8430 HANDOUT 1

PETE L. CLARK

1. Statement of the Problem

For which primes p do there exist integers x, y such that $p = x^2 + ny^2$?

We will abbreviate the clause "there exist integers x, y such that $p = x^2 + ny^2$" to either "p is of the form $x^2 + ny^2$" or (worse!) to "$p = x^2 + ny^2$."

Unless otherwise noted, the following conventions are in force: $p > 2$, $(n, p) = 1$, and $n > 0$. These are in increasing order of seriousness: $p > 2$ is almost harmless; $(n, p) = 1$ will be an important technical assumption, and if n were negative the theory would have a quite different flavor. At times we will relax one or more of these conventions to see what happens, but this will happen with clear warning.

2. The fundamental congruence

The following observation will be our constant companion throughout the course.

Proposition 1. *Let n be any integer and p any prime. Then $p = x^2 + ny^2$ implies $-n$ is a square modulo p.*

Proof: Reducing the equation mod p, we get $x^2 \equiv -ny^2 \pmod{p}$. If $y \equiv 0 \pmod{p}$, then $x^2 \equiv 0 \pmod{p}$ hence $x \equiv 0 \pmod{p}$; then $p|x$, $p|y$ and thus $p^2 \mid x^2 + ny^2 = p$, a contradiction. So y is invertible mod p and we may write $-n \equiv (\frac{-x}{y})^2 \pmod{p}$.

3. When $\mathcal{O}_n$ is a PID

For any $n \in \mathbb{Z}$, define the **quadratic ring** $\mathcal{O}_n$ as the quotient ring $\mathbb{Z}[t]/(t^2 + n)$.

Exercise 1.3.1.
a) Show that in all cases the map the map $x + yt + \ldots + (t^2 + n) \mapsto (x, y)$ defines an isomorphism of additive groups from $\mathcal{O}_n$ to $\mathbb{Z}^2$.
b) Observe that if $n = 0$, the ring $\mathcal{O}_n$ is nonreduced, i.e., has nilpotent elements.
c) If $n = -m^2$, show that $\mathcal{O}_n$ is not an integral domain and is **not**[1] isomorphic to $\mathbb{Z} \times \mathbb{Z}$ as a ring.
d) Otherwise, show that $\mathcal{O}_n$ is an integral domain, with quotient field $\mathbb{Q}(\sqrt{-n})$.
e) Explain why the notation $\mathbb{Z}[\sqrt{-n}]$ is appropriate for $\mathcal{O}_n$ under the conditions of part d) but not those of part b) or c).

Exercise 1.3.2: Suppose that $n = -m^2$, so that $\mathcal{O}_n$ is not an integral domain. Determine exactly which integers N are of the form $x^2 + ny^2$.

[1]This corrects a longstanding error in these notes.

In the sequel we shall assume that n is not of the form $-m^2$. Again, the majority of our interest will be in the case $n > 0$, but for the rest of this section we also entertain the case of an arbitrary integer n not of the form $-m^2$.

Theorem 2. *Let $n \neq -m^2$ be an integer. Suppose that $\mathcal{O}_n$ is a principal ideal domain (henceforth PID). Then for any prime p (including $p = 2$ and $p \mid n$), if $-n$ is a square mod p then $p = |x^2 + ny^2|$.*

Proof: To say that $-n$ is a square mod p is to say that there exists $x \in \mathbb{Z}$ such that $p \mid x^2 + n$. In the ring $\mathcal{O}_n$ the latter factors as $(x + \sqrt{-n})(x - \sqrt{-n})$.

Suppose, for the sake of contradiction, that p is irreducible in $\mathcal{O}_n$. Then, since $\mathcal{O}_n$ is a PID, the principal ideal (p) is prime, i.e., it satisfies **Euclid's Lemma**: if $\alpha, \beta \in \mathcal{O}_n$ are such that $p \mid \alpha\beta$, then $p \mid \alpha$ or $p \mid \beta$. Thus under our assumption we get $p \mid x \pm \sqrt{-n}$, which would mean that the element $\frac{x}{p} \pm \frac{\sqrt{-n}}{p}$ of the quotient field $\mathbb{Q}(\sqrt{-n})$ actually lies in $\mathcal{O}_n$, i.e., $\frac{x}{p}$, $\frac{1}{p}$ are both integers – this is the content of Exercise 1.1a) – but clearly $\frac{1}{p}$ is not an integer, contradiction.

Therefore p factors nontrivially in $\mathcal{O}_n$, meaning there exist nonunits $\alpha = x + \sqrt{-n}y$ and $\beta \in \mathcal{O}_n$ such that $p = \alpha\beta$. To finish the proof we need some simple properties of norms. **norm map** $N : \mathbb{Q}(\sqrt{-n}) \to \mathbb{Q}$ by $N(x + \sqrt{-n}y) = x^2 + ny^2$.

Exercise 1.3.3: For any integer n define the norm map: $N : \mathcal{O}_n \to \mathbb{Z}$ by
$N(x + yt + \ldots + (t^2 + n)) = x^2 + ny^2$.
a) Show that $N(\mathcal{O}_n) \subset \mathbb{N}$ iff $n \geq 0$.
b) Show that N is multiplicative: for all $\alpha, \beta \in \mathcal{O}_n$, $N(\alpha\beta) = N(\alpha)N(\beta)$.
c) Show that if α is a unit of $\mathcal{O}_n$, then $N(\alpha)$ is a unit of $\mathbb{Z}$, i.e., is ± 1.
d) Show that if $-n$ is not a square, then conversely an element $\alpha \in \mathcal{O}_n$ of norm ± 1 must be a unit in $\mathcal{O}_n$. Does this hold in general?
e) When $n = 1$, show that there are exactly four units in $\mathcal{O}_n$, all of norm 1. When $n > 1$, show that there are exactly 2 units, all of norm 1.

