ON THE EXTENSION OF WILSON'S THEOREM TO QUADRATIC FIELDS

By SETSUO OHNARI*

In the theory of numbers the following theorem of Wilson is very familiar to us:

p: a prime number $(p-1)! \equiv -1 \pmod{p}$.

Our main purpose of this paper is to prove two theorems, theorem 2 and theorem 4 in section 2 and 3, extending the above theorem of Wilson. First in theorem 2 the prime number p is transposed into a rational integer m which is not always prime, and second in theorem 4 the prime number p is transposed into an integral ideal M of quadratic field. To attain our purpose let us explain the right-hand side -1 of the congruence in the theorem as a representative of the element, whose order is 2, of $G(p)$; where $G(p)$ denotes a group of reduced residue classes of the ring of all rational integers to modulus p, and let us explain the left-hand side $(p-1)!$ as a product of all elements of $\mathfrak{S}(p)$; where $\mathfrak{S}(p)$ denotes a complete system of representatives of $G(p)$.

In section 1 we shall prove a few lemmata about a finite Abelian group in preparation for applications in the succeeding sections. In section 2 we shall prove the case in which the theorem is formulated by using a rational integer m, which is not always prime, as modulus. In section 3 we shall prove the case in which the theorem is formulated by using an integral ideal M of quadratic field as modulus.

We shall define several notations at the beginning of each section.

I wish to express my indebtedness to Professor Kazuo Matsuzaka of Hitotsubashi University for many helpful teachings and many useful discussions on the results to be described in this paper.

§1. *A few lemmata about finite Abelian group.*

In this section we shall use the following notations.

- G will denote a finite Abelian group.
- e will denote the identity element of G.
- $|G|$ will denote number of elements of G.
- S will denote the set of all elements of G whose order is 2.
- $|S|$ will denote number of elements of S.

Lemma 1.

$$G-\{e\} \subseteq S \Longrightarrow \prod_{x \in G} x = \begin{cases} e; & |G|=1 \text{ or } |G| \geqq 3 \\ a; & |G|=2,\ G=\{a, e\},\ a \neq e \end{cases}$$

* Assistant Professor (*Jokyōju*) in Mathematics.

Proof. If $|G|=1$ or 2, the above lemma is clearly true. Let $|G|\geqq 3$. For a fixed element $a\in G-\{e\}$, we shall define an equivalence relation R_1 of G as follows;

$$xR_1y\ (x, y\in G)\Longleftrightarrow y=x \text{ or } y=xa.$$

For any $x\in G$, xR_1xa, but $x\neq xa$. Therefore each equivalence class of G with respect to R_1 contains at least two elements. Since any equivalence classes of G with respect to R_1 cannot contain more than three elements by definition of R_1, each equivalence class always contains two distinct elements $\{x, xa\}$ of G. Therefore $|G|$ is even and

$$\prod_{x\in G} x=\prod_{\{x,xa\}\in G/R_1} x(xa)=a^{n/2}.$$

If we can prove that $n/2$ is even, this lemma is clearly true by the assumption $a^2=e$. Accordingly let us assume that $n/2$ is odd. Then $a^{n/2}=a$. Similarly using $b\in G-\{e, a\}$ by the assumption $|G|\geqq 3$ we obtain

$$\prod_{x\in G} x=b^{n/2}=b.$$

Therefore we get $a=b$, which is in contradiction to $a\neq b$.

Lemma 2.

$$\prod_{x\in G} x=\begin{cases} a; & |S|=1,\ S=\{a\} \\ e; & |S|\neq 1\end{cases}$$

Proof. Let us define a subgroup H of G and an equivalence relation R_2 of $G-H$ as follows;

$$H=\{x\in G;\ x^2=e\}$$

$$xR_2y(x,\ y\in G-H)\Longleftrightarrow x=y \text{ or } xy=e.$$

Then it is clear that each class of $G-H$ with respect to R_2 contains two distinct elements $\{x, x^{-1}\}$. Therefore

$$\prod_{x\in G-H} x=\prod_{\{x,x^{-1}\}\in G/R_2} xx^{-1}=e.$$

Therefore

$$\prod_{x\in G} x=\prod_{x\in G-H} x\cdot\prod_{x\in H} x=\prod_{x\in H} x.$$

Since if $|S|=1$, $H=\{e, a\}$ and if $|S|\neq 1$, $H=\{e\}$ or $|H|\geqq 3$, we complete the proof by the lemma 1.

§2. *The case in which modulus m is a rational integer.*

In this section we shall use the following notations.

- $\mathbf{Z}$ will denote the ring of all rational integers.
- m will denote a rational integer such that $m>1$.
- $N(m)$ will denote number of solutions of congruence $x^2\equiv 1 \pmod m$.
- $p, p_1, p_2, p_3, \ldots$ will denote odd prime numbers.
- $e, e_1, e_2, e_3, \ldots$ will denote natural numbers.
- $G(m)$ will denote a group of reduced residue classes of $\mathbf{Z}$ to modulus m.
- $\mathfrak{S}(m)$ will denote a complete system of representatives of $G(m)$.
- $I(m)$ will denote number of elements of $G(m)$ whose order is 2.

Proposition 1. $N(p^e)=2$,

where $e=1, 2, 3, \ldots$ and p is an odd prime number.

Proof. It is clear that $1\neq -1 \pmod{p^e}$ and $\pm 1 \pmod{p^e}$ are solutions of congruence

$x^2\equiv 1 \pmod{p^e}$. Conversely if $x^2\equiv 1 \pmod{p^e}$ then $(x+1)(x-1)\equiv 0 \pmod{p^e}$. So there exist f and g such that

$$f, g\in \mathbf{Z};\quad f\geqq 0,\ g\geqq 0,\ f+g=e,\qquad x+1\equiv 0 \pmod{p^f},\ x-1\equiv 0 \pmod{p^g}.$$

If $f>0$ and $g>0$,

$$x+1\equiv 0 \pmod{p},\quad x-1\equiv 0 \pmod{p},$$

then we get $2\equiv 0 \pmod{p}$. This is a contradiction. Therefore $f=0$ or $g=0$. If $f=0$, $x\equiv 1 \pmod{p^e}$ and if $g=0$, $x\equiv -1 \pmod{p^e}$.

Proposition 2. $\qquad N(p_1^{e_1}p_2^{e_2}\dots p_r^{e_r})=2^r$,

where $e_1, e_2, \dots, e_r$ are natural numbers and $p_1, p_2, \dots, p_r$ are r odd prime numbers which are distinct, and $r\geqq 2$.

Proof. By proposition 1 and by familiar relation

$$x^2\equiv 1 \pmod{p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}} \Longleftrightarrow x^2\equiv 1 \pmod{p_\nu^{e_\nu}}\ \mathit{for}\ \nu=1, 2, \dots, r,$$

this proposition is clear.

