manuscript No.
(will be inserted by the editor)

Euler's groups of powers of prime complex integers

Vladimir I. Arnold

the date of receipt and acceptance should be inserted later

Abstract The article describes Euler's group $\Gamma(z)$, formed by the invertible elements of the ring of the residues of the integer complex numbers modulo numbers divisible by z.

The answers are proved for the primary cases $z=(1+i)^m$ and $z=(p+iq)^m$, $p^2+q^2=4k+3$ being prime.

Keywords Gauss complex integers · Complex prime numbers · Arithmetics of complex integers · Primary complex numbers · Euler's function · Complex Diophantine geometry

Mathematics Subject Classification (2010) 11A05 · 11A25 · 11A41 · 11R04

1 What is Euler's group of a complex integer?

The ring $\mathbb{Z}_{\mathbb{C}}$ of the complex integer numbers contains for each complex integer $z=x+iy$ ($x\in\mathbb{Z}$, $y\in\mathbb{Z}$) the ideal $z\mathbb{Z}_{\mathbb{C}}$ of the elements divisible by z.

The quotient ring (formed by the residues modulo $z\in\mathbb{Z}_{\mathbb{C}}$) consists of $|z|^2=x^2+y^2$ elements:

$$\mathbb{Z}_z=\mathbb{Z}_{\mathbb{C}}/(z\mathbb{Z}_{\mathbb{C}}).$$

The invertible elements of the quotient ring form (commutative, multiplicative) *Euler's group of complex integer z*

$$\Gamma(z)=\big\{r\in\mathbb{Z}_z:\exists w\in\mathbb{Z}_z\mid rw=1\big\}.$$

The number of elements of this group is Euler's function's value, $\varphi(z)$.

The present paper describes these groups, the complex integer z being a power of a prime complex integer.

The prime complex integers are subdivided into three types.

I. The real prime number 2 is not prime from the complex point of view, having smaller divisors:

$$2=(1+i)(1-i).$$

Vladimir I. Arnold (1937–2010)
Steklov Mathematical Institute, 8 Gubkina St., Moscow, 119991, Russia

Therefore, the even prime number 2 is replaced in the complex case by four complex prime numbers

$$(\pm 1 \pm i).$$

II. The real prime number 3 remains prime from the complex point of view. Every real prime number $r = 4k+3$ is replaced in the complex case by four complex prime numbers

$$\pm r, \quad \pm ir.$$

III. The real prime number 5 is no longer prime from the complex point of view:

$$5 = (\pm 2 \pm i)(\pm 2 \mp i) = (\pm 1 \pm 2i)(\pm 1 \mp 2i).$$

Every real prime number $r = 4k+1$ is replaced in the complex case by eight complex prime numbers

$$(\pm p \pm iq), \quad (\pm q \pm ip),$$

where $p^2 + q^2 = r$.

Euler's groups of powers of complex prime numbers are given in the following list.

I. $z = (1+i)^n$.

$$\Gamma(z) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_{2^{a-1}}, \qquad n = 2a, \qquad a \geqslant 6,$$
$$\Gamma(z) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^{a-1}} \times \mathbb{Z}_{2^{a-1}}, \qquad n = 2a+1, \qquad a \geqslant 6.$$

In both the cases Euler's function has the value $\varphi(z) = 2^{n-1}$.

II. $z = (4k+3)^n$, $4k+3$ being a real prime number.

$$\Gamma(z) \simeq \mathbb{Z}_u \times (\mathbb{Z}_v)^2, \qquad \text{where} \quad u = (4k+3)^2 - 1,\ v = (4k+3)^{n-1}.$$

Euler's function has the value $\varphi(z) = (4k+3)^{2n} - (4k+3)^{2n-2} = 8(k+1)(2k+1)(4k+3)^{2n-2}$. In the case $4k+3 = 3$ one gets $\varphi\big((3+i0)^n\big) = 8 \cdot 9^{n-1}$, for $4k+3 = 7$ one gets $\varphi\big((7+i0)^n\big) = 48 \cdot 49^{n-1}$.

III. $z = (p+iq)^m$, the number $n = p^2 + q^2 = 4k+1$ being a real prime.

$$\Gamma(z) \simeq \mathbb{Z}_{(n-1)n^{m-1}}, \qquad \varphi\big((p+iq)^m\big) = \varphi(n^m) = (n-1)n^{m-1}.$$

The proofs of these results are different in the three cases I, II and III. The case II has been studied in [1], where the proof is given for the prime $4k+3 = 3$ with all the details (other primes of this form, like 7 and so on, behave similarly).

The proofs for the case I are contained below (in § 2 for $n = 2a$ and in § 3 for $n = 2a+1$).

The proofs for the case III are given below in § 4.

For the powers $z_n = (1+i)^n$, Euler's groups $\Gamma(z_n)$ for small even n, calculated explicitly (being long for the large values of n), provide the following list:

n	2	4	6	8	10	12
$\Gamma(z_n)$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2 \times (\mathbb{Z}_4)^2$	$(\mathbb{Z}_4)^2 \times \mathbb{Z}_8$	$\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_{16}$	$\mathbb{Z}_4 \times \mathbb{Z}_{16} \times \mathbb{Z}_{32}$

Theorem 1 *Euler's group $\Gamma(z_n)$, where $n = 2a \geqslant 6$, is isomorphic to the direct product of three cyclical groups*

$$\Gamma(z_n) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^p} \times \mathbb{Z}_{2^q},$$

where $p = a-2$, $q = a-1$.

