Ex Equations like \( y^2 = x^3 + 7 \) are called “elliptic curves”. They arise in solving integrals for, say, the period of a body in a planetary orbit.

(Lebesgue, 1869) The equation \( y^2 = x^3 + 7 \) is insoluble over \( \mathbb{Z} \).

Proof. If \( x \) is even, \( x = 2\alpha \Rightarrow \) RHS = \( 8\alpha^3 + 7 = 8\beta + 7 \), where \( \beta = \alpha^3 \). But \( 0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1, 4^2 \equiv 0, 5^2 \equiv 1, 6^2 \equiv 4 \) and \( 7^2 \equiv 1 \) (mod 8) so \( y^2 \equiv 7 \) (mod 8) has no solution. Hence \( x \) is odd. Write

\[
\begin{align*}
y^2 + 1 &= x^3 + 8 \\
&= (x + 2)(x^2 - 2x + 4) \\
&= (x + 2)((x - 1)^2 + 3)
\end{align*}
\]

If \( x = 2n + 1 \) (odd) then \( (x - 1)^2 + 3 = 4n^2 + 3 = 4m + 3 \), \( m = n^2 \) so (see back) must have a prime factor of the form \( p = 4\ell + 3 \). But then \( y^2 + 1 \equiv qp \equiv 0 \) (mod \( p \)) But (lemma later) \( p \equiv 3 \) (mod 4) \Rightarrow \( y^2 \equiv -1 \) (mod \( p \)) has no solution. \( \square \)

We frequently need to know the answer to the following: When does \( x^2 \equiv r \) (mod \( p \)) have a solution \( x \)? Or, more generally, \( x^2 \equiv \alpha \) (mod \( m \)). The answer is given by the theory of quadratic reciprocity due to Gauss. This will be developed later.
6 Pell’s Equation

\[ x^2 - Ny^2 = 1 \]

Trivial solution \( x = 1, \ y = 0, \ x, y \geq 0. \)

\( N = -1 \Rightarrow (x, y) = (1, 0) \) or \( (0, 1) \) are trivial solutions only.

\( N \leq -2 \Rightarrow (x, y) = (1, 0). \)

Let \( N > 0 \) and not a square: If \( N = M^2, \ x^2 - Ny^2 = x^2 - (My)^2 = (x - My)(x + My) = 1 \Rightarrow x - My = 1 \) and \( x + My = 1 \) so we can get all solutions. Indeed \( (x, y) = (1, 0) \) for \( x, y \geq 0. \)

**Note:** Solutions to Pell’s equation provide good *rational approximations* for square roots, since \( x^2 = Ny^2 + 1 \)

\[ \Rightarrow \left( \frac{x}{y} \right)^2 = N + \frac{1}{y^2} \]

\[ \Rightarrow \frac{x}{y} \approx \sqrt{N} \] if \( y \) is large.

**Note:** This type of equation has a long and interesting history, and has lots of applications, especially to fields \( F = \mathbb{Q}(\sqrt{N}) \).

**Ex** (Euler, 1770) A *triangular number* has the form \( \frac{n(n+1)}{2} \). Which numbers are both triangular and square?

\( m^2 = n(n + 1)/2 \)

\[ \Rightarrow 8m^2 + 1 = 4n^2 + 4n + 1 = (2n + 1)^2 \]

\[ \Rightarrow x^2 - 2y^2 = 1 \] where \( x = 2n + 1, \ y = 2m. \)

So solutions to this Pellian equation produce (all) square triangular numbers.

**Definition** A *fundamental solution* to \( x^2 - dy^2 = 1 \) is \( (r, s) \) where any other positive solution satisfies \( r < x \) and \( s < y. \)

**Theorem 21 (Lagrange)** Let \( (r, s) \) be the least positive (or fundamental) solution to \( x^2 - dy^2 = 1, \) where \( d \) is not a square. Then every solution to this equation is given by \( (x_n, y_n) \) where

\[ x_n + \sqrt{d}y_n = (r + s\sqrt{d})^n \]

for \( n = 1, 2, 3, \ldots \)

**Proof.**

\[ x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) \]

\[ = (r + s\sqrt{d})^n(r - s\sqrt{d})^n \]

\[ = (r^2 - s^2d)^n = 1^n = 1 \]
Hence \((x_n, y_n)\) is a solution.

Let \((a, b)\) be a solution. Suppose \(\forall n = 1, 2, 3, \ldots, (a, b) \neq (x_n, y_n)\). Then there is a positive integer \(m\) with

\[
(r + s\sqrt{d})^m < a + b\sqrt{d} < (r + s\sqrt{d})^{m+1}
\]

(17)

But \((r + s\sqrt{d})^{-m} = (r - s\sqrt{d})^m\) so \((??) \Rightarrow \)

\[
1 < (a + b\sqrt{d})(r - s\sqrt{d})^m < (r + s\sqrt{d})
\]

(18)

Let \(u + v\sqrt{d} = (a + b\sqrt{d})(r - s\sqrt{d})^m\) so

\[
\begin{align*}
    u^2 - v^2d &= (u + v\sqrt{d})(u - v\sqrt{d}) \\
    &= (a + b\sqrt{d})(r - s\sqrt{d})^m(a - b\sqrt{d})(r + s\sqrt{d})^m \\
    &= (a^2 - b^2d)(r^2 - s^2d)^m = 1 \cdot 1^m = 1
\end{align*}
\]

Thus \((u, v)\) is a solution.

But \(1 < u + v\sqrt{d} \Rightarrow 0 < u - v\sqrt{d} < 1\) so

\[
2u = (u + v\sqrt{d}) + (u - v\sqrt{d}) > 1 + 0 > 0
\]

And \(2v\sqrt{d} = (u + v\sqrt{d}) - (u - v\sqrt{d}) > 1 - 1 = 0\) so \(u > 0, v > 0\) and \(u + v\sqrt{d} < r + s\sqrt{d}\) by \((??)\), contradiction the assumption that \((r, s)\) is the fundamental solution. Hence \((a, b) = (x_n, y_n)\) for some \(n\). □

Finding the least positive solution is not easy however and requires the theory of continued fractions of J. L. Lagrange. Frenicle’s table for non-square \(d\) up to 50 is given below.
Pell's equation

Euler, after a cursory reading of Wallis's *Opera Mathematica*, mistakenly attributed the first serious study of nontrivial solutions to equations of the form \( x^2 - dy^2 = 1 \), where \( x \neq 1 \) and \( y \neq 0 \), to Cromwell's mathematician John Pell. However, there is no evidence that Pell, who taught at the University of Amsterdam, had ever considered solving such equations. They would be more aptly called Fermat's equations, since Fermat first investigated properties of nontrivial solutions of each equations. Nevertheless, Pellian equations have a long history and can be traced back to the Greeks. Theon of Smyrna used \( x/y \) to approximate \( \sqrt{2} \), where \( x \) and \( y \) were integral solutions to \( x^2 - 2y^2 = 1 \). In general, if \( x^2 = dy^2 + 1 \), then \( x^2/y^2 = d + 1/y^2 \). Hence, for \( y \) large, \( x/y \) is a good approximation of \( \sqrt{d} \), a fact well known to Archimedes.

Archimedes's *problema bovinum* took two thousand years to solve. According to a manuscript discovered in the Wolfenbüttel library in 1773 by Gotthold Ephraim Lessing, the German critic and dramatist, Archimedes became upset with Apollonius of Perga for criticizing one of his works. He devised a cattle problem that would involve immense calculation to solve and sent it off to Apollonius. In the accompanying correspondence, Archimedes asked Apollonius to compute, if he thought he was smart enough, the number of the oxen of the sun that grazed once upon the plains of the Sicilian isle Trinacria and that were divided according to color into four herds, one milk white, one black, one yellow and one dappled, with the following constraints:

- white bulls = yellow bulls + \( \left( \frac{1}{2} + \frac{1}{3} \right) \) black bulls,
- black bulls = yellow bulls + \( \left( \frac{1}{4} + \frac{1}{5} \right) \) dappled bulls,
- dappled bulls = yellow bulls + \( \left( \frac{1}{6} + \frac{1}{7} \right) \) white bulls,
- white cows = \( \left( \frac{1}{3} + \frac{1}{4} \right) \) black herd,
- black cows = \( \frac{1}{4} + \frac{1}{5} \) dappled herd,
- dappled cows = \( \frac{1}{5} + \frac{1}{6} \) yellow herd, and
- yellow cows = \( \frac{1}{6} + \frac{1}{7} \) white herd.

Archimedes added, if you find this number, you are pretty good at numbers, but do not pat yourself on the back too quickly for there are two more conditions, namely:

- white bulls plus black bulls is square and
dappled bulls plus yellow bulls is triangular.

Archimedes concluded, if you solve the whole problem then you may 'go forth as conqueror and rest assured that thou art proved most skillful in the science of numbers'.

The smallest herd satisfying the first seven conditions in eight unknowns, after some simplifications, lead to the Pellian equation \( x^2 - 4729494 y^2 = 1 \). The least positive solution, for which \( y \) has 41 digits, was discovered by Carl Amthov in 1880. His solution implies that the number of white bulls has over 2 \( \times \) 10^5 digits. The problem becomes much more difficult when the eighth and ninth conditions are added and the first complete solution was given in 1965 by H.C. Williams, R.A. German, and C.R. Zarnke of the University of Waterloo.
Baudhayana noted that \( x = 577 \) and \( y = 408 \) is a solution of \( x^2 - 2y^2 = 1 \) and used the fraction \( \frac{577}{408} \) to approximate \( \sqrt{2} \). In the seventh century Brahmagupta considered solutions to the Pellian equation \( x^2 - 92y^2 = 1 \), the smallest solution being \( x = 1151 \) and \( y = 120 \). In the twelfth century the Hindu mathematician Bhaskara found the least positive solution to the Pellian equation \( x^2 - 61y^2 = 1 \) to be \( x = 226,153,980 \) and \( y = 1766,319,049 \).

In 1657, Fermat stated without proof that if \( d \) was positive and nonsquare, then Pell's equation had an infinite number of solutions. For if \((x, y)\) is a solution to \( x^2 - dy^2 = 1 \), then \( 1^2 = (x^2 - dy^2)^2 = (x^2 + dy^2)^2 - (2xy)^2 \). Thus, \((x^2 + dy^2, 2xy)\) is also a solution to \( x^2 - dy^2 = 1 \). Therefore, if Pell's equation has a solution, it has infinitely many.

In 1657 Fermat challenged William Brouncker, of Castle Lynn in Ireland, and John Wallis to find integral solutions to the equations \( x^2 - 151y^2 = 1 \) and \( x^2 - 313y^2 = 1 \). He cautioned them not to submit rational solutions for even 'the lowest type of arithmetician' could devise such answers. Wallis replied with \((1728, 1480, 140, 634, 693)\) as a solution to the first equation. Brouncker replied with \((126, 862, 368, 7170, 685)\) as a solution to the second. Lord Brouncker claimed that it only took him about an hour or two to find his answer. Samuel Pepys, secretary of the Royal Society, had a low opinion of Brouncker's moral character but thought that his mathematical ability was quite adequate. In the section on continued fractions, in this chapter, we will demonstrate the method Wallis and Brouncker used to generate their answers.

<table>
<thead>
<tr>
<th>(d)</th>
<th>(x)</th>
<th>(y)</th>
<th>(d)</th>
<th>(x)</th>
<th>(y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>26</td>
<td>51</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>27</td>
<td>26</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>28</td>
<td>127</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>29</td>
<td>9801</td>
<td>1820</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>4</td>
<td>30</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>2</td>
<td>31</td>
<td>1520</td>
<td>273</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>3</td>
<td>32</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>1</td>
<td>33</td>
<td>23</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>34</td>
<td>35</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
<td>6</td>
<td>35</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>3</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>7</td>
<td>2</td>
<td>37</td>
<td>73</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>649</td>
<td>180</td>
<td>38</td>
<td>37</td>
<td>6</td>
</tr>
<tr>
<td>14</td>
<td>15</td>
<td>4</td>
<td>39</td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>1</td>
<td>40</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td>41</td>
<td>2049</td>
<td>320</td>
</tr>
<tr>
<td>17</td>
<td>33</td>
<td>8</td>
<td>42</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>17</td>
<td>4</td>
<td>43</td>
<td>3482</td>
<td>531</td>
</tr>
<tr>
<td>19</td>
<td>170</td>
<td>39</td>
<td>44</td>
<td>199</td>
<td>30</td>
</tr>
<tr>
<td>20</td>
<td>9</td>
<td>2</td>
<td>45</td>
<td>161</td>
<td>24</td>
</tr>
<tr>
<td>21</td>
<td>55</td>
<td>12</td>
<td>46</td>
<td>24335</td>
<td>3588</td>
</tr>
<tr>
<td>22</td>
<td>197</td>
<td>42</td>
<td>47</td>
<td>48</td>
<td>7</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
<td>5</td>
<td>48</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>24</td>
<td>5</td>
<td>1</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td>50</td>
<td>99</td>
<td>14</td>
</tr>
</tbody>
</table>
7 Continued Fractions

Ex

\[
1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}} = 1 + \frac{1}{2 + \frac{1}{13/4}}
\]
\[
= 1 + \frac{1}{2 + \frac{4}{13}}
\]
\[
= 1 + \frac{1}{30/13}
\]
\[
= 1 + \frac{13}{30}
\]
\[
= \frac{43}{30}
\]

looks silly until we consider some interesting continued fraction expansions

\[\pi: [3, 7, 25, 2, 393, \ldots] \text{ i.e.} \]
\[3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{293 + \ldots}}} \]

\[e: [2, 1, 2, 1, 4, 1, 6, 1, 1, \ldots] \]
\[\sqrt{2}: [1, 2, 2, 2, 2, \ldots] \]
\[\sqrt{3}: [1, 1, 2, 1, 2, 1, 2, 1, 2, \ldots] \]
\[\sqrt{5}: [2, 4, 4, 4, \ldots] \]
\[\sqrt{n^2 + 1}: [n, 2n, 2n, \ldots] \text{ (Euler)} \]

**Definition** By a simple continued fraction (or C.F.) we mean an expression

\[
a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}} = [a_0, a_1, a_2, \ldots]
\]

where \(a_0 \in \mathbb{Z}\) and \(a_i \in \mathbb{N}\) for \(i \geq 1\).

