# Gaussian integers



**Author:** Jamal Abo Mokh
**Course:** 1040279 - Ring and Fields Theory

**Definition 1.1** Let $\mathbb{Z}[i]$ be the guassian integers. and let's consider $N$ an euclidean norm:

$$N(a+bi) = a^2 + b^2$$

**Lemma 1.1** The function, $\varphi\colon \mathbb{Z}[i] \to \mathbb{Z}[i]$:

$$\varphi(z) = \bar{z}$$

Defines an automorphism.

***Proof.*** First, it's clear that the function defines a homomorphism, since:

$$\varphi(u(z+w)) = \overline{u(z+w)} = \bar{u}(\bar{z}+\overline{w}) = \varphi(u)\big(\varphi(z)+\varphi(w)\big)$$

moreover, $\varphi(0) = 0,\ \varphi(1) = 1.$ and we have:

$$z \in \ker\varphi \iff \bar{z} = 0 \iff z = 0$$

and since:

$$\varphi(\varphi(z)) = z$$

it's surjective completing the proof. □

**Lemma 1.2** Let $p \in \mathbb{Z}.$ and $z \in \mathbb{Z}[i]$:

$$p \mid z \iff p \mid \bar{z}$$

***Proof.***

$$p \mid z \iff z = up \iff \bar{z} = \bar{u}p \iff p \mid \bar{z}$$

□

**Lemma 1.3** let $z \in \mathbb{Z}[i]$.

$$z \in \mathbb{Z}[i]^\times \iff N(z) \in \mathbb{Z}^\times$$

***Proof.*** If $z \in \mathbb{Z}[i]^\times$, then we can write:

$$z^{-1}z = 1$$

therefore,

$$1 = N(1) = N(z^{-1}z) = N(z^{-1})N(z)$$

In particular, $N(z) \in \mathbb{Z}^\times$. In the other direction, we have by definition, $\exists \alpha \in \mathbb{Z}$ :

$$N(z)\alpha = 1$$

In particular, $N(z) \in \mathbb{Z}^\times$. Since we have:

$$\mathbb{Z}^\times = \{-1, 1\}$$

then by the positivity of $N$, we conclude:

$$z\bar{z} = N(z) = 1$$

as reuqired. □

**Definition 1.2** An irreducible $p$ in $\mathbb{Z}$ that "splits" is one that is reducible in $\mathbb{Z}[i]$

**Lemma 1.4** If $p \in \mathbb{Z}$ irreducible, such that it's reducible in $\mathbb{Z}[i]$ (splits). Then exists $z \in \mathbb{Z}[i]$ such that:

$$N(z) = p$$

***Proof.*** Since $p$ is reducible in $\mathbb{Z}[i]$, then we can write it as:

$$p = ab$$

for $a, b$ non units. therefore,

$$p^2 = N(p) = N(ab) = N(a)N(b)$$

by lemma (1.3), both $N(a), N(b)$ are non units in $\mathbb{Z}$. Since $\mathbb{Z}$ is PID, we have $p$ prime in $\mathbb{Z}$. therefore,

$$p \mid N(a)N(b) \implies p \mid N(a) \quad \vee \quad p \mid N(b)$$

In particular, wlog, $N(b)$ cannot be 1. hence,

$$N(a) = p$$

as required. □

**Lemma 1.5** Let $R, S$ are commutative rings with identity. If exists $\varphi\colon R \to S$ homomorphism then:

$$P \text{ solvable in } R \implies P^{\varphi} \text{ solvable in } S$$

***Proof.*** I'll defer the proof for now, since this is a general rings theorem. □

**Lemma 1.6** Let $n \in \mathbb{Z}$. If $n \bmod 4 = 3$, Then there exists so pair $x, y \in \mathbb{Z}$ such that:

$$x^2 + y^2 = n$$

***Proof.*** Define the following, $\varphi\colon \mathbb{Z} \to \mathbb{Z}_4$ by:

$$\varphi(x) = x \bmod 4$$

It's clear $\varphi$ defines homomorphism. therefore, by lemma (1.5) a solution in $\mathbb{Z}$ implies a solution in $\mathbb{Z}_4$. such that:

$$\varphi(x^2 + y^2) = \varphi(n) \implies a^2 + b^2 = 3$$

But exists no pair, $a, b \in \mathbb{Z}_4$ such that:

$$a^2 + b^2 = 3$$

hence, no such $x, y$ exists. □

**Lemma 1.7** Let $p \in \mathbb{Z}$ be prime. then the following are exclusive:

1. $p = 2$
2. $p \equiv_4 1$
3. $p \equiv_4 3$

***Proof.*** If $p = 2$ were done. otherwise, $p$ is non even, therefore, $p \bmod 4 \neq 0, 2$.

establishing the result. □

**Lemma 1.8** Let $p \in \mathbb{Z}$ prime. If $p \equiv_4 1$ then exists $x \in \mathbb{Z}_p$ such that:

$$x^2 \bmod p = -1$$

***Proof.*** Since $p$ is prime, we know that:

$$\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$$

Since $4 \mid p - 1$, then, exists $0 \neq \alpha \in \mathbb{Z}_{p-1}$ such that:

$$ord(\alpha) = 4$$

which implies exists $\beta \in \mathbb{Z}_p^\times$ such that:

$$\beta^4 \equiv_p 1$$

consequently, we have:

$$(\beta^2 - 1)(\beta^2 + 1) = 0$$

Since $\mathbb{Z}_p$ is field (in particular integral domain), then it has no zero divisors. therefore,

$$\beta^2 - 1 = 0 \quad \vee \quad \beta^2 + 1 = 0$$

If, $\beta^2 - 1 = 0$, then:

$$\beta^2 \equiv_p 1$$

In contradiction to $ord(\beta) = 4$. hence,

$$\beta^2 \equiv_p -1$$

as required. □

**Lemma 1.9** If exists $x \in \mathbb{Z}_p$ such that:

$$x^2 \equiv_p -1$$

Then $p$ splits in $\mathbb{Z}[i]$

***Proof.*** By the assumption, we have that $p \mid x^2 + 1$. Since we can write:

$$x^2 + 1 = (x - i)(x + i)$$

In $\mathbb{Z}[i]$, then if $p$ were to be irreducible in $\mathbb{Z}[i]$ then it's also prime, but it does not divide neither $(x - i),\ (x + i)$. hence splits. □

**Corollary 1.1** If $p \in \mathbb{Z}$ prime, such that $p \equiv_4 1$ then $p$ splits in $\mathbb{Z}[i]$.

***Proof.*** By the the lemma (1.8), exist $x \in \mathbb{Z}_p$ such :

$$x^2 \equiv_p -1$$

by the lemma (1.9), $p$ splits in $\mathbb{Z}[i]$ □

**Lemma 1.10** Let $p \in \mathbb{Z}$ be prime. then:

1. $p = 2 \ \vee \ p \equiv_4 1$ then exists a solution to $N(z) = p$
2. $p \equiv_4 3$ then exists no solution to $N(z) = p$

***Proof.*** If $p = 2$ then exists the trivial solution:

$$1^2 + 1^2 = 2$$

Assume, $p \neq 2$.

If $p \equiv_4 3$, then by lemma (1.6) there cannot exists a solution to:

$$x^2 + y^2 = p$$

Otherwise, If $p \equiv_4 1$, then by corollary (1.1), we have $p$ splits in $\mathbb{Z}[i]$, therefore, by lemma (1.4) exists a solution. □

***Theorem 1.1*** Let $2 \neq p \in \mathbb{Z}$ be prime. the following are equivalent:

1. $\exists x \in \mathbb{Z}_p \;\; x^2 = -1$
2. $p$ splits in $\mathbb{Z}[i]$
3. $\exists a, b \in \mathbb{Z} \;\; a^2 + b^2 = p$
4. $p \equiv_4 1$

***Proof.*** We'll compose the lemmas

1. By lemma (1.9) we showed (1) $\implies$ (2)
2. By lemma (1.4) we showed (2) $\implies$ (3)
3. By lemmas (1.7), (1.10), we showed (3) $\iff$ (4).
4. By lemma (1.8) we showed (4) $\implies$ (1)

Hence, we closed the circle. as required.

□

**Lemma 1.11** Let $n \in \mathbb{Z}$ such that exists $z \in \mathbb{Z}[i]$ such that:

$$N(z) = n$$

then for any $\alpha \in \mathbb{N}$ exists $w \in \mathbb{Z}[i]$ such that:

$$N(w) = n^{\alpha}$$

***Proof.*** Simply, we have

$$n^{\alpha} = (n)^{\alpha} = (N(z))^{\alpha} = N(z^{\alpha})$$

for $z^{\alpha} = w \in \mathbb{Z}$. as required. □

**Lemma 1.12** Let $p \in \mathbb{Z}$ prime. If $p \equiv_4 3$ then:

$$\alpha \bmod 2 = 0 \implies \exists z \in \mathbb{Z} \;\; N(z) = p^{\alpha}$$

***Proof.*** Assume $2 \mid \alpha$, then since we have:

$$N(p) = p^2$$

then applying lemma (1.11) on $\alpha/2$ establishes the result. □

***Theorem 1.2*** Let $n \in \mathbb{Z}$ such that:

$$n = \prod p_i^{\alpha_i}$$

Therefore,

$$\exists z \in \mathbb{Z}[i] \;\; N(z) = n \iff \Big(p_k \bmod 4 = 3 \implies \alpha_k \bmod 2 = 0\Big)$$

***Proof.*** By theorem (1.1) and lemma (1.12), then for each $p_k$ exists $z_k \in \mathbb{Z}[i]$ such that:

$$N(z_k) = p^{\alpha_k}$$

Hence, we have:

$$N(w) = N(\prod z_k) = \prod N(z_k) = \prod p^{\alpha_k} = n$$

Proving $\implies$ direction, by induction:

**Base Case.** $n \leq 2$ the case is trivial.

**Inductive Step.** Let $p$ in the factors of $n$ such that $p \bmod 4 = 3$.

By theorem (1.1) we have that $p$ is prime in $\mathbb{Z}[i]$. Therefore, since:

$$p \mid N(z) = z\bar{z}$$

Hence, we have $p \mid z$ since it's prime in $\mathbb{Z}[i]$. Therefore, $z = wp$. Consequently,

$$n = N(z) = N(w)N(p) = N(w)p^2$$

As a result:

$$N(w) = \frac{n}{p^2} = m < n$$

Applying the induction hypothses to $m$, we obtain that:

$$\nu_p(m) \bmod 2 = 0$$

Since we have:

$$\nu_p(n) = \nu_p(m) + 2$$

we have established the result.

□