Math 154. Diophantine applications of class groups

1. Motivation

In this handout we wish to give two completely different classical applications of class groups to solving concrete Diophantine problems. By way of motivation, recall that if $p \neq 2$ is a positive odd prime then we saw via arithmetic in $\mathbf{Z}[i]$ that $p = x^2 + y^2$ for some $x, y \in \mathbf{Z}$ if and only if $-1 \equiv \square \bmod p$ (which in turn is the same as the congruential condition $p \equiv 1 \bmod 4$ by quadratic reciprocity). If you think about it, this is quite remarkable: the property of p being the value of an integral binary quadratic form $(x^2 + y^2)$ is equivalent to a congruential condition ($p \equiv 1 \bmod 4$) away from finitely many exceptions (such as $p = 2$). Recall also that in Homework 2, Exercise 1(ii), you similarly used arithmetic in $\mathbf{Z}[\sqrt{-2}]$ to show that if $p \neq 2$ is a positive odd prime then $p = x^2 + 2y^2$ if and only if $2 \equiv \square \bmod p$, which in turn is equivalent to the congruential condition $p \equiv \pm 1 \bmod 8$ by quadratic reciprocity. A related method handles the analogous problem for $x^2 + 3y^2$ by using the imaginary quadratic field $\mathbf{Q}(\sqrt{-3})$; there is a mild complication due to the fact that the ring of integers is not $\mathbf{Z}[\sqrt{-3}]$ but rather is $\mathbf{Z}[\zeta_3] = \mathbf{Z}[(1 + \sqrt{-3})/2]$, and in Exercise 2 of Homework 2 you saw how to deal with that.

But how about the general problem of characterizing those positive primes p having the form $p = x^2 + ny^2$ for a fixed non-square integer $n > 2$? As you might imagine, this is closely tied up with arithmetic questions in the imaginary quadratic field $\mathbf{Q}(\sqrt{-n})$, and the simplest cases to first consider are when n is squarefree and $n \equiv 1, 2 \bmod 4$ (so $\mathbf{Z}[\sqrt{-n}]$ is the ring of integers). But our old method that worked well for $n = 1, 2$ can hit a new problem: what do we do if $\mathbf{Z}[\sqrt{-n}]$ is not a PID? In general there are serious problems due to the intervention of non-trivial class groups, and a completely satisfactory answer can only be understood using the full power of class field theory (and is also the motivating theme in the book *Primes of the form* $x^2 + ny^2$ that I do not recommend). But for some small n we can overcome these class group obstructions without needing techniques as advanced as class field theory, and in §**??** we work out the first nontrivial case $n = 5$ (for which the associated imaginary quadratic field $\mathbf{Q}(\sqrt{-5})$ has class number 2, as will be proved in a later lecture).

Another classical application of class groups to Diophantine problems is analyzing $\mathbf{Z}$-solutions to equations of the form $y^2 = x^3 + k$ for various nonzero $k \in \mathbf{Z}$. This equation can be rewritten as $x^3 = y^2 - k$, so clearly the case when k is a square is rather special (since if $k = m^2$ then we have $x^3 = (y - m)(y + m)$ and we can try to play off the two factorizations against each other). Similarly, if k is a cube then $x^3 + k$ factors and we can again try to play elementary games by comparing factorizations. Hence, to make things as interesting as possible let us suppose that k is a non-square and a non-cube. It is natural to work in the quadratic field $\mathbf{Q}(\sqrt{k})$ in which we have $x^3 = (y + \sqrt{k})(y - \sqrt{k})$. (One could instead try to work in the cubic field $\mathbf{Q}(k^{1/3})$ over which $x^3 + k$ admits a linear factor, but that sure sounds worse than working in a quadratic field!)

In the special case $k = -2$ this is the old problem of Fermat which we settled at the beginning of the course by using the fact that $\mathbf{Z}[\sqrt{-2}]$ has unique factorization and its only units are ± 1, which are both cubes. In general the possibility that $\mathbf{Z}[\sqrt{k}]$ may fail to be a UFD is a real problem. Another potential problem is that this ring may have infinitely many units (especially non-cube units!). When $k > 0$ this always happens (remember that k is a non-square now), due to the Dirichlet unit theorem for real quadratic fields, as you considered in Homework 2, Exercise 4. The group of units for $k > 0$ will always be infinite cyclic and hence *modulo cubes of units* the unit group collapses to a nontrivial finite group. Nonetheless, there can still be difficulties (depending on peculiarities of a generator of the unit group up to signs).

