University of Fribourg

Bachelor of Mathematics

Proseminar

Sums of two squares

Author:
Jeannine Coppex

Assistent:
Corina Ciobotaru

January 15, 2017

Contents

1 Number theory

In this chapter, we will use a statement which is known for a long time ago in the history of number theory. Lagrange prooved already in 1770 that every integer can be represented as a sum of two squares.

1.1 Introduction

Claim 1.1.1 *$\forall$ $a \in \mathbb{Z}$ we have $a^2 \equiv 0$ or $1 (mod\ 4)$.*

Proof:
For a $\in \mathbb{Z}$ even:
Every even number is a mulitple of 2. So for a = $\pm$2n $\Rightarrow$a^2 = 4n^2 $\equiv$0(mod 4).
For a $\in \mathbb{Z}$ odd:
Odd integers in (mod 4) are always equivalent to 1 or 3. For a$\equiv$1(mod 4) it is clear that a^2 $\equiv$1(mod 4). For a$\equiv$3(mod 4) we get a^2 $\equiv$ 9 $\equiv$ 1 (mod 4).
So $\forall$ a $\in \mathbb{Z}$ we get a^2 $\equiv$ 0 or 1(mod 4).
Knowing this, we easily find that n $\equiv$ 3 (mod 4) can not be a sum of two squares.

Gaussian Integers are definied as:

$$\mathbb{Z}[i] := \{a+bi:\ a,b \in \mathbb{Z},\ i^2 = -1\}.$$

The **Norm of** α: $N(\alpha) := \alpha\,\overline{\alpha}$.

In the following chapter, we will study the properties of $\mathbb{Z}$. The Arithmetic in the Ring of Gaussian Integers is similar to that ones in $\mathbb{Z}$.

1.2 Sums of two squares

Definition 1.2.1 *For $k \geq 2$ and $n \in \mathbb{N}$, let $r_k(n)$ be the number of representations of n as a sum of k-squares, that is the number of solutions of the equation $x_0^2 + x_1^2 + \ldots + x_{k-1}^2 = n$:*

$$r_k(n) = |\ \{(x_0,\ldots,x_{k-1}) \in \mathbb{Z}^k : \sum_{i=0}^{k-1} x_i^2 = n\}|.$$

Definition 1.2.2 *We say that $\alpha \in \mathbb{Z}[i] \backslash \{0\}$ is a unit if α is invertible in $\mathbb{Z}[i]$, i.e. $\frac{1}{\alpha} \in \mathbb{Z}[i]$. So the units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.*

Definition 1.2.3 *We say that two Gaussian Integers α, β are called associated, if there exists a unit $\epsilon \in \mathbb{Z}[i]$ so that $\alpha = \epsilon\beta$, $\epsilon \in \{\pm 1, \pm i\}$.*

Definition 1.2.4 *A Gaussian Integer $\pi \in \mathbb{Z}[i]$ is prime, if π is not a unit and for every factorisation $\pi = \alpha\beta$ in $\mathbb{Z}[i]$, either α or β is a unit in $\mathbb{Z}[i]$.*

Proposition 1.2.5 *Let α and β be elements in $\mathbb{Z}[i]$. Then there exist γ and $\delta \in \mathbb{Z}[i]$ s.t. $\alpha = \beta\gamma + \delta$ and $N(\delta) < N(\beta)$.*

Proof:
Let $\beta \neq 0$, so we can form $\frac{\alpha}{\beta} = \gamma + \frac{\delta}{\beta}$, where $\gamma, \delta \in \mathbb{Z}[i]$.
With δ and β, we devide two Gaussian Integers, so we get a complex number. Define x:= Re(γ) + Re($\frac{\delta}{\beta}$) and y:= Im(γ) + Im($\frac{\delta}{\beta}$), where x,y $\in \mathbb{R}$. Let m,n $\in \mathbb{Z}$ s.t.
|x-m| $\leq \frac{1}{2}$ and |y-n| $\leq \frac{1}{2}$. Set γ= m+ni $\in \mathbb{Z}[i]$ and δ=β[(x-m)+i(y-n)]=β[x+iy]=$\beta \cdot \frac{\alpha}{\beta}$=$\alpha$.
As $\delta = \alpha$-$\beta\gamma$ with α,β,$\gamma \in \mathbb{Z}[i]$, δ is an element in $\mathbb{Z}[i]$ too.
We will show know, that N(δ)<N(β):
$\frac{\delta}{\beta}$ = x-m+i(y-n) $\Rightarrow |\frac{\delta}{\beta}|^2 = (x-m)^2+(y-n)^2 \leq \frac{1}{2}$. Using the definition of m and n earlier we know that $(x-m)^2 \leq \frac{1}{4}$ and $(y-n)^2 \leq \frac{1}{4}$. So we get $|\frac{\delta}{\beta}|^2 \leq \frac{1}{2} \Rightarrow$N($\frac{\delta}{\beta}$) $\leq \frac{1}{2}$
$\Rightarrow$N(δ) $\leq \frac{1}{2}N(\beta)$<N(β) as $\beta \neq$0. So we find N(δ)<N(β). □

Definition 1.2.6 *Let α and β be $\in \mathbb{Z}[i]$.*
i) We say that α dividies β, if $\exists\ \gamma \in \mathbb{Z}[i]$ s.t. β=$\gamma\alpha$.
ii) We say that $\delta \in \mathbb{Z}[i]$ is a greatest common divisor(gcd) of α and β, if δ divides α and β and if $\gamma \in \mathbb{Z}[i]$ divides α and β, then it also divides δ.

