ON CYCLOTOMIC QUINQUISECTION

By W. Burnside.

[Received November 25th, 1914.—Read December 10th, 1914.—
Received, in revised form, January 12th, 1915.]

If p is a prime and q a factor of $p-1$, there is an equation of degree q with rational coefficients, each of whose roots is the sum of $(p-1)/q$ of the primitive p-th roots of unity, no such p-th root occurring in more than one of the sums. The equation is an Abelian equation with a cyclical group. The determination of the system of relations expressing any rational function of the roots of this equation as a linear function of the roots, has been called by Cayley the problem of cyclotomic q-section. He worked out the theory completely in Vol. xi (Old Series) of our *Proceedings* for the cases $q=3$ and $q=4$. In a short note in Vol. xii, he refers to the case of quinquisection, and gives in tabular form the solution for primes under 100. It is not indicated how this table was constructed, nor is the problem of quinquisection in its general form really attacked at all. So far as I am aware the problem has not been directly dealt with since. The nature of the algebraic "field," determined by the equation of the q-th degree above referred to, has formed the subject of various investigations during the last twenty years; but the determination of the system of integers on which all rational relations between the roots depend, has not, I believe, been considered.

This problem is completely solved here for the case $q=5$. It is shewn to depend on the two diophantine equations

$$12^2p = [4p-16-25(A+B)]^2+5.15^2(A-B)^2+2.15^2C^2+2.15^2D^2,$$

$$0 = [4p-16-25(A+B)](A-B)+3(C^2+4CD-D^2).$$

In the first paragraph of the paper certain general formula are proved which hold when q is any odd prime. These could easily be extended to the case in which q is any number. In the succeeding paragraphs the problem of quinquisection is dealt with.

1. *Notation.*—p is an odd prime,

q is an odd prime factor of $p-1$, and $p-1=qt$,

w is an assigned primitive p-th root of unity,

a is an assigned primitive root of the congruence

$$a^{p-1}\equiv 1 \pmod{p},$$

β is an assigned primitive root of the congruence

$$\beta^{q-1}\equiv 1 \pmod{q}.$$

Each of the $p-1$ primitive p-th roots of unity is included just once in the form

$$w^{a^{i+xq}} \quad (i=0,\,1,\,\ldots,\,q-1\,;\; x=0,\,1,\,\ldots,\,t-1).$$

Put

$$A_i=\sum_{x=0}^{x=t-1} w^{a^{i+xq}} \quad (i=0,\,1,\,\ldots,\,q-1).$$

Each A_i consists of the sum of t distinct primitive p-th roots of unity, and each primitive p-th root occurs just once in one of the A_i's. When w is replaced by w^{a^q}, each A_i remains unaltered. When w is replaced by w^a the A_i's undergo the cyclical permutation

$$(A_0A_1\ldots A_{q-1}).$$

If w' is any root occurring in A_i, then

$$A_i=\sum_{x=0}^{x=t-1} w'^{a^{xq}}.$$

In particular, since t is even, if A_i contains w' it will also contain w'^{-1}.

When i is replaced by βi, the A_i's undergo the permutation

$$\begin{pmatrix} A_0 & A_1 & A_2 & \ldots & A_{q-1} \\ A_0 & A_\beta & A_{2\beta} & \ldots & A_{(q-1)\beta} \end{pmatrix},$$

where the suffixes are reduced (mod q). This leaves A_0 unchanged and gives a regular circular permutation of the other A_i's.

If A_i and A_j are two distinct A's, and if the product A_iA_j is formed without reduction, *i.e.*, without taking account of the relation

$$1+w+w^2+\ldots+w^{p-1}=0,$$

it will consist of the product of t^2 primitive p-th roots, because if w' occurs in A_i, then w'^{-1} does *not* occur in A_j. Moreover, since A_iA_j is unaltered when w is replaced by w^{a^q}, the product can be arranged as the sum of a number of A's. Hence

$$A_i A_j = \sum_{k=1}^{k=t} c_{ijk} A_k,$$

where the c's are zeroes or positive integers, such that

$$\sum_{k=1}^{k=t} c_{ijk} = t.$$

The product A_i^2 will contain t units and t^2-t primitive roots of unity, so that

