CONSTRUCTION OF THE HEPTADECAGON AND QUADRATIC RECIPROCITY

YURI BURDA AND LIUDMYLA KADETS

Abstract. In this note we present a construction of a regular 17-gon using ruler and compass. We relate steps in this construction to quadratic reciprocity and some trigonometric identities.

Dans cette note, nous présentons une construction à la règle et au compas de l'heptadécagone. Nous établisson des liens les étapes de cette construction de réciprocité quadratique et des identitiés trigono-métriques.

1. Introduction

Galois theory completely answers the question which regular n-gons can be constructed using ruler and compass only:

Theorem 1.1. *A regular n-gon can be constructed using ruler and compass if and only if $n = 2^m \cdot p_1 \cdot \ldots p_k$ where $p_1, \ldots, p_k$ are distinct primes of the form $2^{2^s} + 1$.*

Unfortunately Galois theory can only guide one how to make appropriate constructions (or warn that some constructions are not possible). The work of making explicit constructions remains to be done even after the general theory is well-understood.

It is even more perplexing that the construction of a regular 17-gon has been accomplished first by Gauss in the end of eighteenth century, long after the ancient geometers constructed regular 3-, 4-, 5-, 6-, 8-, 10-, 12-, 15- and 16-gons, but shortly before Galois theory appeared.

In this note we present an explicit construction of the regular 17-gon. The text of this note is divided to three parts. The regular text can be read as one text that presents a construction of the 17-gon without referring to any ideas that appeared after Gauss. This text however contains some choices and constructions which can be much better understood in the framework of a more general theory. Such explanations are provided in paragraphs emphasized by a side line. Finally the paragraphs emphasized by a bold side line relate the construction of the 17-gon with other works of Gauss.

2. Acknowledgements

We would like to thank Askold Khovanskii, whose wonderful lectures on Galois theory inspired us to think about construction of a 17-gon.

We would also like to thank Boris Kadets for telling us several beautiful proofs of quadratic reciprocity.

3. Plan of construction

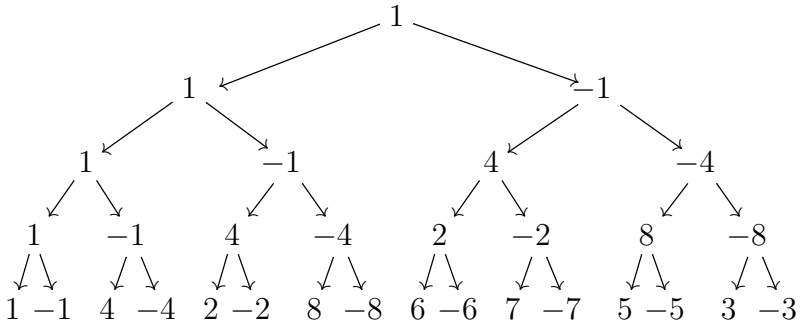
If we identify the plane $\mathbf{R}^2$ with the plane of complex numbers $\mathbf{C}$, then constructing a regular n-gon becomes equivalent to constructing a primitive root of unity ξ of order n (e.g. of $\xi = e^{\frac{2\pi i}{n}}$). Indeed, if this number is already constructed, then its powers are exactly the vertices of the n-gon.

The basic tool used in constructions using ruler and compass is as follows: if z_1 and z_2 are the two solutions of the quadratic equation $z^2 + az + b = 0$ and the points a, b have already been constructed, then points z_1, z_2 can also be constructed.

Our plan is to present an explicit sequence of quadratic equations with the following properties:

- The first equation has integer coefficients,
- The coefficients of every equation are either integers, or are equal (up to a sign) to the roots of the previous equation,
- The solutions of the last equation contain the number ξ.

This sequence of equations will moves us along the rows of the following diagram:



The arrows in this tree point away from a number towards its square roots modulo 17.

With each node in the tree we associate the number $\sum_i \xi^i$ over the set of numbers i from the last row which can be reached from the given node by following the arrows.

We will show that numbers associated to nodes in line i satisfy explicit quadratic equations whose coefficients are either integers or numbers associated to nodes from the previous line (up to a sign).

Remark 3.1. The minimal equation over the field $\mathbf{Q}$ satisfied by the root of unity ξ of order p is $1 + x + \ldots + x^{p-1} = 0$. Its Galois group is the cyclic group $G = \mathbf{Z}_p^*$. For every divisor d of $p - 1$ this group contains a unique group of order d. In particular if $p = 2^k + 1$, the subgroups of the group G form a chain $G = G_k \supset G_{k-1} \supset \ldots \supset$

$G_0 = \{1\}$ with G_m of order 2^m. By Galois correspondence this chain of subgroups corresponds to a chain of quadratic field extensions $\mathbf{Q}(\xi) = L_0 \supset L_1 \supset \ldots \supset L_k = \mathbf{Q}$.

The numbers written in the m-th row of the tree are the elements of the group G_m. The numbers $\sum_{i \in G_m} \xi^i$ associated to the nodes of the diagram generate the extension $L_m/\mathbf{Q}$. The quadratic equation that we find on step number m has coefficients in L_{m-1} and its roots generate the extension L_m/L_{m-1}.

