Tutorial 2

1. Find all possible solutions of the following Diophantine equation:

   \[ 407x + 946y = 143. \]

   \textbf{Solution.}

   Apply the Euclidean Algorithm to 407 and 946.

   \[ 946 = 2 \cdot 407 + 132 \]
   \[ 407 = 3 \cdot 132 + 11 \]
   \[ 132 = 12.11. \]

   Hence

   \[ 11 = 407 - 3.132 \]
   \[ = 407 - 3(946 - 2.407) \]
   \[ = 7.407 - 3.946. \]

   Hence

   \[ 143 = 11.13 = 91.407 - 39.946. \]

   Every solution can be written in the form:

   \[ x = 91 + \frac{946}{11}k, \quad y = -39 - \frac{407}{11}k, \]

   where \( k \in \mathbb{Z}. \)

   Hence every solution can be written in the form

   \[ x = 91 + 86k, \quad y = -39 - 37k, \]

   where \( 4 \in \mathbb{Z}. \)

2. Decide if the equation \( 317x + 419y = 21 \) can be solved in \( \mathbb{Z}. \) If it can, solve it.

   \textbf{Solution.}

   \[ 419 = 1.317 + 102 \]
   \[ 317 = 3.102 + 11 \]
   \[ 102 = 9.11 + 3 \]
   \[ 11 = 3.3 + 2 \]
   \[ 3 = 1.2 + 1 \]
   \[ 2 = 2.1 \]
So the gcd \((419, 317) = 1\), and 1 divides 21. Hence a solution exists.

This time we’ll apply a Magic Table:

\[
\begin{array}{cccccc}
1 & 3 & 9 & 3 & 1 & 2 \\
0 & 1 & 1 & 14 & 37 & 115 \\
1 & 0 & 1 & 3 & 28 & 87 \\
\end{array}
\]

Hence

\[317.152 - 115.419 = -1\]

and so, multiplying by \(-21\), we get

\[317.(-3192) + 419.(2415) = 21.\]

Every solution can be written in the form

\[x = -3192 + 419k, \quad y = 2415 - 317k,\]

where \(k\) is any integer.

3. Apply the Euclidean Algorithm to the numbers 377 and 233 in the usual way and then again allowing negative remainders, in order to have a remainder which is least in absolute value after each division. What do you notice?

Solution.

\[
\begin{align*}
377 &= 1.233 + 144 \\
233 &= 1.144 + 89 \\
144 &= 1.89 + 55 \\
89 &= 1.55 + 34 \\
55 &= 1.34 + 21 \\
34 &= 1.21 + 13 \\
21 &= 1.13 + 8 \\
13 &= 1.8 + 5 \\
8 &= 1.5 + 3 \\
5 &= 1.3 + 2 \\
3 &= 1.2 + 1 \\
2 &= 2.1.
\end{align*}
\]

Allowing negative remainders we have

\[
\begin{align*}
377 &= 2.233 - 89 \\
233 &= -3. - 89 - 34 \\
-89 &= 3. - 34 + 13 \\
-34 &= -3.13 + 5 \\
13 &= 3.5 - 2 \\
5 &= -3. - 2 - 1 \\
-2 &= 2. - 1.
\end{align*}
\]
This is obviously about half as long as the first. For other pairs of numbers, in general it will be best to choose sometimes a positive remainder and sometimes a negative remainder if we are to get a remainder of least absolute value after each division. So in general the speed of the algorithm is approximately doubled and in the case of Fibonacci numbers it is very nearly exactly twice as fast. I will finish with a Magic Table here to show you how it works.

\[
\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \\
0 & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 21 & 34 & 55 & 89 & 144 & 233 & 377 \\
1 & 0 & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 21 & 34 & 55 & 89 & 144 & 233 \\
\end{array}
\]

\[
\begin{array}{cccc}
2 & -3 & 3 & -3 \\
0 & 1 & 2 & -5 \\
1 & 0 & 1 & -3 \\
\end{array}
\]