$$A_i^2 = t + \sum_{k=1}^{k=t} c_{iik} A_k,$$

where again the c's are zeroes or positive integers, and

$$\sum_{k=1}^{k=t} c_{iik} = t-1.$$

Let w' be a root occurring in A_i, and suppose that of the t distinct roots in $w'A_j$ just x belong to A_k. Since both A_j and A_k are unaltered, when w^{α^q} is written for w^α it follows that of the t distinct roots in $w'^{\alpha^q} A_j$ just x belong to A_k. Hence

$$x = c_{ijk}.$$

Let $$w^{\alpha^{j+a_1 q}}, \quad w^{\alpha^{j+a_2 q}}, \quad \ldots, \quad w^{\alpha^{j+a_x q}}$$

be the roots occurring in A_j which, when multiplied by w^{α^i}, give roots occurring in A_k, so that

$$w^{\alpha^i + \alpha^{j+a_1 q}} = w^{\alpha^{k+b_1 q}}, \quad \ldots, \quad w^{\alpha^i + \alpha^{j+a_x q}} = w^{\alpha^{k+b_x q}},$$

while no further relation such as

$$w^{\alpha^i + \alpha^{j+a_{x+1} q}} = w^{\alpha^{k+b_{x+1} q}}$$

holds. Then

$$w^{-\alpha^i + \alpha^{k+b_1 q}} = w^{\alpha^{j+a_1 q}}, \quad \ldots, \quad w^{-\alpha^i + \alpha^{k+b_x q}} = w^{\alpha^{j+a_x q}},$$

and no further similar relation holds. Since $w^{-\alpha^i}$ is a root occurring in A_i, this is equivalent to the equation

$$c_{ijk} = c_{ikj},$$

i.e., the numerical value of the symbol c_{ijk} is independent of the sequence of the letters in the suffix. Moreover the same reasoning clearly holds when two of the letters in the suffix are the same, *i.e.*,

$$c_{iik} = c_{iki}.$$

Further, since writing w^a for w changes A_i into A_{i+1}, the relation

$$A_{i+1}A_{j+1} \sum_{k=0}^{k=t} c_{ijk}A_{k+1}$$

follows from

$$A_iA_j = \sum_{k=0}^{k=t} c_{ijk}A_k.$$

Hence, since the equation for the A's is irreducible,

$$c_{i+1,\,j+1,\,k+1} = c_{ijk}.$$

The complete multiplication table of the A's, viz., the set of relations

$$A_i^2 = t + \sum_1^t c_{iik}A_k,$$

$$A_iA_j = \sum_1^t c_{ijk}A_k$$

$$(i, j = 0, 1, 2, \ldots, q-1)$$

is materially simplified by these relations among the c's. Moreover, the fact that this system of relations is invariant when the A's and the c's simultaneously undergo the permutations

$$\begin{pmatrix} A_i \\ A_{i\beta} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} c_{ijk} \\ c_{i\beta,\,j\beta,\,k\beta} \end{pmatrix}$$

indicates that any system of equations connecting the reduced c's must be invariant for a certain cyclical permutation of the reduced c's.

2. *Quinquisection.*—I consider now in particular the case $q = 5$. The complete multiplication table of the A's arises in this case from the three relations

$$A_0^2 = \lambda + c_{000}A_0 + c_{001}A_1 + c_{002}A_2 + c_{003}A_3 + c_{004}A_4,$$

$$A_0A_1 = c_{010}A_0 + c_{011}A_1 + c_{012}A_2 + c_{013}A_3 + c_{014}A_4,$$

$$A_0A_2 = c_{020}A_0 + c_{021}A_1 + c_{022}A_2 + c_{023}A_3 + c_{024}A_4,$$

by the cyclical permutation $(A_0A_1A_2A_3A_4)$, where λ stands for $\frac{1}{5}(p-1)$. Taking account of the previously obtained relations between the c's, we may write