Remark:
i) If there exists a gcd, it is unique up to mulitplication by $\epsilon \in \{\pm 1, \pm i\}$.
ii) Whenever (α,β)=$\pm 1, \pm i$, we say α and β are relatively prime. In this case, we write (α,β)=1.

Proposition 1.2.7 *For all $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$ $\exists$ a gcd $(\alpha, \beta) \in \mathbb{Z}[i]$. Moreover, we have that Bézout's Lemma holds, e.g. $\exists\ \nu, \mu \in \mathbb{Z}[i]$ s.t. $(\alpha, \beta) = \alpha\nu + \beta\mu$.*

Proof:
Let $\alpha, \beta \in \mathbb{Z}[i]$ that will be fixed for what follows.
Define: I:=$\{\alpha\nu+\beta\mu$: $\nu, \mu \in \mathbb{Z}[i]\}$. Obviously, I is an Ideal, e.g. I is an abelian group respective to addition and I is closed under multiplication. Let $\tau = \alpha\nu_0+\beta\mu_0$ be an element $\neq 0$ of minimal Norm in I. From the fact that $\alpha \in$ I and for every $\eta \in \mathbb{Z}[i]$ we have $\eta\tau \in$ I it follows that for every $\delta \in \mathbb{Z}[i]$ we have δ=$\eta\tau$+$\alpha \in$ I.
Claim: (α, β)=τ.
Using Proposition 1.2.5, we can find $\gamma, \delta \in \mathbb{Z}[i]$ s.t. α=$\tau\gamma$+δ and N(δ)<N(τ). The element $\tau \neq$0 is of minimal Norm, so the norm of the element δ can only be smaller if it's equal to 0. With this information we get the equation 0=α-$\tau\gamma$ and therefore, we know that α=$\tau\gamma$. So τ divides α. With exactly the same argument one can find that τ divides β too. Since τ=$\alpha\nu_0$+$\beta\mu_0$, every common divisor of α and β also divides τ. Hence we found a gcd (α, β) and Bézout's Relation hold with $\nu = \nu_0$ and $\mu = \mu_0$. □

Proposition 1.2.8 *$\pi \in \mathbb{Z}[i]$ is prime $\Leftrightarrow$ ($\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ or $\pi \mid \beta$, where α,$\beta \in \mathbb{Z}[i]$).*

Proof:
"$\Rightarrow$": If $\pi \mid \alpha\beta$, then $\alpha\beta$=$\pi\sigma$ for a $\sigma \in \mathbb{Z}[i]$.
Suppose, π does not divide α.
To show: π divides β.
Consider (π, α):
As a gcd of π and α divides π and π is prime, it follows that (π, α)=1. Then: 1=$\pi\nu$+$\alpha\mu$

for some $\nu, \mu \in \mathbb{Z}[i]$. Multiplying the equation by β we get
$\beta = \pi\beta\nu + \alpha\beta\mu = \pi\beta\nu + \pi\sigma\mu = \pi(\beta\nu + \sigma\mu)$, so π divides β.

"$\Leftarrow$": If $\pi = \alpha\beta$, then π divides the product $\alpha\beta$. Assume: $\pi \mid \beta$, i.e. $\beta = \pi\gamma$ for a $\gamma \in \mathbb{Z}[i]$. Then we have: $\pi = \alpha\beta = \alpha\pi\gamma$. Canceling out π we get $1 = \alpha\gamma$, so α is a unit. Therefore, in the equation $\pi = \alpha\beta$, α is a unit, which means that π is prime. By assuming $\pi \mid \alpha$, we get that β is a unit and π would also be prime. □

Knowing this, we will be able to show that factorisation in $\mathbb{Z}[i]$ is unique.

Proposition 1.2.9 *Every $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ can be represented as a unique product of primes in $\mathbb{Z}[i]$. More precisely: If $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, then $\alpha = \pi_1 \ldots \pi_k$ for some primes $\pi_1, \ldots, \pi_k \in \mathbb{Z}[i]$ and if*
$\alpha = \pi_1 \ldots \pi_k = \sigma_1 \ldots \sigma_l$ are two factorisations of α into primes, then $k=l$ and, after an eventually permutation of the indices, π_i is associated to σ_i, where $1 \leq i \leq k$.

