Vertices of polygons

David Pierce

April 1, 2009

1 The pentagon

Vertices of a regular pentagon can be obtained as the solutions in $\mathbb{C}$ of the equation

$$x^5 - 1 = 0 \tag{1}$$

(Fig. 1). To find these solutions, we can use the factorization

$$x^5 - 1 = (x - 1) \cdot (x^4 + x^3 + x^2 + x + 1).$$

So 1 is a solution of (1), and the other solutions are solutions of

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0. \tag{2}$$

To solve *this,* we can make a substitution, letting

$$y = x + \frac{1}{x} \tag{3}$$

so that

$$y^2 = x^2 + 2 + \frac{1}{x^2}.$$

Then (2) becomes

$$y^2 + y - 1 = 0. \tag{4}$$

So y is quadratic, and x is quadratic in y, and we can find our solutions. The question arises: Is a similar analysis possible for $x^{17} - 1$? How did Gauss factorize this in the *Disquisitiones Arithmeticae* [1]?

The inspiration for this article was a conversation with Sasha Borovik at Zencefil restaurant in İstanbul on a rainy holiday Monday, October 29, 2007.

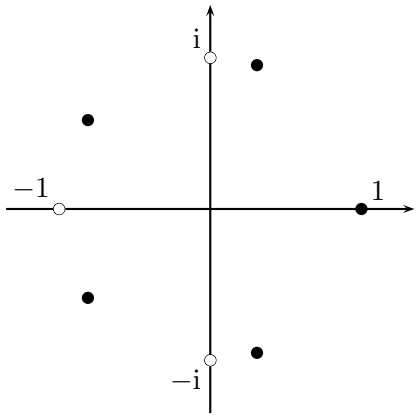

Figure 1: The five 5th roots of 1

2 The numbers for the pentagon

Just to see the numbers, let us first continue the analysis of (1). From (4) and (3) we have*

$$y = \frac{-1 \pm \sqrt{5}}{2}, \qquad x^2 - yx + 1 = 0, \qquad x = \frac{y \pm \sqrt{(y^2 - 4)}}{2}.$$

As $y^2 - 4 = -y - 3$ by (4), so we can also write

$$x = \frac{y \pm \sqrt{(-y - 3)}}{2}.$$

Since $-y - 3 = -(5 \pm \sqrt{5})/2 < 0$, the four solutions to (2) are (as in Fig. 2)

$$\frac{-1 + \sqrt{5}}{4} \pm \frac{\mathrm{i}}{2}\sqrt{\frac{5 + \sqrt{5}}{2}}, \qquad \frac{-1 - \sqrt{5}}{4} \pm \frac{\mathrm{i}}{2}\sqrt{\frac{5 - \sqrt{5}}{2}}.$$

3 Seventeenth roots of unity: first attempt

Suppose we want to solve

$$x^{17} - 1 = 0. \tag{5}$$

Besides 1, the solutions are the solutions of $x^{16} + x^{15} + x^{14} + \cdots + x^2 + x^1 + 1 = 0$ and therefore of

$$x^8 + x^7 + x^6 + \cdots + x^{-6} + x^{-7} + x^{-8} = 0. \tag{6}$$

We can attempt here the same substitution (3) as before. After the computations in Table 1, we obtain

*I prefer writing $\sqrt{5}$ to $\sqrt{5}$: the overline or *vinculum* is not needed here as a grouping symbol, as it is in $\sqrt{y^2 - 4}$; though even here, one may, as I shall, write $\sqrt{(y^2 - 4)}$. Compare $\log x$ with $\log(1 + x)$.