Proposition 3.

$$N(2^e)=\begin{cases}1;\ e=1,\\ 2;\ e=2,\\ 4;\ e\geqq 3.\end{cases}$$

Proof. It is clear that, if $e=1$, $1 \pmod 2$ is only one solution of congruence $x^2\equiv 1 \pmod 2$ and if $e=2$, $\pm 1 \pmod{2^2}$ are only two solutions of congruence $x^2\equiv 1 \pmod{2^2}$. Let us assume $e\geqq 3$. We shall prove by the induction on e that ± 1, $\pm 1+2^{e-1} \pmod{2^e}$ are only four solutions of congruence $x^2\equiv 1 \pmod{2^e}$. For $e=3$, the conclusion is clearly true. Let us assume that the conclusion is true for some $e\geqq 3$. If $x^2\equiv 1 \pmod{2^{e+1}}$, $x^2\equiv 1 \pmod{2^e}$. By the assumption of induction we obtain $x\equiv\pm 1$, $\pm 1+2^{e-1} \pmod{2^e}$. Therefore there exist y and z in Z such that $x=\pm 1+2^e y$, $x=\pm 1+2^{e-1}+2^e z$. But considering $e\geqq 3$, we obtain

$$\begin{aligned}(\pm 1+2^{e-1}+2^e z)^2&=\pm 1+2^{e-1}(1+2z)^2\\ &=1\pm 2^e(1+2z)+2^{2e-2}(1+2z)^2\\ &\equiv 1\pm 2^e(1+2z) \pmod{2^{e+1}}\\ &\not\equiv 1 \pmod{2^{e+1}}.\end{aligned}$$

Accordingly $x=\pm 1+2^e y$. It is clear that

$$1+2^e y\not\equiv -1+2^e y' \pmod{2^{e+1}}\quad (y, y'\in \mathbf{Z}),$$
$$1+2^e y\equiv 1+2^e y' \pmod{2^{e+1}} \Longleftrightarrow y\equiv y' \pmod 2\quad (y, y'\in \mathbf{Z}),$$
$$-1+2^e y\equiv -1+2^e y' \pmod{2^{e+1}} \Longleftrightarrow y\equiv y' \pmod 2\quad (y, y'\in \mathbf{Z}),$$

so complete system of representatives of $\{\pm 1+2^e y, y\in \mathbf{Z}\}$ with respect to modulus 2^{e+1} is $\{\pm 1, \pm 1+2^e\}$.

Propositiosn 4.

$$N(2^e p_1^{e_1}p_2^{e_2}\dots p_r^{e_r})=\begin{cases}2^r\ \ ;\ e=0 \text{ or } 1,\\ 2^{r+1};\ e=2,\\ 2^{r+2};\ e\geqq 3.\end{cases}$$

where $e_1, e_2, \dots, e_r$ are natural numbers and $p_1, p_2, \dots, p_r$ are odd prime numbers and $r\geqq 0$, but if $r=0$, then $e\geqq 1$.

Proof. If $r=0$, this is the same with proposition 3. Therefore let us assume $r\geqq 1$. If $e=0$, this is the same with proposition 2. If $e\geqq 1$, by familiar relation

$$x^2\equiv 1 \pmod{2^e p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}} \Longleftrightarrow \begin{cases}x^2\equiv 1 \pmod{2^e}\\ x^2\equiv 1 \pmod{p_\nu^{e_\nu}},\ \nu=1, 2, \dots, r\end{cases}$$

and by propositions 1, 2 and 3, this proposition is clear.

We have obtained the following two theorems which depend upon the conclusions of propositions 1, 2, 3 and 4. The first theorem, theorem 1, is clear by proposition 4. The second theorem, theorem 2, is clear by lemma 2 and theorem 1. Now we can obtain the theorem of Wilson on odd prime numbers as corollary of theorem 2.

Theorem 1.

$$I(m)=1 \Leftrightarrow N(m)=2 \Leftrightarrow m=4 \textit{ or } p^e \textit{ or } 2p^e$$

where e is arbitrary natural number and p is arbitrary odd prime number.

Theorem 2.

$$\prod_{x \in \mathfrak{S}(m)} x \equiv \begin{cases} -1 \pmod{m}; & m=4 \textit{ or } p^e \textit{ or } 2p^e \\ 1 \pmod{m}; & \textit{other cases} \end{cases}$$

where e is arbitrary natural number and p is arbitrary odd prime number.

Corollary 1. (theorem of Wilson)

$$(p-1)! \equiv -1 \pmod{p}$$

where p is arbitrary odd prime number.

§3. *The case in which modulus M is an integral ideal of quadratic field.*

In this section we shall use the following notations.

m will denote a rational integer which does not contain any square factors without 1.

ω is $\sqrt{m}$ if $m\equiv 2, 3, \pmod{4}$ and is $\dfrac{1+\sqrt{m}}{2}$ if $m\equiv 1 \pmod{4}$.

$\mathbf{Z}$ will denote the ring of all rational integers.

$\mathbf{Q}$ will denote the field of all rational numbers.

O_m will denote the ring of all integers in $Q(\sqrt{m})$.

$M, M_1, M_2, M_3, \ldots$ will denote integral ideals of O_m.

$P, Q, R, P_1, P_2, P_3, \ldots$ will denote prime ideals of O_m.

$e, f, e_1, e_2, e_3, \ldots$ will denote natural numbers.

$N(M)$ will denote norm of integral M over $\mathbf{Q}$.

$N_m(M)$ will denote number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{M}$.

$G_m(M)$ will denote a group of reduced residue classes of O_m with respect to modulus integral ideal M.

$\mathfrak{S}_m(M)$ will denote a complete system of representatives of $G_m(M)$.

$\mathfrak{F}_m(M)$ will denote representative system of all solutions in O_m of congruence $\xi^2\equiv 1 \pmod{M}$.

$I_m(M)$ will denote number of elements, whose order is 2, of $G_m(M)$.

Let us call the prime ideal which divides $O_m \cdot 2$ (this means the integral ideal generated by 2 in O_m) even prime ideal, and we shall use notations such as P, Q. Let us call the prime ideal which does not divide $O_m \cdot 2$ odd prime ideal, and we shall use notations such as $R, P_1, P_2, P_3, \ldots$. About even prime ideals we have a familiar result;

$$O_m \cdot 2 = \begin{cases} PQ,\ Q=P' \neq P; & m\equiv 1 \pmod{8}, \\ P & ; m\equiv 5 \pmod{8}, \\ P^2 & ; m\equiv 2, 3 \pmod{4}, \end{cases}$$

where P' will denote a conjugate ideal of P over $\mathbf{Q}$.

Proposition 5. $N_m(R^e)=2$,

where e is arbitrary natural number and R is arbitrary odd prime ideal of O_m.

Proof. The proof is similar to that of proposition 1 in § 2.

Corollary 2. $\mathfrak{F}_m(R^e)=\{\pm 1\}$

Proposition 6. $N_m(p_1^{e_1}p_2^{e_2}\dots p_r^{e_r})=2^r$,

where $e_1, e_2, \dots, e_r$ are arbitrary natural numbers and $p_1, p_2, \dots, p_r$ are arbitrary odd prime ideals which are pairwise coprime and $r\geqq 2$.

Proof. The proof is similar to that of proposition 2 in § 2.

