# Solutions of congruence equations via an imprimitive action of some modular subgroups

Seda Öztürk[1], Yavuz Kesicioğlu[2] and Hatice Şengül[3]

[1], [3]Department of Mathematics, Faculty of Science, Karadeniz Technical University, Trabzon, Türkiye
[2]Department of Mathematics, Faculty of Science and Arts, Recep Tayyip Erdoğan University, Rize, Türkiye
E-mail: seda.ozturk@ktu.edu.tr[1], yavuz.kesicioglu@erdogan.edu.tr[2], ecitah28@gmail.com[3]

**Abstract**

Let $N$ be a positive integer and $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ the prime power decomposition of $N$ where $p_i \equiv 1 \pmod 4$, for all $1 \leq i \leq r$. There, without the Girard-Fermat Theorem by no means, are integers $a$ and $x$ such that $a^2 + x^2 \equiv 0 \pmod N$ by using a special imprimitive action of some modular subgroups. Finally we put a conjecture at the end of the paper.

*2010 Mathematics Subject Classification.* **20H05**. 11F06, 05C25.
*Keywords.* congruence equations, modular subgroup, imprimitive action.

## 1 Introduction

The characterization of prime numbers of rational integers are so important not only in number theory but also in almost all areas of mathematics. One of the important theorems is the Girard-Fermat Theorem on which several authors worked, see [4, 10, 9], is as follows.

**Theorem 1.1.** Let $p$ be a prime of the form $p \equiv 1 \pmod 4$, then there exist integers $x$ and $y$ such that $p = x^2 + y^2$.

Of course, our claim in abstract follows from Theorem 1.1, which will mention at the end of paper. But here, we prove the claim by using completely a different approach, an imprimitive action for some modular subgroups. For this, we outline the followings.

The modular group $\Gamma$ consists of $2 \times 2$ matrices with determinant 1 and integers entries. That is,

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \text{ are integers and } ad - bc = 1 \right\}$$

which is the well known discrete group on which several works were performed [2, 1, 5, 6].We below give some subgroups of $\Gamma$ which will be needed in the subsequent work. For any natural number $N$,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \,(\text{mod } N) \right\},$$

$$\Gamma_{0,n}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv d \,(\text{mod } n), \text{ or equivalently} \right.$$

$$\left. a^2 \equiv 1 \,(\text{mod } n),\ n | N \right\},$$

**Advanced Studies: Euro-Tbilisi Mathematical Journal** 16, supplement issue 3 (2023), pp. 139–143.
DOI: 10.32513/asetmj/1932200823310
Tbilisi Centre for Mathematical Sciences.
*Received by the editors:* 23 july 2023.
*Accepted for publication:* 05 October 2023.

and that,

$$\Lambda_n(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a^2 \equiv d^2 \,(\mathrm{mod}\ n), \text{ or equivalently } a^4 \equiv 1 \,(\mathrm{mod}\ n),\ n|N \right\}$$

are all subgroups of $\Gamma$.

We now introduce imprimitive transitive permutation groups as follows.

Let $(G, X)$ be a transitive permutation group. The relation on $X$ defined by, for all $a, b \in X$,

$$a \approx b \text{ if and only if } g(a) \approx g(b) \text{ for all } g \in G,$$

is an equivalence relation called $G$-invariant, and the equivalence classes are called blocks.

It is easily seen that any transitive permutation group $(G, X)$ has at least two $G$-invariant equivalence relations as

**(i)** $a \approx b \iff a = b$ (trivial relation),

**(ii)** $a \approx b$, for all $a, b \in X$ (universal relation)

If the group $(G, X)$ has a $G$-invariant equivalence relation other than the above two then the relation (or the group $(G, X)$) is called imprimitive otherwise primitive.

**Lemma 1.2.** [3, Theorem 1.6.5] Let $(G, X)$ be a transitive permutation group. Then, for all $a \in X$, the stabilizer $G_a$ is maximal in $G$ if and only if the group $(G, X)$ is primitive.