The list of the values $z_n = (1+i)^n$ starts from

n	1	2	3	4	5	6	7	8
z_n	$1+i$	$2i$	$-2+2i$	-4	$-4-4i$	$-8i$	$8-8i$	16
$\lvert z_n\rvert^2$	2	4	8	16	32	64	128	256
$\varphi(z_n)$	1	2	4	8	16	32	64	128

The fourth line contains the values of Euler’s function

$$\varphi(z_n) = \bigl|\Gamma(z_n)\bigr|,$$

it is the “number of the residues modulo z_n, which are relatively prime with z_n”, that is the number of the invertible elements of the ring $\mathbb{Z}_{z_n}$.

Lemma 1 *A residue $r = x + iy \in \mathbb{Z}_{z_n}$ modulo $z_n = (1+i)^n$ is invertible if and only if the integer $x+y$ is odd.*

Proof Consider the product

$$x + iy = (1+i)(u+iv)$$

(where $x = u - v$, $y = u + v$). If the integer $x+y$ is even, there exist integers

$$u = (x+y)/2, \quad v = (y-x)/2.$$

In this case the element $z = x + iy$ is not invertible, since

$$zw = (1+i)(u+iv)w \not\equiv 1 \ \bigl(\operatorname{mod}(1+i)\bigr).$$

When $x+y$ is odd, we find the representation

$$z = 1 + tz_1, \quad t = u + iv,$$

where $u = (x-1+y)/2$, $v = (y+1-x)/2$. This representation proves that z is invertible in $\mathbb{Z}_{z_n}$, since

$$w = z^{-1} = 1 - (tz_1) + (tz_1)^2 - (tz_1)^3 + \cdots .$$

This geometrical progression is finite in the ring $\mathbb{Z}_{z_n}$, where $z_1^n = 0$. □

The Lemma provides the values of Euler’s function φ at the complex points z_n:

$$\varphi(z_n) = \bigl|\mathbb{Z}_{z_n}\bigr|/2 = |z_n|^2/2 = 2^{n-1}.$$

Therefore, the commutative group $\Gamma(z_n)$ is of order $\bigl|\Gamma(z_n)\bigr| = 2^{n-1}$. Consequently, its representation in the form of a product of cyclical groups is

$$\Gamma(z_n) \simeq (\mathbb{Z}_2)^{a_1} \times (\mathbb{Z}_4)^{a_2} \times (\mathbb{Z}_8)^{a_3} \times \cdots ,$$

the integer a_s being the multiplicity of the multiplier $\mathbb{Z}_{2^s}$:

$$\bigl|\Gamma(z_n)\bigr| = 2^{a_1+2a_2+3a_3+\cdots}.$$

We have thus proved

Lemma 2 *The multiplicities of the cyclical multipliers of Euler’s group $\Gamma(z_n)$ satisfy the relation*

$$a_1 + 2a_2 + 3a_3 + \cdots = n - 1.$$

2 The case of the even powers of the smallest complex prime integer $1+i$

We start from counting the solutions of each of the following equations

$$w=1, \quad w^2=1, \quad w^4=1, \quad w^8=1, \quad \dots$$

for the elements $w \in \Gamma(z_{2a})$ of Euler's group of $(1+i)^{2a}$.

For a cyclical group $\mathbb{Z}_{2^r}$ these numbers of the solutions form the sequence

$$\left\{1,\, 2,\, 2^2,\, 2^3,\, \dots,\, 2^r\right\}.$$

It follows that for the product group $\mathbb{Z}_{2^p} \times \mathbb{Z}_{2^q}$, where $q=p+s$, the numbers of the solutions form the sequence

$$\left\{1,\, 4,\, 4^2,\, \dots,\, 4^p;\;\; 4^p \cdot 2,\, 4^p \cdot 2^2,\, \dots,\, 4^p \cdot 2^s\right\}$$

(the multiplier 4 being added p times and the multiplier 2 being added s times).

Similarly, for three multipliers

$$\mathbb{Z}_{2^p} \times \mathbb{Z}_{2^q} \times \mathbb{Z}_{2^r}$$

(where $p \leqslant q < r$, $q=p+s$, $r=q+t$) the sequence of the numbers of the solutions takes the form

$$\left\{1,\, 8,\, 8^2,\, \dots,\, 8^p;\;\; 8^p \cdot 4,\, 8^p \cdot 4^2,\, \dots,\, 8^p \cdot 4^s;\;\; 8^p \cdot 4^s \cdot 2,\, \dots,\, 8^p \cdot 4^s \cdot 2^t\right\}.$$

The products of more multipliers provide similar sequences. This reasoning yields the following conclusion:

Lemma 3 *The number of the square roots of* 1 *in the group*

$$\Gamma \simeq (\mathbb{Z}_2)^{a_1} \times (\mathbb{Z}_4)^{a_2} \times \cdots \times (\mathbb{Z}_{2^h})^{a_h}$$

equals

$$2^{a_1+a_2+\cdots+a_h}.$$

The number of the roots w of equation $w^2=1$ in Euler's group $\Gamma(z_n)$, where $z_n=(1+i)^n$, can be easily computed explicitly.

