THE MORDELL EQUATION

PETE L. CLARK

1. The coprime powers trick in $\mathbb{Z}$

We have by now seen several ways in which the fundamental theorem of arithmetic can be used to solve Diophantine equations, and that suitably generalized, these techniques often apply to more general unique factorization domains.

We will now consider another such technique, the **coprime powers trick**. In the interest of linear exposition, we present the technique first and then give an application. However, the reader might prefer to skip ahead and see how it is used.

Proposition 1. *(Coprime Powers Trick, v. 1)*
Let $n \in \mathbb{Z}^+$, let $x, y, z \in \mathbb{Z}$ be such that $\gcd(x, y) = 1$ and $xy = z^n$.
a) There exist $a, b \in \mathbb{Z}$ such that $x = \pm a^n,\ y = \pm b^n$.
b) If n is odd, then there exist $a, b \in \mathbb{Z}$ such that $x = a^n,\ y = b^n$.

Proof. If $x, y \in \mathbb{Z}$, then $x = \pm y$ iff $\mathrm{ord}_p(x) = \mathrm{ord}_p(y)$ for all prime numbers p. We exploit this as follows: for any prime p, take ord_p of both sides of $xy = z^n$ to get

$$\mathrm{ord}_p(x) + \mathrm{ord}_p(y) = n\,\mathrm{ord}_p(z).$$

Since x and y are relatively prime, at least one of $\mathrm{ord}_p(x),\ ord_p(y)$ is equal to 0, and therefore they are both divisible by n. Now define $a, b \in \mathbb{Z}^+$ as follows:

$$a = \prod_p p^{\frac{\mathrm{ord}_p(x)}{n}},\ b = \prod_p p^{\frac{\mathrm{ord}_p(y)}{n}}.$$

Then for all primes p, $\mathrm{ord}_p(a^n) = n\,\mathrm{ord}_p(a) = \mathrm{ord}_p(x)$ and $\mathrm{ord}_p(b^n) = n\,\mathrm{ord}_p(b) = \mathrm{ord}_p(y)$. We conclude $x = \pm a^n$, $y = \pm b^n$, establishing part a). Part b) follows upon noticing that if n is odd, $(-1)^n = -1$, so we may write $x = (\pm a)^n$, $y = (\pm b)^n$. □

1.1. An application.

Theorem 2. *The only integral solutions to*

$$y^2 - y = x^3 \tag{1}$$

are $(0, 0)$ and $(0, 1)$.

Proof. Suppose $(x, y) \in \mathbb{Z}^2$ satisfy equation (1), i.e., $y(y-1) = x^3$. As for any two consecutive integers, y and $y - 1$ are relatively prime. We can therefore apply Proposition 1b) to conclude that there exist $a, b \in \mathbb{Z}$ such that

$$y = a^3,\ y - 1 = b^3.$$

This gives

$$1 = y - (y-1) = a^3 - b^3 = (a-b)(a^2 + ab + b^2),$$

Thanks to Keith Conrad for pointing out a simplfication in the proof of Theorem 3.

and the only way this can happen is for

$$a - b = a^2 + ab + b^2 = \pm 1.$$

Suppose first that $a - b = 1$, so $b = a - 1$; then

$$1 = a^2 + ab + b^2 = a^2 + a(a-1) + (a-1)^2 = 3a^2 - 3a + 1,$$

or

$$3a^2 - 3a = 0.$$

The solutions of this quadratic are $a = 0$ and $a = 1$. If $a = 0$, then $y = a^3 = 0$, and $x^3 = 0^2 - 0 = 0$: we get the solution $(x, y) = (0, 0)$ to (1). If $a = 1$, then $y = 1$ and $x^3 = 1^2 - 1 = 0$: we get the solution $(x, y) = (0, 1)$.
Next suppose that $a - b = -1$, so $b = a + 1$; then

$$-1 = a^2 + ab + b^2 = a^2 + a(a+1) + (a+1)^2 = 3a^2 + 3a + 1,$$

or

$$3a^2 + 3a + 2 = 0,$$

a quadratic equation with discriminant $3^2 - 4 \cdot 3 \cdot 2 = -13 < 0$; thus there are no real solutions. □

