Computations of some cyclotomic units in Z[ζ]

Martin Rupp

SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

18/June/2023

Contents

Abstract

We present some elementary computations involved with the inverse of the cyclotomic units $S(p,k) = 1 + \zeta + \zeta^2 + \ldots + \zeta^k$ in $\mathbb{Z}[\zeta]$ where ζ is a $p^t h$-root of unity ζ_p ($\zeta^p = 1$), p a prime and $k < p - 1$. The goal is to 'play a little' with some of the cyclotomic units.

1 case $k = 1$

We start with $S = S(\zeta, 1) = \frac{1}{1+\zeta}$. If S has an inverse in $\mathbb{Z}[\zeta]$, it must be :

$$S^{-1} = \sum_{i=1...p-2} a_i \zeta^i, a_i \in \mathbb{Z}$$

Note: We have

$$1 + \zeta + ...\zeta^{p-1} = 0$$

.

We can try to solve that equation for simple values of p. For example we try $p = 3$.

1.1 $p = 3$

We must have :

$$1 = (1 + \zeta)(a_0 + a_1\zeta)$$

This leads to:

$$1 = a_0 + (a_1 + a_0)\zeta + a_1\zeta^2$$

or

$$0 = a_0 - 1 - a_1 + a_0\zeta$$

since $1 + \zeta + \zeta^2 = 0$.
We get $a_0 = 0$ and $a_1 = -1$. So that:

$$\frac{1}{1 + \zeta} = -\zeta$$

Which is indeed straightforward to check since this leads to

$$1 = -(1 + \zeta)(\zeta) = -\zeta - \zeta^2$$

Now we try with $p = 5$.

1.2 $p = 5$

We use the same technique and we get:

$$1 = (1+\zeta)(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)$$

This leads to:

$$0 = a_0 - 1 - a_3 + (a_0 + a_1 - a_3)\zeta + (a_1 + a_2 - a_3)\zeta^2 + a_2\zeta^3$$

Which resolves as $a_0 = 0, a_1 = -1, a_2 = 0, a_3 = -1$
Then:

$$\frac{1}{1+\zeta} = -\zeta - \zeta^3$$

We can verify that computation by checking that, indeed:

$$1 = (1+\zeta)(-\zeta - \zeta^3) = -\zeta - \zeta^2 - \zeta^3 - \zeta^4$$

1.3 $p > 5$

We can identify a general pattern which consists in using the identity $1 = -\zeta - \zeta^2 \ldots - \zeta^{p-1} = (1+\zeta)(-\zeta - \zeta^3 \ldots - \zeta^{p-2})$ so that, in general:

$$\frac{1}{1+\zeta} = -\zeta - \zeta^3 \ldots - \zeta^{p-2}$$

We can also have tried to determine directly the coefficients $a_0 \ldots a_{p-2}$ by solving the equations:

$$\begin{aligned} a_0 - a_{p-2} - 1 = 0; \\ a_{p-3} = 0; \\ a_{i-1} + a_i - a_{i-2} = 0; (i = 2 \ldots p-3). \end{aligned}$$

2 case $k = 2$

2.1 $p \equiv 1(\mod 3)$

We now try to compute $S^{-1} = \frac{1}{1+\zeta+\zeta^2}$.

We could try to consider - again - the sum $-\zeta - \zeta^4 \ldots - \zeta^{3i+1} \ldots$ as a possible candidate for S^{-1}. This will work *only* if $p \equiv 1(\mod 3)$.

In the case where $p \equiv -1(\mod 3)$, we have to find an other method.

Again we try small values of p (but such that $p \equiv 1(\mod 3)$) in order to find a hint.

