---

1. Let $p \in \mathbb{Z}$ be a prime. Let us consider the principal ideal
$$(p) := p\mathbb{Z}[i] \lhd \mathbb{Z}[i].$$
Since $\mathbb{Z}[i]$ is a P.I.D. we can factorise (p) into prime ideals. Show that exactly one of the following holds,
   a) The ideal (p) is prime in $\mathbb{Z}[i]$. (In this case we say (p) is *inert*.)
   b) The ideal (p) splits into two distinct prime ideals in $\mathbb{Z}[i]$. (In this case we say (p) is *totally split*.)
   c) The ideal (p) is a square of a prime ideal in $\mathbb{Z}[i]$. (In this case we say (p) is *ramified*.)

   Can you classify which primes are inert, totally split and ramified?
   Hint: Consider the norm of the ideal (p) i.e. $|\mathbb{Z}[i]/(p)|$ and use Fermat's last theorem.
2. We saw in the lecture that
$$\mathbb{Z}[i]/(a+bi) \simeq \mathbb{Z}^2/\mathbb{Z}^2 \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$
as $\mathbb{Z}$-modules. Using this we concluded that
$$|\mathbb{Z}[i]/(a+bi)| = \left|\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right| = a^2+b^2.$$
In this exercise we will prove a more general version of this statement. Recall that a *lattice* $\Lambda \subseteq \mathbb{R}^n$ is a discrete subgroup containing a basis of $\mathbb{R}^n$; cf. §A.2.1 in the lecture notes.
If $\Lambda \subseteq \mathbb{R}^n$ is a lattice, then $\Lambda = \mathbb{Z}^n g$ for some $g \in \mathrm{GL}_n(\mathbb{R})$; cf. Lem. 3 in §A.2.1 of the lecture notes. Throughout this exercise, $\Lambda \subseteq \mathbb{R}^n$ is a lattice and $\Lambda' \leqslant \Lambda$ is a subgroup.
   a) Show that if $\Lambda' < \mathbb{R}^n$ is a lattice $[\Lambda\colon \Lambda'] < \infty$ and
$$\mathrm{covol}(\Lambda') = \mathrm{covol}(\Lambda)[\Lambda\colon \Lambda'].$$
   b) Show that in general
$$\Lambda' = \mathbb{Z}^n M g \text{ for some matrix } M \in M_2(\mathbb{Z}).$$
   c) Suppose that $\Lambda' < \mathbb{R}^n$ is a lattice and let $M \in M_2(\mathbb{Z})$ as in the previous subexercise. Show that $M \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ and
$$[\Lambda\colon \Lambda'] = |\det(M)|.$$
3. Recall that in class we have proven the following statement.
   Let p be an odd prime and assume that -1 is a square in $\mathbb{F}_p$. Then p is a sum of two squares.

   This was proven by showing that there exists $r \in \mathbb{Z}[i]$ a non-unit such that $(r)|(p)$ but $(p) \nmid (r)$. However, the proof did not give us a way to determine r.
   In this exercise, we will give a constructive proof of the implication and we will use this to write a computer program to identify all representations of an admissible odd prime as a sum of two squares.

a) Let p and odd prime and $m \in \mathbb{Z}$ such that $m^2 = -1 (\mathrm{mod}\, p)$. Let

$$\pi = (m + i, p) \subset \mathbb{Z}[i]$$

be the ideal generated by p and $m + i$. Show that π is a prime ideal and that, for any generator r of π, we have $p = \mathrm{Nr}(r)$.

b) Show the converse: Assuming that p is an odd prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, deduce that $(a + ib) \subset \mathbb{Z}[i]$ is a prime ideal generated by p and an element of the form $m + i$ with $m \in \mathbb{Z}$ a square root of -1 mod p.

c) Using that $\mathbb{Z}[i]$ is Euclidean, find a generator of π.

d) Write a function that takes as input a prime $p \equiv 1 (\mathrm{mod}\, 4)$ and returns a list containing all pairs $(a, b) \in \mathbb{Z}^2$ such that $p = a^2 + b^2$.

You might want to use some of the following commands:

```
GF(p)                  # finite field of cardinality p
PolynomialRing(k, 't') # ring of polynomials in
                       # variable t with coefficients
                       # in k
P.roots()              # list of roots of polynomial
                       # P with multiplicities
x.lift()               # if x is in the field k = GF(p),
                       # then x.lift() is a represen-
                       # tative of x in ZZ
```