$$
\begin{array}{rccccccccccccccccc}
y = & & & & & & & x & & +x^{-1} & & & & & & & & \\
y^2 = & & & & & & x^2 & & +2 & & +x^2 & & & & & & & \\
y^3 = & & & & & x^3 & & +3x & & +3x^{-1} & & +x^3 & & & & & & \\
y^4 = & & & & x^4 & & +4x^2 & & +6 & & +4x^{-2} & & +x^4 & & & & & \\
y^5 = & & & x^5 & & +5x^3 & & +10x & & +10x^{-1} & & +5x^{-3} & & +x^5 & & & & \\
y^6 = & & x^6 & & +6x^4 & & +15x^2 & & +20 & & +15x^{-2} & & +6x^{-4} & & +x^6 & & & \\
y^7 = & x^7 & & +7x^5 & & +21x^3 & & +35x & & +35x^{-1} & & +21x^{-3} & & +7x^{-5} & & +x^7 & & \\
y^8 = x^8 & & +8x^6 & & +28x^4 & & +56x^2 & & +70 & & +56x^{-1} & & +28x^{-4} & & +8x^{-6} & & +x^8 \\
\hline
y^8 = x^8 & & +8x^6 & & +28x^4 & & +56x^2 & & +70 & & +56x^{-1} & & +28x^{-4} & & +8x^{-6} & & +x^8 \\
y^7 = & x^7 & & +7x^5 & & +21x^3 & & +35x & & +35x^{-1} & & +21x^{-3} & & +7x^{-5} & & +x^7 & & \\
-7y^6 = & & -7x^6 & & -42x^4 & & -105x^2 & & -140 & & -105x^{-2} & & -42x^{-4} & & -7x^{-6} & & & \\
-6y^5 = & & & -6x^5 & & -30x^3 & & -60x & & -60x^{-1} & & -30x^{-3} & & -6x^{-5} & & & & \\
15y^4 = & & & & 15x^4 & & +60x^2 & & +90 & & +60x^{-2} & & +15x^{-4} & & & & & \\
10y^3 = & & & & & 10x^3 & & +30x & & +30x^{-1} & & +10x^{-3} & & & & & & \\
-10y^2 = & & & & & & -10x^2 & & -20 & & -10x^{-2} & & & & & & & \\
-4y = & & & & & & & -4x & & -4x^{-1} & & & & & & & & \\
1 = & & & & & & & & 1 & & & & & & & & & \\
\hline
 & x^8+x^7+x^6+x^5 & & +x^4 & & +x^3 & & +x^2 & +x & +1 & x^{-1} & & +x^{-2} & +x^{-3} & +x^{-4}+x^{-5}+x^{-6}+x^{-7}+x^{-8} & & &
\end{array}
$$

Table 1: Reduction of $(x^{17}-1)/(x-1)x^8$

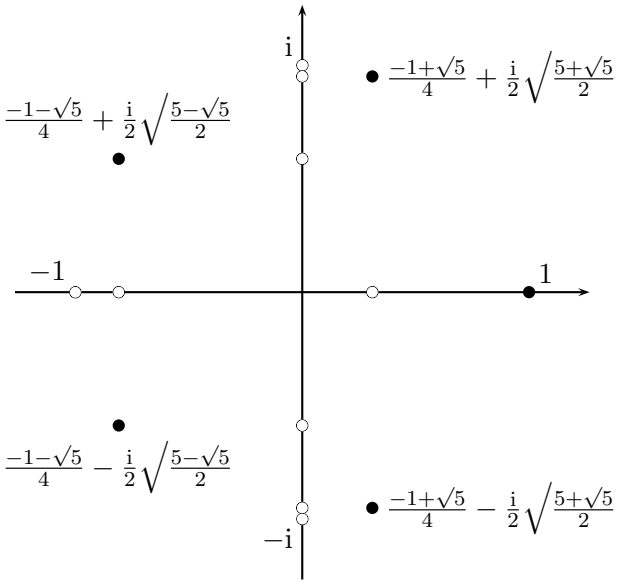

Figure 2: The five 5th roots of 1, evaluated

$$y^8 + y^7 - 7y^6 - 6y^5 + 15y^4 + 10y^3 - 10y^2 - 4y + 1 = 0.$$

It is not clear how to proceed from here. However, Galois theory will illuminate the general situation.

4 Galois analysis

Let n be a positive integer, and let A be the set of solutions in $\mathbb{C}$ of

$$x^n - 1 = 0.$$

Then A is an order-n cyclic subgroup of $\mathbb{C}^\times$. Indeed, we have a homomorphism $x \mapsto \exp(2\pi \mathrm{i} x/n)$ from $\mathbb{Z}$ into $\mathbb{C}^\times$ with image A and kernel (n). If ζ is a generator of A, then $\mathbb{Q}(A) = \mathbb{Q}(\zeta)$. Let G be the Galois group (namely, the group of automorphisms) of this field. Then we have an isomorphism $x \mapsto \sigma_x$ from $(\mathbb{Z}/(n))^\times$ to G, where

$$\sigma_x(\zeta) = \zeta^x.$$

In particular, G is cyclic if and only if n has a primitive root: equivalently, n is 2, 4, an odd prime power, or twice an odd prime power. Let us suppose that we are in the special case where n is a Fermat prime, namely a prime p, where

$$p = 2^{2^m} + 1$$

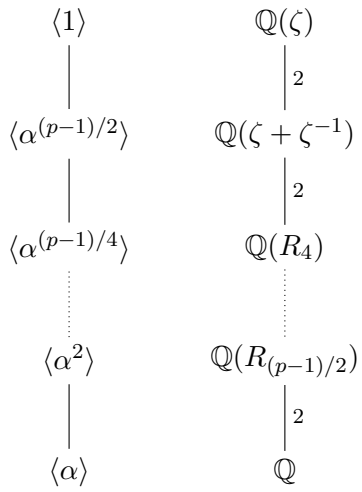

Table 2: The Galois correspondence for $\mathbb{Q}(\exp(2\pi\mathrm{i}/(2^{2^m}+1)))$