Lemma 4 *The number of the square roots w of* 1 *in Euler's group $\Gamma(z_n)$, where $z_n=(1+i)^n$, $n=2a \geqslant 6$, equals* 8.

Proof Two roots $w=1$ and $w=-1$ are obvious. When w is a root, the shifted version $w'=w+2^{a-1}t$ is also a root:

$$(w')^2 = w^2 + 2 \cdot w 2^{a-1} t + 2^{2a-2} t^2 \equiv w^2 \pmod{2^a}.$$

Choosing $t=0,\ 1,\ i,\ 1+i$, we deduce from the root $w=1$ four shifted versions w', and from the root $w=-1$ we deduce four more shifted roots.

We prove now that there exist no other square roots $w=x+iy$ of 1 in our Euler's group.

Indeed, we find

$$w^2 = x^2 - y^2 + 2ixy,$$

and therefore the complex congruence $w^2 \equiv 1 \pmod{2^a}$ implies two real congruences

$$x^2 - y^2 \equiv 1 \pmod{2^a}, \quad 2xy \equiv 0 \pmod{2^a}.$$

The first congruence shows that x and y are different modulo 2. Considering the residues modulo 4, we see that x is odd, y being even:

$$x = 2A+1, \quad y = 2B.$$

The second congruence shows that

$$(2A+1)B \equiv 0 \pmod{2^{a-2}},$$

implying that $B = 2^{a-2}c$, $y = 2^{a-1}c$.

Now the congruence $x^2 - y^2 \equiv 1 \pmod{2^a}$ provides the condition

$$4A^2 + 4A - 4B^2 \equiv 0 \pmod{2^a},$$
$$A^2 + A \equiv 0 \pmod{2^{a-2}}.$$

This congruence implies the divisibility by 2^{a-2} either of A or of $A+1$:

$$\text{either } A = 2^{a-2}g \quad \text{or } A = 2^{a-2}g - 1,$$

and therefore

$$\text{either } x = 2^{a-1}g + 1 \quad \text{or } x = 2^{a-1}g - 1.$$

To get all the possible values of $x \pmod{2^a}$, it suffices to choose $g = 0$ or 1, providing totally 4 values.

In each of these 4 cases $y = 2^{a-1}c$ (c being 0 or 1), providing the $4 \cdot 2 = 8$ roots w of the equation $w^2 = 1$. We have thus proved that this equation has no other solutions in Euler's group $\Gamma(z_n)$. □

Lemma 4 together with Lemma 3 imply

Corollary 1 *Euler's group $\Gamma(z_n)$, $z_n = (1+i)^n$ (where $n = 2a \geqslant 6$), has 3 cyclical multipliers $\mathbb{Z}_{2^s}$, their multiplicities a_s satisfying the two conditions*

$$\begin{cases} a_1 + a_2 + \cdots = 3, \\ a_1 + 2a_2 + 3a_3 + \cdots = n-1. \end{cases}$$

Study now the degree 4 roots of 1 in our Euler's group $\Gamma(z_n)$ (where $z_n = (1+i)^n$, $n = 2a \geqslant 6$).

Lemma 5 *The number of the roots of degree 4 from 1 in this Euler group equals 64.*

Proof The 8 square roots w of 1 all have one of the following two forms:

$$w \in \{1 + c\xi, \ -1 + c\xi\},$$

where $\xi = 2^{a-1}$, $c \in \{0, \ 1, \ i, \ 1+i\}$.

For the case $c = 0$ the square roots of these values w are provided, first, by the evident roots

$$\sqrt{w} \in \{1, \ -1\}, \quad \sqrt{w} \in \{i, \ -i\}.$$

Each of these 4 values provides (being shifted by $c'\xi$, which shift does not change the value of the square modulo 2^a) a quadruple of roots. This way we get 16 roots of degree 4 from 1 (their squares being 1 and -1).

To move from $\sqrt{w}$ to $\sqrt{w+c\xi}$, note that

$$w+c\xi = w(1+c''\xi), \quad \text{where } c''=c/w.$$

The Newton binomial formula provides

$$(w+c\xi)^{1/2} = w^{1/2}\left(1+\frac{c''\xi}{2}+\frac{\frac{1}{2}\left(-\frac{1}{2}\right)}{2}(c''\xi)^2+\cdots\right).$$

The denominator in the term containing $(c''\xi)^k$ equals $2^k k!$. The number of the factors 2 in the prime multipliers decomposition of the integer $k!$ equals

$$j(k) = [k/2]+[k/4]+\cdots \leqslant k/2+k/4+\cdots < k:$$

k	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$j(k)$	1	1	3	3	4	4	7	7	8	8	10	10	11	11	15

Therefore, the summand of the binomial series

$$\frac{(c''2^{a-1})^k}{2^k k!}$$

is divisible by $2^{(a-1)k-k-k} = 2^{(a-3)k}$, and thus this summand equals 0 modulo 2^{a-2} (for sufficiently large k). Thus, the binomial series has a finite number of terms, and we get (for every of the 4 values $c=0,\ 1,\ i,\ 1+i$) an octagon of the square roots (similarly to the case $c=0$ considered above).

