A QUICK ROUTE TO UNIQUE FACTORIZATION IN QUADRATIC ORDERS

PAUL POLLACK AND NOAH SNYDER

Abstract. We give a short proof — not relying on ideal classes or the geometry of numbers — of a known criterion for quadratic orders to possess unique factorization.

1. Introduction.

Let D be a quadratic discriminant, meaning that D is a nonsquare integer with $D \equiv 0, 1 \pmod 4$. Set $D = 4d + \sigma$, where $\sigma \in \{0, 1\}$, and let $\tau = \frac{\sigma+\sqrt{D}}{2}$. It is easy to check that $\tau^2 \in \mathbb{Z} + \mathbb{Z}\tau$, so that

$$\begin{aligned}\mathbb{Z}[\tau] &= \mathbb{Z} + \mathbb{Z}\tau \\ &= \left\{ \frac{u + v\sqrt{D}}{2} : u, v \in \mathbb{Z}, u \equiv vD \pmod 2 \right\}.\end{aligned}$$

In what follows, we write $\mathcal{O}_D$ (for "order of discriminant D") in place of $\mathbb{Z}[\tau]$.

Our aim with this note is to showcase a simple proof of the following criterion for unique factorization in $\mathcal{O}_D$. We remind the reader that if R is a domain then $\pi \in R$ is *irreducible* if π is nonzero and not a unit, and if whenever $\pi = \alpha\beta$ with $\alpha, \beta \in R$, either α or β is a unit. The element $\pi \in R$ is *prime* if π is nonzero and not a unit, and if whenever $\pi \mid \alpha\beta$ (with $\alpha, \beta \in R$) either $\pi \mid \alpha$ or $\pi \mid \beta$; equivalently, a prime is a nonzero element of R for which the principal ideal (π) is a prime ideal of R. Prime elements are always irreducible; the converse holds in a UFD (unique factorization domain), but not in general.

Theorem 1. *Suppose that every rational prime number*

$$p \le \begin{cases} \sqrt{|D|/3} & \text{if } D < 0, \\ \sqrt{D/5} & \text{if } D > 0 \end{cases} \tag{1}$$

that is irreducible in $\mathcal{O}_D$ is also prime in $\mathcal{O}_D$. Then $\mathcal{O}_D$ is a unique factorization domain.

1.1. Examples.

(i) $[D = 73]$ Since $\sqrt{73/5} = 3.8\ldots$, the conditions of Theorem 1 concern only the primes $p = 2$ and $p = 3$. Neither 2 nor 3 is irreducible, since

$$2 = \frac{9+\sqrt{73}}{2} \cdot \frac{9-\sqrt{73}}{2}, \quad \text{while} \quad 3 = (2\sqrt{73} + 17) \cdot (2\sqrt{73} - 17).$$

(It is easy to check that all of the factors listed here are nonunits.) We conclude that $\mathcal{O}_D = \mathbb{Z}[\frac{1+\sqrt{-73}}{2}]$ is a UFD.

The number 73 is not particularly special.[1] It is widely believed that there are infinitely many $D > 0$ for which $\mathcal{O}_D$ is a UFD. In fact, Cohen and Lenstra have precise conjectures predicting, for instance, that $\mathcal{O}_p$ is a UFD for 75.44... % of primes $p \equiv 1 \pmod 4$ (see [2, §5.10] and [3, 4, 20]).