$$c_{000} = a, \qquad c_{001} = c_{010} = a, \qquad c_{002} = c_{020} = b,$$

$$c_{003} = c_{022} = c, \qquad c_{004} = c_{001} = d, \qquad c_{012} = c_{014} = c_{021} = e,$$

$$c_{013} = c_{023} = c_{024} = f.$$

The relations are then

$$\left.\begin{aligned} A_0^2 &= \lambda+\alpha A_0+aA_1+bA_2+cA_3+dA_4 \\ A_0A_1 &= \quad aA_0+dA_1+eA_2+fA_3+eA_4 \\ A_0A_2 &= \quad bA_0+eA_1+cA_2+fA_3+fA_4 \end{aligned}\right\}, \tag{i}$$

where

$$\left.\begin{aligned} \alpha+a+\ b+\ c+d &= \lambda-1 \\ a+d+2e+\ f \quad &= \lambda \\ b+c+\ e+2f \quad &= \lambda \end{aligned}\right\}. \tag{ii}$$

These give

$$\left.\begin{aligned} \alpha &= \lambda-1-a-b-c-d \\ e &= \tfrac{1}{3}(\lambda-2a-2d+b+c) \\ f &= \tfrac{1}{3}(\lambda+a+d-2b-2c) \end{aligned}\right\}. \tag{iii}$$

When $q=5$, we may take the β of § 1 to be 2. If i is replaced by βi, the A's undergo the permutation $(A_1A_2A_4A_3)$, and it is found that equations (i) remain unaltered, if the coefficients undergo the permutation $(abdc)(ef)$. It follows that whatever set of relations are found between the coefficients, they must be changed into themselves by the permutation $(abdc)(ef)$. This is clearly true of equations (ii).

The equations (i) and those derived from them by the permutation $(A_0A_1A_2A_3A_4)$ may be used to express any rational integral function of the A's as a linear function. In particular, if ϵ is a primitive fifth root of unity, they give

$$(A_0+\epsilon A_1+\epsilon^2A_2+\epsilon^3A_3+\epsilon^4A_4)^2 = f(\epsilon)(A_0+\epsilon^2A_1+\epsilon^4A_2+\epsilon A_3+\epsilon^3A_4),$$

where

$$f(\epsilon) = \alpha+2e+2f+(b+2a+2f)\epsilon+(d+2b+2e)\epsilon^2+(a+2c+2e)\epsilon^3 \\ +(c+2d+2f)\epsilon^4.$$

Hence

$$(A_0+\epsilon A_1+\epsilon^2A_2+\epsilon^3A_3+\epsilon^4A_4)^4 = [f(\epsilon)]^2 f(\epsilon^2)(A_0+\epsilon^4A_1+\epsilon^3A_2+\epsilon^2A_3+\epsilon A_4).$$

But equations (i) also give

$$(A_0+\epsilon A_1+\epsilon^2A_2+\epsilon^3A_3+\epsilon^4A_4)(A_0+\epsilon^4A_1+\epsilon^3A_2+\epsilon^2A_3+\epsilon A_4) = p,$$

so that $$(A_0+\epsilon A_1+\epsilon^2A_2+\epsilon^3A_3+\epsilon^4A_4)^5 = p\,[f(\epsilon)]^2 f(\epsilon^2).$$

Writing ϵ^{-1} for ϵ, and multiplying the two equations together,

$$p^3 = [f(\epsilon)]^2 f(\epsilon^2) f(\epsilon^3)\,[f(\epsilon^4)]^2,$$

whence $$p = f(\epsilon)f(\epsilon^4).$$

This equation can be written in the form

$$p = (a_1\epsilon+a_2\epsilon^2+a_3\epsilon^3+a_4\epsilon^4)(a_1\epsilon^4+a_2\epsilon^3+a_3\epsilon^2+a_4\epsilon).$$

When ϵ is replaced by ϵ^2, the coefficients undergo the permutation $(a_1 a_2 a_4 a_3)$. Apart from this the integers a_1, a_2, a_3, a_4 are unique. For the only modification possible in the two factors, if the coefficients are to be integers, is to multiply one factor by an arbitrary unit (of the field of the fifth roots of unity) and the other by the reciprocal unit. When this is done it is found that the coefficients entering in the two factors are no longer the same, unless the unit is a power of ϵ.

