1. Show that there are infinitely many basic Pythagorean triples \((x, y, z)\) in which \(z - x = 2\) and list the first five.

**Solution**

We have \(x, y, z\) pairwise co-prime and \(x\) is odd, \(y\) is even and \(z\) is odd, in which there are integers \(a > b\) such that

\[
\begin{align*}
x &= a^2 - b^2 \\
y &= 2ab \\
z &= a^2 + b^2,
\end{align*}
\]

where \((a, b) = 1\).

Since \(z - x = 2b^2\) it follows that \(b = 1\). Now \(a\) and \(b\) are not both odd, because then \(z = a^2 + b^2\) is even. Hence \(a = 2A\) must be even. But then

\[
\begin{align*}
x &= 4A^2 - 1 \\
y &= 4A \\
z &= 4A^2 + 1.
\end{align*}
\]

This is a basic Pythagorean triple for any value of \(A\) and so there are infinitely many such.
2. (i) Find integers $u$ and $v$ such that $733u + Dv = 1$.

(ii) Given that $733 = (27 + 2i)(27 - 2i)$ find $D^{-1}$ modulo $27 + 2i$ in $\mathbb{Z}[i]$.

(iii) Write your answer $D = a + ib$ where $N(a + ib) \leq \frac{1}{2}N(27 + 2i)$.

**Solution**

(i) Suppose my $D = 75$. Then we have:

\[
\begin{align*}
733 &= 9.75 + 58 \\
75 &= 1.58 + 17 \\
58 &= 3.17 + 7 \\
17 &= 2.7 + 3 \\
7 &= 2.3 + 1 \\
3 &= 3.1
\end{align*}
\]


(ii) Hence $75(-215) = 1 + 733.22 = 1 + (27 + 2i)(27 - 2i)22$ and so $64(-215) \equiv 1 \pmod{27 + 2i}$.

Hence $D^{-1} = -215 \pmod{27 + 2i}$.

(iii) Calculate:

\[
\begin{align*}
\frac{-215}{27 + 2i} &= \frac{-215(27 - 2i)}{(27 + 2i)(27 - 2i)} \\
&= \frac{-5805 + 54i}{733} \\
&\approx -8.
\end{align*}
\]

Hence $D^{-1} = -215$ modulo $27 + 2i$.

Hence $-215 = -8(27 + 2i) + 1 + 16i$ and so $D^{-1} = -215 = 1 + 16i \in \mathbb{Z}[i]_{27+2i}$. Note that $N(1 + 16i) = 257 \leq \frac{1}{2}733$.

3. (i) List the elements of the ring $F = \mathbb{Z}_2[x]_{x^3 + x + 1}$ and find the inverses of each element if they exist.

(ii) Find a generator of $F^* = \mathbb{Z}_2[x]_{x^3 + x + 1}^*$ if it exists.
(iii) Show that \(x^7 = 1 \in \mathbb{F}\) and hence \(x = x^{-6} = (x^{-3})^2\). Hence find \(y \in \mathbb{F}\) such that \(y^2 = x\).

**Solution**

(i) \[
\begin{align*}
X & \quad 0 & 1 & x & x+1 & x^2 & x^2+1 & x^2+x & x^2+x+1 \\
X^{-1} & * & 1 & x^2+1 & x^2+x & x^2+x+1 & x & x+1 & x^2
\end{align*}
\]

Hence every non-zero element has an inverse and \(\mathbb{Z}_2[x]_{x^3+x+1}\) is a field with 8 elements.

(ii) Here are the powers of \(x\):

\[
\begin{array}{cccccccc}
n & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
x^n & x & x^2 & x+1 & x^2+x & x^2+x+1 & x^2+1 & x & \ldots
\end{array}
\]

Hence \(x\) is a generator. The generators are then \(x, x^2, x^3, x^4, x^5, x^6\).

(iii) It is clear that \(y = x^{-3} = (x^{-1})^3\) will do. Now from part (i), \(x^{-1} = x^2 + 1\). Hence

\[
y = (x^{-1})^3
= (x^2 + 1)^3
= x^6 + 3x^4 + 3x^2 + 1
= x^2 + 1 + x^2 + x + x^2 + 1
= x^2 + x.
\]

Check that \((x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + x + x^2 = x\).

4. (i) Explain why there is only one rational number \(\frac{p}{q}\) such that \(|\frac{p}{q} - \frac{1}{\sqrt{733}}| < \frac{1}{q^2}\) with \(q \geq D\).

(ii) Explain why there are infinitely many rational numbers \(\frac{p}{q}\) such that \(|\sqrt{733} - \frac{p}{q}| < \frac{1}{q^2}\) and find three such numbers.

(iii) Find non-zero integers \(x, y\) such that \(x^2 - 733y^2 = 1\).

**Solution**

(i) Suppose that \(\left|\frac{1}{D} - \frac{p}{q}\right| < \frac{1}{q^2}\) with \(q \geq D\). Then, multiplying by \(qD\) we have

\[
|q - pD| < \frac{D}{q}.
\]

But if \(q \geq D\), \(\frac{D}{q} \leq 1\) and so \(|q - pD| < \frac{D}{q} \leq 1\). But then \(q - pD\) is a non-negative integer < 1. Thus \(q - pD = 0\) and \(\frac{p}{q} = \frac{1}{D}\).

(ii) \(\sqrt{733} = [27, 13, 1, 1, 13, 54]\) and

\[
\begin{array}{cccccccc}
27 & 13 & 1 & 1 & 13 & 54 \\
0 & 1 & 27 & 352 & 379 & 731 & 9882 \\
1 & 0 & 1 & 13 & 14 & 27 & 365
\end{array}
\]

Convergents \(\frac{p}{q}\) of the form

\[
\frac{27}{1}, \frac{352}{13}, \frac{379}{14}, \ldots
\]
all satisfy the condition $\left| \frac{p}{q} - \sqrt{733} \right| < \frac{1}{q^2}$. Since $\sqrt{733}$ is irrational, the continued fraction for $\sqrt{733}$ is infinite and so there are infinitely many convergents from the Magic table.

(iii) From the Magic Table above:

$$9882^2 - 733.365^2 = -1.$$ To find integers $x, y$ such that $x^2 - 733y^2 = 1$, either continue the Magic Table one more cycle, or calculate as follows:

$$9882^2 - 733.365^2 = -1,$$ and so

$$(9882 - 365\sqrt{733})(982 + 365\sqrt{733}) = -1,$$ and squaring

$$(9882 - 365\sqrt{733})^2(9882 + 365\sqrt{733})^2 = 1$$

$$(9882^2 + 365^2.733 - 2.9882.365\sqrt{733})(9882^2 + 365^2.733 + 2.9882.365\sqrt{733}) = 1$$

$$(195307849 - 7213860\sqrt{733})(195307849 + 7213860\sqrt{733}) = 1$$

$$(195307849^2 - 7213860^2.733) = 1.$$ Hence two numbers such that $x^2 - 733y^2 = 1$ are $x = 195307849$ and $y = 7213860$