**Lemma 1.3.** [5, p.319] Let $(G, X)$ be a transitive permutation group, $H$ a subgroup of $G$, and for some $a \in X$,

$$G_a \lneqq H \lneqq G \tag{1.1}$$

and that if for any $x, y \in X, x = g(a), y = h(a)$, for some, $g, h \in G$ then, the relation defined by

$$x \approx y \text{ if and only if } gh^{-1} \in H$$

is an imprimitive $G$-invariant equivalence relation and the number of blocks is the index $|G : H|$.

## 2 Main calculations

**Lemma 2.1.** Let $n, N$ be naturel numbers, $n$ odd and $n \mid N$ and that $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime power decomposition of $n$. Then $p_i \equiv 3 \pmod 4$ for $1 \leq i \leq r$ if and only if $\Lambda_n(N) = \Gamma_{0,n}(N)$.

*Proof.* It is clear that $\Gamma_{0,n}(N) \leq \Lambda_n(N)$. For the converse, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda_n(N)$. Then $a^4 \equiv 1 \pmod n$. So we get $(a^2 - 1)(a^2 + 1) \equiv 0 \pmod n$. Since, for all $1 \leq i \leq r$, the legendre symbol $\left(\frac{-1}{p_i}\right) \neq 1$, $p_i \equiv 3 \pmod 4$. This shows that $p_i \mid a^2 - 1$, that is, $a^2 \equiv 1 \pmod n$. This gives that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_{0,n}(N)$. This completes the proof. Q.E.D.

**Corollary 2.2.** Let $n, N$ be as above. If one of the prime divisor of $p$ of $n$ is of the form $p \equiv 1 \pmod 4$ then $\Gamma_{0,n}(N) < \Lambda_n(N)$.

*Proof.* The proof follows easily from Lemma 2.1. Q.E.D.

We use Lemma 1.3 to calculate some indexes of some modular subgroups from above. Let $G = \Gamma_0(N), H = \Gamma_{0,n}(N)$ and $G_\alpha = \Gamma_0(N)_\infty =$ the stabilizier of $\infty$ in $\Gamma_0(N)$, and $X = \mathbb{Q}_N = \{\frac{a}{bN} \mid a, b \in \mathbb{Z}\}$. Then we get $\Gamma_0(N)_\infty < \Gamma_{0,n}(N) < \Gamma_0(N)$. Of course, it is easy to see that $\Gamma_0(N)$ is transitive on $\mathbb{Q}_N$. As in Lemma 1.3, if $\frac{r}{sN}, \frac{x}{yN} \in \mathbb{Q}_N$ then there exist elements $g, h$ in $\Gamma_0(N)$ and that $g(\infty) = \frac{r}{sN}$ and $h(\infty) = \frac{x}{yN}$. Therefore

$$\frac{r}{sN} \approx \frac{x}{yN} \iff gh^{-1} \in \Gamma_{0,n}(N).$$

$g = \begin{pmatrix} r & r_0 \\ sN & s_0 \end{pmatrix}$, $h = \begin{pmatrix} x & x_0 \\ yN & y_0 \end{pmatrix}$, $gh^{-1} = \begin{pmatrix} ry_0 - r_0yN & -rx_0 + r_0x \\ sNy_0 - s_0yN & -sNx_0 + s_0x \end{pmatrix} \in \Gamma_{0,n}(N)$ if and if only $ry_0 \equiv s_0x \pmod n$. Since, $rs_0 \equiv 1 \pmod n, xy_0 \equiv 1 \pmod n$ then $s_0 \equiv r^{-1} \pmod n$ and $y_0 \equiv x^{-1} \pmod n$. That is, at the end,

$$\frac{r}{sN} \underset{n}{\approx} \frac{x}{yN} \iff r^2 \equiv x^2 \pmod n.$$

Therefore with this relation "$\underset{n}{\approx}$" $(\Gamma_0(N), \mathbb{Q}_N)$ is an imprimitive transitive permutation group by using the subgroup $\Gamma_{0,n}(N)$. The number $\gamma(n)$ of equivalence classes under $\underset{n}{\approx}$ is give by $\gamma(n) =\mid \Gamma_0(N) : \Gamma_{0,n}(N) \mid$ by lemma 1.3.

**Proposition 2.3.** Let $n, N$ be positive integers $n \mid N, n \geq 2$ odd, and let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime power decomposition of $n$ then $\gamma(n) = \frac{\varphi(n)}{2^r}$, where $\varphi$ is the Euler function.

*Proof.* We first show that $\gamma$ is a multiplicative function. Let $n = n_1 \cdot n_2$ with $(n_1, n_2) = 1$. We have to show that

$$r \underset{n}{\approx} x \text{ if and only if } r \underset{n_1}{\approx} x \text{ and } r \underset{n_2}{\approx} x$$

where $r \underset{n}{\approx} x$ shows $\frac{r}{sN} \underset{n}{\approx} \frac{x}{yN}$.

It is clear that $r \approx x$ gives $r \underset{n_1}{\approx} x$ and $r \underset{n_2}{\approx} x$. For the converse, suppose that $r_1 \underset{n_1}{\approx} x_1$ and $r_2 \underset{n_2}{\approx} x_2$. Since $(n_1, n_2) = 1$, there exist integers $k_1, k_2, k_3, k_4$ such that

$$r_1 - r_2 = -k_1n_1 + k_2n_2 \text{ and } x_1 - x_2 = -k_3n_1 + k_4n_2$$

Therefore $r_1 + k_1n_1 = r_2 + k_2n_2$ and $x_1 + k_3n_1 = x_2 + k_4n_2$. So it is easily seen that $(r_1 + k_1n_1)^2 \equiv (x_1 + k_3n_1)^2 \pmod{n_1 \cdot n_2}$. That is $r_1 + k_1n_1 \underset{n}{\approx} x_1 + k_3n_1$ (or $r_2 + k_2n_2 \underset{n}{\approx} x_2 + k_4n_2$). This concludes that $\gamma(n) = \gamma(n_1) \cdot \gamma(n_2)$, which is what we want. Therefore, it is enough to calculate only $\gamma(p^\alpha)$ where $p^\alpha \mid N$ and $\left(p^\alpha, \frac{N}{p^\alpha}\right) = 1$. Let $r \underset{p^\alpha}{\approx} x$. Then $r^2 \equiv x^2 \pmod{p^\alpha}$. Notice that $x \underset{p^\alpha}{\approx} p^\alpha - x$. So the representatives can be choosen from the sequence $1, 2, \ldots, \frac{p^\alpha - 1}{2}$, whose number is $\frac{\varphi(p^\alpha)}{2}$. $r^2 \equiv x^2 \pmod{p^\alpha}$ gives $(r - x)(r + x) \equiv 0 \pmod{p^\alpha}$. Therefore, $p^\alpha \mid r - x$ or $p^\alpha \mid r + x$. From the choice of representatives we get $p^\alpha \mid r - x$. That is, $r = x$. This completes the proof that $\gamma(p^\alpha) = \frac{\varphi(p^\alpha)}{2}$. This concludes that $\gamma(n) = \frac{\varphi(n)}{2^r}$. Q.E.D.

**Lemma 2.4.** Let $p$ is a prime of the form $p \equiv 1 \pmod 4$ and $\alpha$ be a positive integer. Then $\mid \Lambda_{p^\alpha}(p^\alpha) : \Gamma_{0,p^\alpha}(p^\alpha) \mid = 2$

*Proof.* Let $\mathbb{Q}(p^\alpha)$ denote the orbit of $\infty$ under $\Lambda_{p^\alpha}(p^\alpha)$. Then $\mathbb{Q}(p^\alpha) = \{\frac{a}{bp^\alpha} : a^4 \equiv 1 \pmod{p^\alpha}\}$. From $a^4 \equiv 1 \pmod{p^\alpha}$ we get $a \equiv 1 \pmod{p^\alpha}$, or $a \equiv -1 \pmod{p^\alpha}$, or $a^2 + 1 \equiv 0 \pmod{p^\alpha}$. So we have $\frac{\mp 1 + kp^\alpha}{bp^\alpha} \in \mathbb{Q}(p^\alpha)$ where $k, b \in \mathbb{Z}$. On the other hand $p \equiv 1 \pmod 4$ gives a solution $p_0$ of $a^2 + 1 \equiv 0 \pmod{p^\alpha}$. Then $\frac{\mp p_0 + lp^\alpha}{cp^\alpha} \in \mathbb{Q}(p^\alpha)$ where $l, c \in \mathbb{Z}$. Consequently, it is easily seen that $\mathbb{Q}(p^\alpha) = \{\frac{\mp 1 + kp^\alpha}{bp^\alpha}, \frac{\mp p_0 + lp^\alpha}{cp^\alpha} : k, b, l, c \in \mathbb{Z} \quad \text{and} \quad p_0^2 \equiv -1 \pmod{p^\alpha}\}$.

Now we will get the primitive transitive permutation group $\big(\Lambda_{p^\alpha}(p^\alpha), \mathbb{Q}(p^\alpha)\big)$ by the group $\Gamma_{0,p^\alpha}(p^\alpha)$ as follows. As in Lemma 1.3, if $\frac{r}{sp^\alpha}, \frac{x}{yp^\alpha} \in \mathbb{Q}(p^\alpha)$ then

$$\frac{r}{sp^\alpha} \approx \frac{x}{yp^\alpha} \iff x^2 \equiv r^2 \pmod{p^\alpha}. \tag{2.1}$$

So it is easily seen that $\frac{\mp 1 + kp^\alpha}{bp^\alpha} \approx \frac{\mp 1 + mp^\alpha}{cp^\alpha}$ and $\frac{\mp p_0 + lp^\alpha}{tp^\alpha} \approx \frac{\mp p_0 + up^\alpha}{vp^\alpha}$ for all $k, m, b, c, , l, t, u, v \in \mathbb{Z}$. And that $\frac{\mp 1 + kp^\alpha}{bp^\alpha} \not\approx \frac{\mp p_0 + lp^\alpha}{cp^\alpha}$. Therefore, there are just 2 classes of the equivalence relation. This completes the proof. Q.E.D.

**Theorem 2.5.** Let $N$ be an odd natural number and that $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime power decomposition of $N$, where $p_i \equiv 1 \pmod 4, 1 \le i \le r$. Then, there are $x, a \in \mathbb{Z}$ such that $x^2 + a^2 \equiv 0 \pmod N$.

*Proof.* Let $N = N_1 \cdot N_2$ with $(N_1, N_2) = 1$. We show that if $x_1^2 + a_1^2 \equiv 0 \pmod{N_1}$ and $x_2^2 + a_2^2 \equiv 0 \pmod{N_2}$ then there exist integers $x$ and $a$ such that $x^2 + a^2 \equiv 0 \pmod N$. For this let $x = N_2 x_1 + N_1 x_2$ and $a = N_2 a_1 + N_1 a_2$ then it is easily seen that $x^2 + a^2 \equiv 0 \pmod N$. So to prove the theorem it is enough to prove it only for prime powers $p^\alpha$ with $p \equiv 1 \pmod 4$. Let $G = \Gamma_0(p^\alpha), H = \Lambda_{p^\alpha}(p^\alpha), X = \mathbb{Q}_{p^\alpha}$. If we use Lemma 1.3 we get that $(\Gamma_0(p^\alpha), \mathbb{Q}_{p^\alpha})$ is an imprimitive transitive permutation group with respect to $\Lambda_{p^\alpha}(p^\alpha)$. In this situation, imprimitive equivalence relation occurs as

$$\frac{a}{bp^\alpha} \approx \frac{x}{yp^\alpha} \,(\text{or shortly } a \approx x) \iff a^4 \equiv x^4 \pmod{p^\alpha}. \tag{2.2}$$