These computations provide $8\cdot 8=64$ roots of degree 4 from 1 in $\Gamma(z_n)$ (proving also that there are no others). □

Comparing Lemma 5 which we have thus proved with the sequence of the numbers of roots (mentioned above, see the text preceding Lemma 3) we deduce (from the numbers $(1,\ 8,\ 64)$ of the roots of degrees $(1,\ 2,\ 4)$) that the minimal multiplier is $\mathbb{Z}_{2^p}$, where $p \geqslant 2$. The presence of the multiplier $\mathbb{Z}_4$ is implied by the following reasoning: otherwise each root of degree 4 from 1 were a square, while the equation $(x+iy)^2 \equiv i \pmod{2^q}$ is unsolvable, the product $2xy$ being even.

Therefore (for $n=2a>6$) we get the decomposition

$$\Gamma(z_n) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^q} \times \mathbb{Z}_{2^r},$$

where $2 \leqslant q \leqslant r$, implying the relation

$$2+q+r = n-1, \quad q+r = 2a-3.$$

As we will prove below, $q=a-2$, $r=a-1$. The proof of these equalities starts from the following fact.

Lemma 6 *For every element z of the group of Euler $\Gamma(z_n)$ (where $n=2a>6$), there holds the relation $z^{2^k}=1$ for every $k \geqslant a$.*

Proof The representation $z = 1 + tz_1$ (explained above, in the proof of Lemma 1) implies for $z \in \Gamma(z_n)$ the relation

$$z^2 = 1 + 2tz_1 + t^2 2i = 1 + 2t_1.$$

Therefore, there hold also the relations

$$z^4 = 1 + 4t_1 + 4t_1^2 = 1 + 4t_2,$$
$$z^8 = 1 + 8t_2 + 16t_2^2 = 1 + 8t_3,$$

and so on till

$$z^{2^s} = 1 + 2^s t_s.$$

Knowing that $2^a = 0$ in the quotient ring $\mathbb{Z}_{z_{2a}}$, we find $z^{2^a} = 1$. □

Lemma 6 implies that in the above factorization of the Euler group into the cyclical ones, the numbers q and r do not exceed a. Therefore, the relation $q + r = 2a - 3$ might hold only for the two cases:

$$\text{either } (q = a - 3,\ r = a) \quad \text{or } (q = a - 2,\ r = a - 1).$$

We will prove now that the first case is impossible. To see this, consider the real Euler group $\Gamma(2^a)$. It is proved in my book [2] that $\Gamma(2^a) \simeq \mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2$. The elements of the form $1 + 4c \in \Gamma(2^a)$ form in this real Euler group a cyclical subgroup of order 2^{a-2}.

If for the complex Euler group it were

$$\Gamma(z_{2a}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^q} \times \mathbb{Z}_{2^r},$$

where $(q = a - 3,\ r = a)$, then the above cyclical real subgroup would lie in $\mathbb{Z}_{2^a}$, and its elements would be squares.

Consider, however, its element 5. If in $\Gamma(z_{2a})$ there were the relation

$$5 \equiv (x + iy)^2 \pmod{2^a},$$

one would have the real relations

$$x^2 - y^2 \equiv 5 \pmod{2^a}, \quad 2xy \equiv 0 \pmod{2^a}.$$

The first relation implies (considering the residues modulo 4) that x is odd, y being even:

$$x = 2A + 1, \quad y = 2B.$$

The congruences take the form

$$4A^2 + 4A - 4B^2 \equiv 4 \pmod{2^a}, \quad (2A + 1)B \equiv 0 \pmod{2^{a-2}}.$$

Therefore, one would have

$$A^2 + A \equiv 1 \pmod{2^{a-2}}, \quad B \equiv 0 \pmod{2^{a-2}}.$$

The product $A(A + 1)$ being always even, the first congruence is impossible, excluding the case $r = a$.

Thus, $(q = a - 2,\ r = a - 1)$, proving Theorem 1. □

3 The odd powers of the smallest complex prime number 1 + *i*

This sequence of complex integers starts from the terms $\{z_1, z_3, \ldots\}$:

a	0	1	2	3	4	5
z_{2a+1}	$1+i$	$2i-2$	$-4-4i$	$-8i+8$	$16+16i$	$32i-32$
$\varphi(z_{2a+1})$	1	4	16	64	256	1024
$\Gamma(z_{2a+1})$	$\{1\}$	$\mathbb{Z}_4$	$\mathbb{Z}_4 \times (\mathbb{Z}_2)^2$	$(\mathbb{Z}_4)^3$	$\mathbb{Z}_4 \times (\mathbb{Z}_8)^2$	$\mathbb{Z}_4 \times (\mathbb{Z}_{16})^2$

The fundamental domain for the quotient ring

$$\mathbb{Z}_{z_{2a+1}} = \mathbb{Z}_{\mathbb{C}}/(z_{2a+1}\mathbb{Z}_{\mathbb{C}})$$

may be chosen to be the square with sides

$$(z_{2a+1},\, iz_{2a+1}) = (2^a + i\,2^a,\ -2^a + i\,2^a).$$

The area of this domain equals 2^{2a+1}. Therefore the quotient ring consists of

$$\left|\mathbb{Z}_{z_{2a+1}}\right| = 2^{2a+1}$$

elements.

