Pure and Applied Mathematics Journal
2016; 5(4): 93-96
http://www.sciencepublishinggroup.com/j/pamj
doi: 10.11648/j.pamj.20160504.11
ISSN: 2326-9790 (Print); ISSN: 2326-9812 (Online)

Some New Results About Trigonometry in Finite Fields

Habib Hosseini[1, *], Naser Amiri[2]

[1]Department of Mathematics, Firoozabad Branch, Islamic Azad University, Firoozabad, Iran

[2]Department of Mathematics, Tehran Payame Noor University, Tehran, Iran

Email address:

math12shahrad@gmail.com (H. Hosseini), amiri@susc.ac.ir (N. Amiri)

[*]Corresponding author

To cite this article:

Habib Hosseini, Naser Amiri. Some New Results About Trigonometry in Finite Fields. *Pure and Applied Mathematics Journal.* Vol. 5, No. 4, 2016, pp. 93-96. doi: 10.11648/j.pamj.20160504.11

Received: April 23, 2016; **Accepted**: May 21, 2016; **Published**: June 17, 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 are two field, we say that F is an extension of K, if $K \subseteq F$ or there exist a monomorphism f: $K \to F$. recall that $F[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | a_i \in F, n \geq 0\}$, $F[x]$ 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 $\overline{K}$, 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 $p_1, p_2, \ldots, p_n$, p are prime numbers. Can we replace square root by cube roots.

In attempting to answer the question, for which p, $\sqrt{2 + \sqrt{p}} \in \mathbb{F}_p$, we are naturally led to use the formula, $cos^2\theta = \frac{1+cos2\theta}{2}$. 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 *16th* root of unity, such that $\frac{\theta+\theta^{-1}}{2} = \frac{\sqrt{2+\sqrt{2}}}{2}$. 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 are two field, we say that F is an extension of K if $K \subseteq F$ or there exist a monomorphism $f: K \to F$. recall that $F[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | a_i \in F, n \geq 0\}$, $F[x]$ 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 $\overline{K}$, is the set of all algebraic elements in F over K.

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

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 $1 \leq n \leq k - 1$. We have two make the assumption $p \nmid k$ because if $p \mid k$, then there are no primitive *kth* root of unity in $\overline{\mathbb{F}_p}$.

(2) We can defined $sin[k] = \{s(\theta) = \frac{\theta-\theta^{-1}}{2i} | \theta$ *is the kth root of unity*$\}$, 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 λ: $\mathbb{F} \to \mathbb{F}$ 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.

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

Proof: Assume $\theta + \theta^{-1} \in \mathbb{F}_p$. If $\theta \in \mathbb{F}_p$, then $p \equiv 1 (mod$

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 $p \equiv -1(mod\ k)$.

Conversely, let $p \equiv \pm 1(mod\ k)$. If $p \equiv 1(mod\ k)$ 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 $p \equiv -1(mod\ k)$ then $\theta^p = \theta^{-1}$ whence $(\theta+\theta^{-1})^p = \theta + \theta^{-1}$, 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 $p \equiv \pm 1(mod\ k)$.

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 $cos[k] \cap \mathbb{F}_p = \emptyset$.

Lemma 4. Let θ be a primitive *kth* root of unity in $\overline{Q}$ the algebraic closure of the rationales *Q*. Let $R = Z[\theta]$, the subring of $\overline{Q}$ 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 (,) denote the highest common factor. Let *S* be the valuation ring of $Q(\theta)$ containing the ring $A = \{xy^{-1} | \ x, y \in R, y \notin P\}$, and let *M* be the maximal ideal of *S*. Then $\overline{\theta} = \theta + M$ 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 $\overline{\theta}$ is a primitive root of unity in $\frac{S}{M}$.

Remark. For the basic properties of valuation rings the reader can consults. 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 $k \in A$. 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 are meaningful in *A/M*.

2. Some Properties

Corollary 5. Let (*q*, 10) = 1. Then

$$\sqrt{2+\sqrt{2+\cdots+\sqrt{2+\frac{\sqrt{5}-1}{2}}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1(mod\ 2^n.5)$$

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 *5th* root of unity viewed as an element of the complex number. Thus $b_1 + id_1$ is a *5th* primitive root of unity in $\overline{\mathbb{F}_p}$ provided $p \neq 5$. Moreover, it is easy to check that $(b_n + id_n)^2 = b_{n-1} \pm id_{n-1}$ and so $\theta = b_n + id_n$ is a primitive $2^{n-1}.5$ 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: $\frac{\sqrt{5}-1}{2} \in \mathbb{F}_q \Leftrightarrow p \equiv \pm 1(mod\ 5)$ or $\sqrt{5} \in \mathbb{F}_p \Leftrightarrow p \equiv \pm 1(mod\ 5)$.

Corollary 6. Assume (2, *q*) = 1. Then $\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1(mod\ 2^{n+2})$ 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 $\sqrt{2+\sqrt{2+\cdots+\sqrt{3}}} \in \mathbb{F}_q \Leftrightarrow q \equiv \pm 1(mod\ 2^{n+2}.3)$, 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 $2^{n+2}.3$ root of unity.

