Introduction to Number Theory
8. exercise set, solutions

1. Assume that $1+i|a+bi$. Then there exists $c+di \in \mathbb{Z}[i]$ s.t. $a+bi = (c+di)(1+i)$. Opening the brackets and equating real and imaginary parts we get $a = c-d$ and $b = c+d$. This means that $a+b = 2c$ is even and thus a and b have the same parity i.e. $a \equiv b \pmod 2$. On the other hand, if $a \equiv b \pmod 2$ we can find integers c, d s.t. $a = c-d$ and $b = c+d$. Therefore also the other direction holds. □

2. This follows immediately from the definition of divisibility. □

3. We prove that no such triangle exists. Assume otherwise. Then we know that sides of the triangle are of the form $t(a^2-b^2)$, $2abt$ and $t(a^2+b^2)$ for some integers $a > b \geq 1$, $t \geq 1$. Now by assumption $100 = t(a^2-b^2+2ab+a^2+b^2)$ or $50 = at(a+b)$. In particular $a|50$ so $a \in \{1,2,5,10,25,50\}$. If $a \geq 10$, then clearly $at(a+b) \geq 10 \cdot 11 > 50$. Also $a > 1$ so actually $a \in \{2,5\}$. If $a = 2$ we must have $b = 1$ which does not yield solution as $3 \not| 50$. If $a = 5$ then $10 = t(5+b)$ which has no solution when $b < 5$. So the equation $50 = at(a+b)$ has no solution. This contradiction finishes the proof.

4. (i) Notice that $10 = 2 \cdot 5 = (1+i)(1-i)(1+2i)(1-2i)$. From the lectures we know that $1 \pm i$ are primes. On the other hand $N(1+2i) = N(1-2i) = 5 = 4+1$ is a prime so also $1 \pm 2i$ are primes. Since $\mathbb{Z}[i]$ is an UFD it follows that only prime factors are $1 \pm i$ and $1 \pm 2i$.

(ii) As $N(2-7i) = 53$ is a prime of the form $4k+1$ it follows that 53 is a Gaussian prime.

5. We prove the statement by induction on n. The case $n = 2$ follows from the definition of primality. Assume that the statement is true for some $n \geq 2$. Let π be a prime and $\pi|\lambda_1 \cdots \lambda_n \lambda_{n+1}$. Then $\pi|\lambda_1 \cdots \lambda_n$ or $\pi|\lambda_{n+1}$. If $\pi|\lambda_1 \cdots \lambda_n$ then $\pi|\lambda_i$ for some $i \in \{1, ..., n\}$ by induction assumption. This proves the claim. □

6. (i) Let $x = \{\lambda_0; \lambda_1, \lambda_2, ...\}$ be a second degree algebraic number. Then we have

$$B_k = -\frac{1}{\alpha_k}(A_k \alpha_k^2 + C_k)$$

for every k. We know that $\alpha_{k+1} = 1/(\alpha_k - \lfloor \alpha_k \rfloor) > 1$ so we have a lower bound for the sequence $\{\alpha_k\}$. To prove that there is an uniform upper bound, recall that $\lambda_k = \lfloor \alpha_k \rfloor$ so it suffices to prove that the sequence $\{\lambda_k\}$ is bounded from above. By exercise 7. of set 7. this is equivalent to the statement that there exists $c > 0$ s.t. the inequality

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q^2}$$

holds for all rationals p/q. But this is true by Liouville's theorem as x is a second degree algebraic number. Therefore the sequence $\{\alpha_k\}$ is bounded and the boundedness of $\{B_k\}$ follows immediately from the boundedness of the sequences $\{A_k\}$ and $\{C_k\}$. □

(ii) Consider the function $f(x,y) = 2Axy + B(x+y) + 2C$ which is clearly continuous. Then

$$B_k = q_{k-1} q_{k-2} f\left(\frac{p_{k-1}}{q_{k-1}}, \frac{p_{k-2}}{q_{k-2}} \right).$$

