Units in quadratic number fields

A well-known problem in number theory is: Fix $a \in \mathbb{Z}$

Find all integer solutions $(m,n) \in \mathbb{Z}^2$

to $m^2 - an^2 = 1$

This is known as Pell's equation

Of course if $a \le -2$ then the only solutions are $(m,n) = (\pm 1, 0)$

If $a = -1$ the only solutions are $(m,n) = (\pm 1, 0)$ or $(m,n) = (0, \pm 1)$

If $a = 0$ then n is arbitrary and we can take $m = \pm 1$

~~But if~~ If $a = 1$ we must have $(m+n)(m-n) = 1$ giving $n = 0$ and $m = \pm 1$

$m = \pm 1$. Similarly if $a = b^2$, $b \in \mathbb{Z}$ then $n = 0$ and $m = \pm 1$

But if $a > 0$ and a is not the square of an integer

then there are infinitely many solutions. Why?

Because then $\mathbb{Z}[\sqrt{a}]$ is a commutative ring and

$\theta : m + n\sqrt{a} \longrightarrow m - n\sqrt{a}$ $(m, n \in \mathbb{Z})$ is a ring automorphism,

that is, an isomorphism of $\mathbb{Z}[\sqrt{a}]$ to itself.

So $\{m + n\sqrt{a} : m, n \in \mathbb{Z}, m^2 - an^2 = 1\}$ is closed under multiplication and is a group under multiplication. $m^2 - an^2 = 1$

$\Leftrightarrow m + n\sqrt{a}$ is a unit in $\mathbb{Z}[\sqrt{a}]$.

~~$m+n\sqrt{a}$ and $m - n\sqrt{a}$ have different~~ $|m + n\sqrt{a}| \ne |m - n\sqrt{a}|$

So ~~on~~ w.l.g. $|m + n\sqrt{a}| > 1$ and $|m - n\sqrt{a}| < 1$.

<u>Theorem</u> There are infinitely many solutions $(m,n) \in \mathbb{Z}^2$ to $m^2 - an^2 = 1$. In fact for each $N \in \mathbb{Z}_+$ $\exists\, (m,n) \in \mathbb{Z}^2$ s.t. $|m - \sqrt{a}\,n| < \frac{1}{N}$ and $m^2 - an^2 = 1$.

Proof The proof is surprisingly indirect. The first step is to fix N and consider $m, n \in \mathbb{N}$ with $m, n \leq N$

Then $|m + n\sqrt{a}| \leq (1+\sqrt{a})N$ $\quad |m - n\sqrt{a}| \leq |\sqrt{a}|N$

~~So the points $(m+n\sqrt{a}$~~, $m - n\sqrt{a}$) lie in the interval ~~rectangle~~ ~~[0, (1+\sqrt{a})N]~~ $\times [-\sqrt{a}N, N]$

and there are $(N+1)^2$ such points. So there are 2 points within $\frac{(\sqrt{a}+1)}{N}$ of each other $\quad |(m_1 - n_1\sqrt{a}) - (m_2 - n_2\sqrt{a})| \leq \frac{\sqrt{a}+1}{N}$

$|m_1 - m_2| \leq N \quad |n_1 - n_2| \leq N$ $\quad$ ~~$|(m_1-m_2) - (n_1-n_2)\sqrt{a}| \times |(m_1-m_2)+(n_1-n_2)\sqrt{a}|$~~

$$|(m_1 - m_2) - (n_1 - n_2)\sqrt{a}| \times |(m_1 - m_2) + (n_1 - n_2)\sqrt{a}| \leq |(\sqrt{a}+1)|^2$$

Put $m_N = (m_1 - m_2)$ and $n_N = n_1 - n_2$

$$|m_N^2 - n_N^2 a| \leq (\sqrt{a}+1)^2 \qquad |m_N + n_N\sqrt{a}| \leq N(\sqrt{a}+1)$$

$$|m_N - n_N\sqrt{a}| \leq \frac{\sqrt{a}+1}{N}$$

We never have $m - n\sqrt{a} = 0$. So there are infinitely many such (m_N, n_N). Since $\{m_N^2 - n_N^2 a\}$ is a sequence of bounded integers, one integer value must be taken infinitely often. So we can assume

$$m_N^2 - n_N^2 a = k \qquad \forall N, \text{ where } k \in \mathbb{Z} \setminus \{0\}.$$

Now to find just one unit, we only need find N_1 and N_2 with $(m_{N_1}, n_{N_1}) \neq \pm(m_{N_2}, n_{N_2})$ and

