A refinement of Bezout's Lemma and elements of order 3 in some rational quaternion algebras

John Voight
Dartmouth College

joint work with
Donald Cartwright and Xavier Roulleau

2023 Joint Mathematics Meetings
AMS Special Session
Quaternions
7 January 2023

Bézout coefficients

Let $a, b \in \mathbb{Z}_{>0}$ have $\gcd(a, b) = 1$.

Theorem (~~Bézout~~ Bachet 1624)

There exist $u, v \in \mathbb{Z}$ such that $au - bv = 1$.

We call u, v **Bézout coefficients**.

What conditions can we put on the Bézout coefficients?

Given one solution (u_0, v_0), all solutions are parametrized by $t \in \mathbb{Z}$:

$$u = u_0 + bt$$
$$v = v_0 + at$$

So we may suppose that $u, v > 0$.

Moreover, we may choose u modulo m arbitrarily, if $\gcd(m, ab) = 1$.

Square Bézout coefficients

Can we suppose that $u = x^2$ and $v = y^2$ are squares ($x, y \in \mathbb{Z}$)? This is the Diophantine equation

$$ax^2 - by^2 = 1.$$

To solve with $x, y \in \mathbb{Q}$, we have the **Hilbert equation**, so we need

$$\left(\frac{a, -b}{\mathbb{Q}}\right) \simeq \mathrm{M}_2(\mathbb{Q})$$

which holds if and only if $(a, -b)_p = 1$ for all $p \mid d$ odd. (These give necessary, local conditions for a solution over $\mathbb{Z}$.)

Square Bézout coefficients

The Diophantine equation $ax^2 - by^2 = 1$ is a norm equation or not-quite-Pell equation.

Scaling gives

$$(ax)^2 - aby^2 = a.$$

Letting $d := ab > 1$, we solve

$$\mathrm{Nm}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(ax + \sqrt{d}y) = a.$$

Let

$$\mathfrak{a} = a\mathbb{Z} + \sqrt{d}\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}].$$

Then $\mathfrak{a}$ is an ideal, and

$$\begin{aligned}(ax)^2 - dy^2 = a &\Leftrightarrow ax + \sqrt{d}y \in \mathfrak{a} \text{ has norm } a \\ &\Leftrightarrow \mathfrak{a} = (ax + \sqrt{d}) \text{ is narrowly principal}\end{aligned}$$

so the obstruction to the integral local–global principle is found in the narrow class group $\mathrm{Cl}^+ \mathbb{Z}[\sqrt{d}]$.

Infinitely many solutions arise multiplying by $\mathbb{Z}[\sqrt{d}]^1 = \langle \eta \rangle$.

Norm Bézout coefficients

What about asking that u, v are norms from a quadratic extension?

We focus on a special case, specific to original motivation.

Let $\omega = \dfrac{-1+\sqrt{-3}}{2}$, so $\omega^2 + \omega + 1 = 0$. Consider the **Eisenstein integers** $\mathbb{Z}[\omega] \subseteq \mathbb{Q}(\omega)$. Let

$$L := \mathrm{Nm}_{\mathbb{Q}(\omega)|\mathbb{Q}}(\mathbb{Z}[\omega])$$

be the **Löschian numbers**. Explicitly,

$$\begin{aligned}\mathrm{Nm}(x+\omega y) &= x^2 - xy + y^2 = (x - y/2)^2 + 3y^2/4 \geq 0 \\ &= (x+y)^2 - 3xy \equiv 0, 1 \pmod 3.\end{aligned}$$

$L_{>0} := L \cap \mathbb{Z}_{>0}$ is closed under multiplication, generated by

$$\begin{aligned}&\{3\} \cup \{p : p \text{ prime with } p \equiv 1 \pmod 3\} \\ &\cup \{q^2 : q \text{ prime with } q \equiv 2 \pmod 3\}.\end{aligned}$$

Under what circumstances can we take the Bézout coefficients to be Löschian numbers?

Main result

Question

Under what circumstances can we take the Bézout coefficients to be Löschian numbers?

The answer is not always "yes". For $(a, b) = (5, 3)$, we have $5 \cdot 2 - 3 \cdot 3 = 1$ so the general solution is $(u, v) = (2 + 3t, 3 + 5t)$ and $u \notin L$.

But this is a minor inconvenience: we can solve with $(a, b) = (3, 5)$, e.g. $3 \cdot 7 - 5 \cdot 4 = 1$.

Theorem (Cartwright–Roulleau–V)

Let $a, b \in \mathbb{Z}_{>0}$ be coprime, $d := ab$. Then the following statements hold.

(a) *There exist infinitely many $u, v \in L$ such that $au - bv = \pm 1$.*

(b) *If $d \equiv 0, 2 \pmod 3$, then moreover $3 \nmid uv$.*

(If $d \equiv 1 \pmod 3$, we must have $3 \mid uv$.)

Quaternions!

We need to solve the Diophantine equation

$$a \operatorname{Nm}(\mu) - b \operatorname{Nm}(\nu) = a(t^2 - tx + x^2) - b(y^2 - yz + z^2) = \pm 1$$

for $\mu, \nu \in \mathbb{Z}[\omega]$. We recognize this a *quaternion* norm equation, or a not-quite-quaternion-Pell equation!

We rinse and repeat, but with quaternions!

