Algebraic Number Theory
Manuel Luethi
Federico Viola

Exercise Sheet 3
Spring 2024

---

1. Let $j := (-1 + \mathrm{i}\sqrt{3})/2 = e^{2\mathrm{i}\pi/3}$.
   a) Show that $\mathbb{Z}[j]$ is a Euclidean ring (and thus principal).
   b) Let $\alpha = a + bj \in \mathbb{Z}[j]$. Show that
   $$|\mathbb{Z}[j]/(\alpha)| = a^2 - ab + b^2.$$
   c) Let $p \geqslant 2$ be a prime number. Prove that we have a ring isomorphism
   $$\mathbb{Z}[j]/(p) \cong \mathbb{F}_p[X]/(X^2 + X + 1).$$
   d) Deduce that $p \geqslant 5$ is not prime in $\mathbb{Z}[j]$ if and only if -3 is a square modulo p.
   e) Show that -3 is a square modulo p if and only if $p \equiv 1 \mod 3$.
   Hint: If -3 is a square mod p, construct an element of order 3 in $\mathbb{F}_p^\times$. This is an explicit instance of quadratic reciprocity.
   f) Conclude that a prime $p \geqslant 5$ is of the form $a^2 - ab + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 3$.
   Remark: You have classified the primes that are representable by the quadratic form $X^2 - XY + Y^2$.
2. **Completing the descent step of Fermat's last theorem for n=3**
   Following the notation of the lecture notes, we start with a solution
   $$x^3 + y^3 = 3^{3v} z^3$$
   with $\gcd(x, y, z) = 1$, $3 \nmid xyz$ and $v \geqslant 1$
   We factorised
   $$x^3 + y^3 = (x + y)(x + yj)(x + yj^2)$$
   in $\mathbb{Z}[j]$ and used that $\mathbb{Z}[j]$ is a P.I.D. to obtain
   $$\begin{aligned} x + y &= 3^{3v-1}\rho_0^3 \\ x + yj &= \pi_3 \rho_1^3 \\ x + yj^2 &= \overline{\pi_3 \rho_1^3} \end{aligned}$$
   where $\pi_3 = 1 - j$, $\rho_0 \in \mathbb{Z}$, $\rho_1 \in \mathbb{Z}[j]$. We will now construct a strictly smaller solution. We denote $\rho_1 = a + bj$.
   a) Show that
   $$x + y = 9ab(a - b)$$
   b) Show that $a, b, a - b$ are cubes in $\mathbb{Z}$. (You may like to begin by showing that they are pairwise co prime.)
   c) Deduce from the previous parts that
   $$a^2 b - ab^2 = 3^{3(v-1)}\rho_0^3.$$
   If $3 \nmid ab$ use the above equation to complete the descent step.
   Hint: If $p \neq 3$ is a prime and
   $$p \mid \gcd(a^2 b, ab^2, \rho_0^3)$$
   show that
   $$p^3 \mid \gcd(a^2 b, ab^2, \rho_0^3).$$

d) Assume $3|a$ (the case $3|b$ is similar). Use the identity

$$a^2b - ab^2 = (a-b)^2b + (a-b)b^2$$

to complete the descent step.

3. The goal of this exercice is to prove Fermat's Theorem for $n = 4$: if $(x, y, z) \in \mathbb{Z}^3$ is a solution of $X^4+Y^4 = Z^4$, then $xyz = 0$. A solution (x, y, z) satisfying $xyz = 0$ is called a trivial solution. In fact, we will prove that there are no non-trivial solution to the equation

$$X^4 + Y^4 = Z^2,$$

which clearly implies Fermat for $n = 4$. We do this by contradiction. Let (x, y, z) be a non-trivial solution. Show that :

a) We can assume that $0 < x, y, z,\ (x, y) = 1,\ x$ odd and y is even.

b) Using the parametrization of the primitive Pythagorean triple, show that there exists $0 < m, n$ such that $(m, n) = 1,\ x^2 + n^2 = m^2$ and n is even.

c) m and $\frac{n}{2}$ are squares. (**Hint:** compute $m\frac{n}{2}$)

d) there exists r, s with $(r, s) = 1,\ m = r^2 + s^2$ and $n = 2rs$. Conclude that both r, s are squares and that there exists u, v, w such that

$$w^2 = u^4 + v^4$$

and $0 < w < z$.

e) Conclude.

4. In SageMath, the ring of integers, i.e. the Gaussian integers, inside the field of Gaussian numbers can be defined using the following lines:

```
K.<i> = NumberField(x^2 + 1)
OK = K.ring_of_integers()
```

We can determine the gcd of two Gaussian integers by first declaring them as elements in the ring of Gaussian integers and then invoking the built-in gcd function:

```
z = gcd(OK(17),OK(21+1*i))
```

A Gaussian number can be viewed as an element in the field $\mathbb{C}$ by embedding:

```
z = OK(3+2*i)
z_complex = z.complex_embedding()
```

a) If you have not done so already, use the gcd function and the algorithm from the last exercise sheet, write a function that takes as input a prime $p \equiv 1 \bmod 4$ and returns all the Gaussian integers $z \in \mathbb{Z}[i]$ satisfying $\mathrm{Nr}(z) = p$.

b) Write a function that takes as inputs a parameter $0 < c \leqslant 1$, a number $T > 0$, and returns the list of all Gaussian integers z (viewed as elements in the complex plane) whose squared absolute value is a prime in $[cT, T]$.
Hint: Look at the function `next_prime()`.

c) Using the function `list_plot()`, plot the set

$$A_{c,T} = \frac{1}{\sqrt{T}}\big\{z \in \mathbb{Z}[i] \colon \mathrm{Nr}(z) \text{ is prime and } cT \leqslant \mathrm{Nr}(z) \leqslant T\big\}.$$

d) Given $0 \leqslant \alpha < \beta < 1$ and $c \in (0, 1)$, numerically evaluate the share of elements $z \in A_{c,T}$ in the sector of angles between $2\pi\alpha$ and $2\pi\beta$, i.e. determine

$$\Omega_{c,T}(\alpha, \beta) = \frac{1}{|A_{c,T}|}\big\{z \in A_{c,T} \colon \mathrm{Arg}(z) \in [2\pi\alpha, 2\pi\beta)\big\}.$$

Can you come up with a conjecture about the behaviour of $\Omega_{c,T}(\alpha, \beta)$ as T becomes large?

Hint: In order to calculate the argument of `y = z.complex_embedding()`, you explicitly convert it to a complex number, cf. `y.arg()` vs. `CC(y).arg()`.