for some m.[†] Let α be a generator of G. Then $\alpha = \sigma_r$ for some primitive root r of p. The subgroups of G are just the groups $\langle\alpha^{2^k}\rangle$, where $k \leqslant m$. Moreover,

$$\langle\alpha^{2^k}\rangle \subseteq \langle\alpha^{2^\ell}\rangle \iff \ell \leqslant k;$$

so the set of subgroups of G is linearly ordered by inclusion. Fix a generator ζ of A: say

$$\zeta = \exp\Big(\frac{2\pi\mathrm{i}}{p}\Big).$$

Suppose $p-1$ is factorized as $k\cdot\ell$. Then the subgroup $\langle\alpha^k\rangle$ of G has order ℓ. We define

$$R_\ell = \sum_{\xi\in\langle\alpha^k\rangle} \xi(\zeta) = \sum_{x\in\langle r^k\rangle} \zeta^x,$$

where $\langle r^k\rangle$ is understood as a subgroup of $(\mathbb{Z}/(p))^\times$. Then R_ℓ is the sum of ℓ elements of $A\smallsetminus\{1\}$. In particular,

$$R_1 = \zeta, \qquad R_2 = \zeta+\zeta^{-1}, \qquad R_{p-1} = -1$$

(since the coefficient of x^{p-2} in $(x^p-1)/(x-1)$ is 1). In general, α^k fixes R_ℓ, but not $R_{2\ell}$ (if indeed $\ell < p-1$). Therefore the fixed field of $\langle\alpha^k\rangle$ is precisely $\mathbb{Q}(R_\ell)$, and we have the Galois correspondence in Table 2. As $R_2 = \zeta+\zeta^{-1}$, so $R_2\cdot\zeta^{\pm1} = \zeta^{\pm2}+1$, and therefore ζ and ζ^{-1} are the solutions of

$$x^2 - R_2\cdot x + 1 = 0. \tag{7}$$

[†]The only way 2^k+1 can be prime is if k is a power of 2. The Fermat number $2^{2^m}+1$ is apparently [3] known to be prime when $0\leqslant m\leqslant 4$, but composite when $5\leqslant m\leqslant 32$. It is also composite for certain m as large as 2478782; but its status is unknown when $m = 33$.

We have seen how to obtain the minimal polynomial of R_2 by means of the substitution (3) in $\sum_{k=0}^{p-1} x^k/x^{(p-1)/2}$. When $p = 5$, this is all we need do to find the roots of $x^p - 1$. When $p = 17$, more work is needed. As it happens, this work is done in Hardy & Wright [2, §5.8, pp. 57–62], though not explicitly with the theoretical framework made possible by Gauss.

5 Periods

Let us still suppose $k \cdot \ell = p - 1 = 2^{2^m}$, and now also $\ell < p - 1$. So R_ℓ is quadratic over $\mathbb{Q}(R_{2\ell})$. Moreover, the conjugate of R_ℓ over this field is $R_{2\ell} - R_\ell$. This is a sum indexed by the coset of $\langle \alpha^k \rangle$ in $\langle \alpha^{k/2} \rangle$. In general, if $s \in (\mathbb{Z}/(p))^\times$, let us define

$$R_{(\ell,s)} = \sum_{x \in \langle r^k \rangle s} \zeta^x = \sum_{\xi \in \langle \alpha^k \rangle \sigma_s} \xi(\zeta).$$

In Gauss's terminology [1, §VII, ¶343], which Hardy and Wright also use, this is a **period.** By the Galois correspondence, we must have

$$\mathbb{Q}(R_{(\ell,s)}) = \mathbb{Q}(R_\ell).$$

Also, $R_{(\ell,1)} = R_\ell$, and the conjugate of R_ℓ over $\mathbb{Q}(R_{2\ell})$ is some $R_{(\ell,s)}$, where $R_{(\ell,s)} + R_\ell = R_{2\ell}$. Then the minimal polynomial of R_ℓ over $\mathbb{Q}(R_{2\ell})$ takes the form

$$x^2 - R_{2\ell} x + R_\ell \cdot R_{(\ell,s)}$$

for some s. The minimal polynomials for other periods are similar. We shall be able to understand the constant terms of these by means of one of Gauss's observations. To avoid superscripts, let us denote ζ^x also by $\exp x$. (One might write $\exp_\zeta(x)$ to be precise.) Then

$$R_{(\ell,s)} = \sum_{j \in \mathbb{Z}/(\ell)} \exp(r^{jk} \cdot s).$$

This makes sense also when $s = 0$, and then we have

$$R_{(\ell,0)} = \ell.$$

Indeed, the definition of $R_{(\ell,s)}$ makes sense whenever $k \cdot \ell = \phi(n)$ for some n of which r is a primitive root. The following is [1, §VII, ¶345].