Remark: When $n = -d$ with d a positive nonsquare integer, the ring $\mathcal{O}_n$ has infinitely many units of norm 1. Equivalently, **Pell's equation** $x^2 - dy^2 = 1$ has infinitely many solutions. There are known necessary and sufficient conditions on d for $x^2 - dy^2 = -1$ to have solutions (i.e., for there to exist units of norm -1), but these are rather subtle, e.g. involving the period length of the continued fraction expansion of $\sqrt{d}$. For more on this, see e.g. `http://math.uga.edu/ pete/4400pellnotes.pdf`.

To finish the proof of the theorem: applying N to the equation $p = \alpha\beta$ we get

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Therefore we must have

$$p = |N(\beta)| = |N(\alpha)| = |N(x + \sqrt{-n}y)| = |x^2 + ny^2|.$$

Theorem 2 leads swiftly to both positive and negative results.

Exercise 1.3.4: Show that for $n = 1, \pm 2, -3$, $\mathcal{O}_n$ is a PID. (Suggestion: Show that for these values, $|N| : \mathcal{O}_n \to \mathbb{Z}$ is a Euclidean norm.)

Corollary 3. *(Fermat) A prime $p = x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \pmod 4$.*

Proof: By Exercise 1.3.4, the Gaussian integer ring $\mathcal{O}_1 = \mathbb{Z}[\sqrt{-1}]$ is a PID. Since -1 is, like any integer, a square modulo 2, according to the theorem we have $2 = x^2 + y^2$. Otherwise p is an odd prime, and the condition that -1 be a square mod p is precisely that $p \equiv 1 \pmod 4$. This is the celebrated **First Supplement to the Quadratic Reciprocity Law**.

Corollary 4. *(Fermat) A prime $p = x^2 + 2y^2$ iff $p = 2$ or $p \equiv 1$ or $3 \pmod 8$.*

Proof: By Exercise 1.3.4, $\mathcal{O}_2 = \mathbb{Z}[\sqrt{-2}]$ is a PID. Again we certainly have -2 is a square mod 2, so that 2 is of the form x^2+2y^2. Otherwise p is an odd prime and we want to work out the condition $(\frac{-2}{p}) = 1$. This symbol is equal to $(\frac{2}{p}) \cdot \frac{-1}{p}$. By the **Second Supplement to the Quadratic Reciprocity Law**, $(\frac{2}{P}) = 1$ iff $p \equiv 1, 7 \pmod 8$ and equals -1 iff $p \equiv 3, 5 \pmod 8$. Combining this with the conditions for $(\frac{-1}{p}) = 1$, we want the product to be 1, so we want either both symbols to be 1 or both to be -1. It is easy to see tht the former occurs iff $p \equiv 1 \pmod 8$ and the latter occurs iff $p \equiv 3 \pmod 8$.

Proposition 5. *For $n \in \mathbb{Z}^+$, 2 is of the form $x^2 + ny^2$ iff $n = 1, 2$.*

Exercise 1.3.5: Prove Proposition 5.

But now suppose $n > 2$. Consider the situation of the theorem with $p = 2$. We certainly do have that $-n$ is a square mod 2 – every integer is! – and by Proposition 5, 2 is certainly not of the form $x^2 + 2y^2$. The inexorable conclusion:

Corollary 6. *For no $n > 2$ is the ring $\mathcal{O}_n$ a PID.*

Remark: The condition that irreducible elements generate prime ideals holds for any Unique Factorization Domain (UFD),[2] thus for $n > 2$ $\mathcal{O}_n$ is not even a UFD.

This is a distressingly typical example of how far one gets in algebraic number theory by hoping that all the rings which arise naturally in one's Diophantine problems are UFD's. Compare: if for an odd prime p the cyclotomic ring $\mathbb{Z}[\zeta_p] = \mathbb{Z}[t]/(t^{p-1} + t^{p-2} + \ldots + t + 1)$ is a UFD, then is not too hard to establish Fermat's Last Theorem in exponent p. In 1847 Lamé announced in the Paris Academy of Sciences his complete proof of FLT but was immediately shot down by Liouville, who noticed that Lamé had blithely assumed unique factorization in $\mathbb{Z}[\zeta_p]$, whereas in fact Kummer had already shown that this fails for $p = 23$ (and in fact it fails for all larger primes). It is tempting to chastise Lamé for his lack of familiarity with the quadratic form $x^2 + ny^2$ and the quadratic ring $\mathcal{O}_n$, but of course this is unfair and backwards: the notion of an "ideal number" was invented by Kummer himself for exactly these reasons and was then gradually developed over the next century to give ideals as we now know them.

Kummer discovered that a weaker condition on $\mathbb{Z}[\zeta_p]$ than unique factorization would suffice: the natural line of attack needs that if $\alpha_1, \ldots, \alpha_p$ are elements of $\mathbb{Z}[\zeta_p]$ which are (i) not simultaneously divisible by any nonunit in the ring and (ii) have product equal to a pth power, then each α_i is equal to a pth power times a unit in the ring. But this latter condition will hold in any Dedekind domain in

[2]This is very close to being a characteristic property of UFDs: a Noetherian integral domain in which irreducible elements are prime is a UFD.

which each ideal whose pth power is principal is itself principal. If $\mathbb{Z}[\zeta_p]$ has this property then p is called a **regular prime**; for such primes Kummer proved FLT.[3]

4. All about an ideal

We can restate the problem as one of the principality of a certain ideal in $\mathcal{O}_n$.