Proof:
Existence:
By induction over $N(\alpha)$. The case $N(\alpha)=1$ is trivial. Induction step: For $N(\alpha)>1$ there are two cases:
i) if α is a prime, then there is nothing to prove
ii) if α is not a prime:
Factorize $\alpha = \beta\gamma$ where $\beta, \gamma \in \mathbb{Z}[i]$ not invertible. Then $N(\alpha) = N(\beta)N(\gamma)$, where $N(\beta)$, $N(\gamma) < N(\alpha)$ and by induction assumption, β and γ are products of primes in $\mathbb{Z}[i]$, so α is also a product of primes.
Uniqueness:
Assume $\alpha = \pi_1 \ldots \pi_k = \sigma_1 \ldots \sigma_l$ with $k \leq l$. $\Rightarrow \pi \mid \sigma_1 \ldots \sigma_l$ and π is prime. According to proposition 1.2.8, π_1 divides at least one of the σ_i's, say $\pi_1 \mid \sigma_1$. We can write $\sigma_1 = \epsilon_1\pi_1$, $\epsilon_1 \in \mathbb{Z}[i]$. σ_1 is prime, so ϵ_1 must be a unit. Replace $\sigma_1 = \epsilon_1\pi_1$ in the equation of α $\Rightarrow \pi_2 \ldots \pi_k = \epsilon_1\sigma_2 \ldots \sigma_l$. Iteratively, we get $1 = \epsilon_1 \ldots \epsilon_k \sigma_{k+1} \ldots \sigma_l$. We can assume $k<l$.
Taking norms: $N(1) = 1 = N(\sigma_{k+1}) \ldots N(\sigma_l) \Rightarrow 1 = N(\sigma_{k+1}) = \ldots = N(\sigma_l)$ ↯ to $k<l$ as σ_i is prime. $\Rightarrow k=l$. □

Now we give some applications of the arithmetic of $\mathbb{Z}[i]$ with respect to the problem of sums of two squares. We introduce a field:

$\mathbb{F}_q$ is the finite field of q elements, where q is an integer.
$\mathbb{F}_q^*$ is the multiplicative groupe of elements $\neq 0$ in $\mathbb{F}_q$.
The following famous theorem was first stated by Fermat, and more than 100 years later, it was proved by Euler.

Theorem 1.2.10 *Let p be an odd prime in $\mathbb{N}$. The following statements are equivalent:*
i) $p \equiv 1 \pmod 4$;
ii) -1 is a square in $\mathbb{F}_p$, i.e. the congruence $x^2 \equiv -1 \pmod p$ has a solution in $\mathbb{Z}$;
iii) p is a sum of two squares (so $r_2(p)>0$).

Proof:
For y $\in \mathbb{F}_p^*$ define the Packet $P_y := \{y,-y,y^{-1},-y^{-1}\}$. One can easily see that all the elements from P_y are in $\mathbb{F}_p$, as $\mathbb{F}_p^*$ is a multiplicative group. Test the Packet on equalities: Consider the following three cases:
1) y=-y
2) $y=y^{-1}$
3) $y = -y^{-1}$
All other equalities in P_y would reduce to the problem of the three cases considered above.
Ad 1):
This case is not possible.
Proof:
y $\in \mathbb{F}_p^*$. If y=-y $\Rightarrow$ 2y=0(mod p) $\Rightarrow$ either p|2 or p|y. We can neither have p|2 as p is odd, nor p|y as y $\in$ {1,2,...,p-1}.
Ad 2):
This case is possible.
Proof:
$y=y^{-1}$(mod p) $\Rightarrow y^2 = 1$(mod p) $\Rightarrow y^2$-1=0(mod p) $\Rightarrow$(y+1)(y-1)=0(mod p)
$\Rightarrow$p|(y+1)(y-1). So either p|(y+1) that implies y$\equiv$-1(mod p) or p|(y-1) that implies y$\equiv$1(mod p). So for $y=y^{-1}$ we find P_y ={1,-1}=:P_1, which is a Packet with only 2 elements.
Ad 3):
This case can also be possible, when -1 is a square modulo p, because $y=-y^{-1}$
$\Rightarrow y^2$=-1(mod p) so -1 is a square modulo p. In this case, P_y has two elements.
Note that P_1 is always present.

Ad i)$\Rightarrow$ ii):
From p$\equiv$1(mod 4) it follows that p-1=4k for a k$\in \mathbb{Z}$. As $\mathbb{F}_p^*$ has p-1 elements we get the equation $|\mathbb{F}_p^*| = 4k$.
$$|\mathbb{F}_p^*| = |\dot{\cup}_{y\in\mathbb{F}_p{}^*}| = \sum_{y\in\mathbb{F}_p{}^*} |P_y| = |P_1| + \sum_{\substack{y\in\mathbb{F}_p{}^* \\ P_y \neq P_1}} |P_y| = 2 + \sum_{\substack{y\in\mathbb{F}_p{}^* \\ P_y \neq P_1}} |P_y| = 4k$$

To fulfill the equation, there must be just one more Packet with only two elements.

So -1 is a sqaure modulo p.
Ad ii)$\Rightarrow$i)
Consider p $\equiv$ 3(mod 4) where p-1$\equiv$ 4k+2.
$$|\mathbb{F}_p^*| = |\dot{\cup}_{y\in\mathbb{F}_p{}^*}| = \sum_{y\in\mathbb{F}_p{}^*} |P_y| = |P_1| + \sum_{\substack{y\in\mathbb{F}_p{}^* \\ P_y \neq P_1}} |P_y| = 2 + \sum_{\substack{y\in\mathbb{F}_p{}^* \\ P_y \neq P_1}} |P_y| = 4k+2$$
To fulfill the equation in this case, there is no other Packet than P_1 present. This implies that for p$\equiv$3(mod 4) the Packet where -1 is a square modulo p is not present. So if -1 is a square modulo p, then p$\equiv$1(mod 4).