2. The Mordell Equation

We now turn to a family of Diophantine equations which has received persistent attention over the centuries and remains of interest to this day. Namely, fix an integer k and consider

$$y^2 + k = x^3. \tag{2}$$

We wish to find all integral solutions. If $k = 0$ we get the "degenerate" equation $y^2 = x^3$. A moment's thought shows that this equation has solution set $\{(x, y) = (a^2, a^3) \mid a \in \mathbb{N}\}$. In particular there are infinitely many solutions. The great Philadelphian mathematician Louis J. Mordell showed that conversely, for each nonzero k, (2) has only finitely many integer solutions. Because of this and other results over the course of his long career, (2) is often called the **Mordell Equation**, despite the fact that other distinguished mathematicians also worked on it. In particular, the case of $k = -2$ was considered by Claude-Gaspar Bachet and Fermat in the seventeenth century, and the following result is attributed to Fermat.

Theorem 3. *(Fermat) The only integral solutions to*

$$y^2 + 2 = x^3 \tag{3}$$

are $(3, 5)$ *and* $(3, -5)$.

Proof. We wish to argue similarly to the previous result, but here the only factorization in sight takes place over the quadratic ring $\mathbb{Z}[\sqrt{-2}]$, namely:

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Looking back at the previous argument, it seems that what we would like to say is that there are elements $\alpha = a + b\sqrt{-2}, \beta = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ such that

$$y + \sqrt{-2} = \alpha^3, \ y - \sqrt{-2} = \beta^3.$$

The justification for this will be a version of the coprime powers trick in the ring $\mathbb{Z}[\sqrt{-2}]$, but let us assume it just for a moment and see what comes of it.

By expanding out α^3 we get

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2},$$

and this means that

$$y = a^3 - 6ab^2 = a(a^3 - 6b^2),$$
$$1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2).$$

Again this very much limits our options: we must have

$$b = 3a^2 - 2b^2 = 1$$

or

$$b = 3a^2 - 2b^2 = -1.$$

Taking the first option – $b = 1$ – gives $3a^2 = 2b^2 + 1 = 3$, so $a = \pm 1$. Taking $(a, b) = (1, 1)$ leads to $y = 1(1^3 - 6 \cdot 1^2) = -5$, so $x^3 = y^2 + 2 = 5^2 + 2 = 27$, so $x = 3$: we get the solution $(x, y) = (3, 5)$. Taking $(a, b) = (-1, 1)$ leads to $y = -1((-1)^3 - 6 \cdot 1^2) = 7$, so $x^3 = y^2 + 2 = 7^2 + 2 = 51$, which has no integral solutions since 51 is not a perfect cube.

The second option – $b = -1$ – gives $3a^2 = 2b^2 + 1 = 3$, so again $a = \pm 1$. Taking $(a, b) = (1, -1)$ leads to $y = 1(1^3 - 6 \cdot (-1)^2) = -5$, and as above we get $x = 3$ and the solution $(x, y) = (3, -5)$. Taking $(a, b) = (-1, -1)$ leads to $y = -1((-1)^3 - 6 \cdot (-1)^2) = 7$, which as above yields no solution. □

The time has come to justify our assumption that there exist elements α, β as above. The justification is in two parts: first, we need a version of the coprime powers trick that applies to the domain $\mathbb{Z}[\sqrt{-2}]$; and second we need to verify that the hypotheses are justified in our particular case: in particular, that the elements $y \pm \sqrt{-2}$ of $\mathbb{Z}[\sqrt{-2}]$ are indeed coprime!

3. The coprime powers trick in a UFD

3.1. **ord functions and coprime powers.** Let R be a UFD and $x, y \in R$. We say that x, y are **coprime** if $z \mid x$, $\mid z \mid y$ implies $z \in R^\times$. Equivalently, x and y are coprime if there is not prime element which divides both of them.

Proposition 4. *(Coprime powers trick, v. 2) Let R be a UFD, $n \in \mathbb{Z}^+$, and let $x, y, z \in R$ be coprime elements such that $xy = z^n$.*
a) There exist $\alpha, \beta \in R$ and units $u, v \in R^\times$ such that

$$x = u\alpha^n, \ y = v\beta^n.$$

b) If every unit in R is an nth power, then there exist $\alpha, \beta \in R$ such that

$$x = \alpha^n, y = \beta^n.$$

In other words, if in a UFD the product of two relatively prime elements is a perfect nth power, then each of them is a perfect nth power, up to a unit.