Let us consider number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{M}$ where an integral ideal M *of* O_m is divided by a few even ideals of O_m, classified into four cases in accordance with the decomposition form of 2 in $\mathbf{Q}(\sqrt{m})$.

Proposition 7. *When* $m\equiv 1 \pmod 8$, *let us put* $O_m\cdot 2=PQ$, $Q=P'\neq P$. *Then*

$$N_m(P^e)=N_m(Q^e)=\begin{cases}1; & e=1,\\ 2; & e=2,\\ 4; & e\geqq 3.\end{cases}$$

Proof. $N(P)=2$, therefore $N(P^e)=2^e$. Since P^e is a primitive ideal, using canonical basis over $\mathbf{Z}$, we obtain

$$P^e=\mathbf{Z}\cdot 2^e+\mathbf{Z}(r+\omega),\quad N(r+\omega)\equiv 0 \pmod{2^e}.$$

Since any integer of O_m is congruent to some rational integer, we obtain a complete system of representatives of O_m to modulus P^e;

$$\{0, 1, 2, \dots, 2^e-1\}.$$

Taking away the rational integers

$$\{0\cdot 2, 1\cdot 2, 2\cdot 2, \dots, (2^{e-1}-1)2\}$$

which are divided by P from the above complete system of representatives of O_m to modulus P^e, we get a representative system $\mathfrak{S}_m(P^e)$ of $G_m(P^e)$;

$$\mathfrak{S}_m(P^e)=\{1, 3, 5, \dots, 2^e-1\}.$$

Therefore $\mathfrak{S}_m(P)=\{1\}$, then it is clear that number of solution in O_m of congruence $\xi^2\equiv 1 \pmod{P}$ is only one and it is $1 \pmod{P}$. Since $\mathfrak{S}_m(P^2)=\{1, 3\}$, regarding $1^2\equiv 1 \pmod{P^2}$ and $3^2-1=2\cdot 2^2+0\cdot(r+\omega)\in P^2$ where $3\equiv -1 \pmod{P^2}$, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^2}$ is two and they are $\pm 1 \pmod{P^2}$.

Let us assume $e\geqq 3$. For any rational integer x in $\mathfrak{S}_m(P^e)$, if $x^2\equiv 1 \pmod{P^e}$, then $x^2\equiv 1 \pmod{Q^e}$, then $x^2\equiv 1 \pmod{P^eQ^e}$ i.e. $x^2\equiv 1 \pmod{2^e}$, then $x\equiv \pm 1, \pm 1+2^{e-1} \pmod{2^e}$. Conversely if $x\equiv \pm 1, \pm 1+2^{e-1} \pmod{2^e}$, then $x^2\equiv 1 \pmod{2^e}$ by the proof of proposition 3, then $x^2\equiv 1 \pmod{P^e}$, therefore $N_m(P^e)=4$ for $e\geqq 3$. Similarly we can obtain $N_m(Q)=1$, $N_m(Q^2)=2$ and $N(Q^e)=4$ for $e\geqq 3$, This completes the proof.

Corollary 3.

$$\mathfrak{F}_m(P^e)=\mathfrak{F}_m(Q^e)=\begin{cases}\{1\} & ;\ e=1,\\ \{\pm 1\} & ;\ e=2,\\ \{\pm 1, \pm 1+2^{e-1}\} & ;\ e\geqq 3.\end{cases}$$

Proposition 8. *When* $m\equiv 5 \pmod 8$, *let us put* $O_m\cdot 2=P$. *Then*

$$N_m(P^e)=\begin{cases}1; & e=1,\\ 4; & e=2,\\ 8; & e\geqq 3.\end{cases}$$

Proof. Using canonical basis over $\mathbf{Z}$, $P=2(\mathbf{Z}\cdot 1+\mathbf{Z}\cdot\omega)$. Thus $P^e=2^e(\mathbf{Z}\cdot 1+\mathbf{Z}\cdot\omega)$

$=\mathbf{Z}\cdot 2^e+\mathbf{Z}\cdot 2^e\omega$, therefore a necessary and sufficient condition that $\xi=x+y\omega$ $(x, y\in \mathbf{Z})$ should be a solution of congruence $\xi^2\equiv 1 \pmod{P^e}$ is

$$\begin{cases} x^2+\dfrac{m-1}{4}y^2\equiv 1 \pmod{2^e}, & (1)\\ (2x+y)y\equiv 0 \pmod{2^e}, & (2)\end{cases}$$

where $\omega^2=\omega+\dfrac{m-1}{4}$. Now a representative system of ring of residue classes of O_m to modulus P^e is

$$\{x+y\omega\in O_m;\ 0\leqq x<2^e,\ 0\leqq y<2^e,\ x,\ y\in \mathbf{Z}\}$$

and a necessary and sufficient condition that elements $x+y\omega$ of the above set should be divided by $2\cdot O_m=P$ is $x, y\equiv 0 \pmod 2$. Therefore we get the following complete system of representatives of a group $G_m(P^e)$;

$$\mathfrak{S}_m(P^e)=\{x+y\omega\in O_m;\ 0\leqq x<2^e,\ 0\leqq y<2^e, \text{ and } x \textit{ or } y\equiv 1 \pmod 2)\ x, y\in \mathbf{Z}\}. \qquad (3)$$

When $e=1$, $y\equiv 0 \pmod 2$ by (2), therefore $x\equiv 1 \pmod 2$ by (3). Conversely if $x\equiv 1 \pmod 2$, $y\equiv 0 \pmod 2$, it is clear that (1) and (2) are concluded. So number of solution in O_m of congruence $\xi^2\equiv 1 \pmod P$ is only one and it is

$$x+y\omega;\ x\equiv 1 \pmod 2,\ y\equiv 0 \pmod 2.$$

When $e=2$, $y\equiv 0 \pmod 2$ by (2), thus $x\equiv 1 \pmod 2$ by (3). Therefore $x\equiv 1, 3 \pmod{2^2}$, $y\equiv 0, 2 \pmod{2^2}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{p^2}$ is four and they are

$$x+y\omega;\ x\equiv 1, 3 \pmod{2^2},\ y\equiv 0, 2 \pmod{2^2}.$$

When $e\geqq 3$, $y\equiv 0 \pmod 2$ by (2), thus $x\equiv 1 \pmod 2$ by (3).

Therefore $\quad x\equiv 1, 3, 5, \dots, 2^e-1 \pmod{2^e}$,

$\qquad\qquad y\equiv 0, 2, 4, \dots, 2^e-2 \pmod{2^e}$;

namely $\quad x\equiv 2k-1 \pmod{2^e}$, $1\leqq k\leqq 2^{e-1}$,

$\qquad\qquad y\equiv 2l-2 \pmod{2^e}$, $1\leqq l\leqq 2^{e-1}$.