Ad ii)⇒iii):
-1 is a square modulo p ⇒ ∃ x ∈ $\mathbb{Z}$ s.t. $x^2+1\equiv 0 \pmod p \Rightarrow p|x^2+1=(x+i)(x-i)$, x± i ∈ $\mathbb{Z}$ [i], but p ∤ x+i and p ∤ x-i in $\mathbb{Z}$ [i] because p ∤ x and p ∤ 1 in $\mathbb{Z}$. Therefore, by Proposition 1.2.8, p is not prime in $\mathbb{Z}$ [i]. Thus ∃ a factorisation p = $\alpha\beta$, where α,β∈ $\mathbb{Z}$ [i] are no units. ⇒ N(α)>1 and N(β)>1. Taking norms, one gets: N(p)=N($\alpha\beta$)=N(α)N(β) ⇒ p^2=N(α)N(β), this implies N(α)=N(β)=p and as a norm is a sum of two squares, this also holds for p, so p is a sum of two squares.

Ad iii)⇒ ii):
p is a sum of two squares, therefore we can write: $p=a^2+b^2$. Multiplying the equation by c^2 yields: $pc^2=(ac)^2 + (bc)^2$ Reducing modulo p we get:

$$0 \equiv (ac)^2 + (bc)^2 (mod\, p) \tag{1.1}$$

Claim: a and b are invertible.
Proof:
For a=0, $p = b^2$ would be a contradiction to the assumption, that p is a sum of two squares. Thus a≠0. Moreover, a≠p, since $p=p^2+b^2$ is not possible. For b we find the same statements. Therefore, we observe that 0<a,b<p ⇒ a,b ∈ $\mathbb{F}_p^*$.
Since b is invertible, there ∃ c ∈ $\mathbb{Z}$ s.t bc≡1(mod p). Inserting this in (1.1) we get:
$0 \equiv (ac)^2+1 \pmod p \Rightarrow -1\equiv (ac)^2$ ⇒ -1 is a square mod p.
As i)⇔ii) and ii)⇔iii) it follows that i)⇔iii). □

The next corollary is a very famous statement of Fermat and Euler.

Corollary 1.2.11 *(The two square theorem)*
An integer n ≥ 2 is a sum of two squares ($r_2(n)>0$) ⇔ every prime number p≡ 3(mod 4) appears with even exponent in the factorisation of n into primes.

Proof:
"⇒": Let $n=a^2+b^2$ be a sum of two squares. Let p be an odd prime dividing n. Let p^k the highest exponent of p s.t. p^k divides a and b.
Define x:= $\frac{a}{p^k}$ and y:= $\frac{b}{p^k}$ ⇒ $x^2+y^2 = \frac{a^2}{p^{2k}}+\frac{b^2}{p^{2k}} = \frac{n}{p^{2k}}$.
So we found the equation: $\frac{n}{p^{2k}} = x^2+y^2$.
Suppose: p still divides $\frac{n}{p^{2k}}$, so $x^2+y^2 \equiv 0 \pmod p$. But x and y are not both divisible by p, so either x(mod p) ∈ $\mathbb{F}_p^*$ or y(mod p) ∈ $\mathbb{F}_p^*$. So x or y admits an invers element in $\mathbb{F}_p^*$, say cx=1(mod p). Then, by multiplying the equation $x^2+y^2 \equiv 0 \pmod p$ by c^2, we get $1+(cy^2)\equiv 0 \pmod p$. Hence $(cy^2)\equiv -1 \pmod p$. So -1 is a square modulo p. Then, by Theorem 1, we know that $p \equiv 1 \pmod 4$.
By assuming p| $\frac{n}{p^{2k}}$ we showed that p≡ 1(mod 4). So we conclude that for p≡ 3(mod 4), p can not not divide $\frac{n}{p^{2k}}$. Therefore, p appears with even exponent in the factorisation of n into primes.

"⇐": Fatorize n into primes where $p_i \equiv 3 \pmod 4$ and $q_j \equiv 1 \pmod 4$:

$$n = {p_1}^{2a_1} \cdot \ldots \cdot {p_k}^{2a_k} \cdot {q_1}^{b_1} \cdot \ldots \cdot {q_l}^{b_l}$$

But $q_j \equiv 1 \pmod 4$ so by Theorem 1.2.10, q_j is a sum of two squares. For $p_i \equiv 3 \pmod 4$ $\Rightarrow {p_i}^{2a_i} \equiv 1 \pmod 4$ and ${p_i}^{2a_i}$ is a sum of two squares. Thus n is a product of elements which are sums of two squares. But every sum of two squres can be represented by a norm, e.g. $p_i = N(a+ib)$ and therefore
$p_i \cdot p_j = N(a+ib)N(c+id)=N[(a+ib)(c+id)]=N(e+if)$ for e=ac-bd and f=(ad+bc), so every product of sums of two squares is a sum of two squares. By induction, this conclusion also holds for a product of k+l elements, like in our case. So $n \geq 2$ is a sum of two squares. □

The following Lemma is a useful criterion for a Gaussian integer to be relatively prime to a rational integer.

