To ask for $671^{-1} \in \mathbb{Z}_{911}$ is to ask for an integer $x$ such that $671x$ is one more than a multiple of 911, that is, to ask for integers $x, y$ such that $671x + 911y = 1$. This is an example of a (linear) Diophantine equation named after a Greek mathematician Diophantus of the 5th century AD who wrote a book on the solution of equations in integers.

We have seen that we can calculate $671^{-1} \in \mathbb{Z}_{911}$ by at most 911 calculations. The equivalent formulation of the problem, solve $671x + 971y = 1$ in $\mathbb{Z}$, has one negative feature, at least on the surface. It would seem that we have translated a finite calculation (albeit 911 multiplications) into a form which might appear to be an infinite problem. Though 911 is a large number, it’s smaller than infinity!

In this lecture, we will consider the solution of linear Diophantine equations in two variables $ax + by = c$. We want to know: Are there integers $x$ and $y$ on this straight line in the plane? Can a straight line in the plane avoid all points with integer coordinates? Well, of course that is possible. It seems clear that the line $ex + \pi y = \sqrt{2}$ has no integer solutions (and that is true). Here however, we only want to think about equations $ax + by = c$ with integer coefficients $a, b, c$. Can such a line avoid all integers points?

The answer is again, yes. For example, the line $2x + 4y = 7$ has no integer solutions, because if there were any, the left hand side would be even while the right hand side is odd. Similarly, the line $3x + 9y = 7$ has no integer solutions because the lhs is a multiple of 3 while the rhs is not. Hence we can agree:

Remark 1. If $ax + by = c$ with $a, b, c \in \mathbb{Z}$ in which $d = (a, b)$ does not divide $c$, then there are no integer solutions.

For obviously if there were integers $x, y$ such that $ax + by = c$, then $d|a, b, ax, by$ and so $d|ax + by = c$.

What if $d = (a, b)$ does divide $c$?

First to make the problem a bit simpler, we’ll divide $d$ out. So if $d = (a, b)|c$ then $a = Ad$, $b = Bd$ and $c = Cd$ for integers $A, B, C$ and so we have $Ax + By = C$ with integers $A, B, C$. It is an easy exercise to show that when you remove the gcd of $a$ and $b$ to get integers $A$ and $B$, then the gcd $(A, B) = 1$.

Hence we are now facing an equation $Ax + By = C$ with integer coefficients $A, B, C$ and $(A, B) = 1$, which of course divides $C$!

Remark 2: Given $Ax + By = C$ with $(A, B) = 1$, then there always exists integers $x$ and $y$ which satisfy $Ax + By = C$.

The proof of this remark is not difficult. Apply Euclid’s Algorithm to the integers $A$ and $B$ and then read it backwards or apply a Magic Table to it.
Since the gcd \((A, B) = 1\), we find integers \(u\) and \(v\) such that \(Au + Bv = 1\).

Now multiply by \(C\). We get \(AuC + BvC = C\) and we have found integers \(x = uC\) and \(y = vC\) such that \(Ax + By = C\). This completes a proof of Remark 2.

Remark 3. There are always infinitely many solutions \(x, y \in \mathbb{Z}\) of the equation \(Ax + By = C\) when \(A, B, C \in \mathbb{Z}\) and \((A, B) = 1\).

Here is a proof of this. Suppose we have found a solution \((x_1, y_1)\) of \(Ax + By = C\). Then we know \(Ax_1 + By_1 = C\).

Hence \(Ax_1 + ABk - ABk + By_1 = C\) and so \(A(x_1 + Bk) + B(y_1 - Ak) = C\) for any integer \(k\). Hence we have found infinitely many pairs which solve \(Ax + By = C\), namely \(x = x_1 + Bk, y = y_1 - Ak\) for any integer \(k\).

We are now close to

**Theorem 2.** Suppose we have \(ax + by = c\) with \(a, b, c \in \mathbb{Z}\).

(i) If \(d = (a, b) \nmid c\), then there are no integer solutions \(x, y\).

(ii) If \(d = (a, b) \mid c\), there are *always* infinitely many integer solutions \(x, y\) (and we can find them using Euclid’s Algorithm).