Let n be any integer not of the form $-m^2$, so $\mathcal{O}_n$ is an integral domain. Let p be any prime, and consider the principal ideal $(p) = p\mathcal{O}_n$.

Lemma 7. *The following are equivalent:*
(i) $-n$ is a square mod p.
*(ii) The ideal (p) of $\mathcal{O}_n$ is **not** prime.*

Proof: Of course an ideal I in a commutative ring R is prime iff R/I is an integral domain. Here we have

$$\mathcal{O}_n/(p) = \mathbb{Z}[t]/(p, t^2 + n) = \mathbb{F}_p[t]/(t^2 + n).$$

The ring $\mathbb{F}_p[t]$ is a PID, so the ideal $(t^2 + n)$ in it is not prime iff $t^2 + n$ factors over $\mathbb{F}_p$. Evidently this last condition occurs iff $-n$ is a square mod p.

Suppose now that $-n$ is a square mod p, as it must be in order for p to be of the form $x^2 + ny^2$. Then $p\mathcal{O}_n$ is not a prime ideal, so it is certainly not a maximal ideal, so it is properly contained in some maximal ideal $\mathfrak{p}$ of $\mathcal{O}_n$. In fact, because the ideals containing (p) in $\mathcal{O}$ correspond to the ideals of the quotient ring $\mathbb{F}_p[t]/(t^2 + n)$, one sees immediately that if $p = 2$ or $p \mid n$ there is a unique maximal ideal $\mathfrak{p}$ containing p; otherwise there are two maximal ideals containing p. We leave it as an informal exercise to the reader to show that complex conjugation on $\mathbb{Q}(\sqrt{-n})$ – otherwise known as the unique order 2 automorphism of anything in sight – interchanges the two maximal ideals containing p, so we may denote them as $\mathfrak{p}$ and $\overline{\mathfrak{p}}$.

Either way, it must be the case that $\mathcal{O}/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$.

Exercise 1.4.1: a) Suppose R is an integral domain which is finitely generated as a $\mathbb{Z}$-module. Show that if I is any nonzero ideal of R, then R/I is finite.
(If you don't know where to start, the magic words are "integral extension." See e.g. `http://math.uga.edu/ pete/4400algebra3.pdf`.)
b) Deduce that in such a ring, every nonzero prime ideal is maximal: the Krull dimension of R is at most 1.

Exercise 1.4.2: In particular, the previous exercise applies to $\mathcal{O}_n$, so for any nonzero ideal I of this ring, we get a positive integer $N(I) := \#\mathcal{O}_n/I$. Show that if $I = (x + \sqrt{-n}y)$ is a principal ideal, $N(I) = |x^2 + ny^2|$.
(Hint: use $x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$.)

[3]It has long been conjectured that the set of regular primes has density more than one half, but it is still not known whether there are infinitely many regular primes despite the fact that we know (i) there are infinitely many irregular primes and (ii) nevertheless FLT holds for these primes as well!

Theorem 8. *Let $n \neq -m^2$ be an integer, and p be any prime number.*
a) $-n$ is a square mod p iff $\mathcal{O}_n$ contains an ideal $\mathfrak{p}$ of norm p.
b) p is of the form $|x^2 + ny^2|$ iff $\mathcal{O}_n$ contains a principal ideal of norm p.

Proof: Part b) is immediate from the preceding exercise. We showed the "only if" direction of part a) above. Finally, we saw above that if $-n$ is not a square mod p, the principal ideal $(p) = p\mathcal{O}_n$ is prime. By Exercise 1.4.1 it is therefore maximal, so the only two ideals containing p are (p), of norm p^2, and $\mathcal{O}_n$ itself, of norm 1.

Note that by comparing Proposition 5 and Theorem 8 we get:

Corollary 9. *For $n \geq 3$, the unique ideal $\mathfrak{p}_2$ of norm 2 in $\mathcal{O}_n$ is nonprincipal.*

This is a bit misleading in that, depending upon the shape of the prime factorization of n, there are two quite different explanations for the non-principality of $\mathfrak{p}_2$.

5. When $\mathcal{O}_n$ is Dedekind

Let us end by making contact with the next important idea in basic algebraic number theory: that of a Dedekind domain. A **Dedekind domain** is an integral domain R satisfying the following conditions:

(DD1) R is Noetherian.
(DD2) Every nonzero prime ideal of R is maximal.
(DD3) R is integrally closed in its quotient field K: if $\alpha \in K$ and there exists $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in R[t]$ such that $P(\alpha) = 0$, then $\alpha \in R$.

Remark: According to this definition, any field is Dedekind domain, of course in a quite trivial way. In general discussions of Dedekind domains the case of a field is often excluded, but this is so harmless as to not be worth fussing about.

There are many other characterizations. Here are two of the most important examples of Dedekind domains:

Proposition 10. *Any PID is a Dedekind domain.*

Exercise 1.5.1: Prove Proposition 10.