Before giving the proof, we set up a more general notion of "ord functions". We work in the context of an integral domain R which satisfies the ascending chain condition on principal ideals (ACCP). In plainer terms we assume that there is no

infinite sequence $\{x_i\}_{i=1}^{\infty}$ of elements of R such that x_{i+1} properly divides[1] x_i for all i. This is a very mild condition: it is satisfied by any Noetherian ring and by any UFD: c.f. [Factorization in Integral Domains].

Now let π be a nonzero prime element of R, and let $x \in R \setminus \{0\}$. The condition (ACCP) ensures that there exists a largest non-negative integer n such that $\pi^n \mid x$, for otherwise $\pi^n \mid x$ for all n and $\{\frac{x}{\pi^n}\}$ is an infinite sequence in which each element properly divides the previous one. We put $\mathrm{ord}_\pi(x)$ to be this largest integer n. In other words, $\mathrm{ord}_\pi(x) = n$ iff $\pi^n \mid x$ and $\pi^{n+1} \nmid x$. We formally set $\mathrm{ord}_\pi(0) = +\infty$, and we extend ord_π to a function on the fraction field K of R by multiplicativity:

$$\mathrm{ord}_\pi\left(\frac{x}{y}\right) := \mathrm{ord}_\pi(x) - \mathrm{ord}_\pi(y).$$

This generalizes the functions ord_p on $\mathbb{Z}$ and $\mathbb{Q}$, and the same properties hold.

Proposition 5. *Let R be an (ACCP) domain with fraction field K. Let π be a nonzero prime element of R and $x, y \in K \setminus \{0\}$. Then:*
a) $\mathrm{ord}_\pi(xy) = \mathrm{ord}_\pi(x) + \mathrm{ord}_\pi(y)$.
b) $\mathrm{ord}_\pi(x+y) \geq \min(\mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y))$.
c) Equality holds in part b) if $\mathrm{ord}_\pi(x) \neq \mathrm{ord}_\pi(y)$.

Proof. We will suppose for simplicity that $x, y \in R \setminus \{0\}$. The general case follows by clearing denominators as usual. Put $a = \mathrm{ord}_\pi(x)$, $b = \mathrm{ord}_\pi(y)$. By hypothesis, there exists x', y' such that $x = \pi^a x'$, $y = \pi^b y'$ and $\pi \nmid x', y'$.
a) $xy = \pi^{a+b}(x'y')$. Thus $\mathrm{ord}_\pi(xy) \geq a + b$. Conversely, suppose that $\pi^{a+b+1} \mid xy$. Then $\pi \mid x'y'$, and, since π is a prime element, this implis $\pi \mid x'$ or $\pi \mid y'$, contradiction. Thus $\mathrm{ord}_\pi(xy) = a + b = \mathrm{ord}_\pi(x) + \mathrm{ord}_\pi(y)$.
b) Let $c = \min a, b$, so $x + y = \pi^c(\pi^{a-c}x' + \pi^{b-c}y'$, and thus $\pi^c \mid x + y$ and $\mathrm{ord}_\pi(x+y) \geq c = \min(\mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y))$.
c) Suppose without loss of generality that $a < b$, and write $x + y = \pi^a(x' + \pi^{b-a}y')$. If $\pi^{a+1} \mid x + y = \pi^a x' + \pi^b y'$, then $\pi \mid x' + \pi^{b-a}y'$. Since $b - a > 0$, we have $\pi \mid (x' + \pi^{b-a}y') - (\pi^{b-a}y') = x'$, contradiction. □

Suppose that π and π' are associate nonzero prime elements, i.e., there exists a unit $u \in R$ such that $\pi' = u\pi$. Then a moment's thought shows that the ord functions ord_π and $\mathrm{ord}_{\pi'}$ coincide. This means that ord_π depends only on the principal ideal $\mathfrak{p} = (\pi)$ that the prime element π generates. We could therefore redefine the ord function as $\mathrm{ord}_\mathfrak{p}$ for a nonzero principal prime ideal $\mathfrak{p} = (\pi)$ of R, but for our purposes it is convenient to just choose one generator π of each such ideal $\mathfrak{p}$. Let $\mathcal{P}$ be a maximal set of mutually nonassociate nonzero prime elements, i.e., such that each nonzero prime ideal $\mathfrak{p}$ contains exactly one element of $\mathcal{P}$.

