We now begin the more systematic investigation of equations of
degree two and three.\footnote{For degree one, see the material on linear Diophantine equations in [NZM].}

**The equation** $x^2 + y^2 = z^2$ (*Pythagorean triples*). First note that from any solution we get infinitely many by $(kx, ky, kz)$, $k \in \mathbb{Z}$.

**Definition 1.** A triple $(a, b, c) \in \mathbb{Z}^3$ is **primitive** if $\gcd(a, b, c) = 1$, and **Pythagorean** if $a^2 + b^2 = c^2$.

We shall now find all primitive Pythagorean triples. First, we cannot have $a, b, c \equiv 0 \pmod{2}$ (since the gcd is 1); and so $a$ and $b$ cannot both be even (otherwise, $c$ would be). If $a$ and $b$ were both odd, then $a^2 + b^2 \equiv 1 + 1 = 2$; but $c^2 \equiv 2$ is impossible! Without loss of generality we can therefore assume $a$ even and $b$ odd, hence $c$ odd.

Next, put $a = 2n$, and note that $a^2 = c^2 - b^2 = (c - b)(c + b)$. \footnote{For degree one, see the material on linear Diophantine equations in [NZM].}

Put $c - b = 2v$, $c + b = 2w$; we then have

$$(2n)^2 = 2v \cdot 2w$$

hence

$$n^2 = vw$$

where $n, v, w \neq 0$. If a prime $g \mid v, w$, then $g$ divides $w - v = b$ and $w + v = c$, which gives $g \mid a$, a contradiction. Therefore $(v, w) = 1$.

But if $v$ and $w$ have no common prime factors, the Fundamental Theorem of Arithmetic (unique factorization in $\mathbb{Z}$) together with equation (1) imply $v = r^2$ and $w = s^2$. We conclude that $b = w - v = s^2 - r^2$, $c = w + v = s^2 + r^2$, and $a^2 = 4n^2 = 4vw = 4r^2s^2 = (2rs)^2$.
\[ \Rightarrow \quad a = 2rs. \] Conversely, we can check that each such triple is Pythagorean (try it!), proving the

**Theorem 2.** The complete list of primitive Pythagorean triples is

\[
\left\{ (2rs, s^2 - r^2, s^2 + r^2) \mid r, s \in \mathbb{Z} \setminus \{0\}; \ (r, s) = 1; \ r, s \text{ not both odd} \right\}.
\]

(To get all Pythagorean triples, change the conditions on \( r, s \) to just \( r, s \in \mathbb{Z} \).)

**Remark 3.** It is easy to see that \( (r, s) = 1 \Rightarrow \) no odd prime factor of \( r \) can divide \( s^2 - r^2 \) or \( s^2 + r^2 \). But what about 2? 2 divides 2rs, and will divide \( s^2 \pm r^2 \Leftrightarrow s \) and \( r \) are both even or both odd. If \( (r, s) = 1 \) they can’t both be even.

**Example 4.** \( r = 40 \) and \( s = 81 \) give \( (a, b, c) = (6480, 4961, 8161) \). So \( 4961^2 + 6480^2 = 8161^2 \) (apparently written down by the Babylonians!).

The equation \( c^2 - b^2 = n \). We shall seek, for given \( n \) (e.g. \( a^2 \) in the Pythagorean equation), the number of solutions to this one.

**Definition 5.** \( \sigma_k(n) := \sum_{d|n} d^k \) (for \( n \in \mathbb{N} \)), so in particular \( \sigma_0(n) \) is the number of positive divisors of \( n \).

The table

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sigma_0(n) )</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

suggests

**Lemma 6.** \( \sigma_0(n) \) odd \( \iff \) \( n \) is a square.

**Proof.** Factors come in pairs \( d \) and \( \frac{n}{d} \), unless (when \( d = \sqrt{n} \)) \( n \) is a square. \( \square \)

**Lemma 7.** \( \sigma_0(p^m) = m + 1 \).

**Proof.** Since this is obvious, I’ll prove that a cow has nine legs instead. A cow has four more legs than no cow. No cow has five legs. Done. \( \square \)
Lemma 8. \( \sigma_0 \) is multiplicative: \((m, n) = 1 \implies \sigma_0(mn) = \sigma_0(m)\sigma_0(n)\).