Lemma 1.2.12 *Let $m \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[i]$, then $(m,\alpha) = 1 \Leftrightarrow (m, N(\alpha)) = 1$.*

Proof:
"⇒": Suppose that $(m,\alpha)=1$. We know by Bézout's Lemma, that there $\exists\ \gamma,\delta \in \mathbb{Z}[i]$, s.t. $1=\gamma m+\delta\alpha$. By applying the norm to $\delta\alpha = 1-\gamma m$ we get $N(\delta)N(\alpha)=N(1-\gamma m) = (1-\gamma m)(1-\bar{\gamma}m)=1-(\gamma+\bar{\gamma})m+N(\gamma)m^2 \Rightarrow N(\delta)N(\alpha)+(\gamma+\bar{\gamma})m-N(\gamma)m^2=1$. So if there $\exists$ an element $\beta \in \mathbb{Z}[i]$ that divides m and $N(\alpha)$, then it also divides 1. Therefore, β must be a unit $\Rightarrow (m,N(\alpha))=1$.

"⇒": Suppose that $(m,N(\alpha))=1$. If $\delta \in \mathbb{Z}[i]$ divides m and α, then δ divides m and $N(\alpha)= \alpha\bar{\alpha} \Rightarrow \delta \mid 1 \Rightarrow \delta$ is a unit $\Rightarrow (m,\alpha)=1$. □

Now we can characterize the primes in $\mathbb{Z}[i]$.

Proposition 1.2.13 *A Gaussian integer $\pi \in \mathbb{Z}[i]$ is prime if and only if one of the following three mutually exclusive cases occur:*
i) $N(\pi) = 2$ (in this case π is an associate of 1+i; that is, $\pi \in \{1\pm i, -1\pm i\}$);
ii) $N(\pi) = p$, where p is a prime in $\mathbb{Z}$ and $p \equiv 1 \pmod 4$;
iii) π is associate to q, where q is a prime in $\mathbb{Z}$, and $q \equiv 3 \pmod 4$.

Proof:
"⇒": Let π be a prime in $\mathbb{Z}[i]$ and p a prime in $\mathbb{Z}$, that divides $N(\pi) \Rightarrow (p, N(\pi))=p$. Set $\delta=(p,\pi)$. So δ is either π or it is associated to 1. By Lemma 1, δ is not a unit, as $(p,N(\pi))\neq 1$. But π is prime, so we may assume $\delta=\pi$. We can writre: $p=\pi\gamma$, $\gamma \in \mathbb{Z}[i]$. By taking the norms we get: $p^2 = N(\pi)N(\gamma) \Rightarrow p = \frac{N(\pi)}{p} N(\gamma) \in \mathbb{Z}$. Two cases appear:

a) $\frac{N(\gamma)}{p}=1 \Rightarrow N(\pi)=p$ and therefore, p is a sum of two squares. By Theorem 1.2.10, $p \equiv 1 \pmod 4$ for $p \geq 3$ or $p = 2$. So we showed i) and ii).
b) $N(\gamma)=1$ implies $p^2=N(\pi)$, what shows that π is associated to p and hence p is prime in $\mathbb{Z}[i]$. If p could be written as a product p=(a+ib)(a-ib), then either a+ib or a-ib were

a unit and p could not be a sum of two squares. By Theorem 1.2.10, this would imply that p≠1(mod4) and therefore p≡3(mod 4).

"⇐":
To show:
i)N(π)=2 implies $\pi \in \mathbb{Z}[i]$ is prim.
ii)N(π)=p implies $\pi \in \mathbb{Z}[i]$ is prim.
iii)π associated to q, where q prime in $\mathbb{Z}$ and q≡ 3(mod 4) implies $\pi \in \mathbb{Z}[i]$ is prim.

First we will show a genereal statement:
Claim:
If N(π) is prime in $\mathbb{Z}$, then π is prime in $\mathbb{Z}[i]$.
Proof:
Let N(π) be a prime in $\mathbb{Z}$. Suppose $\pi=\alpha\beta$, $\alpha,\beta \in \mathbb{Z}[i]$. Taking norms we get N($\pi$)=N($\alpha$)N($\beta$) and as N($\pi$) is a prime in $\mathbb{Z}$, either N(α) or N(β) is a unit, so N(α)=1 or N(β)=1 and therefore, either α or β is invertible in $\mathbb{Z}[i]$. So π is prime in $\mathbb{Z}[i]$.

Ad i) and ii):
For N(π)=2 and N(π)=p, N(π) is a prime in $\mathbb{Z}$ and as it was shown in the claim, π is prime in $\mathbb{Z}[i]$.
Ad iii):
Given q≡3(mod 4). Set q=$\alpha\beta$, where $\alpha,\beta \in \mathbb{Z}[i]$. Take the norms: q^2=N(α)N(β). From Theorem 1.2.10 it is clear that q can not be a sum of two squares. So in the equation qq=N(α)N(β), N(α)=N(β)=q is not possible. Hence, either N(α) or N(β) is equal to one. So either q^2=N(α) or q^2=N(β)⇒ 1=N(α) or 1=N(β). This implies that α or β is a unit in $\mathbb{Z}[i]$, hence q is prime in $\mathbb{Z}[i]$. As π is associated to q, π is prime $\in \mathbb{Z}[i]$. □

Some more definitions are needed to introduce Legendre's formula for $r_2(n)$.
• d_1(n) is the number of divisors of n $\in \mathbb{N}$ which are congruent to 1 modulo 4;
• d_3(n) is the number of divisors of n $\in \mathbb{N}$ which are congruent to 3 modulo 4;
• d(n) is the number of divisors of n $\in \mathbb{N}$.