**Note:** \([a_0] = a_0, [a_0, a_1] = \frac{a_0a_1 + 1}{a_1} \]
\([a_0, a_1, a_2] = \frac{a_2a_1a_0 + a_2 + a_0}{a_2a_1 + 1}\)

Generally, \([a_0, \ldots, a_n] = \frac{p_n}{q_n} \] where \(p_n\) and \(q_n\) are polynomials in the \(a_i\), linear in any given \(a_j\), and \(a_0\) does not occur in the denominator \(q_n\). \((p_n, q_n)\) are called the \(n^{\text{th}}\) convergents.

**Note:** \([a_0, \ldots, a_n] = [a_0, \ldots, a_{n-1}, \frac{1}{a_n}]\)

**Proposition** If \([a_0, \ldots, a_m] = [b_0, \ldots, b_n]\), \(a_i, b_i \in \mathbb{N}, a_m, b_n > 1 \) then \(m = n\) and \(a_i = b_i \forall i\).
Proof. This follows by induction from

\[ [a_0, \ldots, a_m] = a_0 + \frac{1}{[a_1, \ldots, a_m]} = b_0 + \frac{1}{b_1, \ldots, b_n} \]

if we can show \([a_1, \ldots, a_m] > 1\) when \(a_1, \ldots, a_m > 1\). But this is so since

\[ [a_1, \ldots, a_m] = a_1 + \frac{1}{a_2 + \ldots} \]

Let \(a_i > 0\) and \(\forall n\) let \(\tau_n = [a_0, \ldots, a_n]\) then \(\tau_n\) can be computed using the recursive formulas

\[
\begin{align*}
p_0 &= a_0 & p_1 &= a_0a_1 + 1 & p_n &= a_np_{n-1} + p_{n-2} \\
q_0 &= 1 & q_1 &= a_1 & q_n &= a_nq_{n-1} + q_{n-2}
\end{align*}
\]

so \(\tau_0 = \frac{p_0}{q_0}\), \(\tau_1 = \frac{p_1}{q_1}\) and \(\tau_n = \frac{p_n}{q_n}\).

Proof.

\[ \tau_n = [a_0, \ldots, a_n] = [a_0, \ldots, a_{n-1} + \frac{1}{a_n}] = \frac{p'_{n-1}}{q'_{n-1}} \]

where these belong to \(a_0, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\) i.e. (induction)

\[
\frac{p'_{n-1}}{q'_{n-1}} = \frac{(a_{n-1} + \frac{1}{a_n})p_{n-2} + p_{n-3}}{(a_{n-1} + \frac{1}{a_n})q_{n-2} + q_{n-3}} = \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} \]

(induction again!)

Hence \(p_n = a_np_{n-1} + p_{n-2}\) and \(q_n = a_nq_{n-1} + q_{n-2}\) \(\Box\)

\((p_n, q_n)\) are called the \(n^{th}\) convergents of the C.F.

Let \(\theta \in \mathbb{R} \setminus \mathbb{Z}, \theta > 1\). \(a_0 = \lfloor \theta \rfloor\) so \(\theta = a_0 + \frac{1}{\theta_1}\). \(\theta_1 > 1\) defines \(\theta_1\). Continue with \(\theta_1 = a_1 + \frac{1}{\theta_2}\) so \(a_1 = \lfloor \theta_1 \rfloor\), \(\theta_2 > 1\) if \(\theta_1 \notin \mathbb{Z}\) etc \(\theta_n = a_n + \frac{1}{\theta_{n+1}}\), \(a_n = \lfloor \theta_n \rfloor\), \(\theta_{n+1} > 1\) if \(\theta_n \notin \mathbb{Z}\). We get

\[
\theta = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots + \frac{1}{a_n + \frac{1}{\theta_{n+1}}}}}}
\]

so \(\theta = [a_0, a_1, \ldots, a_n + \frac{1}{\theta_{n+1}}]\)

**Proposition** The expansion stops if \(\theta_n = a_n\) is in \(\mathbb{N}\) and then \(\theta \in \mathbb{Q}^+\) i.e. is a positive rational number. Conversely, if \(\theta \in \mathbb{Q}^+\), the C.F. expansion is finite.
Proof. Let \( \theta = \frac{u}{v} \in \mathbb{Q}^+ \), \( u, v \in \mathbb{N} \). Use division

\[
\begin{align*}
    u &= a_0v + r_1 & 0 < r_1 < v \\
    v &= a_1r_1 + r_2 & 0 < r_2 < r_1 \\
    r_1 &= a_2r_2 + r_3 & 0 < r_3 < r_2 \\
    &\vdots \\
    r_{n-1} &= a_nr_n + 0
\end{align*}
\]

as if we were doing the Euclidean algorithm. These equations give

\[
\begin{align*}
    \theta &= \frac{u}{v} = a_0 + \frac{r_1}{v} = a_0 + \frac{1}{v.a_1} = a_0 + \frac{1}{\theta_1} \\
    \theta_1 &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{r_1/r_2} = a_1 + \frac{1}{\theta_2} \\
    &\vdots \\
    \theta_n &= \frac{r_{n-1}}{r_n} \in \mathbb{N}
\end{align*}
\]

so the C.F. expansion is finite. \( \Box \)

**Proposition** \( \forall n \geq 2 \)
\[
\theta = \frac{\theta_np_{n-1} + p_{n-2}}{\theta_nq_{n-1} + q_{n-2}}
\]

*Proof.* The definition of \( \theta_n \) is \( \theta = [a_0, \ldots, a_{n-1}, \theta_n] \) so \( \theta = \frac{p_n}{q_n} = \frac{\theta_np_{n-1} + p_{n-2}}{\theta_nq_{n-1} + q_{n-2}} \) using \( a_n \) and \( \theta_n \) for this particular C.F. \( \Box \)

**Ex** \( \sqrt{2} = [1, 2, 2, \ldots] \)

\[
(\sqrt{2} - 1)(\sqrt{2} + 1) = 2 - 1 = 1 \Rightarrow \sqrt{2} - 1 = \frac{1}{1+\sqrt{2}} \text{ so } \sqrt{2} = 1 + \frac{1}{1+\sqrt{2}}.
\]

We now copy the expression for \( \sqrt{2} \) in the RHS into the \( \sqrt{2} \) on the RHS successively (photocopy model for recursion).

\[
\sqrt{2} = 1 + \frac{1}{1 + \frac{1}{1+\sqrt{2}}} = 1 + \frac{1}{2 + \frac{1}{1+\sqrt{2}}} = 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{1+\sqrt{2}}}}
\]

etc. leading to \( \sqrt{2} = [1, 2, 2, 2, \ldots, 2, 1 + \sqrt{2}] \). If we continue indefinitely we obtain \( \sqrt{2} = [1, 2, 2, \ldots] = [1, 2] \).

Every quadratic irrational has a periodic continued fraction—this characterises quadratic irrationals.
$\sqrt{2} = [1, 2, \ldots, 2, 1 + \sqrt{2}]$ so $a_0 = 1$, $a_1 = 2, \ldots$

\[
\begin{align*}
p_0 &= a_0 = 1 \\
q_0 &= 1 \\
\tau_0 &= \frac{p_0}{q_0} = \frac{1}{1} = 1
\end{align*}
\]

\[
\begin{align*}
p_1 &= a_0a_1 + 1 = 3 \\
q_1 &= a_1 = 2 \\
\tau_1 &= \frac{p_1}{q_1} = \frac{3}{2} = 1.5
\end{align*}
\]

\[
\begin{align*}
p_2 &= a_2p_1 + p_0 = 7 \\
q_2 &= a_2q_1 + q_0 = 5 \\
\tau_2 &= \frac{p_2}{q_2} = \frac{7}{5} = 1.4
\end{align*}
\]

and the approximation $\tau_n \approx \sqrt{2}$ gets better.

**Theorem 22** Let $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$, $i \geq 1$. Then $(\tau_n)$ converges to an irrational number $\theta$. The $a_i$ are uniquely determined by the C.F. expansion of $\theta$. Conversely, if $\theta$ is an irrational number, and $\tau_n = [a_0, \ldots, a_n]$ are obtained by expanding $\theta$ as a C.F. then

$$\theta = \lim_{n \to \infty} \tau_n.$$ 

**Proof.** The sequences $(p_n)$ and $(q_n)$ are both strictly monotonically increasing sequences of natural numbers.
Claim:
\[ p_n q_{n-1} = p_{n-1} q_n = (-1)^{n-1} \quad (19) \]
∀\( n \geq 1 \). If \( n = 1 \) this is \( p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) 1 - a_0 a_1 = a = (-1)^{1-1} \) which is true. Assume it is true for \( n = m \). Then
\[
p^{m+1} q_m - p_m q_{m+1} = (a_m p_m + p_{m-1}) q_m - p_m (a_m q_m q_{m-1}) = p_{m-1} q_m - p_m q_{m-1} = - (p_m q_{m-1} - p_{m-1} q_m) = - (-1)^{m-1} = (-1)^m
\]
Hence, by induction, the claim is true ∀\( n \geq 1 \).

Divide (19) by \( q_n q_{n-1} \) to obtain
\[
\frac{p_n}{q_n} = \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}
\]
or
\[
\tau_n - \tau_{n-1} = \frac{(-1)^{n-1}}{q_n q_{n-1}}
\]
(20)
Apply this to \( \theta = [a_0, \ldots, a_{n-1}, \theta_n] \) to get
\[
\theta - \tau_n = \frac{(-1)^{n-1}}{q_{n-1}(\theta_n q_{n-1} + q_{n-2})}
\]
(21)
But \( \theta_i > 0 \) and \( q_i \to \infty \)
\[
\therefore \quad \lim_{n \to \infty} \tau_n = \theta
\]
since RHS of (19) \( \to 0 \). The proof of uniqueness is similar to that given above when \( \theta \in \mathbb{Q}^+ \). □

Aside
Numbers of the form \( \alpha + \beta \sqrt{d} \), \( d \in \mathbb{N}, \ d \neq m^2 \) are a field, \( F = \mathbb{Q}(\sqrt{d}) \), the "extension" of \( \mathbb{Q} \) by \( \sqrt{d} \):
\[
\frac{1}{\alpha + \beta \sqrt{d}} = \frac{\alpha - \beta \sqrt{d}}{\alpha^2 - \beta^2 d} = \frac{\alpha}{\alpha^2 - \beta^2 d} - \frac{\beta}{\alpha^2 - \beta^2 d} \sqrt{d} \in \{\alpha_1 + \beta_1 \sqrt{d}\}
\]

Diophantine Approximation

Equation (19) implies
\[
\left| \frac{\theta - p_n}{q_n} \right| = \frac{1}{q_n(\theta_{n+1} q_n + q_{n-1})} < \frac{1}{q_n q_{n+1}} \quad (22)
\]
The numbers \( q_0, q_1, \ldots \) are strictly increasing in \( \mathbb{N} \). The continued fraction process provides us with an infinite sequence of rational approximations to an irrational number, \( \theta \), namely the convergents \( \frac{p_n}{q_n} \in \mathbb{Q} \). How rapidly do they approach \( \theta \)?

By (??), if \( \frac{x}{y} \) is a convergent,

\[
\left| \theta - \frac{x}{y} \right| < \frac{1}{y^2}
\]

It is possible to prove that (Hurwitz, 1891) any irrational number \( \theta \) has an infinite number of rational approximations which satisfy

\[
\left| \theta - \frac{x}{y} \right| < \frac{1}{\sqrt{5}y^2} \tag{23}
\]

This is the best possible: If we choose \( \beta > \sqrt{5} \) then there are numbers \( \eta \in \mathbb{R} \setminus \mathbb{Q} \) for which there are only a finite number of rationals \( \frac{x}{y} \) with

\[
\left| \eta - \frac{x}{y} \right| < \frac{1}{\beta y^2}.
\]

e.g. the golden ratio

\[
g = 1 + \frac{1}{1 + \frac{1}{1 + \cdots}} = 1 + \frac{1}{g}
\]

so \( g^2 - g - 1 = 0 \) \( \Rightarrow \) \( g = \frac{1 + \sqrt{5}}{2} \).

Inequalities of the form (??) will be very important later when we study rational, algebraic, irrational and transcendental numbers such as \( \frac{401}{403} \), \( \frac{1+\sqrt{5}}{2} \) and \( e \) or \( \pi \).

