DOI: 10.2478/auom-2014-0010
An. Şt. Univ. Ovidius Constanţa
VERSITA
Vol. 22(1),2014, 121–125

Euclidean quotient rings of $\mathbb{Z}[\sqrt{-5}]$

Tiberiu Dumitrescu and Alexandru Gica

Abstract

For a prime p, we prove elementarily that the ring $\mathbb{Z}[\sqrt{-5}, 1/p]$ is Euclidean if and only if it is a PID iff $p = 2$ or p is congruent to 3 or 7 modulo 20.

1 Introduction

Recall that an integral domain D is called *Euclidean* if there exists a map $f : D \to \mathbb{N}$ such that $f^{-1}(0) = \{0\}$ and for all $a, b \in D - \{0\}$, there is a $q \in D$ such that $f(a - bq) < f(b)$ (see [4]). It is a classical result (see for instance [4]) that there exist only five quadratic imaginary fields which have Euclidean rings of integers, namely $\mathbb{Q}(\sqrt{d})$, where

$$-d = 1, 2, 3, 7, 11.$$

It is well-known that an Euclidean domain is a principal ideal domain (PID), but the converse is not true (see for instance [1], [2]).

The ring $\mathbb{Z}[\sqrt{-5}]$ is an easy exemple of a ring of algebraic integers which is not a PID. The purpose of this note is to find *by elementary means* those natural primes p such that the ring of quotients $\mathbb{Z}[\sqrt{-5}, 1/p]$ is Euclidean.

Note that this problem can be rather easily solved using strong results of Algebraic Number Theory and supposing that some generalized Riemann hypotheses are true. Let $\mathbb{Q}(\sqrt{d})$ be a quadratic imaginary field and D its ring of integers. By Lenstra's Theorem [5, Theorem 9.1], $D[1/p]$ is a PID if and

Key Words: Euclidean domain, PID.
2010 Mathematics Subject Classification: 13F07, 13F10.
Received: August, 2013.
Revised: September, 2013.
Accepted: September, 2013.

only if it is Euclidean (supposing that some generalized Riemann hypotheses are true). Therefore $\mathbb{Z}[\sqrt{-5}, 1/p]$ is a PID if and only if it is Euclidean (under the above suppositions).

By Minkowski bound arguments, it can be shown that the class group of $\mathbb{Z}[\sqrt{-5}]$ is cyclic of order two. So $\mathbb{Z}[\sqrt{-5}, 1/p]$ is a PID if and only if $p = 2$ or p is odd and $p\mathbb{Z}[\sqrt{-5}]$ is a product of two non-principal prime ideals (see for instance [3, Theorem 40.4]). The last condition holds if and only if $p \equiv 3, 7 \pmod{20}$.

2 Results

The main result of this note (Theorem 2.8) shows that, for a prime number p, $\mathbb{Z}[\sqrt{-5}, 1/p]$ is Euclidean if and only if it is a PID if and only if $p = 2$ or p is congruent to 3 or 7 modulo 20. The proof is elementary and there is no reference to any generalized Riemann hypotheses. Throughout this note, the terminology and notations are standard as in [1] or [3].

Proposition 2.1. *Let p be a prime number. If $\mathbb{Z}[\sqrt{-5}, 1/p]$ is a PID, then $p = 2$ or p is congruent to 3 or 7 modulo 20.*

Proof. We may suppose that $p > 2$. Set $D = \mathbb{Z}[\sqrt{-5}]$ and assume that $D[1/p]$ is a PID. If -5 is not a quadratic residue modulo p, then p is a prime element of D (because $D/(p) \simeq \mathbb{F}_{p^2}$), so Nagata's Theorem (see for instance [6, section 4]) shows that D is a PID, a contradiction. The same argument can be used when $p = 5$, because $D[1/5] = D[1/\sqrt{-5}]$ and $\sqrt{-5}$ is a prime element of D (since $D/(\sqrt{-5}) \simeq \mathbb{F}_5$). Hence -5 is a quadratic residue modulo p and $p \neq 5$, that is, $p \equiv 1, 3, 7, 9 \pmod{20}$ (a fact easily seen by quadratic reciprocity). Assume that $p \equiv 1, 9 \pmod{20}$. Note that 2 is not prime in $D[1/p]$, because $D[1/p]/(2) \simeq \mathbb{Z}_2[X]/(X + \overline{1})^2$. In order to complete the proof, it suffices to show that 2 is irreducible in $D[1/p]$. Deny. From a proper factorization of 2, we derive the existence of integers m, n, t, $t \geq 0$, such that $2p^t = m^2 + 5n^2$. As $p \equiv 1, 9 \pmod{20}$, we get $2p^t \equiv 2, 3 \pmod{5}$ and $m^2 + 5n^2 \equiv 0, 1, 4 \pmod{5}$, a contradiction. $\square$

