189-235A: Basic Algebra I
Assignment 5
Due Wednesday, November 20

1. Let $R = \mathbf{Z}[i]$ be the ring of Gaussian integers, and define the norm of an element $z = a+bi$ to be $|z| := z\bar{z} = a^2+b^2 \in \mathbf{Z}$. Show that R has a Euclidean division algorithm, in the sense that if z and w are Gaussian integers, there exist $q, r \in R$ for which

$$z = qw + r, \qquad \text{and} \qquad |r| < |w|.$$

(Hint: let q be the Gaussian integer whose real and imaginary parts are as close as possible to those of the complex number z/w.)

2. Use the result of question 1 to show that every ideal in $R = \mathbf{Z}[i]$ is principal.

3. Let p be a prime number of the form $4m + 1$ with $m \in \mathbf{Z}$. Show that p can be written as the sum of two integer squares: $p = a^2 + b^2$, for some integers $a, b \in \mathbf{Z}$. (Hint: Recall the fact shown in a previous assignment that the integer $t = (2m)!$ satisfies $t^2 + 1 \equiv 0 \pmod{p}$. Now, consider the ideal $I = (p, t + i)$ of $\mathbf{Z}[i]$ generated by p and $t + i$. Show that this ideal is not equal to R, and apply the result of problem 2 to it[1].)

[1]The theorem that every prime which is 1 mod 4 can be written as the sum of two integer squares was proved by Fermat. Its proof is one of the early landmarks of the subject, and is quite beautiful. Note that this proof uses Gaussian integers and involves substantial ideas from ring theory, even though the result is completely elementary and is, ostensibly, just a statement about regular integers.

4. Keeping notations as in problem 3, show that the function $\varphi : R \longrightarrow \mathbf{Z}/p\mathbf{Z}$ defined by

$$\varphi(a + bi) = [a - bt]_p,$$

where $[j]_p$ denotes the residue class of the integer j modulo p, is a ring homomorphism, and that I is its kernel. What is the quotient R/I isomorphic to?

5. Let $F = \mathbf{Z}/p\mathbf{Z}$ be the finite field with p elements, and let $G = \mathbf{GL}_2(F)$ be the group of invertible 2×2 matrices with entries in F. What is the cardinality of G? (Hint: how many possibilities are there for the first row of an invertible matrix? And, once the first row has been chosen, how many possibilities remain for the second row?)

6. List all the elements of order 2 in the dihedral group D_8 of order 8 (the group of symmetries of the square). Same question for the so-called quaternion group

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

of size 8, whose elements satisfy the rules

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i.$$

Show that D_8 and Q_8 are not isomorphic (i.e., there is no isomorphism between these two groups.)

7. Show that the group $\mathbf{GL}_2(\mathbf{Z}/2\mathbf{Z})$ of 2×2 matrices with entries in the field with two elements is isomorphic to the symmetric group S_3 on three elements. (Hint: consider the natural action of G on the set of non-zero column vectors in $(\mathbf{Z}/2\mathbf{Z})^2$.)

8. Let $P = \{0, 1, 2, \infty\} = \mathbf{Z}/3\mathbf{Z} \cup \{\infty\}$ be the so-called "projective line" over $\mathbf{Z}/3\mathbf{Z}$. Show that every element of the group $G = \mathbf{GL}_2(\mathbf{Z}/3\mathbf{Z})$ induces a permutation on P, whereby the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sends $j \in P$ to $\frac{aj+b}{cj+d}$, with the natural conventions. What is the kernel of the resulting homomorphism

$$\varphi : G \longrightarrow S_P$$

from G to the group $S_P \simeq S_4$ of permutations on P? Is φ surjective?

9. Let S be a subset of a group G. The centraliser of S, denoted $Z(S)$, is the set of $a \in G$ which commute with every $s \in S$, i.e., such that $as = sa$ for all $s \in S$. Show that $Z(S)$ is a subgroup of G.

10. Recall that the *conjugacy class* of a in a group G is the set of all elements of G which are of the form $a^{g^{-1}} := gag^{-1}$ for some $g \in G$. Show that a normal subgroup of G is a disjoint union of conjugacy classes. List the conjugacy classes in S_4 and use this to give a complete list of all the normal subgroups of S_4. Same question for S_5.