Now suppose that R is a UFD, and $x \in R \setminus \{0\}$ is an element such that $\mathrm{ord}_\pi(x) = 0$ for all $\pi \in \mathcal{P}$. Then x is not divisible by any irreducible elements, so is necessarily a unit. In fact the same holds for elements $x \in K \setminus \{0\}$, since we can express $x = \frac{a}{b}$ with a and b not both divisible by any prime element. (In other words, in a UFD we can reduce fractions to lowest terms!) It follows that any $x \in K \setminus \{0\}$ is determined

[1]We say that a properly divides b if $a \mid b$ but a is not associate to b.

up to a unit by the integers $\mathrm{ord}_\pi(x)$ as π ranges over elements of $\mathcal{P}$. Indeed, put

$$y = \prod_{\pi \in \mathcal{P}} \pi^{\mathrm{ord}_\pi x}.$$

Then we have $\mathrm{ord}_\pi(\frac{x}{y}) = 0$ for all $\pi \in \mathcal{P}$, so that $\frac{x}{y} = u$ is a unit in R, and $x = yu$.

After these preparations, the proof of Proposition 4 is straightforward: we have $xy = z^n$. For any prime element p, take ord_p of both sides to get

$$\mathrm{ord}_p(x) + \mathrm{ord}_p(y) = n\,\mathrm{ord}_p(z).$$

But since x and y are assumed coprime, for any fixed prime p, we have either $\mathrm{ord}_p(x) = 0$ or $\mathrm{ord}_p(y) = 0$. Either way we get that $n \mid \mathrm{ord}_p(x)$ and $n \mid \mathrm{ord}_p(y)$ (since $n \mid 0$ for all n). So the following are well-defined elements of R:

$$x' = \prod_{p \in \mathcal{P}} p^{\frac{\mathrm{ord}_p(x)}{n}},$$

$$y' = \prod_{p \in \mathcal{P}} p^{\frac{\mathrm{ord}_p(y)}{n}},$$

where the product extends over a maximal set of pairwise nonassociate nonzero prime elements of R. By construction, we have $\mathrm{ord}_p((x')^n) = n\,\mathrm{ord}_p(x') = n\frac{\mathrm{ord}_p(x)}{n} = \mathrm{ord}_p(x)$ for all $p \in \mathcal{P}$, so the elements x and $(x')^n$ are associate: i.e., there exists a unit u in R such that $x = u(x')^n$. Exactly the same applies to y and y': there exists a unit $v \in R$ such that $y = v(y')^n$.

3.2. **Application to the Bachet-Fermat Equation.**

To complete the proof of Theorem 3 we need to verify that the hypotheses of Proposition 4b) apply: namely, that every unit in $\mathbb{Z}[\sqrt{-2}]$ is a cube and that the elements $y + \sqrt{-2}$, $y - \sqrt{-2}$ are indeed relatively prime. For the former, we are fortunate in that, as for $\mathbb{Z}$, the only units in $R = \mathbb{Z}[\sqrt{-2}]$ are ± 1, both of which are indeed cubes in R.

For the latter, we suppose that $d \in R$ is a common divisor of $y + \sqrt{-2}$ and $y - \sqrt{-2}$. Then also $d \mid (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$, i.e., there exists $d' \in R$ with $dd' = 2\sqrt{-2}$. Taking norms of both sides we get

$$N(d)N(d') = N(2\sqrt{-2}) = 8,$$

so $N(d) \mid 8$. Moreover, there exists $\alpha \in R$ such that $d\alpha = y + \sqrt{-2}$, hence

$$N(d)N(\alpha) = N(d\alpha) = N(y + \sqrt{2}) = y^2 + 2 = x^3,$$

so $N(d) \mid x^3$. We claim that x must be odd. For if not, then reducing the equation $x^3 = y^2 + 2 \bmod 8$ gives $y^2 \equiv 6 \pmod 8$, but the only squares mod 8 are $0, 1, 4$. Thus x^3 is odd and $N(d) \mid \gcd(x^3, 8) = 1$ so $d = \pm 1$ is a unit in R.