For the second example, let K be any algebraic number field, i.e., a field extension of $\mathbb{Q}$ of finite degree. Let $\mathcal{O}_K$ be the ring of all algebraic integers of K, i.e., elements α of K satisfying a monic polynomial with $\mathbb{Z}$-coefficients. Then $\mathcal{O}_K$ is a Dedekind domain. First, as a $\mathbb{Z}$-module, $\mathcal{O}_K \cong \mathbb{Z}^r$, $r = [K : \mathbb{Q}]$, and since $\mathbb{Z}$ is a Noetherian ring, all of the $\mathbb{Z}$-submodules of $\mathcal{O}_K$ are finitely generated: this is in two ways stronger than saying that all ideals are finitely generated (two ways since an ideal is a very special kind of $\mathbb{Z}$-module, and finite generation as an ideal is a weaker condition than finite generation as a $\mathbb{Z}$-module). We saw in Exercise 1.4.1 that nonzero prime ideals of a domain which is finitely generated as a $\mathbb{Z}$-module are maximal and this applies to $\mathcal{O}_K$. Finally one must check the integral closure property, which is always the most subtle. Here the idea is that by definition $\mathcal{O}_K$ is obtained as the integral closure of $\mathbb{Z}$ in K, and a basic (but not tautological) tenet of the theory of integral extensions is that integral closures are integrally closed.

Now of course we come to the question of whether $\mathcal{O}_n$ is a Dedekind domain. We have already seen that it satisfies (DD1) and (DD2). What is at issue is whether it is integrally closed in its quotient field $\mathbb{Q}(\sqrt{-n})$.

First, for any rational number r, the field obtained by adjoining to $\mathbb{Q}$ $\sqrt{-n}$ is the same as the field obtained by adjoining $\sqrt{-nr^2} = r\sqrt{-n}$. The upshot of this is that in contrast to the quadratic rings, the distinct quadratic fields are given by $\mathbb{Q}(\sqrt{-n})$ for $-n$ a *squarefree* integer not equal to 0 or 1. So if for some integer $d > 1$ we have $d^2 \mid n$, then the quotient field of $\mathcal{O}_n$ contains the element $\sqrt{\frac{-n}{d^2}} = \frac{\sqrt{-n}}{d}$, but $\mathcal{O}_n$ does not contain this element and hence is not integrally closed.

Now let $-n$ (not 0 or 1) be squarefree and take $N = -n$ for notational simplicity. Consider an arbitrary element $\alpha = r + s\sqrt{N}$ of $\mathbb{Q}(\sqrt{N})$, with $r, s \in \mathbb{Q}$. Then

$$\frac{\alpha - r}{s} = \sqrt{N},$$

$$\frac{\alpha^2 - 2r\alpha + r^2}{s^2} = N,$$

$$\alpha^2 - 2r\alpha + r^2 - Ns^2 = 0.$$

Thus the minimal polynomial of α is $t^2 - 2rt + r^2 - s^2N = 0$.

Exercise 1.5.2: Let R be a UFD with quotient field F, K a field extension of F, and α an element of K which is algebraic over F, i.e., satisfies some nonzero polynomial with F-coefficients. Show that the following are equivalent:
(i) α satisfies a monic polynomial with R coefficients.
(ii) The minimal polynomial of α (i.e., the unique monic polynomial of minimal degree satisfied by α) has integral coefficients.

Therefore in order for α to be an algebraic integer it is necessary and sufficient that there are integers u and v such that

$$2r = u,\ r^2 - Ns^2 = v.$$

Case 1: u is even. Then $r \in \mathbb{Z}$, hence $Ns^2 = r^2 - v \in \mathbb{Z}$. Since N is squarefree, $s \in \mathbb{Z}$ and we get (unshockingly) that $r + s\sqrt{N}$ is an algebraic integer.

Case 2: u is odd. Then $N(2s)^2 = u^2 - 4v$. Again, since N is squarefree this shows that $2s \in \mathbb{Z}$. However, if s were an integer, the left hand side would be even, whereas the right hand side is odd. Thus there must exist an odd integer w such that $2s = w$, i.e., $Nw^2 = u^2 - 4v$. If we reduce modulo 4, then we get $N \equiv 1 \pmod 4$. Conversely, if $N \equiv 1 \pmod 4$ and $r = \frac{u}{2}$ and $s = \frac{w}{2}$ are half-integers, then $2r = u$ and $r^2 - Ns^2 = \frac{u^2 - Nv^2}{4}$ are integers, so $r + s\sqrt{N}$ is an algebraic integer.

Theorem 11. *Let N be a squarefree integer, not equal to 0 or 1. Then the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{N})$ is:*
- $\mathbb{Z}[\sqrt{N}] = \{x + y\sqrt{N} \mid x, y \in \mathbb{Z}\}$, *if* $N \equiv 2, 3 \pmod 4$,
- $\mathbb{Z}[\frac{1+\sqrt{N}}{2}] = \{\frac{x}{2} + \frac{y}{2}\sqrt{N} \mid x, y \in \mathbb{Z},\ x \equiv y \pmod 2\}$ *if* $N \equiv 1 \pmod 4$.

We have proven everything except that in the case $N \equiv 1 \pmod 4$, the set of elements $x + y\sqrt{N}$ with x and y either both integers or both half integers can be

described in the two ways of the statement of the theorem. The second expression should be obvious after a moment's thought, whereas the first requires a small computation which we leave to the reader.

Corollary 12. *The quadratic ring $\mathcal{O}_n$ is a Dedekind domain iff n is squarefree and congruent to* 1 *or* $2 \pmod 4$.