13 -233 -237
-8 21 55 -144 -233

4. Evaluate the following fractions:

\[
1, \quad 1 + \frac{1}{3}, \quad 1 + \frac{1}{3 + \frac{1}{9}}, \quad 1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3 + \frac{1}{2}}}}
\]

\[
1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3 + \frac{1}{2}}}}, \quad 1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3 + \frac{1}{2}}}}
\]

**Solution.**

Use the Magic Table.

\[
\begin{array}{cccccccc}
1 & 1 & 3 & 9 & 3 & 1 & 2 \\
0 & 1 & 1 & 4 & 37 & 115 & 152 & 419 \\
1 & 0 & 1 & 3 & 28 & 87 & 115 & 317 \\
\end{array}
\]

The required values are thus

\[
1, \quad \frac{4}{3}, \quad \frac{37}{28}, \quad \frac{115}{87}, \quad \frac{152}{115}, \quad \frac{419}{317}.
\]

5. Suppose that \(a_1, a_2, \ldots, a_n\) are the partial quotients in the Euclidean Algorithm applied to two positive numbers \(a\) and \(b\). Define

\[
p_{-1} = 0, \quad p_0 = 1, \quad p_{k+1} = a_{k+1}p_k + p_{k-1}
\]

\[
q_{-1} = 1, \quad q_0 = 0, \quad q_{k+1} = a_{k+1}q_k + q_{k-1}.
\]

Show by induction on \(n\) that

(i) \(p_{n-1}q_n - p_nq_{n-1} = (-1)^{n-1}\)

(ii) \(p_{n-1}q_{n+1} - p_{n+1}q_{n-1} = (-1)^{n+1}a_{n+1}\).

**Solution.**

(i) Induction on \(n\).
If \( n = 0 \), then
\[
p_{-1}q_0 - p_0q_{-1} = 0.0 - 1.1 = -1 = (-1)^{0-1}.
\]
Suppose that
\[
p_{k-1}q_k - q_{k-1}p_k = (-1)^{k-1}.
\]
Consider
\[
p_kq_{k+1} - p_{k+1}q_k.
\]
Then
\[
p_kq_{k+1} - p_{k+1}q_k = p_k(a_{k+1}q_k + q_{k-1}) - (a_{k+1}p_k + p_{k-1})q_k
\]
\[
= p_kq_{k-1} - p_{k-1}q_k
\]
\[
= -(-1)^{k-1}, \text{ by induction}
\]
\[
= (-1)^k = (-1)^{k+1-1},
\]
as required. The result follows by induction.

(ii) Again use induction. If \( n = 0 \), then
\[
p_{-1}q_1 - p_1q_{-1} = 0.1 - a_1 = (-1)^3a_1.
\]
Suppose that
\[
p_{k-1}q_{k+1} - p_{k+1}q_{k-1} = (-1)^{k+1}a_{k+1}.
\]
Consider
\[
p_kq_{k+2} - p_{k+2}q_k.
\]
Then
\[
p_kq_{k+2} - p_{k+2}q_k = p_k(a_{k+2}q_{k+1} + q_k) - (a_{k+2}p_{k+1} + p_k)q_k
\]
\[
= a_{k+2}(p_kq_{k+1} - p_{k+1}q_k)
\]
\[
= a_{k+2}(-1)^k = (-1)^{k+2}a_{k+2},
\]
by the first part.

The result follows by induction for all \( n \).

6. (i) Show that \( x^{40} \equiv 1 \pmod{100} \), for every integer \( x \) with \( (x, 100) = 1 \).

(ii) Is this true if \( (x, 100) \neq 1 \)?

Solution.

(i) If \( x \equiv 1, 3, 7, 9 \pmod{10} \), then it is easy to show that \( x^4 \equiv 1 \pmod{10} \).
But then \( x^4 = 1 + 10k \), for some integer \( k \) and so
\[
x^{40} = (1 + 10k)^{10}
\]
\[
= 1 + 100k + \binom{10}{2}100k^2 + \binom{10}{3}1000k^3 + \ldots
\]
\[
\equiv 1 \pmod{100},
\]
since it is easy to see that 100 divides every term occurring in the expansion of \( (1 + 10k)^{10} \).