(1) $I_{N_1} = \{(p + q\sqrt{a})(m_{N_1} + n_{N_1}\sqrt{a}) : p, q \in \mathbb{Z}\} = \{(p+q\sqrt{a})(m_{N_2} + n_{N_2}\sqrt{a}) : p, q \in \mathbb{Z}\} = I_{N_2}$

that is, the principal ideals in $\mathbb{Z}[\sqrt{a}]$ generated by $m_{N_1} + n_{N_1}\sqrt{a}$ and $m_{N_2} + n_{N_2}\sqrt{a}$ are the same. For then $\exists\, p_1, q_1, p_2, q_2 \in \mathbb{Z}$ with $q_1, q_2 \neq 0$ and

$$m_{N_2} + n_{N_2}\sqrt{a} = (p_1 + q_1\sqrt{a})(m_{N_1} + n_{N_1}\sqrt{a}), \quad m_{N_1} + n_{N_1}\sqrt{a} = (p_2 + q_2\sqrt{a})(m_{N_2} + n_{N_2}\sqrt{a})$$

Then

$$m_{N_1} + n_{N_1}\sqrt{a} = (p_2+q_2\sqrt{a})(p_1+q_1\sqrt{a})(m_{N_2}+n_{N_2}\sqrt{a})$$

and $(p_2+q_2\sqrt{a})(p_1+q_1\sqrt{a}) = 1$

$q_1, q_2 \neq 0 \Rightarrow (p_2, q_2) = \pm(p_1, -q_1)$

and $p_1^2 - aq_1^2 = \pm 1$ $\quad q_1 \neq 0 \Rightarrow |p_1 + \sqrt{a}q_1| \neq \pm 1$

Then $(p_1+\sqrt{a}q_1)^k$ is a unit $\forall k \in \mathbb{Z}_+$

and if $p+\sqrt{a}q = (p_1+\sqrt{a}q_1)^k$ for any even k

$p^2 - aq^2 = 1$.

It remains to show (1) for some $(m_{N_1}, n_{N_1}) \neq \pm(m_{N_2}, n_{N_2})$

Since $m_N^2 - n_N^2 a = k$ $\forall N$ we have

$k \in I_{N}$ $\forall N$ and $m+n\sqrt{a} \in I_N$ if $m \equiv 0 \bmod k$ and $n \equiv 0 \bmod k$

I_N is closed under addition. ~~So it~~ If

$$J_N = \{m+n\sqrt{a} : m+n\sqrt{a} \in I_N,\ 0 < m,n < k\}$$

then $I_N = \{m'+n'\sqrt{a} : m' \equiv m \bmod k,\ n' \equiv n \bmod k,$ some $m+n\sqrt{a} \in J_N\}$

So $I_{N_1} = I_{N_2} \Leftrightarrow J_{N_1} = J_{N_2}$

But J_N is finite and there are only finitely many possibilities for J_N. So there must be ~~$N_1 \neq N$~~ N_1 and N_2 with $(m_{N_1}, n_{N_1}) \neq \pm(m_{N_2}, n_{N_2})$

and $J_{N_1} = J_{N_2}$ and $I_{N_1} = I_{N_2}$. $\square$.

<u>Theorem</u> ~~There~~ For $a \in \mathbb{Z}_+$, $a \geq 2$ and not an integer square, the units are of the form $\{\pm(p \pm q\sqrt{a})^k : k \in \mathbb{N}\}$ for some unit $p + q\sqrt{a}$.

<u>Proof</u> ~~If~~ There is $\delta > 0$ such that

$|(m + n\sqrt{a}) \pm 1| \geq \delta$ $\forall$ units $m + n\sqrt{a}$ with

$n \neq 0$. For $m - n\sqrt{a} = \pm(m + n\sqrt{a})^{-1}$

and if $|m + n\sqrt{a} \pm 1| < \delta$ then we also

have $|(m - n\sqrt{a}) \pm 1| < \dfrac{\delta}{1-\delta}$

and hence $|2n\sqrt{a}| \leq \dfrac{2\delta}{1-\delta}$ and $\sqrt{a} \leq \dfrac{\delta}{1-\delta}$

So now choose a unit $p + q\sqrt{a}$ such that

$1 < p + q\sqrt{a}$ and $p + q\sqrt{a} \leq m + n\sqrt{a}$ $\forall$ units $m + n\sqrt{a}$

with $m + n\sqrt{a} > 1$.

It suffices to show that if $m + n\sqrt{a}$ is a unit with $m + n\sqrt{a} > 1$ then $\exists\, k \in \mathbb{Z}_+$ s.t. $m + n\sqrt{a} = (p + q\sqrt{a})^k$.

Suppose not. Then $\exists\, k \in \mathbb{Z}_+$ st. $(p + q\sqrt{a})^k < m + n\sqrt{a} < (p + q\sqrt{a})^{k+1}$

and $1 < (m + n\sqrt{a})(p + q\sqrt{a})^{-k} < p + q\sqrt{a}$, contradicting the definition of $p + q\sqrt{a}$.