6. Orders and Discriminants

Let K be a number field of degree $[K : \mathbb{Q}] = d$, and let Λ be a full $\mathbb{Z}$-lattice in K, i.e., the $\mathbb{Z}$-span $\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$ of a $\mathbb{Q}$-basis $e_1, \ldots, e_n$ for K. We can use the multiplicative structure on K to endow it with a symmetric $\mathbb{Q}$-bilinear form:

$$\langle x, y \rangle := tr(xy),$$

where $\mathrm{tr} : K \to \mathbb{Q}$ is the usual trace map, e.g. defined by $\mathrm{tr}(\alpha)$ is the trace of the linear transformation $\alpha\cdot$ of K. We define the **discriminant** $\Delta(\Lambda)$ of the lattice Λ as the determinant of the matrix with (i, j) entry $T(i, j) = \mathrm{tr}(e_i e_j)$. One needs to check that this is well-defined:

Exericse 1.6.1:
a) Let $\sigma_1, \ldots, \sigma_n$ denote the distinct embeddings of K into an algebraically closure. Show that the discriminant of Λ with respect to the $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ can also be computed as $\det(M(i, j))^2$, where $M(i, j) = (\sigma_i e_j)$.
b) Deduce that $\Delta(\Lambda)$ is independent of the choice of $\mathbb{Z}$-basis. (This uses the "lucky" fact that $(\mathbb{Z}^\times)^2 = \{1\}$.)

Roughly speaking, one should think of the discriminant of Λ as being the square of its volume.

For N a nonsquare integer, let us compute the discriminant of $\mathbb{Z}[\sqrt{N}]$, viewed as a lattice in $\mathbb{Q}(\sqrt{N})$. A $\mathbb{Z}$-basis is given by $(1, \sqrt{N})$. Using Exercise 6.1.1, we can compute the discriminant as the square of the determinant of the 2×2 matrix $[[11]][[\sqrt{N} - \sqrt{N}]$: it is $(-2\sqrt{N})^2 = 4N$.

By definition, the discriminant *of the number field* K is the discriminant of the ring $\mathcal{O}_K$ of all algebraic integers. For those who are paying attention, we have not proved that $\mathcal{O}_K$ is a full $\mathbb{Z}$-lattice in K in the general case, but in the case we care about, that of a quadratic field, we have proved this and more: we know exactly what $\mathbb{Z}$-lattice it is. In general, if R is a Dedekind domain with quotient field F and K/F is a finite separable field extension, then the integral closure S of R in K is a Dedekind domain which is, as an R-module, at least locally free of rank n, so if R is a PID it is (in any reasonable sense) a full R-lattice. This applies with $R = \mathbb{Z}$ to give the case for number fields.

Anyway, we know that the ring of integers of $\mathbb{Q}(\sqrt{N})$ has integral basis $1, \sqrt{N}$ if $N \equiv 2, 3 \pmod 4$, and has integral basis $1, \frac{1+\sqrt{N}}{2}$ if $N \equiv 1 \pmod 4$. So:

Proposition 13. *The discriminant of the quadratic field $\mathbb{Q}(\sqrt{N})$ is:*
- $4N$, *if* $N \equiv 2, 3 \pmod 4$
- N, *if* $N \equiv 1 \pmod 4$.

Proof: We have already computed the discriminant in the first case. In the second case, we get

$$(\frac{1-\sqrt{D}}{2} - \frac{1+\sqrt{D}}{2})^2 = D.$$

Quadratic orders: An **order** in a number field K is a full $\mathbb{Z}$-lattice $\mathcal{O}$ which is also a subring.[4] Because an algebraic number α is an algebraic integer iff the $\mathbb{Z}$-algebra $\mathbb{Z}[\alpha]$ it generates is a finitely generated $\mathbb{Z}$-module, and submodules of finitely generated $\mathbb{Z}$-modules are finitely generated, it follows that all elements of an order $\mathcal{O}$ are integers, so that $\mathcal{O}$ is a subring of $\mathcal{O}_K$, which (by the above remarks; again, we have shown this in the quadratic case) is itself an order and therefore the unique **maximal order**.

Example: Any subring of a number field contains the usual integers $\mathbb{Z}$, so the only order in $\mathbb{Q}$ is $\mathbb{Z}$ itself.

We will find all orders $\mathcal{O}$ in a quadratic field $K = \mathbb{Q}(\sqrt{N})$. Write the ring of integers as $\mathbb{Z}[\theta_N]$, where θ_N is either $\sqrt{N}$ or $\frac{1+\sqrt{N}}{2}$, depending upon $N \pmod 4$. Either way, every element of the ring of integers $\mathcal{O}_K$ is of the form $a + b\theta_N$ for $a, b \in \mathbb{Z}$. Clearly $\mathcal{O}$ must contain such an element with $b \neq 0$, otherwise it would just be the ordinary integers $\mathbb{Z}$ and not have K as its field of fractions. But since $\mathcal{O}$ contains $\mathbb{Z}$, it contains $a + b\theta_N - a = b\theta_N$ for some nonzero integer b. It follows that there is a least positive integer $\mathfrak{f}$ such that $\mathfrak{f}\theta_N \in \mathcal{O}$, called the **conductor** of the order.

Exercise 1.6.2: a) Let $\mathcal{O} \subset \mathcal{O}_K$ be an order in a quadratic field. Show that the conductor $\mathfrak{f}$ is the index of the quotient abelian group $\mathcal{O}_K/\mathcal{O}$.
b) Let $n \neq -m^2$ be an integer, and write $n = f^2N$, where N is squarefree. Then our quadratic ring $\mathcal{O}_n = \mathbb{Z}[\sqrt{-n}]$ is an order in $\mathbb{Q}(\sqrt{N})$. Show that its conductor is (alas!) f if $N \equiv 2, 3 \pmod 4$ and $2f$ if $N \equiv 1 \pmod 4$.