(ii) $[D = -163]$ Since $\sqrt{163/3} = 7.3\ldots$, we must check $p = 2, 3, 5, 7$. As $\tau = \frac{1+\sqrt{-163}}{2}$ is a root of the monic irreducible polynomial $X^2 - X + 41$, we have that $\mathbb{Z}[\tau] \cong \mathbb{Z}[x]/(X^2 - X + 41)$. Hence, for each prime p,

$$\mathbb{Z}[\tau]/(p) \cong (\mathbb{Z}[X]/(p))/(X^2 - X + 41) \cong \mathbb{F}_p[x]/(X^2 - X + 41).$$

It is straightforward to check that $X^2 - X + 41$ is irreducible modulo p for each of $p = 2, 3, 5, 7$. (For the odd primes p in this list, it suffices to observe that the discriminant -163 of $X^2 - X + 41$ is a nonsquare mod p.) Therefore, $\mathbb{Z}[\tau]/(p)$ is a field, whence (p) is a prime ideal of $\mathcal{O}_D$ and p is a prime element. So the criterion of Theorem 1 is again satisfied and $\mathcal{O}_D$ is a UFD. The number -163 *is* special; as shown by Heegner, it is the largest (in absolute value) negative D for which $\mathcal{O}_D$ is a UFD ([9]; see also [5]).

We do not claim that Theorem 1 is new. When $\mathcal{O}_D$ is the full collection of algebraic integers inside $\mathbb{Q}(\sqrt{D})$ (the so-called "maximal order"), basic algebraic number theory says that $\mathcal{O}_D$ is a Dedekind domain with finite class group. Furthermore, results from the geometry of numbers imply that every ideal class is represented by an ideal with norm bounded by the quantities appearing on the right of (1) (see [1, Theorem 13.7.10, p. 399] for $D < 0$ and [2, Exercise 17, p. 300] for $D > 0$). So Theorem 1 follows easily (in this case).

It seems of some interest — e.g., for the teaching of basic courses in algebra and number theory — to give a proof of Theorem 1 requiring as little machinery as possible. Several close relatives of Theorem 1 have been proved in the literature without reference to algebraic number theory; see [6, 8, 10, 14, 15, 17, 19, 21, 22]. However, all of these papers either establish results weaker or less complete than Theorem 1, or their proofs depend on auxiliary results from the geometry of numbers or the theory of Diophantine approximation. (For example, the beautifully simple method of Ramirez V. in [17] gives a very satisfactory result when $D < 0$, but only a partial result for $D > 0$.) Apart from a few easy lemmas concerning the "norm" map (see the Notation section below), our proof of Theorem 1 is self-contained, resting only on the commutative ring theory seen in a first graduate algebra course.

Notation. We let K be the fraction field of $\mathcal{O}_D$, so that $K = \mathbb{Q}(\sqrt{D})$, and we denote conjugation in K with a bar. The *norm* of $\alpha \in K$, denoted $N(\alpha)$, is defined by $N(\alpha) = \alpha\bar{\alpha}$. We recall that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in K$, that the norm sends nonzero elements of $\mathcal{O}_D$ to nonzero integers, and that α is a unit of $\mathcal{O}_D$ if and only if $N(\alpha) = \pm 1$. Readers are invited to prove these results themselves; alternatively, they may consult, e.g., [11, Chapter 2].

2. Proof of Theorem 1.

Our proof makes crucial use of the following lemma, which also features in the arguments of [8, 15, 17, 19, 21, 22].

Lemma 2. *Let $\alpha \in \mathcal{O}_D$. If $N(\alpha) = \pm p$, where p is a rational prime, then α is prime in $\mathcal{O}_D$.*

[1] See [13] for a counterpoint to this claim.

Proof. Since $\alpha\bar{\alpha} = \pm p$, there is a canonical surjection $\mathcal{O}_D/(p) \twoheadrightarrow \mathcal{O}_D/(\alpha)$. Since $\bar{\alpha}$ is not a unit, the corresponding kernel is nontrivial (containing, e.g., $\alpha \bmod p$). Thus, $\#\mathcal{O}_D/(\alpha)$ is a proper divisor of $\#\mathcal{O}_D/(p) = p^2$. (The last equality comes from noting that $a + b\tau$, for $0 \le a, b < p$, form a complete residue system mod p.) Since α is not a unit, $\#\mathcal{O}_D/(\alpha) > 1$. Therefore, $\#\mathcal{O}_D/(\alpha) = p$, and so $\mathcal{O}_D/(\alpha) \cong \mathbb{F}_p$. Hence, (α) is a prime (in fact, maximal) ideal of $\mathcal{O}_D$, so that α is prime in $\mathcal{O}_D$. □

We turn now to the proof of Theorem 1. A simple induction on $|N(\alpha)|$ shows that every nonzero, nonunit $\alpha \in \mathcal{O}_D$ has a factorization into irreducibles. So it remains only to prove uniqueness. We reduce this (as in [15, 19, 22]) to the following claim.

Claim. *Every prime in $\mathbb{Z}$ factors as a product of primes in $\mathcal{O}_D$.*

To see why this suffices, recall that an element with a factorization into primes necessarily has this as its only factorization into irreducibles (up to order and unit factors). This is clear from the usual proof of unique factorization in a Euclidean domain or PID (compare with the proof of Proposition 12.2.14(a) in [1]). Since every rational integer larger than 1 factors as a product of rational primes, our claim implies that all those integers factor uniquely in $\mathcal{O}_D$. But this implies that every $\alpha \in \mathcal{O}_D$, not zero and not a unit, also factors uniquely: If α had two factorizations, we could cook up two factorizations of $|N\alpha| = \pm\alpha\bar{\alpha}$ by concatenating our factorizations of α with a fixed factorization of $\pm\bar{\alpha}$.

Proof of the claim. Assuming the claim to be false, let p be the smallest prime for which it fails. Then

$$p > \begin{cases} \sqrt{|D|/3} & \text{when } D < 0, \\ \sqrt{D/5} & \text{when } D > 0. \end{cases} \tag{2}$$

Indeed, suppose otherwise. Since p does not factor as a product of primes, it itself is not prime. But then the hypothesis of Theorem 1 tells us that p factors nontrivially in $\mathcal{O}_D$. Write $p = \pi_1 \cdots \pi_k$, with $k \ge 2$ and all the π_i irreducible. Taking norms, $p^2 = N(\pi_1) \cdots N(\pi_k)$, and so $k = 2$ and $N(\pi_1) = N(\pi_2) = \pm p$. By Lemma 2, both π_1 and π_2 are prime, and so p factors into primes after all, an absurdity.

Let

$$m(X) = X^2 - \sigma X + \frac{\sigma - D}{4} \in \mathbb{Z}[X]$$

be the minimal polynomial of τ. Then $\mathbb{Z}[\tau] \cong \mathbb{Z}[X]/(m(X))$ and $\mathbb{Z}[\tau]/(p) \cong \mathbb{F}_p[X]/(m(X))$. Since p is not prime in $\mathcal{O}_D$, the quotient ring $\mathbb{Z}[\tau]/(p)$ is not a field, and so $m(X)$ factors nontrivially over $\mathbb{F}_p$. Thus, for some integers x and x',

$$m(X) \equiv (X - x)(X - x') \pmod{p}. \tag{3}$$

Comparing coefficients of X on both sides, we find that $x + x' \equiv \sigma \pmod{p}$, and so we can assume that

$$\frac{p + \sigma}{2} \le x \le p \quad \text{if } D > 0, \qquad \text{and} \qquad \sigma \le x \le \frac{p + \sigma}{2} \quad \text{if } D < 0.$$

By (3), $m(x) \equiv 0 \pmod{p}$. Moreover, our inequalities for x guarantee that

$$|m(x)| < p^2.$$

Indeed, if $D > 0$, then (keeping in mind (2))

$$p^2 > m(x) = \left(x - \frac{\sigma}{2}\right)^2 - \frac{D}{4} \ge \frac{p^2 - D}{4} > -p^2,$$

while if $D < 0$, then

$$0 < m(x) = \left(x - \frac{\sigma}{2}\right)^2 + \frac{|D|}{4} \leq \frac{p^2 + |D|}{4} < p^2.$$

Write $m(x) = pr$, where $|r| < p$. By the minimality of p, every prime dividing r factors into primes of $\mathcal{O}_D$, and so r itself factors, up to sign, as a product of primes of $\mathcal{O}_D$. Thus, for some primes $\eta_1, \dots, \eta_\ell$ of $\mathcal{O}_D$,

$$(x - \tau)(x - \bar{\tau}) = m(x) = \pm p\eta_1 \cdots \eta_\ell.$$

Since η_1 is prime, η_1 divides either $x - \tau$ or $x - \bar{\tau}$. Divide both sides of the equation by η_1 and continue the process with η_2. Eventually we are led to a factorization of the form

$$\frac{x-\tau}{\Pi_1} \cdot \frac{x-\bar{\tau}}{\Pi_2} = \pm p, \qquad \text{where} \qquad \Pi_1 = \prod_{i \in \mathcal{I}} \eta_i, \quad \Pi_2 = \prod_{i \in \mathcal{I}^c} \eta_i$$

for some $\mathcal{I} \subset \{1, 2, \dots, k\}$, where $\mathcal{I}^c = \{1, 2, \dots, k\} \setminus \mathcal{I}$. Multiplying by ± 1 if necessary, we obtain a factorization of p as $\alpha\beta$, say. If α or β is a unit, then the other is a unit multiple of p. But that implies $p \mid x - \tau$ or $p \mid x - \bar{\tau}$, which is absurd. (Both $\{1, \tau\}$ and $\{1, \bar{\tau}\}$ are $\mathbb{Z}$-module bases of $\mathcal{O}_D$, and so when a multiple of p is written as $a + b\tau$ or $a + b\bar{\tau}$, both a and b must be multiples of p.) So α, β are nonunits. Now taking norms shows that $N\alpha = N\beta = \pm p$, so that α, β are prime by Lemma 2. Thus, p has a factorization into primes of $\mathcal{O}_D$ after all, contradicting the choice of p. $\square$

Remark. In 1912/1913, Frobenius [7] and Rabinowitsch [16] (independently) published the following striking result: For each integer $q \geq 2$,

$$x^2 - x + q \text{ is prime for all integers } 0 < x < q \quad \text{if and only if} \quad \mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{1 - 4q})] \text{ is a UFD;}$$

see [12, Chapter 11] for an exposition. For example, since $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-163})]$ is a UFD, the polynomial $x^2 - x + 41$ assumes prime values for $x = 1, 2, \dots, 40$. The "only if" half of the proof is the more difficult of the two, and for this most modern treatments fall back on the theory of the class group. Theorem 1 allows one to fashion a completely elementary proof (apply Theorem 1 in place of Proposition 11.13 in [12]; alternatively, Ramirez V.'s Theorem 3.1 from [17] can be used). Indeed, these arguments prove a sharper version of the forward direction, which has the following consequence: $x^2 - x + 41$ being prime for just $x = 1, 2, 3, 4$ implies that $x^2 - x + 41$ must continue being prime all the way to $x = 40$. Certain relatives of Rabinowitsch's theorem for real quadratic orders can be given elementary proofs in a parallel way (compare with [18]).

Acknowledgements. The authors are supported by the National Science Foundation (NSF) under awards DMS-2001581 (P. P.) and DMS-1454767/DMS-2000093 (N. S.). They thank Enrique Treviño and the referees for helpful suggestions. In particular, they are grateful to a referee for pointing out that the argument applies for orders other than the maximal one.

References

[1] Artin, M. (2011). *Algebra*. 2nd ed. Boston: Prentice Hall.

[2] Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics, Vol. 138. Berlin: Springer-Verlag.

[3] Cohen, H., Lenstra, Jr., H. W. (1984). Heuristics on class groups. In: Chudnovsky, D. V., Chudnovsky, G. V., Cohn, H., Nathanson, M. B., eds. *Number Theory (New York, 1982)*. Lecture Notes in Math, Vol. 1052. Berlin: Springer, pp. 26–36.

