# ON CYCLOTOMIC NUMBERS OF ORDER SIXTEEN

EMMA LEHMER

It has been shown by Dickson **(1)** that if $(i, j)_8$ is the number of solutions of

$$g^{8\nu+i} + 1 \equiv g^{8\mu+j} \pmod{p},$$

then $64(i, j)_8$ is expressible for each $i, j$, as a linear combination with integer coefficients of $p$, $x$, $y$, $a$, and $b$ where

$$p = x^2 + 4y^2 = a^2 + 2b^2 = 8n + 1,$$

and

$$a \equiv b \equiv 1 \pmod{4},$$

while the sign of $y$ and $b$ depends on the choice of the primitive root $g$. There are actually four sets of such formulas depending on whether $p$ is of the form $16n + 1$ or $16n + 9$ and whether 2 is a quartic residue or not.

We have recently **(2)** written out these formulas in detail and have shown that if 2 is not a quartic residue of $p = 16n + 1$ and if we define the $i$th class as the class containing $t^i$ where

$$t \equiv \sqrt{2} \pmod{p},$$

then the sign of $y$ is such that

$$\tfrac{1}{2}y \equiv -1 \pmod{4}$$

in the formulas for the cyclotomic constants $(i, j)_8$. The sign of $b$ still remains in doubt.

The question has been raised by various people interested in the problem whether or not constants $\alpha$, $\beta$, $\gamma$, $\delta$, $\epsilon$ can be found such that

$$256\ (i, j)_{16} = p + \alpha x + \beta y + \gamma a + \delta b + \epsilon$$

at least for some $i, j$. To settle this problem the following experiment was undertaken on the SWAC.[1] Eight primes $p$ of the form $32n + 1$ for which 2 is not a quartic residue were selected and the $i$th class was defined as before as the class containing $t^i$. (Since $-1$ is a 16-ic residue of such primes, there was no ambiguity of sign in choosing the square root.) The SWAC calculated the 51 independent cyclotomic constants for these eight primes. The remaining 205 constants can be obtained from these by the relations

$$(i, j)_{16} = (j, i)_{16} = (16 - i, j - i)_{16}.$$

Received January 25, 1954.

[1] The National Bureau of Standards Western Automatic Computer for the use of which we are grateful.

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press

Then the constants of order eight could be obtained on the one hand from the relation

$$(i,j)_8 = (i,j)_{16} + (i+8,j)_{16} + (i,j+8)_{16} + (i+8,j+8)_{16},$$

and on the other from the formulas for $(i,j)_8$ in terms of $x$, $y$, $a$, $b$. Comparing these results, proper signs were affixed to $b$ as well as $x$, $y$, and $a$. These decompositions will be found in the table, together with the 51 cyclotomic constants.

Finally, five of the eight primes, namely $p = 193$, 449, 641, 769, and 1409, were selected and an attempt was made to find a simultaneous solution of the five equations of the form

$$\alpha x_\nu + \beta y_\nu + \gamma a_\nu + \delta b_\nu + \epsilon = 256\,A_\nu - p_\nu$$

for $\nu = 1, 2, 3, 4$, and 5, where we let $(i,j)_{16} = A_\nu$ for these primes $p_\nu$ and for fixed $i, j$. We obtain

$$\begin{aligned}
-7\alpha + \phantom{1}6\beta - 11\gamma - \phantom{1}6\delta + \epsilon &= 256A_1 - \phantom{1}193,\\
-7\alpha - 10\beta + 21\gamma + \phantom{1}2\delta + \epsilon &= 256A_2 - \phantom{1}449,\\
25\alpha - \phantom{1}2\beta + 21\gamma - 10\delta + \epsilon &= 256A_3 - \phantom{1}641,\\
25\alpha + \phantom{1}6\beta - 11\gamma + 18\delta + \epsilon &= 256A_4 - \phantom{1}769,\\
25\alpha + 14\beta + 21\gamma + 22\delta + \epsilon &= 256A_5 - 1409.
\end{aligned}$$