Exercise 1.6.3: a) Show that the discriminant of $R(N, \mathfrak{f}) = \mathfrak{f}^2 \cdot \Delta(N)$, where $\Delta(N) = N$ if $N \equiv 1 \pmod 4$ and $4N$ otherwise.
b) Conclude that a nonsquare integer D is the discriminant of some quadratic order iff $D \equiv 0, 1 \pmod 4$.
c) Does it make any sense to speak of a quadratic ring of discriminant 0? Or of square discriminant m^2? (Hint: yes.)

In view of this exercise, we define a **quadratic discriminant** to be a nonsquare integer D which is 0 or $1 \pmod 4$, and for any such number D we denote by $\mathcal{O}(D)$ the unique quadratic order of discriminant D.

Our original problem was to determine which primes p were represented by x^2+ny^2, i.e., which primes are norms from the quadratic ring $\mathbb{Z}[\sqrt{-n}]$. When the squarefree part N of n is 1 or $2 \pmod 4$, we are therefore studying all orders in the quadratic field $\mathbb{Q}(\sqrt{-N})$; however when $N \equiv 3 \pmod 4$, we are rather studying all orders in $\mathbb{Q}(\sqrt{-N})$ of even conductor. But this is close enough to the general case that it

[4]Just to be sure, I consider the multiplicative identity 1 part of the structure, so a subring S of R needs to contain the multiplicative identity 1 of R.

will be conceptually easier to slightly expand our problem and study *all* orders in (at least imaginary) quadratic fields.

In other words, for a fixed quadratic discriminant D, we wish to study the set of primes p which are of the form $N(\alpha)$ for $\alpha \in \mathcal{O}(D)$. For completeness, we record the analogues of previous theorems in this level of generality:

Theorem 14. *a) If a prime p is of the norm $N(\alpha)$ for some $\alpha \in \mathcal{O}(D)$, then D is a square modulo p.*
b) If $\mathcal{O}(D)$ is a PID, then every $p > 2$ such that D is a square mod p is of the form $N(\alpha)$, $\alpha \in \mathcal{O}(D)$.

Exercise 1.6.4: Prove Theorem **??**. (Hint: Write $\mathcal{O}(D) = \mathbb{Z}[\tau_D]$, and figure out how the minimal polynomial of τ_D factors modulo p.)

Note that this result does not completely generalize Theorem 2 in that in part b) we now, truly, need p to be odd. The point is that in general the minimal polynomial to τ_D has a slightly more complicated shape than $t^2 - D$, and – as you will see in doing the Exercise – the condition that this minimal polynomial factors modulo 2 is not automatic and thus cannot be equivalent to the tautology "D is a square mod 2". This in fact motivates us to reserve the symbol $(\frac{D}{2})$ to mean something different and slightly more sophisticated than "D is a square modulo 2":

Exercise 1.6.5: Let D be a quadratic discriminant and p be a prime. Define the **Kronecker symbol** $(\frac{D}{2})$ to be
• 0 if the ideal (p) in $\mathcal{O}(D)$ is not prime and is contained in a unique prime ideal;
• -1 if the ideal (p) in $\mathcal{O}(D)$ is prime;
• 1 if the ideal (p) is not prime and is contained in two prime ideals.
a) Show that the Kronecker symbol agrees with the Legendre symbol whenever both are defined.
b) Show that $(\frac{D}{2})$ depends only on $D \pmod 8$ and thus explicitly compute it.

Exercise 1.6.6:
a) Show that any number field $K \neq \mathbb{Q}$ has infinitely many distinct orders.
b)* Show that it need not be the case that there exists an algebraic integer α such that every order in K is of the form $\mathbb{Z}[f\alpha]$ for some $f \in \mathbb{Z}^+$.[5] Indeed, even the full ring of integers need not be of this form.

The set of all orders in a higher degree number field is very complicated. On the other hand the study of nonmaximal orders is also very useful – much more useful than you might think by reading most standard texts on algebraic number theory, which tend to say little or nothing about non-maximal orders. Let me just make a vague remark that will become successively less vague as the course progresses: despite its relatively elementary description, of the most enduringly mysterious objects in algebraic number theory is the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ of a number field K. As we shall see, for a nonmaximal order $\mathcal{O}$ in K, by being a bit more careful one can still define a class group (or, as we shall call it later, a **Picard group** $\mathrm{Cl}(\mathcal{O})$,

[5]Off the top of my head, it seems possible that this *never* happens for $[K : \mathbb{Q}] > 2$.

which surjects onto the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ and fits into an exact sequence

$$1 \to \mathcal{O}_K^\times/\mathcal{O}^\times \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1.$$

All the groups in this sequence are finite. Thus the strucutre of $\mathrm{Cl}(\mathcal{O})$ can be deduced from that of $\mathcal{O}$ together with that of some rather more tractable invariants of K. In the case of a quadratic field K, we will see that this leads to an explicit formula for $\frac{\#\mathrm{Cl}(\mathcal{O})}{\#\mathrm{Cl}(\mathcal{O}_K)}$, a formula which will be quite useful in the explicit construction of abelian extensions of K and (when K is imaginary) in the analysis of elliptic curves with complex multiplication.