2.2 $p = 5$

In that case, we have to solve the equation:

$$1 = (1 + \zeta + \zeta^2)(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)$$
$$(a_0, a_1, a_2, a_3) \in \mathbb{Z}.$$

This leads to:

$$1 = a_0 - a_2 + (a_1 + a_0 - a_2 - a_3)\zeta + (a_1 + a_0 - a_3)\zeta^2 + a_1\zeta^3$$

which has a solution as: $a_0 = a_3 = 1; a_1 = a_2 = 0$.
Then we get finally:

$$\frac{1}{1 + \zeta + \zeta^2} = 1 + \zeta^3$$

Which is also straightforward to verify since this is equivalent to:

$$1 = (1 + \zeta + \zeta^2)(1 + \zeta^3) = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5$$

2.3 $p \equiv -1(\mod 3)$

Once again, we identify a pattern, which involves the identify

$$1 + \zeta + \zeta^2 + \dots \zeta^p = (1 + \zeta + \zeta^2)(1 + \zeta^3 + \zeta^6 + \dots \zeta^{3i} + \dots \zeta^{p-2})$$

(which is possible since $p \equiv -1(\mod 3)$)

3 computation of S^{-1} for some special values of k and p

3.1 $p \equiv \pm 1(\mod k + 1)$

The two methods developed before will work in the general case when $k$and p are linked by the relation:

$$p \equiv \pm 1(\mod k + 1)$$

- if $p \equiv 1(\mod k + 1)$ then for $p = u(k + 1) + 1$:

$$\frac{1}{1+\zeta+\dots\zeta^k} = -\zeta - \zeta^{k+2} - \zeta^{2(k+1)+1} \dots - \zeta^{(u-1)(k+1)+1}$$

- if $p \equiv -1(\mod k+1)$ then for $p = u(k+1)-1$:

$$\frac{1}{1+\zeta+\dots\zeta^k} = 1 + \zeta^{k+1} + \zeta^{2(k+1)} \dots + \zeta^{(u-1)(k+1)}$$

Besides these cases where p and k are linked by a special relationship, there does not seems to have a way to compute S^{-1} so we try again a direct computation in the case of $k = 4$ and $p = 13$, since in that precise case $13 \equiv 3(\mod 5)$ what doesn't fits in the previous schemes.

3.2 $k = 4$ and $p = 13$

We must solve

$$1 = (1+\zeta+\zeta^2+\zeta^3+\zeta^4)(a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3+a_4\zeta^4+a_5\zeta^5+a_6\zeta^6+a_7\zeta^7+a_8\zeta^8+a_9\zeta^9+a_{10}\zeta^{10}+a_{11}\zeta^{11})$$

we then need to distribute the 5 powers of ζ to the left part of the equation. This will involves 60 computations so we stream these computations inside the following table.

We display a table where we fill in the cell (i, j), the value of a_j's for the i^th power of ζ (e.g : $\zeta^0 \dots \zeta^k$).

1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6	ζ^7	ζ^8	ζ^9	ζ^{10}	ζ^{11}
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}
$-a_{11}$	$a_0 - a_{11}$	$a_1 - a_{11}$	$a_2 - a_{11}$	$a_3 - a_{11}$	$a_4 - a_{11}$	$a_5 - a_{11}$	$a_6 - a_{11}$	$a_7 - a_{11}$	$a_8 - a_{11}$	$a_9 - a_{11}$	$a_{10} - a_{11}$
$a_{11} - a_{10}$	$-a_{10}$	$a_0 - a_{10}$	$a_1 - a_{10}$	$a_2 - a_{10}$	$a_3 - a_{10}$	$a_4 - a_{10}$	$a_5 - a_{10}$	$a_6 - a_{10}$	$a_7 - a_{10}$	$a_8 - a_{10}$	$a_9 - a_{10}$
$a_{10} - a_9$	$a_{11} - a_9$	$-a_9$	$a_0 - a_9$	$a_1 - a_9$	$a_2 - a_9$	$a_3 - a_9$	$a_4 - a_9$	$a_5 - a_9$	$a_6 - a_9$	$a_7 - a_9$	$a_8 - a_9$
$a_9 - a_8$	$a_{10} - a_8$	$a_{11} - a_8$	$-a_8$	$a_0 - a_8$	$a_1 - a_8$	$a_2 - a_8$	$a_3 - a_8$	$a_4 - a_8$	$a_5 - a_8$	$a_6 - a_8$	$a_7 - a_8$
$a_0 - a_8$	$a_0 + a_1 - a_8 - a_9$	$a_0 + a_1 + a_2 - a_8 - a_9 - a_{10}$	$a_0 + a_1 + a_2 + a_3 - a_8 - a_9 - a_{10} - a_{11}$	$a_0 + a_1 + a_2 + a_3 + a_4 - a_8 - a_9 - a_{10} - a_{11}$	$a_1 + a_2 + a_3 + a_4 - a_8 - a_9 - a_{10} - a_{11}$	$a_2 + a_3 + a_4 + a_5 - a_8 - a_9 - a_{10} - a_{11}$	$a_3 + a_4 + a_5 + a_6 - a_8 - a_9 - a_{10} - a_{11}$	$a_4 + a_5 + a_6 + a_7 - a_8 - a_9 - a_{10} - a_{11}$	$a_5 + a_6 + a_7 - a_9 - a_{10} - a_{11}$	$a_6 + a_7 - a_9 - a_{10} - a_{11}$	$a_7 - a_{11}$