Now

$$f(\epsilon) = (2a+b-\alpha-2e)\epsilon+(2b+d-\alpha-2f)\epsilon^2+(2c+a-\alpha-2f)\epsilon^3$$
$$+(2d+c-\alpha-2e)\epsilon^4$$
$$= [a+d+\tfrac{1}{2}(b+c)-\alpha-2e](\epsilon+\epsilon^4)+[\tfrac{1}{2}(a+d)+b+c-\alpha-2f](\epsilon^2+\epsilon^3)$$
$$+[a-d+\tfrac{1}{2}(b-c)](\epsilon-\epsilon^4)+[b-c-\tfrac{1}{2}(a-d)](\epsilon^2-\epsilon^3).$$

Put
$$A+D = 2a, \qquad B+C = 2b,$$
$$A-D = 2d, \qquad B-C = 2c,$$

so that A, B, C, D are integers, and equations (iii) become

$$\alpha = \lambda-1-A-B, \quad e = \tfrac{1}{3}(\lambda-2A+B), \quad f = \tfrac{1}{3}(\lambda+A-2B).$$

Then $$f(\epsilon) = \left(\frac{4-p}{3}+\frac{10A}{3}+\frac{5B}{6}\right)(\epsilon+\epsilon^4)+\left(\frac{4-p}{3}+\frac{5A}{6}+\frac{10B}{3}\right)(\epsilon^2+\epsilon^3)$$
$$+\left(D+\frac{C}{2}\right)(\epsilon-\epsilon^4)+\left(C-\frac{D}{2}\right)(\epsilon^2-\epsilon^3)$$
$$= P(\epsilon+\epsilon^4)+Q(\epsilon^2+\epsilon^3)+R(\epsilon-\epsilon^4)+S(\epsilon^2-\epsilon^3), \text{ say,}$$
$$f(\epsilon^4) = P(\epsilon+\epsilon^4)+Q(\epsilon^2+\epsilon^3)-R(\epsilon-\epsilon^4)-S(\epsilon^2-\epsilon^3),$$

and
$$p = P^2(\epsilon^2+\epsilon^3+2)+Q^2(\epsilon+\epsilon^4+2)-2PQ$$
$$-R^2(\epsilon^2+\epsilon^3-2)-S^2(\epsilon+\epsilon^4-2)-2RS(\epsilon^2+\epsilon^3-\epsilon-\epsilon^4).$$

Since P, Q, R, S are rational, this involves

$$p = \tfrac{3}{2}P^2+\tfrac{3}{2}Q^2-2PQ+\tfrac{5}{2}R^2+\tfrac{5}{2}S^2.$$
$$0 = P^2-Q^2-R^2+S^2-4RS.$$

When for P, Q, R, S their values in terms of A, B, C, D are entered, these equations become

$$12^2 p = [4p-16-25(A+B)]^2+5.15^2[A-B]^2+2.15^2C^2+2.15^2D^2, \quad \text{(iv)}$$

$$0 = [4p-16-25(A+B)][A-B]+3[C^2+4CD-D^2]. \quad \text{(v)}$$

It follows from the preceding remarks concerning the factors of p, that an integral solution of (iv) and (v) exists, and that apart from the obvious substitution

$$A' = B, \quad B' = A, \quad C' = -D, \quad D' = C,$$

it is unique.