**Quadratic Irrationals**

- solutions to *quadratic equations* with \( \mathbb{Z} \) coefficients e.g. \( x^2 - 2 = 0 \) \( \Rightarrow \) \( x = \sqrt{2} \).
- simplest type of irrational e.g. \( (\sqrt{4+7^{1/3}})^{1/5} \) is ‘more’ irrational as is \( \pi \) (see later)

**Ex** \( \theta = \frac{24 + \sqrt{15}}{17} : 3 < \sqrt{15} < 4 \) \( \Rightarrow \) \( |\theta| = 1 \) and

\[
\theta = 1 + \frac{1}{\theta_1}
\]

\[
\theta_1 = \frac{1}{\theta - 1} = \frac{17}{7 - \sqrt{15}} = \frac{7 + \sqrt{15}}{2}
\]

\[
[\theta_1] = 5
\]

\( \Rightarrow \) \( \theta_1 = 5 + \frac{1}{\theta_2} \)
\[ \theta_2 = \frac{1}{\theta_1 - 5} = \frac{2}{\sqrt{15} - 3} = \frac{\sqrt{15} + 3}{3} \]

\[ \lfloor \theta_2 \rfloor = 2 \]

\[ \Rightarrow \theta_2 = 2 + \frac{1}{\theta_3} \]

\[ \theta_3 = \frac{1}{\theta_2 - 2} = \frac{3}{\sqrt{15} - 3} = \frac{\sqrt{15} + 3}{2} \]

\[ \lfloor \theta_3 \rfloor = 3 \]

\[ \Rightarrow \theta_3 = 3 + \frac{1}{\theta_4} \]

\[ \theta_4 = \frac{1}{\theta_3 - 3} = \frac{2}{\sqrt{15} - 3} = \frac{\sqrt{15} + 3}{3} \text{ so } \theta_4 = \theta_2 \]

\[ \Rightarrow \frac{25 - \sqrt{15}}{17} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3}}}}} \]

**Ex**

\[ \sqrt{2} = [1, \frac{2}{2}] \]
\[ \sqrt{3} = [1, \frac{1}{2}] \]
\[ \sqrt{5} = [2, \frac{1}{2}] \]
\[ \sqrt{6} = [2, \frac{2}{4}] \]

H. Davenport, *The Higher Arithmetic*

**Ex** \[ \sqrt{50} = [7, \frac{14}{4}] \]
Purely periodic fractions

Ex

\[
\sqrt{2} + 1 = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}
\]

\[
\sqrt{6} + 2 = [4, 2]
\]

These numbers are easier to deal with than those with a ‘preperiod’.

Ex

\[
\alpha = 4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{3 + \ddots}}}} = [4, 1, 3, \alpha]
\]

using the equations on page 70 we get convergents \([\frac{4}{5}, \frac{5}{6}, \frac{19}{24}, \frac{5}{6}, \ldots]\).

\[
\alpha = \cfrac{19\alpha + 5}{4\alpha + 1} \Leftrightarrow \alpha = \cfrac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}
\]

Hence \(4\alpha^2 - 18\alpha - 5 = 0\) and \(\alpha\) is a quadratic irrational.

Now consider the number \(\beta\) which has the period of \(\alpha\) reversed:

\[
\beta = [3, 1, 4] \Rightarrow \beta = \cfrac{19\beta + 4}{5\beta + 1}
\]

\[
\Rightarrow 5\beta^2 - 18\beta - 4 = 0
\]

The equations are the same if \(-\frac{1}{\beta} = \alpha \Rightarrow -\frac{1}{\beta}\) is the second root of the equation for \(\alpha\) called the (algebraic) conjugate of \(\alpha\) or \(\bar{\alpha}\).

In general let \(\alpha = [a_0, \ldots, a_n, \alpha]\) be purely periodic, then

\[
\alpha = \cfrac{p_n\alpha + p_{n-1}}{q_n\alpha + q_{n-1}}
\]

Let \(\beta = [a_n, \ldots, a_0] = [a_n, \ldots, a_0, \beta]\) then (Ex)

\[
\beta = \cfrac{p_n\beta + q_n}{p_{n-1}\beta + q_{n-1}}
\]
As before $-\frac{1}{\beta}$ is the conjugate of the root $\alpha$.

**Note:** If $\beta > 1$ then $-1 < -\frac{1}{\beta} < 0$.

**Theorem 23** Any purely periodic continued fraction represents a quadratic irrational number $\alpha > 1$ with a conjugate $\overline{\alpha}$ satisfying $-1 < \overline{\alpha} < 0$. This conjugate is $\overline{\alpha} = -\frac{1}{\beta}$ where $\beta$ is defined by the C.F. of $\alpha$ with the period reversed.

**Remark** (Galois, 1828) This property characterises numbers with purely periodic continued fractions.

**Definition** A quadratic irrational $\alpha$ is reduced if $\alpha > 1$ and $-1 < \overline{\alpha} < 0$.

**Theorem 24** If $\alpha$ is reduced, its C.F. expansion is purely periodic.

**Proof.** There are integers $a, b, c$ such that $a \alpha^2 + b \alpha + c = 0$. Solving for $\alpha$:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{P \pm \sqrt{D}}{Q}$$

where $P, Q \in \mathbb{Z}$, $D \in \mathbb{N}$, $D \neq m^2$. Assume the sign is positive, else multiply by $(-1)$ so

$$\alpha = \frac{P + \sqrt{D}}{Q}$$

so $\overline{\alpha}$, the other root, is

$$\overline{\alpha} = \frac{P - \sqrt{D}}{Q}.$$ 

Note that

$$\frac{P^2 - D}{Q} = \frac{b^2 - (b^2 - 4ac)}{2ac} = 2c \Rightarrow Q | P^2 - D$$

But $1 < \alpha$ and $-1 < \overline{\alpha} < 0$ so

(i) $\alpha - \overline{\alpha} > 0 \Rightarrow \frac{\sqrt{D}}{Q} > 0 \Rightarrow Q > 0$

(ii) $\alpha + \overline{\alpha} > 0 \Rightarrow \frac{P}{Q} > 0 \Rightarrow P > 0$

(iii) $\overline{\alpha} < 0 \Rightarrow \frac{P}{\sqrt{D}} < 0$

(iv) $1 < \alpha \Rightarrow Q < P + \sqrt{D} < 2\sqrt{D}$

$\Rightarrow P, Q \in \mathbb{N}$, $P < \sqrt{D}$, $Q < 2\sqrt{D}$ and $Q | P^2 - D$. \hfill (24)

Now expand $\alpha$ as a C.F.

$$\alpha = a_0 = \frac{1}{\alpha_1}, \ a_0 = \lfloor \alpha \rfloor, \ \alpha_1 > 1$$

$\Rightarrow \alpha = a_0 + \frac{1}{\alpha}$

$\Rightarrow \overline{\alpha_1} = -\frac{1}{a_0 - \alpha} \Rightarrow -1 < \overline{\alpha_1} < 0$
Hence $\alpha_1$ is reduced also. Similarly $\alpha_2$, $\alpha_3$, ... are reduced.

Now

$$\frac{1}{\alpha_1} = \alpha - a_0 = \frac{P + \sqrt{D}}{Q} - a_0 = \frac{P - Qa_0 + \sqrt{D}}{Q}$$

so let $P_1 = -P + Qa_0$ so

$$\alpha_1 = \frac{Q}{-P_1 + \sqrt{D}} = \frac{P_1 + \sqrt{D}}{Q_1}$$

where $Q_1Q = D - P_1^2$ and $Q_1 \in \mathbb{Z}$ since $Q|D - P^2$ and $p_1 \equiv -P \pmod{Q}$.

Then

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}$$

and since $\alpha_1$ is reduced, $p_1 > 0$, $Q_1 > 0$ and get the conditions (??) above using (??).

We carry on with the C.F. process, using $\alpha_1$ instead of $\alpha$, ... Each complete quotient $\frac{P_n}{Q_n}$ has the form

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n}$$

where $P_n, Q_n$ satisfy (??) There are only a finite set of possibilities for the pairs $(P_n, Q_n)$ so eventually we come to a pair $(P_m, Q_m) = (P_n, Q_n)$, $m > n$ so $\alpha_m = \alpha_n$ and so the C.F. is periodic from this point on.

Claim: The C.F. is purely periodic.

Subclaim: $\alpha_{n-1} = \alpha_{m-1}$. If this were so we would be able to work back to get, eventually, $\alpha_0 = \alpha_{m-n}$ proving pure periodicity. Proof of the subclaim: $\alpha_n = a_n + \frac{1}{\alpha_{n-1}} \Rightarrow \overline{\alpha_n} = a_n + \frac{1}{\overline{\alpha_{n-1}}}$. Let $\beta_n = -\frac{1}{\overline{\alpha}_n}$ then $-1 < \overline{\alpha}_n < 0 \Rightarrow 1 < \beta_n$ and $-\frac{1}{\beta_n} = a_n - \beta_{n+1}$ or $\beta_{n+1} = a_n + \frac{1}{\beta_n}$ so $a_n = [\alpha_n] = [\beta_{n+1}]$. Now let $n < m$ and $\alpha_n = \alpha_m$ so $\overline{\alpha}_n = \overline{\alpha}_m \Rightarrow \beta_n = \beta_m$ and $a_{n-1} = [\beta_n] = [\beta_m] = a_{m-1}$. But $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$, $\alpha_{m-1} = a_{m-1} + \frac{1}{\alpha_m} \Rightarrow \alpha_{n-1} = \alpha_{m-1}$. Applying this again successively $\alpha = \alpha_0 = \alpha_{m-n} = \alpha_r$ say, and

$$\alpha = [a_0, a_1, \ldots, a_{r-1}, \alpha_r]$$

pure periodic with period length $r$. □
### Continued fractions

#### TABLE I

<table>
<thead>
<tr>
<th>$N$</th>
<th>Continued fraction for $\frac{1}{N}$</th>
<th>$x$</th>
<th>$y$</th>
<th>$x^2 - Ny^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$1; 2$</td>
<td>1</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>3</td>
<td>$1; 1, 2$</td>
<td>2</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>5</td>
<td>$2; 4$</td>
<td>2</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>6</td>
<td>$2; 2, 4$</td>
<td>5</td>
<td>2</td>
<td>$+1$</td>
</tr>
<tr>
<td>7</td>
<td>$2; 1, 1, 1, 4$</td>
<td>8</td>
<td>3</td>
<td>$+1$</td>
</tr>
<tr>
<td>8</td>
<td>$2; 1, 4$</td>
<td>3</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>10</td>
<td>$3; 6$</td>
<td>3</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>11</td>
<td>$3; 3, 6$</td>
<td>10</td>
<td>3</td>
<td>$+1$</td>
</tr>
<tr>
<td>12</td>
<td>$3; 2, 6$</td>
<td>7</td>
<td>2</td>
<td>$+1$</td>
</tr>
<tr>
<td>13</td>
<td>$3; 1, 1, 1, 1, 6$</td>
<td>18</td>
<td>5</td>
<td>$-1$</td>
</tr>
<tr>
<td>14</td>
<td>$3; 1, 2, 1, 6$</td>
<td>15</td>
<td>4</td>
<td>$+1$</td>
</tr>
<tr>
<td>15</td>
<td>$3; 1, 6$</td>
<td>4</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>17</td>
<td>$4; 8$</td>
<td>4</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>18</td>
<td>$4; 4, 8$</td>
<td>17</td>
<td>4</td>
<td>$+1$</td>
</tr>
<tr>
<td>19</td>
<td>$4; 2, 1, 3, 1, 2, 8$</td>
<td>170</td>
<td>39</td>
<td>$+1$</td>
</tr>
<tr>
<td>20</td>
<td>$4; 2, 8$</td>
<td>9</td>
<td>2</td>
<td>$+1$</td>
</tr>
<tr>
<td>21</td>
<td>$4; 1, 1, 2, 1, 1, 8$</td>
<td>55</td>
<td>12</td>
<td>$+1$</td>
</tr>
<tr>
<td>22</td>
<td>$4; 1, 2, 4, 2, 1, 8$</td>
<td>197</td>
<td>42</td>
<td>$+1$</td>
</tr>
<tr>
<td>23</td>
<td>$4; 1, 3, 1, 8$</td>
<td>24</td>
<td>5</td>
<td>$+1$</td>
</tr>
<tr>
<td>24</td>
<td>$4; 1, 8$</td>
<td>5</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>26</td>
<td>$5; 10$</td>
<td>5</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>27</td>
<td>$5; 5, 10$</td>
<td>26</td>
<td>5</td>
<td>$+1$</td>
</tr>
<tr>
<td>28</td>
<td>$5; 3, 2, 3, 10$</td>
<td>127</td>
<td>24</td>
<td>$+1$</td>
</tr>
<tr>
<td>29</td>
<td>$5; 2, 1, 1, 2, 10$</td>
<td>70</td>
<td>13</td>
<td>$-1$</td>
</tr>
<tr>
<td>30</td>
<td>$5; 2, 10$</td>
<td>11</td>
<td>2</td>
<td>$+1$</td>
</tr>
<tr>
<td>31</td>
<td>$5; 1, 1, 3, 5, 3, 1, 1, 10$</td>
<td>1520</td>
<td>273</td>
<td>$+1$</td>
</tr>
<tr>
<td>32</td>
<td>$5; 1, 1, 1, 10$</td>
<td>17</td>
<td>3</td>
<td>$+1$</td>
</tr>
<tr>
<td>33</td>
<td>$5; 1, 2, 1, 10$</td>
<td>23</td>
<td>4</td>
<td>$+1$</td>
</tr>
<tr>
<td>34</td>
<td>$5; 1, 4, 1, 10$</td>
<td>35</td>
<td>6</td>
<td>$+1$</td>
</tr>
<tr>
<td>35</td>
<td>$5; 1, 10$</td>
<td>6</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>37</td>
<td>$6; 12$</td>
<td>6</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>38</td>
<td>$6; 6, 12$</td>
<td>37</td>
<td>6</td>
<td>$+1$</td>
</tr>
<tr>
<td>39</td>
<td>$6; 4, 12$</td>
<td>25</td>
<td>4</td>
<td>$+1$</td>
</tr>
<tr>
<td>40</td>
<td>$6; 3, 12$</td>
<td>19</td>
<td>3</td>
<td>$+1$</td>
</tr>
<tr>
<td>41</td>
<td>$6; 2, 2, 12$</td>
<td>32</td>
<td>5</td>
<td>$-1$</td>
</tr>
<tr>
<td>42</td>
<td>$6; 2, 12$</td>
<td>13</td>
<td>2</td>
<td>$+1$</td>
</tr>
<tr>
<td>43</td>
<td>$6; 1, 3, 1, 5, 1, 3, 1, 1, 12$</td>
<td>3482</td>
<td>531</td>
<td>$+1$</td>
</tr>
<tr>
<td>44</td>
<td>$6; 1, 1, 2, 1, 1, 1, 12$</td>
<td>199</td>
<td>30</td>
<td>$+1$</td>
</tr>
<tr>
<td>45</td>
<td>$6; 1, 2, 2, 1, 1, 12$</td>
<td>161</td>
<td>24</td>
<td>$+1$</td>
</tr>
<tr>
<td>46</td>
<td>$6; 1, 3, 1, 1, 2, 6, 2, 1, 1, 12$</td>
<td>24335</td>
<td>3588</td>
<td>$+1$</td>
</tr>
<tr>
<td>47</td>
<td>$6; 1, 5, 1, 12$</td>
<td>48</td>
<td>7</td>
<td>$+1$</td>
</tr>
<tr>
<td>48</td>
<td>$6; 1, 12$</td>
<td>7</td>
<td>1</td>
<td>$+1$</td>
</tr>
<tr>
<td>50</td>
<td>$7; 14$</td>
<td>7</td>
<td>1</td>
<td>$-1$</td>
</tr>
</tbody>
</table>
Now consider the table on page 77: \( N \in \mathbb{N}, n \neq m^2 \). All the continued fractions are of a special form:

1. None are purely periodic \( \sqrt{N} = -\sqrt{N} < -1 \) but \( a_0 = \lfloor \sqrt{N} \rfloor \), \( \alpha = a_0 + \sqrt{N} \) has \( 1 < \alpha \) and \( -1 < \frac{1}{\alpha} < 0 \) and the continued fraction of \( \alpha \) begins with \( 2a_0 \) since \( \lfloor a_0 + \sqrt{N} \rfloor = a_0 + \lfloor \sqrt{N} \rfloor = 2a_0 \). Hence \( a_0 + \sqrt{N} = [2a_0, a_1, \ldots, a_n, 2a_0] \) eventually since it is purely periodic.
2. There is one preperiod term for \( \sqrt{N} \) (with a periodic part consisting of symmetric terms), followed by \( 2a_0 \):

\[
\sqrt{N} = [a_0, a_1, a_2, \ldots, a_2, a_1, 2a_0]
\]

**Ex**

\[
\sqrt{53} = [7, 3, 1, 1, 3, 14]
\]

**Theorem (Lagrange)** A continued fraction is periodic \( \iff \) it is the continued fraction of a quadratic irrational. **Ex**

\[
\frac{2^{1/3}}{2 + \frac{5^2}{2 + \frac{7^2}{2 + \cdots}}} = [1, 3, 1, 5, 11, 4, 1, \ldots]
\]

\[
\frac{e - 1}{e + 1} = [2, 6, 10, 14, \ldots]
\]

\[
e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]
\]

The simple continued fraction for \( \pi \) does not show any obvious pattern but clear patterns do emerge in the beautiful non-simple continued fractions

\[
\frac{4}{\pi} = 1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{2 + \frac{7^2}{2 + \cdots}}}}
\]

(Brouckner), giving convergents 1, 3/2, 15/13, 105/76, 315/263, ... (Sloane's A025557 and A007509) and

\[
\frac{\pi}{2} = 1 - \frac{1}{3 - \frac{1}{1 - \frac{1}{1 - \frac{1}{1 - \frac{1}{1 - \frac{1}{3 - \cdots}}}}}}
\]

Return to the Fundamental Solution to Pell’s Equation
Let \( \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n} \) be the two convergents just preceding \( 2a_0 \). i.e

\[
\frac{p_{n-1}}{q_{n-1}} = [a_0, \ldots, a_{n-1}]
\]
\[
\frac{p_n}{q_n} = [a_0, \ldots, a_{n-1}, a_n]
\]

Now \( \alpha = \sqrt{N} = \frac{a_{n+1}p_n + p_{n-1}}{a_nq_n + q_{n-1}} \) (1) where

\[
\alpha_{n+1} = 2a_0 + \frac{1}{a_1 + \ldots}
\]
\[
= [2a_0, a_1, a_2, \ldots]
\]
\[
= a_0 + \sqrt{N}
\]

Substituting this value for \( \alpha_{n+1} \) in 1 and simplifying gives

\[
\sqrt{N}(\sqrt{N} + a_0)q_n + \sqrt{N}q_{n-1} = (\sqrt{N} + a_0)p_n + p_{n-1}
\]

Equating rational and irrational parts:

\[
\Rightarrow Nq_n = a_0p_n + p_{n-1}
\]
\[
a_0q_n + q_{n-1} = p_n
\]
\[
\Rightarrow p_{n-1} = Nq_n - a_0p_n
\]
\[
q_{n-1} = p_n - a_0q_n
\]

Substitute in equation (1) on page 74 to get

\[
p_n(p_n - a_0q_n) - q_n((Nq_n - a_0p_n) = (-1)^{n-1}
\]
\[
\Rightarrow p_n^2 - Nq_n^2 = (-1)^{n-1}
\]

Hence \( x = p_n, y = q_n \) is a solution to \( s^2 - Ny^2 = 1 \) if \( n \) is odd and \( x^2 - Ny^2 = -1 \) if \( n \) is even. In the latter case apply the same argument to the convergents at the end of the second period: \( [a_0, a_1, \ldots, a_n, 2a_0, a_1, \ldots, a_{2n+1}] \) so \( x = p_{2n+1}, y = q_{2n+1} \) solve

\[
x^2 - Ny^2 = (-1)^{2n+1-1} = (-1)^{2n} = 1
\]

Ex \( N = 21 \)

\[
\sqrt{21} = [4, 1, 1, 2, 1, 1, 8] \text{ so } n = 5 \text{ odd}
\]
Convergents: \( \frac{4}{1}, \frac{5}{1}, \frac{9}{2}, \frac{23}{5}, \frac{32}{7}, \frac{55}{12} = \frac{p_5}{q_5}, \ldots \)

So \( x_1 = p_5 = 55, \ y_1 = q_5 = 12 \) solves \( x_1^2 - 21y_1^2 = 1 \)

This gives the fundamental solution. Other solutions are

\[
x^m + y^m \sqrt{21} = (x_1 + y_1 \sqrt{21})^m, \ m = 2, 3, 4, \ldots
\]

\textbf{Ex} \quad N = 29

\[
\sqrt{29} = [5, \frac{2}{1}, 1, 2, 10] \quad \text{so} \ n = 4 \text{ even}
\]

Convergents: \( \frac{5}{1}, \frac{11}{2}, \frac{16}{3}, \frac{27}{5}, \frac{70}{13}, \frac{727}{135}, \frac{1524}{283}, \frac{2251}{418}, \frac{3774}{701}, \frac{9801}{1820} = \frac{p_9}{q_9} \)

So \( x_1 = 9801, \ y_1 = 1820 \) gives the fundamental solution.

\textbf{Note}

1. Not all details have been proved, e.g. that the C.F. expansion gives all of the solutions, including the fundamental.

2. There are deep mysteries tied up in C.F. expansions e.g. why are they closely related to \textbf{quadratic} irrationals?
8 Quadratic Reciprocity

Let $p$ be an odd prime $p \in \{3, 5, 7, \ldots\}$, $n \in \mathbb{Z}$, $p \nmid n$.

- If $x^2 \equiv n \pmod{p}$ has a solution $x \in \mathbb{Z}$ let $(n | p) = 1$.
- If $x^2 \equiv n \pmod{p}$ has no solution let $(n | p) = -1$.
- If $p|n$ let $(n | p) = 0$.

This defines the **Legendre symbol**, $(n | p)$.

Ex $p = 11$:

\[
\begin{align*}
1^2 & \equiv 1 \\
2^2 & \equiv 4 \\
3^2 & \equiv 9 \\
4^2 & = 16 = 11 + 5 \equiv 5 \\
5^2 & = 25 = 22 + 3 \equiv 3 \\
6^2 & \equiv (11 - 5)^2 \equiv (-5)^2 \equiv 5^2 \equiv 3 \\
7^2 & \equiv (-4)^2 \equiv 5 \\
8^2 & \equiv (-3)^2 \equiv 9 \\
9^2 & \equiv (-2)^2 \equiv 4 \\
10^2 & \equiv (-1)^2 \equiv 1 \\
11^2 & \equiv 0 \pmod{11}
\end{align*}
\]

So the quadratic residues are $1, 3, 4, 5, 9 \Rightarrow (n | 11) = 1$
the non-residues are $\therefore 2, 6, 7, 8, 10 \Rightarrow (n | 11) = -1$
and $(11 | 11) = 0$.

**Proposition**  $a \equiv b \pmod{p} \Rightarrow (a | p) = (b | p)$

*Proof.  $a = b + lp$ so if $p|a \Rightarrow p|b \Rightarrow (a | p) = 0 \Leftrightarrow (b | p) = 0$. Also $(a | p) = 1 \Leftrightarrow x^2 \equiv a \pmod{p}$ has a solution $\Leftrightarrow x^2 \equiv a \equiv b$ has a solution. □

**Proposition**  Let $p \in \mathbb{P}$ be odd. Every (reduced) residue system mod $p$ contains exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues mod $p$. The quadratic residues belong to the residue classes containing the numbers:

\[ R = \left\{ 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \right\} \]
Proof. Claim: the numbers in $R$ are distinct mod $p$: If $x^2, y^2 \in \mathbb{R}$ and $x^2 \equiv y^2 \mod p \Rightarrow (x - y)(x + y) \equiv 0 \mod p \Rightarrow p | (x - y)(x + y)$ But $0 < x + y \leq \frac{p-1}{2} + \frac{p-1}{2} < p$ so $p | x - y \Rightarrow x \equiv y \mod p \Rightarrow x = y.$

Since $(p - k)^2 = p^2 - 2pkKk^2 \equiv k^2 \mod p$ and $\{1, 2, \ldots, p - 1\}$ is a complete set of representatives, every quadratic residue is congruent to one of the numbers in $R$. \qed

Ex  $p = 7$

\[
\begin{align*}
1^2 &\equiv 1 \\
2^2 &\equiv 4 \\
3^2 &\equiv 2
\end{align*}
\]

The number of residues is $\frac{7-1}{2} = 3$. So

1, 4, 2 are residues

3, 5, 6 are non-residues

Ex  For all odd $p$, $(1 | p) = 1$.

Ex  For all odd $p$ and $m \in \mathbb{Z}$, $(m^2 | p) = 1$.

Ex  Fix $p$ and let $f(n) = (n | p)$ so $f : \mathbb{Z} \to \{-1, 0, 1\}$. Then $f(n + p) = (n + p | p) = (n | p) = f(n)$ so $f$ is periodic with period $p$. It is also completely multiplicative. $f(ab) = f(a)f(b) \forall a, b \in \mathbb{Z}$.

**Theorem 25 (Euler)** Let $p \in \mathbb{P}$ be odd. Then $\forall n \in \mathbb{Z}$,

\[(n | p) \equiv n^{\frac{p-1}{2}} \mod p.\]

Proof. Note $\frac{p-1}{2} \in \mathbb{N}$. If $p \nmid n$ both sides are zero so suppose $p \mid n$.

Let $(n | p) = 1$. Then $\exists x$ so $x^2 \equiv n \mod p$

\[\Rightarrow n^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \mod p\]

by Fermat’s little theorem. Hence

\[n^{\frac{p-1}{2}} \equiv (n | p) \text{ if } (n | p) = 1\]

Let $(n | p) = -1$. Consider the polynomial

\[f(x) = x^{\frac{p-1}{2}} - 1, \quad \partial f = \text{degree of } f = \frac{p-1}{2}\]

So, over any field, $f$ has at most $\frac{p-1}{2}$ roots, hence the congruence $f(x) \equiv 0 \mod p$ has at most $\frac{p-1}{2}$ solutions. But the $\frac{p-1}{2}$ quadratic residues mod $p$ are solutions (the case $(n | p) = 1$) so the non-residues are not. Hence

\[n^{\frac{p-1}{2}} \not\equiv 1 \mod p \text{ if } (n | p) = -1.\]
But
\[ n^{p-1} - 1 = \left( n^{\frac{p-1}{2}} - 1 \right) \left( n^{\frac{p-1}{2}} + 1 \right) \]
and \( p | n^{p-1} - 1 \) so
\[ n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \]
Hence
\[ n^{\frac{p-1}{2}} \equiv -1 = (n \mid p) \pmod{p} \]

□

Proposition \( f(n) = (n \mid p) \) is completely multiplicative.