The last few years have seen amazing advances in the study of orders of number fields of (at least somewhat) higher degree, due especilaly to work of Manjul Bhargava. It would be perhaps overly optimistic to hope that we may discuss some of Bhargava's work at the end of the course, but it is not completely impossible.

7. The Cases of Class Number 1 (Part I)

Early on we exhausted the cases in which $\mathbb{Z}[\sqrt{-n}]$ is a PID: $n = 1, 2$. But what if $\mathbb{Z}[\sqrt{-n}]$ fails to be a PID "only because" it is not integrally closed? One way to interpret this is to see if we can solve our problem for a *non-maximal* imaginary quadratic order $\mathcal{O}$ when the maximal order $\mathcal{O}_K$ is a PID. This amounts to contemplating a representation of p as the norm of an element α in the maximal order and trying to see if that either automatically means that α is in the smaller order $\mathcal{O}$ or if there is some closely related $\alpha' \in \mathcal{O}$ of norm p.

$n = 4$: This case is a model of simplicity. We know that a prime p is of the form $x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \pmod 4$. So, given that we can write $p = x^2 + y^2$, can we also write it as $u^2 + 4w^2 = u^2 + (2y)^2$? In other words, is there some way to write p as a sum of two squares one of which is even? Clearly yes, so:

Theorem 15. *A prime p is of the form $x^2 + 4ny^2$ iff $p \equiv 1 \pmod 4$.*

Next we cite the following fact:

Proposition 16. *For $D = -3, -7, -11$, the full ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-n}}{2}]$ is Euclidean with repect to the norm map, hence is a PID.*

Exercise 1.7.1: Prove Proposition 16.

Exercise 1.7.2: For $D = -3,\ -7, -11$, find all primes p which are of the form $N(\alpha)$ for $\alpha \in \mathcal{O}(D)$.

Now suppose that $n = 3$, 7, 11, or more generally that $n \equiv 1 \pmod 4$ is squarefree, so that norm form on $\mathcal{O}_K$ can be written as $N(\frac{x}{2} + \frac{y}{2}\sqrt{-n}) = \frac{x^2+ny^2}{4}$ for integers x, y of equal parity.

So let us look at the case of the order $\mathbb{Z}[\sqrt{-3}]$: i.e., the ring $\mathcal{O}_3 = \mathcal{O}(-12)$. According to Theorem X.X, we can represent an odd prime p as $\frac{x^2}{4} + n\frac{y^2}{4}$ with $x \equiv y \pmod 2$ iff $1 = (\frac{-3}{p})$. Using **Quadratic Reciprocity** we get $(\frac{-3}{p}) = (\frac{p}{3})$, so a prime can be represented iff $p \equiv 1 \pmod 3$. Clearing the denominator, we have

shown for any $p \equiv 1 \pmod 3$, we may write

$$4p = x^2 + 3y^2$$

with the extra condition that x and y have equal parity. So the question is: given that we have such a representation, can we find one (not necessarily the one we start with) which has $x = 2X$ and $y = 2Y$ both even? If so, we divide both sides by 4 and get $p = X^2 + 3Y^2$.

Let's experiment, starting with $p = 7$. We can write $28 = 4 \cdot 7$ as $4^2 + 3 \cdot 2^2$, which is the way we want to write it – so that $7 = 2^2 + 3 \cdot 1^2$. However we can also write it as $1^2 + 3 \cdot 3^2$, which is not of the form we want. As in the case of $n = -2$ above, this suggests that we look at the units in $\mathcal{O}_K$. The ring of integers of $\mathbb{Q}(\sqrt{-3})$ has, uniquely among all quadratic fields, six units, the 6th roots of unity, generated by $\zeta_6 = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Let's try multiplying by ζ_6 and see what happens:

$$(1 + 3\sqrt{-3}) \cdot (\frac{1}{2} + \frac{1}{2}\sqrt{-3}) = -4 + 2\sqrt{-3}.$$

Success! I leave you the fun of confirming that this happens in general:

Exericse 1.7.3: Suppose that $4p = x^2 + 3y^2 = N(x + \sqrt{-3}y)$, with x and y both odd. Show that

$$N(x \pm y\sqrt{-3}) \cdot N(\frac{1}{2} + \frac{1}{2}\sqrt{-3}) = 4p \cdot 1 = 4p$$

expresses $4p$ in the form $(x')^2 + 3(y')^2$ with x', y' even, and conclude that p is of the form $x^2 + 3y^2$.

Thus we (you and I) have proved:

Theorem 17. *A prime p is of the form $x^2 + 3y^2$ iff $p = 3$ or $p \equiv 1 \pmod 3$.*

Exercise 1.7.4: a) Suppose that x and y are integers of the same parity, and $p \equiv 1 \pmod 3$ is a prime, such that $x^2 + 3y^2 = 4p$. Show that there exist $X,\ Y \in \mathbb{Z}$ of the same parity with $4p = X^2 + 3Y^2$ and $3 \mid Y$.
b) Conclude that a prime p is a norm from the ring $\mathcal{O}(27)$ of conductor 3 in $\mathbb{Q}(\sqrt{-3})$ iff $p \equiv 1 \pmod 3$.

Try to work out the $n = 7$ ($D = -28$) case for yourself:

Theorem 18. *A prime p is of the form $x^2 + 7y^2$ iff $p = 7$ of $p \equiv 1, 2, 4 \pmod 7$.*

Exercise 1.7.5: Prove Theorem 18. Some hints:
a) If $p \neq 7$ is an odd prime, use Quadratic Reciprocity to show that $(\frac{-7}{p}) = 1$ iff $p \equiv 1, 2, 4 \pmod 7$.
b) Working as above, deduce that for $p \equiv 1, 2, 4 \pmod 7$, we have $4p = x^2 + 7y^2$ for integers x and y of equal parity.
c) Show that it is not possible for x and y both to be odd.