3.3. **Application to the Mordell Equation with $k = 1$.**

Theorem 6. *The only integer solution to $y^2 + 1 = x^3$ is $(1, 0)$.*

Proof: This time we factor the left hand side over the UFD $R = \mathbb{Z}[\sqrt{-1}]$:

$$(y + \sqrt{-1})(y - \sqrt{-1}) = x^3.$$

If a nonunit d in R divides both $y+\sqrt{-1}$ and $y-\sqrt{-1}$, then it divides $(y+\sqrt{-1})-(y-\sqrt{-1}) = 2\sqrt{-1} = (1+\sqrt{-1})^2\sqrt{-1}$. The element $1+\sqrt{-1}$, having norm $N(1+\sqrt{-1}) = 2$ a prime number, must be an irreducible (hence prime) element of R. So $1+i$ is the only possible common prime divisor. We compute

$$\frac{y \pm \sqrt{-1}}{1+\sqrt{-1}} \cdot \frac{1-\sqrt{-1}}{1-\sqrt{-1}} = \frac{y \pm 1 + (y \pm 1)\sqrt{-1}}{2},$$

which is an element of R iff y is odd. But consider the equation $y^2+1 = x^3$ modulo 4: if y is odd, then $y^2+1 \equiv 2 \pmod 4$, but 2 is not a cube modulo 4. Therefore we must have that y is even, so that $y \pm \sqrt{-1}$ are indeed coprime. Moreover, although the unit group of R is slightly larger in this case – it is $\{\pm 1, \pm\sqrt{-1}\}$ – it is easily checked that every unit is a cube in R. So Proposition 4b) applies here, giving $\alpha, \beta \in R$ such that

$$y + \sqrt{-1} = \alpha^3, \ y - \sqrt{-1} = \beta^3.$$

Again we will put $\alpha = a + b\sqrt{-1}$ and expand out α^3, getting

$$y + \sqrt{-1} = a^3 - 3b^2a + (3a^2b - b^3)\sqrt{-1},$$

or

$$y = a(a^2 - 3b^2), \ 1 = b(3a^2 - b^2).$$

So we have either $1 = b = 3a^2 - b^2$, which leads to $3a^2 = 2$, which has no integral solution, or $-1 = b = 3a^2 - b^2$, which leads to $a = 0$, so $\alpha = -\sqrt{-1}$, $y = (-\sqrt{-1})^3 - \sqrt{-1} = 0$, $x = 1$ and thus to $(x, y) = (1, 0)$.

4. Beyond UFDs

The situation here is somewhat analogous to our study of the equations $x^2+Dy = p$, where the assumption that he quadratic ring $\mathbb{Z}[\sqrt{-D}]$ is a UFD leads to a complete solution of the problem. However there are also some differences. First, whereas in the present situation we are using the assumption that $\mathbb{Z}[\sqrt{-k}]$ is a UFD in order to show that $y^2 + k = x^3$ has very few solutions, earlier we used the assumption that $\mathbb{Z}[\sqrt{-D}]$ is a UFD to show that the family of equations $x^2 + Dy^2 = p$ had many solutions, namely for all primes p for which $-D$ is a square mod p.

A more significant difference is that the assumption $\mathbb{Z}[\sqrt{-D}]$ was necessary as well as sufficient for our argument to go through: we saw that whenever $D < -3$ 2 is not of the form x^2+Dy^2. On the other hand, suppose $\mathbb{Z}[\sqrt{-k}]$ is not a UFD: must the coprime powers trick fail? It is not obvious, so let us study it more carefully.

We would like to axiomatize the coprime powers trick. There is an agreed upon definition of coprimality of two elements x and y in a general domain R: if $d \mid x$ and $d \mid y$ then d is a unit. However it turns out to be convenient to require a stronger property than this, namely that the ideal $\langle x, y\rangle = \{rx + sy \mid r, s \in R\}$ generated by x and y be the unit ideal R. More generally, for two ideals I, J of a ring, the sum $I + J = \{i + j \mid i \in I, j \in J\}$ is an ideal, and we say that I and J are **comaximal** if $I + J = R$; equivalently, the only ideal which contains both I and J is the "improper" ideal R. Since every proper ideal in a ring is contained in a maximal, hence prime, ideal, the comaximality can be further reexpressed as the property that there is no prime ideal $\mathfrak{p}$ containing both I and J. (This will be the formulation which is most convenient for our application.)