We solve that system of equations very easily and we find that the only non-null terms are:

$$a_0 = a_4 = a_8 = -1$$

hence :

$$\frac{1}{1+\zeta+\zeta^2+\zeta^3+\zeta^4} = -\zeta - \zeta^3 - \zeta^6 - \zeta^8 - \zeta^{11}$$

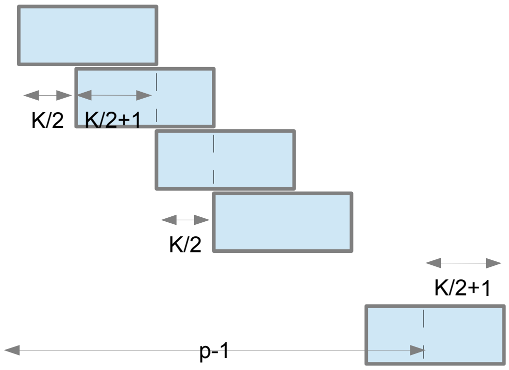
We see that - again - there is a pattern which seems to be close to the previous patterns we saw but this is slightly different :

$--$	$--$	$--$	$--$	$--$										
$-\zeta$	$-\zeta^2$	$-\zeta^3$	$-\zeta^4$	$-\zeta^5$										
$--$	$--$	$--$	$--$	$--$										
		$--$	$--$	$--$	$--$	$--$								
		$-\zeta^3$	$-\zeta^4$	$-\zeta^5$	$-\zeta^6$	$-\zeta^7$								
		$--$	$--$	$--$	$--$	$--$								
					$--$	$--$	$--$	$--$	$--$					
					$-\zeta^6$	$-\zeta^7$	$-\zeta^8$	$-\zeta^9$	$-\zeta^{10}$					
					$--$	$--$	$--$	$--$	$--$					
							$--$	$--$	$--$	$--$	$--$			
							$-\zeta^8$	$-\zeta^9$	$-\zeta^{10}$	$-\zeta^{11}$	$-\zeta^{12}$			
							$--$	$--$	$--$	$--$	$--$			
										$--$	$--$	$--$	$--$	$--$
										$-\zeta^{11}$	$-\zeta^{12}$	-1	$-\zeta$	$-\zeta^2$
										$--$	$--$	$--$	$--$	$--$

We indeed can identify a pattern where the sum $1 = 2(-\zeta - \zeta^2 \ldots - \zeta^{p-1}) - 1$ is been created by juxtaposing '5-length' blocks with common intersections. The end of a block i is the start of the block $i+2$. And the end of the blocks must insert with the beginning of the blocks by removing one last element...

That will work only for a special value of the 'shift' between the block i and the block $i+1$.