Theorem (Gauss)**.** *Suppose n has primitive root r, and $k \cdot \ell = \phi(n)$. Then*

$$R_{(\ell,s)} \cdot R_{(\ell,t)} = \sum_{x \in \langle r^k \rangle s} R_{(\ell,x+t)}. \tag{8}$$

x	0	1	2	3	4	5	6	7	(mod 16)
3^x	1	3	−8	−7	−4	5	−2	−6	(mod 17)
3^{8+x}	−1	−3	8	7	4	−5	2	6	(mod 17)

Table 3: Powers of 3 *modulo* 17

Proof. Just compute:

$$\begin{aligned} R_{(\ell,s)} \cdot R_{(\ell,t)} &= \sum_{(i,j)\in(\mathbb{Z}/(\ell))^2} \exp(r^{ik}\cdot s + r^{jk}\cdot t) \\ &= \sum_{(i,j)\in(\mathbb{Z}/(\ell))^2} \exp(r^{jk}\cdot (r^{(i-j)k}\cdot s + t)) \\ &= \sum_{(i,j)\in(\mathbb{Z}/(\ell))^2} \exp(r^{jk}\cdot (r^{ik}\cdot s + t)) \end{aligned}$$

since $(i,j) \mapsto (i-j,j)$ is a permutation of $(\mathbb{Z}/(\ell))^2$. Hence

$$R_{(\ell,s)} \cdot R_{(\ell,t)} = \sum_{i\in\mathbb{Z}/(\ell)} \sum_{j\in\mathbb{Z}/(\ell)} \exp(r^{jk}\cdot (r^{ik}\cdot s + t)) = \sum_{i\in\mathbb{Z}/(\ell)} R_{(\ell, r^{ik}\cdot s + t)},$$

which yields the claim. □

6 The heptakaidecagon

Henceforth let $n = p = 17$. We want to find the roots of (5). These are the vertices of a regular heptadecagon, or heptakaidecagon (Fig. 3; the Greek for 17 is **ἑπτακαίδεκα,** *seven and ten*). Let r be the primitive root 3 of 17. The powers of 3 are in Table 3. The Galois correspondence now is in Table 4. We aim to express generators of the subfields of $\mathbb{Q}(\zeta)$ by radicals. Towards this end, we can arrange the powers of 3 according to the cosets of subgroups of $\mathbb{Z}/(16)$, as in Table 5. Hence the distinct sums $R_{(\ell,s)}$ are the nodes of the tree in Table 6. In applying Gauss's theorem, it will be useful to note that $R_{(2,-s)} = R_{(2,s)}$ and to have some other such equations, as in Table 7. (In practice, it may be easier just to refer to Table 5.) We have already seen that ζ and ζ^{-1} are the solutions of (7). In particular,

$$\zeta^{\pm 1} = \frac{R_2 \pm \sqrt{({R_2}^2 - 4)}}{2}. \tag{9}$$

So we want now to find R_2 by radicals. From Table 6, we have

$$R_2 + R_{(2,4)} = R_4.$$

From (8) and Tables 3 and 6, we have

$$R_2 \cdot R_{(2,4)} = \sum_{x\in\langle 3^8\rangle} R_{(2,x+4)} = R_{(2,5)} + R_{(2,3)} = R_{(4,3)}.$$

