Introduction to Number Theory
9. exercise set, solutions

1. (i) Note that $90 = 2 \cdot 3^2 \cdot 5$. The only prime factor of the form $\equiv 3 \pmod 4$ is 3. Its exponent is even so 90 can be written as a sum of two squares. This can be done in $4(1+1) = 8$ different ways by the formula of the lectures.

(ii) Note that $2331 = 3^2 \cdot 7 \cdot 37$. Now $7 \equiv 3 \pmod 4$ and its exponent is odd. Therefore 2331 cannot be written as a sum of two squares.

2. (i) Observe that $1 + 3i = i(3 - i)$ and $1 - 3i = -i(3 + i)$ so there is no contradiction as prime factor is unique up to associates.

(ii) Similarly there is no contradiction as $3 - 2i = -i(2 + 3i)$ and $3 + 2i = i(2 - 3i)$.

3. Let $n \in \mathbb{N}$. Let us consider pairs of integers (x, y) s.t. $x^2 + y^2 = k$ for some integer $1 \leq k \leq n$. The number of such pairs is

$$\sum_{k=1}^{n} r_2(k).$$

Identifying each such pair as a point in the plane we see that all of them lie inside a circle of radius $\sqrt{n}$.

We assign to each of such lattice point a unit square with sides parallel to the coordinate axis in the way that the given point is in one of the vertices of the assigned square (in the first quadrant the given point is the upper-right corner of the assigned square. In other quadrants assign squares which are obtained from squares of the first quadrant by an appropriate rotation). Simple comparison of areas shows that

$$\sum_{k=1}^{n} r_2(k) \leq \pi(\sqrt{n})^2 = \pi n.$$

The squares chosen above do cover the circle of radius $\sqrt{n} - 1$. Therefore

$$\pi(\sqrt{n} - 1)^2 \leq \sum_{k=1}^{n} r_2(k).$$

Now we have

$$\pi \cdot \frac{(\sqrt{n} - 1)^2}{n} \leq \frac{1}{n} \sum_{k=1}^{n} r_2(k) \leq \pi.$$

Letting $n \longrightarrow \infty$ gives the claim as the lower bound goes to π. □

4. Let's write down a Gaussian prime factorization for n. We know that Gaussian primes are $1 \pm i$, $a \pm bi$ with $a^2 + b^2$ prime $\equiv 1 \pmod 4$ and primes $\equiv 3 \pmod 4$ as well as their associates. Now

$$\begin{aligned} n &= 2^e \prod_{j=1}^{k} p_i^{\alpha_i} \prod_{n=1}^{\ell} q_n^{\beta_n} \\ &= i^e (1+i)^{2e} \prod_{j=1}^{k} (a_j + b_j i)^{\alpha_j} (a_j - b_j i)^{\alpha_j} \prod_{n=1}^{\ell} q_n^{\beta_n}. \end{aligned}$$

Now the number of factors is simply

$$4(2e+1)^2 \prod_{j=1}^{k} (\alpha_j + 1)^2 \prod_{n=1}^{\ell} (\beta_n + 1)^2,$$

as $a_j + b_j i, a_j - b_j i$ are not associates for any j and $1+i|n$ if and only if $1-i|n$. The factor 4 comes from the number of units. □

5. Let $\lambda = a+bi$ be a Gaussian integer. The following method yields its prime factors. First we calculate $N(\lambda) = a^2 + b^2$ and decompose it to a product of primes

$$N(\lambda) = 2^e \prod_{j=1}^{k} p_j^{\alpha_j} \prod_{n=1}^{\ell} q_n^{\beta_n},$$

where $p_j \equiv 1 \pmod 4$ and $q_n \equiv 3 \pmod 4$.

If $e > 0$ then $1+i$ is a prime factor of λ. If $\beta_n > 0$ for some n then q_n is a prime factor of λ. Suppose that $\alpha_j > 0$. We have $p_j = (a_j + b_j i)(a_j - b_j i)$ for some integers a_j, b_j. Then we know that at least one of the factors $a_j + b_j i$, $a_j - b_j i$ is a prime factor of λ. Analysis for each of these primes is easy.

Consider the example $\lambda = 7+i$. Then $N(\lambda) = 50 = 2 \cdot 5^2$. We immediately get that $1+i$ is a prime factor. Note that $5 \equiv 1 \pmod 4$. As $5 = (2+i)(2-i)$ we need to check that which of $2+i$, $2-i$ divide $7+i$. But this is straightforward to do by hand. It turns out that only $2+i$ divides it. Therefore the prime factors of $7+i$ are $1+i$ and $2+i$ as well as their unit multiples.