The invertible elements $x+iy$ are exactly those, for which the sums $x+y$ are odd (the proof is similar to that of Lemma 1 in § 1). The area of the elementary square of the lattice of the invertible elements equals 2. Therefore the number of the invertible elements equals

$$\left|\Gamma(z_{2a+1})\right| = \varphi(z_{2a+1}) = 2^{2a} = 4^a.$$

In the case $a = 1$ one has $z_3 = 2i - 2$. The group $\Gamma(z_3)$ is therefore formed by the 4 residues $\{1, -1, i, -i\}$:

$$\Gamma(z_3) \simeq \mathbb{Z}_4.$$

In the case $a = 2$, where $z_5 = -4 - 4i$, the group $\Gamma(z_5)$ consists of the 16 residues

$$x + iy \quad : \quad (0 < x+y < 8,\ \ 0 < y-x < 8),$$

the integers x and y being different modulo 2:

$$\{1,\ 3,\ 5,\ 7,\ i,\ 3i,\ 5i,\ 7i,\ \pm1+2i,\ \pm2+3i,\ \pm2+5i,\ \pm1+6i\}.$$

In their group, there hold the relations

$$1^2 = 3^2 = 5^2 = 7^2 = (\pm1+2i)^2 = (\pm1+6i)^2 = 1,$$
$$i^2 = (3i)^2 = (5i)^2 = (7i)^2 = (\pm2+3i)^2 = (\pm2+5i)^2 = -1 = 7.$$

The number of the elements of this commutative group being equal to $2^4 = 16$, it is the product of the cyclical groups $\mathbb{Z}_{2^b}$:

$$\Gamma(z_5) \simeq (\mathbb{Z}_2)^{s_1} \times (\mathbb{Z}_4)^{s_2} \times (\mathbb{Z}_8)^{s_3} \times \cdots,$$

whence $2^{s_1+2s_2+3s_3+\cdots} = 2^4$, and therefore

$$s_1 + 2s_2 + 3s_3 + \cdots = 4.$$

The number of the square roots from 1 in this group being equal to 8:

$$2^{s_1+s_2+s_3+\cdots} = 8, \quad s_1+s_2+s_3+\cdots = 3.$$

Therefore, there hold the relations

$$s_2+2s_3 = 1, \qquad s_3 = 0, \quad s_2 = 1, \quad s_1 = 2.$$

We have thus proved the isomorphism

$$\mathit{\Gamma}(z_5) \simeq (\mathbb{Z}_2)^2 \times \mathbb{Z}_4.$$

The calculation of the next groups $\mathit{\Gamma}(z_{2a+1})$ might be performed similarly, but it might also be replaced by the following

Theorem 2 *Euler's group $\mathit{\Gamma}(z_{2a+1})$, where $a \geqslant 3$, is isomorphic to the product of three cyclical groups,*

$$\mathit{\Gamma}\big((1+i)^{2a+1}\big) \simeq \mathbb{Z}_4 \times (\mathbb{Z}_{2^{a-1}})^2.$$

Proof Reasoning as above, we get the relation

$$\mathit{\Gamma} = \mathit{\Gamma}\big((1+i)^{2a+1}\big) \simeq (\mathbb{Z}_2)^{s_1} \times (\mathbb{Z}_4)^{s_2} \times \cdots,$$

whence the identity

$$2^{\sum\limits_r (rs_r)} = 2^{2a}.$$

The number of the square roots from 1 in group $\mathit{\Gamma}$ equals $2^{\sum\limits_r s_r}$ (each multiplier $\mathbb{Z}_{2^r}$ contributing 2 elements of the product-root, being encountered s_r times).

Lemma 7 *For each $a \geqslant 2$ the number of the square roots from* 1 *in the complex Euler group $\mathit{\Gamma}\big((1+i)^{2a+1}\big)$ equals* 8.

Proof It is easy to find 8 roots: one starts from $z = 1$, and starting from a root z of equation $z^2 = 1$ one finds more roots, shifting the known root by the halfperiods:

$$z' = z + c, \qquad \text{where} \quad c = 2^{a-1}(i \pm 1).$$

Indeed,

$$(z')^2 = z^2 + 2cz + c^2,$$

the terms $2c = 2^a(i \pm 1)$ and $c^2 = 2^{a-2}(i \pm 1)2^a(i \pm 1)$ belonging to the ideal $(1+i)^{2a+1}\mathbb{Z}_{\mathbb{C}}$ generated additively by $2^a(i \pm 1)$, when $a \geqslant 2$. The elements 2^{a+1} and $i\,2^{a+1}$ belong to this ideal.

Each root $z = \pm 1$ of equation $z^2 = 1$ generates 4 shifted roots

$$z' = z + 2^{a-1}\big[u(i-1) + v(i+1)\big],$$

where $(u,v) \in \big\{(0,0),\ (0,1),\ (1,0),\ (1,1)\big\}$.