Proof. \( p \mid m \) or \( p \mid n \Rightarrow p \mid mn \Rightarrow (mn \mid p) = 0 \), hence \( f(mn) = f(m) \cdot f(n) \) if \( p \mid m \) or \( p \mid n \). Let \( p \nmid m \) and \( p \nmid n \). Then \( p \nmid mn \) so
\[ (mn \mid p) \equiv (mn)^{\frac{p-1}{2}} = f(mn) = m^{\frac{p-1}{2}} \cdot n^{\frac{p-1}{2}} \equiv (m \mid p)(n \mid p) \pmod{p} \]
But each of \((mn \mid p), (m \mid p)\) or \((n \mid p)\) is \pm 1 so the difference \((mn \mid p) - (m \mid p)(n \mid p)\) is 0, \pm 2. But this difference is divisible by \( p \), hence it is 0, and therefore, \((mn \mid p) = (m \mid p)(n \mid p) \Rightarrow f(mn) = f(m) \cdot f(n)\) so \( f \) is completely multiplicative. □

Proposition
\[ (-1 \mid p) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases} \]

Proof. By Euler, Theorem 29,
\[ (-1 \mid p) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \]
since each side is \pm 1, they must be equal. □

Ex \( p = 5, \frac{p-1}{2} - 2 \)
\[
\begin{array}{c|ccccc}
  n & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
(n \mid 5) & 0 & 1 & 1 & 0 & & \\
\end{array}
\]
\( p = 7 \)
\[
\begin{array}{c|cccccccc}
  n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
(n \mid 7) & 0 & 1 & -1 & -1 & & & & \\
\end{array}
\]

Proposition
\[ (2 \mid p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases} \]
\[
\begin{array}{c|cccccccc}
  p & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
\times & R & R & N & N & N & R & R & R & R \\
\end{array}
\]
Proof. Consider the $\frac{p-1}{2}$ congruences mod $p$:

\[
\begin{align*}
p - 1 &\equiv 1(-1)^1 \\
2 &\equiv 2(-1)^2 \\
p - 3 &\equiv 3(-1)^3 \\
\vdots \\
r &\equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}}
\end{align*}
\]

Multiply these together and note that each integer on LHS is even, since $p$ is odd.

\[
\Rightarrow 2 \cdot 4 \cdot 6 \cdots (p - 1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+3+\cdots+\frac{p-1}{2}} \pmod{p}
\]

\[
\Rightarrow 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \pmod{p}
\]

But $p \nmid \left(\frac{p-1}{2}\right)!$, hence, by Euler, Theorem 29,

\[
(2 \mid p) = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}
\]

and since LHS and RHS are $\pm 1$ we have

\[
(2 \mid p) = (-1)^{\frac{p^2-1}{8}}
\]

\[\square\]

Euler’s theorem is normally too computationally expensive to compute $(n \mid p)$. Gauss’ lemma and Reciprocity theorem, proved below, both give better ways to evaluate this function.

\[
\text{Note: } f : \mathbb{Z} \to \{-1, 0, 1\} \subset S' \cup \{0\} = \{z \in \mathbb{C} : |z| = 1\} \cup \{0\} \text{ is an example of a so-called character an extension of the group character } \chi : \mathbb{Z} / p\mathbb{Z} \to S', \chi \left([n]_p\right) = (n \mid p)
\]

Theorem 26 (Gauss) Let $p \nmid n$ and consider the residues mod $p$ of the $\frac{p-1}{2}$ multiples of $n$, $M = \{n, 2n, 3n, \ldots, \frac{p-1}{2}n\}$ which are the least positive residue representatives, i.e. which lie in $\{1, \ldots, p\}$. If $m$ is the number which exceed $\frac{p}{2}$, then $(n \mid p) = (-1)^m$.

Proof. If $p \mid in - jn$ with $1 \leq i, j \leq \frac{p-1}{2}$. Then $p \mid (i - j)n$ but $p \nmid n$ $\Rightarrow i = j$. hence the numbers in $M$ are incongruent mod $p$.

Consider their least positive residues and put them in two disjoint sets $A = \{a_1, \ldots, a_k\}$.
and \( B = \{b_1, \ldots, b_n\} \) where \( a_i \equiv tn \pmod{p} \), \( 1 \leq t \leq \frac{p-1}{2} \), \( 0 < a_i < \frac{p}{2} \) and \( b_i \equiv sn \pmod{p} \), \( 1 \leq s \leq \frac{p-1}{2} \), \( \frac{p}{2} < b_i < p \) (1).

Since \( A \cap B = \emptyset \), \( m + k = \frac{p-1}{2} \). Let \( c_i = p - b_i \), \( 1 \leq i \leq m \) and \( C = \{c_1, \ldots, c_m\} \). Now \( 0 < c_i < \frac{p}{2} \) by (1).

Claim \( A \cap C = \emptyset \): If \( c_i = a_j \Rightarrow p - b_i = a_j \Rightarrow a_j + b_j = p \equiv 0 \pmod{p} \) \( \therefore tn + sn = (t + s)n \equiv 0 \pmod{p} \) for some \( s \) and \( t \) with \( 1 \leq s, t < \frac{p}{2} \). But this is impossible since \( 1 < s + t < p \Rightarrow p \nmid s + t \). Hence \( A \cap C = \emptyset \).

Hence \( \#(A \cup C) = m + k = \frac{p-1}{2} \) integers in \([1, \frac{p-1}{2}]\). Hence

\[ A \cup C = \{a_1, \ldots, a_k, c_1, \ldots, c_m\} = \{1, 2, \ldots, \frac{p-1}{2}\} \]

Now form the product of all of the elements in \( A \cup C \):

\[ a_1a_2 \cdots a_kc_1c_2 \cdots c_m = \left(\frac{p-1}{2}\right)! \]

But \( c_i = p - b_i \) so

\[
\left(\frac{p-1}{2}\right)! = a_1 \cdots a_k(p-b_1) \cdots (p-b_m) \\
\equiv (-1)^m a_1 \cdots a_kb_1 \cdots b_m \pmod{p} \\
\equiv (-1)^m n(2n)(3n) \cdots \left(\frac{p-1}{2}\right) n \pmod{p} \\
\equiv (-1)^m n^{p-1} \left(\frac{p-1}{2}\right)! \pmod{p}
\]

\( \Rightarrow n^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p} \) and \( (n \mid p) = (-1)^m \) follows by Theorem 29. \( \square \)

**Theorem 27** If \( m \) is defined as in Theorem 30 above

\[ m \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jn}{p} \right\rfloor + (n-1) \left(\frac{p^2-1}{8}\right) \pmod{2} \]

so if \( n \) is odd:

\[ m \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jn}{p} \right\rfloor \pmod{2} \]

**Note** (1) If \( n \in \mathbb{N}, n = 2^am, a \geq 0, m \) odd, so

\[ (n \mid p) = (2 \mid p)^a (m \mid p) \text{ where } m \text{ is odd} \]

\[ = (-1)^{\frac{p^2-1}{8}} (m \mid p) \]
(2) \((n \mid p) = (-1)^m\) so only the value of \(m \pmod{2}\) (its \text{parity}) is needed to compute the Legendre symbol.

**Proof.** The number \(m\) is the number of least positive residues of \(n, 2n, \ldots, \frac{p-1}{2}n\) exceeding \(\frac{p}{2}\). Let \(jn\) be one of these

\[
\frac{jn}{p} = \left\lfloor \frac{jn}{p} \right\rfloor + \left\{ \frac{jn}{p} \right\} \quad \text{where } 0 < \left\{ \frac{jn}{p} \right\} < 1
\]

so \(jn = p \left\lfloor \frac{jn}{p} \right\rfloor + p \left\{ \frac{jn}{p} \right\} = p \left\lfloor \frac{jn}{p} \right\rfloor + r_j\) where \(0 < r_j < p\).

The number \(r_j\) is the least positive residue of \(jn\): \(r_j = jn - p \left\lfloor \frac{jn}{p} \right\rfloor\) (1). Using the same notation as in the previous theorem,

\[
\{r_1, \ldots, r_{\frac{p-1}{2}}\} = \{a_1, \ldots, a_k, b_1, \ldots, b_m\}
\]

\[
\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{a_1, \ldots, a_k, c_1, \ldots, c_m\}
\]

\(c_i = p - b_i\)

Add all of the elements in each set:

\[
\sum_{j=1}^{\frac{p-1}{2}} r_j = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j \quad (2)
\]

\[
\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j \quad (3)
\]

In (2) use (1) for \(r_j\):

\[
\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = n \sum_{j=1}^{\frac{p-1}{2}} j - p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jn}{p} \right\rfloor \quad (4)
\]

(3) is \(mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{j=1}^{\frac{p-1}{2}} j\) (5)

Add (4) and (5) to get

\[
2 \left( \sum_{i=1}^{k} a_i \right) + mp = (n + 1) \left( \frac{p^2 - 1}{8} \right) - p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jn}{p} \right\rfloor
\]

But \(-p \equiv 1 \pmod{2}\) and \(n + 1 \equiv n - 1 \pmod{2}\), hence

\[
m \equiv (n + 1) \left( \frac{p^2 - 1}{8} \right) + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jn}{p} \right\rfloor \pmod{2}
\]
Theorem 28 (Quadratic Reciprocity Law, Gauss, 1796) If \( p \) and \( q \) are distinct odd primes, then

\[
(p \mid q) (q \mid p) = (-1)^{\frac{(p-1)(q-1)}{4}} \tag{1}
\]

Proof. \((q \mid p) = (-1)^m\) where

\[
m = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor \pmod{2}
\]

Similarly \((p \mid q) = (-1)^n\) where

\[
n = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor \pmod{2}
\]

Hence \((p \mid q) (q \mid p) = (-1)^{m+n}\) and (1) follows from the claimed identity:

\[
\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor = \left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right) \tag{2}
\]

Consider the rectangle with given vertices. (In the illustration, \( p = 7, \ q = 5 \).)

The diagonal does not pass through any lattice point, because if so, \( y = \frac{q}{p}x \) at the lattice point \((x, y)\). \( \Rightarrow \) \( xq = yp \Rightarrow p \mid x \) and \( q \mid y \) so \( x \geq p, \ y \geq q \) and the point \((x, y)\) must be outside the rectangle.
The total number of lattice points inside the rectangle is \((\frac{p-1}{2}) (\frac{p-1}{2}) = c\)

The total number of points in the triangle below the diagonal is

\[
b = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor
\]

The number above is

\[
a = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor
\]

So \(a + b = c\) and so (2) follows, hence (1). \(\square\)

**Ex** \((219 \mid 383)\). Note \(383 \in \mathbb{P}\). Now \(219 = 3 \cdot 73\) \((73 \in \mathbb{P})\) so, by multiplicativity

\[
(219 \mid 383) = (3 \mid 383) (73 \mid 383).
\]

Reciprocity implies that

\[
(3 \mid 383) (383 \mid 3) = (-1)^{\frac{(383-1)(3-1)}{4}} = -1
\]

so

\[
(3 \mid 383) = - (3 \mid 3) \text{ using periodicity mod 3}
= 1
\]

Also

\[
(73 \mid 383) = (383 \mid 73) (-1)^{\frac{(383-1)(73-1)}{4}}
= (18 \mid 73)
= (2 \mid 73) (3 \mid 73)^2
= (-1)^{\frac{73^2-3}{8}}
= 1
\]

Hence \((219 \mid 383) = 1 \cdot 1 = 1\) and \(x^2 \equiv 219 \pmod{383}\) has a solution.
9 Elliptic Equations and Curves

- Diophantine family with interesting properties.
- Used in factoring and encryption.
- Curves have their own intrinsic arithmetic.

Ex (see above) \( y^2 = x^3 + 7 \) has no \( \mathbb{Z} \) solutions.

General (Weierstrass) form:

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6
\]

\( y \to \frac{1}{2}(y - a_1 x - a_3) \) and multiplication by 4 gives

\[
y^2 = 4x^3 + (a_1^2 + ra_2)x^2 + 2(2a_4 + a_1 a_3)x + (a_3^2 + 4a_6)
\]

\( x \to \frac{x - 3(a_1^2 + 4a_2)}{36}, \ y \to \frac{y}{108} \) and multiplying by 108^2 we get

\[
y^2 = x^3 - Ax - B
\]

and Proposition If the \( a_i \in \mathbb{Z} \) so are \( A \) and \( B \).

Discriminant

Definition \( \Delta = 16(4A^3 - 27B^2) \)

If \( y^2 = F(x) \) is an elliptic curve where \( F(x) \) is a cubic polynomial with integer coefficients with roots \( r_1, r_2, r_3 \in \mathbb{C} \) then the discriminant

\[
\Delta = \prod_{i<j}(r_i - r_j)^2 \in \mathbb{N}
\]

if the roots are distinct.

- If \( \Delta = 0 \) then \( x^3 - Ax - B = (x - 2\alpha)(x + \alpha)^2, \ \alpha = \sqrt[3]{\frac{A}{B}}. \)

  1. If \( \Delta = 0 \) and \( A \neq 0 \) then the curve \( y^2 = x^3 - Ax - B \) crosses itself—known as a node.
2. If $\Delta = 0$ and $A = B = 0$ we have a **cusp**.

• If $\Delta \neq 0$ curve is **non-singular** i.e. ‘interesting’.

Can use *Mathematica* to plot elliptic curves e.g.

```mathematica
ContourPlot[y^2 - x^3 + x, {x, -4, 4}, {y, -4, 4}, PlotPoints->200,
Contours->{0}, ContourShading->False]
```

**Line intersection property**: each non-vertical line meeting a curve $E(\mathbb{R})$ in two points $P, Q$ meets it in a third point $R$.

*Proof*. If the line is $y = mx + c$ solve with $y^2 = x^3 - Ax - B$ so $(mx + c)^2 = x^3 - Ax - B$ has **two solutions** $x_1, 7x_2$ if $P = (x_1, y_1), Q = x_2y_2$ and therefore a third $x_3$ so let $R = (x_3, mx_3 + c)$ □
Now if $P, Q$ have rational coordinates, $m, c \in \mathbb{Q}$, so if $A, B \in \mathbb{Z}$ then $x_1x_2x_3 = -(B) = B$ so if $x_1, y_1 \in \mathbb{Q}$ and $x_2, y_2 \in \mathbb{Q}$ so does $x_3$ and hence $y_3 \in \mathbb{Q}$.

This simple observation enables us to generate new $\mathbb{Q}$ solutions or points on $E(\mathbb{R})$ out of old.

**Vertical lines:** We say each vertical line meets the curve again “at $\infty$” and give this point a label 0 or zero.

**Note:**

1. $P' = Q'$ is possible but we still get a third point $R$.