Regarding $m=8m'+5$ $(m'\in \mathbf{Z})$, let us replace x and y in (1) and (2) with the above x and y. Then

$$[\text{left-hand side of (1)}]\equiv 4\{k(k-1)+(2m'+1)(l-1)^2\}+1 \pmod{2^e},$$
$$[\text{left-hand side of (2)}]\equiv 4(2k+l-2)(l-1) \pmod{2^e}.$$

So (1) and (2) are equivalent to the following (4) and (5)

$$\begin{cases} k(k-1)+(2m'-1)(l-1)^2\equiv 0 \pmod{2^{e-2}}, & (4)\\ (2k+l-2)(l-1)\equiv 0 \pmod{2^{e-2}}. & (5)\end{cases}$$

Since the first term of left-hand side of (4) is even, the second term of left-hand side of (4) is also even. Therefore l is odd, thus the first factor of left-hand side of (5) is odd. Therefore the second factor of (5) is divided by 2^{e-2}. Then by (4), we obtain

$$k(k-1)\equiv 0 \pmod{2^{e-2}},\ 1\leqq k\leqq 2^{e-1}.$$

If k is even, $k\equiv 0 \pmod{2^{e-2}}$, thus $k=2^{e-2}$ or 2^{e-1}. If k is odd, $k\equiv 1 \pmod{2^{e-2}}$, thus $k=1$ or $1+2^{e-2}$. While

$$l\equiv 1 \pmod{2^{e-2}},\quad 1\leqq l\leqq 2^{e-1}.$$

Thus $l=1$ or $1+2^{e-2}$. Therefore we get $x\equiv \pm 1$ or $\pm 1+2^{e-1} \pmod{2^e}$, $y\equiv 0$ or $2^{e-1} \pmod{P^e}$. Since the converse is clear number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$ is eight and they are

$$x+y\omega;\ x\equiv \pm 1,\ \pm 1+2^{e-1} \pmod{2^e},\ y\equiv 0,\ 2^{e-1} \pmod{2^e}.$$

Corollary 4.

$$\mathfrak{Z}_m(P^e)=\begin{cases}\{1\} & ;\ e=1\\ \{\pm 1,\ \pm 1+2\omega\} & ;\ e=2\\ \{\pm 1,\ \pm 1+2^{e-1},\ \pm 1+2^{e-1}\omega,\ \pm 1+2^{e-1}+2^{e-1}\omega\} & ;\ e\geqq 3.\end{cases}$$

Proposition 9. *When* $m\equiv 2 \pmod 4$, *let us put* $2\cdot O_m=P^2$. *Then*

$$N_m(P^e)=\begin{cases}1;\ e=1,\\ 2;\ e=2,\ 3,\\ 4;\ e=4,\\ 8;\ e\geqq 5.\end{cases}$$

Proof. Using canonical basis, we obtain

$$P=s(\mathbf{Z}\cdot n_0+\mathbf{Z}\cdot(r+\omega)),\ s,\ n_0,\ r\in\mathbf{Z},\ 0\leqq r<n_0.$$

Then because of $N(P)=2=s^2n_0$, $s=1$, $n_0=2$. And because of $N(r+\omega)\equiv 0 \pmod{n_0}$, $r=0$. Therefore, $P=\mathbf{Z}\cdot 2+\mathbf{Z}\cdot\omega$. Now if e is even, let us put $e=2e'$, $e'\in\mathbf{Z}$. Then

$$P^e=(P^2)^{e'}=O_m\cdot 2^{e'}=\mathbf{Z}\cdot 2^{e'}+\mathbf{Z}\cdot 2^{e'}\omega.$$

If e is odd, let us put $e=2e'+1$, $e'\in\mathbf{Z}$. Then

$$P^e=(P^2)^{e'}P=2^{e'}(\mathbf{Z}\cdot 2+\mathbf{Z}\cdot\omega)=\mathbf{Z}\cdot 2^{e'+1}+\mathbf{Z}\cdot 2^{e'}\omega.$$

Therefore a necessary and sufficient condition that $x+y\omega$ $(x,\ y\in\mathbf{Z})$ should be a solution in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$ is if $e=1$,

$$x^2+my^2\equiv 1 \pmod 2, \tag{6}$$

and if $e=2e'\geqq 2$,

$$\begin{cases}x^2+my^2\equiv 1 \pmod{2^{e'}}, & (7)\\ 2xy\equiv 0 \pmod{2^{e'}}, & (8)\end{cases}$$

and if $e=2e'+1\geqq 3$,

$$\begin{cases}x^2+my^2\equiv 1 \pmod{2^{e'+1}}, & (9)\\ 2xy\equiv 0 \pmod{2^{e'}}. & (10)\end{cases}$$

Now a complete system of representatives of ring of residue classes of O_m to modulus P^e is if $e=2e'\geqq 2$,

$$\{x+y\omega\in O_m;\ 0\leqq x<2^{e'},\ 0\leqq y<2^{e'},\ x,\ y\in\mathbf{Z}\}$$

and if $e=2e'+1\geqq 1$,

$$\{x+y\omega\in O_m;\ 0\leqq x<2^{e'+1},\ 0\leqq y<2^{e'},\ x,\ y\in\mathbf{Z}\},$$

and a necessary and sufficient condition that the integer $x+y\omega$ above should be divided by P, is $x\equiv 0 \pmod 2$ in both cases. Therefore we get a system of representatives of $G_m(P^e)$: if $e=2e'\geqq 2$,

$$\mathfrak{S}_m(P^e)=\{x+y\omega\in O_m;\ 0\leqq x<2^{e'},\ 0\leqq y<2^{e'},\ x\equiv 1 \pmod 2,\ x,\ y\in\mathbf{Z}\} \tag{11}$$

and if $e=2e'+1\geqq 1$,

$$\mathfrak{S}_m(P^e)=\{x+y\omega\in O_m;\ 0\leqq x<2^{e'+1},\ 0\leqq y<2^{e'},\ x\equiv 1 \pmod 2,\ x,\ y\in\mathbf{Z}\}. \tag{12}$$

When $e=1$, $x\equiv 1 \pmod 2$ by (6) because m is even. Since the converse is clear, number of solution in O_m of congruence $\xi^2\equiv 1 \pmod P$ is only one $\pmod P$ and it is

$$x+y\omega,\ x\equiv 1 \pmod 2.$$

For if $x\equiv 1 \pmod 2$, $x'\equiv 1 \pmod 2$, $y,\ y'\in\mathbf{Z}$,

$$(x+y\omega)-(x'+y'\omega)=(x-x')+(y-y')\omega\in\mathbf{Z}\cdot 2+\mathbf{Z}\cdot\omega=P,$$

i.e. $x+y\omega\equiv x'+y'\omega \pmod P$.

When $e=2$, $x\equiv 1 \pmod 2$ by (7) because m is even. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^2}$ is two $\pmod{P^2}$ and they are

$$x+y\omega,\ x\equiv 1 \pmod 2.$$

For if $x\equiv 1 \pmod 2$, $x'\equiv 1 \pmod 2$, $y\equiv y' \pmod 2$

$$(x+y\omega)-(x'+y'\omega)=(x-x')+(y-y')\omega\in \mathbf{Z}\cdot 2+\mathbf{Z}\cdot 2\omega=P^2,$$

i.e. $x+y\omega\equiv x'+y'\omega \pmod{P^2}$,

but if $x\equiv 1 \pmod 2$, $x'\equiv 1 \pmod 2$, $y\not\equiv y' \pmod 2$,

$$(x+y\omega)-(x'+y'\omega)=(x-x')+(y-y')\omega\notin \mathbf{Z}\cdot 2+\mathbf{Z}\cdot 2\omega=P^2,$$

i.e. $x+y\not\equiv x'+y'\omega \pmod{P^2}$.