4 use of patterns



We aim at reproducing the same pattern by shifting a block of $k+1$ (consecutive) 'bricks' (one such 'brick' being a $-\zeta^i$ for some integer i) by a length of l. At the end of the process we must have obtain a piece of block of length $k+1-l$ and this means there must be an *odd* amount of blocks. Besides this is clearly possible to connect the last 'protuberant' piece of the blocks (minus one 'brick') to the start of the chain only if $k+1-l = l+1$ Besides, the process of forming blocks ends when the "horizontal distance" between the start of the first block and the end of the penultimate block is $p-1$.

we must have then $k = 2l$ what means that k must be even.

That leads to $N(k+1) + k/2 = p - 1$ or $p \equiv (k/2) + 1 (\mod k+1)$

Note that this is still a progress because this is a more general case since in the case $k = 2$, this leads to $p \equiv -1 (\mod 3)$ and we find the previous result.

Indeed for the case when $k = 2$ (and only for that case), the last coefficient in the factoring term is in ζ^{p-1} what means we have to turn the coefficients that are 0 into coefficients that are $+1$ and the coefficients that are -1 into coefficients that are 0.

For example when we take $k = 2$ and $p = 5$ like we did previously $(5 \equiv 2/2 + 1 (\mod (2+1)))$, we get:

$$
\begin{array}{cccccc}
-- & -- & -- & & & \\
-\zeta & -\zeta^2 & -\zeta^3 & & & \\
-- & -- & -- & & & \\
 & -- & -- & -- & & \\
 & -\zeta^2 & -\zeta^3 & -\zeta^4 & & \\
 & -- & -- & -- & & \\
 & & & -- & -- & -- \\
 & & & -\zeta^4 & -1 & -\zeta \\
 & & & -- & -- & --
\end{array}
$$

We get $-\zeta - \zeta^2 - \zeta^4 = 1 + \zeta^3$.

If $k = 4$, we can invert $1 + \zeta + \zeta^2 + \zeta^3$ that way for all p such that $p \equiv 3(\mod 5)$, and so on ...

5 General case

In order to compute the inverse of $1+\zeta+\ldots\zeta^k$ we could consider the following 'technique' (see [Washington], Lemma 1.3):

$$1 + \zeta + \ldots \zeta^k = \frac{1 - \zeta^{k+1}}{1 - \zeta} \in \mathbb{Z}$$

.

Then we must have:

$$\frac{1}{1 + \zeta + \ldots \zeta^k} = \frac{1 - \zeta}{1 - \zeta^{k+1}}$$

.

We can find $s \in \mathbb{Z}$ such that: $1 = s(k+1)(\mod p)$.

Indeed following Bezout's theorem , since $k+1$ and p are primes between each others, there exists (s,t) in $\mathbb{Z}$ such that $s(k+1) + tp = 1$.

Then we can write:

$$\frac{1 - \zeta}{1 - \zeta^{k+1}} = \frac{1 - \zeta^{s(k+1)}}{1 - \zeta^{k+1}}$$

In the case where $s > 0$, this leads to:

$$1 + \zeta^{k+1} + \zeta^{2(k+1)} + \ldots + \zeta^{(k+1)(s-1)}$$

.

In the case where $s < 0$, this leads to:

$$-\zeta^{(k+1)s}(1 + \zeta^{-(k+1)} + \zeta^{-2(k+1)} + \ldots + \zeta^{(k+1)(-s-1)})$$

.

or, equivalently:

$$-\zeta^{(k+1)s} - \zeta^{(k+1)(s-1)} - \zeta^{(k+1)(s-2)} + \ldots - \zeta^{-(k+1)}$$

It has to be noticed that all coefficients in the sums are unique since $is \equiv js(\mod p$ implies that $i = j$ otherwise we would have that $s|p$. This infers that the coordinates of the inverse are only $-1, +1$ or 0.

So the process here is twofold:

1) Compute s using the extended Euclidean algorithm.

2) Compute the residues of $i(k+1)$ modulo p for $i = 1 \dots s-1$ if $s > 0$ and for $i = s \dots -1$ if $s < 0$.

