NOTES FOR ALGEBRAIC NUMBER THEORY M3P15

AMBRUS PÁL

1. Gaussian Integers

The Gaussian integers are complex numbers of the form:

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

Proposition 1.1. *Gaussian integers form a subring of complex numbers.*

Proof. Clearly $\mathbb{Z}[i]$ contains 0 and 1, so we only need to show that it is closed under addition and multiplication. We compute:

$$(a + bi) + (x + yi) = (a + x) + (b + y)i,$$
$$(a + bi)(x + yi) = (ax - by) + (ay + bx)i.$$

□

Proposition 1.2. *The function:*

$$N : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N} - \{0\}$$

given by the rule:

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

is well-defined and it is a homomorphism of semi-groups, i.e. it is multiplicative.

Proof. Note that:

$$N(a + bi) = (a + bi)\overline{(a + bi)}.$$

In particular for every non-zero $a + bi \in \mathbb{Z}[i]$ the number $N(a + bi)$ is positive, and therefore the function N is well-defined. Since it is the restriction of the complex norm onto $\mathbb{Z}[i]$, it is multiplicative, too. □

Proposition 1.3. *Let A, B, C, D be four points on the plane such that the rectangle $\overline{ABCD}$ is a square with sides of length one. Let P be an point on $\overline{ABCD}$. Prove that the distance of P from one of the four points A, B, C, D is at most $\frac{\sqrt{2}}{2}$.*

Proof. For one of the four triangles $\overline{ABP}$, $\overline{BCP}$, $\overline{CDP}$ or $\overline{ADP}$ the angle at P is at least 90 degrees. We may assume that this holds for the triangle $\overline{ABC}$ without the loss of generality. Let a, b, and c denote the length of the sides $\overline{AP}$, $\overline{BP}$ or $\overline{AB}$, respectively. Let α denote the angle at P. By the cosine law:

$$1 = c^2 = a^2 + b^2 - 2ab\cos(\alpha) \geq a^2 + b^2$$

since α is at least 90 degrees. We may assume that $a \geq b$ without the loss of generality. Then

$$1 \geq 2b^2.$$

□

Date: February 8, 2013.

Proposition 1.4. *The ring of Gaussian integers is an Euclidean domain.*

Proof. It will be enough to show that for every $x, y \in \mathbb{Z}[i] - \{0\}$ such that x does not divide y there is a $q \in \mathbb{Z}[i]$ such that $N(r) < N(x)$ where $r = y - xq$. Let $z = y/x$. Since on the complex plane the Eisenstein integers are the vertices of a mosaic which consists of squares whose sides have length one, there is a $q \in \mathbb{Z}[i]$ such that $|z - q| \leq \frac{\sqrt{2}}{2}$ by the previous proposition. For this choice of q we get

$$N(r) = |r|^2 = |y - xq|^2 = |z - q|^2 |x|^2 \leq \frac{1}{2} N(x).$$

□

Proposition 1.5. *We have* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Proof. First note that $u = a + bi \in \mathbb{Z}[i]$ is a unit if and only if $N(a + bi) = 1$. Indeed if $N(a + bi) = 1$ then $1 = (a + bi)\overline{(a + bi)}$ and since $\overline{(a + bi)} \in \mathbb{Z}[i]$ we get that $a + bi$ is a unit. On the other hand if $u \in \mathbb{Z}[i]^*$ then there is a $v \in \mathbb{Z}[i]$ such that $uv = 1$. By the multiplicativity of the the norm $N(u)N(v) = 1$. We get that $N(u)$ is a positive integer which divides 1, so it must be equal to 1. Let $a+bi \in \mathbb{Z}[i]$ be a unit. By the above

$$1 = N(a + bi) = a^2 + b^2,$$

and hence either $a = \pm 1$ and $b = 0$ or $b = \pm 1$ and $a = 0$. □

Lemma 1.6. *Let $u \in \mathbb{Z}[i]$ be a prime. Then either $u = \pm p, \pm ip$ where $p \in \mathbb{Z}$ is a prime number or $N(u) \in \mathbb{Z}$ is a prime number.*

Proof. Note that u divides the integer $N(u)$ so it must divide one of its prime factors, say $p \in \mathbb{Z}$. By the multiplicativity of the norm the integer $N(u)$ divides $N(p) = p^2$. Because u is not a unit we get that $N(u) = p$ or $N(u) = p^2$. We may assume that we are in the second case. Let $p = uv$ with $v \in \mathbb{Z}[i]$. By the multiplicativity of the the norm $N(u)N(v) = N(p)$. Because $N(u) = N(p)$ we get that $N(v) = 1$. The claim now follows from the previous proposition. □

Lemma 1.7. *Let $p \in \mathbb{Z}$ be an odd prime number. Then -1 is square mod p if and only if $p \equiv 1 \bmod 4$.*

Proof. Recall that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$. In particular $-1 \bmod p$ is its unique element of order 2, since p is odd. Moreover -1 is square mod p if and only if $(\mathbb{Z}/p\mathbb{Z})^*$ has and element of order 4. This happens if and only if 4 divides the order of this group, that is $p \equiv 1 \bmod 4$. □

Proposition 1.8. *A prime number $p \in \mathbb{N}$ is a prime of $\mathbb{Z}[i]$ if and only if $p \equiv -1$ mod 4.*

Proof. By the above p remains a prime in $\mathbb{Z}[i]$ if and only if it is not a norm of an element of $\mathbb{Z}[i]$. Since $1 + 1 = 2$, this is not the case for 2. When $p \equiv -1 \bmod 4$ the congruence

$$x^2 + y^2 \equiv p \mod 4$$

has no nontrivial solution so p must remain a prime in $\mathbb{Z}[i]$. So we may assume that $p \equiv 1 \bmod 4$. Suppose that p remains a prime! By the previous lemma the congruence $x^2 + 1 \equiv 0 \bmod p$ has a solution. Let x be such a solution; then p divides one of the Gaussian integers $x + i$ or $x - i$, since it divides their product. This implies that p divides ± 1 which is a contradiction. □

Theorem 1.9. *For every positive integer n the Diophantine equation:*

$$a^2 + b^2 = n, \quad a, b \in \mathbb{Z}$$

has a solution if and only if for every prime number $p \in \mathbb{N}$ such that $p \equiv -1 \bmod 4$ has an even exponent in the prime factorisation of n.

Proof. First note that this Diophantine equation has a solution if and only if n is the norm of a Gaussian integer. So in particular it has a solution for n prime when $p = 2$ or $p \equiv 1 \bmod 4$ and for $n = p^2$. Because the norm is multiplicative it also has a solution for any positive integer which can written as a product of such numbers. Therefore the condition is sufficient.

Assume now that $N(a + ib) = n$ with $a + bi \in \mathbb{Z}[i]$. Let p be a prime factor of n with number $p \equiv -1 \bmod 4$. It remains a prime in $\mathbb{Z}[i]$. By conjugating the unique prime factorisations of $a + bi$ and $a - bi$ we get that p has the same exponent in the prime factorisation of $a + bi$ and $a - bi$. Therefore it must have an even exponent in the prime factorisation of n, and hence the condition is necessary, too. $\square$