$y^2 = x^3 - 2$

Canonical name	Y2X32
Date of creation	2013-03-22 14:52:05
Last modified on	2013-03-22 14:52:05
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	10
Author	CWoo (3771)
Entry type	Application
Classification	msc 12D05
Classification	msc 11R04
Synonym	$y^2 + 2 = x^3$
Synonym	finding integer solutions to $y^2 + 2 = x^3$
Related topic	UFD

We want to solve the equation $y^2 = x^3 - 2$ over the integers.

By writing $y^2 + 2 = x^3$ we can factor on $\mathbb{Z}[\sqrt{-2}]$ as

$$(y - i\sqrt{2})(y + i\sqrt{2}) = x^3.$$

Using congruences modulo 8, one can show that both x, y must be odd, and it can also be shown that $(y - i\sqrt{2})$ and $(y + i\sqrt{2})$ are relatively prime (if it were not the case, any divisor would have even norm, which is not possible).

Therefore, by unique factorization, and using that the only `http://planetmath.org/UnitsOfQu` on $\mathbb{Z}[\sqrt{-2}]$ are $1, -1$, we have that each factor must be a cube.

So let us write

$$(y + i\sqrt{2}) = (a + bi\sqrt{2})^3 = (a^3 - 6ab^2) + i(3a^2b - 2b^3)\sqrt{2}$$

Then $y = a^3 - 6ab^2$ and $1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$. These two equations imply $b = \pm 1$ and thus $a = \pm 1$, from where the only possible solutions are $x = 3, y = \pm 5$.

References

[1] Esmonde, Ram Murty; *Problems in Algebraic Number Theory*. Springer.