For example, in the case $k = 2$ the ring of integers of $\mathbf{Q}(\sqrt{k})$ is $\mathbf{Z}[\sqrt{k}]$ and this is a UFD with fundamental unit $u = 1 + \sqrt{2}$, so to find all solutions to $y^2 = x^3 + 2$ with $x, y \in \mathbf{Z}$ (e.g., $(-1, \pm 1)$ are two such solutions) we first observe that x must be odd (as $2 \bmod 8$ is not a square) and hence infer from the factorization $x^3 = (y + \sqrt{2})(y - \sqrt{2})$ that $y + \sqrt{2} = \pm u^j (a + b\sqrt{2})^3$ with $a, b \in \mathbf{Z}$. Absorbing powers of u^3 and the sign (if it occurs) into $(a + b\sqrt{2})^3$ brings us to three cases: $y + \sqrt{2} = u^j (a + b\sqrt{2})^3$ with $j = 0, \pm 1$. But $-1/u$ is conjugate to u, so by applying the Galois conjugation if necessary (which swaps $\sqrt{2}$ and $-\sqrt{2}$ but has no effect on x or y) we just have to treat the cases $j = 0, 1$. The case $j = 0$ is easy to rule out since the $\sqrt{2}$-part of $(a + b\sqrt{2})^3 = a(a^2 + 6b^2) + b(3a^2 + 2b^2)\sqrt{2}$ has all monomials divisible by one of the unknowns $a, b \in \mathbf{Z}$

(forcing $b = \pm 1$, from which we can get a contradiction when trying to solve for a). However, analysis of the case $j = 1$ runs into a problem because

$$(1+\sqrt{2})(a+b\sqrt{2})^3 = (a^3+6ab^2+6a^2b+4b^3) + (a^3+6ab^2+3a^2b+2b^3)\sqrt{2}$$

and understanding integer solutions to the resulting cubic equation $a^3+6ab^2+3a^2b+2b^3 = 1$ is a decidedly nontrivial matter (least of all because there *are* some integer points on this cubic, such as $(\pm 1, 0)$ corresponding to $(x,y) = (-1, \pm 1)$). Hence, when $k > 0$, if congruence arguments do not rule out the possibility of solutions then the presence of nontrivial units can create serious algebraic difficulties. (In some cases one gets lucky; e.g., for $k = 6$ a suitable analysis with units leads to a cubic equation in (a,b) for which there is a congruential obstruction to an integral solution, and so $y^2 = x^3 + 6$ has no integer solution).

The possibility that $\mathbf{Q}(\sqrt{k})$ has class number larger than 1 is also a serious problem. Below we explain in the special case $k = -51$ how this potential problem can be bypassed whenever the class number is not divisible by 3. So this teaches us a good lesson: even when the UFD property fails, we can sometimes use algebraic number theory (and especially the divisibility properties of the class number) to infer that things work out "as if" the UFD property held!

It should also be noted that the problem of understanding the structure of the set of $\mathbf{Z}$-points and $\mathbf{Q}$-points on cubic curves like $y^2 = x^3 + k$ for general k is really not best handled by the methods of algebraic number theory alone, but rather by working within the general arithmetic theory of elliptic curves over number fields (in which algebraic number theory plays a surprisingly decisive role!). But that is a saga for another course, so here we will stick to some illustrative examples in special cases.

2. Primes of the form $x^2 + 5y^2$

Which primes p have the form $x^2 + 5y^2$? Let us assume $p \neq 2, 5$, so p is unramified in the corresponding imaginary quadratic field $\mathbf{Q}(\sqrt{-5})$ (with discriminant -20). A necessary condition is that -5 is square modulo p. Indeed, if p is any prime whatsoever and $p = x^2 + 5y^2$ with $x, y \in \mathbf{Z}$ then p cannot divide y (as otherwise $p|x$, so p^2 divides $x^2 + 5y^2 = p$, a contradiction), so the congruence $x^2 \equiv -5y^2 \bmod p$ can be rewritten as $-5 \equiv (xu)^2 \bmod p$ where $uy \equiv 1 \bmod p$. Hence, indeed the condition $-5 \equiv \square \bmod p$ is a necessary condition. But it is *not* sufficient! In fact, by quadratic reciprocity we see that for $p \neq 2, 5$,

$$-5 \equiv \square \bmod p \Leftrightarrow p \equiv 1, 3, 7, 9 \bmod 20,$$

and the primes $3, 7, 23$ are of this type yet (by inspection) are not of the form $x^2 + 5y^2$.

