$ whence $\theta^q = \pm c$. But $c \notin \mathbb{F}_q$ and so $c^q = -c$ Therefore $\theta^q = \left(c + is\right)^q = -c + is$. Hence $\theta^{q+1} = -1$ and so $\theta^{2(q+1)} = 1$. Therefore $2q \equiv -2 \left(mod\, k\right)$. So $q \not\equiv \pm 1 \left(mod\ k\right)$ and thus k is even and $q \equiv -1 \left(mod\, \frac{k}{2} \right)$. Therefore $q \equiv 1 \left(mod\, 4\right)$, $q \equiv -1 \left(mod\, \frac{k}{2} \right)$ and $q \not\equiv \pm 1 \left(mod\ k\right)$. It is easily seen that these three condition are equivalent to $k = 8m + 4$ and $q \equiv 4m + 1 \left(mod\ k\right)$ for some m.

Corollary 13. For any k, either $\sin\left[k\right] \subset \mathbb{F}_q$ or $\sin\left[k\right] \cap \mathbb{F}_q = \varnothing$.

Proof. As $s\left(\theta\right) \in \mathbb{F}_q$ depends only on q and k and not particular primitive root chosen, finally, we determine

how many distinct values of $c(\theta)$ and $s(\theta)$ there are as θ varies over the primitive kth root of unity.

3. Conclusion

We conclude that in the field of real numbers, trigonometric ratios are defined as defined in finite fields. As well as relations between trigonometric ratios hold in the field of real numbers, finite fields are also established under the circumstances.

References

[1] Delbaen, F. and Schachermayer, W. (2006) The Mathematics of Arbitrage. Springer, Berlin.

[2] Karl, G. (1994) Operator Trigonometry. *Linear and Multilinear Algebra*, **37**, 139-159. http://dx.doi.org/10.1080/03081089408818318

[3] Lima, J.B. and Campello de Souza, R.M. (2013) Fractional Cosine and Sine Transforms over Finite Fields. *Linear Algebra and Its Applications*, **438**, 3217-3230. http://dx.doi.org/10.1016/j.laa.2012.12.021

[4] Karl, G. (2010) Operator Trigonometry of Multivariate Finance. *Journal of Multivariate Analysis*, **101**, 374-384.

[5] Lang, S. (1994) Algebra. 2nd Edition, Addison-Wesley Publishing Company.

[6] Karl, G. (1997) Operator Trigonometry of Iterative Methods. *Numerical Linear Algebra with Applications*, **4**, 333-347. http://dx.doi.org/10.1002/(SICI)1099-1506(199707/08)4:4<333::AID-NLA113>3.0.CO;2-I

[7] John, B. (2008) Geometry and Trigonometry. Engineering Mathematics Pocket Book (Fourth Edition), 105-148.

[8] Carl, S. and Jeff, Z. (2013) College Trigonometry. Lorain County Community College.

[9] Gauss, C.F. (1965) Disquisitrones Arithmetica. English Translation, Bravncshweig.

[10] Chowla, S. (1965) The Riemann Hypothesis Hilbert's Tenth Problem. Gorden and Breach Science Publishers.

[11] Honghai, L., George, M.C. and Dave, P.B. (2009) Fuzzy Qualitative Trigonometry. *International Journal of Approximate Reasoning*, **51**, 71-88.