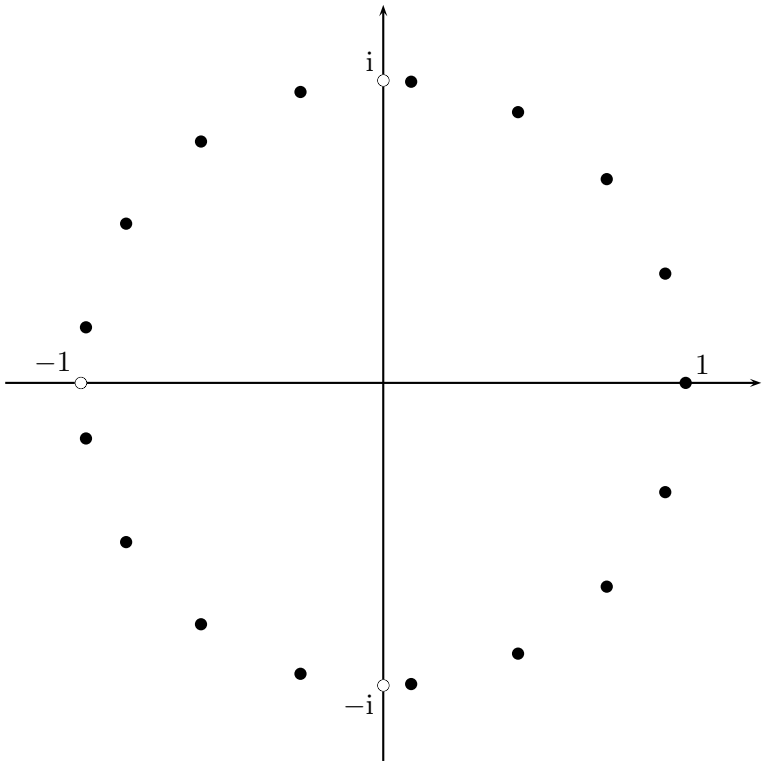

Figure 3: The seventeen 17th roots of 1

Therefore R_2 and $R_{(2,4)}$ are the solutions of

$$x^2 - R_4 \cdot x + R_{(4,3)} = 0. \tag{10}$$

The two solutions are real, and R_2 is the greater (Fig. 4). Hence

$$R_2 = \frac{R_4 + \sqrt{({R_4}^2 - 4R_{(4,3)})}}{2}.$$

To find $R_{(4,3)}$, we have

$$R_{(4,3)} + R_{(4,6)} = R_{(8,3)},$$

as well as

$$\begin{aligned} R_{(4,3)} \cdot R_{(4,6)} = \sum_{x \in \langle 3^4 \rangle 3} R_{(4,x+6)} &= R_{(4,3+6)} + R_{(4,-3+6)} + R_{(4,5+6)} + R_{(4,-5+6)} \\ &= R_{(4,-8)} + R_{(4,3)} + R_{(4,-6)} + R_{(4,1)} \\ &= R_{(4,8)} + R_{(4,3)} + R_{(4,6)} + R_{(4,1)} = -1. \end{aligned}$$

Hence $R_{(4,3)}$ and $R_{(4,6)}$ are the solutions of

$$x^2 - R_{(8,3)} \cdot x - 1 = 0. \tag{11}$$

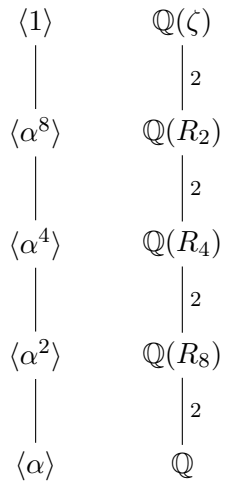

Table 4: The Galois correspondence for $\mathbb{Q}(\exp(2\pi\mathrm{i}/17))$

x	0	4	2	6	1	5	3	7	$(\mathrm{mod}\,16)$
3^x	1	-4	-8	-2	3	5	-7	-6	$(\mathrm{mod}\,17)$
3^{8+x}	-1	4	8	2	-3	-5	7	6	$(\mathrm{mod}\,17)$

Table 5: Powers of 3 again, in cosets

The greater is $R_{(4,3)}$ (Fig. 5); so

$$R_{(4,3)} = \frac{R_{(8,3)} + \sqrt{({R_{(8,3)}}^2 + 4)}}{2}.$$

Similarly,

$$\begin{aligned} R_4 + R_{(4,2)} &= R_8, \\ R_4 \cdot R_{(4,2)} &= \sum_{x \in \langle 3^4 \rangle} R_{(4,x+2)} = R_{(4,3)} + R_{(4,1)} + R_{(4,6)} + R_{(4,-2)} \\ &= R_{(4,3)} + R_{(4,1)} + R_{(4,6)} + R_{(4,2)} = -1, \end{aligned}$$