From the multiplication table of the A's, and the relation

$$A_0+A_1+A_2+A_3+A_4 = -1,$$

the equation of the fifth degree which they satisfy can be calculated, the only symmetric function which involves rather lengthy arithmetic being the product. I find the equation to be

$$x^5+x^4-\tfrac{2}{5}(p-1)x^3+\left[\tfrac{1}{3}p(A+B)-\frac{2(p-1)(2p+3)}{3.5^2}\right]x^2$$
$$+\left[\tfrac{1}{9}p\left(\frac{p-1}{5}+A+B\right)^2-pAB-\frac{(p-1)^2}{5^3}\right]x$$
$$+\tfrac{1}{5}p\left[\frac{1}{5.6^3}\left(5(A+B)-\frac{4p-4}{5}\right)^3+\frac{1}{6^2}\left(\frac{2p-2}{5}-A-B\right)^2\right.$$
$$\left.+\tfrac{1}{4}(A-B)^2+\tfrac{1}{8}(A-B)(D^2-C^2)\right]-\frac{(p-1)^3}{5^5} = 0.$$

The coefficients are, as they should be, invariant for the substitution

$$A' = B, \quad B' = A, \quad C' = -D, \quad D' = C.$$

I have verified the numerical values of the above coefficients in the two cases $p = 11$ and $p = 41$, which make it probable that they are correct.

3. If the prime p is not too great, the determination of the integral solutions of (iv) and (v) does not involve lengthy calculations. When $C^2+4CD-D^2$ has a given value m, while C and D are integers, C^2+D^2 is less than $m/\surd 5$. Hence combining the two equations

$$|\,14p-16-25(A+B)\,|+15\surd 5\,|\,A-B\,| < 12\surd p.$$

If $p \equiv 1 \pmod 3$, $A+B \equiv 0 \pmod 3$, while if $p \equiv -1 \pmod 3$, $A+B \equiv 1 \pmod 3$. Hence the successive values of first term on the right in this inequality differ by 75, and the number of possibilities for $(A+B)$ and $|A-B|$ is not very great. It is to be noticed that $|A-B|$ cannot be zero, and that $|A-B|$ and $A+B$ are of the same parity.

Finally, the four solutions of the two equations given by applying the substitution

$$A' = B, \quad B' = A, \quad C' = -D, \quad D' = C,$$

to any one of them correspond to the permutation $(abdc)(ef)$ of the original coefficients.

As an example I take the case $p = 271$. Here $A+B = 3E$, and the inequality is

$$|356-25E| + 5\sqrt{5}\,|A-B| < 4\sqrt{(271)}.$$

This gives

$$E = 13, \quad |A-B| = 1 \text{ or } 3,$$
$$E = 14, \quad |A-B| = 2 \text{ or } 4,$$
$$E = 15, \quad |A-B| = 1 \text{ or } 3.$$

The values of C^2+D^2 in the six cases are 65, 45, 75, 55, 76 and 46 respectively. The only possible one is the first, and this gives

$$C^2+D^2 = 65,$$
$$C^2+4CD-D^2 = \pm 31,$$

according as $A-B$ is $\mp$. The $+$ sign must be taken for $A-B$, and then $C = 1$, $D = 8$. Hence

$$A+B = 39, \quad A-B = 1, \quad C = 1, \quad D = 8,$$

giving

$$a = 14, \quad b = 10, \quad c = 9, \quad d = 6,$$
$$a = 14, \quad e = 11, \quad f = 12.$$

For primes less than 100, the table is

p	A	B	C	D
11	0	1	1	0
31	1	2	4	-1
41	4	3	3	0
61	5	4	4	-1
71	7	6	2	3

4. It is found on trial that the equations (iv) and (v) are the conditions that equations (i) and those derived from them by the permutation $(A_0A_1A_2A_3A_4)$ should, with the relations (ii), form a consistent multiplication table for a set of symbols A_i $(i = 0, 1, 2, 3, 4)$, such that $A_iA_j = A_jA_i$. It was, in fact, in this way that I was originally led to them. This result is still true, if in (iv) and (v), p is replaced by $5\lambda+1$, without making any assumption at all with regard to λ, a, a, b, c, d, e, f, except that they obey the ordinary laws of arithmetic. If, however, (iv) and (v) are arrived at in this way, there is clearly no direct way of shewing that, when $\lambda = (p-1)/5$, and the other letters are positive integers, (iv) and (v) have only one system of solutions.

I have carried the case $q = 7$ so far as to assure myself that it is not quite parallel with that of $q = 5$. A set of three simultaneous Diophantine relations occur, but they are *not* sufficient to ensure that the equations expressing the products of the A's form a consistent multiplication table.