Let us next look at $n = 11$. For odd $p \neq 11$, the fundamental congruence $(\frac{-11}{p}) = 1$ is equivalent (via Quadratic Reciprocity) to p being a square mod 11,

i.e., $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. But it is obviously not the case that $5 = x^2 + 11y^2$.

It turns out that these are all the "trivial" cases of our *original* problem, which considers only orders of even conductor in $\mathbb{Q}(\sqrt{N})$ when $N \equiv 1 \pmod 4$. To be more precise:

Theorem 19. *(Landau, 1903) For a positive integer n, TFAE:*
a) If $p > 2$ is such that $(\frac{-n}{p}) = 1$, then $p = x^2 + ny^2$.
b) $n = 1$, 2, 3, 4 or 7.

As we shall see, these are exactly the values of n for which a certain abelian group attached to the ring $\mathbb{Z}[\sqrt{-n}]$, the **ideal class group**, is trivial. Evidently we must make our way to the definition of the ideal class group of a not-necessarily maximal order in order to give such a proof. But in fact Landau's proof is quite elementary, using no algebraic number theory whatsoever, and is given quite early in Cox's book (p. 31). This latter proof uses some simple properties of quadratic forms, and it is a good example of a fact which, while possible to state and prove both in the language of ideals and ideal classes and in that of quadratic forms and equivalence classes, is probably more natural and transparent on the quadratic forms side. In the fullness of time we will see both proofs.

Now I must stop and raise a question of a kind that I strongly advise you *not* to ask about any living mathematician, at least not in their presence: why wasn't Theorem 19 proved by Gauss a century before? I can imagine that the answer Gauss would give: he probably could have proved the theorem if he wanted, but he was much more preoccupied with a more important theorem: namely, what about the case of representations by other quadratic orders, including maximal orders $\mathcal{O}(N)$, $N \equiv 1 \pmod 4$? The result here is the following:

Theorem 20. *(Heegner-Baker-Stark) For a quadratic discriminant $D < 0$, TFAE:*
a) If $p > 2$ is such that $(\frac{D}{p}) = 1$, then p is a norm from $\mathcal{O}(D)$.
b) $D = -3,\ -4, -7,\ -8,\ -11,\ -12,\ -16,\ -19,\ -27, -28,\ -43,\ -67,\ -163$.

Remark: The fundamental discriminants in the list (those of conductor 1) correspond to quadratic fields whose ring of integers is a PID, so the theorem asserts (and can be seen without too much trouble to be equivalent to asserting) that the complete list of such imaginary quadratic fields is $\mathbb{Q}(\sqrt{D}$ with

$$D = -3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163.$$

Note that to show that b) implies a) we must show (in addition to what we have already shown) that $\mathcal{O}(D)$ is a PID when $D = -19,\ -43,\ -67,\ -163$. This is a bit harder than the other PID results, since for these values $\mathcal{O}(D)$ is not a norm-Euclidean ring. But for at least 150 years we have known an algorithm that, given a number field K, will decide if the ring of integers is a PID. Moreover, in the case of quadratic fields this computation can be done with the aid of quadratic forms, and goes back all the way to Gauss, who certainly knew the implication b) $\implies$ a) of the theorem.

The converse, that a) $\implies$ b), is something else altogether! It was conjectured by Gauss in his *Disquisitiones Arithmeticae* and was from that point onward viewed as one of the most important problems of algebraic number theory. As far as I am

aware, the finiteness of the set of discriminants described in part a) was first proved by Heilbronn in the 1930's, and in 1935 Siegel was able to show that if the list in part b) were incomplete, it was only by one, fundamental, discriminant. Number theorists were haunted by this spectral "10th imaginary quadratic field of class number one" for at least the next 20 years. In 1952, the (amateur!) mathematician Kurt Heegner wrote a paper purporting to prove that there was no such field. The paper did not inspire confidence in the mathematical community: leading experts were not able to follow its reasoning and viewed it as obscure: according to Harold Stark, Heegner appeared to rely quite heavily on some assertions of the eminent late 19th century mathematician Weber, assertions which had never been proven and were viewed with suspicion by contemporary experts. Heegner died in 19XX. The first accepted proofs were given at about the same time in 1966 by Andrew Baker (using deep results in transcedence theory) and Harold Stark (using modular functions). According to Stark, he looked at Heegner's proof as a graduate student couldn't understand it, but after he found his own proof he looked again, and quite surprisingly to everyone, he found that he could now understand it and see that it was completely correct! Stark has at several points written about the issue, starting in a 1969 Journal of Number Theory article with the memorable title *On the "gap" in a theorem of Heegner*. In a more recent paper, he says that certain things in Heegner's paper relied on the unjustified work of Weber but the solution of class number one, upon close inspection, simply does not. For that matter, also in the late 60's Bryan Birch weighed in by proving the conjectures of Weber mentioned in Heegner's paper, so some sources also give him some of the credit!

All in all it is one of the most curious and poignant stories in the history of mathematics. My heart goes out to Kurt Heegner, an amateur mathematician (surely the greatest such of all time?) who did what Gauss could not but whose work was not accepted within his own lifetime. On the other hand, it will be my great pleasure to be able to discuss a proof of the Heegner-Baker-Stark theorem later in the course.