(ii) If \( (x, 100) \neq 1 \), then \( x \) is either divisible by 2 or by 5. In any case raising \( x \) to any power always produces an even integer or one which ends in 5.
It is clear that such an integer cannot end in 1.
7. Show that if $x^{-1}$ exists modulo $n$ if and only if $(x, n) = 1$.

Solution.

If $(x, n) = 1$, then by reading the Euclidean Algorithm backwards or otherwise, we have $1 = xu + nv$, for some integers $u, v$. Then $u$ is the inverse of $x$ modulo $n$.

Conversely, if $x$ has an inverse $u$ (mod $n$), then $xu \equiv 1$ (mod $n$) and so $xu - 1 = vn$, for some integer $v$. Then $(x, n)|x, xu, vn, xu + vn = 1$ and so $(x, n) = 1$.

8. Consider the following two steps in the Euclidean algorithm applied to $a, b$ with $a > b > 0$.

\[ a = bq_1 + r_1 \quad 0 \leq r_1 < b \]
\[ b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1 \]

(a) Show that if $r_1 \leq \frac{1}{2}b$, then $r_2 < \frac{1}{2}b$.

(b) Show that if $r_1 > \frac{1}{2}b$, then $q_2 = 1$ and so $r_2 < \frac{1}{2}b$.

(c) Hence show that $r_{2k} < \frac{1}{2^k}b$ for each $k$ and so $r_{2k} = 0$ when $k < \frac{2\ln b}{\ln 2} < 2.89 \ln b$. (Hence the algorithm terminates in less than $2.89 \ln b$ steps. So Euclid’s Algorithm for two numbers say with 100 digits (that is around $10^{100}$) will terminate in at most $2.89 \ln(10^{100}) = 2.89 \times 100 \ln 10 \leq 665$ steps.)

Solution.

\[ a = bq_1 + r_1 \quad 0 \leq r_1 < b \]
\[ b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1 \]

If $r_1 \leq \frac{1}{2}b$, then $r_2 < r_1 \leq \frac{1}{2}b$.

If $r_1 > \frac{1}{2}b$, then $r_1q_2 > 2r_1 > b$, if $q_2 \geq 2$. Since $r_1q_2 = b - r_1 \leq b$, we must have $q_2 = 1$. But then $b = r_1 + r_2$ and so $r_2 = b - r_1 < b - \frac{1}{2}b = \frac{1}{2}b$.

Finally the Euclidean Algorithm has the form

\[ a = bq_1 + r_1 \quad 0 \leq r_1 < b \]
\[ b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1 \]
\[ r_1 = r_2q_3 + r_3 \quad 0 \leq r_3 < r_2 \]
\[ r_2 = r_3q_4 + r_4 \quad 0 \leq r_4 < r_3 \]
\[ \vdots \]
\[ r_{n-2} = r_{n-1}q_n + r_n \quad 0 \leq r_n < r_{n-1} \]
\[ r_{n-1} = r_nq_{n+1}. \]

Now apply part (b) to the first two equations. We get $r_2 < \frac{1}{2}b$, while applying it to the third and fourth equations we get $r_4 < \frac{1}{2^2}b$.

Thus $r_4 < \frac{1}{2^2}b$. Similarly, $r_{2k} < \frac{1}{2^{2k}}b$.

If $k$ is such that $\frac{1}{2^k}b < 1$, then $r_{2k} = 0$, since $r_{2k} \geq 0$ and is an integer.
So the Algorithm terminates after $2k$ steps where $\frac{1}{2\pi} b < 1$. (It may terminate before this!)

Now $\frac{1}{2\pi} b < 1$ when $b < 2^k$, that is when $\ln b < k \ln 2$.

Hence $r_{2k} = 0$, when $2k > \frac{2 \ln b}{\ln 2} = 2.88539\ldots \ln b$. 