When $e=3$, $x^2+my^2\equiv 1 \pmod 2$ by (9), therefore $x\equiv 1 \pmod 2$. Then if we put $x=2x'+1$, $x'\in\mathbf{Z}$ in (9), using $m=4m'+2$, $m'\in\mathbf{Z}$, we get $2y^2\equiv 0 \pmod{2^2}$. Therefore $y^2\equiv 0 \pmod 2$; namely $y\equiv 0 \pmod 2$. Therefore $x\equiv\pm 1 \pmod{2^2}$, $y\equiv 0 \pmod 2$. Since the converse is clear, number of solutions of congruence $\xi^2\equiv 1 \pmod{P^3}$ is two and they are

$$x+y\omega,\ x\equiv\pm 1 \pmod{2^2},\ y\equiv 0 \pmod 2.$$

When $e=4$, similarly as above we get $x\equiv 1 \pmod 2$, $y\equiv 1 \pmod 2$. Therefore $x\equiv \pm 1 \pmod{2^2}$, $y\equiv 0, 2 \pmod{2^2}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^4}$ is four and they are

$$x+y\omega,\ x\equiv\pm 1 \pmod{2^2},\ y\equiv 0, 2 \pmod{2^2}.$$

When $e=2e'+1$, $e'\geqq 2$, $x\equiv 1 \pmod 2$ by (9), therefore $y\equiv 0 \pmod{2^{e'-1}}$ by (10), therefore

$$x\equiv 1, 3, 5, \dots, 2^{e'+1}-1 \pmod{2^{e'+1}},$$
$$y\equiv 0, 2^{e'-1} \pmod{2^{e'}}.$$

For the convenience of putting y into (9) let us consider y to modulus $2^{e'+1}$. Then we get

$$y\equiv 0,\ 2^{e'-1},\ 2^{e'},\ 3\cdot 2^{e'-1} \pmod{2^{e'+1}}.$$

But in any case $my^2\equiv 0 \pmod{2^{e'+1}}$. For if $y\equiv 2^{e'-1} \pmod{2^{e'+1}}$, then for some rational integers m', y',

$$my^2=(4m'+2)(2^{e'+1}y'+2^{e'-1})^2=2^{e'+1}\cdot 2^{e'-2}(2m'+1)(4y'+1)^2\equiv 0 \pmod{2^{e'+1}},$$

and if $y\equiv 3\cdot 2^{e'-1} \pmod{2^{e'+1}}$, then for some rational integers m', y'

$$my^2=(4m'+2)(2^{e'+1}y'+3\cdot 2^{e'-1})^2=2^{e'+1}\cdot 2^{e'-2}(2m'+1)(4y'+3)^2\equiv 0 \pmod{2^{e'+1}}$$

and if $y\equiv 0, 2^{e'}$, the conclusion is clear. Therefore if we put

$$x\equiv 2k-1 \pmod{2^{e'+1}} \quad 1\leqq k\leqq 2^{e'}$$

into (9) we get

$$k(k-1)\equiv 0 \pmod{2^{e'-1}}.$$

If k is even, then $k\equiv 0 \pmod{2^{e'-1}}$, $1\leqq k\leqq 2^{e'}$, then $k=2^{e'-1}, 2^{e'}$, then $x\equiv -1+2^{e'}$, $-1+2^{e'+1}$ $(\equiv -1) \pmod{2^{e'+1}}$. If k is odd, then $k\equiv 1 \pmod{2^{e'-1}}$, $1\leqq k\leqq 2^{e'}$, then $k=1$, $1+2^{e'-1}$, then $x\equiv 1$, $1+2^{e'} \pmod{2^{e'+1}}$. So we get $x\equiv\pm 1$, $\pm 1+2^{e'} \pmod{2^{e'+1}}$, $y\equiv 0$, $2^{e'-1} \pmod{2^{e'}}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$, $e=2e'+1$, $e'\geqq 2$ is eight and they are

$$x+y\omega,\ x\equiv\pm 1,\ \pm 1+2^{e'} \pmod{2^{e'+1}},\ y\equiv 0,\ 2^{e'-1} \pmod{2^{e'}}.$$

When $e=2e'$, $e'\geqq 3$, $x\equiv 1 \pmod 2$ by (7), therefore $y\equiv 0 \pmod{2^{e'-1}}$ by (8) therefore

$$x\equiv 1, 3, 5, \dots, 2^{e'}-1 \pmod{2^{e'}},$$
$$y\equiv 0,\ 2^{e'-1} \pmod{2^{e'}}.$$

But in both cases, $my^2\equiv 0 \pmod{2^{e'}}$. For if $y\equiv 2^{e'-1} \pmod{2^{e'}}$, then for some rational integers m', y'

$$my^2=(4m'+2)(2^{e'}y'+2^{e'-1})^2=2^{e'}\cdot 2^{e'-1}(2m'+1)(2y'+1)^2\equiv 0 \pmod{2^{e'}}$$

and if $y\equiv 0 \pmod{2^{e'}}$, the conclusion is clear. Therefore if we put

$$x\equiv 2k-1 \pmod{2^{e'}} \quad 1\leqq k\leqq 2^{e'-1}$$

into (7), we get

$$k(k-1)\equiv 0 \pmod{2^{e'-2}}.$$

If k is even, then $k\equiv 0 \pmod{2^{e'-2}}$, $1\leqq k\leqq 2^{e'-1}$, then $k=2^{e'-2}, 2^{e'-1}$, then $x\equiv -1+2^{e'-1}$, $-1+2^{e'}$ $(\equiv -1) \pmod{2^{e'}}$. If k is odd then $k\equiv 1 \pmod{2^{e'-2}}$, $1\leqq k\leqq 2^{e'-1}$, then $k=1$, $1+2^{e'-2}$, then $x\equiv 1$, $1+2^{e'-1} \pmod{2^{e'}}$. So we get $x\equiv \pm 1$, $\pm 1+2^{e'-1} \pmod{2^{e'}}$, $y\equiv 0$, $2^{e'-1} \pmod{2^{e'}}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$ $e=2e'$, $e'\geqq 3$, is eight and they are

$$x+y\omega,\ x\equiv \pm 1,\ \pm 1+2^{e'-1} \pmod{2^{e'}},\ y\equiv 0,\ 2^{e'-1} \pmod{2^{e'}}.$$

Corollary 5.