Proposition 2.2. *If p is a prime number congruent to 3 or 7 modulo 20, then $3p = a^2 + 5b^2$ for some integers a, b.*

Proof. Since $9 = 2^2 + 5$, we may suppose that $p > 3$. As $p \equiv 3, 7 \pmod{20}$, $m^2 \equiv -5 \pmod{p}$ for some integer m. Consider set $\Gamma = \{x + my \mid x, y \in \mathbb{Z}, 0 \leq x < \sqrt{2p}$ and $0 \leq y < \sqrt{p/2}\}$. Let $[\ ]$ denote the floor function. Note that there are $([\sqrt{2p}]+1)([\sqrt{p/2}]+1) > \sqrt{2p}\sqrt{p/2} = p$ pairs (x, y) of integers with $0 \leq x < \sqrt{2p}$, $0 \leq y < \sqrt{p/2}$. By Pigeon-hole Principle, there exists two distinct pairs (x, y) and (x', y') with $0 \le x, x' < \sqrt{2p}$ and $0 \le y, y' < \sqrt{p/2}$ such that $x + my \equiv x' + my' \pmod{p}$. Set $a = x - x'$ and $b = y - y'$. Then $a + mb \equiv 0 \pmod{p}$. So $0 \equiv a^2 - m^2b^2 \equiv a^2 + 5b^2 \pmod{p}$, because $m^2 \equiv -5 \pmod{p}$. Since $(a, b) \neq 0$, $|a| < \sqrt{2p}$ and $|b| < \sqrt{p/2}$, we have $0 < a^2 + 5b^2 < 2p + 5p/2 < 5p$, hence $a^2 + 5b^2 = kp$ for some integer k between 1 and 4. If k is 1 or 4, then $kp \equiv 2, 3 \pmod{5}$ and $a^2 + 5b^2 \equiv 0, 1, 4 \pmod{5}$, a contradiction. Assume that $a^2 + 5b^2 = 2p$. It follows that a, b are odd. Then $c = (a + 5b)/2$ and $d = (a - b)/2$ are integers and $c^2 + 5d^2 = (3/2)(a^2 + 5b^2) = 3p$. □

Let p be a prime number. It is well-known that the map $\phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$ given by $\phi(z) = |z|^2$ is multiplicative. Consider also the multiplicative map $\nu_p : \mathbb{N} \to \mathbb{N}$ given by $p^k n \mapsto n$, where p does not divide n. Then $N = N_p = \nu_p \phi$ is a multiplicative map. N can be extended canonically to a multiplicative map $N : \mathbb{Q}(\sqrt{-5}) \to \mathbb{Q}$. After this extension, N restricts to a map $\mathbb{Z}[\sqrt{-5}, 1/p] \to \mathbb{N}$. Note that if z is a nonzero element of $\mathbb{Z}[\sqrt{-5}, 1/p]$, $N(z)$ is the cardinality of the factor ring $\mathbb{Z}[\sqrt{-5}, 1/p]/(z)$.

We say that the domain $\mathbb{Z}[\sqrt{-5}, 1/p]$ is *norm Euclidean* if it is Euclidean with respect to N. Also, we say that $x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is a *p-critical point*, if p divides $x^2 + 5y^2$.

Proposition 2.3. *Let p be a prime number. Assume that for every $z \in \mathbb{Q}(\sqrt{-5})$, there exists a p-critical point $t \in \mathbb{Z}[\sqrt{-5}]$ such that $|z - t| < \sqrt{p}$. Then $\mathbb{Z}[\sqrt{-5}, 1/p]$ is norm Euclidean.*

Proof. Set $D = \mathbb{Z}[\sqrt{-5}, 1/p]$. It suffices to show that for every $z \in \mathbb{Q}(\sqrt{-5}) - \{0\}$, there exists $t \in D$ such that $N(z - t) < 1$. Indeed, if $\alpha, \beta \in D - \{0\}$ and $\gamma \in D$ is chosen such that $N(\alpha/\beta - \gamma) < 1$, then $N(\alpha - \beta\gamma) = N(\beta)N(\alpha/\beta - \gamma) < N(\beta)$. Now let $z \in \mathbb{Q}(\sqrt{-5}) - \{0\}$ and let us look for a $t \in D$ such that $N(z - t) < 1$. Write $z = (a + b\sqrt{-5})/c$ with a, b, c integers, $c \neq 0$. Since $N(z - t) = N(zp - tp)$ and $tp \in D$ whenever $t \in D$, we may assume that c is not divisible by p. Moreover, multiplying by some power of c, we may assume that c is congruent to 1 modulo p. By hypothesis, there exists a p-critical point $x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that $|(a + b\sqrt{-5} - z) - (x + y\sqrt{-5})| < \sqrt{p}$. So $|z - t| < \sqrt{p}$, where $t = (a - x) + (b - y)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Moreover, $z - t = (1/c)((a - ca + cx) + (b - cb + cy)\sqrt{-5})$ and $(a - ca + cx)^2 + 5(b - cb + cy)^2$ is a multiple of p because $x + y\sqrt{-5}$ is a p-critical point and $c \equiv 1 \pmod{p}$. Hence $N(z - t) \le |z - t|^2/p < p/p = 1$. □

Lemma 2.4. *Let p be a prime number and $x_j + y_j\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, $j = 1, 2$, two p-critical points. If p divides $x_1x_2 + 5y_1y_2$, then $k_1(x_1 + y_1\sqrt{-5}) + k_2(x_2 + y_2\sqrt{-5})$ is a p-critical point for every integers k_1, k_2.*

Proof. Simply note that $(k_1x_1 + k_2x_2)^2 + 5(k_1y_1 + k_2y_2)^2 = k_1^2(x_1^2 + 5y_1^2) + k_2^2(x_2^2 + 5y_2^2) + 2k_1k_2(x_1x_2 + 5y_1y_2)$ is divisible by p. □

Proposition 2.5. *Let p be a prime number. Assume there exist two distinct nonzero p-critical points $z_j = x_j + y_j\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, $j = 1, 2$, such that*

(1) *p divides $x_1x_2 + 5y_1y_2$,*

(2) *the triangle Oz_1z_2 has circumscribed circle radius less than $\sqrt{p}$.*

Then $\mathbb{Z}[\sqrt{-5}, 1/p]$ is norm Euclidean.

Proof. By (1) and Lemma 2.4, we have the lattice of p-critical points $k_1z_1 + k_2z_2$, $k_1, k_2 \in \mathbb{Z}$. The open discs of radius $\sqrt{p}$ centered in the vertices of this lattice cover the plane, because the open discs of radius $\sqrt{p}$ centered in O, z_1, z_2, $z_1 + z_2$ cover the parallelogram $Oz_1z_2(z_1 + z_2)$, cf. (2). Apply Proposition 2.3. □

Lemma 2.6. *A triangle whose sides measure $\sqrt{3}$, $\sqrt{3}$ and $\sqrt{2}$ has circumscribed circle radius equal to $3/\sqrt{10}$, so less than 1.*

Proof. By Heron's formula, the area is $S = (1/4)[(2 + 3 + 3)^2 - 2(2^2 + 3^2 + 3^2)]^{1/2} = \sqrt{5}/2$, so the circumscribed circle radius is $(\sqrt{3}\sqrt{3}\sqrt{2})/(4S) = 3/\sqrt{10}$. □

Proposition 2.7. *If $p = 2$ or p is a prime number congruent to 3 or 7 modulo 20, then $\mathbb{Z}[\sqrt{-5}, 1/p]$ is norm Euclidean.*

Proof. We use Proposition 2.5. Assume that $p \equiv 3, 7 \pmod{20}$ and $p > 3$. By Proposition 2.2, $3p = a^2 + 5b^2$ for some integers a, b. We consider two cases. Case (i): $a \equiv b \pmod 3$. Then $z_1 = a + b\sqrt{-5}$ and $z_2 = (2a - 5b)/3 + ((a + 2b)/3)\sqrt{-5}$ are in $\mathbb{Z}[\sqrt{-5}]$. Note that $z_1 \neq z_2$, otherwise we get $2a^2 = p$, a contradiction. We have $|z_1|^2 = a^2 + 5b^2 = 3p$, $|z_2|^2 = (1/9)((2a - 5b)^2 + 5(a + 2b)^2) = (1/9)(9a^2 + 45b^2) = 3p$ and $|z_1 - z_2|^2 = (1/9)((a + 5b)^2 + 5(b - a)^2) = (1/9)(6a^2 + 30b^2) = 2p$. Hence z_1, z_2 are p-critical points and the sides of triangle Oz_1z_2 are $\sqrt{3p}$, $\sqrt{3p}$, $\sqrt{2p}$. By Lemma 2.6, the triangle Oz_1z_2 has circumscribed circle radius $< \sqrt{p}$, so condition (2) of Proposition 2.5 holds. Condition (1) of Proposition 2.5 also holds because, using the notations there, $x_1x_2 + 5y_1y_2 = a(2a - 5b)/3 + 5b(a + 2b)/3 = (2a^2 + 10b^2)/3 = 2p$.