4. Step 0

Let $\xi \neq 1$ be a root of unity of order p. Then

$$\sum_{i=1}^{p-1} \xi^i = \frac{\xi^p - \xi}{\xi - 1} = -1$$

Thus the number associated to the root of the diagram is -1.

5. Step 1 — Quadratic Residues

Theorem 5.1. *Let Q be the set of quadratic residues modulo an odd prime p. Let ξ be a primitive root of unity of order p and let $x = \sum_{i \in Q} \xi^i$.*

If $p = 4m + 1$ then $x^2 + x - \frac{p-1}{4} = 0$.

If $p = 4m - 1$ then $x^2 + x + \frac{p+1}{4} = 0$.

Remark 5.2. For any odd prime p the group $\mathbf{Z}_p^*$ has a unique subgroup of index 2: the group Q formed by the quadratic residues modulo p. The group $\mathbf{Z}_p^*$ is the Galois group of the Galois extension $\mathbf{Q}(\xi)/\mathbf{Q}$: the element $m \in \mathbf{Z}_p^*$ acts by automorphism that sends ξ to ξ^m. The orbit of $x = \sum_{i \in Q} \xi^i$ under the action of this group consists of two elements. Hence x is a root of a quadratic equation with rational coefficients, which theorem 5.1 describes explicitly.

Proof. To compute x we compute instead $y = \sum_{i=0}^{p-1} \xi^{i^2}$ (note that $y = 2x - 1$). The conjugate of y is $\overline{y} = \sum_{i=0}^{p-1} \xi^{-i^2}$ and hence

$$y\overline{y} = \left(\sum_{i=0}^{p-1} \xi^{i^2}\right)\left(\sum_{i=0}^{p-1} \xi^{-j^2}\right) = \sum_{i,j=0}^{p-1} \xi^{i^2 - j^2}$$

The coefficient at ξ^k in this formula is equal to the number of solutions (i, j) of the congruence $i^2 - j^2 \equiv k \mod p$. An invertible change of variables $(a, b) = (i - j, i + j)$ transforms the congruence $i^2 - j^2 \equiv k$

mod p to the congruence $ab \equiv k \mod p$. It has $p-1$ solutions if $k \neq 0$ and $2p-1$ solutions if $k = 0$.

Thus

$$y\overline{y} = 2p - 1 + (p-1)\sum_{k=1}^{p-1} \xi^k = 2p - 1 - (p-1) = p.$$

If $p \equiv 1 \mod 4$ then $\overline{y} = y$. Indeed, since -1 is a quadratic residue modulo p, the sum $\sum_{i=0}^{p-1} \xi^{-i^2}$ is the same as the sum $\sum_{i'=0}^{p-1} \xi^{i'^2}$.

If $p \equiv -1 \mod 4$ then $\overline{y} = -y$. Indeed, since -1 is a quadratic non-residue modulo p, in the sum $y + \overline{y}$ every power of ξ appears exactly twice. Hence $y + \overline{y} = 2\sum_{k=0}^{p-1} \xi^k = 0$.

In both cases $y = 2x - 1$ and the result follows. □

It follows that the numbers associated to the nodes in the second line are solutions of the equation $x^2 + x - \frac{17-1}{2} = 0$, i.e. $x_1, x_2 = \frac{-1\pm\sqrt{17}}{2}$.

Remark 5.3. It is interesting to note that the proof of theorem 5.1 can be used to give a simple and elegant proof of Gauss's quadratic reciprocity law.

To find whether p is a quadratic residue modulo a prime q it is enough check whether $\sqrt{p}$ belongs to $\mathbf{Z}_q$ or not.

The elements of $\mathbf{Z}_q$ are precisely the q roots of the equation $y^q = y$, so checking whether an element y from an extension of $\mathbf{Z}_q$ belongs to $\mathbf{Z}_q$ is equivalent to checking whether $y^q = y$.

Let now as before $y = \sum_{i=0}^{p-1} \xi^{i^2}$ for a primitive root of unity ξ of order p lying in some extension of $\mathbf{Z}_q$.

The arguments from the proof of theorem 5.1 show that if $p \equiv 1 \mod 4$, then $y = \sqrt{p}$. This element belongs to $\mathbf{Z}_q$ if and only if $y^q = y$. However in extensions of $\mathbf{Z}_q$ the formula $(a+b)^q = a^q + b^q$ holds, and hence $y^q = \sum_{i=0}^{p-1} \xi^{i^2 q}$. Thus $y^q = y$ if and only if q is a quadratic residue modulo p.

Thus if $p \equiv 1 \mod 4$ and $q \neq p$ are primes, then p is a square modulo q if and only if q is a square modulo p.

If $p \equiv -1 \mod 4$, then $y = \sqrt{-p}$ and the same arguments show that $-p$ is a square modulo q if and only if q is a square modulo p.