Proposition 2.1. *For a positive prime $p \neq 2, 5$,*

$$-5 \equiv \square \bmod p \Leftrightarrow p = x^2 + 5y^2 \textit{ for some } x, y \in \mathbf{Z} \textit{ or } 2p = x'^2 + 5y'^2 \textit{ for some } x', y' \in \mathbf{Z},$$

and the two possibilities on the right cannot both occur for the same p.

There is a better result which can be deduced from this proposition: for $p \neq 2, 5$, we have $p = x^2 + 5y^2$ for some $x, y \in \mathbf{Z}$ if and only if $-5 \equiv \square \bmod p$ (i.e., $p \equiv 1, 3, 7, 9 \bmod 20$) *and* $p \equiv 1 \bmod 4$, so in other words a necessary and sufficient condition is that $p \equiv 1, 9 \bmod 20$. Indeed, if $p = x^2 + 5y^2$ then p is a square modulo 5, hence $p \equiv 1, 4 \bmod 5$, so the proposition implies that $p \equiv 1, 9 \bmod 20$. Conversely, if $p \equiv 1, 9 \bmod 20$ (so $p \equiv 1, 4 \bmod 5$ and $(-5|p) = 1$) then the proposition shows that if p does not have the form $x^2 + 5y^2$ then $2p$ has such a form and hence $2p$ is a square modulo 5. That forces $p \equiv 2, 3 \bmod 5$, which is a contradiction.

The key point to be learned from the proof below is that the cause of the more subtle nature of the statement of the proposition (in contrast with what we have seen for $x^2 + ny^2$ for $n = 1, 2, 3$) is that $\mathbf{Q}(\sqrt{-5})$ has nontrivial class group. In fact, if the class group has size more than 2 then in general the condition that $p = x^2 + ny^2$ *cannot* be characterized (with finitely many exceptions) by congruential conditions on p. (For example, if $p \neq 2, 23$ then $p = x^2 + 23y^2$ if and only if $p \equiv \square \bmod 23$ and $t^3 - t - 1 \equiv 0 \bmod p$ has a solution; this is related to the fact that $\mathbf{Q}(\sqrt{-23})$ has class number 3.) But to explain why involves class field theory, so rather beyond the level of this course.

Our proof of the proposition rests on the fact, to be proved in a later lecture, that the class group for $\mathbf{Q}(\sqrt{-5})$ is of order 2 and is generated by the unique prime ideal $\mathfrak{p}_2$ over the ramified prime 2. We have

$(2) = \mathfrak{p}_2^2$, and explicitly $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ (though this explicit expression for $\mathfrak{p}_2$ will not be used below). Since $x^2 + 5y^2 = (x + y\sqrt{-5})(x - y\sqrt{-5})$ and $\mathbf{Z}[\sqrt{-5}]$ is the ring of integers of $K = \mathbf{Q}(\sqrt{-5})$ with unit group $\mathscr{O}_K^\times = \{\pm 1\}$, we may rephrase the condition $p = x^2 + 5y^2$ as the condition on ideals that $(p) = \mathfrak{a}\overline{\mathfrak{a}}$ for a *principal* ideal $\mathfrak{a}$ of $\mathscr{O}_K$. (Here we use positivity of p and of the norm for imaginary quadratic fields to avoid unit difficulties caused by passing from equality of principal ideals back to equality of elements.) How do we tell when (p) admits such a factorization $\mathfrak{a}\overline{\mathfrak{a}}$ in principal ideals? The key point is to forget about principality and to ask the weaker question of when (p) admits such a factorization in ideals at all!

Now the arithmetic of quadratic fields comes in. Since $p \neq 2, 5$, so it is unramified in K, we know that it is either split or inert: either $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ with a prime ideal $\mathfrak{p} \neq \overline{\mathfrak{p}}$ or (p) is prime. In the second case it is impossible to write $(p) = \mathfrak{a}\overline{\mathfrak{a}}$ for an ideal $\mathfrak{a}$ of $\mathscr{O}_K$ (consider the consequences in terms of the prime ideal factorization of $\mathfrak{a}$!), whereas in the first case we see by *unique prime factorization* for the hypothetical $\mathfrak{a}$ that the only possibilities are $\mathfrak{a} = \mathfrak{p}$ or $\mathfrak{a} = \overline{\mathfrak{p}}$. Since the conjugation action on ideals has no effect on whether or not an ideal is principal, we see that (for $p \neq 2, 5$) $p = x^2 + 5y^2$ for $x, y \in \mathbf{Z}$ if and only if two properties hold: p is *split* in K and the prime ideal factors $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ of $p\mathscr{O}_K$ are *principal.* The condition that the unramified prime p be split in K is exactly that $\mathrm{disc}(K/\mathbf{Q}) = -20$ is a square modulo p, or in other words $-5 \equiv \square \bmod p$. So now we have identified the real difficulty: given that this congruence condition holds, how do we distinguish whether or not the prime ideal factors of $p\mathscr{O}_K$ are actually principal? This is where knowledge of the class group saves the day.

As we noted above (and will be proved in a later lecture), the class group of $\mathbf{Q}(\sqrt{-5})$ has order 2 and is generated by $\mathfrak{p}_2$. Hence, *exactly* one of two possibilities happens when $p\mathscr{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ is split: either $\mathfrak{p}$ is principal (this is exactly when $p = x^2 + 5y^2$ with $x, y \in \mathbf{Z}$, with $\mathfrak{p} = (x \pm y\sqrt{-5})$) or $\mathfrak{p}\mathfrak{p}_2$ is principal. Consider the consequences in this second case, as follows. In such cases we have

$$(2p) = \mathfrak{p}_2^2\mathfrak{p}\overline{\mathfrak{p}} = (\mathfrak{p}\mathfrak{p}_2) \cdot \overline{\mathfrak{p}\mathfrak{p}_2}$$

since $\overline{\mathfrak{p}_2} = \mathfrak{p}_2$ (as $\mathfrak{p}_2$ is the *unique* prime ideal factor of (2)), and if $x' + y'\sqrt{-5}$ is a generator of the principal ideal $\mathfrak{p}\mathfrak{p}_2$ then this says $(2p) = ({x'}^2 + 5{y'}^2)$ as principal ideals of $\mathscr{O}_K$, so $2p = {x'}^2 + 5{y'}^2$ in $\mathbf{Z}$! Observe that, conversely, if $p \neq 2$ and $2p = {x'}^2 + 5{y'}^2$ for some $x', y' \in \mathbf{Z}$ then -5 is still a square modulo p (as y' cannot be divisible by p, since otherwise p would also have to divide x' and hence p^2 would divide ${x'}^2 + 5{y'}^2 = 2p$, a contradiction since $p \neq 2$).

The two cases $p = x^2 + 5y^2$ and $2p = {x'}^2 + 5{y'}^2$ cannot both occur for $p \neq 2, 5$. Indeed, if they did then it would say that $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ for a *principal* prime ideal $\mathfrak{p} \neq \overline{\mathfrak{p}} \neq \mathfrak{p}_2$ and likewise that the ideal $(2p) = \mathfrak{p}_2^2\mathfrak{p}\overline{\mathfrak{p}}$ would have to have the form $\mathfrak{a}\overline{\mathfrak{a}}$ for some principal ideal $\mathfrak{a}$. In such a situation, the only possibilities for the prime ideal factorization of $\mathfrak{a}$ are $\mathfrak{p}\mathfrak{p}_2$ or $\overline{\mathfrak{p}}\mathfrak{p}_2$. But both of these possibilities lead to a contradiction, as the *non-principal* fractional ideal $\mathfrak{p}_2$ for $\mathscr{O}_K$ would have to equal one of the two fractional ideals $\mathfrak{p}^{-1}\mathfrak{a}$ or $\overline{\mathfrak{p}}^{-1}\mathfrak{a}$ which are each principal by inspection (due to the principality of both $\mathfrak{p}$ and $\mathfrak{a}$).

3. The cubic curve $y^2 = x^3 - 51$

We now prove that the equation $y^2 = x^3 - 51$ has no $\mathbf{Z}$-solutions. This is interesting for two reasons: (i) it has a $\mathbf{Q}$-solution, such as $(1375/9, 50986/27)$ (and infinitely many more), and (ii) it has solutions modulo m for all $m > 1$. Point (ii) shows that this problem cannot be fruitfully analyzed by congruential methods alone, and point (i) shows that we must make essential use of integrality in our analysis.

To argue by contradiction, suppose that there exist $x, y \in \mathbf{Z}$ such that $y^2 = x^3 - 51 = x^2 - 3 \cdot 17$. We first make some elementary congruential observations. Necessarily x is odd, as otherwise -51 would be a square modulo 8, which it is not (as $-51 \equiv 5 \bmod 8$). Likewise, $\gcd(y, 51) = 1$ since otherwise y would be divisible by 3 or 17 and hence likewise for $x^3 = y^2 + 51$, so x^3 and y^2 are both divisible by p^2 with $p \in \{3, 17\}$, contradicting that $51 = x^3 - y^2$ is not divisible by p^2 (as 51 is even squarefree).

For $\alpha = (1 + \sqrt{-51})/2$ (which has minimal polynomial $t^2 - t + 13$ over $\mathbf{Q}$) we have

$$x^3 = y^2 + 51 = (y - \sqrt{-51})(y + \sqrt{-51}) = (y - (2\alpha - 1))(y + (2\alpha - 1))$$

in the ring of integers $\mathbf{Z}[\alpha]$ of $K = \mathbf{Q}(\sqrt{-51})$. I claim that the principal ideals $(y + \sqrt{-51})$ and $(y - \sqrt{-51})$ in $\mathbf{Z}[\alpha] = \mathscr{O}_K$ are relatively prime. Suppose to the contrary, so they share a common prime factor $\mathfrak{p}$. That is, there is a maximal ideal $\mathfrak{p}$ of $\mathscr{O}_K$ which contains $y+\sqrt{-51}$ and $y-\sqrt{-51}$, so it contains their difference $2\sqrt{-51}$. Hence, $\mathfrak{p}|(2)(\sqrt{-51})$, so either $\mathfrak{p}|(2)$ or $\mathfrak{p}|(\sqrt{-51})$. But in $\mathscr{O}_K = \mathbf{Z}[\alpha] \simeq \mathbf{Z}[t]/(t^2-t+13)$ the ideal (2) is prime (as $t^2-t+13 \bmod 2$ is irreducible in $\mathbf{F}_2[t]$), so the possibility $\mathfrak{p}|(2)$ says exactly that $\mathfrak{p}=(2)$, but this is not possible since the ideal $\mathfrak{p}$ contains $(y+\sqrt{-51})(y-\sqrt{-51}) = y^2+51 = x^3$ with $x^3 \in \mathbf{Z}$ an odd integer (so the containment $2 \in \mathfrak{p}$ would force $\mathfrak{p}$ to contain $\gcd_{\mathbf{Z}}(x^3, 2) = 1$, a contradiction). The other possibility is that $\mathfrak{p}|(\sqrt{-51})$, but in that case we'd have $\sqrt{-51} \in \mathfrak{p}$ (so $51 \in \mathfrak{p}$), yet $y+\sqrt{-51} \in \mathfrak{p}$ so necessarily $y \in \mathfrak{p}$. This is again an absurdity because $\gcd_{\mathbf{Z}}(y, 51) = 1$ and $1 \notin \mathfrak{p}$.

Now that we have proved that $(y+\sqrt{-51})$ and $(y-\sqrt{-51})$ are share no common prime ideal factors in $\mathscr{O}_K = \mathbf{Z}[\alpha]$, the condition that their product is the cube ideal $(x)^3$ forces each of these two given principal ideals to have their prime factors all occurring with multiplicity divisible by 3. (Here we use uniqueness of prime factorization in ideals!) Hence, we'd have $(y+\sqrt{-51}) = \mathfrak{a}^3$ and $(y-\sqrt{-51}) = \mathfrak{b}^3$ for some nonzero ideals $\mathfrak{a}, \mathfrak{b} \in \mathscr{O}_K$. Are these ideals principal? Here is where class numbers save the day: one can show (as you will on Homework 9) that $\mathbf{Q}(\sqrt{-51})$ has class number 2. Hence, the class group for $\mathbf{Q}(\sqrt{-51})$ is a 2-torsion group, so any fractional ideal whose mth power is principal with an odd m must itself be principal! (We are applying to the class group the general fact that if an element of a finite group is killed by an integer coprime to the order of the group then it must be the trivial element.) Taking $m=3$, we deduce the crucial fact that $\mathfrak{a} = (a)$ and $\mathfrak{b} = (b)$, or in other words $y+\sqrt{-51} = ua^3$ and $y-\sqrt{-51} = vb^3$ for some $u, v \in \mathscr{O}_K^\times$ and some $a, b \in \mathscr{O}_K$. It is "as if" $\mathscr{O}_K$ were a UFD!

The unit group $\mathscr{O}_K^\times$ is $\{\pm 1\}$ since K is imaginary quadratic distinct from $\mathbf{Q}(i)$ and $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$, so units are cubes and hence $y+\sqrt{-51}$ is itself a cube in $\mathscr{O}_K = \mathbf{Z}[\alpha]$. Thus, there exist integers r, s such that

$$(y-1)+2\alpha = y+\sqrt{-51} = (r+s\alpha)^3 = (r^3-39rs^2-13s^3)+3s(r^2+rs-4s^2)\alpha$$

(using the relation $\alpha^2-\alpha+13=0$). The key point is not the explicit formula on the right side, but just that the coefficient of α lies in $3\mathbf{Z}$. Since the α-coefficient on the left side is 2, we have a contradiction