$$\mathfrak{F}_m(P^e)=\begin{cases}\{1\} & ;\ e=1\\ \{1,\ 1+\omega\} & ;\ e=2\\ \{\pm 1\} & ;\ e=3\\ \{\pm 1,\ \pm 1+2\omega\} & ;\ e=4\\ \{\pm 1,\ \pm 1+2^{e'},\ \pm 1+2^{e'-1}\omega,\ \pm 1+2^{e'}+2^{e'-1}\omega\} & ;\ e=2e'+1,\ e'\geqq 2\\ \{\pm 1,\ \pm 1+2^{e'-1},\ \pm 1+2^{e'-1}\omega,\ \pm 1+2^{e'-1}+2^{e'-1}\omega\} & ;\ e=2e'.\ e'\geqq 3.\end{cases}$$

Proposition 10. *When* $m\equiv 3 \pmod 4$, *let us put* $O_m\cdot 2=P^2$. *Then*

$$N_m(P^e)=\begin{cases}1;\ e=1,\\ 2;\ e=2,\ 3,\\ 4;\ e=4,\\ 8;\ e\geqq 5.\end{cases}$$

Proof. Using canonical basis we get

$$P=\mathbf{Z}\cdot 2+\mathbf{Z}\cdot(1+\omega),$$

$$P^e=\begin{cases}\mathbf{Z}\cdot 2^{e'}+\mathbf{Z}\cdot 2^{e'}\omega & ;\ e=2e',\\ \mathbf{Z}\cdot 2^{e'+1}+\mathbf{Z}\cdot 2^{e'}(1+\omega); & e=2e'+1,\end{cases}$$

in the same way as the proof in the proposition 9. Therefore a necessary and sufficient condition that $\xi=x+y\omega$, $x, y\in\mathbf{Z}$ should be a solution in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$ is if $e=1$,

$$x^2-2xy+my^2\equiv 1 \pmod 2, \tag{13}$$

and if $e=2e'\geqq 2$,

$$\begin{cases}x^2+my^2\equiv 1 \pmod{2^{e'}}, & (14)\\ 2xy\equiv 0 \pmod{2^{e'}}, & (15)\end{cases}$$

and if $e=2e'+1\geqq 3$,

$$\begin{cases}x^2-2xy+my^2\equiv 1 \pmod{2^{e'+1}}, & (16)\\ 2xy\equiv 0 \pmod{2^{e'}}. & (17)\end{cases}$$

Now a complete system of representatives of residue classes of O_m to modulus P^e is if $e=2e'\geqq 2$,

$$\{x+y\omega\in O_m;\ 0\leqq x<2^{e'},\ 0\leqq y<2^{e'},\ x,\ y\in\mathbf{Z}\},$$

and if $e=2e'+1\geqq 1$,

$$\{x+y\omega\in O_m;\ 0\leqq x<2^{e'+1},\ 0\leqq y<2^{e'},\ x,\ y\in\mathbf{Z}\}$$

and a necessary and sufficient condition that elements $x+y\omega$ in the above set should be divided by P is $x\equiv y \pmod 2$ in both cases, since $x+y\omega=x-y+y(1+\omega)$. Therefore we get a system of representatives of $G_m(P^e)$, if $e=2e'\geqq 2$,

$$\mathfrak{S}_m(P^e)=\{x+y\omega\in O_m;\ 0\leqq x<2^{e'},\ 0\leqq y<2^{e'},\ x\not\equiv y \pmod 2,\ x,\ y\in\mathbf{Z}\} \tag{18}$$

and if $e=2e'+1\geqq 1$,

$$\mathfrak{S}_m(P^e)=\{x+y\omega\in O_m;\ 0\leqq x<2^{e'+1},\ 0\leqq y<2^{e'},\ x\not\equiv y \pmod 2,\ x,\ y\in\mathbf{Z}\}. \tag{19}$$

When e=1, $x^2+y^2\equiv 1 \pmod 2$ by (13), therefore $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$ or $x\equiv 1 \pmod 2$, $y\equiv 0 \pmod 2$. But both should be contained in the same residue class of $O_m \pmod P$, because if $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$ and $x'\equiv 1 \pmod 2$, $y'\equiv 0 \pmod 2$,

$$(x+y\omega)-(x'+y'\omega)=\{(x-x')-(y-y')\}+(y-y')(1+\omega)\in \mathbf{Z}\cdot 2+\mathbf{Z}\cdot(1+\omega)=P$$

i.e. $\quad x+y\omega\equiv x'+y'\omega \pmod P$.

Therefore number of solution in O_m of congruence $\xi^2\equiv 1 \pmod P$ is only one $\pmod P$ and it is

$$x+y\omega,\quad x\not\equiv y \pmod 2.$$

When $e=2$, $x^2+y^2\equiv 1 \pmod 2$ by (14), therefore $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$ or $x\equiv 1 \pmod 2$, $y\equiv 0 \pmod 2$. But in this case $x+y\omega$, $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$ and $x'+y'\omega$, $x'\equiv 1 \pmod 2$, $y'\equiv 0 \pmod 2$ belong to two distinct residue classes of O_m to modulus P^2, because

$$(x+y\omega)-(x'+y'\omega)=(x-x')+(y-y')\omega\notin \mathbf{Z}\cdot 2+\mathbf{Z}\cdot 2\omega=P^2,$$

i.e. $\quad x+y\omega\not\equiv x'+y'\omega \pmod{P^2}$.

Therefore number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^2}$ is two and they are

$$x+y\omega,\ \begin{cases}x\equiv 0 \pmod 2\\ y\equiv 1 \pmod 2,\end{cases}\ \begin{cases}x\equiv 1 \pmod 2\\ y\equiv 0 \pmod 2.\end{cases}$$

When $e=3$ we get $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$ or $x\equiv 1 \pmod 2$ $y\equiv 0 \pmod 2$ in the same way as the case $e=1, 2$ in this proposition. If $x\equiv 0 \pmod 2$, $y\equiv 1 \pmod 2$, for some rational integers x', y',

$$[\text{left-hand side of (16)}]=(2x')^2-2\cdot 2x'\cdot(2y'+1)+m(2y'+1)^2\equiv m \pmod 4,$$

then $m\equiv 1 \pmod 4$. This is a contradiction. So $x\equiv 1 \pmod 2$, therefore $x\equiv \pm 1 \pmod{2^2}$, $y\equiv 0 \pmod 2$. Since the converse is clear number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^3}$ is two and they are

$$x+y\omega,\ x\equiv\pm 1 \pmod{2^2},\ y\equiv 0 \pmod 2.$$

When $e=4$, we get $x\equiv 1 \pmod 2$, $y\equiv 0 \pmod 2$ in the same way as the case $e=3$ in this proposition. Therefore $x\equiv\pm 1 \pmod{2^2}$, $y\equiv 0, 2 \pmod{2^2}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^4}$ is four and they are

$$x+y\omega,\ x\equiv\pm 1 \pmod{2^2},\ y\equiv 0, 2 \pmod{2^2}.$$

When $e=2e'+1$, $e'\geqq 2$, we get $x\equiv 1 \pmod 2$, $y\equiv 0 \pmod 2$ in the same way as the case $e=3$ in this proposition. Therefore

$$\begin{cases}x\equiv 1, 3, 5, \dots, 2^{e'+1}-1 \pmod{2^{e'+1}}\\ y\equiv 0, 2, 4, \dots, 2^{e'}-2 \pmod{2^{e'}},\end{cases}$$

then let us put using some rational integer $x'y'$,

$$\begin{cases}x=2^{e'+1}x'+2k-1, & 1\leqq k\leqq 2^{e'},\\ y=2^{e'}y'+2l-2, & 1\leqq l\leqq 2^{e'-1}.\end{cases}$$