6. Assume that $x^2 + y^2 = z^2$ for some $x, y, z \in \mathbb{Z}$. It is enough to consider the case where $(x, y, z) = 1$. As in the lectures we can assume that x is odd and y is even. Then z must be odd. Note that $z^2 = x^2 + y^2 = (x+iy)(x-iy)$. Let $\pi \in \mathbb{Z}[i]$ be s.t. $\pi | x+iy, x-iy$. Now $N(\pi)|z^2$ so $N(\pi)$ is odd. Also π divides $(x+iy)+(x-iy) = 2x$ and $(x+iy)-(x-iy) = 2yi$. Thus $N(\pi)|4x^2, 4y^2$. As $(x, y) = 1$ it follows that $N(\pi) = 1$ so π is a unit. This implies that $x+iy$ and $x-iy$ are squares up to a unit.

If $x + iy = i(a+bi)^2$ we get $x = -2ab$ which is a contradiction as x was odd. Therefore $x + iy = (a+bi)^2$ for some integers $a, b \in \mathbb{Z}$. By comparing real and imaginary parts we get $x = a^2 - b^2$ and $y = 2ab$. Then we also get $z = a^2 + b^2$. Cases where units are $-1, -i$ are symmetric to previous cases. □

7*. For simplicity let us consider residue classes modulo Gaussian prime $a+bi$. We prove that the number of different residue classes modulo $a+bi$ is $N(a+bi) = a^2 + b^2$. The same result holds also for all Gaussian integers but is slightly harder to prove.

Let us first consider the case where the norm a^2+b^2 is a prime $p \equiv 1 \pmod 4$. If $b = 0$ the statement is clear so assume that $b \neq 0$. Obviously $i \equiv -ab^{-1} \pmod{a+bi}$ where $b^{-1} \in \mathbb{Z}$ is s.t. $bb^{-1} \equiv 1 \pmod p$. Therefore for every $c + di \in \mathbb{Z}[i]$ we have $c + di \equiv c - dab^{-1} \pmod{a+bi}$. In particular every Gaussian integer is congruent to an integer mod $a+bi$. By further reducing modulo p we see that every Gaussian integer is congruent to some of the numbers $\{0, 1, ..., p-1\}$ modulo $a+bi$. Standard arguments (as earlier in the course) verify that this is a complete residue system. Thus there were $p = N(a+bi)$ different residue classes.

For primes $p \equiv 3 \pmod 4$ one can use the same standard methods to prove that $\{c + di : 0 \leq c, d \leq p-1\}$ is a complete residue system mod p in $\mathbb{Z}[i]$. This set has $p^2 = N(p)$ elements.

8** (i) Observe that $x^2 + 4 = y^3$ can be written as $(x+2i)(x-2i) = y^3$. The greatest common divisor of $x+2i$ and $x-2i$ divides $(x+2i)-(x-2i) = 4i$, so no primes (with the exception of $1+i$ and its associates) can divide both $x+2i$ and $x-2i$. Paying particularly careful attention to the prime $1+i$ and its associates, we can straightforwardly deduce that

$x + 2i$ and $x - 2i$ must be perfect cubes over the Gaussian integers. Now we get

$$x + 2i = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$$

for some integers a, b.

Hence, equating real and imaginary parts, we get $x = a^3 - 3ab^2$ and $2 = (3a^2 - b^2)b$. The second of these is easy to solve, noting that b must be in the set $\{\pm 1, \pm 2\}$ leading to the following solutions: $(a, b) = (\pm 1, 1)$ or $(\pm 1, -2)$. Substituting back into $x = a^3 - 3ab^2$, this gives the solutions solutions $(x, y) = (\pm 2, 2), (\pm 11, 5)$.

(ii) The equation is equivalent to $x^5 = (y + i)(y - i)$. If x is even, then $y^2 \equiv -1 \pmod 4$, which is impossible. So x is odd. Then y is even and consequently the elements $y + i$ and $y - i$ are coprime in $\mathbb{Z}[i]$. Since x^5 is a fifth power, it follows that $y + i$ and $y - i$ are both fifth powers. Let $a, b \in \mathbb{Z}[i]$ be such that

$$y + i = (a + bi)^5 = a(a^4 - 10a^2b^2 + 5b^4) + b(5a^4 - 10a^2b^2 + b^4)i.$$

It holds that $1 = b(5a^4 - 10a^2b^2 + b^4)$ and therefore $b = \pm 1$. It is now easy to get that the only solution is $(x, y) = (1, 0)$.