6. Step 2

Lemma 6.1. *For any* $\xi \neq \pm 1$

$$(\xi + \xi^{-1})(\xi^2 + \xi^{-2})(\xi^4 + \xi^{-4}) \cdot \ldots \cdot (\xi^{2^n} + \xi^{-2^n}) = \frac{\xi^{2^{n+1}} - \xi^{-2^{n+1}}}{\xi - \xi^{-1}}$$

This identity can be easily verified by multiplying both sides by $\xi - \xi^{-1}$ and then n times using the identity $(\xi^{2^k} - \xi^{2^k})(\xi^{2^k} + \xi^{2^k}) = (\xi^{2^{k+1}} - \xi^{2^{k+1}})$.

Corollary 6.2. *If $\xi \neq \pm 1$ is a root of unity of order p for $p = 2^{n+1}+1$, then*

$$(\xi + \xi^{-1})(\xi^2 + \xi^{-2})(\xi^4 + \xi^{-4}) \cdot \ldots \cdot (\xi^{2^n} + \xi^{-2^n}) = -1.$$

Let now $c_k = \xi^k + \xi^{-k}$.

Lemma 6.3. *For any m, n*

$$c_m \cdot c_n = c_{m+n} + c_{m-n}.$$

Remark 6.4. If ξ is in fact $e^{i\alpha}$, then $c_k = 2\cos k\alpha$. With this in mind lemma 6.3 follows from the formula $2\cos(m\alpha)\cos(n\alpha) = \cos((m+n)\alpha) + \cos((m-n)\alpha)$. In a similar fashion corollary 6.2 follows from the identity

$$2^n \cos\alpha \cos(2\alpha)\cos(4\alpha) \cdot \ldots \cdot \cos(2^n\alpha) = \frac{\sin(2^{n+1}\alpha)}{\sin\alpha}.$$

Now we find a quadratic equation whose roots are $c_1 + c_4$ and $c_2 + c_8$.

The sum of these roots is $c_1 + c_2 + c_4 + c_8$, which we found in the previous step: it is a root x_1 of the equation $x^2 + x - 4 = 0$.

To find the product $(c_1 + c_4)(c_2 + c_8)$ we argue as follows: corollary 6.2 applied to the root of unity ξ implies that $c_1c_2c_4c_8 = -1$. The same corollary applied to the root of unity ξ^3 implies the identity $c_3c_6c_{12}c_{24} = -1$, i.e. $c_3c_6c_5c_7 = -1$.

Substituting the identities $c_3c_5 = c_2 + c_8$, $c_6c_7 = c_1 + c_4$ into $c_3c_6c_5c_7 = -1$ we get $(c_1 + c_4)(c_2 + c_8) = -1$.

Thus $c_1 + c_4$ and $c_2 + c_8$ are the two solutions y_1, y_2 of the equation $y^2 - x_1y - 1 = 0$ where x_1 is a solution of $x^2 + x - 4 = 0$.

Similarly $c_3 + c_5$ and $c_6 + c_7$ are the two solutions y_3, y_4 of the equation $y^2 - x_2y - 1 = 0$ for another solution x_2 of the equation $x^2 + x - 4 = 0$.

7. Step 4

The numbers c_1 and c_4 satisfy $c_1 + c_4 = y_1$ and $c_1c_4 = c_3 + c_5 = y_3$ and hence c_1, c_4 are the two solutions of the equation $z^2 - y_1z + y_3 = 0$.

8. Final step

$\xi + \xi^{-1} = c_1$, while $\xi \cdot \xi^{-1} = 1$, so ξ and ξ^{-1} are the solutions of $w^2 - c_1w + 1 = 0$.

9. Combining the steps together

In the sequence of four quadratic equations that we have to solve, four times we make the choice of which of the two roots to take. This leads to 16 different answers, each one being a different primitive root of unity of order 17.

If we choose $\xi = e^{\frac{2\pi i}{17}}$, then we can actually trace the choices which lead to a formula for ξ:

$$c_1 + c_2 + c_4 + c_8 = \frac{-1+\sqrt{17}}{2}$$

$$c_3 + c_5 + c_6 + c_7 = \frac{-1-\sqrt{17}}{2}$$

$$c_1 + c_4 = \frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2}$$

$$c_3 + c_5 = \frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2}$$

$$c_1 = \frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2} + \sqrt{\left(\frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2}\right)^2 - 4\frac{\frac{-1-\sqrt{17}}{2}+\sqrt{\frac{17+\sqrt{17}}{2}}}{2}}}{2}$$

$$\xi = \frac{1}{2}\left(\frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2} + \sqrt{\left(\frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2}\right)^2 - 4\frac{\frac{-1-\sqrt{17}}{2}+\sqrt{\frac{17+\sqrt{17}}{2}}}{2}}}{2}\right) +$$

$$+\frac{1}{2}\left(\sqrt{\left(\frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2} + \sqrt{\left(\frac{\frac{-1+\sqrt{17}}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}}{2}\right)^2 - 4\frac{\frac{-1-\sqrt{17}}{2}+\sqrt{\frac{17+\sqrt{17}}{2}}}{2}}}{2}\right)^2} - 4\right)$$

University of Toronto
E-mail address: yburda@math.toronto.edu

E-mail address: lucy.kadets@math.toronto.edu