so R_4 and $R_{(4,2)}$ are the solutions of

$$x^2 - R_8 \cdot x - 1 = 0, \tag{12}$$

and R_4 is the greater (Fig. 6), so

$$R_4 = \frac{R_8 + \sqrt{({R_8}^2 + 4)}}{2}.$$

It remains to find R_8 and $R_{(8,3)}$. We have

$$R_8 + R_{(8,3)} = -1,$$

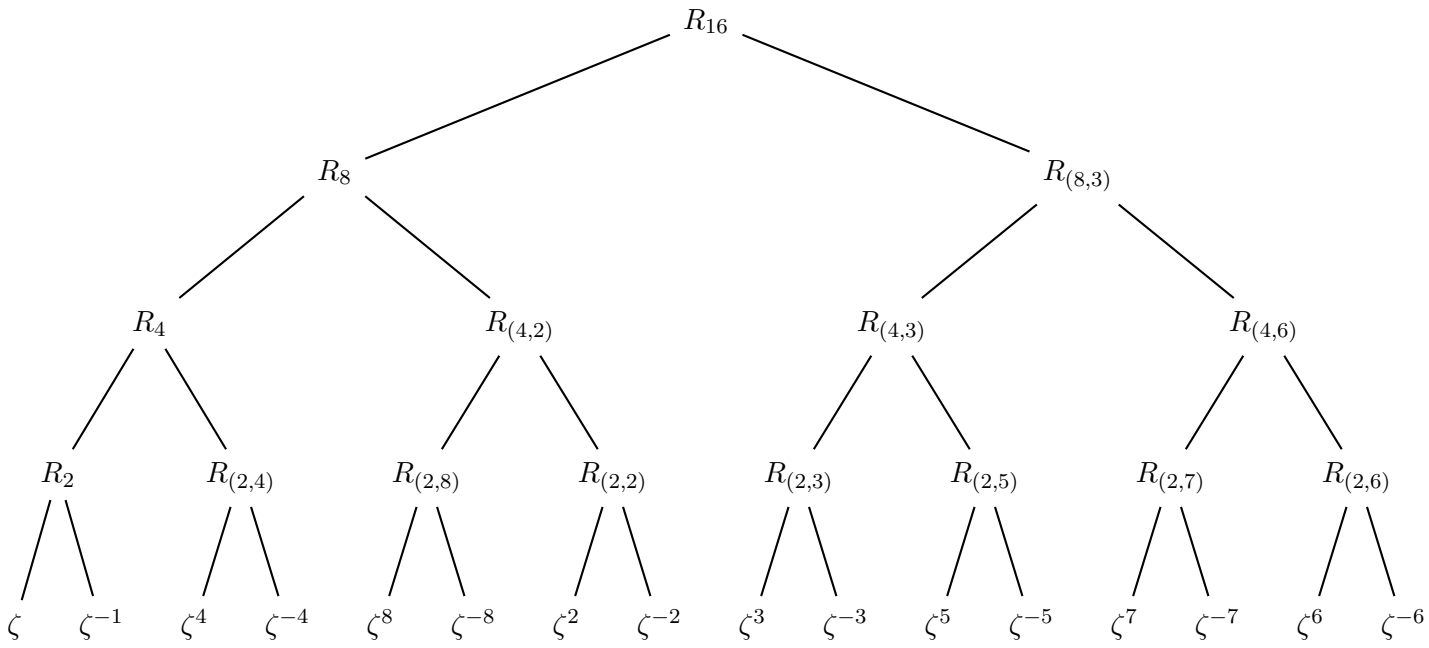

Table 6: Tree of periods

	8	6	−7	4	−3	7	3	2	$\log(-x) \pmod{16}$
	0	−2	1	−4	5	−1	−5	−6	$\log x \pmod{16}$
0	1	2	3	4	5	6	7	8	$x \pmod{17}$
0	1	2	3	1	3	6	6	2	y, where $R_{(4,y)} = R_{(4,\pm x)}$
0	1	1	3	1	3	3	3	1	y, where $R_{(8,y)} = R_{(8,\pm x)}$

Table 7: Which periods are which

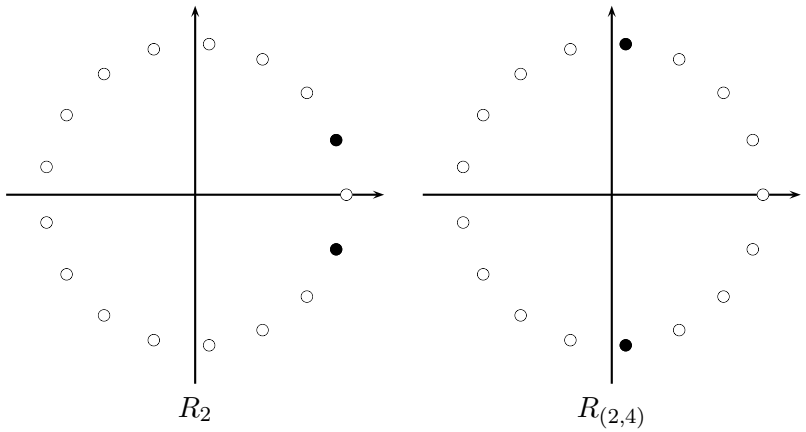

Figure 4: The order-2 subgroup and a coset

and also

$$\begin{aligned} R_8 \cdot R_{(8,3)} &= \sum_{x \in \langle 3^2 \rangle} R_{(8,x+3)} \\ &= R_{(8,4)} + R_{(8,2)} + R_{(8,-1)} + R_{(8,7)} + R_{(8,-5)} + R_{(8,-6)} + R_{(8,1)} + R_{(8,5)} \\ &= R_8 + R_8 + R_8 + R_{(8,3)} + R_{(8,3)} + R_{(8,3)} + R_8 + R_{(8,3)} \\ &= 4 \cdot (R_8 + R_{(8,3)}) = -4. \end{aligned}$$