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

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

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

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 $q \equiv \pm 1(mod\ 17)$, 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 *17th* root of unity in $\overline{\mathbb{F}_q}$. Since $q \equiv \pm 1(mod\ 17)$ we see $\lambda^q = \lambda$ and $\lambda \in \mathbb{F}_q$. On the other hand one checks easily that $(2\lambda+1)^2 = 17$, 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 $q \equiv \pm 1(mod\ 17)$ 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 $\lambda = \frac{-(\sqrt{17}+1)}{2}$ we see that $\sqrt{2(17-\sqrt{17})} \in \mathbb{F}_q$ or $\sqrt{2(17+\sqrt{17})} \in \mathbb{F}_q$. Since $\sqrt{2(17-\sqrt{17})}.\sqrt{2(17+\sqrt{17})} = \pm 8\sqrt{17} \in \mathbb{F}_q$. we see that both element $\sqrt{2(17-\sqrt{17})}$ *and* $\sqrt{2(17+\sqrt{17})}$ 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 $q \equiv \pm 1(mod\ 17)$.

Remark. 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 $\sqrt{2(17+\sqrt{17})} \in \mathbb{F}_q$ if and only if $q \equiv \pm 1, \pm 4(mod\ 17)$.

Proof. if $\lambda = \sqrt{2(17+\sqrt{17})} \in \mathbb{F}_q$ then also $\sqrt{17} \in \mathbb{F}_q$ and $q \equiv \pm 1, \pm 4, \pm 2, \pm 8(mod\ 17)$. 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 $p \equiv \pm 1, \pm 4, \pm 2, \pm 8(mod\ 17)$ and therefore $p^r \equiv \pm 1, \pm 4, \pm 2, \pm 8(\ mod\ 17)$, too. On the other hand p, when r is even, is congruent to one of the elements $\pm 1, \pm 4, \pm 2, \pm 8$. 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 $\sqrt{2(17+\sqrt{17})} \in \mathbb{F}_q$. If $q \equiv \pm 1$ or $q \equiv \pm 4$ we see that $\alpha^q = \alpha$ and $\alpha \in \mathbb{F}_q$. Hence $q \equiv \pm 1, \pm 4(mod\ 17)$. So $\sqrt{2(17+\sqrt{17})} \in \mathbb{F}_q$.

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

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

Therefore the inclusion $\sqrt{17+\sqrt{17}} \in \mathbb{F}_q$ depends only on $q(mod\ 136)$. we now focus attention on $s(\theta) = \frac{\theta-\theta^{-1}}{2i}$ 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 $sin[k] = \{s(\theta) | \theta$ *is a primitive kth root of unity*$\}$, 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 $s(\theta) \in \mathbb{F}_q$ iff one of the following holds:

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

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

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

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

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 $q \equiv -1(mod\ 4)$. On the other hand $q \not\equiv 1(mod\ k)$ Since $\theta \notin \mathbb{F}_q$ and so $q \equiv -1(mod\ k)$, with $c \in \mathbb{F}_q$, implies that $q \equiv -1(mod\ [4, k])$.

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

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

Proof. As $s(\theta) \in \mathbb{F}_q$ 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] Carl stitz, Jeff zeager, College Trigonometry, lorain county community college, july 4, 2013.

[2] R. M. Campello de Souza, H. M. de Oliveira and D. Silva, "The Z Transform over Finite Fields," *International Telecommunications Symposium*, Natal, Brazil, 2002.

[3] M. M. Campello de Souza, H. M. de Oliveira, R. M. Campello de Souza and M. M. Vasconcelos, "The Discrete Cosine Transform over Prime Finite Fields," *Lecture Notes in Computer Science*, LNCS 3124, pp. 482–487, Springer Verlag, 2004.

[4] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, "Trigonometry in Finite Fields and a New Hartley Transform," *Proceedings of the 1998 International Symposium on Information Theory*, p. 293, Cambridge, MA, Aug. 1998.

[5] F. Delbaen, W. Schachermayer, The Mathematics of Arbitrage, Springer, Berlin, 2006.

[6] Chowla, S, The Riemann hypottesis Hilbert's tenth problem, Gorden and Breach Seience Publishers (1965).

[7] Lang, S, Algebra, second Edition Addison - Wesley publishing company 1994.

[8] K. Gustafson, Operator trigonometry, Linear and Multilinear *Algebra,* 37:139-159 (1994).

[9] K. Gustafson, Operator trigonometry of iterative methods, Numer. Linear Algebra Appl. 4 (1997) 333–347.

[10] J. B. Lima, R. M. Campello de Souza, Fractional cosine and sine transforms over finite fields, Linear Algebra and its Applications, Volume 438, Issue 8, 15 April 2013, Pages 3217-3230.

[11] Karl Gustafson, Operator trigonometry of multivariate finance, Journal of Multivariate Analysis, Volume 101, Issue 2, February 2010, Pages 374-384.

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

[13] Honghai Liu, George M. Coghill, Dave P. Barnes, Fuzzy qualitative trigonometry, International Journal of Approximate Reasoning, Volume 51, Issue 1, December 2009, Pages 71-88.

[14] Gauss, C. F., Disquisitrones arithmetica, Bravncshweig 1801, English translation, Yale paperbound, 1965.

[15] Rudolf Lidl, Harald Niederreiter, Finite Fields and Their Applications, second edition, Cambridge University Press, 1994.