It is clear that $a \approx a + p^\alpha$ and that $l \approx p^\beta - l$. So, the representatives of the equivalence classes can be choosen from the sequence $1, 2, ..., \frac{p^\alpha - 1}{2}$. From this we get, if $\mid a \mid = \mid x \mid$ and $a^4 \equiv x^4 \pmod{p^\alpha}$, that is $p^\alpha \mid a^2 - x^2$ or $p^\alpha \mid a^2 + x^2$. The case $p^\alpha \mid a^2 - x^2$ does not occur otherwise $p^\alpha \mid (a-x)(a+x)$. Then $p^\alpha \mid a - x$ or $p^\alpha \mid a + x$. From the choice of representatives $a = x$ which is not the case. Consequently $p^\alpha \mid a^2 + x^2$ that is $x^2 + a^2 \equiv 0 \pmod{p^\alpha}$. This completes the proof.

Q.E.D.

As promised above we conclude the paper to prove Theorem 2.5 for primes $p \equiv 1 \pmod 4$ by using the Girard-Fermat Theorem (Theorem 1.1). Since $p \equiv 1 \pmod 4$, then by the Girard-Fermat Theorem, there exist integers $u$ and $v$ such that $u^2 + v^2 = p$. And then for any natural number $\beta$, if we take $x + iy = (u + iv)^\beta$, then we get $x^2 + y^2 = p^\beta$ and that $(x, p) = (y, p) = 1$. If $(a, p) = 1$ then there exists an integer $k$ such that $kx \equiv a \pmod{p^\beta}$. Therefore $k^2x^2 + k^2y^2 \equiv a^2 + (ky)^2 \pmod{p^\beta}$. So, $a^2 + (ky)^2 \equiv 0 \pmod{p^\beta}$.

As a last step we give the conjecture

**Conjecture.** The Girard-Fermat Theorem can be obtained by means of Theorem 2.5.

**Acknowledgements**
The authors thank to the editors and reviewers for their valuable support.

## References

[1] M. Akbaş, *On suborbital graphs for the modular group*, Bull. London Math. Soc. **33** (2001) 647–652 .

[2] M. Akbaş and D. Singerman, *The Normalizer of* $\Gamma(N)$ *in* $PSL(2,\mathbb{R})$, Glasgow Math. J. **32** (1990) 317–327,

[3] N. L. Biggs and A.T. White , *Permutation groups and combinatorial structures*, LMS Lect. Note Ser., CUP, Cambridge (1979).

[4] D. R. Heath-Brown, *Fermat's two-squares theorem*, Invariant (1984) 3–5.

[5] G. A. Jones, D. Singerman and K. Wicks, *The modular group and generalized Farey graphs*, LMS Lect. Note Ser. **160** (1991) 316–338.

[6] M. Newman, *The structure of some subgroups of the modular group*, Illinois J. Math. **6** (1962) 480–487 .

[7] H. Şengül , *Signature and congruence equations*, PhD Thesis, Karadeniz Technical University, Trabzon (2021).

[8] Y. Varouchas, *Une démonstration élémentaire du théorème des deux carrés*, La Caverne, I.R.E.M. de Lorraine, France, Bulletin No.6, février, (1984) 31–39.

[9] K. S. Williams, *Heath-Brown's elementary proof of the Girard-Fermat theorem*, Carleton Coordinates, Carleton University, Ottawa, Ontario, Canada, January (1985) 4–5.

[10] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, American Mathematical Monthly **97** (1990) 144.

[11] Ş. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press (2004).