Consider the (crossed product) quaternion order

$$\mathcal{O} := \mathbb{Z}[\omega] + \mathbb{Z}[\omega]j \subset B := \left(\frac{-3, d}{\mathbb{Q}}\right).$$

So $j\omega = \omega^2 j$. Then we solve

$$\operatorname{nrd}(a\mu + \nu) = a^2 \operatorname{Nm}(\mu) - d \operatorname{Nm}(\nu) = \pm a.$$

Quaternion order

Let $\mathcal{O} = \left(\dfrac{\mathbb{Z}[\omega], -d}{\mathbb{Z}}\right) \subset B = \left(\dfrac{-3, d}{\mathbb{Q}}\right)$.

We have $3 \neq p \in \operatorname{Ram} B$ if and only if $p \equiv 2 \pmod 3$ and $\operatorname{ord}_p(d)$ is odd.

The order $\mathcal{O}$ has $N := \operatorname{discrd} \mathcal{O} = 3d$ and is classified locally by $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and the $\mathbb{F}_p$-algebra $\overline{\mathcal{O}_p} := \mathcal{O}_p / \operatorname{rad}(\mathcal{O}_p)$:

- If $p \nmid N$, then $\mathcal{O}_p \simeq \mathrm{M}_2(\mathbb{Z}_p)$.
- If $p \mid N$ and $p \equiv 1 \pmod 3$, then $\mathcal{O}_p$ is residually split (Eichler, $\overline{\mathcal{O}_p} \simeq \mathbb{F}_p \times \mathbb{F}_p$).
- If $p \mid N$ and $p \equiv 2 \pmod 3$, then $\mathcal{O}_p$ is residually inert (Pizer, $\overline{\mathcal{O}_p} \simeq \mathbb{F}_{p^2}$).
- If $p = 3$, then $\mathcal{O}_3$ is hereditary (if $3 \nmid d$) or residually ramified ($\overline{\mathcal{O}_p} \simeq \mathbb{F}_p$, if $3 \mid d$).

Class number

Recall that the **(right) class set** $\operatorname{Cls}\mathcal{O}$ is the set of classes of invertible (equivalently, locally principal) right $\mathcal{O}$-ideals under the equivalence $I \sim J$ if and only if $I = \alpha J$ for some $\alpha \in B^\times$.

Proposition

$\#\operatorname{Cls}\mathcal{O} = 1$, *i.e., every invertible right* $\mathcal{O}$*-ideal is principal.*

Since B is indefinite, it satisfies strong approximation:

"ideal classes in $\operatorname{Cls}\mathcal{O}$
are determined by
their reduced norms (in a ray class group)"

Class number: idelic

$$\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \quad \text{(profinite completion of } \mathbb{Z}\text{)}$$

$$\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_p{}' \mathbb{Q}_p \quad \text{(finite adeles)}$$

$$\widehat{B} = B \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}$$

$$\widehat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}.$$

Then $\operatorname{Cls} \mathcal{O} = B^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times$ and

$$\operatorname{nrd}\colon B^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times \leftrightarrow \mathbb{Q}^\times \backslash \widehat{\mathbb{Q}}^\times / \operatorname{nrd} \widehat{\mathcal{O}}^\times =: G.$$

Then G is a class group of $\mathbb{Z}$.

From the local description, we have

$$\operatorname{nrd}(\widehat{\mathcal{O}}^\times) = \prod_p \operatorname{nrd}(\mathcal{O}_p^\times) \geq \mathbb{Z}_3^{\times 2} \prod_{p \neq 3} \mathbb{Z}_p^\times$$

so G admits a surjection from the ray class group of conductor 3 which is trivial, so $G = \{1\}$.

End of proof

We solve the Diophantine equation

$$\mathrm{nrd}(a\mu + \nu) = a^2(t^2 - tx + x^2) - d(y^2 - yz + z^2) = \pm a$$

with $a\mu + \nu \in \left(\dfrac{\mathbb{Z}[\omega], -d}{\mathbb{Z}}\right)$.

We consider

$$I := a\mathbb{Z}[\omega] + j\mathbb{Z}[\omega] \subseteq \mathcal{O}$$

an invertible (locally principal) right $\mathcal{O}$-ideal with $\mathrm{nrd}(I) = a\mathbb{Z}$.
Then $I = \alpha\mathcal{O}$ is principal, with $\mathrm{nrd}(\alpha) = \pm a$. ($\alpha$ is an *Atkin–Lehner involution*.)

We obtain infinitely many solutions multiplying by $\mathcal{O}^1$ (infinite, finitely generated: acts discretely and properly on the upper half-plane).

Applications and conclusion

Theorem (Cartwright–Roulleau–V)

Let $a, b \in \mathbb{Z}_{>0}$ be coprime, $d := ab$. Then there exist infinitely many $u, v \in L = \mathrm{Nm}(\mathbb{Z}[\omega])$ such that $au - bv = \pm 1$.

- $\#\,\mathrm{Cls}\,\mathcal{O} = 1$ also allows us to count elements of order 3 in $\mathcal{O}$ up to conjugation by $\mathcal{O}^\times$, using local embedding numbers (in an explicit manner).
  To $\gamma = t + x\omega + (y + z\omega)j \in \mathcal{O}^\times$ with order 3, we attach the pair $(a, b) = (\gcd(t, d), \gcd(t + 1, d))$.
- This counts the number of inequivalent ways of writing a generalized Kummer surface X in the form $\widetilde{A/G}$ for $\#G = 3$.
- Our theorem generalizes to other imaginary quadratic fields (in progress).