So far that doesn't give a generic , 'global' formula because it depends on a series of algorithmic computations, same as the way we computed the "coordinates" a_i $i = 0, 1, \dots, p-2$.

For example, we consider again, $p = 13$ and $k = 4$. We have $-5 \times (k+1) + 2 \times p = 1$ so:

$$\frac{1}{1+\zeta+\zeta^2+\zeta^3+\zeta^4} = -\zeta^{-25}(1+\zeta^5+\zeta^{10}+\zeta^{15}+\zeta^{20}).$$

This leads to:

$$-\zeta - \zeta^3 - \zeta^6 - \zeta^8 - \zeta^{11}$$

.

and we find the result that we knew already.

The computation of s from k and p has logarithmic time complexity. We then compute several values here of the coefficients of the inverse.

p=11
1/S(1,11)=-ζ -ζ^3 -ζ^5 -ζ^7 -ζ^9 ($s = -5$)
1/S(2,11)=1 +ζ^3 +ζ^6 +ζ^9 ($s = 4$)
1/S(3,11)=1 +ζ^4 +ζ^8 ($s = 3$)
1/S(4,11)=-ζ -ζ^6 ($s = -2$)
1/S(5,11)=1 +ζ^6 ($s = 2$)
1/S(6,11)=-ζ -ζ^4 -ζ^8 ($s = -3$)
1/S(7,11)=-ζ -ζ^3 -ζ^6 -ζ^9 ($s = -4$)
1/S(8,11)=1 +ζ^3 +ζ^5 +ζ^7 +ζ^9 ($s = 5$)
1/S(9,11)=-ζ ($s = -1$)
p=13
1/S(1,13)=-ζ -ζ^3 -ζ^5 -ζ^7 -ζ^9 -ζ^{11} ($s = -6$)
1/S(2,13)=-ζ -ζ^4 -ζ^7 -ζ^{10} ($s = -4$)
1/S(3,13)=-ζ -ζ^5 -ζ^9 ($s = -3$)
1/S(4,13)=-ζ -ζ^3 -ζ^6 -ζ^8 -ζ^{11} ($s = -5$)
1/S(5,13)=-ζ -ζ^7 ($s = -2$)
1/S(6,13)=1 +ζ^7 ($s = 2$)
1/S(7,13)=1 +ζ^3 +ζ^6 +ζ^8 +ζ^{11} ($s = 5$)
1/S(8,13)=1 +ζ^5 +ζ^9 ($s = 3$)
1/S(9,13)=1 +ζ^4 +ζ^7 +ζ^{10} ($s = 4$)
1/S(10,13)=1 +ζ^3 +ζ^5 +ζ^7 +ζ^9 +ζ^{11} ($s = 6$)

1/S(11,13)=-ζ $(s=-1)$
p=17
1/S(1,17)=-ζ -ζ^3 -ζ^5 -ζ^7 -ζ^9 -ζ^{11} -ζ^{13} -ζ^{15} $(s=-8)$
1/S(2,17)=1 +ζ^3 +ζ^6 +ζ^9 +ζ^{12} +ζ^{15} $(s=6)$
1/S(3,17)=-ζ -ζ^5 -ζ^9 -ζ^{13} $(s=-4)$
1/S(4,17)=1 +ζ^3 +ζ^5 +ζ^8 +ζ^{10} +ζ^{13} +ζ^{15} $(s=7)$
1/S(5,17)=1 +ζ^6 +ζ^{12} $(s=3)$
1/S(6,17)=1 +ζ^4 +ζ^7 +ζ^{11} +ζ^{14} $(s=5)$
1/S(7,17)=-ζ -ζ^9 $(s=-2)$
1/S(8,17)=1 +ζ^9 $(s=2)$
1/S(9,17)=-ζ -ζ^4 -ζ^7 -ζ^{11} -ζ^{14} $(s=-5)$
1/S(10,17)=-ζ -ζ^6 -ζ^{12} $(s=-3)$
1/S(11,17)=-ζ -ζ^3 -ζ^5 -ζ^8 -ζ^{10} -ζ^{13} -ζ^{15} $(s=-7)$
1/S(12,17)=1 +ζ^5 +ζ^9 +ζ^{13} $(s=4)$
1/S(13,17)=-ζ -ζ^3 -ζ^6 -ζ^9 -ζ^{12} -ζ^{15} $(s=-6)$
1/S(14,17)=1 +ζ^3 +ζ^5 +ζ^7 +ζ^9 +ζ^{11} +ζ^{13} +ζ^{15} $(s=8)$
1/S(15,17)=-ζ $(s=-1)$