Theorem 1.2.14 *For $n \in \mathbb{N}$, n>0 we have $r_2(n)=4(d_1(n)-d_3(n))$.*

Proof:
Define: δ(n):=d_1(n)-d_3(n).
1.Case: Assume that N $\in \mathbb{N}$ odd:
Then N can be represented as a product of terms, which are congruent to 1(mod 4) or 3(mod 4). So N=km, where

$$k= \prod_{h=1}^{a} p_h{}^{r_h} \ (p_h \equiv 1 (\text{mod } 4))$$
$$m= \prod_{j=1}^{b} q_j{}^{s_j} \ (q_j \equiv 3 (\text{mod } 4)).$$

Assume l|N s.t. l≡1(mod 4).
Then l=$k_l m_l$ ⇒q_j's of m_l have to be of even power ⇒$m_l \equiv 1(\text{mod } 4)$. Hence, the m_l's are in $d_1(m)$.
⇒$d_1(N)=d(k)d_1(m)$.
Now assume that l|N s.t. l≡3(mod 4).
Then l can be written as l=$k_l m_l$ ⇒$m_l \equiv 3(\text{mod } 4)$
⇒$d_3(N)=d(k)d_3(m)$
⇒$\delta(N)=d_1(N)-d_3(N)=d(k)(d_1(m)-d_3(m))= d(k)\delta(m)$.
So we found $\delta(N)=d(k)\delta(m)$.
Claim:

$$\delta(m)=\begin{cases}0 & \text{if at least one } s_j \text{ is odd}\\ 1 & \text{if all } s_j\text{'s are even, that is, if m is a square.}\end{cases}$$

Proof:
Set m'=$\frac{m}{q_1^{s_1}}$. It is easy to check that $\delta(1)=1$. For s_1 even, we get:

$$d_1(m)=(\tfrac{s_1}{2}+1)d_1(m')+\tfrac{s_1}{2}d_3(m')$$
$$d_3(m)=\tfrac{s_1}{2}d_1(m')+(\tfrac{s_1}{2}+1)d_3(m')$$

so $\delta(m)=\delta(m')$.
For s_1 odd, we get:

$$d_1(m)=\tfrac{s_1+1}{2}d_1(m')+\tfrac{s_1+1}{2}d_3(m')=d_3(m)$$

hence $\delta(m)=d_1(m)-d_3(m)=0$, which proves the claim. From this, we deduce

$$\delta(N)=\begin{cases}d(k) & \text{if m is a square}\\ 0 & \text{otherwise.}\end{cases}$$

Notice that n could be even or odd. Write $n=2^tN$, so n is either odd, for t=0, or even, for t≥1. Thus $\delta(n)=\delta(2^tN)=\delta(N)$, because by multiplying by 2, all additional divisors are divisible by 2, so $d_1(N)$ and $d_3(N)$ are the same as $d_1(n)$ and $d_3(n)$.
Assume m is not a square:
Then in the factorisation of m there are some primes q_j s.t. $q_j \equiv 3(\text{mod } 4)$ with odd exponent. Then by Corollary 1.2.11 N is not a sum of two squares. So we can write $r_2(N)=0$ hence $r_2(n)=0$. Now as $d_1(N)=d_1(n)$ and $d_3(N)=d_3(n)$ and because $\delta(N)=d_1(N)-d_3(N)=0$ we get $d_1(n)-d_3(n)=0$. So $r_2(n)=4(d_1(n)-d_3(n))=0$. The theorem holds in this case.
Assume m is a square:
By Corollary 1.2.11 we know that $r_2(n)>0$. Idea: On one hand, write n as a sum of two squares and on the other, factor n into primes in $\mathbb{Z}[i]$ using unique factorisation and the description of primes in $\mathbb{Z}[i]$ from Proposition 4 and 1.2.13. With this, we get:

$$n=A^2+B^2=(A+iB)(A-iB)=(-i)^t(1+i)^{2t}\prod_{h=1}^{a}\pi_h^{r_h}\,\bar{\pi}_h^{r_h}\prod_{j=1}^{b}q_j^{s_j}$$

where $\pi_h \in \mathbb{Z}[i]$ is a prime s.t. N(π)=p_h. Further, r_2(n)is the number of factorisations of n as (A+iB)(A-iB) in $\mathbb{Z}[i]$. Factorisation is unique and N(A+iB)=N(A-iB), therefore we must have:

$$A+iB=u(1+i)^t \prod_{h=1}^{a} \pi_h{}^{w_h}\ \bar{\pi}_h{}^{u_h} \prod_{j=1}^{b} q_j{}^{\frac{s_j}{2}}$$
$$A-iB=u'(1+i)^t \prod_{h=1}^{a} \pi_h{}^{u_h}\ \bar{\pi}_h{}^{w_h} \prod_{j=1}^{b} q_j{}^{\frac{s_j}{2}}$$

with u,u' units s.t. uu'=$(-i)^t$ and $u_h+w_h=r_h$ ($1\leq h\leq a$), where u and the u_h's are unique up to equivalence. Therefore, the number of possible choices for A+iB is

$$4\prod_{h=1}^{a}(r_h+1)=4d(k)=4\delta(N)=4d(n).\ \square$$

1.3 Exercices

1)
Task:
Describe an infinite, one-parameter family of solutions x=f(m),y=g(m), z=h(m) where $x^2+y^2=z^2$ and (x,y,z)=1.
Solution:
Let m$\in \mathbb{N}$. Then x=2m+1=f(m), $y=2m^2+2m=g(m)$, $z=2m^2+2m+1=h(m)$
$z^2=(2m^2+2m+1)^2=[2m(m+1)+1]^2=[2m(m+1)]^2+4m(m+1)+1=[2m(m+1)]^2+(2m+1)^2$
$=x^2+y^2$
Show (x,y,z)=1:
(x,y)=(2m+1,2m(m+1))=1, because a divisor of y either divides 2m or m+1. But 2m is not a divisor of x=2m+1 and m+1 can not divide 2m+1.
Obviously, (y,z)=(2m(m+1),2m(m+1)+1)=1. From (x,y)=1 and (y,z)=1 it follows directly that (x,y,z)=1.

2)
Task:
Prove, without appealing to Theorem 1.2.14, that $d_1(n)$-$d_3(n) \geq 0$.
Proof by induction:
We can asssume n=mp, where p is a prime.
Three cases occur: p≡1(mod 4), p=2 and p≡3(mod 4).
First consdier p≡1(mod 4).
Then for every divisor d of n, d|n ⇒either d=m_1p, where m_1|m or d|m. So if m_1|m where m_1≡1(mod 4), then m_1p≡1(mod 4)1(mod 4)≡1(mod 4), hence d≡1(mod 4). On the other hand, if m_1|m with m_1≡3(mod 4), then m_1p≡3(mod 4)1(mod 4)≡3(mod 4), hence d≡3(mod 4). So we found the following two equations: $d_1(n)=d_1(m)$ and $d_3(n)=d_3(m)$. This implies that $d_1(n)$-$d_3(n)=d_1(m)$-$d_3(m)$ and we know from the proof of the Theorem 1.2.14 that $d_1(m)$-$d_3(m)=0$. So $d_1(n)$-$d_3(n) \geq 0$.

Now, consider the second case, where p=2. So we get n=m·2. Every divisor of two

is either equivalent to 2(mod 4) or to 0(mod 4), so this factor will not change anything on the number of divisors. Therefore, we get the same as in the first case, where we had p≡1(mod 4). So $d_1(n)=d_1(m)$ and $d_3(n)=d_3(m)$. This implies that $d_1(n)-d_3(n)=d_1(m)-d_3(m)=0\geq 0$.
For the third case, assume p≡3(mod 4).
Then for every divisor d of n, d|n ⇒either $d=m_1p$, where $m_1|m$ or d|m. So if $m_1|m$ where $m_1\equiv 1(\text{mod } 4)$, then $m_1p\equiv 1(\text{mod } 4)3(\text{mod } 4)\equiv 3(\text{mod } 4)$, hence d≡3(mod 4). On the other hand, if $m_1|m$ with $m_1\equiv 3(\text{mod } 4)$, then $m_1p\equiv 3(\text{mod } 4)3(\text{mod } 4)\equiv 1(\text{mod } 4)$, hence d≡1(mod 4). So we found the following two equations: $d_1(n)=d_3(m)$ and $d_3(n)=d_1(m)$. This implies that $d_1(n)-d_3(n)=d_3(m)-d_1(m)$ and we know from the proof of the Theorem 1.2.14 that $d_1(m)-d_3(m)=0$, hence $d_3(m)-d_1(m)=0$. So $d_1(n)-d_3(n)\geq 0$.
Therefore, we proved all three cases. □

3)
Task:
Let m,n be rational integers. Prove that m,n are relatively prime in $\mathbb{Z}[i]$ ⇔ m,n are relatively prime in $\mathbb{Z}$.
Proof:
"⇒": m,n are relatively prime in $\mathbb{Z}[i]$
⇒∃ $\alpha,\beta \in \mathbb{Z}[i]$ s.t. $m\alpha+n\beta = \pm 1, \pm i$
So we have four different cases:
I: $m\alpha + n\beta = 1$
II: $m\alpha + n\beta$ = -1
III: $m\alpha + n\beta$ = i
IV: $m\alpha + n\beta$ = -i

<u>For I:</u>
$m\alpha + n\beta = 1$ where $\alpha, \beta \in \mathbb{Z}[i]$
⇒$m(a_1+b_1i) + n(a_2+4i) = 1$ for $a_1,a_2,b_1,b_2 \in \mathbb{Z}$
⇒$ma_1+na_2+i(mb_1+nb_2)=1$
$ma_1+na_2 = 1$ and $mb_1+nb_2 = 0$
⇒we found $a_1,a_2 \in \mathbb{Z}$ s.t. $ma_1+na_2 = 1$
⇒m,n are relatively prime in $\mathbb{Z}$.