2. If $P''Q''$ is vertical, then their $x$-coordinates are the same so $P'' = (x_1, y_1)$, $Q'' = (x_2, y_2)$ $\Rightarrow$ $x_1 = x_2$ so $y_2^2 = x_1^3 - Ax_1 - B = x_2^3 - Ax_2 - B = y_1^2$. Hence $y_2 = -y_1$ and the curve is symmetric about $OX$.

**The group law: definition of $+$**

If $P, Q \in E(\mathbb{R})$ and $R'$ has the same $x$-coordinate as $R$, the third point on the line through $P$ and $Q$, but with $y$-coordinate negated, let $R' = P + Q$. This defines $+$.

- $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R' = (x_3, y_3)$ then $x_1 \neq x_2$ $\Rightarrow$

\[
\begin{align*}
x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\
y_3 &= -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_3 - \frac{y_1x_2 - y_2x_1}{x_2 - x_1}
\end{align*}
\]

(A).

- $P = Q$ $\Rightarrow$

\[
\begin{align*}
x_3 &= \left(\frac{3x_1^2 - A}{2y_1}\right)^2 - x_1 - x_2 \\
y_3 &= \frac{3x_1^2 - A}{2y_1}(x_1 - x_3) - y_1
\end{align*}
\]

(B).
\[ P = Q' \Rightarrow 0 = P + Q. \]

Notes:

1. The proof of these formulas are an exercise in coordinate geometry.

2. \( P'' = P \) since \((x_1, -(y_1)) = (x_1, y_1)\).

3.
\[
Q + P = \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^2 x_1 - x_2, \frac{y_1 - y_2}{x_1 - x_2} x_3 - \frac{y_2 x_1 - y_1 x_2}{x_1 - x_2}
\]
\[
= \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 x_1 - x_2, \frac{y_2 - y_1}{x_2 - x_1} x_3 - \frac{y_1 x_2 - x_2 y_1}{x_2 - x_1}
\]
\[
= P + Q
\]
so + is commutative.

4. + is also associative \((P + Q) = R = P + (Q + R)\).

5. + takes a point with \( \mathbb{Q} \) coordinates to a point with \( \mathbb{Q} \) coordinates i.e. \(+ : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})\).

Write \( 2P \) instead of \( P + P \) and \( nP \) for \( P + (n - 1)P \).

Note: We could have \( P \neq 0 \) but \( nP = 0 \) for some \( n > 1 \).

Ex \( y^2 = x^3 - 63x - 162 : P_1 = (-6, 0), P_2 = (-3, 0), P_3 = (9, 0) \) all satisfy \( 2P_i = 0 \)

Ex \( y^2 = x^3 - 2, 5^2 = 3^3 \Rightarrow \)
\[
P = (3, 5) \in E(\mathbb{Z}) \subset E(\mathbb{Q})
\]
\[
2P = \begin{pmatrix} 129 \\ 100 \end{pmatrix}, \begin{pmatrix} -383 \\ 1000 \end{pmatrix}
\]
\[
3P = \begin{pmatrix} 164,323 \\ 29,241 \end{pmatrix}, \begin{pmatrix} 66,234,835 \\ 5,000,211 \end{pmatrix}
\]
etc and $nP \neq 0 \ \forall n \in \mathbb{N}$.

**Ex** $y^2 = x^3 - 11$, $P = (3, 4)$, $Q = (15, 58)$ generate an ‘independent’ set of two dimensions $nP + mQ = 0 \Rightarrow n = m = 0$ and $E(\mathbb{Q})$ has no torsion points.

**Ex** (Mestre) $y^2 - 246xy + 36,599,029y = x^3 - 19,339,780x - 36,239,244$ has at least 12 independent points.

**Conjecture** $\forall n \in \mathbb{N} \exists$ an elliptic curve with at least $n$ independent points.

**Note:** Finding points can be difficult: (Bremner, Cassels) $y^2 = 36,239,244$; $P = (0, 0)$, $2P = 0$ the next simplest point is

\[
\left(\frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100},\right.
\frac{256256267988926809388776834045513089648669153204356603464786949}{490078023219787588959802933995928925096061616470779979261000}\left.
\right).

**Theorem (Mazur)** The number, $t$, of torsion points for an elliptic curve $E(\mathbb{Q})$ is one of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 16\}$. Also, if $A, B \in \mathbb{Z}$, a torsion point has integral coordinates and either $y = 0$ (so $2(x, y) = 0$) or $y^2 | \Delta$.

There are infinitely many no-torsion points if there are any at all.

**Definition** The rank of a curve $E(\mathbb{Q})$ is an integer $r$ such that there are $r$ independent points on the curve and every rational point can be expressed as a sum of multiples of these points and some torsion point.

**Theorem (Mordell)** $0 \leq r < \infty$ os each curve has finite rank.

**Note:**

1. The structure of $E(\mathbb{Q})$ is that of a finitely generated abelian group. $G \cong T \oplus \mathbb{Z}^r$ where the torsion elements $T$ form a subgroup.

2. Finding $r$ is a very difficult problem.

**Elliptic curves mod $p$**

We can often get insight into $\mathbb{Q}$ points on curve by considering them modulo $p$, where $p$ is a prime. If $p \neq 2$ or $3$, formulas (A) and (B) still work so they define $+$ for $E(\mathbb{Z}_p) \times E(\mathbb{Z}_p) \to E(\mathbb{Z}_p)$ with $\mathbb{Z}_p = \{[0], \ldots, [p - 1]\} = GF(p)$ the finite field of order $p$. 
Ex

\[ y^2 \equiv x^3 - Ax - B \pmod{p} \]
\[ y^2 \equiv x^3 + x + 2 \pmod{11} \]

The solutions are \{(1, \pm2), (2, \pm1), (4, \pm2), (5, 0), (6, \pm2), (7, 0), (10, 0)\} = S and 0 = \infty making 12. All points are torsion since they are finite in number.

How many points are in \(E(\mathbb{Z}_p)\)? \(x\) can have \(p\) values, so \(x^3 - Ax - B\) at most \(p\). If these were random, we would expect about half to be quadratic residues and half non-residues, the residues giving two possible values of \(y\).

**Theorem (Hasse)** \(|\#E(\mathbb{Z}_p) - (P + 1)| < 2\sqrt{p}\)

**Proposition** \(p \equiv 1 \pmod{4} \Rightarrow \) the number of points on \(y^2 \equiv x^3 - x\) is exactly \(p\) (mod \(p\)) (including \(\infty\)).

Any integral solution of \(y^2 = x^3 - Ax - B\) becomes a modular solution of the congruence \(y^2 \equiv x^3 - AX - B\) (mod \(p\)).

**Warning:** Over \(\mathbb{Z}\), we may have \(\Delta \neq 0\) (a requirement), but \(\Delta \equiv 0 \pmod{p}\) when \(P \mid \Delta\). and such a curve would not be elliptic mod \(p\). If \(\Delta \neq 0 \pmod{p}\) we have good reduction, so we assume this is so.
\[ E : y^2 = x^3 - Ax - B, \ A, b \in \mathbb{Z}, \ \Delta = 16(4A^3 - 27B^2) \neq 0, \ D = 4A^3 - 27B^2 \]

Map

\[ \theta : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = GF(p) \ (\mathbb{Z}_p \text{ before}) \]

\[ n \mapsto [n]_p \]

**Theorem (Nagell-Lutz)** Points of \( E(\mathbb{Q}) \) of finite order have integer coordinates, i.e. are in \( E(\mathbb{Z}) \).

We map \( E(\mathbb{Q}) \) to \( E(\mathbb{Z}_p) \) through considering \( y^2 \equiv x^3 - Ax - B \mod p \)

**Theorem (Reduction Theorem)** Let \( T \subset E(\mathbb{Q}) \) be the subgroup of all points of finite order (the torsion subgroup). If \( p \nmid 2D, \ p \in \mathbb{P} \) then reduction mod \( p \) is an isomorphism of \( T \) onto a subgroup of \( E(\mathbb{Z}_p) \).

**Theorem (Lagrange)** If \( S \subset G \) and \( S \) is a subgroup of the finite group \( G \), then \( \#(S) \mid \#(G) \), i.e. the order of \( S \) divides the order of \( G \).

**Corollary** If \( P \in T \) and the order of \( P \) in \( E(\mathbb{Q}) \) is \( m \in \mathbb{N} \) then \( m \mid \#E(\mathbb{Z}_p) \forall p \nmid 2D \).

These theorems can be used to determine the points of finite order of an elliptic curve \( E(\mathbb{Q}) \).

**Ex** \( E : y^2 = x^3 + 3, \ D = -3^5 \) so let \( p \geq 5, \ p \in \mathbb{P} \). Then \( \#E(\mathbb{Z}_5) = 6, \ #E(\mathbb{Z}_7) = 13 \Rightarrow \#T \mid 6 \) and \( \#T \mid 13 \Rightarrow \#T = 1 \Rightarrow T = \{0\} \) so \( T \) has no (finite) points of finite order. Note \((1, 2) \in E(\mathbb{Q}) \) since \( 2^2 = 1^3 + 3 \) so \((1, 2) \) has infinite order and \( E(\mathbb{Q}) \) has an infinite number of points.

**Ex** \( E : y^2 = x^3 - 43x + 166, \ D = 912^{15} \cdot 13 \). Exploring small integers \((x, y) \in \mathbb{Z}^2 \) we find \( P = (3, 8) \in E \). Using the point doubling formula above the \( x \)-coordinates of \( 2P, 4P, \ldots \) are \( x(P) = 3, \ x(2P) = -5, \ x(4P) = 11, \ x(8P) = 3 \) so \( x(P) = x(8P) \Rightarrow 8P = \pm P \) so \( P \) is a point of finite order.

Since \( 3 \nmid 2D \), by the Reduction Theorem, \( T \) is isomorphic to a subgroup of \( E(\mathbb{Z}_3) \). \( \#E(\mathbb{Z}_3) = 7 \) so \( \#(T) = 1 \) or 7. But \( 0 \in T \) and so does \( P = (3, 8) \) so \( \#(T) = 7 \). The only abelian group of order 7 is \( \mathbb{Z}_7 \), a cyclic group generated by \( P \) (which must be of order 7 since its order divides 7). Computing \( \{0, P, 2P, 3P, 4P, 5P, 6P\} \) we get

\[
T = \{0, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}.
\]

**Congruent Number Problem**
Find a simple test to determine whether or not $n \in \mathbb{N}$ is the area of a right triangle, all of whose sides are of $\mathbb{Q}$ length.

Ex

\[ 6 = \frac{1}{2} \cdot 3 \cdot 4 \text{ so } 6 \text{ is congruent.} \]

Ex Fermat $n = 1$ is not congruent. ($X^4 + Y^4 \neq Z^4 \forall X, Y, Z \in \mathbb{Z}$).

Ex Euler $n = 7$ is congruent.

\{1, 2, 3, 4\} are not congruent but \{5, 6, 7\} are congruent.

Problem: Find a nice criteria to check $n$.

Theorem (Tunnell, 1983) Let $n$ be an odd square-free natural number. Then if $n$ is congruent, the number of triples satisfying $2x^2 + y^2 + 8z^2 = n$ is twice the number of triples $(x, y, z)$ satisfying $2x^2 + y^2 + 32z^2 = n$.

Let $n$ be square-free and let $X, Y, Z \ (X < Y < Z)$ be sides of a right triangle with area $n$. The number $n \in \mathbb{N}$ is fixed.
So \( n = \frac{1}{2}XY, \ x^2 + Y^2 = Z^2. \)

**Proposition** There is a 1-1 correspondence between the right triangles given above and rational numbers \( x \) for which \( x, x+n, x-n \) are each the square of a rational number. The correspondence is

\[
(X, Y, Z) \mapsto x = \left( \frac{Z}{2} \right)^2
\]

\[
x \mapsto X = \sqrt{x+n} - \sqrt{x-n}
Y = \sqrt{x+n} + \sqrt{x-n}
Z = 2\sqrt{x}
\]

In particular, \( n \) is congruent \( \Leftrightarrow \exists x \in \mathbb{Q}^+ \) such that \( x, x+n, x-n \) are squares of rational numbers.

**Proof.** \((\Rightarrow)\) Let \( X, Y, Z \in \mathbb{Q}^+ \) be a triple with \( n = \frac{1}{2}XY, \ X^2 + Y^2 = Z^2. \) Then \( X^2+Y^2 = Z^2 \) and \( 2XY = 4n \Rightarrow (X \pm Y)^2 = Z^2 \pm 4n \Rightarrow (1) \ (\frac{x \pm y}{2})^2 = (\frac{Z}{2})^2 \pm n = x \pm n \)

if \( x = (\frac{Z}{2})^2. \) So \( x, x \pm n \) are squares of rational numbers.