Notice that the condition that x and y be coprime can be rephrased as saying

that the only *principal* ideal (d) containing both x and y is the improper ideal $R = (1)$. So the notions of coprime and comaximal elements coincide in a principal domain, but not in general.

Now, for a positive positive integer n, say that an integral domain R has property **CM(n)** if the comaximal powers trick is valid in degree n: namely, for all $x, y, z \in R$ with $\langle x, y\rangle = R$ and $xy = z^n$, then there exist elements $a, b \in R$ and units $u, v \in R$ such that $x = ua^n$, $y = vb^n$. Exactly as above, if we also have $(R^\times)^n = (R^\times)$ – i.e., every unit in R is an nth power – then the units u and v can be omitted. Now consider the following

Theorem 7. *Let $k \in \mathbb{Z}^+$ be squarefree with $k \equiv 1, 2 \pmod 4$. Suppose that the ring $\mathbb{Z}[\sqrt{-k}]$ has property CM(3). Then:*
a) If there exists an integer a such that $k = 3a^2 \pm 1$, then the only integer solutions to the Mordell equation $y^2 + k = x^3$ are $(a^2 + k, \pm a(a^2 - 3k))$.
b) If there is no integer a as in part a), the Mordell equation $y^2 + k = x^3$ has no integral solutions.

Proof. Suppose (x, y) is an integral solution to $y^2 + k = x^3$. Reduction mod 4 shows that x is odd. Also $\gcd(k, x) = 1$: otherwise there exists a prime p dividing both k and x, so $p \mid x^3 - k = y^2$ and $p \mid y^2 \implies p^2 \mid x^3 - y^2 = k$, contradicting the squarefreeness of k. Now consider

$$(y + \sqrt{-k})(y - \sqrt{-k}) = x^3.$$

We wish to show that $\langle y + \sqrt{-k}, y - \sqrt{-k}\rangle = R$. If not, there exists a prime ideal $\mathfrak{p}$ of R with $y \pm \sqrt{-k} \in \mathfrak{p}$. Then $(y + \sqrt{-k}) - (y - \sqrt{-k}) = 2\sqrt{-k} \in \mathfrak{p}$, hence also $-(2\sqrt{-k})^2 = 4k \in \mathfrak{p}$. Moreover $\mathfrak{p}$ contains $y^2 + k = x^3$ and since it is prime, it contains x. But since x is odd and $\gcd(x, k) = 1$, also $\gcd(x, 4k) = 1$, so that there exist $m, n \in \mathbb{Z}$ with $1 = xm + 4kn$ and thus $1 \in \mathfrak{p}$. Moreover, either $k = 1$ (a case which we have already treated) or $k > 1$ and the only units of $\mathbb{Z}[\sqrt{-k}]$ are ± 1. Therefore there exists $\alpha = a + b\sqrt{-k} \in R$ such that

$$y + \sqrt{-k} = \alpha^3 = (a + b\sqrt{-k})^3 = a(a^2 - 3kb^2) + b(3a^2 - kb^2)\sqrt{-k}.$$

So $b = \pm 1$ and $k = db^2 = 3a^2 \pm 1$. The integer a determined by this equation is unique up to sign. So $y = \pm a(a^2 - 3k)$, and one easily computes $x = a^2 + k$. □

Since property CM(3) holds in the PIDs $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$, whatever else Theorem 7 may be good for, it immediately implies Theorems 3 and 6. Moreover its proof was shorter than the proofs of either of these theorems! The economy was gained by consideration of not necessarily principal ideals.

Thus, if for a given k as in the statement of Theorem 7 we can find more solutions to the Mordell Equation than the ones enumerated in the conclusion of the theorem we know that $\mathbb{Z}[\sqrt{-k}]$ does not satisfy property CM(3). In the following examples we simply made a brute force search over all x and y with $|x| \leq 10^6$. (There is, of course, no guarantee that we will find *all* solutions this way!)

Example: The equation $y^2 + 26 = x^3$ has solutions $(x, y) = (3, \pm 1),\ (35, \pm 207)$, so $\mathbb{Z}[\sqrt{-26}]$ does not have property CM(3).

