Integral solutions of $x^2 \ + \ 4 \ = \ y^3$

In the seventeenth century P. de Fermat described all integral solutions of the Diophantine equations $x^2 + a = y^3$ where $a = 2$ or 4. A link to a proof for $a = 2$ is given in the online file `histmath11.pdf` (in the course directory). We shall use the same general ideas to prove Fermat's result for the case $a = 4$.

As in the case $a = 2$, the proof is based upon the fact that the Gaussian integers $\mathbb{Z}[i]$ form a principal ideal domain (and thus also a unique factorization domain).

Here are three basic facts about Gaussian integers which are helpful:

(1) $a + bi$ is divisible by $1 + i$ if and only if $a \equiv b \bmod 2$.

(2) If $y^3 = x^2 + 4$ then the greatest common divisor $(x + 2i, x - 2i)$ is equal to 1 if x is odd and $(1 + i)^3$ if x is even.

(3) If $y^3 = x^2 + 4$ then $(x + 2i) = i^n(a + bi)^3$ for some integers $n > 0$, a and b.

Derivation of (1). If $a + bi = (1 + i)(c + di)$ for some Gaussian integer $c + di$, then it follows by direct calculation that $a = c - d$ and $b = c + d$, so that $b - a = 2d$. Conversely, if $b - a$ is even, say $2d$, then if we take $c = a + d$ we can check that $a + bi = (1 + i)(c + di)$.■

Derivation of (2). Let Δ be a greatest common divisor of $x + 2i$ and $x - 2i$. Then Δ also divides their difference, which is $4i$ as well as their sum, which is $2x$. Since $(1 + i)^4 = -4$, it follows that up to a unit in $\mathbb{Z}[i]$ the greatest common divisor Δ is a power of $1 + i$; recall that the units in the Gaussian integers are just ± 1 and $\pm i$.

If x is odd, the preceding paragraph implies that Δ divides both 4 and $2x$, where x is odd. This means that Δ must be a power of $1 + i$ (note that $(1 + i)^2 = 2i$). If Δ were a positive power, then by **(1)** it would follow that $x \equiv 2 \bmod 2$; since x is assumed to be odd, this cannot happen, and therefore $x + 2i$ and $x - 2i$ must be relatively prime.

On the other hand, if x is even and we write $x = 2z$, then the equation $x^2 + 4 = y^3$ becomes $4(z^2 + 1) = y^3$. This implies that y must be even (otherwise 4 would not divide y^3), which in turn implies that 8 divides y^3 and hence 2 must divide $z^2 + 1$. Since the latter is even, it follows that z^2 and hence also z must be odd. By **(1)** we see that $1 + i$ must divide $z + i$, and since we have

$$2 \quad = \quad (1 + i)(1 - i) \quad = \quad (1 + i)^2 \cdot i^3$$

it follows that $(1 + i)^3$ must divide $x + 2i = 2z + 2i$. However, since $(1 + i)^4 = 4$ we also know that $(1 + i)^4$ does not divide $x + 2i$ (the imaginary part is not divisible by 4). By the initial paragraph of this derivation, it follows that $(1 + i)^3$ must be a/the greatest common divisor of $x \pm 2i$ if x is even.■

Derivation of (3). Write $x + 2i = u \cdot v \cdot \prod_j \ p_j^{r_j}$ where u is a unit in $\mathbb{Z}[i]$, while $v = 1$ if x is odd and $(1 + i)^3$ if x is even, and the p_j are inequivalent primes in the sense that none is equal to a unit times another in the list, and furthermore none of these primes are equivalent to $1 + i$. Taking conjugates, we see that $x - 2i = \overline{u} \cdot \overline{v} \cdot \prod_j \ \overline{p_j}^{r_j}$.

If x is odd, then by **(2)** we know that $x + 2i$ and $x - 2i$ are relatively prime, and therefore it follows that for all j and k the primes p_j and $\overline{p_k}$ are inequivalent in the sense of the previous paragraph, and furthermore none of these primes is equivalent to $1 + i$. Similarly, if x is even, then by **(2)** we know that the greatest common divisor of $x + 2i$ and $x - 2i$ is equal to $(1 + i)^3$

and $4 = -(1+i)^4$ divides neither. Furthermore, since $1 - i = i(1+i)$ we have $\overline{v} = i^3 v$, so that $x - 2i = i^3\,\overline{u}\cdot v\cdot \prod_j\ \overline{p_j}^{r_j}$. From this and **(2)** we can conclude as before that, if x is even, then for all j and k the primes p_j and $\overline{p_k}$ are still inequivalent in the sense of the previous paragraph.

The preceding discussion yields the following prime factorization in the Gaussian integers:

$$y^3 \quad = \quad (x+2i)(x-2i) \quad = \quad i^3\, u\overline{u}\cdot v^2 \cdot \prod_j\ p_j^{r_j}\cdot \prod_k\ \overline{p_k}^{r_k}$$

Since the left hand side is a perfect cube, it follows that each of the exponents r_j must be divisible by 3.

The final step of the argument is to compare the conclusion of the preceding sentence with the prime factorization for $x + 2i$ described earlier. We already knew that the units in $\mathbb{Z}[i]$ are the powers of i and v is a perfect cube, and now we also know that each term $p_j^{r_j}$ is also a perfect cube. By the unique factorization property for $\mathbb{Z}[i]$ this means that $\prod_j\ p_j^{r_j} = (a+bi)^3$ for some Gaussian integer $a + bi$.■

By the preceding observations we know that $x + 2i = i^n(a+bi)^3$ for some integers n, a, b with $n \geq 0$. Expanding the right hand side, we find that

$$x \ + \ 2i \quad = \quad i^n\Big((a^3 - 3ab^2) \ + \ (3a^2b - b^3)i \Big)\ .$$

This means that either $2 = \pm(3a^2b - b^3)$ or else $2 = \pm(a^3 - 3ab^2)$; note that these two cases are symmetric in a and b. We shall only consider the first of these cases because the other can be handled similarly by switching the roles of a and b throughout.

We know that $\pm 2 = 3a^2b - b^3 = b(3a^2 - b^2)$, and since both terms on the right hand side are integers it follows that either b equals ± 1 or ± 2. If $b = \pm 1$, then we obtain the equation $\pm 2 \ = \ \pm(3a^2 - 1)$, which implies that $a^2 = 1$. On the other hand, if $b = \pm 2$ then we obtain the equation $\pm 2 \ = \ \pm(6a^2 - 8)$, which once again implies that $a^2 = 1$.

By the preceding paragraph, the possibilities for a are ± 1 and the possibilities for b are ± 1 and ± 2. These imply that $x + 2i$ is equal to either $i^n(1 \pm i)^3$ or $i^n(1 \pm 2i)^3$ where n is some nonnegative integer, and if we simplify these expressions we see that $x + 2i$ must be either $i^n(-2 \pm 2i)$ or $i^n(-11 \pm 2i)$.

In the first cases we get that $y = 2$ and $x = \pm 2$, while in the second we get that $y = 5$ and $x = \pm 11$. Therefore the only positive integer solutions to the equation $x^2 + 4 = y^3$ are $x = y = 2$ and $x = 11,\ y = 5$.■