Then we get out of (16) and (17)

$$\begin{cases}k(k-1)-(2k-1)(l-1)+m(l-1)^2\equiv 0 \pmod{2^{e'-1}} & (16)'\\ (2k-1)(l-1)\equiv 0 \qquad\qquad \pmod{2^{e'-2}} & (17)'\end{cases}$$

therefore by (17)$'$ $l\equiv 1 \pmod{2^{e'-2}}$, $1\leqq l\leqq 2^{e'-1}$, then $l=1$, $2^{e'-2}+1$, then $y\equiv 0$, $2^{e'-1} \pmod{2^{e'}}$. When $l=1$, then by (16)$'$ $k(k-1)\equiv 0 \pmod{2^{e'-1}}$. Therefore if k is even, then $k\equiv 0 \pmod{2^{e'-1}}$, $1\leqq k\leqq 2^{e'}$, then $k=2^{e'-1}$, $2^{e'}$, then $x\equiv -1+2^{e'}$, $-1+2^{e'+1}$ $(\equiv -1)$ $\pmod{2^{e'+1}}$. If k is odd, then $k\equiv 1 \pmod{2^{e'-1}}$, $1\leqq k\leqq 2^{e'}$, then $k=1$, $1+2^{e'-1}$, then $x\equiv 1$, $1+2^{e'} \pmod{2^{e'+1}}$. Therefore if $l=1$; namely $y\equiv 0 \pmod{2^{e'}}$, then $x\equiv\pm 1$, $\pm 1+2^{e'} \pmod{2^{e'+1}}$.

Next let us consider the case $l=2^{e'-2}+1$. By (16)$'$ we obtain

$$k(k-1)+2^{e'-2}\equiv 0 \pmod{2^{e'-1}}.$$

Therefore

$$\begin{cases} k(k-1)\equiv 0 \pmod{2^{e'-2}} \\ \dfrac{k(k-1)}{2^{e'-2}}+1\equiv 0 \pmod{2}, \end{cases}$$

where $\dfrac{k(k-1)}{2^{e'-2}}$ is odd. Now if k is even, then $k\equiv 0 \pmod{2^{e'-2}}$ and $\dfrac{k}{2^{e'-2}}\cdot(k-1)$ is odd, therefore $\dfrac{k}{2^{e'-2}}$ is also odd. If we denote

$$\frac{k}{2^{e'-2}}=2k'+1$$

for some rational integer k', we obtain $k=2^{e'-1}k'+2^{e'-2}$, $1\leqq k\leqq 2^{e'}$, then $k=2^{e'-2}$, $2^{e'-2}+2^{e'-1}$, then $x\equiv -1+2^{e'-1}$, $-1+2^{e'-1}+2^{e'} \pmod{2^{e'+1}}$. If k is odd, then $k\equiv 1 \pmod{2^{e'-2}}$ and $k\cdot\dfrac{k-1}{2^{e'-2}}$ is odd, therefore $\dfrac{k-1}{2^{e'-2}}$ is also odd. If we denote

$$\frac{k-1}{2^{e'-2}}=2k'+1$$

for some rational integer k, we obtain $k=1+2^{e'-2}+2^{e'-1}k'$, $1\leqq k\leqq 2^{e'}$, then $k=1+2^{e'-2}$, $1+2^{e'-2}+2^{e'-1}$, then $x\equiv 1+2^{e'-1}$, $1+2^{e'-1}+2^{e'} \pmod{2^{e'+1}}$. Therefore if $l=2^{e'-2}+1$; namely $y\equiv 2^{e'-1} \pmod{2^{e'}}$, then $x\equiv \pm 1+2^{e'-1}$, $\pm 1+2^{e'-1}+2^{e'} \pmod{2^{e'+1}}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$ where $e=2e'+1$, $e'\geqq 2$ is eight and they are

$$x+y\omega,\ \begin{cases} x\equiv \pm 1,\ \pm 1+2^{e'} \pmod{2^{e'+1}} \\ y\equiv 0 \qquad\qquad \pmod{2^{e'}} \end{cases},\ \begin{cases} x\equiv \pm 1+2^{e'-1},\ \pm 1+2^{e'-1}+2^{e'} \pmod{2^{e'+1}} \\ y\equiv 2^{e'-1} \qquad\qquad \pmod{2^{e'}} \end{cases}.$$

When $e=2e'$, $e'\geqq 3$, we get $x\equiv 1 \pmod{2}$, $y\equiv 0 \pmod{2}$ in the same way as the case $e=3$ in this proposition. Therefore

$$\begin{cases} x\equiv 1, 3, 5, \dots, 2^{e'}-1 \pmod{2^{e'}}, \\ y\equiv 0, 2, 4, \dots, 2^{e'}-2 \pmod{2^{e'}}, \end{cases}$$

then let us put using some rational integer x', y'

$$\begin{cases} x=2^{e'}x'+2k-1, & 1\leqq k\leqq 2^{e'-1} \\ y=2^{e'}y'+2l-2, & 1\leqq l\leqq 2^{e'-1}. \end{cases}$$

Then we get out of (14) and (15)

$$\begin{cases} k(k-1)+m(l-1)^2\equiv 0 \pmod{2^{e'-2}} & (14)' \\ (2k-1)(l-1)\equiv 0 \qquad \pmod{2^{e'-2}}, & (15)' \end{cases}$$

therefore by (15)$'$, $l\equiv 1 \pmod{2^{e'-2}}$, $1\leqq l\leqq 2^{e'-1}$, then $l=1$, $1+2^{e'-2}$, then $y\equiv 0$, $2^{e'-1} \pmod{2^{e'}}$.

Now in both cases we obtain $k(k-1)\equiv 0 \pmod{2^{e'-2}}$ by (14)$'$, therefore if k is even, then $k\equiv 0 \pmod{2^{e'-2}}$, $1\leqq k\leqq 2^{e'-1}$, then $k=2^{e'-2}$, $2^{e'-1}$, then $x\equiv -1+2^{e'-1}$, $-1+2^{e'}$ $(\equiv -1) \pmod{2^{e'}}$. If k is odd, then $k\equiv 1 \pmod{2^{e'-1}}$, $1\leqq k\leqq 2^{e'-1}$, then $k=1$, $1+2^{e'-2}$, then $x=1$, $1+2^{e'-1} \pmod{2^{e'}}$. Therefore we obtain $x\equiv \pm 1$, $\pm 1+2^{e'-1} \pmod{2^{e'}}$. Since the converse is clear, number of solutions in O_m of congruence $\xi^2\equiv 1 \pmod{P^e}$, $e=2e'$, $e'\geqq 3$ is eight and they are

$$x+y\omega,\ x\equiv \pm 1,\ \pm 1+2^{e'-1} \pmod{2^{e'}},\ y\equiv 0,\ 2^{e'-1} \pmod{2^{e'-1}}.$$

This completes the proof.