Proof. The divisors of \( mn \) are \( de \) where \( d \mid m \) and \( e \mid n \). In fact, the correspondence between such pairs \((d, e)\) and divisors of \( mn \) is bijective: for if \((d', e')\) is another such pair, and \( d'e' = de \), then \((m, n) = 1 \implies (e', d) = 1 = (e, d') \implies d' = d \) and \( e' = e \).

So if we write \( n = \prod p_i^{m_i} \) as a product of powers of distinct primes, then

\[
\sigma_0(n) = \prod_i (m_i + 1).
\]

Now suppose \((x, y)\) is a solution to our equation, with \( x, y > 0 \). Put \( d = x + y, e = x - y \), so that \( de = n \). Since \( d + e = 2x, d \equiv e \) (2); and since \( d - e = 2y > 0, d > e \). Hence

\[
(x, y) \in \mathcal{S} := \left\{ \left( \frac{d+e}{2}, \frac{d-e}{2} \right) \middle| d > e > 0, de = n, d \equiv e \right\},
\]

and conversely each element of \( \mathcal{S} \) provides a solution.

Theorem 9. The number of elements in \( \mathcal{S} \) is

\[
|\mathcal{S}| = \begin{cases} 
\frac{1}{2} \sigma_0(n) & \text{if } n \text{ odd nonsquare}, \\
\frac{\sigma_0(n)-1}{2} & \text{if } n \text{ odd square}, \\
\frac{1}{2} \sigma_0\left(\frac{n}{4}\right) & \text{if } n \text{ even nonsquare (div. by 4)}, \\
\frac{\sigma_0\left(\frac{n}{4}\right)-1}{2} & \text{if } n \text{ even square (div. by 4)}. 
\end{cases}
\]

If \( n \) is even but \( 4 \nmid n \), then \(|\mathcal{S}| = 0\).

Proof. \((n \text{ odd})\) If \( de = n \), then \( d \equiv e \) (2) is automatic. Furthermore, \( d \) determines \( e \). So \(|\mathcal{S}| \) is the number of divisors of \( n \) with \( d > \frac{n}{\sqrt{d}} \), i.e. \( d > \sqrt{n} \). Of course, \( e \) is in each case \( \frac{n}{d} \), and if \( n \) is a square then we miss out on \( d = \sqrt{n} = e \).

\((n \text{ even})\) If \( de = n \), then one (hence both) of \( d \) and \( e \) must be even. So \( 4 \mid n \) (otherwise there is no solution, and \(|\mathcal{S}| = 0\)). In this case, \( d = 2d', e = 2e' \) and \( d'e' = \frac{n}{4} \); \( \mathcal{S} \) identifies with

\[
\left\{ (d' + e', d' - e') \mid d'e' = \frac{n}{4}, d' > e' > 0 \right\}.
\]

The remainder of the proof is the same as for \( n \text{ odd} \). \( \square \)
Pell’s equation. Let \( d \in \mathbb{N} \) be squarefree, and consider

\[
x^2 - y^2d = \begin{cases} 
\pm 1 & \text{if } d \equiv 2,3 \pmod{4} \\
\pm 4 & \text{if } d \equiv 1 \pmod{4} 
\end{cases}
\]

This equation is closely related to the quadratic number field \( K = \mathbb{Q}[\sqrt{d}] \) with ring of integers

\[
\mathcal{O}_K := \begin{cases} 
\mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod{4} \\
\mathbb{Z} \left[ \frac{1+\sqrt{d}}{2} \right] & \text{if } d \equiv 1 \pmod{4} 
\end{cases}
\]

The units \( \mathcal{O}_K^* \subset \mathcal{O}_K \) are simply the elements which are invertible in \( \mathcal{O}_K \). We claim the following:

**Theorem 10.** For \( d \equiv 2,3 \pmod{4} \) (resp. \( 1 \)), the units \( \mathcal{O}_K^* \) are exactly the numbers \( x + y\sqrt{d} \) (resp. \( \frac{x+y\sqrt{d}}{2} \)) such that \( x, y \) are integers satisfying Pell’s equation (2).

**Proof.** Assume \( d \equiv 2,3 \pmod{4} \), so that the left-hand side of (2) is the norm

\[
N_K(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) \text{ for } K = \mathbb{Q}[\sqrt{d}].
\]

We may view the norm as a homomorphism

\[
N_K : \mathcal{O}_K \setminus \{0\} \to \mathbb{Z} \setminus \{0\}
\]

of multiplicative monoids (i.e. \( N_K(\alpha \beta) = N_K(\alpha)N_K(\beta) \)).

