Problem Set 3.

1. This problem will show that given a Galois extension of the rational field there are infinitely many rational primes p such that the Frobenius element $Frob_p$ is trivial in the Galois group (a very weak version of what Chebotarev density states). For example, taking K to be the n-th cyclotomic field this proves that there are infinitely many primes p in the arithmetic progression $1 + pn$.

   Let K be a number field. Let $p \in \mathbf{Z}$ be a prime number. Let $\mathbf{O}$ be an order in K and consider the ring $\mathbf{O}/p\mathbf{O}$ as an O-module. Since it is finite we can find a maximal strictly increasing chain of ideals $p\mathbf{O} \subset M_1 \cdots M_t \subset \mathbf{O}$ such that M_i/M_{i-1} is a simple $\mathbf{O}$ module hence isomorphic to $\mathbf{O}/P_i$ for some prime ideal P_i containing p. Let $f_i = [\mathbf{O}/P_i : F_p]$ (the residue degree of P_i in $\mathbf{O}$) and let the number of M_j/M_{j+1} isomorphic to O/P_i be e_i (the ramification degree of P_i in $\mathbf{O}$). We call the numbers e_i, f_i the ramification data for p in $\mathbf{O}$.

   a) Show by computing the order of $\mathbf{O}/p\mathbf{O}$ that $[K : Q] = \sum e_i f_i$.

   b) Show that if $\mathbf{O}_1, \mathbf{O}_2$ are two orders, then for all but a finite number of primes the ramification data for p in $\mathbf{O}_1$ is the same as that in $\mathbf{O}_2$.

   c) Show that if α is an algebraic integer for which $K = \mathbf{Q}(\alpha)$ then in the order $\mathbf{Z}[\alpha]$ the ramification data can be computed from the factorization of $f_\alpha(x)$ modulo p and the ramification degrees e_i are 1 if p does not divide the discriminant of $f_\alpha(x)$.

   d) There exist infinitely many primes p for which there exists an index i such that $e_i = f_i = 1$. Hint: by b) it is enough to check this for an order of the form $Z[\alpha]$. Let α be a root of the monic integral polynomial $f(x)$. If there are only finitely many such primes such that there exists an index with $e_i = f_i = 1$, let B be the square of the product of $f(0)$ with $f'(0)$ and all primes such that some $e_i = f_i = 1$. Then $f(Bm) \in (Bm)^2 + f(0)$. If $p|B$ the power that it divides $f(Bm)$ is equal to the power that it divides $f(0)$ since all but the constant term are divisible by a strictly higher power of p. The integers $f(Bm)$ grow without bound, eventually surpassing $f(0)$. Since prime powers of $p|B$ dividing $f(Bm)$ must divide $f(0)$ and $f(Bm)$ is unbounded , there must exist a prime divisor p' of some $f(Bm)$ which does not divide B, so that $f(x)$ has an irreducible linear factor $x - Bm$ modulo p'. Then there is a prime P_i containing $p' \not| B$ with ramification data $e_i = f_i = 1$ for some i, but the assumption was that all such divided B.

   e) When K/Q is Galois, and $\mathbf{O} = \mathbf{O}_K$ show that all ramification data for P_i prime ideal containing p can be computed from inertia and decomposition groups via $e_i = |I_{P_i}|, e_i f_i = |G_{P_I}|$. Show that there exists infinitely many primes p such that

$Frob_p$ is trivial (a baby version of Chebotarev density). Take K to be the $n-th$ cyclotomic field to conclude that there are infinitely many p of the form $nk+1$.

2.

a) Let K be a number field with degree $[K:Q]$. Suppose that $p < [K:Q]$ is a rational prime and there exists $[K:Q]$ distinct prime ideals in $\mathbf{O}_K$ containing p. Show that for any $\gamma \in \mathbf{O}_K$ such that $K = \mathbf{Q}(\gamma)$, the index of $\mathbf{Z}[\gamma]$ in $\mathbf{O}_K$ is divisible by p. Hint: if not O_K/pO_K and $Z[\gamma]/pZ[\gamma]$ are isomorphic rings, so have the same number of prime ideals. Use the assumption $p < [K:Q]$ to bound the number of prime ideals in the latter ring.

b) (Dedekind 1878) Let K be the number field $\mathbf{Q}(\alpha)$, where α is a root of $x^3 + x^2 - 2x + 8 = 0$. Let $\beta = \frac{\alpha+\alpha^2}{2}$. Show that β is not in $\mathbf{Z}[\alpha]$ and compute the discriminant of $\mathbf{Z}[\alpha]$. Show that the maximal order of K is $\mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$. Show that $1, \alpha, \beta$ form an integral basis and compute the discriminant of $\mathbf{O}_K$.

c)) Show that in Dedekind's field K above that all elements are idempotents in $\mathbf{O}_K/2\mathbf{O}_K$ and show that $\alpha, \beta+1, \alpha+\beta$ are orthogonal idempotents summing to 1. Use this to find three distinct prime ideals of $\mathbf{O}_K$ containing 2. Use part a) to show that there is no $\gamma \in \mathbf{O}_K$ such that $Z[\gamma] = \mathbf{O}_K$ by determining an upper bound to the number of ideals in $\mathbf{Z}[\gamma]$ containing 2. Thus the maximal order may not be generated as a ring over the integers by a single algebraic integer.

3. (Stickelberger) Show that the discriminant of an order in a number field has remainder 0 or 1 after division by 4. Hint: Use the definition of the discriminant as the square of a determinant , and use the definition of the determinant of $[r_{ij}]$ as $\sum_\sigma sgn(\sigma) \prod_j r_{j\sigma(j)}$ as σ ranges over all permutations. Write this as a sum over even permutations P, minus a sum over odd permutations N, and show that $P+N$ and $4PN$ are rational using Galois theory, and integers since they are algebraic integers, and that the discriminant is $(P+N)^2 - 4PN$.