Hence R_8 and $R_{(8,3)}$ are the solutions of

$$x^2 + x - 4 = 0; \tag{13}$$

as R_8 is the greater (Fig. 7), we have

$$R_8 = \frac{-1 + \sqrt{17}}{2}, \qquad R_{(8,3)} = \frac{-1 - \sqrt{17}}{2}.$$

In sum, we have the equations in Table 8. Now we can in principle work backwards to obtain ζ explicitly by radicals.

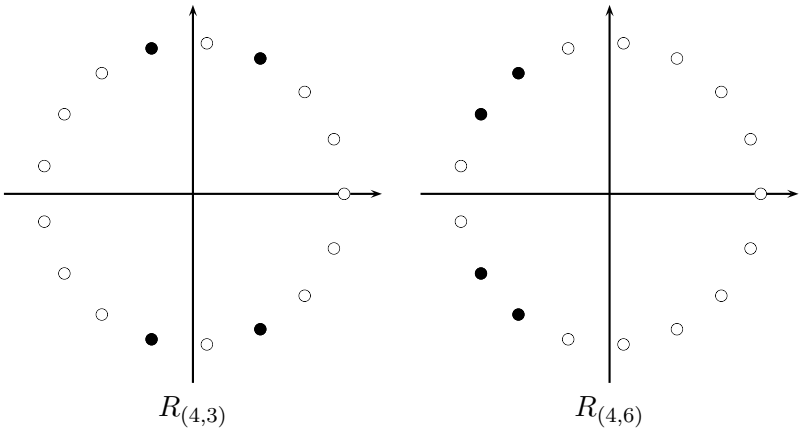

Figure 5: Two order-4 cosets

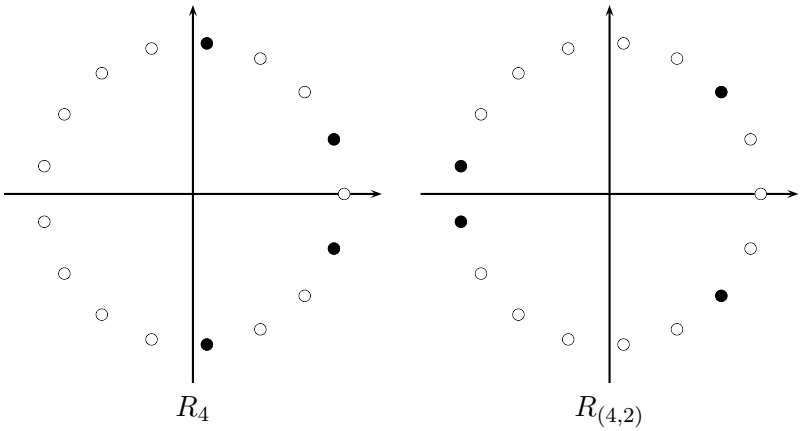

Figure 6: The order-4 subgroup and a coset

7 Clean-up

We may wish to avoid having to use $R_{(4,3)}$ and $R_{(8,3)}$ in finding ζ. To this end, we observe

$$\begin{aligned} R_4 \cdot R_{(4,3)} = \sum_{x \in \langle 3^4 \rangle} R_{(4,x+3)} &= R_{(4,4)} + R_{(4,2)} + R_{(4,-1)} + R_{(4,7)} \\ &= R_4 + R_{(4,2)} + R_4 + R_{(4,6)}; \end{aligned}$$

but since also $R_4 + R_{(4,2)} + R_{(4,3)} + R_{(4,6)} = -1$, we have

$$R_4 \cdot R_{(4,3)} = R_4 - R_{(4,3)} - 1, \qquad R_{(4,3)} = \frac{R_4 - 1}{R_4 + 1}.$$