Let

$$M = \max_{y \in [\alpha-1, \alpha+1]} \left| \frac{\partial}{\partial x} f(x,y) \right| \quad \text{and} \quad N = \max_{x \in [\alpha-1, \alpha+1]} \left| \frac{\partial}{\partial y} f(x,y) \right|.$$

Now, by the mean value theorem and the triangle inequality

$$\begin{aligned}|B_k| &= q_{k-1}q_{k-2}\left|f\left(\frac{p_{k-1}}{q_{k-1}},\frac{p_{k-2}}{q_{k-2}}\right)-f(\alpha,\alpha)\right| \\ &\le q_{k-1}q_{k-2}\left|\frac{\partial}{\partial x}f(\xi)+\frac{\partial}{\partial y}f(\xi)\right|\cdot\left|\left(\frac{p_{k-1}}{q_{k-1}},\frac{p_{k-2}}{q_{k-2}}\right)-(\alpha,\alpha)\right| \\ &\le q_{k-1}q_{k-2}\left|\frac{\partial}{\partial x}f(\xi)+\frac{\partial}{\partial y}f(\xi)\right|\cdot\left(\left|\frac{p_{k-1}}{q_{k-1}}-\alpha\right|+\left|\frac{p_{k-2}}{q_{k-2}}-\alpha\right|\right) \qquad (1)\end{aligned}$$

for some ξ lying in the line segment connecting $(p_{k-1}/q_{k-1}, p_{k-2}/q_{k-2})$ and (α,α). Now by Theorem 5.12. we have

$$\begin{aligned}(1) &\le q_{k-1}q_{k-2}\left(\frac{1}{q_kq_{k-1}}+\frac{1}{q_{k-1}q_{k-2}}\right)(M+N) \\ &\le q_{k-1}q_{k-2}\cdot\frac{2}{q_{k-1}q_{k-2}}(M+N) \\ &= 2(M+N).\end{aligned}$$

This proves that the sequence $\{B_k\}$ is bounded. □

7*. *Solution 1.* As $(\alpha,p)=1$ it suffices to show that $\alpha^p\equiv\alpha \pmod p$. Write $\alpha=a+bi$, where $a,b\in\mathbb{Z}$. Then by binomial theorem

$$\alpha^p-\alpha=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}(bi)^k-(a+bi)\equiv a^p+(bi)^p-a-bi \pmod p$$

in $\mathbb{Z}[i]$. As $p=4k+1$ we have $i^{p-1}=1$. Therefore $a^p+(bi)^p-a-bi=a^p-a+i(b^p-b)$ which is divisible by p in $\mathbb{Z}[i]$ by applying Fermat's little theorem twice. Proof completed. □

If $p=4k-1$, then the statement is not true. Consider for example $p=3$ and $\alpha=1+i$. Then $(3,1+i)=1$ but $(1+i)^2-1=2i-1$ is not divisible by 3.

Solution 2. (Jakob Wartiovaara) Again it suffices to show that $\alpha^p\equiv\alpha \pmod p$. We proceed by induction on α. If $\alpha=0$, the statement is clear. Also, as $p=4k+1$ we have $\varepsilon^p=\varepsilon$ for every unit $\varepsilon\in\{\pm1,\pm i\}$. Assume that the statement is true for some α. Then for any $\varepsilon\in\{\pm1,\pm i\}$ we have

$$(\alpha+\varepsilon)^p-(\alpha+\varepsilon)=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}\varepsilon^k-(a+\varepsilon)\equiv a^p+\varepsilon^p-a-\varepsilon\equiv\alpha^p-\alpha\equiv 0 \pmod p.$$

in $\mathbb{Z}[i]$ by the induction assumption. So if the statement is true for some $\alpha\in\mathbb{Z}[i]$ then it is also true for numbers $\alpha\pm1$ and $\alpha\pm i$. Since any Gaussian integer can be obtained from the origin by adding finitely many units, the statement follows. □