Corollary 6.

$$\mathfrak{F}_m(P^e)=\begin{cases}\{1\} & ;\ e=1,\\ \{1,\ \omega\} & ;\ e=2,\\ \{\pm 1\} & ;\ e=3,\\ \{\pm 1,\ \pm 1+2\omega\} & ;\ e=4,\\ \{\pm 1,\ \pm 1+2^{e'},\ \pm 1+2^{e'-1}+2^{e'-1}\omega,\ \pm 1+2^{e'-1}+2^{e'}+2^{e'-1}\omega\} & \\ & ;\ e=2e'+1,\ e'\geqq 2,\\ \{\pm 1,\ \pm 1+2^{e'-1},\ \pm 1+2^{e'-1}\omega,\ \pm 1+2^{e'-1}+2^{e'-1}\omega\} & \\ & ;\ e=2e',\ e'\geqq 3.\end{cases}$$

Proposition 11.

(i) *When* $m\equiv 1 \pmod 8$, *let us denote the decomposition into products of prime ideals of integral ideal* M *of* O_m *by* $M=P^eQ^fP_1^{e_1}P_2^{e_2}\dots P_r^{e_r}$, *where* P, Q *are even prime ideals of* O_m *such that* $O_m\cdot 2=PQ$, $Q=P'\neq P$, *and* $P_1, P_2, \dots, P_r$ *are odd prime ideals of* O_m *and* $e, f, e_1, e_2, \dots, e_r$ *are nonnegative integers. Then*

$$N_m(M)=\begin{cases}2^r\ ;\ (e,f)=(0,0),\ (0,1),\ (1,0),\ (1,1)\\ 2^{r+1};\ (e,f)=(0,2),\ (1,2),\ (2,1),\ (2,0)\\ 2^{r+2};\ (e,f)=(2,2),\ (0,f),\ (e,0),\ (1,f),\ (e,1)\\ \qquad\qquad \text{where } e,\ f\geqq 3\\ 2^{r+3};\ (e,f)=(2,f),\ (e,2)\ \ \text{where } e,\ f\geqq 3\\ 2^{r+4};\ e,\ f\geqq 3,\end{cases}$$

where if $r=0$, *then* $e\geqq 1$ *or* $f\geqq 1$ *and if* $e=f=0$, *then* $r\geqq 1$.

(ii) *When* $m=5 \pmod 8$, *let us denote the decomposition into products of prime ideals of integral ideal* M *of* O_m *by* $M=P^eP_1^{e_1}P_2^{e_2}\dots P_r^{e_r}$, *where* P *is an even prime ideal of* O_m *such that* $O_m\cdot 2=P$, *and* $P_1, P_2, \dots, P_r$ *are odd prime ideals of* O_m *and* $e, e_1, e_2, \dots, e_r$ *are nonnegative integers. Then*

$$N_m(M)=\begin{cases}2^r\ ;\ e=0,\ 1,\\ 2^{r+2};\ e=2,\\ 2^{r+3};\ e\geqq 3,\end{cases}$$

where if $r=0$, *then* $e\geqq 1$ *and if* $e=0$ *then* $r\geqq 1$.

(iii) *When* $m=2, 3 \pmod 4$, *let us denote the decomposition into products of prime ideals of integral ideal* M *of* O_m *by* $M=P^eP_1^{e_1}P_2^{e_2}\dots P_r^{e_r}$, *where* P *is an even prime ideal of* O_m *such that* $O_m\cdot 2=P^2$, *and* $P_1, P_2, \dots, P_r$ *are odd prime ideals of* O_m *and* $e, e_1, e_2, \dots, e_r$ *are nonnegative integers. Then*

$$N_m(M)=\begin{cases}2^r\ ;\ e=0,\ 1,\\ 2^{r+1};\ e=2,\ 3,\\ 2^{r+2};\ e=4,\\ 2^{r+3};\ e\geqq 5,\end{cases}$$

where if $r=0$, *then* $e\geqq 1$ *and if* $e=0$ *then* $r\geqq 1$.

Proof. It is clear by propositions above mentioned.

We have obtained the following two theorems which depend upon the conclusions of propositions above mentioned. The first theorem, theorem 3, is clear by proposition 11. The second, theorem 4, is clear by lemma 2 and theorem 3.

Theorem 3. *P and Q are even prime ideals of O_m such that*

$O_m\cdot 2=PQ,\ Q=P'\neq P;\ m\equiv 1 \pmod 8$,

$O_m\cdot 2=P\qquad\qquad ;\ m\equiv 5 \pmod 8$,

$$O_m \cdot 2 = P^2 \qquad ; m \equiv 2, 3 \pmod 4,$$

and R is an odd prime ideal of O_m. Then a necessary and sufficient condition that $I_m(M) = 1$; namely $N_m(M)=2$ is

(i) *in the case in which M does not contain any even prime ideals of O_m*

$$M = R^e,$$

(ii) *in the case in which M contains several even prime ideals of O_m*

$$M = \begin{cases} PR^e,\ QR^e,\ PQR^e,\ P^2,\ Q^2,\ P^2Q,\ PQ^2; & m \equiv 1 \pmod 8), \\ PR^e & ; m \equiv 5 \pmod 8), \\ PR^e,\ P^2,\ P^3 & ; m \equiv 2, 3 \pmod 4), \end{cases}$$

where e is arbitrary nonnegative integer.

Theorem 4. (i) *Let M be an integral ideal of O_m which has any type explained in the theorem 3. Then*

$$\prod_{\xi \in \mathfrak{S}_m(M)} \xi \equiv \begin{cases} -1 \pmod M & ; m \equiv 2, 3 \pmod 4 \text{ and } M \neq P^2 \\ 1+\omega \pmod M; & m \equiv 2 \pmod 4 \text{ and } M = P^2 \\ \omega \pmod M & ; m \equiv 3 \pmod 4 \text{ and } M = P^2 \\ -1 \pmod M & ; \text{other cases.} \end{cases}$$

(ii) *Let M be an integral ideal of O_m which does not have any type explained in the theorem 3. Then*

$$\prod_{\xi \in \mathfrak{S}_m(M)} \xi \equiv 1 \pmod M.$$

Remark. Except for the case $m \equiv 2, 3 \pmod 4$ and $M = P^2$, if $N_m(M)=2$, then the element of $G_m(M)$ whose order is 2, is $-1 \pmod M$ but in the case $m \equiv 2 \pmod 4$ and $M = P^2$, we obtained in corollary 5 $N_m(M)=2$ and $1 \equiv -1 \pmod M$ and the element of $G_m(M)$ whose order is 2, is $1+\omega \pmod M$. And in the case $m \equiv 3 \pmod 4$ and $M=P^2$, we obtained in corollary 7 $N_m(M)=2$ and $1 \equiv -1 \pmod M$ and the element of $G_m(M)$ whose order is 2, is $\omega \pmod M$.

REFERENCE

G. H. Hardy & E. M. Wright, *An introduction to the theory of Numbers*, Oxford, fourth edition, 1960.

(May 10, 1977)