Also,

$$R_4{}^2 = R_8 \cdot R_4 + 1, \qquad R_8{}^2 = 4 - R_8.$$

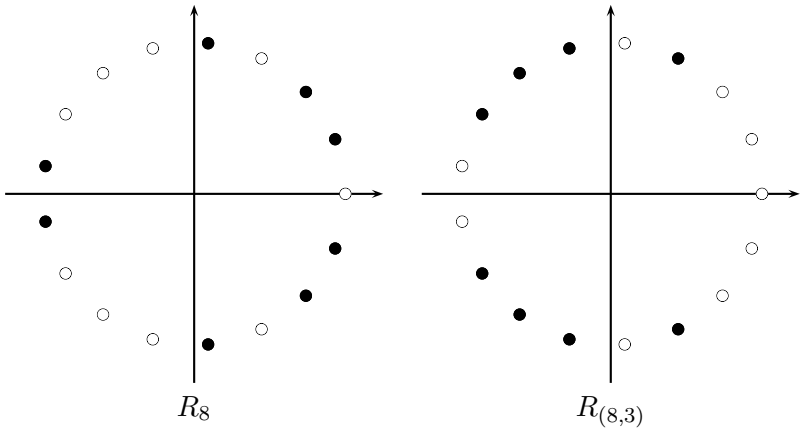

Figure 7: The order-8 subgroup and its coset

Hence, towards an alternative expression for R_2, we have

$$\begin{aligned} {R_4}^2 - 4R_{(4,3)} &= R_8 \cdot R_4 + 1 - 4 \cdot \frac{R_4 - 1}{R_4 + 1} \\ &= \frac{R_8 \cdot {R_4}^2 + R_8 \cdot R_4 + R_4 + 1 - 4R_4 + 4}{R_4 + 1} \\ &= \frac{{R_8}^2 \cdot R_4 + R_8 + R_8 \cdot R_4 - 3R_4 + 5}{R_4 + 1} \\ &= \frac{4R_4 - R_8 \cdot R_4 + R_8 + R_8 \cdot R_4 - 3R_4 + 5}{R_4 + 1} = \frac{R_4 + R_8 + 5}{R_4 + 1}. \end{aligned}$$

Likewise, for ζ itself, we have

$$\begin{aligned} {R_2}^2 - 4 = R_4 \cdot R_2 - \frac{R_4 - 1}{R_4 + 1} - 4 &= \frac{{R_4}^2 \cdot R_2 + R_4 \cdot R_2 - R_4 + 1 - 4R_4 - 4}{R_4 + 1} \\ &= \frac{R_8 \cdot R_4 \cdot R_2 + R_4 \cdot R_2 + R_2 - 5R_4 - 3}{R_4 + 1}. \end{aligned}$$

The situation is now as in Table 9.

References

[1] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn., 1966.

[2] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[3] Wilfrid Keller. Prime factors $k \cdot 2n+1$ of fermat numbers F_m and complete factoring status. `http://www.prothsearch.net/fermat.html`. Accessed December 10, 2007.

x	x	$f(x) = 0$	source
ζ	$\frac{R_2 + \sqrt{({R_2}^2 - 4)}}{2}$	$x^2 - R_2 \cdot x + 1 = 0$	(7)
R_2	$\frac{R_4 + \sqrt{({R_4}^2 - 4R_{(4,3)})}}{2}$	$x^2 - R_4 \cdot x + R_{(4,3)} = 0$	(10)
$R_{(4,3)}$	$\frac{R_{(8,3)} + \sqrt{({R_{(8,3)}}^2 + 4)}}{2}$	$x^2 - R_{(8,3)} \cdot x - 1 = 0$	(11)
R_4	$\frac{R_8 + \sqrt{({R_8}^2 + 4)}}{2}$	$x^2 - R_8 \cdot x - 1 = 0$	(12)
$R_{(8,3)}$	$\frac{-1 - \sqrt{17}}{2}$	$x^2 + x - 4 = 0$	(13)
R_8	$\frac{-1 + \sqrt{17}}{2}$	$x^2 + x - 4 = 0$	(13)

Table 8: The equations for exp(2πi/17)

x	x	$f(x) = 0$
ζ	$\frac{1}{2}\left(R_2 + \sqrt{\frac{R_8 \cdot R_4 \cdot R_2 + R_4 \cdot R_2 + R_2 - 5R_4 - 3}{R_4 + 1}}\right)$	$x^2 - R_2 \cdot x + 1 = 0$
R_2	$\frac{1}{2}\left(R_4 + \sqrt{\frac{R_4 + R_8 + 5}{R_4 + 1}}\right)$	$x^2 - R_4 \cdot x + \frac{R_4 - 1}{R_4 + 1} = 0$
R_4	$\frac{R_8 + \sqrt{(8 - R_8)}}{2}$	$x^2 - R_8 \cdot x - 1 = 0$
R_8	$\frac{-1 + \sqrt{17}}{2}$	$x^2 + x - 4 = 0$

Table 9: The equations for exp(2πi/17), again