Example: The equation $y^2 + 53 = x^3$ has solutions $(x, y) = (9, \pm 26),\ (29, \pm 156)$, so $\mathbb{Z}[\sqrt{-53}]$ does not have CM(3).

Example: The equation $y^2 + 109 = x^3$ has solutions $(x, y) = (5, \pm 4),\ (145, \pm 1746)$. Note that the latter solutions are already impractical to find by hand, so it is easier to observe that 5 is not of the form $a^2 + 109$, $\mathbb{Z}[\sqrt{-109}]$, so by Theorem 7, $\mathbb{Z}[\sqrt{-109}]$ does not have property CM(3).

In fact, whether a ring $\mathbb{Z}[\sqrt{-k}]$ (here we keep the assumptions on k of Theorem 7, so in particular $\mathbb{Z}[\sqrt{-k}]$ is the full ring of algebraic integers of the quadratic field $\mathbb{Q}(\sqrt{-k})$; this would not be the case if $k \equiv 3 \pmod 4$) has property CM(k) can be determined algorithmically. It depends on an all-important numerical invariant called the **class number** of $\mathbb{Z}[\sqrt{-k}]$.

For any integral domain R, we can define an equivalence relation on the nonzero ideals of R. Namely, we decree that $I \sim J$ iff there exist $a, b \in R \setminus \{0\}$ such that $(a)I = (b)J$. Roughly speaking, we regard two ideals as being principal if and only if they differ multiplicatively from a principal ideal. When there are only finitely many equivalence classes, we define the **class number** of R to be the number of equivalence classes.[2] For example, if every ideal of R is principal, then the class number is equal to 1. Conversely, if the class number of R is equal to 1 and I is any nonzero ideal of R, then there exist a, b such that $aI = bR$. Then $b = b \cdot 1 \in aI$, so for some $x \in I$, $ax = b$. In particular $a \mid b$, and it is then easy to see that $I = (\frac{b}{a})R$. Thus the domains with class number one are precisely the principal ideal domains.

Now let K be a number field, and let $\mathbb{Z}_K$ be the ring of all algebraic integers in K. In particular this includes $\mathbb{Z}[\sqrt{-k}]$ for k as above.

Theorem 8. *Let K be a field and $\mathbb{Z}_K$ be the ring of algebraic integers in K. Then:*
a) There are only finitely many equivalence classes of ideals of $\mathbb{Z}_K$, so there is a well-defined class number, denoted $h(K)$.
b) The ring $\mathbb{Z}_K$ is a PID iff it is a UFD iff $h(K) = 1$.
c) Let $n \in \mathbb{Z}^+$. If $\gcd(n, h(K)) = 1$, then $\mathbb{Z}_K$ has property CM(n).

At several points in this course we have flirted with crossing the border into the land of algebraic number theory, but that no such passport is required is one of our ground rules. Because of this it is simply not possible to prove Theorem 8 here. We can only say that the study of such properties of the ring $\mathbb{Z}_K$ is a central topic in the classical theory of algebraic numbers.

Moreover, algorithms for computing the class number have been a very active part of algebraic number theory for more than one hundred years. Such algorithms are available – indeed, they have been implemented in many software packages – the question is only of the speed and memory needed to do the job. The case of (imaginary) quadratic fields is especially classical and relates to (positive definite) binary quadratic forms. So the following table of class numbers of $\mathbb{Q}(\sqrt{-k})$ for squarefree

[2] As we have stated it, the definition makes sense for arbitrary domains and is equivalent to the usual definition for number rings $\mathbb{Z}_K$. For more general domains – and even some quadratic rings – there is another (less elementary) definition which is more useful.

k, $1 \leq k \leq 200$ is more than two hundred years old:

$h(\mathbb{Q}(\sqrt{-k})) =$

1 for $k = 1, 2, 3, 7, 11, 19, 43, 67, 163$
2 for $k = 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187$
3 for $k = 23, 31, 59, 83, 107, 139$
4 for $k = 14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97, 102, 130,$
$133, 142, 155, 177, 190, 193, 195$
5 for $k = 47, 79, 103, 127, 131, 179$
6 for $k = 26, 29, 38, 53, 61, 87, 106, 109, 118, 157$
7 for $k = 71, 151$
8 for $k = 41, 62, 65, 66, 69, 77, 94, 98, 105, 113, 114, 137, 138, 141, 145, 154, 158, 165, 178$
9 for $k = 199$
10 for $k = 74, 86, 122, 166, 181, 197$ 11 for $k = 167$
12 for $k = 89, 110, 129, 170, 174, 182, 186$
13 for $k = 191$
14 for $k = 101, 134, 149, 173$
16 for $k = 146, 161, 185$
20 for $k = 194$