There are no other square roots of 1 in Euler's group $\mathit{\Gamma}\big((1+i)^{2a+1}\big)$. Indeed, denote such a root by $z = x + iy$. The complex congruence

$$z^2 = 1 + 2^a\big[\alpha(i-1) + \beta(i+1)\big]$$

means the pair of real congruences,

$$x^2 - y^2 = 1 + 2^a(\beta - \alpha), \quad 2xy = 2^a(\alpha + \beta). \tag{$*$}$$

The first congruence implies that x and y are different modulo 2. Studying the residues modulo 4, we see that x is odd, y being even:

$$x = 2A+1, \quad y = 2B.$$

The congruences $(*)$ take now the form

$$4(A^2+A-B^2) = 2^a(\beta-\alpha), \quad 4B(2A+1) = 2^a(\alpha+\beta).$$

Thus, B is divisible by 2^{a-2}, and therefore $4B^2$ is divisible by 2^{2a-2}, being thus divisible by 2^a:

$$A^2+A = 2^{a-2}D, \quad B = 2^{a-2}C.$$

The first congruence means that

$$\text{either } A = 2^{a-2}P \quad \text{or } A = 2^{a-2}Q-1,$$

and therefore

$$\text{either } x = 2^{a-1}P+1 \quad \text{or } x = 2^{a-1}Q-1.$$

We obtain therefore for x 8 possible values (inside one fundamental domain for the factorization modulo $2^a(i \pm 1)$).

For $y = 2B$ the divisibility condition $B = 2^{a-2}C$ provides (in this fundamental domain) at most 2 values, and thus one gets 16 possible pairs (x, y).

For each of these pairs one calculates (using $(*)$) the values of the parameters $(\beta - \alpha, \beta+\alpha)$. These values are different modulo 2 in 8 cases from 16, which is impossible for any integer values of α and β.

There remain 8 cases (providing exactly the 8 shifts of the roots $z = \pm 1$ studied above). Lemma 7 is therefore proved. □

Corollary 2 *Euler's group $\Gamma(z_n)$, where $n = 2a+1 > 5$, has 3 cyclical multipliers $\mathbb{Z}_{2^s}$, whose multiplicities a_s satisfy the two relations*

$$\begin{cases} a_1+a_2+\cdots = 3, \\ a_1+2a_2+3a_3+\cdots = 2a. \end{cases}$$

To find these multiplicities, calculate the roots of degree 4 from 1 in Euler's group $\Gamma\big((1+i)^{2a+1}\big)$, where $a > 2$.

Lemma 8 *The number of the solutions of equation $z^4 = 1$ in Euler's group $\Gamma\big((1+i)^{2a+1}\big)$ equals 64.*

Proof All the 8 square roots w from 1, calculated above, are of the forms

$$w \in \{1+c\xi, \ -1+c\xi\},$$

where $\xi = 2^{a-1}$ and $c \in \{0, 1, i, 1+i\}$.

For $c = 0$ one finds immediately the roots

$$\sqrt{w} \in \{\pm 1\}, \quad \sqrt{w} \in \{\pm i\}.$$

Each of these four roots provides (by the shifts at $c'\xi$, which do not change the squares, modulo $(1+i)^{2a+1}$) a quadruple of roots of equation $z^4 = 1$.

Thus we construct 16 roots of degree 4 from 1 in $\Gamma\bigl((1+i)^{2a+1}\bigr)$, whose squares are 1 or -1.

To move from $\sqrt{w}$ to $\sqrt{w+c\xi}$, ξ being 2^{a-1}, represent the sum as the product

$$w+c\xi = w(1+c''\xi), \quad \text{where } c'' = c/w.$$

The Newton binomial formula has the form

$$(w+c\xi)^{1/2} = w^{1/2}\bigl(1+c''\xi/2-(c''\xi)^2/8+\cdots\bigr).$$

The degree k term

$$\frac{(c''\xi)^k}{2^k k!}$$

is divisible by a power of 2, which is growing with k. Therefore, the binomial series is a finite polynomial, providing (for each $c \in \{0,\ 1,\ i,\ 1+i\}$) eight shifted roots (similarly to the situation for $c=0$ described above).

These calculations provide $8\cdot 8 = 64$ roots of degree 4 from 1 in Euler's group $\Gamma = \Gamma\bigl((1+i)^{2a+1}\bigr)$, proving also that there exist no other roots. □

The resulting numbers (1, 8, and 64) of the roots from 1 of degrees (1, 2, and 4) in Γ show that the lowest multiplier in the decomposition of group Γ into the cyclical ones is of the form $\mathbb{Z}_{2^p}$, $p \geqslant 2$.

In fact $p=2$, otherwise each root of degree 4 from 1 were a square, while the congruence

$$(x+iy)^2 \equiv i \ \bigl(\operatorname{mod}(1+i)^{2a+1}\bigr)$$

has no solutions, the integer $2xy$ being even.

Therefore, we have (for $a>2$) the representation

$$\Gamma\bigl((1+i)^{2a+1}\bigr) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^q} \times \mathbb{Z}_{2^r}, \quad 2 \leqslant q \leqslant r,$$

whence $2+q+r = 2a$, $q+r = 2a-2$.

We will prove below that $q = r = a-1$.