If \( \alpha = x + y\sqrt{d} \in \mathcal{O}_K^* \), then there exists \( \beta \in \mathcal{O}_K \) with \( \alpha \beta = 1 \)

\[
\implies 1 = N_K(1) = N_K(\alpha \beta) = N_K(\alpha)N_K(\beta)
\]

with both \( N_K(\alpha), N_K(\beta) \in \mathbb{Z} \). Hence \( N_K(\alpha) = \pm 1 \) and \( (x, y) \) satisfies Pell.

---

2The notation \( \mathbb{Z}[\mu] \) (resp. \( \mathbb{Q}[\mu] \)) means in general the ring of polynomials in \( \mu \) with integer (resp. rational) coefficients, but here \( \alpha \) satisfies a quadratic equation \( \mu^2 = d \) or \( \mu^2 = \mu + b \) (\( b \in \mathbb{Z} \) resp. \( \mathbb{Q} \)), so every “polynomial” is equal to a unique expression of the form \( a + b\mu \), with \( a, b \in \mathbb{Z} \) (resp. \( \mathbb{Q} \)). That is, for our purposes here, \( \mathbb{Z}[\mu] = \{ a + b\mu \mid a, b \in \mathbb{Z} \} \).
Conversely, if $N_K(\alpha) = \pm 1$ for some $\alpha = x + y\sqrt{d} \in \mathcal{O}_K$, then (writing $\tilde{\alpha} = x - y\sqrt{d}$) $a\tilde{\alpha} = \pm 1 \implies \alpha(\pm\tilde{\alpha}) = 1 \implies \alpha$ invertible in $\mathcal{O}_K \implies \alpha \in \mathcal{O}_K^*$.

For the case $d \equiv 1 \pmod{4}$, one just has to write $\alpha = \frac{x + y\sqrt{d}}{2}$ so that $4N_K(\alpha) = x^2 - y^2d$, and Pell again is equivalent to $N_K(\alpha) = \pm 1$. □

Powers of units are units, and it turns out that there exists a “fundamental unit” $u = x_1 + y_1\sqrt{d}$ (to be proved in §IV.C) such that

$$\mathcal{O}_K^* = \left\{ \pm u^\ell \mid \ell \in \mathbb{Z} \right\}.$$ 

Let’s apply this to $d = 5$, for which $\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right]$ and

$$\varphi = \frac{1 + \sqrt{5}}{2}$$

— the golden ratio, which satisfies $1 + \varphi = \varphi^2$ — is our $u$. Writing as above $x + y\sqrt{d} := x - y\sqrt{d}$, and defining $(x_n, y_n) \in \mathbb{Z}^2$ by

$$\varphi^n = \frac{x_n + y_n\sqrt{d}}{2},$$

we have

$$x_n = \varphi^n + \bar{\varphi}^n, \quad y_n = \frac{\varphi^n - \bar{\varphi}^n}{\sqrt{5}}.$$

Since each $\varphi^n \in \mathcal{O}_K^*$, by Theorem 10 each $(x_n, y_n)$ solves the equation

(3) $x^2 - 5y^2 = \pm 4$.

Now $y_0 = 0, y_1 = 1$, and (using $1 + \varphi = \varphi^2, 1 + \bar{\varphi} = \bar{\varphi}^2$)

$$y_{n-2} + y_{n-1} = \frac{\varphi^{n-2} - \bar{\varphi}^{n-2} + \varphi^{n-1} - \bar{\varphi}^{n-1}}{\sqrt{5}}$$

$$= \frac{\varphi^{n-2}(1 + \varphi) - \bar{\varphi}^{n-2}(1 + \bar{\varphi})}{\sqrt{5}}$$

$$= \frac{\varphi^n - \bar{\varphi}^n}{\sqrt{5}}$$

$$= y_n.$$
Therefore the \( \{y_n\} \) are the **Fibonacci numbers**, and the \((\pm x_n, \pm y_n)\) give the complete solutions of (2), which is not just a set but a group (namely \( O^*_Q(\sqrt{5}) \)) of the form [i.e. isomorphic to] \( \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \).