An Easy[1] Proof of Quadratic Reciprocity Using Algebraic Number Theory

Dillon Snyder

University of Connecticut, Storrs

December 15, 2022

[1] This is a matter of perspective

Background

Algebraic Integers: An element $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ where $f(\alpha) = 0$.

Background

Algebraic Integers: An element $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ where $f(\alpha) = 0$.

- $\sqrt{2}$ is an algebraic integer where $f(x) = x^2 - 2$ is the minimum polynomial
- $\frac{1+\sqrt{5}}{2}$ is an algebraic integer where $f(x) = x^2 - x - 1$ is the minimum polynomial
- $\frac{1}{\sqrt{6}}$ is not an algebraic integer (see $f(x) = 6x^2 - 1$ for intuition)

Background

Algebraic Integers: An element $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ where $f(\alpha) = 0$.

- $\sqrt{2}$ is an algebraic integer where $f(x) = x^2 - 2$ is the minimum polynomial
- $\frac{1+\sqrt{5}}{2}$ is an algebraic integer where $f(x) = x^2 - x - 1$ is the minimum polynomial
- $\frac{1}{\sqrt{6}}$ is not an algebraic integer (see $f(x) = 6x^2 - 1$ for intuition)

Ring of Integers: For K, a finite extension of $\mathbb{Q}$, $R \subset K$ is the set of all the elements in K that are algebraic integers.

Background

Algebraic Integers: An element $\alpha \in \mathbb{C}$ is an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ where $f(\alpha) = 0$.

- $\sqrt{2}$ is an algebraic integer where $f(x) = x^2 - 2$ is the minimum polynomial
- $\frac{1+\sqrt{5}}{2}$ is an algebraic integer where $f(x) = x^2 - x - 1$ is the minimum polynomial
- $\frac{1}{\sqrt{6}}$ is not an algebraic integer (see $f(x) = 6x^2 - 1$ for intuition)

Ring of Integers: For K, a finite extension of $\mathbb{Q}$, $R \subset K$ is the set of all the elements in K that are algebraic integers.

For $K = \mathbb{Q}(\sqrt{d})$ where d is square-free, $R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.
In $\mathbb{Z}[i]$, $(1+i)$ is prime because $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2$ which is a field.

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.
In $\mathbb{Z}[i]$, $(1+i)$ is prime because $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2$ which is a field.

Prime Factorization: Ideals in R factor uniquely into prime ideals.

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.
In $\mathbb{Z}[i]$, $(1+i)$ is prime because $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2$ which is a field.

Prime Factorization: Ideals in R factor uniquely into prime ideals.
In $\mathbb{Z}[i]$, $(5) = (1+2i)(1-2i)$.

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.
In $\mathbb{Z}[i]$, $(1+i)$ is prime because $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2$ which is a field.

Prime Factorization: Ideals in R factor uniquely into prime ideals.
In $\mathbb{Z}[i]$, $(5) = (1+2i)(1-2i)$.
In $\mathbb{Z}[\sqrt{10}]$,

- $(13) = (13, \sqrt{10}+6)(13, \sqrt{10}-6)$
- $(2) = (2, \sqrt{10})^2$
- (7) remains prime

Background

Prime Ideal: An ideal $P \subset R$ is prime if R/P is an integral domain.
In $\mathbb{Z}[i]$, $(1+i)$ is prime because $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2$ which is a field.

Prime Factorization: Ideals in R factor uniquely into prime ideals.
In $\mathbb{Z}[i]$, $(5) = (1+2i)(1-2i)$.
In $\mathbb{Z}[\sqrt{10}]$,

- $(13) = (13, \sqrt{10}+6)(13, \sqrt{10}-6)$
- $(2) = (2, \sqrt{10})^2$
- (7) remains prime

Prime Splitting: For two rings of integers $R \subset S$, primes in R may split into prime ideals in S.

Background

Theorem (Dedekind–Kummer)

If $R = \mathbb{Z}[\alpha]$, $f(x)$ is the minimal polynomial for α over $\mathbb{Z}$, and

$$f(x) = g_1(x)g_2(x)\cdots g_r(x) \bmod p$$

for some prime $p \in \mathbb{Z}$ where $g_i(x)$ are distinct monic irreducible polynomials, then

$$(p) = (p, g_1(\alpha))(p, g_2(\alpha))\cdots(p, g_r(\alpha))$$

where $(p, g_i(\alpha))$ are distinct prime ideals.

Example

For $\mathbb{Z}[\sqrt{10}]$,

$$x^2 - 10 = (x+6)(x-6) \bmod 13$$

so

$$(13) = (13, \sqrt{10}+6)(13, \sqrt{10}-6).$$

Background

Corollary

Let d be a square-free integer with $d \equiv 1 \bmod 4$ and $q \in \mathbb{Z}$ be an odd prime, $q \nmid d$. With R being the ring of integers of $\mathbb{Q}(\sqrt{d})$, we have

$$2R = \begin{cases} \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) & \text{if } d \equiv 1 \bmod 8 \\ \text{prime} & \text{if } d \equiv 5 \bmod 8 \end{cases}$$

and

$$qR = \begin{cases} (q, n+\sqrt{d})(q, n-\sqrt{d}) & \text{if } d \equiv n^2 \bmod q \\ \text{prime} & \text{if } d \text{ is not a square} \bmod q. \end{cases}$$

Example

Since $10 \equiv 14^2 \bmod 31$, we have in $\mathbb{Z}[\sqrt{10}]$

$$(31) = (31, 14+\sqrt{10})(31, 14-\sqrt{10})$$

Legendre Symbol

Definition

Let p be an odd prime in $\mathbb{Z}$. For $n \in \mathbb{Z}$ where $p \nmid n$, define the Legendre Symbol

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square} \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

Examples

- $\left(\frac{1}{3}\right) = 1$ because $1 \equiv 1^2 \bmod 3$
- $\left(\frac{2}{7}\right) = 1$ because $2 \equiv 3^2 \bmod 7$
- $\left(\frac{3}{11}\right) = 1$ because $3 \equiv 5^2 \bmod 11$
- $\left(\frac{17}{7}\right) = -1$ because $17 \equiv 3 \bmod 7$ and is not a square
- $\left(\frac{-8}{5}\right) = -1$ because $-8 \equiv 3 \bmod 5$ and is not a square

Properties

- $(\frac{1}{p}) = 1$
- If $m \equiv n \bmod p$, then $(\frac{m}{p}) = (\frac{n}{p})$
- $(\frac{mn}{p}) = (\frac{m}{p})(\frac{n}{p})$
- If $q \equiv 1 \bmod 4$, then $(\frac{-1}{q}) = 1$
- If $q \equiv 3 \bmod 4$, then $(\frac{-1}{q}) = -1$

Quadratic Reciprocity

Theorem

Let p be an odd prime in $\mathbb{Z}$. Then for odd primes q such that $q \neq p$, then

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \bmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Applications

Examples

- $\left(\frac{2}{137}\right) = 1$ because $137 \equiv 1 \bmod 8$. Note: $2 \equiv 31^2 \bmod 137$
- $\left(\frac{5}{11}\right) = 1$ because $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$ since $5 \equiv 1 \bmod 4$. Note: $5 \equiv 4^2 \bmod 11$
- $\left(\frac{2}{41851}\right) = -1$ because $41851 \equiv 3 \bmod 8$
- $\left(\frac{21}{83}\right) = 1$ because $\left(\frac{21}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{7}{83}\right) = 1$ since $7 \equiv 83 \equiv 3 \bmod 4$. Note: $21 \equiv 41^2 \bmod 83$
- $\left(\frac{10}{29}\right) = -1$ because $\left(\frac{10}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{5}{29}\right) = -\left(\frac{29}{5}\right) = -\left(\frac{4}{5}\right) = -1$ because $29 \equiv -3 \bmod 8$ and $5 \equiv 1 \bmod 4$

Proof of Quadratic Reciprocity

Lemma

Let p be an odd prime. Set

$$p^* = \pm p \text{ so that } p^* \equiv 1 \bmod 4.$$

For any odd primes $q \neq p$, in the ring of integers of $\mathbb{Q}(\sqrt{p^*})$, we have

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2}$$

$$\boxed{\left(\frac{q}{p}\right) = -1 \text{ otherwise.}}$$

q is any odd prime

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2}$$

$$\boxed{\left(\frac{q}{p}\right) = -1 \text{ otherwise.}}$$

Recall from the Corollary:

$$\text{qR} = \begin{cases} (q, n+\sqrt{p^*})(q, n-\sqrt{p^*}) & \text{when } p^* \equiv n^2 \bmod q \\ \text{prime} & \text{when } p^* \not\equiv n^2 \bmod q \end{cases}$$

q is any odd prime

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2}$$

$$\boxed{\left(\frac{q}{p}\right) = -1 \text{ otherwise.}}$$

Recall from the Corollary:

$$\text{qR} = \begin{cases} (q, n+\sqrt{p^*})(q, n-\sqrt{p^*}) & \text{when } p^* \equiv n^2 \bmod q \\ \text{prime} & \text{when } p^* \not\equiv n^2 \bmod q \end{cases}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \iff \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4 \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

q is any odd prime

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2}$$

$$\boxed{\left(\frac{q}{p}\right) = -1 \text{ otherwise.}}$$

Recall from the Corollary:

$$\text{qR} = \begin{cases} (q, n+\sqrt{p^*})(q, n-\sqrt{p^*}) & \text{when } p^* \equiv n^2 \bmod q \\ \text{prime} & \text{when } p^* \not\equiv n^2 \bmod q \end{cases}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \iff \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4 \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

$$\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } q \equiv 3 \bmod 4 \end{cases}$$

q is any odd prime

$$\boxed{\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2}$$

$$\boxed{\left(\frac{q}{p}\right) = -1 \text{ otherwise.}}$$

Recall from the Corollary:

$$\text{qR} = \begin{cases} (q, n+\sqrt{p^*})(q, n-\sqrt{p^*}) & \text{when } p^* \equiv n^2 \bmod q \\ \text{prime} & \text{when } p^* \not\equiv n^2 \bmod q \end{cases}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \iff \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4 \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

$$\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } q \equiv 3 \bmod 4 \end{cases}$$

$$\implies \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

$q = 2$

$$\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2$$

$$\left(\frac{q}{p}\right) = -1 \text{ otherwise.}$$

Recall from the Corollary:

$$2R = \begin{cases} \left(2, \frac{1+\sqrt{p^*}}{2}\right)\left(2, \frac{1-\sqrt{p^*}}{2}\right) & \text{when } p^* \equiv 1 \bmod 8 \\ \text{prime} & \text{when } p^* \equiv 5 \bmod 8 \end{cases}$$

$q = 2$

$$\left(\frac{q}{p}\right) = 1 \iff (q) = \mathfrak{p}_1\mathfrak{p}_2 \text{ where } \mathfrak{p}_1 \neq \mathfrak{p}_2$$

$$\left(\frac{q}{p}\right) = -1 \text{ otherwise.}$$

Recall from the Corollary:

$$2R = \begin{cases} \left(2, \frac{1+\sqrt{p^*}}{2}\right)\left(2, \frac{1-\sqrt{p^*}}{2}\right) & \text{when } p^* \equiv 1 \bmod 8 \\ \text{prime} & \text{when } p^* \equiv 5 \bmod 8 \end{cases}$$

$$\iff \left(\frac{2}{p}\right) = 1 \text{ when } p^* \equiv 1 \bmod 8 \text{ and } \left(\frac{2}{p}\right) = -1 \text{ when } p^* \equiv 5 \bmod 8.$$

$$\text{Thus, } \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

∎

References

K. Conrad, (2020)
Algebraic Number Theory

D. Marcus, (2018)
Number Fields
Springer