\((\Leftarrow)\) Given \( x, x \pm n \) being squares, then

\[
X = \sqrt{x+n} - \sqrt{x-n}
Y = \sqrt{x+n} + \sqrt{x-n}
Z = 2\sqrt{x}
\]

satisfy \( X < Y < Z \) and \( X, Y, Z \in \mathbb{Q}^+ \). Finally

\[
XY = (\sqrt{x+n} - \sqrt{x-n})(\sqrt{x+n} + \sqrt{x-n}) = (x+n) - (x-n) = 2n
\]

and

\[
X^2 + Y^2 = (x+n) + (x-n) - 2\sqrt{(x+n)(x-n)} + (x+n) + (x-n) + 2\sqrt{(x+n)(x-n)}
= 4x
= Z^2.
\]
Let \( n \) be a **congruent number**. By the above equation (1),
\[
\left( \frac{X \pm Y}{2} \right)^2 = \left( \frac{Z}{2} \right)^2 \pm \frac{n}{2}XY
\]

Multiply these two equations together:
\[
\left( \frac{X^2 - Y^2}{4} \right)^2 = \left( \frac{Z}{2} \right)^2 - \frac{n^2}{4}
\]

so \( v^2 = u^4 - n^2 \) has a rational solution \( v = \frac{x^2 - y^2}{4}, \ u = \frac{Z}{2} \). Now multiply by \( u^2 : u^6 - n^2u^2 = (uv)^2 \). Let \( x = u^2 = \left( \frac{Z}{2} \right)^2 \) (as before) and \( y = uv = (X^2 - Y^2)/Z/8 \) \( \Rightarrow \) a pair \( (x, y) \in \mathbb{Q}^2 \) satisfying \( y^2 = x^3 - n^2 \)—an elliptic equation \( (y^2 = x(x-n)(x+n)) \).

\[
\begin{align*}
\text{Hence if } n \text{ is congruent, the curve } y^2 &= x^3 - n^2x \text{ has a nontrivial rational point. The converse, that any point } (x, y) \in \mathbb{Q}^2 \text{ must come from such a triangle is false in general.}
\end{align*}
\]

We need extra conditions equivalent to \( \exists Q \in E_n(\mathbb{Q}) \) such that \( (x, y) = P = 2Q \) i.e. \( P \) is a (rational) point which is double a rational point.

**Theorem 32B** Let \( (x, y) \in \mathbb{Q}^2 \) be on \( y^2 = x^3 - n^2x \). Let \( x \) satisfy

(i) it is the square of a rational number,
(ii) its denominator is even,
(iii) its numerator is coprime with \( n \).

Then there is a right triangle with rational sides and area \( n \) under the correspondence of the above Proposition.

**Proof.** Let \( u = \sqrt{x} \in \mathbb{Q}^+ \) (i) and let \( v = \frac{y}{u} \in \mathbb{Q}^+ \). Since \( (x, y) \) is on \( E_n(\mathbb{Q}) : v^2 = \frac{y^2}{x} = x^2 - n^2 \Rightarrow v^2 + n^2 = x^2 \) (1). Let \( t \in \mathbb{N} \) be the denominator of \( u \), i.e. the smallest \( \hat{N} \) so \( tu \in \mathbb{Z} \). By (ii) \( t \) is even.

Because \( n \in \mathbb{N} \), the denominators of \( v^2 \) and \( x^2 \) are the same by (1), namely \( t^4 \).

Hence \( (t^2v)^2 + (t^2n)^2 = (t^2x)^2 \) is a primitive Pythagorean triple with \( t^2n \) even. (Primitive through (iii).) Hence \( \exists a, b \in \mathbb{Z} \) such that \( t^2n = 2ab, \ t^2v = a^2 - b^2, \ t^2x = a^2 + b^2 \). Then the right triangle with sides \( \frac{2a}{t}, \frac{2b}{t}, 2u \) has area \( \frac{1}{2} \cdot \frac{2a}{t} \cdot \frac{2b}{t} = \frac{2ab}{t^2} = n \). Finally, the image of this triangle with \( X = \frac{2a}{t}, \ Y = \frac{2b}{t}, \ Z = 2u \) is \( x = (\frac{Z}{2})^2 \) as required. \( \square \)
Ex (i) and (ii) alone are not sufficient: \( n = 5, \ x = \frac{25}{4}, \ y = \frac{75}{8} \) ⇒ \( X = \sqrt{x+n} - \sqrt{x-n} = \sqrt{5} \notin \mathbb{Q} \).

Back to Tunnell’s theorem \( n \) odd and square-free,

\[
\begin{align*}
n \text{ congruent} & \Rightarrow \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n\} \\
&= 2\#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = n\} (B) \\
(A) & \Rightarrow (B)
\end{align*}
\]

Then, subject to an unproved conjecture, \((B) \Rightarrow (A)\). We can confidently use \(\neg(B) \Rightarrow \neg(A)\).

Ex \(\#\{(x, y, z) : 2x^2 + y^2 + 8z^2 = n\} = \#\{(x, y, z) : 2x^2 + y^2 + 32z^2 = n\}\) if \(n < 8\). So none of \(\{1, 2, 3, 4, 5, 6, 7\}\) can be congruent unless the size of each set is \(O(2 \cdot 0 = 0)\). But \(x^2, y^2 \equiv 0, 1 \text{ or } 4 \pmod{8} \Rightarrow 2x^2 + y^2 + 8z^2 \equiv 5, 7 \pmod{8}\). So e.g. if \(n = 5\) or 7 both of the sets of triples are \(\emptyset\).

Ex The first congruent number \(n \equiv 1, 3 \pmod{8}\) is \(n = 41\):

If \((B) \Rightarrow (A)\) is true, the above argument would imply all of the following (odd, square-free) numbers are congruent, through \(2 \cdot 0 = 0\): \{5, 7, 13, 15, 21, 23, 29, 31, 37, 39, 47\}. 
10 Numbers Rational and Irrational

If $\alpha \in \mathbb{R}$ we say $\alpha \in \mathbb{Q}$ if $\alpha = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$.

**Proposition** $\sqrt{2} \notin \mathbb{Q}$.

**Proof.** Assume $\sqrt{2} \in \mathbb{Q}$

$$\Rightarrow \sqrt{2} = \frac{a}{b}, (a, b) = 1$$

$$\Rightarrow a = \sqrt{2}b$$

$$\Rightarrow a^2 = 2b^2 \Rightarrow 2|a^2 \Rightarrow 2|a$$

So $a = 2c$ and $4c^2 = 2b^2$

$$\Rightarrow 2c^2 = b^2 \Rightarrow 2|b^2 \Rightarrow 2|b$$

Hence $2|a$ and $2|b$ so $2|(a, b)$ so $(a, b) \neq 1$ (!!!). $\square$

We say $\sqrt{2}$ is irrational or $\sqrt{2} \in \mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.

We can generalise the above proposition to get a much wider family of irrational numbers:

**Theorem 29** If $x \in \mathbb{R}$ satisfies the equation

$$x^n + c_1x^{n-1} + \cdots + c_n = 0$$

where $c_i \in \mathbb{Z}$, then $x$ is either an integer or an irrational number.

**Proof.** Let $x \in \mathbb{Q}$ i.e. $x = \frac{a}{b}$, $b > 0$, $(a, b) = 1$. Then

$$a^n = -b(c_1a^{n-1} + c_2a^{n-2}b + \cdots + c_nb^{n-1})$$

If $b > 1$, then $p | b \Rightarrow p | a^n \Rightarrow p | a$ but then $p | (a, b)$ (!!!). Hence $b$ has no prime divisors, so $b = 1$. $\square$

**Corollary** If $m \in \mathbb{N}$ is not an $n^{th}$ power then $m^{1/n} = \sqrt[n]{m} \in \mathbb{I}$ since $\alpha = m^{1/n}$ satisfies $x^n - m = 0$.

**Trigonometric function values and $\pi$**

**Lemma 1** Let $g \in \mathbb{Z}[x]$ (i.e. a polynomial with integral coefficients). Let $h(x) = \frac{x^n g(x)}{n!}$.

If $j \neq n$, $h^{(j)}(0)$ is an integer divisible by $(n + 1)$. If $g(0) = 0, h^{(n)}(0)$ is an integer divisible by $(n + 1)$.

**Proof.** Let $x^n g(x) = c_n x^n + c_{n+1} x^{n+1} + \cdots + c_j x^j + \cdots$. Then $h^{(j)}(0) = \frac{c_j j!}{n!}$. If $j < n$, $c_j = 0$.

If $j > n$, $n + 1 | h^{(j)}(0)$ since $\frac{j!}{n!} = (n + 1)(n + 2) \cdots (j)$. If $j = n \Rightarrow h^{(j)}(0) = c_j \Rightarrow h^{(n)}(0) = c_n$ but $g(0) = 0 \Rightarrow x^n g(x) = x^n [g_1 x + g_2 x^2 + \cdots] = c_{n+1} x^{n+1} + \cdots \Rightarrow n + 1 | h^{(j)}(0)$. $\square$
Lemma 2 If $f(x)$ is a polynomial in $(r - x)^2$, then $f^{(j)}(r) = 0$ for any odd positive integer $j$ i.e. $f'(r) = 0$, $f''(r) = 0, \cdots$.

Proof.

\[
\begin{align*}
    f(x) &= g((r - x)^2) \\
    f'(x) &= -2(r - x)g((r - x)^2) \\
    f''(x) &= 2g((r - x)^2) + r(r - x)^2g((r - x)^2) \\
    f'''(x) &= -4(r - x)g((r - x)^2) - 8(r - x)^3g((r - x)^2) - 8(r - x)g((r - x)^2)
\end{align*}
\]

etc.

So $f^{(j)}(x)$ is a polynomial in odd powers of $(r - x)$ for odd $j$, $f^{(j)}(x) = h(r - x)$. Hence $h(r - x) = -h(x - r)$ like $(x - r), (x - r)^3, \cdots$ $\Rightarrow f^{(j)}(r) = h(0) = -h(0) \Rightarrow 2h(0) = 0 \Rightarrow h(0) = 0 \Rightarrow f^{(j)}(r) = 0$. □

Theorem 30 \(\pi\) is irrational, i.e. $\pi \in \mathbb{I}$.

Proof. Let $f(x) = \frac{x^n(1-x)^n}{n!}$ where $n \in \mathbb{N}$.

By Lemma 1 above, $\forall j, f^{(j)}(0) \in \mathbb{N}$ and $f(x) = f(1-x) \Rightarrow f^{(j)}(1) \in \mathbb{N}$. Since $0 < x < 1 \Rightarrow 0 < x^n < 1$ and $0 < 1 - x < 1 \Rightarrow 0 < (1-x)^n < 1$ we have $0 < f(x) < \frac{1}{n!} (1)$.

Let $\pi^2 = \frac{a}{b}, a \geq 1, b \geq 1, a, b \in \mathbb{N}$ (??). Let $F(x) = b^n[\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)]$. So $F(0) \in \mathbb{Z}$, $F(1) \in \mathbb{Z}$. Now

\[
\frac{d}{dx} \left\{ F'(x) \sin \pi x - \pi F(x) \cos \pi x \right\} = \left\{ F^{(2)}(x) + \pi^2 F(x) \right\} \sin \pi x
\]

\[
= b^n \pi^{2n+2} f(x) \sin \pi x
\]

\[
= \pi^2 a^n f(x) \sin \pi x
\]

So

\[
\begin{align*}
    \pi a^n \int_0^1 f(x) \sin \pi x \, dx &= \left[ \frac{F'(x) \sin \pi x}{\pi} - F(x) \cos \pi x \right]_0^1 \\
    &= F(1) + F(0) \in \mathbb{Z}.
\end{align*}
\]
But by (1),
\[ 0 < \pi a^n \int_0^1 f(x) \sin \pi x \, dx < \frac{\pi a^n}{n!} < 1 \] for \( n \geq n_0 \)
which is a contradiction. Hence \( \pi^2 \) is irrational. \( \square \)

**Corollary** \( \pi \) is irrational: If not \( \pi^2 \) would be rational.

**Note:** With a similar, but more complex proof, we can show \( r \in \mathbb{Q} \setminus \{0\} \Rightarrow \cos r \) is irrational.

**Corollary 1** to the note \( \pi \) is irrational, since if \( \pi \in \mathbb{Q} \), \( \cos \pi \in \mathbb{I} \) but \( \cos \pi = -1 \).

**Corollary 2** All trigonometric functions are irrational at non-zero rational values of their arguments.

**Proof.** \( r \in \mathbb{Q} \) and \( \sin r \in \mathbb{Q} \) \( \Rightarrow \) \( \cos 2r = 1 - 2\sin^2 r \in \mathbb{Q} \), which is false. Similarly, \( \tan r \in \mathbb{Q} \) \( \Rightarrow \) \( \cos 2r = \frac{1 - \tan^2 r}{1 + \tan^2 r} \in \mathbb{Q} \). \( \square \)

**Corollary 3** Any non-zero value of an inverse trigonometric function is irrational at rational values of the argument.

**Proof.** Let \( r \in \mathbb{Q} \) and \( \arccos r = \cos^{-1} r = s \). Suppose \( s \in \mathbb{Q} \) \( \Rightarrow \) \( \cos s = r \) which is false. \( \square \)

**Exponential, hyperbolic and logarithmic functions**

**Note:** \( e^0 = 1 \in \mathbb{Q} \) and \( \sinh 0 = 0 \), \( \cosh 0 = 1 \) but these are the only rational values at rational arguments. The proof is similar to Theorem 34 based on \( \cosh \):

**Corollary 4** \( e^r \in \mathbb{Q} \) \( \Rightarrow \) \( e^{-r} = \frac{1}{e^r} \in \mathbb{Q} \) \( \Rightarrow \) \( \frac{e^r + e^{-r}}{2} \in \mathbb{Q} \) but this is not possible if \( r \in \mathbb{Q} \).

**Theorem 31** \( e \) is irrational, \( e \in \mathbb{I} \).

**Proof.** Claim: \( \forall n \in \mathbb{N} \)
\[ 0 < e - \sum_{j=0}^{n} \frac{1}{j!} < \frac{1}{n \cdot n!} \] (1)

Represent \( e \) by an infinite series \( e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{j!} + \cdots \) so
\[ e - \sum_{j=0}^{n} \frac{1}{j!} = \sum_{j=n+1}^{\infty} \frac{1}{j!} > 0 \]
Also
\[ e - \sum_{j=0}^{n} \frac{1}{j!} = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots \]
\[ = \frac{1}{n!} \left[ \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots \right] \]
\[ < \frac{1}{n!} \left[ \frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots \right] \]
\[ = \frac{1}{n!} \left[ \frac{1}{1 - 1/(n+1)} \right] \text{ (sum of a geometric series } r = \frac{1}{n+1}) \]
\[ = \frac{1}{n! \cdot n} \]
which proves the claim.