[4] Cohen, H., Lenstra, Jr., H. W. (1984). Heuristics on class groups of number fields. In: Jager, H., ed. *Number Theory (Noordwijkerhout, 1983)*. Lectures Notes in Math, Vol. 1068. Berlin: Springer, pp. 33–62.

[5] Cox, D. A. (2013). *Primes of the Form* $x^2 + ny^2$, 2nd ed. Pure and Applied Mathematics. Hoboken, NJ: John Wiley & Sons.

[6] Fendel, D. (1985). Prime-producing polynomials and principal ideal domains. *Math. Mag.* 58(4): 204–210. doi.org/10.2307/2689515

[7] Frobenius, F. G. (1912). Über quadratische Formen, die viele Primzahlen darstellen. *Sitzungsber. d. Kgl. Preuß. Akad. Wiss. Berlin*: 966–980.

[8] Gyarmati, E. (1983). A note on my paper: "Unique prime factorization in imaginary quadratic number fields". *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* 26: 195–196.

[9] Heegner, K. (1952). Diophantische Analysis und Modulfunktionen. *Math. Z.* 56: 227–253. doi.org/10.1007/BF01174749

[10] Lánczi, E. (1965). Unique prime factorization in imaginary quadratic number fields. *Acta Math. Acad. Sci. Hungar.* 16: 453–466. doi.org/10.1007/BF01904852

[11] Lehman, J. L. (2019). *Quadratic Number Theory*. Dolciani Mathematical Expositions. Providence, RI: American Mathematical Society/MAA Press.

[12] Pollack, P. (2017). *A Conversational Introduction to Algebraic Number Theory*. Student Mathematical Library, Vol. 84. Providence, RI: American Mathematical Society.

[13] Pomerance, C., Spicer, C. (2019). Proof of the Sheldon conjecture. *Amer. Math. Monthly*. 126(8): 688–698. doi.org/10.1080/00029890.2019.1626672

[14] Popovici, C. P. (1957). Criteria for the uniqueness of prime factorization in imaginary rings of quadratic integers. *Acad. R. P. Romîne. Bul. Şti. Secţ. Şti. Mat. Fiz.* 9: 5–17.

[15] Popovici, C. P. (1957). On uniqueness of decomposition into prime factors in rings of quadratic integers. *Bull. Math. Soc. Sci. Math. Phys. R. P. Roumaine (N.S.)*. 1(49): 99–120.

[16] Rabinowitsch, G. (1913). Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkörpern. *J. Reine Angew. Math.* 142: 153–164.

[17] Ramírez V., V. J. (2016). A new proof of the unique factorization of $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ for $d = 3, 7, 11, 19, 43, 67, 163$. *Rev. Colombiana Mat.* 50(2): 139–143. doi.org/10.15446/recolma.v50n2.62206

[18] Ramírez V., V. J. (2019). A simple criterion for the class number of a quadratic number field to be one. *Int. J. Number Theory* 15(9): 1857–1862. doi.org/10.1142/S1793042119501033

[19] Snyder, N. (2007). The Minkowski bound. Blog post. sbseminar.wordpress.com/2007/08/16/the-minkowski-bound/

[20] te Riele, H., Williams, H. (2003). New computations concerning the Cohen-Lenstra heuristics. *Experiment. Math.* 12(1): 99–113.

[21] Zaupper, T. (1983). A note on unique factorization in imaginary quadratic fields. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* 26: 197–203.

[22] Zaupper, T. (1990). Unique factorization in quadratic number fields. *Studia Sci. Math. Hungar.* 25(4): 437–445.

Department of Mathematics, University of Georgia, Athens, GA 30602
Email address: pollack@uga.edu

Department of Mathematics, Indiana University, Bloomington, IN 47405
Email address: nsnyder1@indiana.edu