So Theorem 7 applies to give a complete solution to the Mordell equation $y^2+k = x^3$ for the following values of k:

$$1, 2, 5, 6, 10, 13, 14, 17, 21, 22, 30, 33, 34, 37, 41, 42, 46, 57, 58, 62, 65, 69, 70, 73, 74, 77, 78,$$
$$82, 85, 86, 93, 94, 97, 98, 101, 102, 106, 113, 114, 122, 130, 133, 134, 137, 138,$$
$$141, 142, 145, 146, 149, 154, 158, 161, 165, 166, 177, 178, 181, 185, 190, 193, 194, 197.$$

Example: The equation $y^2+47 = x^3$ has solutions $(x, y) = (6, \pm 13),\ (12, \pm 41), (63, \pm 500)$. On the other hand $\mathbb{Z}[\sqrt{-47}]$ has class number 5 so does have property CM(3). Note that $47 \equiv 3 \pmod 4$.

Example: $\mathbb{Z}[\sqrt{-29}]$ has class number 6, but nevertheless $y^2 + 29 = x^3$ has no integral solutions.[3] Thus there is (much) more to this story than the coprime powers trick. For more details, we can do no better than recommend Chapter 26 of L.J. Mordell's *Diophantine Equations*.

5. Remarks and Acknowledgements

Our first inspiration for this material was a short expository note by Keith Conrad:

`http://www.math.uconn.edu/~kconrad/blurbs/ringtheory/ufdapp.pdf`

Therein he proves Theorems 2 and 3 as an application of unique factorization in $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-2}]$. Many more examples of successful (and one unsuccessful!) solution of Mordell's equation for various values of k are given at

[3]How do we know? For instance, we can look it up on the internet:
`http://www.research.att.com/~njas/sequences/A054504`

http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/mordelleqn1.pdf

A range of techniques are showcased here, including the coprime powers trick but also: elementary (but somewhat intricate) congruence arguments and applications of quadratic reciprocity.

Also useful for us were lecture notes of P. Stevenhagen:

http://websites.math.leidenuniv.nl/algebra/ant.pdf

Stevenhagen's treatment is analogous our discussion of quadratic rings. In particular, he first proves Theorem 6. He then assumes that $\mathbb{Z}[\sqrt{-19}]$ satisfies CM(3) and deduces that $y^2 + 19 = x^3$ has no integral solutions; finally he points out $(x, y) = (18, 7)$. We did not discuss this example in the text because it depends critically on the fact that $\mathbb{Z}[\sqrt{-19}]$ is not the full ring of integers in $K = \mathbb{Q}(\sqrt{-19})$: rather $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. For rings like $\mathbb{Z}[\sqrt{-19}]$ the definition we gave of the class number is not the correct one: we should count only equivalence classes of **invertible ideals** – i.e., nonzero ideals I for which there exists J such that IJ is principal. In this amended sense the class number of $\mathbb{Z}[\sqrt{-19}]$ is 3.

Theorem 7 was taken from the classic text of Ireland and Rosen.

A generalization of Theorem 7 appears in §5.3 of lecture notes of Franz Lemmermeyer:

http://www.fen.bilkent.edu.tr/∼franz/ant/ant1-7.pdf

Lemmermeyer finds all integer solutions to the equation $y^2 + k = x^3$ whenever $3 \nmid h(\mathbb{Q}(\sqrt{-k}))$ and $k \not\equiv 7 \pmod 8$. Again we have avoided this case so as not to have to deal with the case where $\mathbb{Z}[\sqrt{-k}]$is not the full ring of integers.

It is interesting to look at the work which has been done on the Mordell equation since Mordell's death in 1972. In 1973, London and Finkelstein found all solutions to Mordell's equation for $|k| \leq 10^2$. The current state of the art is another story entirely: a 1998 paper of Gebel, Pethö and Zimmer solves the Mordell equation for $|k| \leq 10^4$ and for about 90% of integers k with $|k| \leq 10^5$.