As a matter of fact, from the observation of these values, we can identify a few more properties:

i)

$$1/S(p-2,p)=-\zeta$$

, this is obvious both from the identity $(1+\zeta+\ldots\zeta^{p-2})(-\zeta)=1$ and from the fact that $-1\times(p-1)+p=1$. In that case, $s=1$.

ii)

If we can divide $p+1$ in equals parts of length $k+1$, what means that $p\equiv -1(\mod k+1)$, then, since $(k+1)|(p+1)$:

$$1/S(k,p)=1+\sum_{i=1}^{i=(p+1)/(k+1)-1}\zeta^{i(k+1)}$$

$(s=\frac{p+1}{k+1})$

iii)

If we can divide $p-1$ in equals parts of length $k+1$, what means that $p\equiv -1(\mod k+1)$, then since $(k+1)|(p-1)$:

$$1/S(k,p)=-\zeta+\sum_{i=1}^{i=(p-1)/(k+1)-1}-\zeta^{i(k+1)}$$

$(s=\frac{p-1}{k+1})$

iv)

If we can use the pattern we described previously , then k is even and $p \equiv k/2+1(\mod (k+1))$ (or equivalently $2p \equiv 1(\mod (k+1))$).

$$1/S(k,p) = -\zeta + \sum_{i=1}^{i=(p-(k/2)-1)/(k+1)} -\zeta^{i(k+1)+(k/2)} - \zeta^{(i+1)(k+1)}$$

$(s = \frac{2p-1}{k+1})$

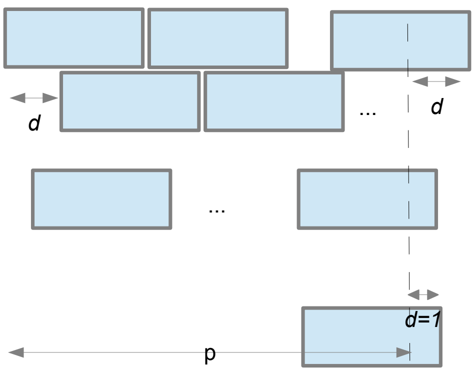
5.1 comment about the patterns

The patterns we identified are then trivially interpreted with the computation of the Bezout coefficients:

In the case $s > 0$, we consider the p powers of ζ from 0 to $p-1$. This is a 'block' of length p. we then consider a sequence of blocks of length $k+1$ that are following each others. Each time that one block reaches the end of the p-block, it starts again, shifted. We stop when the shift value is equals at 1. This happens when we create a 'wall' made of n lines of s $k+1$-blocks such as the shift is '1', e.g. when $s(k+1) = np+1$. Then, since (the sum of the blocks from) one line has value =0, we get the value 1 by summing up all the blocks.

The case $s < 0$ is similar.

The 'patterns' are of course a trivial visualization of the sequence $j(k+1)$, $j = 1 \ldots s$ in $\mathbb{Z}/p\mathbb{Z}$.



6 conclusion

There are no general (non-algorithmic) ways to compute the inverse of $\sum_{i=0}^{i=k} \zeta^i$ in $\mathbb{Z}[\zeta]$. It is possible to identify certain generic patterns that will reach to immediate computation.

References

[Washington] *Introduction to Cyclotomic Fields.*, Springer-Verlag 1982