Case (ii): $a \not\equiv b \pmod 3$, that is, $a + b \equiv 0 \pmod 3$. Then $z_1 = a + b\sqrt{-5}$ and $z_2 = (2a + 5b)/3 + ((2b - a)/3)\sqrt{-5}$ are in $\mathbb{Z}[\sqrt{-5}]$. Note that $z_1 \neq z_2$, otherwise we get $2a^2 = p$, a contradiction. We have $|z_1|^2 = a^2 + 5b^2 = 3p$, $|z_2|^2 = (1/9)((2a+5b)^2 + 5(2b-a)^2) = (1/9)(9a^2 + 45b^2) = 3p$ and $|z_1 - z_2|^2 = (1/9)((a-5b)^2 + 5(a+b)^2) = (1/9)(6a^2 + 30b^2) = 2p$. Hence z_1, z_2 are p-critical points and and the sides of triangle Oz_1z_2 are $\sqrt{3p}$, $\sqrt{3p}$, $\sqrt{2p}$. By Lemma 2.6, the triangle Oz_1z_2 has circumscribed circle radius $< \sqrt{p}$, so condition (2) of Proposition 2.5 holds. Condition (1) of Proposition 2.5 also holds because, using the notations there, $x_1x_2 + 5y_1y_2 = a(2a + 5b)/3 + 5b(2b - a)/3 = (2a^2 + 10b^2)/3 = 2p$.

Similar arguments can be used if p is 2 or 3. When $p = 2$, we set $z_1 = 1 + \sqrt{-5}$, $z_2 = 2$ and we have $|z_1|^2 = 6 = 3p$, $|z_2|^2 = 4 = 2p$ and $|z_1 - z_2|^2 = 6 = 3p$. When $p = 3$, we set $z_1 = 1 + \sqrt{-5}$, $z_2 = 3$ and we have $|z_1|^2 = 6 = 2p$, $|z_2|^2 = 9 = 3p$ and $|z_1 - z_2|^2 = 9 = 3p$. □

Putting Propositions 2.1 and 2.7 together, we have

Theorem 2.8. *For a prime number p, the following assertions are equivalent:*
(*a*) $\mathbb{Z}[\sqrt{-5}, 1/p]$ *is norm Euclidean.*
(*b*) $\mathbb{Z}[\sqrt{-5}, 1/p]$ *is a PID.*
(*c*) $p = 2$ *or* p *is congruent to* 3 *or* 7 *modulo* 20.

Acknowledgement. The publication of this paper is supported by the grant PN-II-ID-WE-2012-4-161.

References

[1] S. Alaca and K. Williams, *Algebraic Number Theory,* Cambridge University Press, 2004.

[2] O.A. Campoli, *A principal ideal domain that is not a Euclidean domain,* Amer. Math. Monthly 95 (1988), 868-871

[3] R. Gilmer, *Multiplicative Ideal Theory*, Marcel Dekker, New York, 1972.

[4] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields,* Expositiones Mathematicae 13 (1995), 385-416.

[5] H. W. Lenstra, *On Artin's conjecture and Euclids algorithm in global fields,* Invent. Math. 42 (1977), 201-224.

[6] P. Samuel, *Unique factorization,* Amer. Math. Monthly 75 (1968), 945-952.

Tiberiu DUMITRESCU,
Faculty of Mathematics and Informatics, University of Bucharest,
14 Academiei Str.,
Bucharest, RO 010014, Romania,
Email: tiberiu@fmi.unibuc.ro

Alexandru Gica,
Faculty of Mathematics and Informatics, University of Bucharest,
14 Academiei Str.,
Bucharest, RO 010014, Romania,
Email: alexgica@yahoo.com