This almost completes the story. There is more to do however. I say that suppose we have a visiting mathematician from Mars or Marrickville, who looks at our equation \(ax + by = c\) and our solutions and says to us. That’s good, but I have a secret method not known to you which gives me this solution \((2012, -4763)\), say. We need to be able be sure that in spite of the fact that he has a different approach, we have found all his solutions including \((2012, -4763)\) and our method hasn’t missed any. How can we be sure of that?

**Theorem 3.** If \(ax + by = c\) with \(a, b, c \in \mathbb{Z}\) and \((a, b) \mid c\) and if we can find a solution \((x_1, y_1)\), then the set of all integer points on this line is given by

\[
\begin{align*}
x &= x_1 + \frac{b}{(a, b)} k, \\
y &= y_1 - \frac{a}{(a, b)} k,
\end{align*}
\]

for any integer \(k\).

Proof.

It is easy to see that each of these points \((x, y)\) lies on the line. For

\[
\begin{align*}
a(x_1 + \frac{b}{(a, b)} k) + b(y_1 - \frac{a}{(a, b)} k) &= ax_1 + by_1 + \frac{ba}{(a, b)} k - \frac{ab}{(a, b)} k \\\n&= c.
\end{align*}
\]

We only need to show that every point on the line has the above form \((x, y)\).

To do this we need two facts.
Fact 1. If \( d = (a, b) \), then \( \left( \frac{a}{d}, \frac{b}{d} \right) = 1 \). For if \( x \) is a positive divisor of \( \frac{a}{d} \) and also \( \frac{b}{d} \), then \( dx|a \) and also \( dx \) divides \( b \). But \( d \) is the greatest positive divisor of \( a \) and \( b \) and so \( ax \leq a, bx \leq b \). This implies that \( x = 1 \) and \( \left( \frac{a}{d}, \frac{b}{d} \right) = 1 \).

Fact 2. If \( x|ab \in \mathbb{Z} \) and \( (x, a) = 1 \), then \( x|b \). For if \( (x, a) = 1 \) applying Euclid’s Algorithm to \( x, a \) and reading it backwards, we have \( 1 = au + xv \), for some integers \( u, v \). But then, multiplying by \( b \) we get \( b = abu + bxv \). Since \( x|ab \) and \( x|bxv \), it follows that \( x \) divides \( abu + bxv = b \).

Now suppose that we have \( ax_1 + by_1 = c \) and we find any other solution \( (x, y) \).

Then we have
\[
ax_1 + by_1 = c \\
ax + by = c.
\]
Subtracting we have \( a(x_1 - x) + b(y_1 - y) = 0 \) and so
\[
a(x - x_1) = b(y_1 - y).
\]
Hence if \( d = (a, b) \),
\[
\frac{a}{d}(x - x_1) = \frac{b}{d}(y_1 - y).
\]
But by Fact 1, \( \left( \frac{b}{d}, \frac{a}{d} \right) = 1 \) and since \( \frac{b}{d} \) divides \( \frac{a}{d}(x - x_1) \) it follows by Fact 2, that \( \frac{b}{d} \) divides \( x - x_1 \) and so
\[
x - x_1 = \frac{b}{d} \ell,
\]
for some integer \( \ell \).

Similarly, \( \frac{a}{d} \) divides \( \frac{b}{d}(y_1 - y) \) and so \( \frac{a}{d} \) divides \( y_1 - y \). Thus
\[
y_1 - y = \frac{a}{d} m,
\]
for some integer \( m \).

Now
\[
x = x_1 + \frac{d}{b} \ell \\
y = y_1 - \frac{a}{d} m, \text{ and so} \\
c = ax + by
\]
\[
= a(x_1 + \frac{b}{d} \ell) + b(y_1 - \frac{a}{d} m) \\
= ax_1 + by_1 + \frac{ab}{d} \ell - \frac{ab}{d} m \\
= c + \frac{ab}{d} \ell - \frac{ab}{d} m \text{ and so} \\
\frac{ab}{d} \ell = \frac{ab}{d} m \text{ and} \\
\ell = m.
\]

This completes the proof of Theorem 3.