Lemma 9 *For each element z of Euler's group $\Gamma\bigl((1+i)^{2a+1}\bigr)$ (where $a \geqslant 2$) there holds the relation $z^{2^k} = 1$ (for every $k \geqslant a$).*

Proof The relation $z = 1+tz_1$ (where $z_1 = 1+i$), discussed in the above proof of Lemma 1, provides, successively, the corollaries

$$\begin{aligned} z^2 &= 1+2tz_1+t^2 2i = 1+2t_1, \\ z^4 &= 1+4t_1+4t_1^2 = 1+4t_2, \\ z^8 &= 1+8t_2+16t_2^2 = 1+8t_3, \quad \ldots, \\ z^{2^s} &= 1+2^s t_s. \end{aligned}$$

The relation $2^a = 0$ in the quotient ring $\mathbb{Z}_{(1+i)^{2a+1}}$ implies the relation $z^{2^a} = 1$, proving Lemma 9. □

This Lemma implies that in the preceding decomposition (just before the Lemma) of Euler's group $\Gamma\left((1+i)^{2a+1}\right)$ into the cyclical multipliers, the numbers q and r do not exceed a. The relation $q+r=2a-2$ can be only realized in the two cases $q \leqslant r$:

$$(q=r=a-1), \quad (q=a-2,\ r=a).$$

We will prove below that the second case never happens.

Consider the multiplicative group of the invertible real residues modulo 2^{a+1},

$$\Gamma(2^{a+1}) = \left\{1,\ 3,\ \dots,\ 2^{a+1}-1\right\}.$$

This group is isomorphic to the product of two cyclical groups

$$\Gamma(2^{a+1}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-1}},$$

as it is proved in the book [2]. Moreover, it is proved there that one may choose as the generator of the second cyclical multiplier the element 5.

The above real Euler group forms a natural subgroup of our complex Euler's group:

$$\Gamma(2^{a+1}) \subset \Gamma\left((1+i)^{2a+1}\right).$$

The complex group's isomorphism to the product

$$\mathbb{Z}_4 \times \mathbb{Z}_{2^q} \times \mathbb{Z}_{2^r} \quad (q=a-2,\ r=a)$$

would provide the projection of the subgroup

$$\mathbb{Z}_{2^{a-1}} \subset \Gamma(2^{a+1})$$

with no nontrivial kernel to the multiplier $\mathbb{Z}_{2^a}$, sending the generator $5 \in \Gamma(2^{a+1})$ to a full square

$$5 = (x+iy)^2 \in \Gamma\left((1+i)^{2a+1}\right).$$

However, the corresponding congruences

$$\begin{cases} x^2 - y^2 = 5 + 2^a(\beta - \alpha), \\ 2xy = 2^a(\beta + \alpha) \end{cases}$$

lead to the conclusions that (as above)

$$\begin{gathered} x = 2A+1, \quad y = 2B, \\ 4(A^2 + A - B^2) = 5 + 2^a(\beta - \alpha), \\ 4B(2A+1) = 2^a(\beta + \alpha), \end{gathered}$$

implying the congruence

$$A^2 + A \equiv 5 \pmod{2^a}.$$

But the product $A(A+1)$ is even, making the preceding congruence impossible. Therefore, $(q,\ r) = (a-1,\ a-1)$, and we obtain (for $a \geqslant 3$) the required isomorphism

$$\Gamma\left((1+i)^{2a+1}\right) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{2^{a-1}} \times \mathbb{Z}_{2^{a-1}}$$

of Theorem 2. □

4 Prime complex divisors of the real primes $n = 4k + 1$

Example The real prime number $n = 5$ is not a complex prime number, since

$$5 = (2+i)(2-i).$$

Every real prime number $n = 4k+1$ has a similar representation

$$n = p^2 + q^2 = (p+iq)(p-iq),$$

being a product of two complex prime integers, $p \pm iq \in \mathbb{Z}_{\mathbb{C}}$.

The complex Euler groups of the powers of $p \pm iq$ are calculated below.

Theorem 3 *Complex Euler's group*

$$\Gamma\left((p+iq)^m\right)$$

is cyclical, its order being equal to the value of the real Euler function φ at point n^m:

$$\Gamma\left((p+iq)^m\right) \simeq \mathbb{Z}_{\varphi(n^m)} = \mathbb{Z}_{(n-1)n^{m-1}}$$

(provided that $n = p^2 + q^2$ is a prime integer, equal to 1 modulo 4).

Proof The proof starts from the following elementary fact.

Lemma 10 *If the odd number $n = p^2 + q^2$ is prime and $(p+iq)^m = P + iQ$, then the integers P and Q are relatively prime.*

Example 1 For $(n = 5,\ p = 2,\ q = 1)$ one gets, for instance, the following values of P and Q:

m	1	2	3	4	5	6
P	2	3	2	-7	-38	-117
Q	1	4	11	24	41	44

Example 2 For $(n = 10,\ p = 3,\ q = 1)$ one gets, for instance, the following values of P and Q:

m	1	2	3	4
P	3	8	18	28
Q	1	6	26	96

The integers P and Q here are not relatively prime ($n = 10$ being not an odd prime number).