<u>For II:</u>
Same as for I, we find the following equation:
ma_1+na_2 = -1
⇒$m(-a_1) + n(-a_2) = 1$
As $a_1, a_2 \in \mathbb{Z}$, their inverse $-a_1,-a_2$ is also $\in \mathbb{Z}$.
⇒we found $-a_1,-a_2 \in \mathbb{Z}$ s.t. $m(-a_1) + n(-a_2) = 1$
⇒m,n are relatively prime in $\mathbb{Z}$.

<u>For III:</u>
$m\alpha + n\beta$ = i where $\alpha, \beta \in \mathbb{Z}[i]$

$\Rightarrow$m(a_1+b_1i) + n(a_2+b_2i)= i for a_1,a_2,b_1,$b_2 \in \mathbb{Z}$
$\Rightarrow$ma_1+na_2+i(mb_1+nb_2)=i
$\Rightarrow$ma_1+na_2 = 0 and mb_1+nb_2 = 1
$\Rightarrow$we found b_1,$b_2 \in \mathbb{Z}$ s.t. mb_1 + nb_2 = 1
$\Rightarrow$m,n are relatively prime in $\mathbb{Z}$.

For IV:
Same as for III, we find the following equation:
mb_1 + nb_2 = -1
$\Rightarrow$m(-b_1) + n(-b_2) = 1
As b_1,$b_2 \in \mathbb{Z}$, their inverse -b_1,-b_2 is also $\in \mathbb{Z}$.
$\Rightarrow$we found -b_1,-$b_2 \in \mathbb{Z}$ s.t. m(-b_1) + n(-b_2) = 1
$\Rightarrow$m,n are relatively prime in $\mathbb{Z}$.

As we found the required property for all four cases, m and n are relatively prime in $\mathbb{Z}$.

"$\Leftarrow$":
(m,n)=$\pm$1 for m,n $\in \mathbb{Z}$
(m,n)=$\pm$1 $\Rightarrow\exists\ \alpha,\beta \in \mathbb{Z}$ s.t. $m\alpha + n\beta = \pm 1$. As every element in $\mathbb{Z}$ is also an element in $\mathbb{Z}[i]$, we already found $\alpha,\beta \in \mathbb{Z}[i]$ s.t. $m\alpha + n\beta = \pm 1$ and therefore m and n are relatively prime in $\mathbb{Z}$ [i]. We still have to find some elements $\gamma,\delta \in \mathbb{Z}[i]$ s.t. mγ+nδ=$\pm$i. For finding these elements, just multiplie the equation $m\alpha + n\beta = \pm 1$ by i. $\square$

4)
Claim:
Let p be an odd prime.
-1 is a square modulo p $\Leftrightarrow$ p$\equiv$ 1 (mod 4)
The aim of the exercice is to give a group theoretical proof.
Proof:
Show that -1 is a square modulo p $\Leftrightarrow$ $\mathbb{F}_p^*$ contains an element of ordre 4
"$\Rightarrow$": -1 is a square modulo p $\Rightarrow\exists$ a $\in \mathbb{F}_p^*$ s.t. $a^2 \equiv$-1(mod p)$\Rightarrow a^4 \equiv$1(mod p), hence a $\in \mathbb{F}_p^*$ is an element of ordre 4.
"$\Leftarrow$": If $\mathbb{F}_p^*$ contains an element of ordre 4$\Rightarrow a^4 \equiv$1(mod p) and $\mathbb{F}_p^*$=<b>, so $b^{p-1} \equiv$1(mod p). Then a can be represented by a power of b, a=$b^k \Rightarrow b^{4k} \equiv$1(mod p). Now we found $b^{p-1} \equiv$1(mod p) and $b^{4k} \equiv$1(mod p) $\Rightarrow$4k|p-1 $\Rightarrow$p$\equiv$1(mod p).
From $b^{4k} \equiv$1(mod p) if follows that b^{4k}-1$\equiv$0(mod p) $\Rightarrow$(b^{2k}-1)(b^{2k}+1)$\equiv$0(mod p). So in case b^{2k}-1$\equiv$0 we have $b^{2k} \equiv$1(mod p). We already know that b^k=a hence b^{2k}=a^2. So the equivalence $a^2 \equiv$1(mod p) should been fulfilled. But as the order of a is four it follows that $a^2 \not\equiv$1(mod p). So b^{2k}-1$\not\equiv$0. Therefore, $b^{2k} \equiv$-1(mod p). So -1 is a square modulo p.
As $\mathbb{F}_p^*$ is a cyclic group, we proved the claim. $\square$

References

[1] Daivdoff Giuliana, Sarnak Peter, Valette Alain: Elementary Number Theory, Group Theory, and Ramanujan Graphs, `https://www.dhbw-mannheim.de/fileadmin/dhbw/download-center/lehrbeauftragte/literaturverzeichnis.pdf`, year of publication 2003, reference 08.10.2016