Now let \( e = \frac{m}{n} \), \( m, n \in \mathbb{N}, \ (m, n) = 1 \), and assume \( n \neq 1 \). Let
\[ \eta = n! \left( e - \sum_{j=0}^{n} \frac{1}{j!} \right) \]
By (1)
\[ 0 < \eta < n! \cdot \frac{1}{n \cdot n!} = \frac{1}{n} \]
But
\[ \eta = n! \left( \frac{m}{n} - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{n!} \right) \in \mathbb{Z} \]
Hence \( e \) is irrational. \( \square \)

**Corollary** \( \sqrt{e} \) is irrational, since otherwise \( e = (\sqrt{e})^2 \) would be in \( \mathbb{Q} \).

**Question**: \( e \) seems to be ‘more’ irrational than \( \sqrt{2} \). We will explore families of irrational numbers below.

Let \( S \subset \mathbb{R} \) be a subset. We say \( S \) has **measure zero** if it is possible to cover \( S \) with a finite or countable set of intervals of arbitrarily small total length. Write \( \mu(S) = 0 \).

**Ex** \( S = \mathbb{N} \):
\[
1 \in \left( 1 - \frac{\varepsilon}{2}, 1 + \frac{\varepsilon}{2} \right)
\]
\[
2 \in \left( 2 - \frac{\varepsilon}{2^2}, 2 + \frac{\varepsilon}{2^2} \right)
\]
\[
j \in \left( j - \frac{\varepsilon}{2^j}, j + \frac{\varepsilon}{2^j} \right) = I_j
\]
So
\[
\mathbb{N} \subset \bigcup_{j=1}^{\infty} I_j
\]
and

\[ \ell(I_j) = \text{length of } I_j \]
\[ = j + \frac{\varepsilon}{2^j} - \left(j - \frac{\varepsilon}{2^j}\right) \]
\[ = \frac{2\varepsilon}{2^j} \]

Then

\[ \sum_{j=1}^{\infty} \ell(I_j) = 2\varepsilon \sum_{j=1}^{\infty} \frac{1}{2^j} = 2\varepsilon \]

which can be made arbitrarily small by choice of \( \varepsilon > 0 \). Hence \( \mu(\mathbb{N}) = 0 \). We can replace \( \mathbb{N} \) by any countable set \( A = \{a_n : n \in \mathbb{N}\} \subset \mathbb{R} \) by defining \( I_j = (a_j - \frac{\varepsilon}{2^j}, a_j + \frac{\varepsilon}{2^j}) \) since \( \ell(I_j) = \frac{2\varepsilon}{2^j} \).

**Definition** A property of real numbers is said to hold “almost everywhere” or to almost all numbers, if the set of numbers which do not have the property has measure zero.

**Ex** \( \mu(\mathbb{Q}) = 0 \) since \( \mathbb{Q} \) is countable. Hence almost all numbers are irrational.

**Note** We can count the numbers in \( \mathbb{Q}^+ \) via listing them and then counting the diagonals, skipping any already counted.
\[ Q^+ = \{ r_n : n \in \mathbb{N} \}. \]

Since \( \ell([0, 1]) = 1 > 0 \) and \([0, 1]\) and (hence) \( \mathbb{R} \) are not of measure 0. Hence, \textit{since the union of any two countable sets is countable}, the irrational numbers \( \mathbb{I} \) are not countable.

\textbf{Proof.} \textit{Let} \( A = \{ a_n : n \in \mathbb{N} \}, \ B = \{ b_n : n \in \mathbb{N} \} \Rightarrow A \cup B = \{ c_n : c_{2n} = a_n, c_{2n-1} = b_n, n = 1, 2, 3, \ldots \} \) \textit{so} \( A \cup B \) \textit{is countable}. \hfill \square

Now let \( S \subset \mathbb{R} \). We say \( S \) is \textbf{dense} in \( \mathbb{R} \) if \( \forall \alpha < \beta \ \exists x \in S \text{ with } \alpha < x < \beta \).

\textbf{Archimedian Axiom (AA)} \( \forall \varepsilon > 0 \ \exists n \in \mathbb{N} \text{ such that } 0 < \frac{1}{n} < \varepsilon \).

\textbf{Proposition} \( \mathbb{Q} \text{ is dense in } \mathbb{R} \).

\textit{Proof.} \textit{Let} \( \alpha < \beta \). \textit{By AA} \( \exists n \in \mathbb{N} \text{ such that } 0 < \frac{1}{n} < \beta - \alpha \). \textit{Let} \( m \in \mathbb{Z} \) \textit{satisfy} \( m < n \beta \leq m + 1 \). \textit{Then} \( \alpha < \beta - \frac{1}{n} \leq \frac{m+1}{n} - \frac{1}{n} = \frac{m}{n} \text{ and } \frac{m}{n} < \beta \). \textit{Hence} \( \alpha < \frac{m}{n} < \beta \) \textit{and we can let} \( x = \frac{m}{n} \). \hfill \square

\textbf{Proposition} \( \mathbb{I} \text{ is dense in } \mathbb{R} \).

\textit{Proof.} \textit{Let} \( \alpha, \beta \in \mathbb{R} \) \textit{have} \( \alpha < \beta \). \textit{Let} \( \alpha < \frac{m}{n} < \beta \) \textit{as above, and using AA choose} \( k \in \mathbb{N} \) \textit{so}

\[ 0 < \frac{1}{k} < \frac{\beta - \frac{m}{n}}{\sqrt{2}}. \]

\textit{Then} \( \alpha < \frac{m}{n} < \frac{m}{n} + \frac{\sqrt{2}}{k} < \beta \) \textit{and} \( x = \frac{m}{n} + \frac{\sqrt{2}}{k} \in \mathbb{I} \). \hfill \square

\textbf{Definition} \textit{A number is} \textbf{algebraic} \textit{if it satisfies an equation}

\[ x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0 \]

\textit{with} \( a_i \in \mathbb{Q} \).
Ex $\sqrt{2}$ satisfies $x^2 - 2 = 0$.

The unique polynomial with leading coefficient 1 (called monic) in $\mathbb{Q}[x]$ of minimal degree which has a given algebraic number $\alpha$ as a root is called the minimal polynomial of $\alpha$, and the degree of this polynomial is called the degree of $\alpha$.

The set of all algebraic numbers is called $\mathbb{A} \subset \mathbb{R}$.

**Proof.** If $\mathbb{A}_n$ is the set of algebraic numbers of degree $n$ for $n = 1, 2, 3, \ldots$ then

$$\mathbb{A} = \bigcup_{n=1}^{\infty} \mathbb{A}_n$$

There are a countable number of polynomials of degree $n$ with $\mathbb{Q}$ coefficients since $p(x) = x^n + a_1x^{n-1} + \cdots + a_n \leftrightarrow (a_1, \ldots, a_n) \in \mathbb{Q}^n$ and the latter is a countable set.

But each polynomial has at most $n$ roots in $\mathbb{R} \Rightarrow \mathbb{A}_n$ is countable. To complete the proof we need to assume that a countable union of countable sets is countable. To see this, use the diagonal counting trick:

$$\begin{align*}
\mathbb{A}_1 &= \{a_{11}, a_{12}, a_{13}, \ldots\} \\
\mathbb{A}_2 &= \{a_{21}, a_{22}, a_{23}, \ldots\} \\
\mathbb{A}_3 &= \{a_{31}, a_{32}, a_{33}, \ldots\} \\
&\vdots
\end{align*}$$

□

Since $\mu(\mathbb{A}) = 0$, almost all numbers are not algebraic. We call these numbers transcendental and the set of all such numbers $T = \mathbb{R} \setminus \mathbb{A}$.

Ex

$$\frac{2^{1/3} + \sqrt{2}}{\sqrt{3}} \in \mathbb{A}, \quad \pi \text{ and } e \in T$$

The former is not difficult, but $\pi$ and $e$ are both very difficult.

Both $\mathbb{Q}$ and $\mathbb{I}$ (and $T$) are dense in $\mathbb{R}$. This implies each real number can be expressed as the limit of rational numbers: Let $\alpha \in \mathbb{R}$ then give $n \in \mathbb{N}$ $\exists r_n \in \mathbb{Q}$ with $\alpha - \frac{1}{n} < r_n < \alpha + \frac{1}{n}$ so $|\alpha - r_n| < \frac{1}{n} \Rightarrow \alpha = \lim_{n \to \infty}$. But this universal fact gives little insight into the difference between $\mathbb{Q}$, $\mathbb{A}$ and $T$.

**Definition** A real number $\alpha$ is said to be approximable by rationals to order $n \in \mathbb{N}$
if \( \exists \) a constant \( C = C(\alpha) > 0 \) such that the inequality

\[
\left| \alpha - \frac{h}{k} \right| < \frac{C}{kn}
\]

has infinitely many rational solutions \( \frac{h}{k} \) where \( k > 0, (h, k) = 1 \).

**Note** Approximable to order 3 \( \Rightarrow \) Approximable to order 2 and 1.

**Theorem 32** If \( \alpha \in \mathbb{I} \), \( \exists \) infinitely many \( \frac{h}{k} \in \mathbb{Q} \) with

\[
\left| \alpha - \frac{h}{k} \right| < \frac{1}{k^2}
\]

i.e. \( \alpha \) is approximable to order 2.

**Proof.** See page 75. If \( \alpha \in \mathbb{I} \) its continued fraction expansion is infinite so the set of convergents \( \frac{p_n}{q_n} \) is infinite and

\[
\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}
\]

so we can let \( \frac{h}{k} = \frac{p_n}{q_n} \).

**OR** Let \( n \in \mathbb{N} \). Consider the \( n + 1 \) real numbers

\[
S = \{0, \alpha - \lfloor \alpha \rfloor, 2\alpha - \lfloor 2\alpha \rfloor, \ldots, n\alpha - \lfloor n\alpha \rfloor\}
\]

and their distribution in the intervals \( \frac{j}{n} \leq x < \frac{j+1}{n}, \ j = 0, \ldots, n \) which cover \([0, 1)\), so contain all of the numbers in \( S \). Hence (by the Dirichlet pigeon-hole principle) two numbers lie in the same interval, say \( 0 \leq n_1 < n_2 \leq n \), \( n_1\alpha - \lfloor n_1\alpha \rfloor, n_2\alpha - \lfloor n_2\alpha \rfloor \in \left[ \frac{j}{n}, \frac{j+1}{n} \right) \). The length of this interval is \( \frac{1}{n} \) so

\[
\left| (n_2\alpha - \lfloor n_2\alpha \rfloor) - (n_1\alpha - \lfloor n_1\alpha \rfloor) \right| < \frac{1}{n}
\]

Let \( k = n_2 - n_1 \) and \( h = \lfloor n_2\alpha \rfloor - \lfloor n_1\alpha \rfloor, k \in \mathbb{N}, h \in \mathbb{Z} \). so \( |k\alpha - h| < \frac{1}{n} \) and

\[
|\frac{k}{k}| < \frac{1}{nk} \leq \frac{1}{k^2}.
\]

Suppose there were only a finite number of such pairs \((h, k)\) : \((h_1, k_1), \ldots, (h_r, k_r)\). Let

\[
\varepsilon = \min \left\{ \left| \alpha - \frac{h_1}{k_1}\right|, \ldots, \left| \alpha - \frac{h_r}{k_r}\right| \right\} > 0.
\]

Use AA to find \( n \in \mathbb{N} \) with \( 0 < \frac{1}{n} < \varepsilon \) so \( \exists h, k \) by (1) so \( |\alpha - \frac{h}{k}| < \frac{1}{nk} \leq \frac{1}{n} < \varepsilon \) so \( \frac{h}{k} \neq \frac{h_i}{k_i} \)

(**!!). □

**Theorem 33** Any rational number is approximable to order 1, but not to any higher order.
Proof. Let $\alpha = \frac{a}{b}$, $(a, b) = 1, b \geq 1$ be rational. Then there are infinitely many solutions $(x, y)$ to $ax - by = 1$ ($x = x_0 + bt, \ y = y_0 + at, \ t \in \mathbb{Z}$ if $(x, y)$ is one solution) and infinitely many with $x > 0$. Then

$$ax - by = 1 \Rightarrow \left| \frac{a}{b} - \frac{y}{x} \right| = \frac{1}{bx} < \frac{2}{x}$$

Hence $\alpha$ is approximable to order 1.

If $\frac{b}{x} \in \mathbb{Q}$ and $\frac{b}{x} \neq \frac{a}{b}$ then

$$\left| \frac{a}{b} - \frac{y}{x} \right| = \left| \frac{ax - by}{bx} \right| \geq \frac{a}{bx}$$

there is no constant $C$ such that $\frac{1}{bx} < \frac{C}{x^2}$ for infinitely many $x \in \mathbb{N}$. Hence $\frac{a}{b} = \alpha$ is not approximable to any order higher than 1. $\square$

**Ex** $\xi = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots + \frac{1}{10^{2m+1}} + \cdots \in \mathbb{I}$. Let $r_m = (m + 1)^{th}$ partial sum of $\xi$, $r_m \in \mathbb{Q}$. $|\xi - r_m| = 10^{-2^{m+1}} + 10^{-2^{m+2}} + \cdots < 2 \cdot 10^{-2^{m+1}} = 2(10^{-2^m})^2$. $r_m = \frac{a}{10^{2m}}, \ a_n \in \mathbb{N}$. So this inequality shows we can approximate $\xi$ to order 2 at least. Hence $\xi \notin \mathbb{Q} \Rightarrow \xi \in \mathbb{I}$. 