Subtracting the first two and the last two we get

$$16\beta - 32\gamma - 8\delta = 256(A_1 - A_2) + 256$$

and

$$8\beta + 32\gamma + 4\delta = 256(A_5 - A_4) - 640.$$

Adding,

$$24\beta - 4\delta = 256(A_1 - A_2 - A_4 + A_5) - 384.$$

From the third and last of the original equations

$$16\beta + 32\delta = 256(A_5 - A_3) - 768.$$

Combining the last two we finally get

$$104\delta = 256(-2A_1 + 2A_2 - 3A_3 + 2A_4 + A_5) - 1536$$

or

$$13\delta = 32(-2A_1 + 2A_2 - 3A_3 + 2A_4 + A_5) - 192.$$

In order that $\delta$ be an integer it is necessary that

$$-2A_1 + 2A_2 - 3A_3 + 2A_4 + A_5 \equiv 6 \pmod{13}.$$

This condition is satisfied only if the constants $A_\nu$ stand for $(4,8)_{16}$ and $(5,10)_{16}$. In these two cases we get the tentative solution

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press

$$256\,(4,8)_{16} = p - 271 - 10x + 8a + 16y$$

and

$$256\,(5,10)_{16} = p - 87 - 18x + 24a + 48y.$$

Unfortunately, neither of these proposed solutions holds for $p = 97$. Hence we must conclude that none of the cyclotomic constants $(i,j)_{16}$ is such that $256(i,j)_{16}$ is expressible as a linear combination with integer coefficients of $p$, $a$, $b$, $x$, $y$, in case $p = 32n + 1$, 2 not a quartic residue and the sign of $b$ taken as consistent with the results on cyclotomic constants of order eight. Other hypotheses may be tested with the information provided by the SWAC, which is contained in the table.

The SWAC has also computed the cyclotomic constants of order sixteen for all other primes less than 1,000, as well as cyclotomic constants of order 24 for the same range.

A similar calculation was undertaken subsequently for primes of the form $32n + 17$. We chose $p = 241, 401, 433, 1009, 1297$, and, as before fixed the signs of $b$ from the formulas giving the cyclotomic numbers of order eight. All these primes are such that $t$, given by

$$t^2 \equiv 2 \pmod{p}, \quad t < \tfrac{1}{2}(p-1),$$

is a non-residue.

The resulting equations are as follows:

$$\begin{aligned}
-15\alpha - 2\beta + 13\gamma + 6\delta + \epsilon &= 256A_1 - 241,\\
\alpha - 10\beta - 3\gamma - 14\delta + \epsilon &= 256A_2 - 401,\\
17\alpha + 6\beta - 19\gamma - 6\delta + \epsilon &= 256A_3 - 433,\\
-15\alpha + 14\beta - 19\gamma - 18\delta + \epsilon &= 256A_4 - 1009,\\
\alpha - 18\beta - 32\gamma + 6\delta + \epsilon &= 256A_5 - 1297.
\end{aligned}$$

Solving these for $\delta$ we get

$$9\delta = 16(2A_1 - 3A_2 + A_3 - A_4 + A_5).$$

Hence the expression $2A_1 - 3A_2 + A_3 - A_4 + A_5 \equiv 0 \pmod 9$ in order to have an integer solution. This was the case only when the $A$'s stood for the cyclotomic constants $(0, 1)$, $(3, 2)$, and $(4, 0)$. In the first case $\beta$ was not an integer, but the remaining two gave tentative solutions

$$256(3,2) = p - 15 + 6x - 8a + 16y$$

and

$$256(4,0) = p + 49 - 10x + 8a + 16y.$$

The first of these was easily disproved from the table for $p = 977$, while the second one held for $p = 977$ and it was necessary to calculate $(4, 0)$ for $p = 1361$. The calculations exhibited eight solutions, while the formula gave only six. So we must regretfully conclude that the cyclotomic constants of order 16 are not expressible in terms of these quadratic partitions alone.

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press

The number $(i, j)$ of solutions of $t^i x^{16} + 1 \equiv t^j y^{16} \pmod{p}$, $t^2 \equiv 2 \pmod{p}$

| $p$ | (0, 0) | (0, 1) | (0, 2) | (0, 3) | (0, 4) | (0, 5) | (0, 6) | (0, 7) | (0, 8) | (0, 9) | (0, 10) | (0, 11) | (0, 12) | (0, 13) | (0, 14) | (0, 15) | (1, 2) | (1, 3) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 97 | 2 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193 | 2 | 0 | 1 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 |
| 449 | 0 | 2 | 1 | 0 | 6 | 4 | 0 | 0 | 2 | 4 | 0 | 4 | 0 | 2 | 0 | 2 | 1 | 2 |
| 641 | 6 | 4 | 1 | 2 | 4 | 4 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 6 | 3 | 1 |
| 673 | 2 | 2 | 3 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 4 | 2 | 6 | 0 | 8 | 2 | 3 | 1 |
| 769 | 2 | 4 | 5 | 0 | 2 | 6 | 4 | 2 | 4 | 0 | 2 | 4 | 4 | 4 | 2 | 2 | 4 | 2 |
| 929 | 0 | 0 | 7 | 2 | 0 | 6 | 6 | 6 | 4 | 4 | 6 | 2 | 8 | 2 | 4 | 0 | 5 | 6 |
| 1409 | 0 | 8 | 5 | 10 | 4 | 10 | 6 | 6 | 8 | 4 | 0 | 4 | 4 | 6 | 10 | 2 | 7 | 3 |

| $p$ | (1, 4) | (1, 5) | (1, 6) | (1, 7) | (1, 8) | (1, 9) | (1, 10) | (1, 11) | (1, 12) | (1, 13) | (1, 14) | (2, 4) | (2, 5) | (2, 6) | (2, 7) | (2, 8) | (2, 9) | (2, 10) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 97 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 193 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 2 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 3 |
| 449 | 2 | 2 | 1 | 4 | 1 | 3 | 1 | 1 | 1 | 3 | 1 | 3 | 2 | 1 | 0 | 3 | 3 | 1 |
| 641 | 2 | 0 | 0 | 2 | 4 | 2 | 1 | 6 | 1 | 3 | 2 | 4 | 5 | 4 | 2 | 2 | 3 | 2 |
| 673 | 2 | 3 | 2 | 4 | 3 | 3 | 3 | 3 | 3 | 1 | 4 | 1 | 3 | 4 | 0 | 1 | 3 | 1 |
| 769 | 3 | 2 | 3 | 3 | 4 | 4 | 0 | 0 | 6 | 2 | 5 | 2 | 4 | 3 | 3 | 2 | 2 | 4 |
| 929 | 4 | 5 | 5 | 4 | 4 | 3 | 2 | 3 | 3 | 6 | 3 | 1 | 2 | 3 | 2 | 4 | 4 | 3 |
| 1409 | 7 | 2 | 5 | 5 | 6 | 8 | 6 | 3 | 9 | 5 | 5 | 7 | 5 | 4 | 3 | 5 | 3 | 3 |

| $p$ | (2, 11) | (2, 12) | (2, 13) | (3, 6) | (3, 7) | (3, 8) | (3, 9) | (3, 10) | (3, 11) | (3, 12) | (4, 8) | (4, 9) | (4, 10) | (4, 11) | (5, 10) | $x$ | $y$ | $a$ | $b$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 97 | 2 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 9 | −2 | 5 | 6 |
| 193 | 0 | 0 | 1 | 1 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | −7 | 6 | −11 | −6 |
| 449 | 3 | 2 | 2 | 3 | 0 | 2 | 2 | 1 | 1 | 2 | 1 | 0 | 3 | 1 | 2 | −7 | −10 | 21 | 2 |
| 641 | 2 | 4 | 1 | 1 | 4 | 4 | 3 | 3 | 3 | 3 | 1 | 2 | 3 | 4 | 2 | 25 | −2 | 21 | −10 |
| 673 | 5 | 1 | 3 | 3 | 5 | 3 | 1 | 3 | 4 | 4 | 4 | 1 | 3 | 0 | 4 | −23 | 6 | 5 | 18 |
| 769 | 4 | 2 | 2 | 2 | 2 | 4 | 4 | 6 | 1 | 5 | 1 | 4 | 6 | 3 | 1 | 25 | 6 | −11 | 18 |
| 929 | 5 | 1 | 7 | 2 | 4 | 4 | 2 | 5 | 2 | 5 | 5 | 2 | 4 | 2 | 4 | −23 | −10 | −27 | 10 |
| 1409 | 8 | 8 | 5 | 3 | 5 | 5 | 7 | 9 | 4 | 6 | 5 | 4 | 8 | 5 | 8 | 25 | 14 | 21 | 22 |

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press

The number $(i, j)$ of solutions of $t^i x^{16} + 1 \equiv t^j y^{16} \pmod{p}$, $t^2 \equiv 2 \pmod{p}$

| $p$ | (0, 0) | (0, 1) | (0, 2) | (0, 3) | (0, 4) | (0, 5) | (0, 6) | (0, 7) | (0, 8) | (0, 9) | (0, 10) | (0, 11) | (0, 12) | (0, 13) | (0, 14) | (0, 15) | (1, 0) | (1, 1) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 241 | 0 | 0 | 1 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 2 |
| 401 | 2 | 0 | 5 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 3 | 1 |
| 433 | 2 | 0 | 5 | 2 | 2 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 2 | 2 | 1 | 2 |
| 977 | 4 | 2 | 3 | 6 | 4 | 6 | 6 | 4 | 0 | 2 | 8 | 4 | 6 | 2 | 2 | 2 | 5 | 4 |
| 1009 | 4 | 2 | 9 | 4 | 4 | 2 | 4 | 0 | 2 | 8 | 2 | 4 | 4 | 2 | 6 | 6 | 2 | 4 |
| 1297 | 6 | 2 | 5 | 8 | 14 | 4 | 2 | 8 | 2 | 6 | 6 | 6 | 0 | 4 | 2 | 6 | 5 | 2 |

| $p$ | (1, 2) | (1, 3) | (1, 4) | (1, 5) | (1, 6) | (1, 7) | (1, 11) | (1, 12) | (1, 13) | (1, 14) | (1, 15) | (2, 0) | (2, 1) | (2, 2) | (2, 3) | (2, 4) | (2, 5) | (2, 6) | (2, 13) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 241 | 1 | 0 | 0 | 1 | 2 | 1 | 0 | 1 | 0 | 1 | 2 | 1 | 2 | 0 | 1 | 1 | 2 | 0 | 1 |
| 401 | 1 | 2 | 1 | 4 | 0 | 1 | 3 | 1 | 1 | 1 | 3 | 1 | 1 | 0 | 1 | 0 | 1 | 3 | 1 |
| 433 | 0 | 2 | 3 | 4 | 2 | 0 | 2 | 3 | 2 | 1 | 1 | 1 | 3 | 3 | 1 | 2 | 2 | 1 | 1 |
| 977 | 4 | 2 | 2 | 4 | 4 | 5 | 0 | 4 | 8 | 3 | 5 | 3 | 4 | 4 | 4 | 1 | 5 | 3 | 4 |
| 1009 | 3 | 6 | 6 | 4 | 4 | 2 | 6 | 7 | 4 | 2 | 3 | 2 | 8 | 6 | 1 | 4 | 5 | 3 | 5 |
| 1297 | 5 | 4 | 4 | 7 | 6 | 4 | 5 | 4 | 6 | 7 | 4 | 9 | 5 | 8 | 6 | 3 | 6 | 5 | 3 |

| $p$ | (2, 14) | (2, 15) | (3, 0) | (3, 1) | (3, 2) | (3, 3) | (3, 4) | (3, 5) | (3, 15) | (4, 0) | (4, 1) | (4, 2) | (4, 3) | (5, 2) | $x$ | $y$ | $a$ | $b$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 241 | 2 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 2 | 0 | 1 | 1 | 3 | −15 | − 2 | 13 | 6 |
| 401 | 2 | 4 | 2 | 1 | 1 | 2 | 1 | 2 | 0 | 1 | 2 | 1 | 3 | 2 | 1 | −10 | − 3 | −14 |
| 433 | 1 | 5 | 1 | 1 | 3 | 2 | 0 | 0 | 2 | 1 | 2 | 2 | 1 | 1 | 17 | 6 | −19 | − 6 |
| 977 | 4 | 3 | 2 | 4 | 9 | 3 | 2 | 3 | 4 | 5 | 4 | 4 | 1 | 6 | −31 | − 2 | − 3 | 22 |
| 1009 | 2 | 6 | 3 | 3 | 5 | 5 | 1 | 3 | 3 | 5 | 4 | 3 | 4 | 3 | −15 | 14 | −19 | −18 |
| 1297 | 2 | 6 | 2 | 6 | 5 | 5 | 8 | 4 | 6 | 3 | 4 | 6 | 6 | 5 | 1 | −18 | −35 | 6 |

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press

## References

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. 57 (1935), 391–242.

2. Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2$ (mod $p$), to appear shortly in the Pacific Journal of Mathematics.

*Berkeley, California*

https://doi.org/10.4153/CJM-1954-046-1 Published online by Cambridge University Press