Proof of Lemma 10 If there were a largest common divisor $d > 1$ of two integers P and Q, the obvious relation

$$P^2 + Q^2 = (p^2 + q^2)^m = n^m$$

would imply that d^2 is divisible by the prime number n, and hence the integers P and Q would be divisible by n.

This divisibility is, however, impossible for the following reason.

Lemma 11 *If $p^2 + q^2 = n$, then there holds the congruence*

$$(p+iq)^m \equiv (2p)^{m-1}(p+iq) \pmod{n}.$$

Proof For $m = 2$ it is obvious:

$$(p+iq)^2 = p^2 - q^2 + 2ipq = 2p^2 - n + 2ipq \equiv 2p(p+iq) \pmod{n}.$$

If the congruence holds for $m = k$, then one gets inductively

$$(p+iq)^{k+1} \equiv (2p)^{k-1}(p+iq)(p+iq) \equiv (2p)^k(p+iq) \pmod{n},$$

and therefore the congruence of Lemma 11 holds for all values of m. □

Applying Lemma 11 to the number $P + iQ = (p+iq)^m$, we conclude that

$$P + iQ \equiv (2p)^{m-1}(p+iq) \pmod{n}.$$

The right-hand side is not divisible by the prime number n (the divisibility of p by the prime n would imply the divisibility of q^2, and hence of q, by this prime n, and then the sum $p^2 + q^2 = n$ would be divisible by n^2).

We have proved that P and Q cannot be both divisible by n, and hence the largest common divisor d of integers P and Q is $d = 1$, which proves Lemma 10. □

Consider now the quotient ring

$$\mathbb{Z}_{(p+iq)^m} = \mathbb{Z}_{\mathbb{C}} \big/ \big((p+iq)^m \mathbb{Z}_{\mathbb{C}}\big).$$

The denominator lattice is generated by the sides of the square

$$P + iQ = (p+iq)^m, \quad i(P+iQ) = -Q + iP.$$

The area of this square equals $(p^2+q^2)^m = n^m$, and thus the quotient ring consists of n^m elements.

Consider now the natural embedding $\mathbb{Z} \subset \mathbb{Z}_{\mathbb{C}}$ of the ring of real integer numbers as of a subring of the ring of the complex integers.

Lemma 12 *The intersection*

$$\mathbb{Z} \cap (p+iq)^m \mathbb{Z}_{\mathbb{C}}$$

is exactly the ideal of the real integers that are divisible by n^m.

Proof Consider an intersection point

$$\alpha(P+iQ) + \beta(-Q+iP) = \gamma + i\,0$$

(with real integers α, β, γ).

The second of these congruences

$$\alpha P - \beta Q = \gamma, \quad \alpha Q + \beta P = 0$$

implies that $(\alpha = P\lambda,\ \beta = -Q\lambda)$ for some real integer λ (the numbers P and Q being relatively prime, according to Lemma 10).

The first congruence takes the form

$$\gamma = (P^2 + Q^2)\lambda = n^m \lambda,$$

proving that the intersection point belongs to $n^m\mathbb{Z}$.

For $\lambda = 1$ we get the intersection point

$$\gamma = P^2 + Q^2 = n^m,$$

proving Lemma 12. □

Lemma 13 *A point $\gamma \in \mathbb{Z}$, that is relatively prime to n^m, defines an invertible element in the quotient ring $\mathbb{Z}_{(p+iq)^m}$. There are no other invertible elements in this quotient ring.*

Proof The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_{\mathbb{C}}$ induces the isomorphic mapping between the n^m-elements quotient rings,

$$\mathbb{Z}_{n^m} \to \mathbb{Z}_{\mathbb{C}} \big/ \big((p+iq)^m \mathbb{Z}_{\mathbb{C}}\big),$$

according to Lemma 12.

The invertible elements are sent by this isomorphism to the invertible elements, and therefore this isomorphism induces an isomorphism of the real Euler group and the complex one,

$$\Gamma(n^m) \simeq \Gamma\big((p+iq)^m\big),$$

provided that $p^2 + q^2 = n$ is an odd prime number. □

This isomorphism proves Theorem 3 (see Fig. 1). □

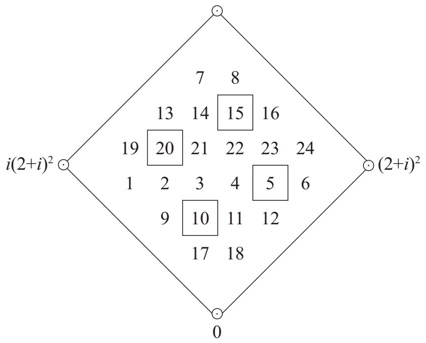

Fig. 1 The isomorphism between the real and complex Euler groups, $\Gamma(25) \simeq \Gamma\big((2+i)^2\big)$. Due to technical reasons, a box around the lowest zero is not drawn.

References

1. Arnold VI (2011) Complex Euler's groups and values of Euler's function at complex integer Gauss points. Funct. Anal. Other Math. 3(2): 169–178
2. Arnold VI (2003) Euler's Groups and Arithmetics of Geometrical Progressions. MCCME (Moscow Center for Continuous Mathematical Education), Moscow (in Russian)